



Security in DME

White Paper about mobile device security with DME

Document version: 1.2
Date: 2010-06-29
Circulation/Restrictions: Internal/Excitor partners
Applies to: DME Server 3.5 and above

Table of contents

1	Security challenges of a mobile workforce.....	3
2	About DME.....	3
2.1	Features and benefits.....	3
3	Structure of the DME system	4
4	Access to corporate data	5
4.1	Exchange	5
4.2	Domino.....	6
5	Authentication	6
5.1	Client authentication	6
5.1.1	SSL connections.....	7
5.1.2	Client signatures	7
5.2	Anonymous users	8
5.3	LDAP/AD groups.....	8
5.4	Authentication on the client.....	8
5.5	Local users	9
6	Encryption	9
6.1	Notes encryption	9
6.2	S/MIME encryption	9
7	Provisioning	10
7.1	OMA DM.....	10
7.2	SMS push.....	10
8	Version control	10
9	Device management.....	10
9.1	Remote decommissioning	10
9.2	Separation of data	11
9.3	Security settings	11
9.4	Application blocking	12
10	Logs, statistics, and reports	13
11	Client differences.....	14
11.1	Remote wipe	14
11.2	The iPhone client	14
11.3	The Java client	15
11.4	The Android client.....	15
12	More information	15

1 Security challenges of a mobile workforce

Security is one of the most significant challenges facing organizations with mobile workforces. The very nature of mobile devices, their small size coupled with users' tendency to carry them everywhere, increases the likelihood of their being dropped, lost or stolen, all of which poses a significant risk to an organization's investment and data. While it might be expensive to continually replace lost or broken mobile devices, the cost multiplies if the lost or stolen devices contain sensitive corporate materials, such as documents, confidential meetings, corporate e-mail or customer information.

Thus in addition to selecting a device management system that can handle the support and administration of mobile devices, you must also select one that allows you to protect your organization from data breaches and leakage.

DME's device management and security tool takes a multi-level approach to protecting your organization's data. This ensures that no matter where the data is, it's secured via DME. And as with the other aspects of device management, the security functions can all be accessed and enabled via DME's secure web interface.

The following description of the principles behind DME's security offering takes you through the levels of DME security.

2 About DME

DME (Dynamic Mobile Exchange) offers synchronization of push e-mail, PIM information (calendar, contacts, to-dos), and optionally files, to mobile devices. It fully integrates mobile device management with state-of-the-art security and efficient software deployment. DME is a mobile client/server solution that works with mobile phones, smartphones and PDAs using Symbian, Windows Mobile, or Java as operating system, as well as Apple iPhone, Android, and BlackBerry devices. DME is developed by Excitor A/S.

DME integrates with the following collaboration systems: Lotus Domino 7.x, 8.x and Microsoft Exchange 2003, 2007, and 2010.

The solution enables large and midsize enterprises to deliver business mobility services to employees and to effectively manage and control mobile devices without compromising security. DME is device, network and operator independent and offers unparalleled TCO, unprecedented data and device security, and a very intuitive interface for users and administrators.

2.1 Features and benefits

- **Convenient for the user:** *Push e-mail, calendar, contacts and to dos*
With DME on your mobile phone, smartphone, or PDA, you get your most critical and often used office tools in your pocket wherever you are, whenever you need it. E-mails appear on your phone the moment they hit your office mailbox.
- **Quickly back in the game:** *Instant service recovery*
Should your phone get lost or stolen, a new DME client can be pushed to a new phone in a few minutes after you purchase a new DME supported phone or borrow one from someone else – no matter where it happens.
- **Fretless security:** *Mobile security policy enforcement*
E-mails are encrypted over the air and on the device itself using full encryption (AES 128-bit or stronger). Shell protection of the entire phone, requiring domain password to access all features except picking up calls, gives you further security options.
- **Freedom and ease-of-use:** *Effective control of all devices*
Gain a complete overview of your devices – regardless of make, model, or platform. Information about the device model, versions and programs installed on the device is listed in the Web-based DME control center for easy administration. Features, settings and available applications and

