

DME version 3.6 SP1

Installing DME: Linux

Installing DME

Created on 18-04-2012

Linux

Contents

Installing DME	3
Anti-virus programs	4
Installation overview	5
Installing DME on Linux	6
Download the Linux installer	6
Main menu	7
Base installation	8
Installing certificate from commercial CA	15
Installing non-commercial certificate	17
Managing certificates using dmecc	18
Clustering	19
The administration web interface	20
Instance management	21
Upgrading DME	24
Kannel install or upgrade	26
Installing and upgrading a connector	27
New connector	28
Upgrading the connector on Linux	29
Adjusting RAM usage	30
Configuring the connector	31
Connectors outside the LAN	31
Removing a connector	32
Configuration in the web interface	32
Exchange NTLM setup	34
Securing database password and data traffic	35
Encrypting database password	35
Encrypting connector traffic	36
Linux installation summary	37
Configuration files	38
Kannel	39
Business continuity	41
Backup	41
Restore	42

Installing DME

Welcome to the DME 3.6 SP1 for Linux installation guide.

Version 3.6 SP1 uses a different architecture and setup compared to DME 2.0 and earlier. An installation now includes a DME Server and at least one DME Connector.

The DME connector can be installed on the DME server, on a dedicated server, or on the collaboration server (IBM Lotus Domino or Microsoft Exchange).

When connecting to IBM Lotus Domino, the DME connector supports two connection modes: *Remote/Corba mode* (using DIIOP as in previous versions of DME) and *Notes session mode*. For more information, see the *Domino Integration Guide*.

Please note

If the DME connector is installed in a different network zone than the DME server (internal LAN/DMZ), the firewall must allow the DME connector to connect to the DME server. For a full description of firewall setup, see the ***firewall setup documentation***

<http://install.excitor.dk/documentation/install/docs/02/fwmap.php> at the Excitor install site.

The ports need to allow all states of the TCP/IP protocol to be enabled, as the connector "pings" the DME server and communicates both ways, though communication is only established from the connector to the server.



On **Linux** installations, you can no longer set the firewall settings for SSH access to the machine in the installer. You need to manage SSH access manually, either during installation of the Linux distribution or via the tools for managing the firewall on the distribution in question.



On **Windows 2003 Server** installations, some of the service functions assign random ports when starting, and sometimes these port choices collide with ports used by DME.

To avoid this, reserve the following ports used by DME: **1098-1099, 1100, 3873, 4444-4446, 4457-4458** by following the procedure described in the Microsoft knowledge base article at: ***Reserving ports on Windows Server 2003***
<http://support.microsoft.com/kb/812873/>.



On **Windows 2008 Server** installations, a built-in firewall is enabled by default. For DME to function correctly, you must either repeat the firewall rules (inbound from devices and connectors and outbound to LAN) as specified in ***firewall setup documentation***

<http://install.excitor.dk/documentation/install/docs/02/fwmap.php> at the Excitor install site, or (preferably) disable the built-in firewall.

To install DME as a cluster, please request separate documentation.

Anti-virus programs

DME is a time-critical application, which relies on good I/O throughput to the filesystem, queues and timeout values to control the flow of data between the collaboration system and the clients.

The use of anti-virus scanners (AV) can in some cases be disruptive to this process. On Windows servers, there can be problems with file locking, and on Linux, AV programs tend to use up large amounts of resources. AV can cause latency issues, and cause packet corruption due to packet inspection of traffic on ports connecting the DME connectors and the DME server.

As a result of this, AV programs can cause intermittent errors in DME, which are hard to pin down. Whenever strange errors occur in DME, the first thing you should do is to turn off AV for troubleshooting purposes and then restart the DME server and connectors to see if the errors can be reproduced without the AV running.

If you require AV system scanning on the DME server, please follow these guidelines:

On the DME server, the following directories must not be scanned realtime:

- `<DMEPATH>\tmp\`
- `<DMEPATH>\work\`
- `<DMEPATH>\data`

Furthermore, due to the packet corruption mentioned earlier, Packet Inspection should be turned off - at least for the DME communication ports **5011** and **5012**. Most packet inspectors do alter packets (despite their claims of the opposite), causing instability and causing the clients to lose the connection - requiring transaction rollbacks and traffic logging issues.

On the DME connector, the **temp** directories must be excluded from the AV realtime scanner. The location of the **temp** directory is either dictated by the **TEMP** and **TMP** environment variables, or the DME connector can be configured to use specific DME temporary folders.

To specify DME-only temporary folders, do the following:

- 1 Open the `dmeconnector\conf\wrapper.conf` file.
- 2 Add the following parameter to add `C:\mytemp` as a new temporary directory for the DME connector:
`wrapper.java.additional.2= -Djava.io.tmpdir=C:\mytemp`

When using pre-caching, you can specify a custom folder for temporary files in the DME connector setup page in the web administration interface. This folder should also be excluded from realtime AV scanning:

- 1 Open the DME web administration interface.
- 2 Click **Connector** > the connector you wish to edit > **Functions**.
- 3 In the **Advanced** section, enter the temporary folder in the field **Connector temp directory**.

The screenshot shows a web interface with a light blue background. At the top, there is a tab labeled 'Advanced'. Below the tab, there are two input fields. The first field is labeled 'Recipient separator' and contains a semicolon (;). The second field is labeled 'Connector temp directory' and contains the text 'c:\mytemp'.

- 4 Click **Save**.
- 5 Restart the connector.

Installation overview

The following is an overview of the installation process. The actual steps involved in completing the installation are described in the subsequent sections of this document.

Please note

In previous versions of DME, a setup wizard started automatically the first time a user logged into the web administration interface. This wizard functionality has been removed, and the basic configuration is handled by the installer.

➤ **Installing DME**


- 1 Install the DME Server (one or more instances).
- 2 If this is a clean (first-time) install, execute the database creation SQL script to create the fields, indexes and constraints correctly (this must be performed before starting DME for the first time). If it is an upgrade of a previous 3.0 installation, run the database upgrade scripts. Note that this applies to MS SQL Server and Remote MySQL databases only.
- 3 Prepare for a cluster setup, including load balancer etc. (optional).
- 4 During the installation, the installer will prompt for some basic configuration information, which you must have ready:
 1. Enter the connection information for the database server (MS SQL Server or Remote MySQL).
 2. The installer will prompt for SSL certificate information to create a certificate request. You can have the request signed by Excitor or a public certificate authority (see **Certificate request** on page 12).
- 5 Perform the following steps for each DME connector:
 1. Install the DME connector, entering the connection information to the DME server (the hostname of the DME server and the display name of the connector – usually including the name of the collaboration server it is connected to). For example excitor.com - London Office - Exchange Mail

2. Upload the DME license to the DME server after starting it. Otherwise the connector cannot bind to the DME server.
3. Start the DME connector, and it will attempt to connect to the DME server. When the DME connector has connected to the DME server, it will be listed in the **Connector** tab in the DME Administration web interface with a green check mark. The details of the connector can be viewed by clicking the display name.
- 6 Log in to the DME administration web interface as SYSADM (password: HeraterSol55) to continue the configuration of the DME server and connectors.
- 7 Change the SYSADM password to a strong password.
- 8 Set up a DME cluster, if applicable.

➤ **Linking the connector and the server**

In the DME web interface, you must provide some information for linking the connector properly with the server. Click the connector in the **Connector** tab, and specify the following:

- In the **Main** panel section: the information you filled in during installation of the connector is already shown.
- In the **Domain** panel section: Provide information about your LDAP/AD directory server.
- In the **Authentication** panel section: Provide information about your LDAP/AD directory server. By default, the directory server specified in the **Domain** panel section is used. Also specify which directory groups should be considered as DME users, superusers, and administrators (if different from standard).
- In the **Functions** panel section: For Domino installations, specify if the connector is using **Notes session** or **Remote/Corba**.

For more information, see the DME Administration Reference (click the  button in the web interface).

Installing DME on Linux

The following sections describe how to install DME on a Linux server.

Download the Linux installer

To get the software, log into your Linux console as **root**, then download and launch the install script using:

```
wget -N http://install.excitor.dk/install/dme-install.sh
```

After download, run the installation program.

```
sh dme-install.sh
```

This launches the latest version of the Linux installer. See the next section for a list of available startup parameters.

```
*****
***                                     ***
***  DME Server Installation            ***
***                                     ***
*****
Please fill in the following information
Enter username: █
```

Note that to install DME, two things are required:

- A username and password - the same username and password which is used for the DME support website (<http://support.excitor.dk>). For compatibility, old passwords used to install previous DME versions can be used, but will be deprecated without further notice.
If the *user name* part of your support site credentials contains special characters, for instance an @ sign, please contact DME Support for new credentials to be able to continue the installation. If your *password* contains invalid special characters (that is, characters other than: a-z, 0-9, and .), log in to the DME support website and change your password.
- To obtain a user name and password, you need to attend and pass the *DME Certification Course*. For more information, see the Excitor website.

Enter your user ID and password, which you have received from Excitor Support.

Startup parameters

You can use startup parameters with the installer to control virtually any option that can be set through the installer, including connector, certificate, and database values.

To view the startup parameters available for the installer, type `sh dme-intall.sh -h` at the prompt. If you cannot read all of the help text, use the following command in the console:

```
dme-install.sh -h | less
```

Main menu

After your credentials have been accepted by the DME support site, the DME Server Installation menu is displayed.

