Installing DME

DME 4.6 for Linux

Document version 1.6

Published 10-05-2017

Contents

DME installation guide 3

Requirements 4

Anti-virus software 4

Installation overview 6

Getting the installation files 7

Installing the DME server 11

Main installation menu 12

Base installation 13

MySQL and MariaDB 14

MySQL/MariaDB on remote host 17

Remote database setup 18

Firewall and other setup 19

Entering certificate information 20

Installation complete 21

Managing SSL certificate 22

Self-signed certificate 23

Commercial certificate 23

Clustering 25

Instance management 26

Creating an instance 27

Viewing instances 30

Removing instances 31

Installing the DME connector 32

Collaboration system considerations 33

Removing a connector 34

Connectors outside the LAN 34

Kannel install or upgrade 36

Detecting SMS modem 37

Installing Kannel package 37

Update Java 38

Settings and security 39

RAM usage 39

Securing the traffic between server and connector(s) 40
Deactivate encryption of traffic between server and connectors . 44
Encrypting the database password 45
Using a proxy 47
Using two NICs 48
DME administration web interface 49
Upgrading 51
Upgrading the DME server 51
Upgrading the DME connector 53
Contact mapping files 54
If the connector upgrade fails 54
Business continuity 55
Backup 55
Restore 55
List of procedures 57

DME installation guide

Welcome to the installation guide for DME 4.6 for Linux.

A DME system consists of a DME Server, at least one DME Connector, a database, and optionally an AppBox (G/On) server. If you want to integrate with an external MDM system, such as SOTI MobiControl, then this must be installed as well.

This document describes how to install the DME Server and the DME Connector on Linux.

You can find information about installing the other components at the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/docs/checklist***.

DME is created by Soliton Systems. This is our logo and contact information:

Soliton Systems Europe
Spotorno Allé 12
2630 Taastrup
Denmark

Phone: +45 70 21 68 00
E-mail: mail@solitonsystems.com
Website: ***Soliton website http://solitonsystems.com/***

Some legal stuff:

Requirements

Before installing DME, make sure your hardware and software comply with the specifications in the **System Requirements** document at the ***DME Resource Center*** ***http://resources.solitonsystems.com/docs/system-requirements***. Also please stop any running Java applications before installing, for the reasons stated in ***Installing the DME server*** on page 11.

Furthermore, please note the following:

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 at the ***DME Resource Center*** ***http://resources.solitonsystems.com/docs/firewall-rules***. 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 cannot 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.

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

Anti-virus software

Before installing DME, please read this note about the use of anti-virus software on the server.

DME is a time-critical application, which relies on good I/O throughput to the file system, 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 Linux servers, 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. In some cases, the AV software must be un-installed completely to be certain that it does not affect the running of DME.

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

On the DME server, exclude the entire DME structure (`<DMEPATH>`) from real-time A/V scanning.

This would typically be everything in and below

- `/var/dme/`

This path includes the connectors.

On both the server and connector servers, exclude the following folders from A/V scanning:

Java

This is your `JAVA_HOME` path.

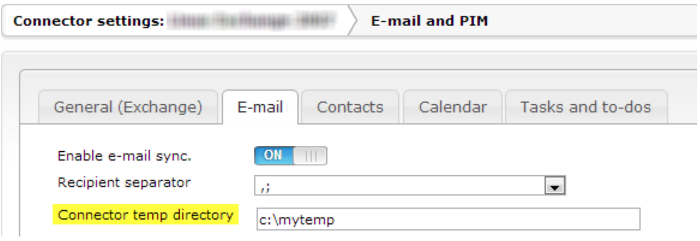
Temporary directories

The paths to exclude are specified in the `TMPDIR` variable.

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 real-time AV scanning:

1. Open the DME web administration interface.
2. Click **Connector** > the connector you wish to edit > **E-mail and PIM** > **E-mail**.

3. In the **Advanced** section, enter the temporary folder in the field **Connector temp directory**.



Connector settings: [redacted] 〉 E-mail and PIM

Enable e-mail sync. ON
Recipient separator ,;
Connector temp directory c:\mytemp

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

Furthermore, due to the packet corruption mentioned earlier, Packet Inspection should be turned off - at least for the DME sync ports `5011`. 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.

Installation overview

This is a high-level overview of the installation process. To go from nothing to a working DME installation, you need to complete the following steps. Each step is explained further on in this guide.

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 installation, run the database upgrade scripts. Note that this does not apply when a local database is used.
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. Connection information for the MS SQL Server or Remote MySQL database server.
   2. SSL certificate information to create a certificate request. You can have the request signed by a public certificate authority.
5. Perform the following steps for each DME connector:
   1. Install the DME connector, entering the information to connect with 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 **company.com - London Office - Exchange Mail**
   2. Start the DME connector. It will attempt to connect to the DME server. If successful, 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.
   3. Upload your DME license to the server.
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.

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

1. In the **Main** panel section: the information you filled in during installation of the connector is already shown.
2. In the **Domain** panel section: Provide information about your LDAP/AD directory server.
3. 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).
4. In the **E-mail and PIM** panel section: For Domino installations, specify if the connector is using **Notes session**.

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

Getting the installation files

To access the installation files, you need to log in to the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/dl/dme-installers*** and go to the **DME installers** page. Contact your DME partner if you do not have a login or you are not authorized to view the page.

You can download the files directly to the server, or you can download them to any computer and then copy the files to a portable medium (for *offline installation*).

➢ *Getting the installation files*

The following applies if you are working from the machine on which DME is to be installed. Note that the machine requires Internet access.

1. Log in to the Linux terminal as `root`.

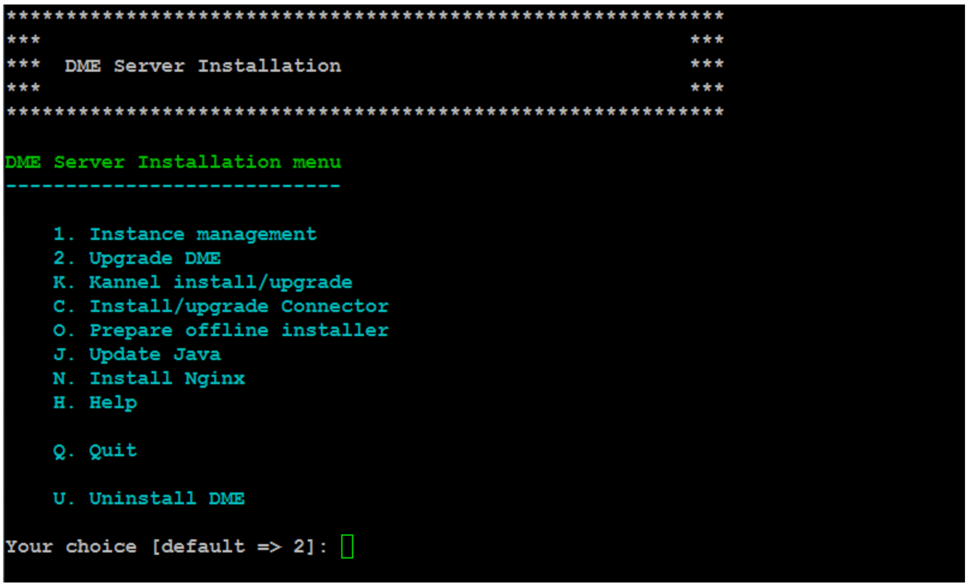
   If you cannot log in as `root`, you can run the commands using `sudo`, `su -root`, or `su -c '<command>'`.