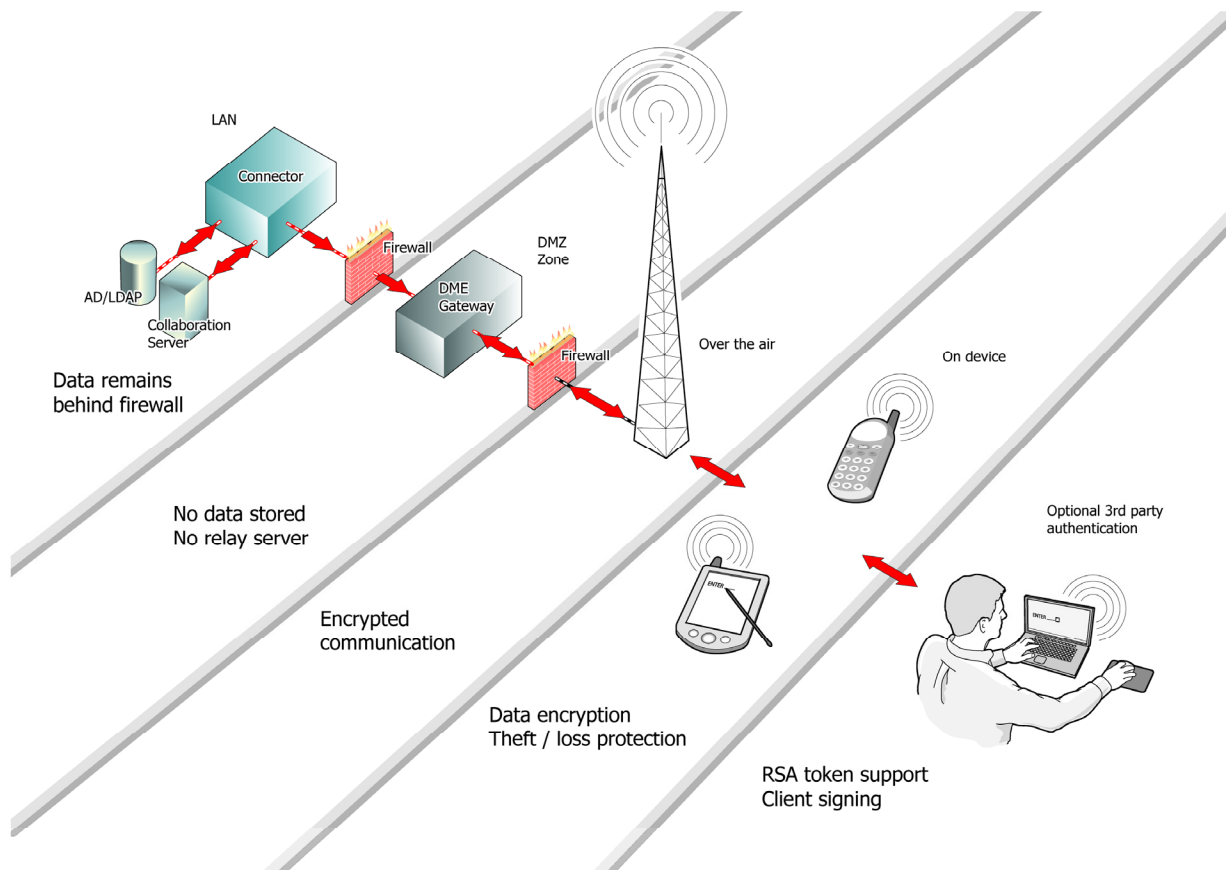
network connections are all controlled centrally and can only be changed by the users to the extent this is allowed by centrally applied security policies. Dividing the devices into groups makes it easy to change settings/features for many devices at a time.

- **Ease-of-use comes in many flavors:** *Simple support and administration*
Push software and upgrades via SMS or WAP to the users, permit them to serve themselves, or automatically upgrade software when the users log on. For support purposes, retrieval of device configurations and connection set-up makes it possible for you to help users who cannot connect, and a log of user actions assists you in identifying the problems and solving them. Notification of changes to server status can be sent to the DME administrators to ensure they are alerted to problems quickly.
- **Cost containment:** *Control of ongoing mobile cost*
Data and voice logging allows you to monitor activity levels real-time, and identify “expensive” behavior which can be reduced. Heavily-used operators can be determined and connection preferences can be set as default. Build advanced reports to get a clear view of your organization’s mobile traffic using the integrated BI reporting tools.
- **Freedom of choice:** *Versatility*
Works on any available network (WLAN/Wi-Fi, GSM, GPRS, 3G/UMTS, EDGE...), operator, and on most devices from leading manufacturers. Works on Lotus Domino and/or Microsoft Exchange collaboration systems.

Please note that the above applies to the full DME client. Note also that due to limitations specific to the iPhone platform, a few of the features mentioned above are not supported on DME for iPhone.

3 Structure of the DME system

DME secures your organization’s data from the moment it leaves the corporate collaboration system, and keeps it safe on the client devices.



The collaboration system and the Active Directory or LDAP servers are connected to the LAN, safely behind the corporate firewall. DME installs one or more *DME connectors* on the LAN and connects them to the collaboration and AD/LDAP systems.

The DME server is installed in a DMZ (“de-militarized zone”) – outside the corporate LAN, but inside the DMZ firewall. The *connectors connect to the DME server*, and maintain the connections to service devices – no connection attempts are made *by the server* into the LAN. The connection between connectors and server can be secured by HTTPS. No relay (“store-and-forward”) servers are used during data transmission. The database used by DME can be placed within the DMZ or the corporate LAN, and is only accessed by the DME server. No corporate data (in terms of e-mails etc.) are stored in the DMZ.