If more than one network interface card (NIC) has been installed and configured, you will be asked which NIC you want to bind DME to. When you have made your choice, the main installation menu is displayed.

```
*****
***                                     ***
***  DME Server Installation           ***
***                                     ***
*****
DME Server Installation menu
-----

 1. Base installation
 2. Upgrade DME             (install Base first)
 K. Kannel install/upgrade
 C. Install/upgrade Connector
 H. Help

 Q. Quit

Your choice [default => 1]: █
```

The menu shows you the options that are currently available. For example, "Instance management" and "Upgrade DME" are not possible on a clean system where the DME base instance has not been installed previously. The installation and upgrade of the Kannel server is present at all times, since it is a separate program and installed separately. Some GSM modems with USB connections are not detected correctly, and are known to cause problems during installation. If Kannel is installed on a server without DME, some manual configuration is required for self-provisioning to work correctly. See the technotes related to Kannel at the Excitor Partner website.

Almost every menu in the installer has a *default choice*, which is selected by pressing Enter - the default item is also identified in the last line where you can type your selection. If there is no default choice, then please read the menu or on-screen help text, since your choice will have an impact on your next step or all instances (if you are about to upgrade the instances).

This menu lets you do a *base* install, manage DME instances, and upgrade DME. The **Instance management** menu item replaces the **Base installation** item if a base instance already exists.

Type your choice, and press Enter:

- Press 1 to perform base installation/Instance management.
- Press 2 to upgrade DME (only possible if DME exists on this machine).
- Press K to install or upgrade Kannel.
- Press C to install or upgrade a DME connector.
- Press H for a short help text for the selectable items.
- Press Q to quit the installer.

Base installation

If you choose to perform a base installation, a list of versions of DME that are available for installation at the Excitor website is shown, along with supported databases.

Note that for new installations, the default version is the latest DME version with MySQL support. If you are upgrading, the default will be the latest DME version that supports the currently used database.

```
*****
***                               ***
*** Base Installation              ***
***                               ***
*****
DME base installation
-----

Fetching a list of available DME Servers that can be installed

Please choose version and release

  1) DMES 3.0 SP3 64bit, with MySQL
  2) DMES 3.0 SP2 64bit, with MySQL
  3) DMES 3.0 SP2 64bit, with MS SQL support

Choose version [default => 1]: █
```

Select a version and press Enter to install it. You are asked to confirm your choice of version.

```
*****
***                               ***
*** Base Installation              ***
***                               ***
*****

The following software will be installed:

    DME Server : DMES-R30-43
      JDK      : 1.6.0_11
      JBoss    : 4.2.3.GA
      MySQL    : 5.0

Do you want to continue (Y/n) ? █
```

Note that this screen shows the version numbers of the auxiliary files installed by DME. Press Enter to continue, or n to return to the main menu.

If you continue, another warning will appear, informing you that for DME to function correctly, specific versions of certain software is required. If this software is already installed on the server, it will be removed, and the correct versions will be installed. Therefore, any other software depending on this software may not work correctly after the installation of DME. In particular, if you are installing MySQL, it is important that you make a full backup of any existing MySQL database before continuing, as your existing copy of MySQL will be removed.

See [Upgrading DME](#) for more information about what to remember in connection with upgrading.

Press y to continue, or n to abort the installation.

MySQL

If MySQL was selected as the DBMS, you can now choose to a local installation (default) or a remote installation.

```
*****
*** Database options ***
*** Localhost or remote host ***
*****
Database location configuration
-----
Use MySQL on localhost or remote host?

  1) MySQL on localhost (default)
  2) MySQL on remote host
  H) Help with options

Select [default is localhost]: █
```

If you select **MySQL on localhost**, you can skip to the section about downloading components.

If you select **MySQL on remote host**, please make sure to review the steps described in following section. The steps described here are also shown if you select **Help with options** in this screen.

MySQL on remote host

MySQL is by default installed on localhost, but it is possible to use a remotely installed MySQL.

If you choose the item **MySQL on remote host**, you will need to install MySQL on a server, and create a database and user that DME can use. You will be asked for the information to connect to the MySQL server after DME has been installed and is ready for final configuration and first start.

The supported versions of MySQL are:

- MySQL 4.1.9-0 for all DME versions up to and including DME 2.0
- MySQL 5.0 for DME 3.x

Please note

MySQL 5.0 with DME 2.0 or DME 1.10 will result in errors that can invalidate your synchronization tables and cause unknown and undocumented errors that cannot be resolved without starting DME on a fresh, new, clean database. So please make sure to install the correct version of MySQL for the DME server!

Create a database on the MySQL server:

- 1 Log in as the MySQL user root:
`root@localhost $ mysql -u root -p`
- 2 Create a database with a name, for instance base for the base DME instance:
`mysql> create database base;`

- 3 Create a user for the DME server. The user needs to be able to access the database from the DME server, so write down the IP address of the server, or configure the user to be able to connect from any IP address.

```
mysql> grant all on base.* to 'base'@'a.b.c.d' identified by
'secretpassword';
```

Substitute 'a.b.c.d' with the IP address of the DME server, or enter a % (percentage sign) for any IP address.

Substitute 'secretpassword' with a strong password of your choice.

The MySQL client will be installed on the DME server to enable database manipulation from the DME server. You can test the connection from the DME installation when you are asked to fill in the DBMS information.

Downloading components

The installer now downloads and installs the software required to run the chosen version/Service Pack with JDK, JBoss and optionally MySQL from the DME support site. The reason for downloading new versions is to make sure any configuration changes to the DME server are updated correctly. An approximate size is calculated for the download so you can estimate the download time.

The download progress is shown as an incremental percentage. The files are not the same size, so the speed will vary from file to file.

You can follow the download progress on screen.

```
*****
***
***   Downloading approx. 260Mb
***
*****

Download progress
-----
Downloading required files for DMES version 3.0-43 (DMES-R30-43)
Please wait while downloading 51 files
 1%  3%  5%  7%  9% 11% 13% 15% 17% 19% █
```

After download, you can monitor the installation progress.

```
*****
***
***   Installing DME dependencies
***
*****

Please wait while installing packages
-----
jdk-6u11-linux-amd64.rpm  installed
MySQL-server-community-5.0.83-0.rhel5.x86_64.rpm █
```

Remote database setup

DME 3.0 cannot upgrade a database installed with previous versions of DME.

When installing DME with a local MySQL database, the database will be created automatically.

If you choose an MS SQL Server database or a remote MySQL database, you must create the database manually, and run a script before starting DME. If you fail to do so, DME will not be able to run. See **MySQL on remote host** on page 10 above and the Database setup section at the **DME install site** <http://install.excitor.dk/documentation/install/index.php> for more information.

You are now asked for connection details for the remote database installation.

```
To enable the DME service to connect with a remote MySQL Server, you
vide
the following information.

MySQL Server's IP address or hostname
and the port number the database is using
Database name to use
Username
Password

Before the connection can be set up, please read the manual or pres
instructions.

Current setup:
1) MySQL host IP      :
2) MySQL host port   : 3306
3) Database name     :
4) Username          :
5) Password          :

T) Test connection
C) Continue

Your choice [default => 1]: █
```

Fill in the required information by entering the menu item number and changing the value. When the connection details are filled in, you can press T to test the connection. The installer writes “passed” or “failed” depending on the result of the test.

If the test fails, you can change the settings you have entered, check that the database is set up correctly, check that there are no firewall or other network problems from the DME server to the database, or consult the documentation for the DBMS.

You can manually bypass the DBMS configuration for the DME instance by pressing Continue. The DME instance will not be able to start properly, and you will later have to change the settings manually in the `dmebaseDB-ds.xml` file, which is located in

```
/var/dme/instances/<instancename>/etc/jboss/dmebaseDB-ds.xml
```

DME depends on the DBMS and cannot function without a DBMS.

Certificate request

As of DME 3.0, DME does not use the built-in Java keystore for certificate handling or the web-based certificate uploading. Therefore you are asked to fill in the certificate details for the DME server or DME instance. The certificates are RSA encoded PEM certificates, which are easier to manage than in previous versions.

In the **Certificate** menu you are asked to enter information about the certificate.

```

Please enter Certificate details
-----
Please enter the details for the certificate used by DME
-----

 1) Common Name (host name) *: dme.excitor.dk
 2) Country code (2 letters) *: DK
 3) Administrator E-mail *:
 4) Organization Name :
 5) Organizational Unit : DME
 6) State or Province :
 7) Locality name :

 H) Help
 C) Continue with the values above

Fields marked with * are mandatory for a
self-signed certificate. All fields must be filled in for a public
Certificate Authority signing of the certificate.

Please enter item to edit: █
    
```

Enter the information to create the certificate request:

- External host name (CN)** Enter the fully qualified host name that the mobile devices will use to connect to the DME server. For instance: `dme.excitor.dk` if the external connection will be to `https://dme.excitor.dk:5011`. It is very important to enter this correctly, otherwise the device cannot connect to the server. Do not use an IP address as host name, as the iOS and Android mobile phone platforms cannot handle IP addresses as CN.
- Country code (C)** 2-letter country code, for instance DK.
- Administrator e-mail** The signed certificate will be sent to this e-mail address.
- Organization name (O)** The name of your company.
- Organizational unit (OU)** Department name or similar, or leave blank.
- State or province (ST)** Name of state/province, or leave blank.
- Locality name (L)** City name.

During the server installation, the information supplied here will be used to create a certificate request, which can be signed by Excitor or a commercially approved certificate authority (CA; for instance Verisign, Thawte, or RapidSSL). If you choose to have it signed by a CA, all fields are mandatory.