2. Download the installation file from the Install site:

   ```
   wget -N
   http://install.solitonsystems.com/install/dme-install.
   sh
   ```

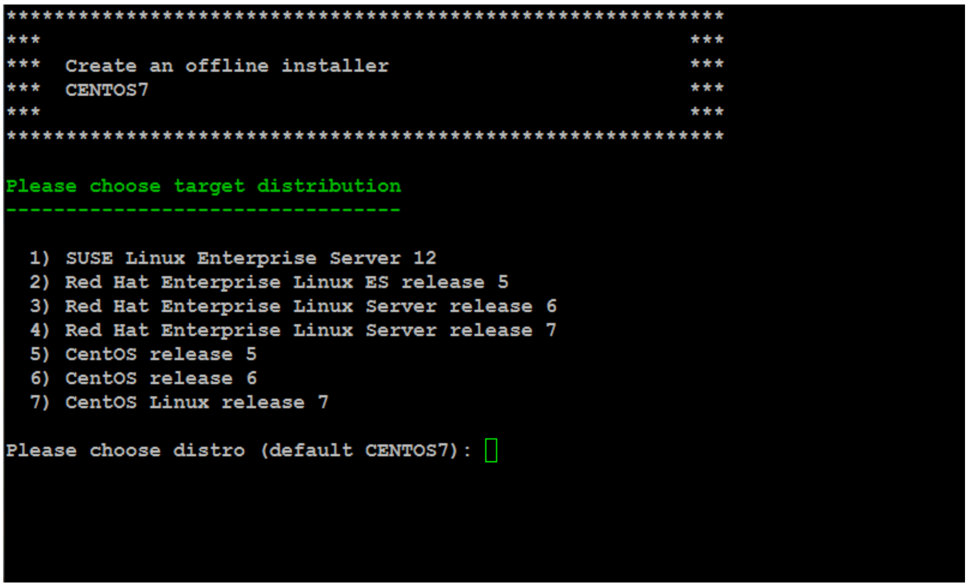
If the machine on which DME is to be installed does not have internet access, you need to get an *offline copy* of the installation files. Do the following from a machine which is connected to the Internet:

1. Get the installer as described above.
2. Run the installer, and choose `O. Prepare offline installation` in the main menu.



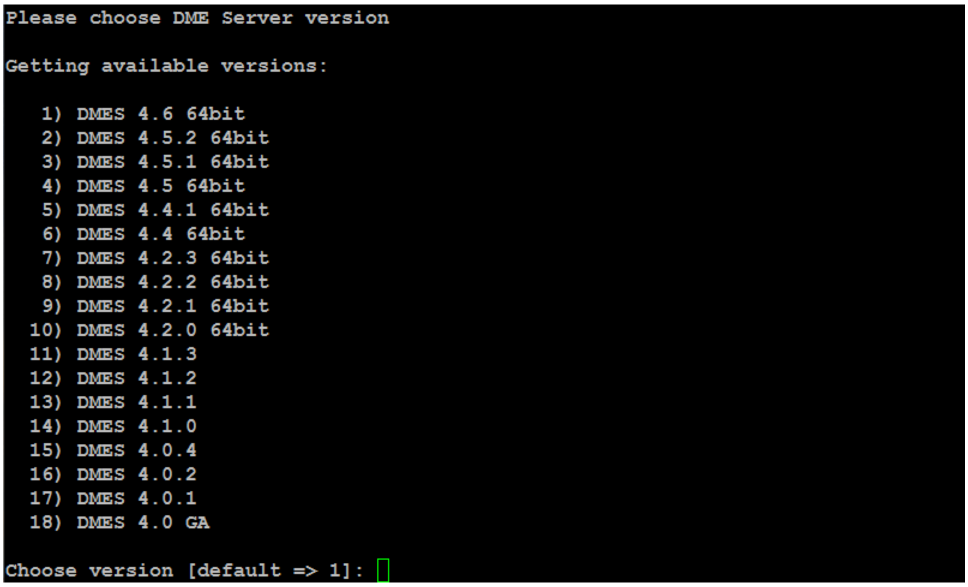
```
*************************************************************
***                                                      ***
***  DME Server Installation                             ***
***                                                      ***
*************************************************************

DME Server Installation menu
----------------------------

    1. Instance management
    2. Upgrade DME
    K. Kannel install/upgrade
    C. Install/upgrade Connector
    O. Prepare offline installer
    J. Update Java
    N. Install Nginx
    H. Help

    Q. Quit

    U. Uninstall DME

Your choice [default => 2]: 
```

3. Select the supported Linux distribution on which you will be installing DME.



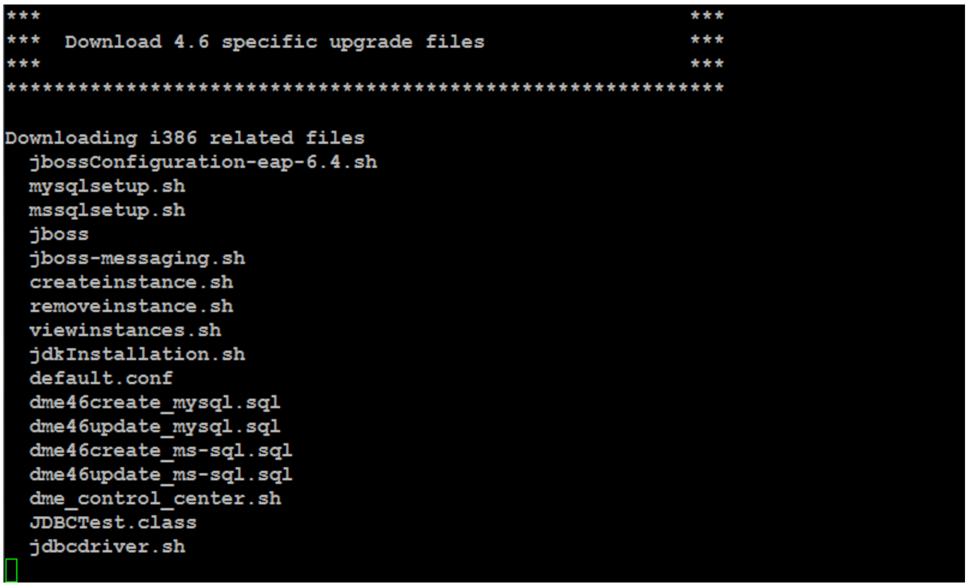
```
**************************************************************
***                                                        ***
***  Create an offline installer                           ***
***  CENTOS7                                               ***
***                                                        ***
**************************************************************

Please choose target distribution
---------------------------------

  1)  SUSE Linux Enterprise Server 12
  2)  Red Hat Enterprise Linux ES release 5
  3)  Red Hat Enterprise Linux Server release 6
  4)  Red Hat Enterprise Linux Server release 7
  5)  CentOS release 5
  6)  CentOS release 6
  7)  CentOS Linux release 7

Please choose distro (default CENTOS7):
```

4. Choose the version of DME you will be installing on the target machine.



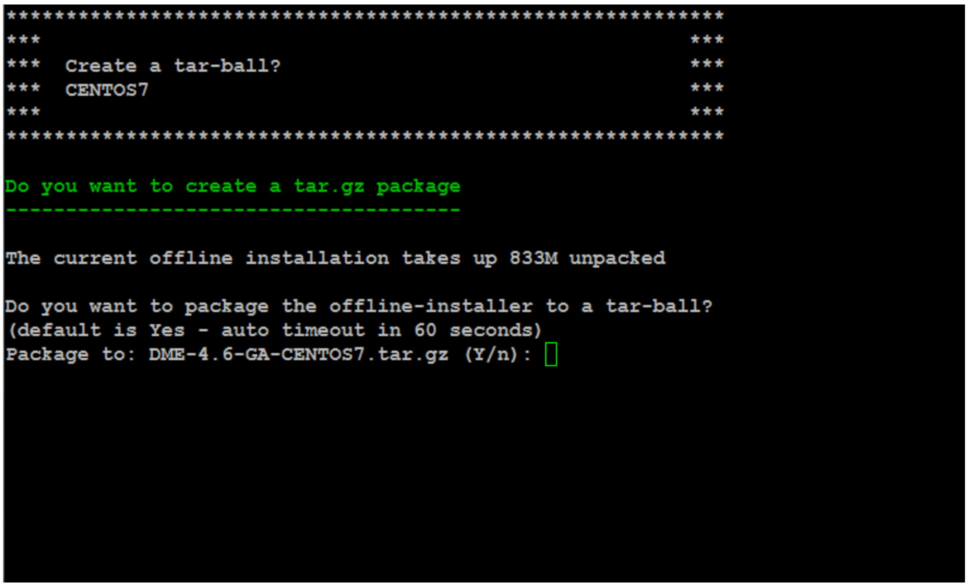
```
Please choose DME Server version

Getting available versions:

   1) DMES 4.6 64bit
   2) DMES 4.5.2 64bit
   3) DMES 4.5.1 64bit
   4) DMES 4.5 64bit
   5) DMES 4.4.1 64bit
   6) DMES 4.4 64bit
   7) DMES 4.2.3 64bit
   8) DMES 4.2.2 64bit
   9) DMES 4.2.1 64bit
  10) DMES 4.2.0 64bit
  11) DMES 4.1.3
  12) DMES 4.1.2
  13) DMES 4.1.1
  14) DMES 4.1.0
  15) DMES 4.0.4
  16) DMES 4.0.2
  17) DMES 4.0.1
  18) DMES 4.0 GA

Choose version [default => 1]:
```