Communication between server and devices is heavily encrypted before being sent over the air. DME supports third party mobile VPN setups as well as token-based authentication such as RSA secure ID.

Data stored on the devices is encrypted. Each item that is viewed by the user (for instance an e-mail or an e-mail attachment) is only decrypted to memory for as long as it is displayed on the screen. When the user closes the e-mail again, the decrypted version is removed from the phone memory.

4 Access to corporate data

In order to synchronize data between mobile devices and the collaboration system, DME needs access to the corporate data stored in the collaboration system.

4.1 Exchange

The connection to the Exchange and Active Directory backend is established using available standard interfaces:

- *LDAP/LDAPS* to the AD system
- *HTTP/HTTPS* to the Exchange frontend server(s)

Encryption towards the AD server is required in order to allow changing the password from the DME client, enforcing the same AD password policy to mobile users that might be unable to change their network password from a PC / laptop.

As with any other feature, the AD password change feature can be disabled on DME if required.

The connection to the Exchange data is established using the user credentials (username and password) sent by the DME client, the same way a user logging into Outlook Web Access would be authenticated. DME supports the use of NTLM, Basic, and Form Based authentication, with or without the use of SSL.

When certificate end-user authentication is used on OWA, DME cannot currently present certificates. Therefore, a separate Exchange front-end/CAS server could be set up that allows only the DME Connector to present username and password credentials. Limitations on which IP address is allowed to connect to this dedicated frontend server can also be enforced in order to increase the security.

4.2 Domino

DME can work with Domino using two modes: DIIOP or Notes Session.

In DIIOP mode, the username and internet password are sent to get access to the mailbox. Therefore a DME user will get the same rights as an Internet user, which are different than the rights given to full Notes clients.

Note that Secure DIIOP is also an option, albeit not recommended due to a considerable performance overhead. Instead, we recommend using Notes Session mode.

In Notes Session mode, a proxy user is used. This user is sending e-mails on behalf on the real user, and is given its own Notes ID key. To the recipient, the e-mails will however appear to have come directly from the sending user, and not from the proxy user. As with any other administrative account, the appropriate policies must be enforced to make sure that this DME proxy ID is not compromised. A very strong password should also be associated with the DME proxy user ID.

The ACLs that the DME proxy user is required to have on the DME users' mailboxes are documented separately.

5 Authentication

Authentication takes places at different levels:

1. Clients that interact with the collaboration system (by synchronizing e-mail, calendar, etc.).
2. "Anonymous" clients – clients that are only used for device management.
3. Membership of a directory group.
4. Users on the client itself.
5. Local access to the DME administration web interface.

5.1 Client authentication

The DME client must be installed on the devices in order for them to access the system. A *server path* is distributed to each client, for instance <https://dme.yourcompany.com:5011>. When the client tries to connect, the user must enter his or her LDAP or AD user name and password.

If the connector that is set up to handle authentication requests is able to verify that the user exists, the password is correct, and the user is member of an LDAP group giving access to the DME service, then the user is granted access to use DME (that is, the functions for which the user has a license).

If the client logs on *for the first time*, the server can do one of three things:

1. Create the client device in DME automatically, and associate it with the user who logged in, or
2. Create the client device in DME automatically, but locked and with no user assigned to it, or

3. Inform the DME administrator that a new device has tried to get access and await administrator approval to create the device in DME.

Furthermore, the user logging in for the first time is created in the DME system as well. Depending on a setting, the new user can be locked, requiring the administrator to unlock the user. Only then can the user synchronize his or her device using DME.

As with any other system, the usual trade-off between administrative ease-of-use and security applies. The more securely and tightly you configure DME, the more administration is required.

To achieve a highly secure DME environment, it is recommended to disable the following settings:

- Auto-create users
- Auto-create devices
- Allow user to change device

... and to enable and lock the following functions/settings:

- Users locked upon creation
- Client signing activated
- Serverpath locked (to prevent another DME server from taking over control of the device)

With the above recommendations, only devices and users created by the administrator in advance are allowed in the system, and only clients and servers presenting the right client/server certificate will be able to communicate.

It also means that users cannot suddenly start using another device – an important thing to remember if client signing is used for two-factor authentication (described later in this document).

To make it easier to implement a new DME installation, DME has functionality to import existing devices, users, and the link between the two. So even though the system has been set to a high level of security, administrators can still create users and devices in batches. This could be relevant when migrating from a legacy solution, or when exporting assets from an asset management system.

When performing their initial registration with the DME server, the DME connectors will also be “locked”, meaning that they need manual release by the administrator. This means that only connectors that we know and trust are allowed to service our users.

On *Linux servers*, you can encrypt the memory paging area to further increase the security on the system. Data tunneled back and forth between devices and server could – in theory – be paged from memory onto the disk, and could – in theory – be reverse engineered to human readable form. Encrypting the paging disk area on the server will effectively remove this possible risk.