To edit an item, type the number of the item, and press Enter.

```

-----
 1) Common Name (host name) *: dme.excitor.dk
 2) Country code (2 letters) *: DK
 3) Administrator E-mail *:
 4) Organization Name :
 5) Organizational Unit : DME
 6) State or Province : Denmark
 7) Locality name : Høje Taastrup

 H) Help
 C) Continue with the values above

Fields marked with * are mandatory for a
self-signed certificate. All fields must be filled in for a public
Certificate Authority signing of the certificate.

Please enter item to edit: 4
Please enter your organization name

Please enter the name of your company or organization
-----
Enter organization name [ ]: Excitor A/S █
    
```

Enter the new detail for the item and press Enter to save the change to the certificate.

When you have changed the items that you need or are required as a minimum for the certificate to be signed, choose item C to continue with the installation.

Note that you can later manage the certificate using the **DME Control Center** (**dmec**), including creating a new CSR file. See *Managing certificates using dmec* on page 18.

When the installer is done, you will have three files in the DME structure (in the directory `/var/dme/instances/base/etc/`). The files are:

- **sslprivatekey.pem**
This is the server's private key, and is not to be shared with anyone.
- **sslcertificate.pem**
This is created during the installation as a temporary certificate that is self-signed. It needs to be exchanged with a signed certificate.
- **signrequest.csr**
This is the file you send to Excitor or a commercial CA for signing.

As mentioned, you can use a public signed certificate or a self-signed certificate. If you choose to have the certificate signed by Excitor, you can do one of two things:

- 1 Either send the certificate request file **signrequest.csr** to support@excitor.com, where a DME support assistant will sign certificate request and return it to the e-mail address entered when creating the request.
- 2 Or upload the **signrequest.csr** file at the **DME Certificate Signing** <http://install.excitor.dk/sign/> page to receive a signed certificate immediately.

See the section *Installing certificate from commercial CA* on page 15 or *Installing non-commercial certificate* on page 17 for information regarding the installation of the signed certificate.

Installation complete

The installation is now complete. You can now install and set up connectors etc. while you wait for the SSL certificate which is signed by Excitor or a trusted certificate authority.

A short description of how to start and stop the DME server is also displayed (run the command **service dme_base start**), along with the URL and the default user name and password for the DME administration web interface.

```
*****
The installation is complete.

Use the following command to start/stop the server
service dme_base [start|stop]

DME will always start automatically after a reboot.
When started (approx. 30-60 seconds), you can
browse to:
    https://172.16.15.161:8080
and use the following information to log in.

    Username: SYSADM
    Password: HeraterSol55

Have a nice day!
*****
Excitor A/S, Spotorno Alle 12, DK-2630 Taastrup
*****
[root@localhost ~]#
```

It is strongly advised that you change user name and password after first login.

If you have installed a new instance, you will be returned to the **Instance management** menu, and will not be prompted with any information. The command for starting and stopping the instance will be the same as for the base instance, but the init script will be named `dme_<instancename>` and not `dme_base`, and all files related to the instance are placed in the directory `/var/dme/instances/<instancename>`.

Installing certificate from commercial CA

When you receive a signed certificate from Excitor or a commercial CA (see **Certificate request** on page 12), it must be installed on the DME server. The certificate is used to sign the SSL connection between the DME server and the devices.

The DME server uses an Apache web server (**x509**) certificate. We recommend using certificates from commercial CAs, and this section describes installing such a certificate. Information about the reason why we do not recommend self-signed CAs, and about installing a self-signed certificate, can be found in the following section.

The intermediate certificate(s) must be in **PEM** format (base64). You need to download the CA's certificate chain and replace the content of the `sslcertificate.pem` and `rootCA.pem` files in the following way. As an example, we use RapidSSL. We assume that you have bought a certificate and are ready to generate the certificate at the RapidSSL website (or equivalent).

Editing certificate files

If you are using a Windows machine for editing/copying the text in the certificate file, you must do so with WordPad or another editor that handles newline characters correctly. *Do not use Notepad, as this will corrupt the file.*

- 1 During the installation of DME, a CSR file is generated (see **Certificate request** on page 12). The file is called `/var/dme/instances/base/etc/signrequest.csr`. Open the file in an editor, and copy the contents of the file. Make sure to include both `-----BEGIN NEW CERTIFICATE REQUEST-----` and `-----END NEW CERTIFICATE REQUEST-----` in the text you copy.

Alternatively, use the **DME Control Center** to display the sign request file, and copy it from the screen. See **Managing certificates using dmecc** on page 18.

- Paste the content into the relevant form field at the RapidSSL website.

- An e-mail will be sent to the address registered as administrator of your domain at whois.com (or to another address, see link to **RapidSSL** https://knowledge.rapidssl.com/support/ssl-certificate-support/index?page=content&id=AR1397&actp=RELATED_RESOURCE). The e-mail contains the SSL certificate itself ("Web Server CERTIFICATE") and at least one intermediate CA certificate.
- Copy the *SSL Certificate*. Make sure to include both -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- in the text you copy.
- Using an editor, open the file **C:\Program Files\dme\jboss\server\default\etc\sslcertificate.pem**. Paste the copied SSL certificate into the file, overwriting any content. Save and close the file.
- Copy the *Intermediate CA certificate* from the e-mail. Make sure to include both -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- in the text you copy.
- Using an editor, open the file **C:\Program Files\dme\jboss\server\default\etc\rootCA.pem**. Delete the content of the file, and paste the copied intermediate certificate into the file.
- If there are multiple, intermediate certificates, repeat steps 6 and 7 above for each certificate (but do not delete the content of the **rootCA.pem** file again!). The intermediate certificates must be pasted into the **rootCA.pem** file in the order in which they are received, and they must be pasted back-to-back with no lines between, like this:

```
-----BEGIN CERTIFICATE-----
...
...Rq/MD53Dg4cOcSEF0==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
miidltccaRKS4...
```

```
...
-----END CERTIFICATE-----
```

9 After pasting all certificates into the file, save and close `rootCA.pem`.

10 Change the permissions of the `.pem` files using:

```
chown jboss:jboss /var/dme/instances/* -R
```

11 Then restart the DME server using:

```
/etc/init.d/dme_base restart
```

If the DME Web interface is not displayed after restart, please check the server log file for SSL related errors. Please also use the following guideline in **Support KB7501** <https://rfs.excitor.com/AddSolution.do?solID=7501> (at the DME Support site) if you have several intermediate CAs to install, as the order of installation is critical.

DME supports the use of wildcard (star) certificates (on the form `*.excitor.com`). Such certificates are accepted by most phones, including iOS devices, Android phones, and most Symbian and Windows Mobile devices. For some older Windows Mobile and Symbian phones you may need to send the server root certificate to them (using the function **Send SSL certificate** in the **Devices** tab of the DME administration web interface) before they can connect to the server.

(Optional) In case you are using a CA that is not in the certificate store on the devices, then you need to convert the `rootCA.pem` file to **DER** format in order to be able to install the certificate on your browser and then send it to the clients. See the last section of **Installing non-commercial certificate** on page 17 for more information.

Installing non-commercial certificate

Please be aware that non-commercial, self-signed certificates from Excitor or others are not known to any mobile devices. This is a problem if you want to provision the DME client using OMA DM or iOS MDM, or if your device is an Android. We therefore strongly recommend using certificates from a commercial CA.

In the case of OMA DM, the device management (DM) client built into the devices requires a known root certificate in order to process OMA provisioning commands from the DME server. Therefore, if you want to provision the DME software to the devices using OMA DM and a self-signed CA, you need to send the root certificate to your devices using the function **Send SSL certificate** in the **Devices** tab of the DME administration web interface prior to installing any software using OMA DM.

For more information, including information about certificates on different client platforms, see **SSL certificates** in the DME Server Administration Reference.

If you have chosen to use a self-signed certificate (signed by Excitor or yourself), or you know that the certificate from the commercial CA you are using is not pre-installed on the devices, you must do the following when you receive the signed certificate from Excitor or a commercial CA (see **Certificate request** on page 12):

1 Install the certificate on the DME server. Save the file as `/var/dme/instances/base/etc/sslcertificate.pem`

2 Convert the file (which is in **PEM** format) to **DER** (binary format). To do this, run the following command:

```
openssl x509 < rootCA.pem -outform der > rootCA.cer
```

Please remember that the binary version of the `rootCA.pem` file (`rootCA.cer`) can only contain one certificate and not the full root certificate chain.

- 3 Restart the DME server to use the certificate.
- 4 Install the certificate in your browser (using the **Server > Certificates > Install root certificate** feature in the DME Web Administration Interface).
- 5 Send the certificate to the clients using the **Devices > Send SSL certificate** feature, if required.

For more information about items 4 and 5, see the *DME Server Administration Reference* http://documentation.excitor.com/server/3_6/index.htm.

Managing certificates using dmecc

If you need to make changes to the SSL certificate used to encrypt the connection between the server and the clients, you can use the **DME Control Center dmecc**.

- 1 Log in as **root**, and run **dmecc**.

The DME Control Center screen is shown:

```
DME Control Center
Select one of the options below:

 1) Manage certificates
 2) View DME configuration

 U) Update this script
 I) Install/update DME software
 C) Collect support information
 E) Encryption related items
 M) Upgrade MySQL to version 5.5 (in development)

 H) Help
 Q) Quit DME Control Center

Enter menu item: █
```

- 2 (Optional) Enter U to update the DME Control Center.

The script checks an Excitor website to see if a newer version is available. If one is available, **dmecc** will exit and then update itself. You will then have to start the script again. If no newer version is available, a message tells you so, and you are returned to the main menu.

- 3 Enter 1 (**Manage certificates**).

- 4 Select the instance for which you want to manage certificates.