5. The installer starts downloading the files required for the selected OS and version of DME.



```
***                                                         ***
***  Download 4.6 specific upgrade files                    ***
***                                                         ***
*************************************************************

Downloading i386 related files
  jbossConfiguration-eap-6.4.sh
  mysqlsetup.sh
  mssqlsetup.sh
  jboss
  jboss-messaging.sh
  createinstance.sh
  removeinstance.sh
  viewinstances.sh
  jdkInstallation.sh
  default.conf
  dme46create_mysql.sql
  dme46update_mysql.sql
  dme46create_ms-sql.sql
  dme46update_ms-sql.sql
  dme_control_center.sh
  JDBCTest.class
  jdbcdriver.sh
```

6. Finally, the installer asks whether you want to create a zipped tarball with the required files in your home directory.



```
*************************************************************
***                                                         ***
***  Create a tar-ball?                                     ***
***  CENTOS7                                                ***
***                                                         ***
*************************************************************

Do you want to create a tar.gz package
--------------------------------------

The current offline installation takes up 833M unpacked

Do you want to package the offline-installer to a tar-ball?
(default is Yes - auto timeout in 60 seconds)
Package to: DME-4.6-GA-CENTOS7.tar.gz (Y/n):
```

The tarball can now be moved to a machine running the specified OS, unpacked, and DME can be installed with no connection to the Install website as described in ***Installing the DME server*** on page 11.

Installing the DME server

➢ ***Installing the DME server***

Before running the installer, decide if you want to run DME with a MySQL on localhost, MySQL on a remote server, or with MS SQL Server. If you go for MySQL on localhost, you should verify that MySQL is in fact installed on the server. If you go for a remote solution, verify that a database and a database user have been created. For more information, see ***MySQL and MariaDB*** on page 14 and subsequent sections.

If you do not set up the database first, the installer will exit at one point and allow you to do it. So it is easier to do it first.

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
```

After deciding about your database platform:

1. Run the installer as `root`:

   `sh dme-install.sh` (the installer; see ***Getting the installation files*** on page 7).

   DME recommends 20 GB free disk space for installation. If less than that is available, a warning will appear. You can then choose to type `quit` to exit the installer, free disk space, and re-run the installer, or you can choose to type `ignore` to proceed with the installation.

   This launches the latest version of the Linux installer.

2. Enter credentials that allow you to download the installation files.

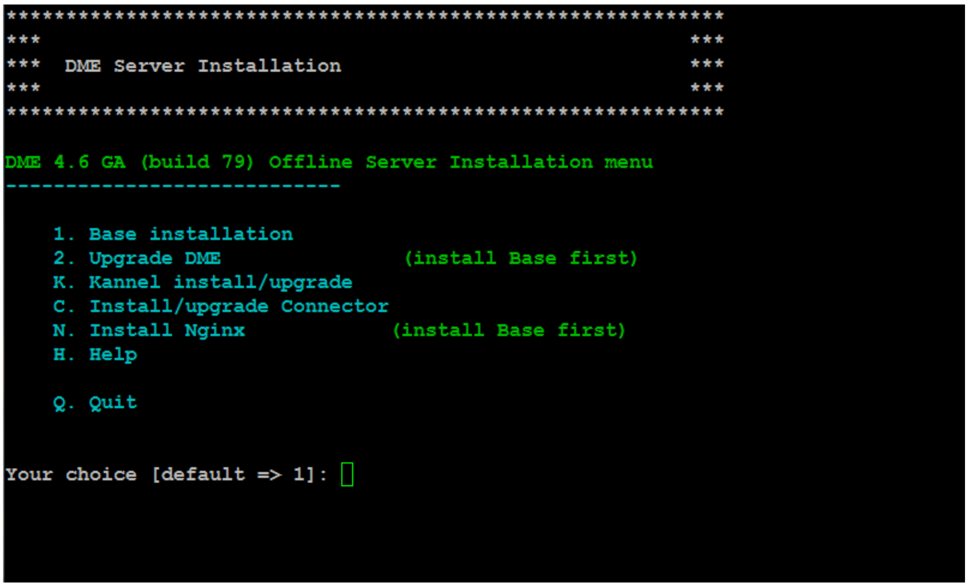
   The credentials you must enter are *either* your username and password for the DME Resource Center, *or* your username and password for the DME support (RFS) site. The installer checks your credentials, and if they are accepted, you can continue.

3. 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 **DME Server Installation** menu is displayed.

See the subsequent sections for details about the main installation menu.

Main installation menu



```
************************************************************
***                                                      ***
***  DME Server Installation                             ***
***                                                      ***
************************************************************

DME 4.6 GA (build 79) Offline Server Installation menu
----------------------------

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

    Q. Quit


Your choice [default => 1]:
```

The main installation menu shows you the options that are currently available. For example, **Instance management** and **Upgrade DME** cannot be selected on a clean system where the DME **base** instance has not yet been installed.

The installation and upgrade of the Kannel server is present in the menu at all times, since Kannel is a separate program and installed separately. If Kannel is installed on a server without DME, some manual configuration is required for self-provisioning to work correctly. Ask DME Support for more information.

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.

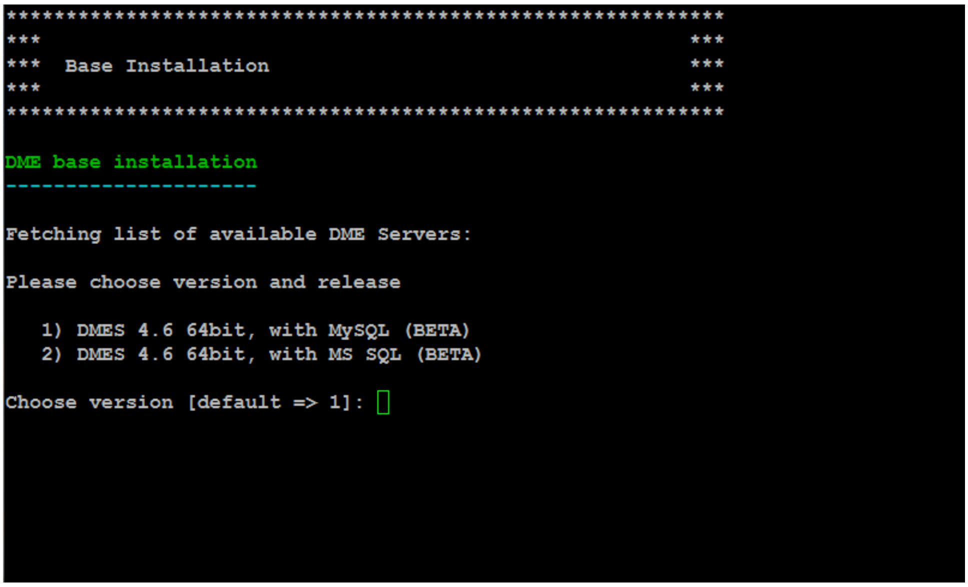
Type your choice, and press **Enter**:

- Press **I** to perform base installation/Instance management (see ***Base installation*** on page 13 or ***Instance management*** on page 26).
- Press **2** to upgrade DME (only possible if DME exists on this machine). See ***Upgrading the DME server*** on page 51.
- Press **K** to install or upgrade Kannel (see ***Kannel install or upgrade*** on page 36).
- Press **C** to install or upgrade a DME connector (see ***Installing the DME connector*** on page 32 and ***Upgrading the DME connector*** on page 53).
- Press **O** to prepare an offline installation (see ***Getting the installation files*** on page 7).
- Press **J** to update Java (if applicable). See ***Update Java*** on page 38.
- Press **H** for a short help text for the selectable items.
- Press **Q** to quit the installer.
- Press **U** to remove DME.

See subsequent sections for more information about each choice.

Base installation

When you choose **Base installation**, the installer will show a list of DME versions that are available for installation.

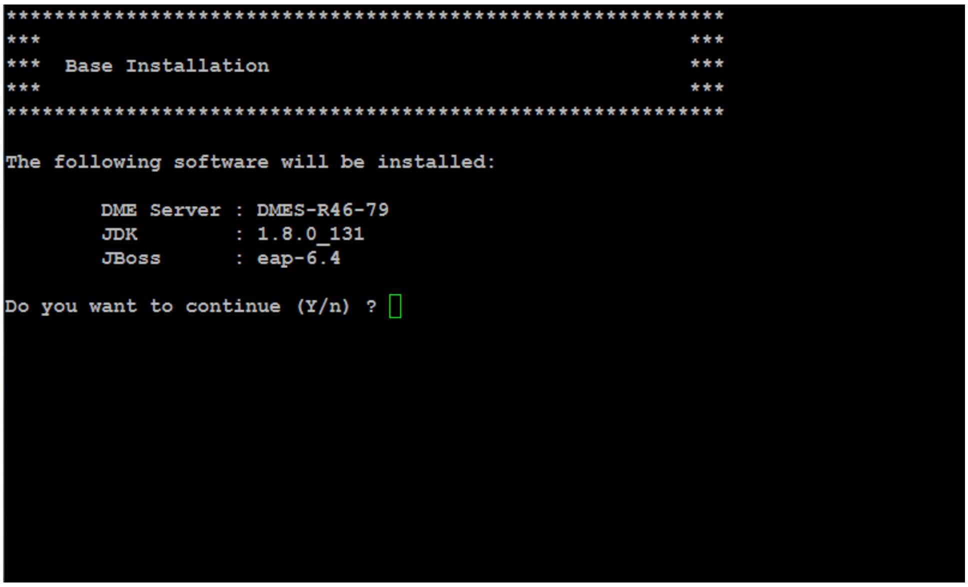