5.1.1 SSL connections

The connection between server and client is encrypted using SSL. By default, Excitor provides an Excitor-signed certificate. However, we strongly recommend that you purchase and install a certificate signed by a public Certificate Authority such as VeriSign or GlobalSign, as such certificates are implicitly accepted by all client devices.

Using the Excitor-signed certificate requires that the users accept some prompts on their device, or that the certificate is sent to the device manually through an action on the server. Some device management features also require you to use a trusted 3rd party certificate, especially for Windows Mobile. Android devices do not allow to install other root CA over the air, and must therefore use a trusted 3rd party certificate.

5.1.2 Client signatures

As an extra security feature, DME can verify the identity of each device that attempts to log on to DME in order to counter spoofing attempts. This is done through a system of public and private keys.

The server generates a key, which is sent to the device. After this, the device is required to present the key to the server every time it connects.

This verification takes place before the regular user validation against the AD/LDAP system, thus preventing potential Denial of Service (DOS) attacks on the LDAP system, where a malicious user sends

very large amounts of login attempts to the DME server – resulting in an overworked LDAP server and possible crash.

The client certificates issued are bound to the IMEI number of the devices, and cannot be moved to any other device to gain access to the DME server.

Client signing can effectively be used as a two-factor authentication, as:

- The user is not allowed to change from one device to another (without approval by the administrators). This way, the device can be seen as a separate “token” tied to the specific user.
- The device is only allowed to connect with the server if it presents the right certificate.
- The user is only allowed to communicate with the server if the correct domain password is presented.

In summary, devices are used as tokens, linked to users and the DME server. Together with LDAP username and password, all three elements must be correct to gain access.

5.2 Anonymous users

Excitor offers a basic client for a number of platforms, called the DME Basic Mobile Device Management client (“Basic MDM”). As the name implies, this client is for device management purposes only, and do not require authentication against the AD/LDAP system.

Such clients are completely disconnected from the corporate collaboration and AD/LDAP systems. The “user name” of the clients in the DME system is auto-generated, and can be changed by the administrator or the user (if permitted).

The DME server can be configured to accept only authenticated users, meaning that the Basic MDM clients mentioned above would be rejected.

5.3 LDAP/AD groups

To gain access to DME functionality, users must be member of at least one group in LDAP/AD configured to allow users access.

This is a simple and effective way of controlling which users are allowed access to the system, and to help facilitate internal service billing etc.

Using an LDAP/AD group to control access, combined with auto-creation of both users and devices will effectively make the DME server “take care of new users”, but as mentioned earlier, this is not the most secure configuration.

The following compromise is often used in the field: during the roll-out phase, devices and users are auto-created and subsequently audited. After the initial roll-out is completed, the DME server is set to not allow any new users without administrator approval.

5.4 Authentication on the client

On the client, the user can log in to the DME client without being in contact with the server. The password is verified by checking whether it can be used to decrypt a 128-bit data encryption key stored on the device. If the key can be decrypted, the password is correct; otherwise, the user is denied access to the client. It is important to stress that the user password is not stored in any form (plain text, cipher text, or as a hashed value) on the device. An attacker can only decrypt the data by performing a brute-force dictionary attack to guess the password. This operation would typically take so long time (measured in years) that any data uncovered this way would be irrelevant. Furthermore, the client typically only stores a limited amount of e-mails and calendar entries on the device, making any attack on the data even more futile.

If enabled, the DME client allows the user to change his or her corporate password from the device, enforcing the same password policy for mobile users and devices as for regular IT devices.

An extra layer of authentication can be implemented, such as RSA SecurID, for even stronger protection of the data. Based on RSA technology, the user is challenged for a one-time token that allows her/him to synchronize data for the time defined in the RSA settings.

5.5 Local users

At least one *local user* is created in the DME database. By default, the user **SYSADM** is created with administrator rights. This user has full access to the DME web administration interface.

There are three types of local users: **Administrators** (full access), **Supervisors** (with access to changing client settings for certain groups of clients), and **Users** (with access to using the DME client for synchronizing items according to his or her license).

An **Administrator** user must also be assigned as **User** in order to be able to use DME.

The DME web administration interface is accessed over a different port (typically 8080) than the regular synchronization (typically 5011). Rules can be set up to ensure access to the web administration interface even if the synchronization port is closed. Also, access to the administration web interface can be restricted to LAN IP addresses or specific IP addresses.

6 Encryption

E-mail and calendar items synchronized to the device¹ are encrypted using AES-128 bit cipher block chaining (CBC) block mode. The encryption key is randomly generated each time a new user logs on using the client. This encryption key is encrypted using a password-derived key according to the specifications set forth by RSA Security in the PKCS#5 specification (Password-Based Cryptography Standard).