- 5 Now enter the details for the certificate. For self-signed certificates, only items 1-3 are required; for commercial CAs, all items must be completed.

```
Please enter Certificate details
Please enter the details for the certificate used by DME
-----
 1) Common Name (host name) *: *.excitor.com
 2) Country code (2 letters) *: DK
 3) Administrator E-mail *:
 4) Organization Name : *.excitor.com
 5) Organizational Unit : GT99183457ASeeADomain
 6) State or Province :
 7) Locality name : Hoeje

 H) Help
 C) Continue with the values above
 S) Get information for signing
 A) Auto-sign the certificate (self-sign by Excitor)
 R) Return to the menu

Fields marked with * are mandatory for a self-signed certificate.
All fields must be completed for a public Certificate Authority signing of the
certificate.

Please enter item to edit: █
```

- 6 When you have entered all the required details, you can choose one of the following options.
1. If you want to continue using the temporary, *self-signed certificate* (not signed by Excitor or a commercial CA), enter C (**Continue with the values above**). This will create a `sslcertificate.pem` file if it does not yet exist, with the new values you have entered here, and will create a new `signrequest.csr` file based on these values - which you can then use for creating a self-signed or commercial certificate.
 2. If you want to send a signrequest to a *commercial CA* (recommended), enter S (**Get information for signing**). This will create a new `signrequest.csr` file based on the entered values, and show the content of the CSR file. Copy the content from the screen, and send it to the commercial CA. See *Installing certificate from commercial CA* on page 15 for information about installing the certificate.
 3. If you want *Excitor to sign* the certificate, enter A (**Auto-sign the certificate (self-sign by Excitor)**). This prompts you for your installer credentials. Enter your install site username and password. The details you have entered are saved as `signrequest.csr`, sent to Excitor, processed, and returned as a `sslcertificate.pem` file. See *Installing non-commercial certificate* on page 17 for information about installing the certificate.

Enter R (**Return to menu**) to return to the main **DME Control Center** menu.

Note that `dmecc` copies the original certificate files `rootCA.cer`, `rootCA.pem`, `signrequest.csr`, `sslcertificate.pem`, and `sslprivatekey.pem` to a backup folder (`tmp.[random name]`) and places the new certificate files in `etc`. It is therefore important that you complete the certificate signing process before the DME server is restarted for any reason.

Below is a screenshot of the folder after generating a new CSR:

```

root@gb1-centos5:/var/dme/instances/base/etc/tmp.BiteYL7942
[root@gb1-centos5 etc]# ls -l
total 32
-rw-rw-r-- 1 jboss jboss 1841 Apr 17 14:19 cryptoKeystore
drwxr-xr-x 2 jboss jboss 4096 Apr 18 09:59 jboss
-rw-r--r-- 1 jboss jboss 1265 Apr 17 14:17 rootCA.cer
-rw-r--r-- 1 jboss jboss 3866 Apr 17 10:16 rootCA.pem
-rw-r--r-- 1 jboss jboss 1815 Apr 18 15:57 signrequest.csr
-rw-r--r-- 1 jboss jboss 1815 Apr 18 15:57 sslcertificate.pem
-rw-r--r-- 1 jboss jboss 1710 Apr 17 10:16 sslprivatekey.pem
drwx----- 2 root root 4096 Apr 18 15:52 tmp.BiteYL7942
[root@gb1-centos5 etc]# cd tmp.BiteYL7942/
[root@gb1-centos5 tmp.BiteYL7942]# ls -l
total 20
-rw-r--r-- 1 root root 1815 Apr 18 15:52 rootCA.cer
-rw-r--r-- 1 root root 1815 Apr 18 15:52 rootCA.pem
-rw-r--r-- 1 root root 1815 Apr 18 15:52 signrequest.csr
-rw-r--r-- 1 root root 1261 Apr 18 15:52 sslcertificate.pem
-rw----- 1 root root 1781 Apr 18 15:52 sslprivatekey.pem

```

Clustering

DME supports clustering and load balancing with a few post-installation adjustments.

To set up DME in a cluster, perform the following steps:

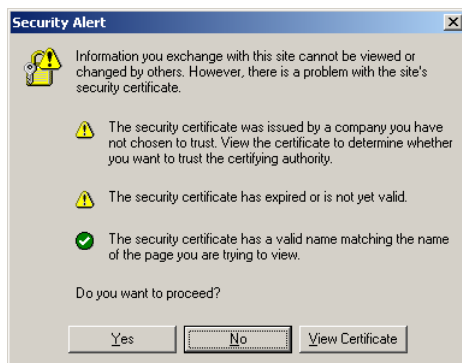
- 1 Install two or more DME 3.0 SP3 servers on separate servers.
- 2 Make sure that all DME servers have access to the database.
- 3 Make sure that the contents of the `.../etc` directory on all servers is identical.
- 4 Make sure the `.../deploy/jboss-messaging.sar/messaging-service.xml` file is identical on all DME servers.
- 5 Set the following variables in the init scripts, so they are identical on all DME servers:

```
CLUSTERPASSWORD="<someClusterPassword>"  
CLUSTERPARTITION="DME-ClusterPartition"
```
- 6 For each connector, the IP address or host name must be appended by `:1100`. This port number makes the connector aware that it is part of a cluster. The addresses of each node can be entered as a comma-separated list when you install the connector, for instance `172.16.15.10:1100,172.16.15.11:1100`. This information is entered in the `dme-config.xml` file, in the `<jboss></jboss>` tag in the `<configuration>` section.

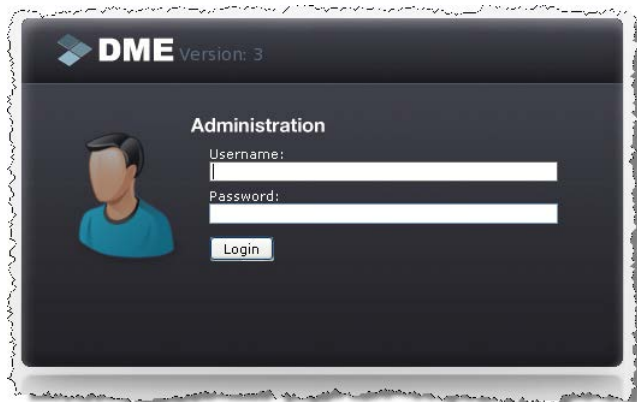
The administration web interface


To administer the DME server, open a browser window and enter the DME server path as the URL.

If you are using a self-signed certificate, the browser will show a security warning, because the certificate is unknown to the browser.



Click **Yes** to proceed. The DME server login screen is shown:



The default user name is SYSADM, and the default password is HeraterSol55 (case sensitive). You can now configure the server and connectors as described elsewhere, notably in the DME Server Administration Reference, which can be found online at the ***DME Documentation*** <http://documentation.excitor.com> site (click  in the DME web interface).

In the DME web interface, make sure to change the SYSADM password to a strong password as soon as possible:

- 1 Click the **Devices** tab
- 2 Locate, and click the SYSADM user
- 3 Click the **User** panel in the user setup page
- 4 Click **Edit password**
- 5 Enter a new, strong password
- 6 Click **Accept**

Instance management

Instances are separate running processes of the DME server, completely separated from each other. Each instance runs in its own JVM, has its own directory structure, init file, DBMS configuration, database, filestore, and its own IP address.

Currently, due to the JBoss Application Server configuration and the desire to keep the alterations of the JBoss configuration to a minimum, it is only possible to install multiple instances on one server by using multiple IP addresses, one for each DME instance.

To create or view instance configuration, first download the newest installation script as described in the introduction to this guide. In the main menu, the default item 1 (**Base installation**) has changed to **Instance management**. Choose this menu item to go to the instance management menu.

```
*****
***                                     ***
*** Instance Management                 ***
***                                     ***
*****
Instance management menu
-----
1) Create another instance
2) View installed instances

H) Help on instances

R) Return to previous menu

Your choice [default => 2]: █
```

The instance management menu gives you the option to create a new instance and enables you to view the currently installed instances. Removing instances is currently not possible, and has to be done manually.

Please note

When you install multiple instances, special care must be taken if you run multiple physical servers, each with multiple instances.

During installation on the same machine, the Linux installation script will isolate each DME instance from the others by incrementing the `CLUSTERUDPGROUP` and `CLUSTERUDPPORT` parameters in the `dme_<instances>` startup scripts. However, if you install multiple instances on another physical machine, then *the same number can be used*, leading to a conflict between instances, where two instances will believe they are part of the same cluster.

To prevent this, you must review the values for `CLUSTERUDPGROUP` and `CLUSTERUDPPORT` to avoid using the same numbers for two different instances located on two physical servers.

Creating an instance

If you choose 1 **Create another instance**, you are guided through a three-step procedure.

- 1 First step is to give the new instance a name. The name is parsed to strip out invalid characters such as `?`, `*`, `.` etc., which could cause problems in the different scripts used to install and upgrade DME. Please avoid characters that will influence the init script, for example any non-alphanumeric characters. Press Enter after typing the name, and Y when when asked to verify the name. The following limitations apply to the instance name:

- The name must not contain characters that are not supported by the file system.
- The name must not start with a number (0-9).
- The name must not be longer than 10 characters.