```
************************************************************
***                                                      ***
***  Base Installation                                   ***
***                                                      ***
************************************************************

DME base installation
---------------------

Fetching list of available DME Servers:

Please choose version and release

   1) DMES 4.6 64bit, with MySQL (BETA)
   2) DMES 4.6 64bit, with MS SQL (BETA)

Choose version [default => 1]: 
```

Please note that showing this list requires Internet access. If you do not have Internet access from the machine on which you want to install DME, you should create an offline installation package on a machine with Internet access, and copy it the DME server.

Select a version, and press **Enter** to install it.

A confirmation screen shows a list of your choice of DME version and any auxiliary files and dependencies that must be installed as well.



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

The following software will be installed:

        DME Server  : DMES-R46-79
        JDK         : 1.8.0_131
        JBoss       : eap-6.4

Do you want to continue (Y/n) ?
```

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 chose a version of DME that runs with 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.

The DME installer will not actually install the database software. See the next section for more information about local databases.

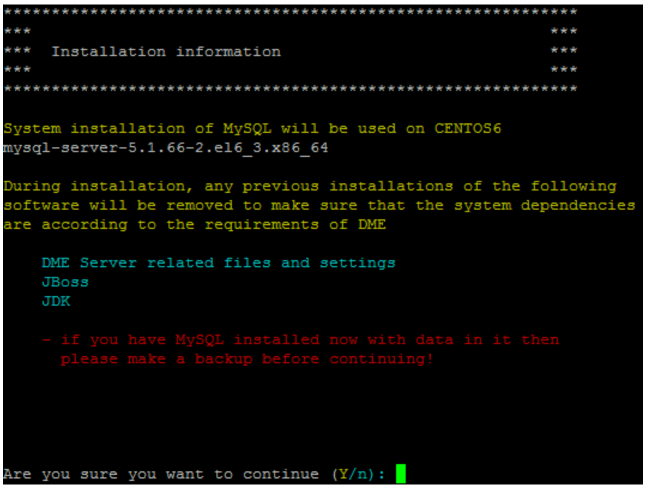
Press **Enter** to continue, or **n** to abort the installation.

MySQL and MariaDB

If you want to run DME with MySQL or MariaDB, the database software must be installed on the machine. This naturally applies when you plan to use MySQL/MariaDB on localhost, but also if you plan on using a remote database server, as DME needs the MySQL/Maria DB client installed to be able to connect to the remote server.

> Please note that installer only makes references to MySQL - however, if you are installing MariaDB, the references to MySQL apply to your MariaDB database.

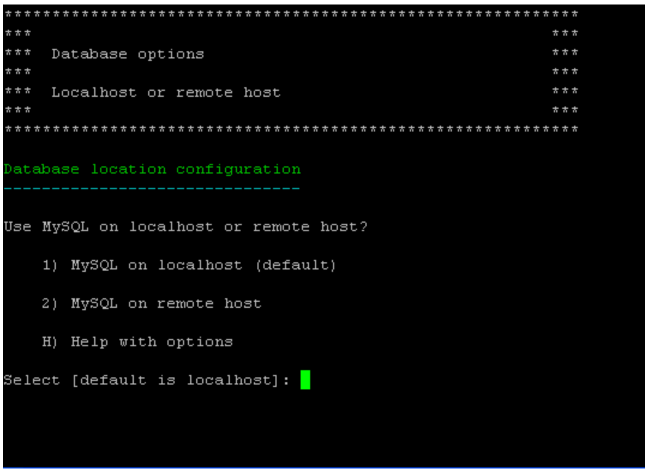
If the database software has already been installed, you should be aware that DME will use the system database. A warning about this is shown when you run the installer - something like this:



```
************************************************************
***                                                      ***
***  Installation information                            ***
***                                                      ***
************************************************************

System installation of MySQL will be used on CENTOS6
mysql-server-5.1.66-2.el6_3.x86_64

During installation, any previous installations of the following
software will be removed to make sure that the system dependencies
are according to the requirements of DME

    DME Server related files and settings
    JBoss
    JDK

    - if you have MySQL installed now with data in it then
      please make a backup before continuing!



Are you sure you want to continue (Y/n): 
```

If any data exists in the database, *now is your last chance to back it up!*

When you press **Enter** to continue at this point in the installation, you can choose to let DME use a local database installation (default) or a remote installation. It may seem a bit odd that you were given the warning above if you are really planning to use a Remote SQL connection, but that is currently how it works.



```
************************************************************
***                                                      ***
***  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**, the installation continues, provided that MySQL/MariaDB has been installed on the current machine.

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.

If the database software has not been installed, the DME installer will exit at this point with a message about how to install MySQL/MariaDB. This is described in the following section - see ***Installing MySQL/MariaDB*** on page 16.

Installing MySQL/MariaDB

If you plan to use MySQL as a database rather than MS SQL Server, you must install the database software locally on your machine. DME cannot install it for you due to licensing restrictions.

Note that on Red Hat Enterprise Linux 7 and CentOS 7, the MySQL database is not included at all. Instead, MariaDB is included. DME is compatible with MariaDB, and will connect to that on RHEL7 and CentOS 7.

➢ *Installing MySQL or MariaDB*

The following steps are required before installing DME, if MySQL or MariaDB is not already installed. The description below is for Red Hat or CentOS, but the process is similar for SuSE using `yast` commands.

1. Make sure that the server machine is patched with the latest updates. Run the command

   ```
   yum update
   ```

   on the command line, and follow the prompts.

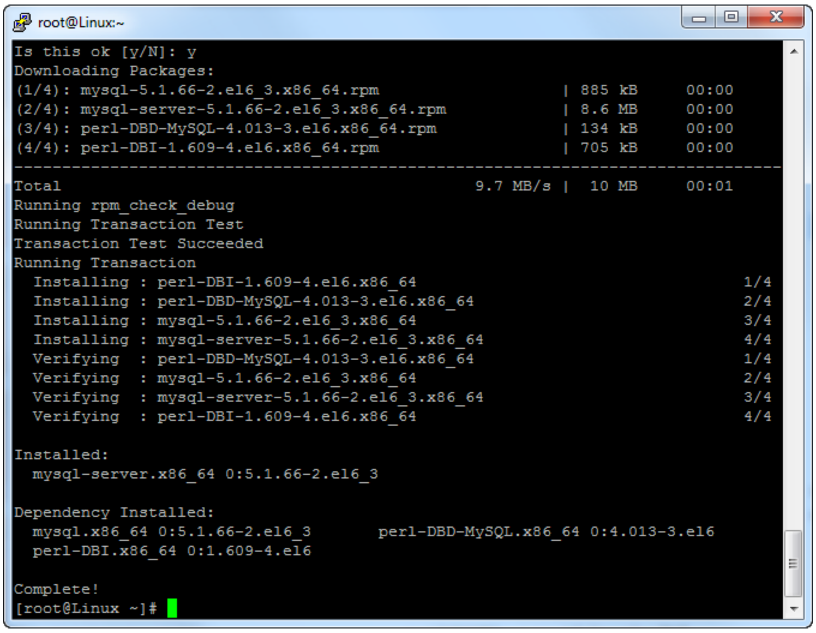
2. Install the MySQL database on the server machine. Run the command

   `yum install mysql-server` (before RHEL/CentOS version 7), *or*

   `yum install mariadb-server` (from RHEL/CentOS version 7)

   and follow the prompts to install the database server.

After installation, the screen might look like this:



```
Is this ok [y/N]: y
Downloading Packages:
(1/4): mysql-5.1.66-2.el6_3.x86_64.rpm                   | 885 kB     00:00
(2/4): mysql-server-5.1.66-2.el6_3.x86_64.rpm            | 8.6 MB     00:00
(3/4): perl-DBD-MySQL-4.013-3.el6.x86_64.rpm             | 134 kB     00:00
(4/4): perl-DBI-1.609-4.el6.x86_64.rpm                   | 705 kB     00:00
--------------------------------------------------------------------------------
Total                                           9.7 MB/s |  10 MB     00:01
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : perl-DBI-1.609-4.el6.x86_64                                  1/4
  Installing : perl-DBD-MySQL-4.013-3.el6.x86_64                            2/4
  Installing : mysql-5.1.66-2.el6_3.x86_64                                  3/4
  Installing : mysql-server-5.1.66-2.el6_3.x86_64                           4/4
  Verifying  : perl-DBD-MySQL-4.013-3.el6.x86_64                            1/4
  Verifying  : mysql-5.1.66-2.el6_3.x86_64                                  2/4
  Verifying  : mysql-server-5.1.66-2.el6_3.x86_64                           3/4
  Verifying  : perl-DBI-1.609-4.el6.x86_64                                  4/4

Installed:
  mysql-server.x86_64 0:5.1.66-2.el6_3

Dependency Installed:
  mysql.x86_64 0:5.1.66-2.el6_3       perl-DBD-MySQL.x86_64 0:4.013-3.el6
  perl-DBI.x86_64 0:1.609-4.el6

Complete!
[root@Linux ~]#
```

3. Run the DME installer again.

When you are running MySQL/MariaDB on localhost, DME will set up the database for you. If you plan to run MySQL/MariaDB on a remote host, you need to set up the database as described in the next section.

MySQL/MariaDB on remote host

Rather than using MySQL or MariaDB installed on localhost, you can use a remotely installed database.

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

DME supports version 5.*x* of MySQL and version 10.*x* of MariaDB.

Create a database on the database server:

1. Log in as the MySQL user **root**:

   ```
   root@localhost $ mysql -u root -p
   ```

2. Create a database. Standard practice is to call the database **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.

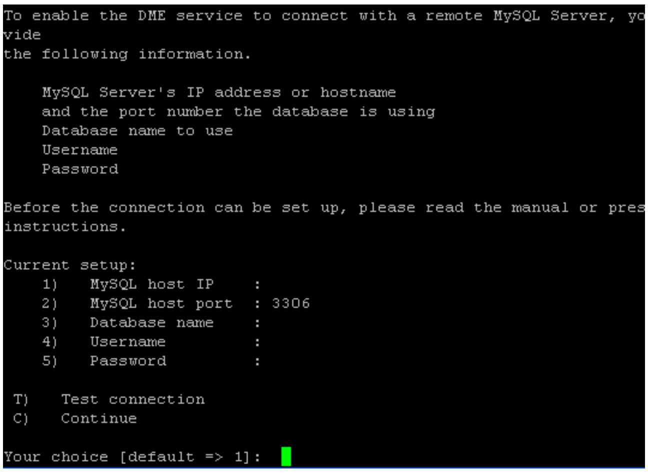
The MySQL / MariaDB client must be installed on the DME server to enable database manipulation from the DME server. You can test the connection from the DME installation when you are asked to fill in the DBMS information.

Remote database setup

When installing DME with a local MySQL database, the database will be created (and upgraded) automatically.

If you chose a remote MySQL database or an MS SQL Server 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/MariaDB on remote host*** on page 17 above and the **Database scripts** section at the ***DME Resource Center https://resources.solitonsystems.com/dl/database-scripts*** for more information.

You are asked for connection details for the remote database installation (note that the screen looks slightly different for MS SQL Server):



```
To enable the DME service to connect with a remote MySQL Server, yo
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.

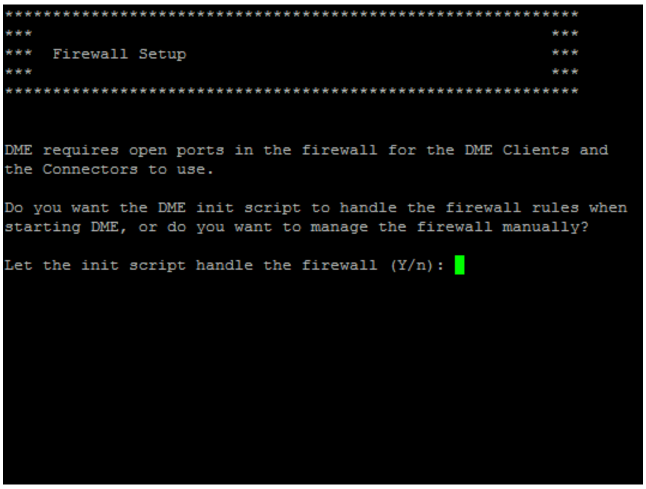
You can manually bypass the DBMS configuration for the DME instance by pressing **C**ontinue. The DME instance will not be able to start properly, and you will later have to change the settings manually in the `dmebaseDB-ds.xml` file, which is located in

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

DME depends on the DBMS and cannot function without one.

Firewall and other setup

After the installer has downloaded DME files and dependencies, you are asked if you want to let the installer handle the firewall.



```
*************************************************************
***                                                       ***
***  Firewall Setup                                       ***
***                                                       ***
*************************************************************


DME requires open ports in the firewall for the DME Clients and
the Connectors to use.

Do you want the DME init script to handle the firewall rules when
starting DME, or do you want to manage the firewall manually?

Let the init script handle the firewall (Y/n):
```

DME requires certain ports in the firewall to be open (see the ***DME Resource Center http://resources.solitonsystems.com/docs/firewall-rules***), which are used by the DME clients and connectors.

If you press **Y** or **Enter** to accept the default choice, you allow the DME init script (which is created by the installer) to open the required ports when DME is started. This is done by adjusting `iptables` settings.

If you do not accept this, you must configure the firewall manually according to the specifications at the **DME Resource Center** (referenced above).

When you have made your choice, the installer proceeds to install and configure software, including the database if you are running MySQL on localhost.

Entering certificate information

A certificate is required to establish an encrypted connection between the DME server and the devices. In the SSL certificate setup screen, you enter information to prepare the certificate request.

DME does not use the built-in Java keystore for certificate handling or the web-based certificate uploading. You must therefore fill in the certificate details for the DME server or DME instance. The certificates are RSA encoded PEM certificates.

Enter the information to create the certificate request. Fields marked with a * are required for self-signed certificate; all fields are required for a public CA certificate (recommended). If the information is not relevant, enter **NA** in the field.

Common Name (external host name, CN)

Enter the host name that the mobile devices will use to connect to the DME server (the *server path*). For instance: **dme.company.com** if the external connection (server path) will be **https://dme.company.com:5011**. It is very important to enter this correctly, as the device cannot connect to the server if you get this wrong. Do not use the IP address as host name, as the iOS and Android mobile devices cannot handle IP addresses as server path.

Country code (C)

2-letter ISO country code, for instance **UK**. For a list of valid country codes, see ***www.iso.org https://www.iso.org/obp/ui/#search***.

Administrator e-mail

Enter **NA**, as the administrator email address is not used.

Organization Name (O)

The name of your company.

Organizational Unit (OU)

Department name or similar.

State or Province (ST)

Name of state/province.

Locality name (L)

City name.

During the server installation, the information supplied here will be used to create a certificate request.

Press a number to edit a field. More help is shown when you edit each field.

Press **C** when you are done.

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

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 at signed certificate.

- **`signrequest.csr`**

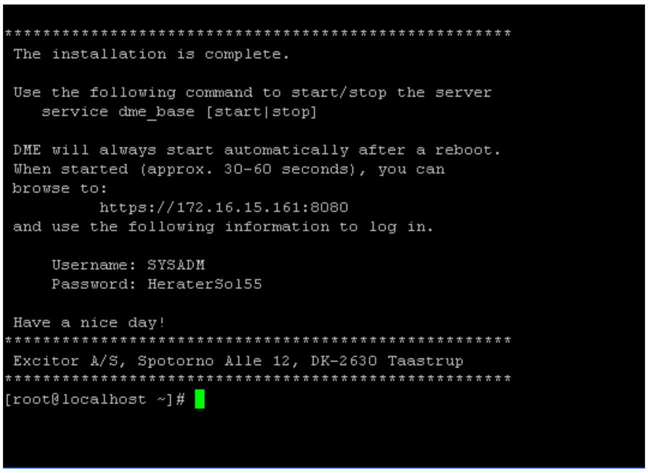
  This is the file you send to Soliton Systems or a commercial CA for signing.