The data storage also includes a message authentication code (MAC) ensuring that data hasn't been tampered with. This way the user can be certain that no data is changed or missing.

DME uses no proprietary implementation to solve authorization, authentication and encryption issues. Instead, DME is based on open secure Internet standards and proven techniques to solve these problems. This makes DME's implementation easy to evaluate as well as a fully transparent process, because no security technologies need to be hidden.

On **Symbian** devices, even stronger protection of the *entire device* can be obtained using the add-on product **SmartEncrypt**, which provides AES-256 encryption of a user-defined area of the phone memory (hard disk) or the entire phone memory.

The interaction between DME and the native application on the client can also be controlled. For instance, you can choose to keep your native calendar application completely separate from the DME calendar, or you can choose to show busy times in the native calendar also but not subject and body, or you can choose to integrate the two calendars completely. From version 3.6, you can even choose not to synchronize contacts with the native contacts application.

6.1 Notes encryption

Lotus Domino users can read, reply to, and forward e-mails that have been encrypted using Notes encryption, on their DME client. Furthermore, the users can create Notes encrypted e-mails from their devices. Notes encryption requires connectors of the Notes Session type.

6.2 S/MIME encryption

The DME server also supports S/MIME, which is an extension of the popular MIME (Multipurpose Internet Mail Extension) electronic mail standard that adds security to protect against interception and e-mail

¹ See the section *Client differences* for exceptions to this.

forgery. DME contains features to handle private S/MIME keys certificate revocation lists, and other aspects of S/MIME, enabling users to create and read S/MIME encrypted e-mails.

7 Provisioning

The DME server allows you to provision two types of software to the mobile clients: DME clients and Other software.

7.1 OMA DM

The principal method of provisioning software is through OMA DM. This requires that the devices are bootstrapped by the DME server. In connection with the bootstrap (or later), the DM process can install the DME client, access points, and bookmarks.

The administrator can monitor the progress of the OMA DM installation jobs.

7.2 SMS push

If OMA DM is not possible, the server falls back to using SMS or WAP push for provisioning software. A ticket is generated, enabling the download of one specified application. This ticket is sent to the appropriate client, which now has some time to download and install the application, until the ticket expires. By default, only the system administrator can issue such a ticket, but the role-based authorization of the server allows users to initialize application download of approved applications through the administration interface (self-provisioning).

8 Version control

In the DME server administration interface, the system administrator can quickly see which version of the DME software is running on the client. If the administrator chooses to up- or downgrade, this can be done effortlessly through the administration interface.

This way, the administrator has full control of which versions are currently in use, ensuring that potential security issues can be closed through appropriate software updates. The administrator can easily block clients that use outdated software.

9 Device management

All devices are managed from the DME web administration interface. Here, the administrator has an overview of all clients on the system. He or she is able to block devices and user accounts from accessing the system.

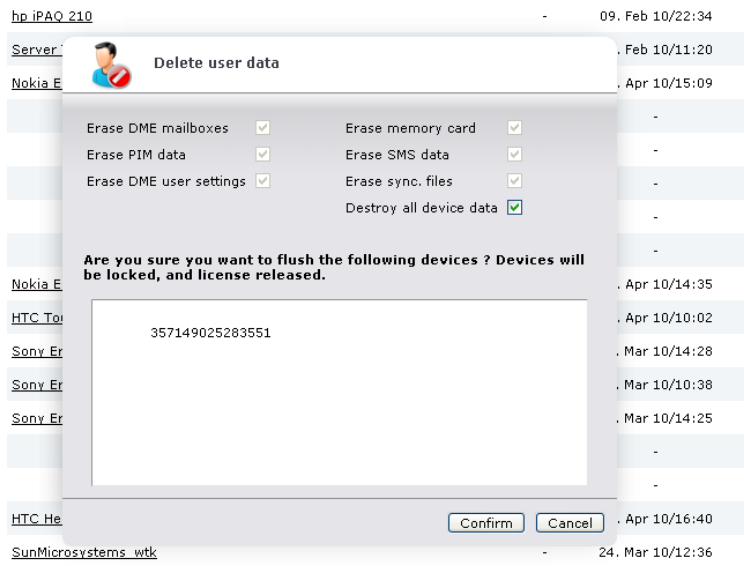
As mentioned previously, user and device accounts can automatically be created the first time a user or device connects. This leaves the system administrator with very little work setting up and installing the system for the first time. After all devices and users have been created, this auto-create feature can be turned off, ensuring that no unauthorized devices are able to connect.

Devices can be divided into groups (manually or based on existing LDAP groups) for differentiated management. Different settings can be applied to individual devices, groups of devices, or all devices (which are then the "default settings" inherited by new devices).

9.1 Remote decommissioning

In the event a mobile device is lost or stolen, the administrator can wipe a device remotely and provision a new device, so that the employee is up and running again with a minimal disruption to his or her work.