The init script to start and stop the instance will be prepended with `dme_` in the `/etc/init.d` directory to make it easier to find and use. The instance, and all files belonging to the instance, are placed in `/var/dme/instances/<instance>`.

```
*****
***                                     ***
*** Enter a unique name for the instance ***
***                                     ***
*****

Instance configuration
-----

All DME Server instances have a name. For example, the
default instance is called "base". Please choose a name
for the new instance.

You can type "quit" to abort to the main menu.
You can type "help" to see some information about the naming conven

Requirements for the instance name:
- allowed characters are: a-z, A-Z, 0-9 and "_"
Characters that are not allowed will be discarded. If the name
is used by another instance, it will be discarded.
Names cannot start with a digit, names will be shortened to 10 char

Please enter a unique name for the instance: MyCompany
```

- 2 Next you need to configure the network interface card and the IP. The IP has to be a valid IP, which the server is able to configure and use. There is currently no limitation to the number of instances or virtual IP's that can be used, except for the limitations of the hardware. If you have multiple configured NICs on the machine, a different NIC can be chosen and configured.

Choose which NIC to bind the DME instance to, and continue. If a NIC already has a DME instance bound to the IP address or all IP addresses on the NIC are used, a virtual NIC will be created automatically with a new IP address that is not used by any other DME instance. If a NIC is not used by any DME instance, the IP on that NIC will be used by the new DME instance.

```
*****
***                                     ***
*** Create virtual interface on physical interface ***
***                                     ***
*****
Instance network menu
-----

The instance needs to be bound to an interface (NIC).

DME needs its own IP address. If you do not have an
unused or free IP address on a NIC, a virtual NIC with
an IP address will be created on a physical NIC.

Please choose the NIC to bind the DME instance to or
bind the virtual NIC to:

    1) eth0, DME instances bound to this interface:
       base      uses IP: 172.16.15.161 eth0

Use "Q" or "quit" to abort the instance installation
Your choice [default -> 1]: █
```

- 3 Finally you will be asked to confirm or change the automatically detected/calculated IP address for the DME instance. The installer will then choose the first available IP address, which is not used by any other DME instance, based on the IP address currently active on the machine.

```
*****
***                                     ***
*** Change IP configuration ***
***                                     ***
*****
Instance IP configuration
-----

On interface: eth0:0

Change auto-detected settings

    1) IP      : 172.16.15.162
    2) Netmask : 24

    A) Abort instance installation

    C) Continue

Please choose an option: █
```

If the NIC or IP address you chose is not configured on the machine, the installer will act depending on the current Linux distribution:

- On RedHat Enterprise Linux and Fedora Core, a network configuration file is created in `/etc/sysconfig/network-scripts/ifcfg-ethX:N`
- On SuSE, the virtual NIC and IP are automatically created when the DME instance is started, if the virtual NIC and IP are not already active.

After changing the network configuration for the instance, it is installed and configured similar to a normal installation.

When you are done, press C to continue. A summary of your selection is shown. Depending on platform and previous setups, you may be prompted to reuse an existing boot file for the virtual NIC.

The installer proceeds to create the new instance, and you will be prompted to enter certificate details as for the base installation (see *Certificate request* on page 12).

When the instance has been installed and preconfigured, you are returned to the **Instance management** menu where you can choose item 2 to view the currently installed instances (see below) or return to the main menu with item R.

Viewing instances

Choose 2 **View installed instances** to see an overview of installed instances.

```
*****
View of installed DME instances
=====
Found 2 instances

base
  IP           : 172.16.15.161/24
  Port         : 5011
  WWW port    : 8080
  Push port   : 5021
  Interface   : eth0
  SSH         : n/a
  HTTPS forward : "false"
  - no connector installed

MyCompany
  IP           : 172.16.15.162/24
  Port         : 5011
  WWW port    : 8080
  Push port   : 5021
  Interface   : eth0:0
  SSH         : n/a
  HTTPS forward : "false"
```

If 3, 4, or more instances are installed, you can scroll using Shift+PgUp and Shift+PgDn.

The items of information displayed are the settings found in the init script, for instance `/etc/init.d/dme_<instance>`, and the content of the `/var/dme/instances/<instance>/etc/jboss/server.xml` file. Furthermore, it specifies if a connector has been set up on this machine for the instance in question. Note that a connector may have been set up on another machine.

Press Enter to return to the **Instance management** menu.

Removing instances

To remove an instance, perform the following manual steps:

- 1 Run `rm -fr /var/dme/instances/<instance>`
- 2 Run `rm /etc/init.d/dme_<instance>`
- 3 Run `rm /etc/init.d/dmec_<instance>` (as of SP3)

-where `<instance>` is the name of the DME instance you want to delete.

To remove the DME database for the instance in question, run the following MySQL command:

```
mysql -e "drop database <instance>;"
```

Upgrading DME

To install a new service pack or version of DME 3.6 SP1 when released by Excitor A/S, download the installer and run the upgrade through the installer as described earlier.

When you have logged in, and the main menu appears, choose the default item 2 - **Upgrade DME**.

```
*****
*** DME Server Installation ***
***                               ***
*****
DME Server Installation menu
-----
 1. Instance management
 2. Upgrade DME
 K. Kannel install/upgrade
 C. Install/upgrade Connector
 H. Help

 Q. Quit

 U. Uninstall DME

Your choice [default => 2]: █
```

Important

Make sure to upgrade the server before any connectors. If you upgrade the connectors first, remember to restart the connectors after upgrading the server.

You will be informed about making a database backup if you choose to upgrade DME. You will have to press R return to the main menu or C to continue with the upgrade. Please do make a backup under all circumstances for safety.

The installer will download and display a list of available versions you can upgrade to. If you already have the latest version of DME installed, you will not be presented with any versions to upgrade to.

Before upgrading, the installer checks if you have less than 20GB free disk space available. If you have less than that amount, the installer shows a warning. The upgrade works by DME creating a backup of the files that will be affected by the upgrade before installing the new files.

After choosing the version you want to upgrade to, the installer will:

- Shut down any running DME instances (this may take a while)
- Download the software required for the upgrade
- Loop through the installed instances and upgrade them one by one
- Start the DME instances that were stopped by the installer

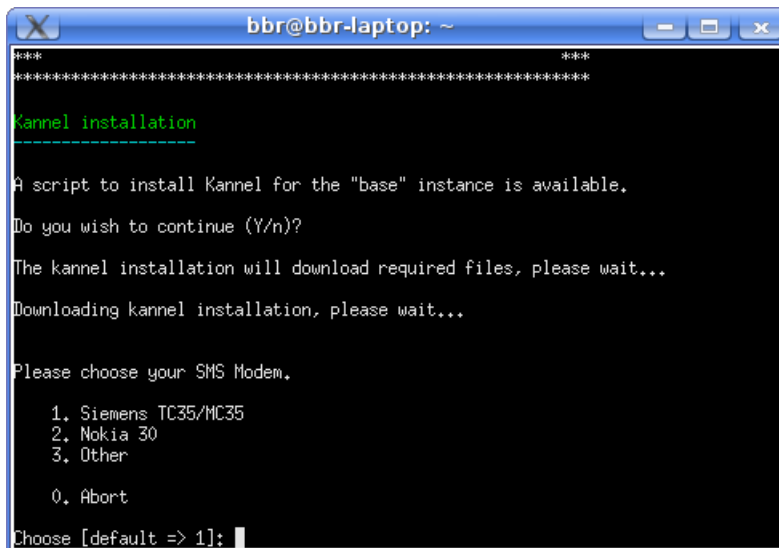
When the installer is finished with the upgrade, you will be presented with the main menu again. The default item will be Q to quit the installer.

When upgrading to DME 3.6, the installer will proceed by running a database migration script, which requires that the database structure for 3.6 is in place. If the installer detects that the MS SQL Server database is not yet ready to be migrated to 3.6 format, it will prompt you to complete the database upgrade by running the relevant database upgrade scripts (see **DME install site** <http://install.excitor.dk>). When this is done, type continue to proceed with the database migration. Note that this applies to MS SQL Server database installations only; MySQL databases are auto-upgraded by the installer.

Kannel install or upgrade

This section describes how to install or upgrade the Kannel server. Kannel is the open-source SMS center software which is used for relaying SMS notifications from the DME server to the clients via an attached SMS modem. The DME clients may also be able to request software by means of SMS messages sent to the Kannel server (see "Appendix B: Self-provisioning" in the "DME Administrator Reference").

When you select 4 **Kannel install/upgrade** from the main menu, the following screen is shown:



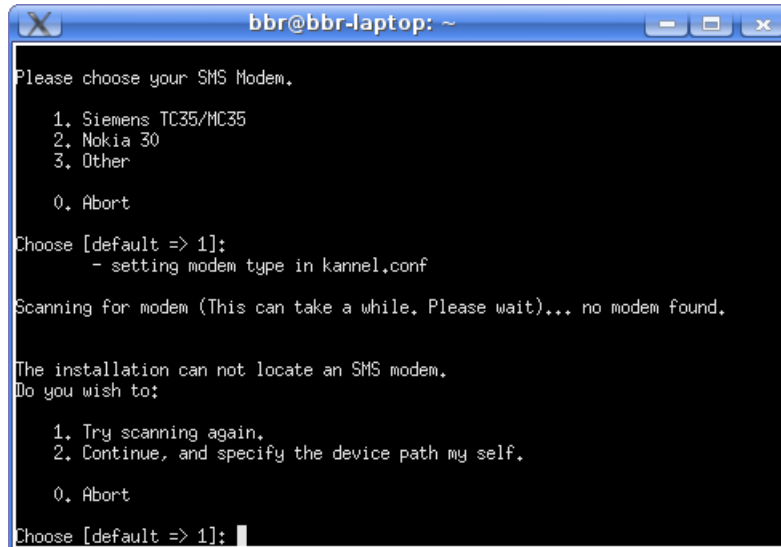
```
***
*****
Kannel installation
-----
A script to install Kannel for the "base" instance is available.
Do you wish to continue (Y/n)?
The kannel installation will download required files, please wait...
Downloading kannel installation, please wait...
Please choose your SMS Modem.
  1. Siemens TC35/MC35
  2. Nokia 30
  3. Other
  0. Abort
Choose [default => 1];
```

The script detects which version of Kannel you need. The script accesses the DME site to get the Kannel installer for the version in question.