For more information about the SSL certificate, see ***Managing SSL certificate*** on page 22.

Installation complete

The installation is now complete. You can now install and set up connectors etc. while you wait for the SSL certificate signed by 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 username 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 username and password after first login. To change the SYSADM password in the DME web interface, see The administration web interface.

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>`.

Next step is to install a connector. See ***Installing the DME connector*** on page 32.

Managing SSL certificate

In order to sign the SSL connection between the DME server and the devices, a certificate must be installed on the DME server.

Two types of certificates can be used with DME:

1. *Self-signed* certificates: These can be used by DME for testing the initial connections, but must not be used in a production system. See ***Self-signed certificate*** on page 23.
2. *Commercial* certificates: These are certificates signed by a commercial Certificate Authority (CA) such as Verisign, RapidSSL, or similar. See ***Commercial certificate*** on page 23.

The following information applies regardless of the type of certificate you are using.

During server installation, you supplied information which is used to create a certificate request (see ***Entering certificate information*** on page 20). The request is saved as a CSR file in the following location:

```
/var/dme/instances/base/etc/signrequest.csr
```

This CSR file is used for generating the certificate. If you need to generate a new CSR file, use the **DME Control Center** (`dmecc`) tool. See Generating new CSR.

The DME server uses an Apache web server (`x509`) certificate.

Self-signed certificate

As part of the installation of DME a Self-signed SSL certificate is installed automatically allowing you to start the server and testing https if settings allows for it. Please note that Android devices cannot connect to Self-signed certificates.

➢ ***Converting PEM certificate file to binary format, and enabling it***

1. To convert the `sslcertificate.pem` file to binary `.der` format, run the following command:

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

   Please note that the binary version of the `rootCA.pem` file (`rootCA.cer`) can only contain one certificate and not the full root certificate chain.
2. The certificate will be used by DME the next time the DME server is restarted.
3. Install the certificate in your browser (using the **Server** > **Certificates** > **Install root certificate** feature in the DME Web Administration Interface).
4. Send the certificate to the clients using the **Devices** > **Send SSL certificate** feature, if required.

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

Some devices can now connect to DME to verify the installation. **Android devices cannot.** As mentioned, this is not for use in a production system.

Commercial certificate

To establish a chain of trust between the device and the DME server, you must install a root certificate and one or more intermediate certificates on the DME server.

In the following, we use the commercial CA **RapidSSL** as an example of how to obtain and install a commercial certificate. It is assumed that you have already bought the certificate and are ready to download it from the RapidSSL website.

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.*

➢ ***Generating and installing commercial certificate***

1. Open the CSR file generated during the DME installation of DME in WordPad (or other professional editor, not Notepad).

   The file was saved in `/var/dme/instances/base/etc/`

   Copy all the contents of the file, including `-----BEGIN CERTIFICATE REQUEST-----` and `-----END CERTIFICATE REQUEST-----`.

   Alternatively, use the **DME Control Center** to display the sign request file, and copy it from the screen. See Managing certificates using dmecc.
2. Paste the content into the relevant form field at the RapidSSL website.
3. An email will be sent to the address registered as approver of your domain (see link to ***RapidSSL https://knowledge.rapidssl.com/support/ssl-certificate-support/index?page=content&id=AR1397&actp=RELATED_RESOURCE)***). Follow the link in the email to approve the issue of the certificate.
4. Download the SSL certificate. The download contains the certificate itself ("Web Server CERTIFICATE") and at least one intermediate CA certificate.
5. Copy the *SSL Certificate*. Make sure to include both `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` in the text you copy.
6. Using an editor, open the file `/var/dme/instances/base/etc/sslcertificate.pem`. Paste the copied SSL certificate into the file, overwriting any content. Save and close the file.
7. Copy the *Intermediate CA certificate*. Make sure to include both `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` in the text you copy.
8. Using an editor, open the file `/var/dme/instances/base/etc/rootCA.pem`. Delete the content of the file, and paste the copied intermediate certificate into the file.
9. If there are multiple, intermediate certificates, repeat steps 7 and 8 above for each certificate, appending to the `rootCA.pem` file. 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-----
miid1tccaRKSK4...
...
-----END CERTIFICATE-----
```

10. After pasting all certificates into the file, save and close `rootCA.pem`.
11. To create the certificate files needed by Nginx, run the `certs\ConvertToNginx.bat` command.
12. Change the permissions of the `.pem` files using:

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

13. 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 Nginx log file for SSL related errors. Please also use the following guideline in ***Support KB7501 https://rfs.solitonsystems.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 `*.company.com`).

CA not on devices

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 part of ***Self-signed certificate*** on page 23 for more information.

Clustering

DME supports clustering and load balancing with a few post-installation adjustments. The following is a brief outline of what this requires.

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

1. Install two or more servers on separate server machines.
2. Make sure that all DME servers have access to the database.
3. Make sure that the certificates in the /var/dme/instances/base/etc directory on all servers are identical.

   Note that the jboss subfolder is server specific.

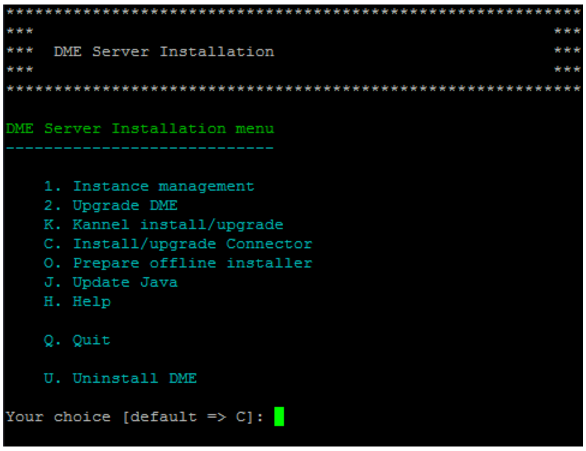
For more information, see ***DME Cluster Configuration*** ***https://resources.solitonsystems.com/content/dme-cluster-configuration***

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. this allows you to for instance run DME for multiple different companies on the same physical server.

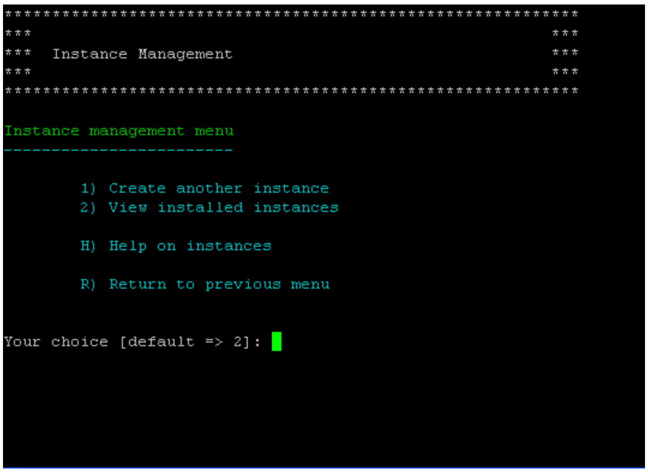
Currently, due to the JBoss Application Server configuration and the desire to keep the alterations of the JBoss configuration to a minimum, it is only possible to install multiple instances on one server by using multiple IP addresses, one for each DME instance.

When the **base** instance has been installed, you can create new instances or view instance configuration. First download the newest installation script as described in the introduction to this guide - see ***Getting the installation files*** on page 7. In the main menu, the default item **1** (**Base installation**) has changed to **Instance management**.