The deployment interface also handles phones that are turned in by employees who have left the organization, so that these can be wiped and reassigned quickly.



The remote wipe feature erases the device as completely as possible. The extent of the wipe varies from platform to platform. See *Client differences* for more details.

With the **Destroy all device data** option, a notification of each completed step in the wipe process is sent to the server. The server is notified by SMS, and the messages can be seen in the administration interface. This way you can see the extent to which the wipe was successful.

9.2 Separation of data

For enterprises supporting a “Bring your own device” roll-out scenario (where employees are offered corporate e-mail and PIM on their private devices), the ability to separate corporate and private data is vital – not only when the employee is still employed by the company, but also when the employee resigns from the position or simply changes phones. Using DME, administrators can be certain that removing the DME application will also effectively remove all enterprise data, without deleting private data.

This data separation is becoming more and more important, as employees are increasingly using social networks etc. to broadcast themselves and using private e-mail and calendar offerings from for instance Google on their devices. Here, neither employees nor the companies wish to get the different contacts, calendar appointments etc. mixed up and exchanged with a system outside of company control.

By using DME for e-mails, and by setting DME to use secure contacts and calendar, companies can rest assured that corporate data and private data are kept separate, and the users can rest assured that when removing the DME service from their devices, only corporate data is removed, keeping private data intact.

9.3 Security settings

Like other settings, all security settings on the devices can be controlled from the server. Through these settings, you can control

- Idle time before automatic logout of DME client
- Action on SIM card change (wipe device, lock device, none)
- Lock applications: Messaging, Calendar, Contacts, To-do, entire device (meaning that the applications mentioned cannot be launched unless you are logged in to the DME client)
- Various password strength requirements, including the use of a PIN code instead of full password
- Attachment upload and download restrictions

- ...and more.

Lock settings for				Range settings		
Device	Superuser	Name	Value	Lock	Values	Last changed
Security						
<input type="checkbox"/>	<input type="checkbox"/>	Logout timeout (min.)	10	<input checked="" type="checkbox"/>	2-20	18. Dec 09/09:00
<input type="checkbox"/>	<input type="checkbox"/>	Action on SIM card change	Lock device (Not available in DM Client)			03. Feb 10/11:35
<input type="checkbox"/>	<input type="checkbox"/>	Lock Messaging	Disabled			18. Dec 09/09:00

All settings (including non-security related settings) can be enforced by the administrator, and some of the settings can be made optional for each device user. Furthermore, some settings can be set to a default value, with a range within which the users may choose their own setting (for instance how many days back you want to synchronize your e-mail: default can be set to 5 days, letting the user choose a value between 1 and 99 days).

With this system, the administrator is free to choose the appropriate security level for each device.

9.4 Application blocking

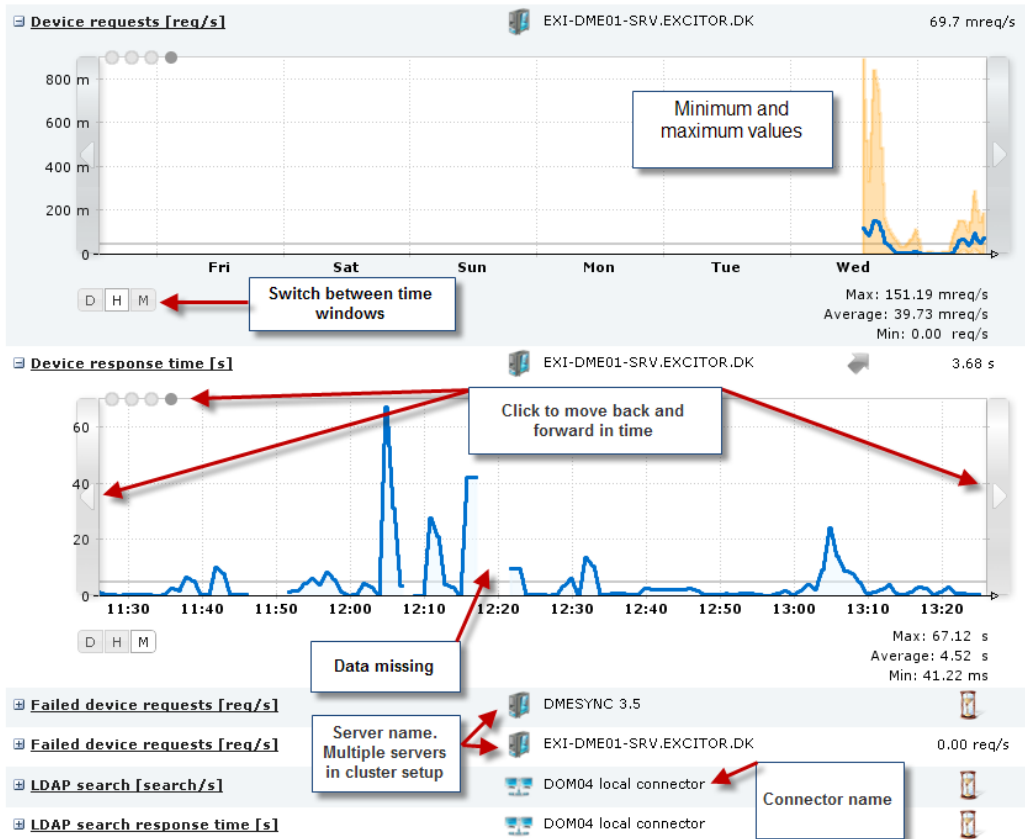
The administrator can block applications installed on the mobile device, using the DME Application Blocker, which scans each device for applications installed on the device.