When the package has been downloaded, you are asked to choose your type of SMS modem. Choose 1 for Nokia 30, 2 for Siemens TC35/MC35, 3 if you have a different modem, or 0 to abort installation.

Detecting SMS modem

The installer tries to auto-detect the presence of an SMS modem. If it fails, it will ask you what to do:



```
bbr@bbr-laptop: ~
Please choose your SMS Modem.
  1. Siemens TC35/MC35
  2. Nokia 30
  3. Other
  0. Abort
Choose [default => 1]:
  - setting modem type in kannel.conf
Scanning for modem (This can take a while. Please wait)... no modem found.
The installation can not locate an SMS modem.
Do you wish to:
  1. Try scanning again.
  2. Continue, and specify the device path my self.
  0. Abort
Choose [default => 1]:
```

Press 1 to perform the auto-detect again (if you for instance forgot to install the modem before installing Kannel), or press 2 to specify the device path yourself (such as `/dev/ttyS0` for COM1).

The installer then finishes the installation of Kannel and configures the modem.

Installing Kannel package

The Kannel installer then proceeds to install the correct version of Kannel.

The SMS/WAP gateway is also started.

The Kannel configuration files (`kannel.conf`, including `supported.modems.conf`) are located in `/var/dme/kannel/*`

The following symbolic links are created:

From `/var/dme/kannel/etc/kannel.conf` to `/etc/kannel.conf`

From `/var/dme/kannel/init.d/kannel` to `/etc/init.d/kannel`

You are then returned to the main menu.

Installing and upgrading a connector

The connector is what binds the DME server, the collaboration system, and the LDAP together.

New connector

Before you install a new connector, you must make sure that Java has *not* already been installed. The reason for this is that the DME connector requires a specific version of Java, which is included in the connector installation kit. (The only exception to this is if you are installing the connector on the DME server machine, in which case the correct version of Java has already been installed.)

To install a DME connector, choose **C Install/upgrade Connector** from the installer main menu.

```
*****
***                                     ***
***  DME Server Installation           ***
***                                     ***
*****
DME Server Installation menu
-----
1. Instance management
2. Upgrade DME
K. Kannel install/upgrade
C. Install/upgrade Connector
H. Help

Q. Quit

U. Uninstall DME

Your choice [default => 2]: █
```

The installer shows a list of DME instances along with an indication of whether a connector has been configured for the instance in question.

```
*****
***                                     ***
***  Choose instance to attach Connector to ***
***                                     ***
*****
Attach Connector to the following instance
List of instances:

1) base (config n/a)
2) MyCompany (config n/a)

C) Create new connector
R) Return to main menu

Choose instance: █
```

To download and install a connector, and connect it with an instance, press the number of the instance. You can also choose **C Create new connector**, and then enter the name of the instance to which you want to connect (for instance in order to install a connector for a DME server which is installed on another machine).

The installer asks to which of the DME service pack versions, which are supported by the current connector, you want to connect.

After selecting the service pack number, the connector is downloaded and installed. The connector can be started and stopped using an init script called **dmec_<instance>**, which is located in the **/etc/init.d** folder - usage: **service dmec_<instance> (start|stop)**.

If no DME server is installed on this machine, or if you need more local connectors than the base connector, then you can install multiple connectors by manually creating directories `/var/dme/instances/`, and then install new connectors in those 'instances' - for example `MyCompany` etc.

The directory name is used for naming the connector for the sake of the init script, but not in the DME web interface.

Example:

To install a new connector eg. called `MyCompany`, do the following:

- 1 Enter `mkdir /var/dme/instances/MyCompany` in the shell to create an "instance" directory.
- 2 Enter `sh dme-install.sh` in the shell to launch the installer.
- 3 Select C in the main menu
- 4 Choose a DME Service Pack level.
- 5 Choose `MyCompany` in the list of instances.
- 6 Enter the IP or hostname of the DME server.

If the connector is part of a cluster, you must add a port number as well. Furthermore, you can add a comma-separated list of multiple DME servers. See **Clustering** on page 19. If you need to change this later, you can do so in the file `dme-config.xml` in the connector's `conf` directory. If you change this file, you must restart the connector.

- 7 Enter the name of the connector as it should be shown in the DME web interface.

After installation, a new init script has been created in `/etc/init.d/` called `dme-MyCompany`, which can be used to start/stop that specific connector.

Upgrading the connector on Linux

To upgrade a connector, download the installer from the **DME install site** <http://install.excitor.dk>, and re-install the connector as outlined in this guide. Be sure to choose the Service Pack level that matches the DME server.

Important

Make sure to upgrade the server before any connectors. If you upgrade the connectors first, remember to restart the connectors after upgrading the server.

When re-installing, the original configuration and cryptokeystore files are not touched.

If you have multiple connectors installed, repeat the upgrade process for each connector, until the Service Pack level of all connectors corresponds with that of the DME server.

Before upgrading, you must ensure that there is sufficient disk space available. The installer will warn you if less than 20GB is available. The upgrade works by DME moving the connector installation to `/var/old_dme/instances/CONNECTORNAME`, installing the new version, and then applying the settings from the previous installation to the new one.

Important

If you run SSL between server and connectors, you will need to check the settings files after an upgrade. See *Securing the traffic between server and connector(s)* for more information.

Contact mapping files

With DME, you can create files for custom mapping of contact fields, for instance in order to always map a company short number to a specific field in the contacts application on the devices. You can even create mappings files that are specific to individual device types, brands, or operating systems. All this is described in separate documentation.

When you upgrade a connector, a backup is made of all the configuration files, including the custom mapping files, as described in the next section. In order to restore the custom mapping functionality, you must copy the custom mapping files back into the connector **conf** directory **before starting the connector**. This is very important, as the mapping of contact fields will be affected on the users' devices if this is not in place before you start the connector.

Sometimes, a new service pack will include changes in the mappings. This is for instance the case when upgrading to DME 3.5 Service Pack 1. In such cases, you need to manually merge the custom mappings into the new contact mapping file. The release notes for a given version or service pack will say if this is required.

Connector backup files

If the upgrade of a DME connector should fail, for instance due to a power outage or similar, the installation is in an incomplete state. However, the installer first makes a complete backup of the connector files. The backup is placed in the following directory:

```
/var/old_dme/instances/[CONNECTORNAME]/connector/conf/
```

You can use the backup to restore any configuration files you may require.

Adjusting RAM usage

If you are running DME on a 64bit OS with plenty of RAM and many DME users per connector (1000+), you can optimize the RAM allocation.

You do this by changing the initial and maximum JVM (Java Virtual Machine) memory settings in the connector configuration files. Normally the connector will be the service on the machine using the most RAM, up to 2 or 4 times more than the DME server. However, you will have to test what works best in your environment. Be sure not to allocate too much RAM, as you may risk that the entire server becomes unstable if you allocate more than the OS can easily spare.

The *location* of the configuration files and *default values* of the two parameters are as follows:

Location of the DME server configuration file (*Windows*):

```
..\dme\jboss\conf\wrapper.conf
```

```
set.MEM_INIT=512
```

```
set.MEM_MAX=1280
```

Windows

Location of the DME connector configuration file (*Windows*):

```
..\dmeconnector\conf\wrapper.conf
```

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=512
```

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024
```

Linux

Location of the DME server configuration file (*Linux*):

```
/etc/init.d/dme_<instancename>
```

```
# MINMEM          This is the minimum amount of RAM in Mb that
DME
#                  is to allocate
```

```
MINMEM=512
```

```
# MAXMEM          This is the maximum amount of RAM in Mb the
DME
#                  is to allocate. This cannot be more than 2048
#                  on a 32bit operating system.
```

```
MAXMEM=1280
```

Location of the DME connector configuration file (*Linux*):

```
/var/dme/instances/<instancename>/connector/conf/wrapper.conf
```

```
# Initial Java Heap Size (in MB)
wrapper.java.initmemory=512
```

```
# Maximum Java Heap Size (in MB)
wrapper.java.maxmemory=1024
```

When you make a change, restart the service, and test the results.

Configuring the connector

The main configuration of a connector is done through the DME administration web interface, in the **Connector** tab.

However, you can configure certain variables by editing the connector init script `dme_<instancename>`. This script is located in the `/var/dme/instances/<instance>/init.d/` folder. (Do not use the symbolic link to the init script found in `/etc/init.d`, since it can cause the symbolic link to be overwritten as a normal file, and updates to the init script will fail in the future.

You can for instance set certain memory options in the script.

Connectors outside the LAN

Connectors can be installed in remote places, even in places that require connection via a remote LAN via a VPN connection (WAN) or via the Internet.

This can cause some problems, since the initial connection between the connector and the DME server uses an initial IP address or hostname to connect to the DME server, with the DME server returning its IP address or hostname (the bind address) via the JNDI protocol. If there is a difference between the connector's connection point (IP or hostname) and the IP or hostname of the DME server, then the connector cannot establish a connection to the DME server.

The connection is established by the connector via the information in the `dme-config.xml` file. If the server IP is for instance `172.16.15.15` and DME is on `172.16.15.15` then DME server will respond via JNDI with the `172.16.15.15` IP address, and the connection is established.