```
************************************************************
***                                                      ***
***  DME Server Installation                             ***
***                                                      ***
************************************************************

DME Server Installation menu
----------------------------

    1. Instance management
    2. Upgrade DME
    K. Kannel install/upgrade
    C. Install/upgrade Connector
    O. Prepare offline installer
    J. Update Java
    H. Help

    Q. Quit

    U. Uninstall DME

Your choice [default => C]:
```

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

➢ ***Creating a new DME instance***

1. In the installer's Instance Management menu, choose 1 **Create another instance**.

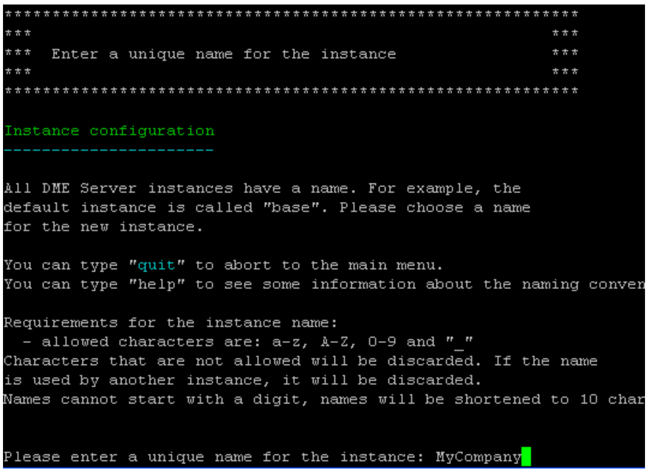
   You are guided through a three-step procedure.

2. 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.

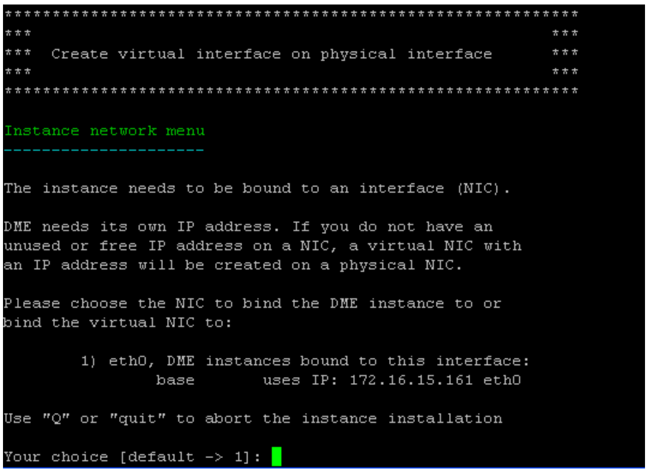
The init script to start and stop the instance will be prepended with `dme_` in the `/etc/init.d` directory to make it easier to find and use. The instance, and all files belonging to the instance, are placed in `/var/dme/instances/<instance>`.



```
************************************************************
***                                                      ***
***  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
```

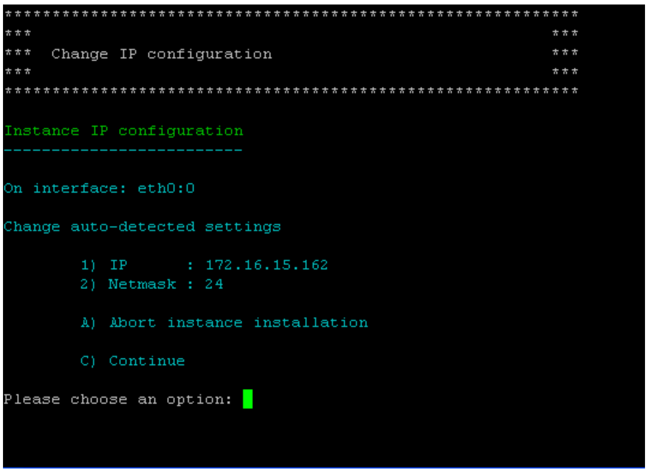
3. Next you need to configure the Network Interface Card and the IP address. The IP has to be a valid IP, which the server is able to configure and use. There is currently no limitation to the number of instances or virtual IP's that can be used, except for the limitations of the hardware. If you have 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]:
```

4. 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. See ***Base installation*** on page 13.

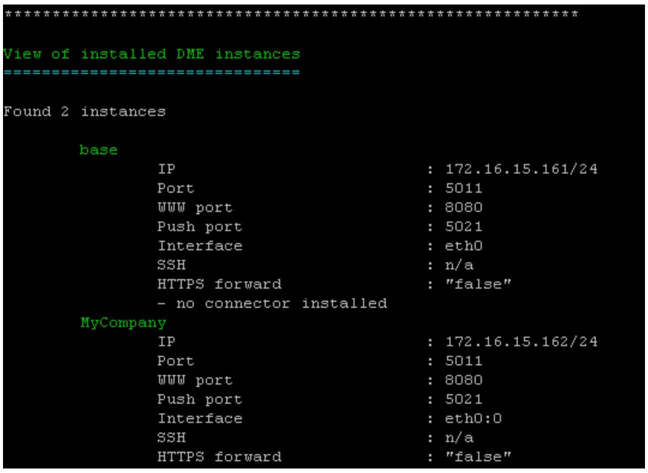
When you are done, press **C** to continue. A summary of your selection is shown. Depending on platform and previous setups, you may be prompted to reuse an existing boot file for the virtual NIC.

The installer proceeds to create the new instance, and you will be prompted to enter certificate details as for the base installation (see ***Entering certificate information*** on page 20).

When the instance has been installed and preconfigured, you are returned to the **Instance management** menu where you can choose item **1** to create another instance, **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>`

-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>;"
```

When all these commands have been run, the instance is completely removed.

Installing the DME connector

➢ ***Connector installation***

1. Run `sh dme-install.sh` (the installer; see ***Getting the installation files*** on page 7) as `root`.

   A connector can generally be installed on any server on the network, including Windows servers. See ***Collaboration system considerations*** on page 33 for information about further requirements that depend on the collaboration system you are using.

   If you are installing a new connector on a Linux server where DME is *not* installed, 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.

2. In the installation screen, press **C** (**Install/upgrade Connector**).

   If multiple instances have been installed, choose the instance to which the connector should be bound.

3. *Version:* A list of available connector versions is displayed. It is important that you choose the same service pack level as that of the DME server instance you are installing for. Default value is the latest connector. Press the number of your choice.

   The connector files are downloaded to disk.

4. *DME connector type:* Choose the collaboration system environment in which the connector will be installed. Press **E** for Microsoft Exchange or **D** for Lotus Domino.

5. *DME connector information:* Enter the IP of the DME server to which the connector is to connect.

   Then enter the display name of the connector. Default name is **Connector** plus a number. This will be shown in the **Connector** tab of the DME server administration web interface.

6. *Installation complete:* The installer now executes the installation.

   The installer shows commands for starting and stopping the connector service. To do this, you use an init script called `dmec_<instance>`, which is located in the `/etc/init.d` folder. Usage:

   ```
   service dmec_<instance> (start|stop)
   ```

7. Press **Enter** to return to the connector installation menu.

All further configuration of the DME connector is done from the DME server web interface. See ***DME administration web interface*** on page 49.

However, you can configure certain variables by editing the connector init script `dmec_<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. See ***RAM usage*** on page 39.

Collaboration system considerations

The possible location of the connector installation depends on whether you run Lotus Domino or Microsoft Exchange as the back-end collaboration system.

Exchange

The connector can be installed on any machine in the network. Access to Active Directory and the Exchange OWA or CAS server are required.

Exchange NTLM authentication

This section only applies to installations where NTLM authentication is used, and not where **Basic** authentication is used.

There are two ways of using NTLM authentication on MS Exchange:

- NTLM v1 support
- NTLM v2 support

The authentication method is configured on the connector.

To determine whether your setup requires NTML v1 or NTML v2, check if the DME connector hangs when testing the connection to your Exchange server using the different NTLM options as authentication.

For more information, see the **Exchange 2003 integration Guide** and the **Exchange 2007/2010 integration Guide** at the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/docs/checklist***.

Domino

On Linux, the connector can be linked with a Domino system in a **DIIOP/Corba** configuration only. **Notes Session** and **Domino Session** modes are only supported on Windows servers, as they require the installation of Windows-only Domino software.

For more information about how Domino should be set up, please see the **Domino Integration Guide** at the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/docs/checklist***.

Removing a connector

It is currently not possible to remove a connector using the installer.

➢ ***Connector removal***

To remove a connector, perform the following steps:

1. Stop the connector (run `service dmec_<instance> stop` as `root`)
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.

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:

- Normally, if the server IP is for instance `172.16.15.15` and DME is on `172.16.15.15`, then the DME server will respond via JNDI with the `172.16.15.15` IP address, and the connection is established.
- With an external connector, 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:

   `/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 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:

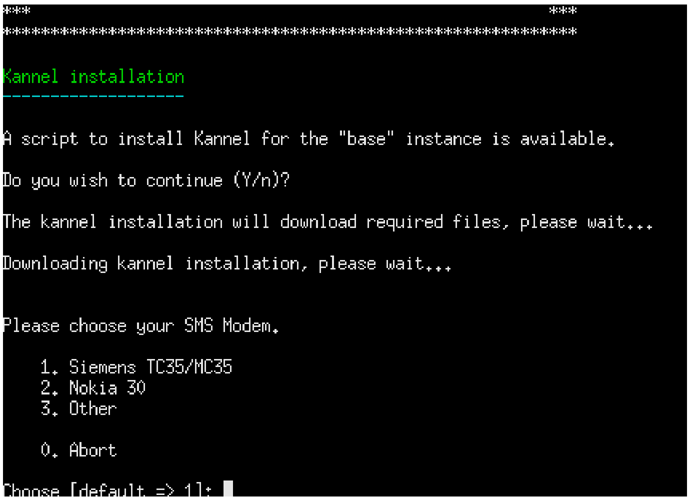
   ```
   172.16.15.15    dme.example.com
   ```

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.

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:



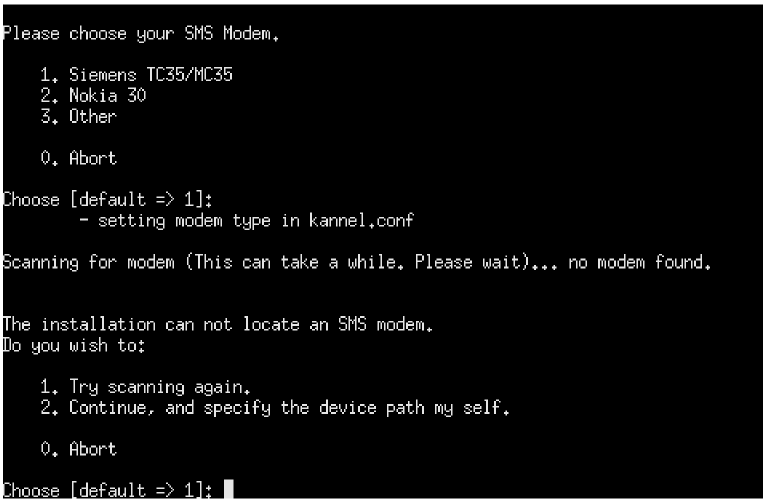
```
***                                                        ***
**************************************************************