Device defaults							Applications	
Block	UniqueID	Name	Type	Platforms	Last changed			
<input type="checkbox"/>	20023710	APIBridge_20023710	Application	Series 60	07. Apr 10/14:46			
<input type="checkbox"/>	101f8512	App. mgr.	Application	Series 60	14. Apr 10/11:35			
<input type="checkbox"/>	2000f85a	App. update	Application	Series 60	13. Apr 10/13:58			
<input type="checkbox"/>	com.android.providers.applications	App. mgr.	Application	Series 60	1:55			
<input type="checkbox"/>	10207983	App. update	Application	Series 60	2:30			
<input type="checkbox"/>	2000a5b6		Application	Series 60	9:24			
<input type="checkbox"/>	20017535	Asphalt4	Application	Series 60	26. Feb 10/22:30			
<input type="checkbox"/>	2001893b	Asphalt4	Application	Series 60	26. Feb 10/22:30			
<input type="checkbox"/>	sudoku.exe	Astraware Sudoku	Application	PocketPC	15. Apr 10/14:08			
<input type="checkbox"/>	at.abraxas	at.abraxas	Application	Android	04. Mar 10/11:08			
<input type="checkbox"/>	atciui.exe	ATCIUI	Application	SmartPhone	15. Apr 10/17:51			
<input type="checkbox"/>	10282bae	ateventobserverapp	Application	Series 60	09. Apr 10/15:04			
<input type="checkbox"/>	au.com.phil.minedemo	au.com.phil.minedemo	Application	Android	19. Mar 10/14:54			
<input type="checkbox"/>	audiomanager.exe	Audio Manager	Application	PocketPC SmartPhone	15. Apr 10/14:24			
<input type="checkbox"/>	1020745a	Audio message	Application	Series 60	13. Apr 10/13:58			
<input type="checkbox"/>	10208ac2	Barcode	Application	Series 60	09. Apr 10/15:04			
<input type="checkbox"/>	bejeweled2.exe	Bejeweled 2	Application	PocketPC	15. Apr 10/14:08			
<input type="checkbox"/>	benudigital.vectronfree	benudigital.vectronfree	Application	Android	13. Apr 10/13:39			
<input type="checkbox"/>	10201b00	Besk	Application	Series 60	14. Apr 10/14:35			
<input type="checkbox"/>	2000459c	bglisten	Application	Series 60	18. Mar 10/12:26			

For instance, the Control Panel and the Installer can be disabled, preventing the user from changing the settings and installing new programs, or the Bluetooth connection can be disabled on the device.

10 Logs, statistics, and reports

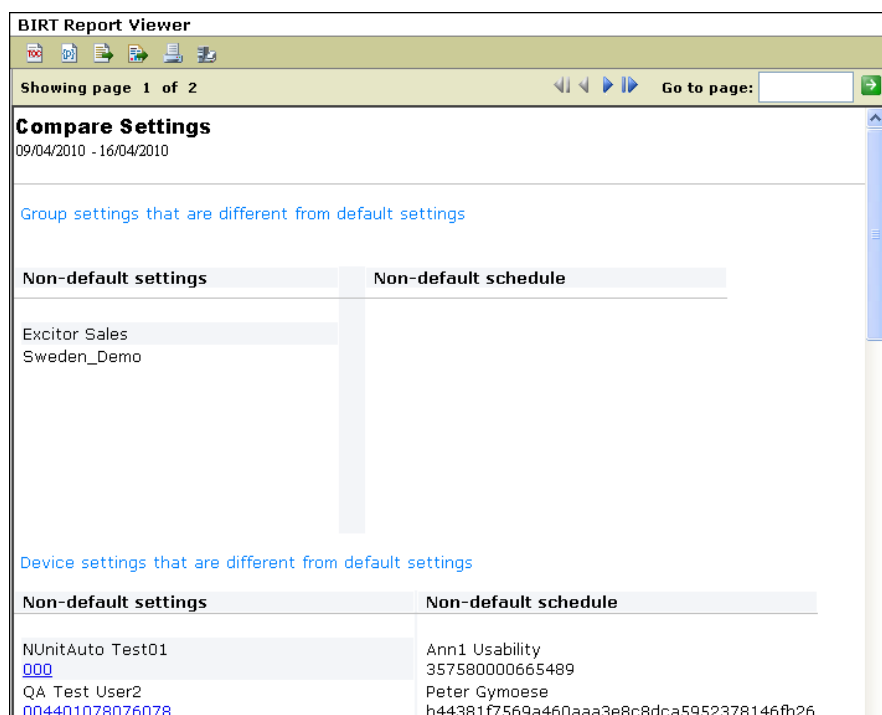
A full, log4j-compliant log is kept on the server for every server event. Built-in statistics round-robin reports let you see “everything” as throughput - number of documents per second parsed back and forth to the collaboration server (e.g. Exchange), or number of requests per second from the devices etc... The statistics module presents data captured (and averages calculated) per minute, per hour and per day. For each of these the administrator can view 4 screens of data.