If the connector's connection point is for instance `dme.example.com` (an external IP address), and the DME server bind address is `172.16.15.15`, then the connector cannot connect to the DME server since it will try to establish the connection to the DME server's bind address (`172.16.15.15`) and not `dme.example.com`.

As a work-around for this problem, you can configure the connector machine in the following way.

- 1 On the machine where the connector is installed, enter the IP and hostname of the DME server in the `hosts` file:

Linux: `/etc/hosts`

Windows: `c:\windows\system32\drivers\etc\hosts`

Enter `x.x.x.x` `dme.example.com`

- 2 On the DME server, set the `IP_ADDRESS` in the `dme_base` init script (Linux) or the bind address in the `wrapper.conf` (Windows) to `dme.example.com` or whatever the DME server's external connection point is, and set up a `hosts` file entry with the local IP address on the machine where the DME server is installed:

`172.16.15.15` `dme.example.com`

This will enable the DME server to bind to the local IP mentioned in the `hosts` file, but it will bind as `dme.example.com` and will return that hostname to the connector, which uses the different IP for `dme.example.com` in its `hosts` file during the connection process. Thus the connection will succeed.

Removing a connector

To remove a connector, perform the following steps:

- 1 Stop the connector (run `service dmec_<instance> stop`)
- 2 Remove the connector's init script in `/etc/init.d`
- 3 Remove the directory `/var/dme/instances/<instance>/connector`
- 4 If the name of the DME server is not the same as the connector name (`<instance>`), remove the entire `<instance>` directory.

Configuration in the web interface

After installing the connector, open the DME server web interface to complete the configuration of the DME connector.

- 1 Click the **Connector** tab.
- 2 Click the connector you just installed (identified by the name you gave it during the installation).
- 3 Click **Functions**.

Configuring DIIOP/Corba connector



In the **Functions** section of the **Connector** setup panel, go to the **Domino integration** group of settings.

➤ **General settings**

- 1 Click **Using Remote / Corba connection**.
- 2 Enter the port used by Corba (default is 63148).
If you change this, remember that the new port must be opened in the firewall.
- 3 Specify if the selected port is a secure (SSL) port by selecting the **Secure (SSL)** field.
Note that this requires that the the Domino administrator has installed the required SSL certificates as described in the Domino documentation.

➤ **Read marks**

- 1 In the **Read marks** fields, specify the server where the DME UnreadMark database is installed. This is required for e-mails in the client to be marked as read or unread.
If you leave the **Server** field blank and specify a database in the **Database** field, DME looks for the database on the current user's mail server, and the database must therefore be installed on all mail servers accessed by DME users. The database location is specified relative to Domino's data directory.

➤ **Encryption**

- 1 In the **Notes encryption** fields, choose if you want to provide encryption by getting the users' ID files from iNotes or from users uploading their ID files to the server. A description of each method is provided in the [Domino integration guide](#).
 1. Click **Get user ID files from iNotes** if you want the users to upload their ID files using the iNotes webmail interface. The users use the **Import Notes ID** function in the **Preferences > Security** page of iNotes to upload their Notes ID to the server, and DME picks it up from there.
 2. Click **Use ID storage database** if you want the users to upload their ID files to a special database provided by DME. If you choose this, you must provide the path to the IDStorage database.
- 2 In the **ID temp directory** field you can specify a path to the location where temporary copies of the ID files are stored when used for decrypting or encrypting e-mails, and by clicking **Shred ID files after use** you can add extra security by wiping the directory after a temporary ID file has been deleted, making it impossible to restore it afterwards.

Configuring Notes session connector



In the **Functions** section of the **Connector** setup panel, go to the **Domino integration** group of settings.

➤ **General settings**

- 1 Click **Using Notes session**.
- 2 The **Notes ID password** field is now available. In this field, enter the password of the proxy user (DME_Proxy) created by the Domino administrator. This user provides access to all DME users in Domino.

➤ **Read marks**

- 1 If you are running a Domino version less than 8, you must install the DME UnreadMark database as described for the DIIOP/Corba connector. See **Configuring DIIOP/Corba connector** on page 32. If you are connecting to Domino version 8 (or above), the **Read marks** fields must be left blank, otherwise the DME server will produce an error.

➤ **Encryption**

- 1 Encryption works in the same way for all types of Domino connectors. See **Configuring DIIOP/Corba connector** on page 32.

Exchange NTLM setup

As of DME 3.6 SP1, there are two ways of using NTLM authentication on MS Exchange: *Java native NTLM support* and *Oakland NTLM*. This is configured on the connector.

By default, the DME connector is configured to use the native Java NTLM. However, in some cases you need to switch to using Oakland. For instance, you need to use Oakland for Exchange 2010 if NTLM SSP v2 is required (the local policy security setting **Network security: Minimum session security for NTLM SSP based (including RPC) servers** is set to Require NTLMv2 for the CAS server).

To switch to Oakland, open the file `wrapper.conf` on the DME connector. This file is located here:

Windows: `C:\Program Files\dmeconnector\conf\`

Linux: `/var/dme/instances/<connector-name>/connector/conf/`

Open the file, and change the additional parameter `oakland=false` to `oakland=true`.

Then restart the DME connector.

To determine whether your setup requires Oakland, check if the DME connector hangs when testing the connection to your Exchange server using NTLM as authentication.

This setting does not affect installations where **Basic** authentication is used.

Securing database password and data traffic

The DME Control Center (**dmecc**) is a tool which is installed together with DME in `/usr/bin/`. It contains several useful tools for managing your DME installation. This section describes two of these tools: **Encrypt database password** and **Encrypt Connector traffic**.

A full description of the **dmecc** is pending.

Encrypting database password

To further enhance security, you can encrypt the password used for the DME database.

- 1 Log in as **root**, and run **dmecc**.

The DME Control Center screen is shown:

```
DME Control Center
Select one of the options below:

 1) Manage certificates
 2) View DME configuration

 U) Update this script
 I) Install/update DME software
 C) Collect support information
 E) Encryption related items
 M) Upgrade MySQL to version 5.5 (in development)

 H) Help
 Q) Quit DME Control Center

Enter menu item: █
```

- 2 (Optional) Enter **U** to update the DME Control Center.

The script checks an Excitor website to see if a newer version is available. If one is available, **dmecc** will exit and then update itself. You will then have to start the script again. If no newer version is available, a message tells you so, and you are returned to the main menu.

- 3 Enter **E (Encryption related items)**.

The **Encryption** menu is shown:

```
Encryption related items
Select one of the options below:

 D) Encrypt database password
 C) Encrypt Connector traffic

 H) Help
 R) Return to main menu

Enter menu item: █
```

- 4 Enter **D (Encrypt database password)**.

A message informs you that the database password will be encrypted for all installed DME Server instances, and that the process cannot be reversed.

- 5 Press **Enter** to continue (or **A** or **Q** to abort).

When you press **Enter**, **dmecc** executes commands which do the following:

1. A Java command outputs an encrypted password based on the current, clear-text password.

2. The encrypted password is entered in a separate section of the `login-config.xml` file (located in the `/var/dme/instances/base/etc/jboss/` directory). The database username is entered here also.
3. The `dmebase-DB-ds.xml` file (located in the `/var/dme/instances/base/etc/jboss/` directory) is altered to use the `EncryptDBPassword` security domain instead of the original, clear-text database password.

For a complete description of the automated steps, see the Windows installation guide (on Windows, the steps have to be performed manually).

When the database password encryption process is complete, you are returned to the **Encryption** menu.

- 6 Exit `dmecc`, and restart the DME server using:

```
/etc/init.d/dme_base restart
```

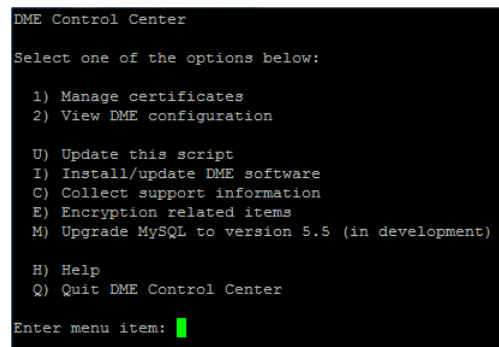
No further action concerning the database password needs to be performed on your part.

Encrypting connector traffic

To further enhance security, you can encrypt the data traffic between the DME server and the DME connector(s). This is most easily done using the **DME Control Center**. If you want to do it manually, please refer to the Windows installation documentation, and substitute the paths mentioned there with the equivalent Linux file paths.

- 1 Log in as `root`, and run `dmecc`.

The DME Control Center screen is shown:



```
DME Control Center
Select one of the options below:

 1) Manage certificates
 2) View DME configuration

U) Update this script
I) Install/update DME software
C) Collect support information
E) Encryption related items
M) Upgrade MySQL to version 5.5 (in development)

H) Help
Q) Quit DME Control Center

Enter menu item: █
```

- 2 (Optional) Enter `U` to update the DME Control Center.

The script checks an Excitor website to see if a newer version is available. If one is available, `dmecc` will exit and then update itself. You will then have to start the script again. If no newer version is available, a message tells you so, and you are returned to the main menu.