These reports help you pinpoint any bottlenecks in the system.

Another set of built-in statistics reports helps you monitor the voice and data traffic on the system.

Finally, DME integrates with the powerful BIRT reporting tool, for instance allowing you to build reports that help you analyze and detect abnormal behaviours. DME supplies a number of default report templates, including a report that shows which devices that deviate from standard security settings:



11 Client differences

As mentioned, platform differences make it impossible to create the exact same security environment on all clients. The most notable differences are within the following areas.

11.1 Remote decommissioning

When decommissioning a device by issuing a wipe command to it, it is usually not possible to delete *all* data from the device. There are a number of reasons for this. When a command is received by the DME client to delete all device data, the client goes through the following procedure:

- First, all processes/applications with a user interface are shut down in order to release any locks they may have on files.
- Then the file system is traversed, and every file is deleted – first in the device memory, then on any memory cards.
- On **Windows** devices, all keys in the registry database that can be deleted are deleted.
- On **Symbian** 3rd edition devices, the process will finish by attempting to factory reset the device.

If any file is locked by an internal process, it will not be deleted. The reason that DME only shuts down external processes is that shutting down an internal process may cause a device reboot. When the device boots up, the DME client will start shutting down the internal process again. This way a reboot loop is started, and the device must be taken to service.

The DME client has access to all public folders, so the entire file system is traversed.

On **iPhone** devices (and iPod touch/iPad), only *Contacts* and *E-mail/PIM* stores are removed when the device is wiped.

11.2 The iPhone client

The client for iPhone and related devices is special in the sense that it is a full DME client, but it is subject to OS limitations imposed by Apple Inc. The following special issues concern the DME client for iPhone (latest version):

- **PIN Code/Swipe login:** Due to the multitasking limitations inherent in the iPhone platform, DME on iPhone is typically shut down more frequently than DME on other platforms. Therefore the decision was made to allow the user to keep the encrypted password in the iPhone storage, *even when DME is shut down*. If the use of PIN code is disabled, the network password is only kept in memory and not stored when the user exits DME (as on other platforms). The encryption of the stored password is *not strong* when using the PIN/swipe code feature, and it is in theory possible for a hacker to break the password, if he gets access to the phone.
- **Password/shell protection:** 3rd party developers cannot protect other areas of the iPhone than the application itself. The DME client has its own mailbox, calendar, and contacts, but cannot password protect the iPhone itself nor the native Contacts application. However, to enable/enforce the native PIN code protection, an iPhone configuration can be pushed to the iPhones from DME.
- **Wipe on SIM change:** DME cannot detect that a SIM card has been changed.
- **Remote wipe:** Only *Contacts* and *E-mail/PIM* stores are removed when the device is wiped. The feature requires SMS or Apple Push. If the DME client is not active, the user must also actively react on the SMS or Apple Push notification to start the wipe process. Therefore the wipe command is camouflaged and presented as "a DME server command".
- **Application and connection blocking:** Not allowed by Apple.
- **Anti-spoofing / device signing certificates:** This is supported on iPhone from version 3.5.4 of the DME client and 3.5 Service Pack 2 of the DME server.
- **RSA SecurID token:** Not supported.

11.3 The Java client

On feature phones (also called Java phones), the sandbox concept of the Java technology has some built-in limitations.

- **Password/shell protection:** Not available.
- **Wipe on SIM change:** Available only on phones running Sony Ericsson Java JP-8.
- **Remote wipe:** Only *Contacts* and *E-mail/PIM* stores are removed when the device is wiped.
- **Application and connection blocking:** Not allowed by the Java platform.

11.4 The Android client

The Android platform (up till the current version 2.1) does not allow the import of CA certificates. For this reason, Android devices require that the DME Server uses a certificate from one the 3rd party vendors whose certificate is preinstalled on the phone.

12 More information

For more information about DME, please go to our website at <http://www.excitor.com>, or contact Excitor A/S at info@excitor.com.