- 3 You can only set up encryption on one instance of the DME server at a time. In the first screen, choose the instance on which you want to encrypt the data traffic.
- 4 You are then asked if you want to create a new keypair and truststore. Enter Y to continue the process. Entering n returns you to the **Encryption** menu.

```
*****
***                                     ***
***   DME Connector Encryption           ***
***                                     ***
*****
Please wait while enabling encryption on the DME Server
Do you want to create a new keypair and truststore (Y/n): █
```

- 5 When you enter y to encrypt the connection to the connector, **dmecc** runs a series of commands that do the following:
 1. An SSL keystore is created on the server using the Java **keytool** command.
This operation involves the use of a password. When using **dmecc** for this operation, the standard connector password is used. This password is stated in line 29 (beginning with **conPass=**) of the **/usr/bin/dmecc** script, and is required later when editing the **wrapper.conf** file on the connectors.
 2. The instance start-up script (for instance **/etc/init.d/dme_base**) is altered.
 3. An SSL pack is downloaded from the Excitor Install site and deployed on the server.
 4. A **truststore** file is generated and placed in the following location:
/var/dme/instances/base/etc/dmessl.truststore
- 6 You must then deploy this **truststore** file on the connectors and manually make a change in the connectors' wrapper files. The **dmecc** cannot do this as there may be no access to the connector machines, and they may run Windows OS.
 1. Copy the **truststore** file from the server:
/var/dme/instances/base/etc/dmessl.truststore to the following folder on the connectors: **/var/dme/instances/<connector-name>/conf**
 2. Insert the following in the **wrapper.conf** file (as one line). Change the **wrapper.java.additional.3=** to a sequential number if 3 is already used. Also change the standard password (can be seen in line 29 (beginning with **conPass=**) of the **/usr/bin/dmecc** script):

**wrapper.java.additional.3=-Djavax.net.ssl.trustStore=
/var/dme/instances/<connector-name>/conf/dmessl.truststore**

**wrapper.java.additional.4=-
Djavax.net.ssl.keyStorePassword=password**
- 7 Finally restart the server and then the connectors.

Secure communication between the DME server and the DME connector(s) is now established.

Linux installation summary

The following is an overview of the location of files installed by DME on a Linux system. The overview is based on an installation of DME Server 3.0 and above.

The server is essentially installed as an instance called **base**. All files used by this instance are located in a folder called

```
/var/dme/instances/base
```

For other instances, a name is given to the instance during installation. The base path of the instance is then the same as for the **base** instance, but **base** is replaced for the instance name. This way, two instances can run and be configured individually, without dependencies outside that folder.

The **base** folder contains a number of subfolders:

```
app  
etc  
etc/jboss  
log  
conf  
deploy  
filestore  
dev  
backup  
bin  
init.d  
lib
```

Furthermore, the following three folders are created by JBoss when DME is started:

```
data  
tmp  
work
```

The folders **tmp** and **work** are temporary folders, and are purged by the init script every time DME is started to avoid old cache information that might cause problems in case the EAR file is updated or replaced. The **data** folder contains information that JBoss needs for its internal messaging system, which among other things is used for managing network push connections.

The folder **/var/dme/backup** is used by the installer when performing upgrades and maintenance.

Configuration files

The folder **etc** contains the main configuration for DME, including **keystore**, **cryptoKeystore**, **license.xml**, and **DMECentralServicesSSL.truststore** (the certificate used for Apple Push Notification and Central Services). These files have symbolic links in the **conf** and **deploy** folders, meaning that you can configure and maintain the instance from *one* location.

The **etc/jboss** folder contains JBoss configuration files for DME:

```
dmebaseDB-ds.xml  
server.xml  
jboss-log4j.xml  
jboss-service.xml  
ejb-deployer.xml  
login-config.xml  
smartlinkConfig.xml
```

Kannel

Kannel can be installed on any of the following GNU/Linux distributions, without having to install DME:

- Red Hat Enterprise Linux Server 4 (RHEL4)
- Red Hat Enterprise Linux Server 5 (RHEL5)
- Fedora Core 5 (FC5)
- Fedora Core 7 (FC7)
- SuSE Linux Enterprise Server 10 (SLES10)

-and probably more. This means that you can install Kannel in a central location for several DME servers to share one SMS modem. This limits the self provisioning feature, as this feature requires a separate Kannel and SMS modem per DME server, since Kannel can only send incoming SMS messages to one URL (one DME server).

The entire configuration for Kannel is installed into

`/var/dme/kannel/`

Subfolders in this folder represent the file system locations where symbolic links are place to enable easy configuration and upgrades.

The `smsmodem` link to `/dev/ttyS0` is located in `/var/dme/kannel/dev/smsmodem`, to which all new DME installations will point by default. Hence, the link in

`/var/dme/instances/<instance>/dev/smsmodem`

points to

`/var/dme/kannel/dev/smsmodem`

which points to

`/dev/ttyS0`

The configuration file `/etc/kannel.conf` is a symbolic link to `/var/dme/kannel/etc/kannel.conf`, and the init script to start and stop Kannel in `/etc/init.d/kannel` points to `/var/dme/kannel/init.d/kannel`.

All log files from Kannel are located in

`/var/dme/kannel/log/`

Business continuity

In case of a disastrous failure of the DME system due to hardware failure or otherwise, it is important to have a business continuity (disaster recovery) plan at hand.

The following steps are required to move DME to another server. The new DME installation will be a replica of the old one. The descriptions cover both Windows and Linux servers and connectors.

Backup

For a successful disaster recovery, an up-to-date backup of the following is required:

From the DME server machine:

- `<DME_HOME>\etc\cryptoKeystore`
- `<DME_HOME>\etc\sslprivatekey.pem`
- `<DME_HOME>\etc\sslcertificate.pem`
- `<DME_HOME>\etc\rootCA.pem`
- `<DME_HOME>\etc\signrequest.csr` (use for renewing certificate)
- `<DME_HOME>\deploy\jboss-web.deployer\server.xml`
- `<DME_HOME>\jboss\conf\wrapper.conf` (Windows only)
- `/init.d/jboss` (Linux only)

`<DME_HOME>` is the DME installation directory:

Windows: `C:\Program Files\dme\jboss\server\default`

Linux: This is typically called `base`, and is usually located in `/var/dme/instances/base/`

From the DME connector machine(s):

- `<CON_HOME>\conf\cryptoKeystore`
- `<CON_HOME>\conf\dme-config.xml`
- `<CON_HOME>\conf\wrapper.conf`
- `<CON_HOME>/connector/bin/dme-connector` (Linux only) "start-up script"

`<CON_HOME>` is the DME Connector directory (on the server where it is installed).

Windows: `C:\Program Files\dmeconnector`

Linux: `/var/dme/instances/<connector-name>/`

DME database:

Make a complete backup of the DME database.

On **Windows**, use your preferred MS SQL Server backup program.

On **Linux**, make an SQL dump of the database, compress the file, and copy it to a safe location. Use this command to export the database (`base` is the default name of the DME database):

```
mysqldump --databases base > /var/dme/backup/<date>/dme_mysqldump.sql
```

Restore

To restore DME after a complete system failure, follow these steps.

Restoring the DME server:

- 1 If the hardware on which the new DME server is to run is not the same as before, you need to obtain a *new license key*. The license key is bound to the hardware MAC address of the DME server. A new license key can be obtained from Excitor A/S. If the Copenhagen office is closed, you can obtain a temporary trial license from your local DME Partner, and replace it with the operational license later on.
- 2 Make a normal installation of the DME Server. Make sure to use the same version of the DME Server as the one you are replacing. You can skip the SSL certificate info section of the installation.
- 3 If you are using a Windows MS SQL Server database, make a connection to the old DME database. Do not start the DME server!
- 4 If you are running on a Linux machine, you need to re-import the MySQL database dump to a new database. Do the following:
 1. Copy the database backup to the new DME server. From the command prompt (\$), type the following commands:
 2. `$ mysql` (to open the MySQL server)
 3. `$ show databases;` (to show all databases on the MySQL server. DME uses `base` by default)
 4. `$ drop database base;` (to delete the DME database just created by the installer)
 5. `$ create database base;` (to create a new, clean database called `base`)
 6. `$ use base;` (to switch to the new database)
 7. `$ \. /var/dme/backup/<date>/dme_mysql_dump.sql;` (to import the dump to the new DME database. Change the path to the database dump as appropriate)
 8. `$ show tables;` (to verify that the dump was imported - there should be a lot of tables present)
 9. `$ quit;` (to exit the MySQL server interface)
- 5 Restore the following files from your backup:
 - `<DME_HOME>\etc\cryptoKeystore`
 - `<DME_HOME>\etc\sslprivatekey.pem`
 - `<DME_HOME>\etc\sslcertificate.pem`
 - `<DME_HOME>\etc\rootCA.pem`
 - `<DME_HOME>\etc\signrequest.csr` (use for renewing certificate)
 - `<DME_HOME>\deploy\jboss-web.deployer\server.xml`
 - `<DME_HOME>\jboss\conf\wrapper.conf` (Windows only)
 - `/init.d/jboss` (Linux only)`<DME_HOME>` is the DME installation directory:

Windows: `C:\Program Files\dme\jboss\server\default`

Linux: This is typically called **base**, and is usually located in
`/var/dme/instances/base/`

- 6 Start the DME server, and log in.

Restoring DME connectors:

- 1 Perform a normal installation of the connector on the Windows or Linux server.
Make sure to use the same version as the DME server.

Do not start the connector!

- 2 Restore the following files from your backup:

`<CON_HOME>\conf\cryptoKeystore`

`<CON_HOME>\conf\dme-config.xml`

`<CON_HOME>\conf\wrapper.conf`

`<CON_HOME>/connector/bin/dme-connector` (Linux only) "start-up script"

`<CON_HOME>` is the DME Connector directory (on the server where it is installed).

Windows: `C:\Program Files\dmeconnector`

Linux: `/var/dme/instances/<connector-name>/`

- 3 Start the connector.

The system is now operational again.