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:



```
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.

Note that some GSM modems with USB connections are not detected correctly, and are known to cause problems during installation.

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:

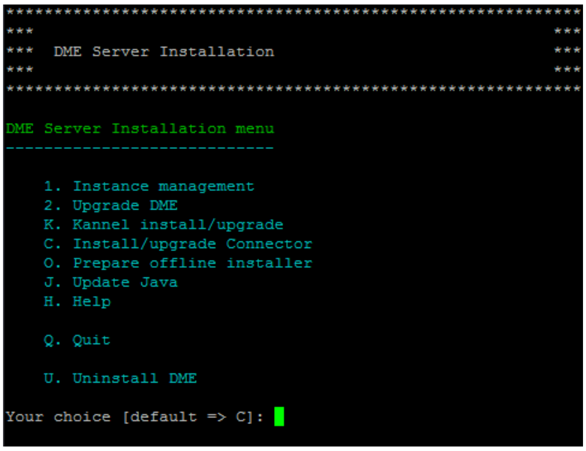
From `/var/dme/kannel/etc/kannel.conf` to `/etc/kannel.conf`

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

You are then returned to the main installer menu.

Update Java

When at least a base instance of DME has been installed, a menu item called **J Update Java** appears in the installation menu:



```
************************************************************
***                                                      ***
***  DME Server Installation                             ***
***                                                      ***
************************************************************

DME Server Installation menu
----------------------------

    1. Instance management
    2. Upgrade DME
    K. Kannel install/upgrade
    C. Install/upgrade Connector
    O. Prepare offline installer
    J. Update Java
    H. Help

    Q. Quit

    U. Uninstall DME

Your choice [default => C]:
```

With this option, you can update the Java version which DME uses with the latest patches, without having to reinstall DME.

➢ ***Updating Java***

1. Run the installer as `root`: `sh dme-install.sh`
2. Press **j** to update Java.

   The installer compares the Java version currently used by DME with the latest Java version.
3. If a Java update is available, the new Java is installed in the DME `<JAVA_HOME>` directory.
4. If an update was performed, restart the DME service: `service dme_base start`

You are returned to the main menu.

Settings and security

This section concerns advanced topics that affect the performance and security of the DME system.

RAM usage

If you are running DME on a server 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 `dmeconnector` service 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:

```
/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
```

Note that 32-bit is no longer supported.

Location of the **DME connector** configuration file:

```
/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.

Securing the traffic between server and connector(s)

To ensure end-to-end SSL encryption from device to DME server, the communication between the DME server and the DME connectors must be encrypted. The following guide shows how to set up secure SSL data channels between the DME server and the DME connectors. The setup is almost identical on WINDOWS and LINUX environments with only the paths and configuration files location being different.

Step 1: Create jbossuser for use in encryption

Precondition 1: Stop all servers and connectors in the environment

Precondition 2: Needs a JAVA installation and JAVA_HOME set to be able to generate/import and export certificate end key store (If JAVA_HOME is not set the full path is needed pointing to the java bin folder when keytool programme is used)

Precondition 3: Manually create a jboss user using the following commandline. The user should be created excactly like this:

User: `jbossremoteuser`

Password: `password1!`

Script can be executed commandline like this:

```
/%JBOSSHOME%/bin>./add-user.sh -a jbossremoteuser
password1!
```

Step 2: Create the SSL keystore on the server (Self signed Certificates)

Create a Keystore (In case of running in a Cluster solution this keystore needs to be on all jboss 6 instances).

Navigate to and create a keystore (server.keystore) using keytool program (part of JAVA sdk):

```
> cd /%JBOSSHOME%/standalone/configuration/
> keytool -genkey -alias server -keyalg DSA -keystore
server.keystore
```

Answer the questions shown below here in a similar way: Change XXX spots, and choose a password. First and last name needs to be "localhost"

Password needs to be placed in the `standalone-full-ha-dme.xml` later on.

```
Enter keystore password:
123456
Re-enter new password:
123456
What is your first and last name?
[Unknown]:  localhost
What is the name of your organizational unit?
[Unknown]:  XXX
What is the name of your organization?
[Unknown]:  XXX
What is the name of your City or Locality?
[Unknown]:  XXX
What is the name of your State or Province?
[Unknown]:  XXX
What is the two-letter country code for this unit?
[Unknown]:  XXX
Is CN=localhost, OU=XXX, O=XXX, L=XXX, ST=XXX, C=XXX correct?
[no]:  yes
Enter key password for <server> (RETURN if same as keystore
password):
123456
Re-enter new password:
123456
```

Make sure permissions on created have the correct permissions.

Step 3. Export Certificate from the keystore

Export the certificate from the keystore which later should be transferred to the connector (ALL connectors if running in Cluster setup):

```
> cd /%JBOSSHOME%/standalone/configuration/
> keytool -export -keystore server.keystore -alias server
-file server.cer
Enter keystore password:  123456
Certificate stored in file <server.cer>
```

Step 4. Make changes to configurations files standalone-full-ha-dme.xml

Open the file named `standalone-full-ha-dme.xml` located:
`/%JBOSSHOME%/standalone/configuration/`

Search for `ApplicationRealm` and replace the tag `<security-realm name="ApplicationRealm">... </security-realm>` with the xml snip below.

Note: remember here to replace the password with the choosen keystore password

```
<security-realm name="ApplicationRealm">
<server-identities>
         <ssl>
           <keystore path="server.keystore"
relative-to="jboss.server.config.dir"
keystore-password="123456" alias="server"
key-password="123456"/>
                     </ssl>
                    </server-identities>
                <authentication>
                    <local default-user="$local"
allowed-users="*" skip-group-loading="true"/>
                    <properties
path="application-users.properties"
relative-to="jboss.server.config.dir"/>
                </authentication>
                <authorization>
                    <properties
path="application-roles.properties"
relative-to="jboss.server.config.dir"/>
                </authorization>
</security-realm>
```

Search again - this time for `<connector name="remoting-connector" socket-binding="remoting"/>`

Comment it out like this:

```
<!-- <connector name="remoting-connector"
socket-binding="remoting"/> -->
```

replace with:

```
<connector name="remoting-connector"
socket-binding="remoting"
security-realm="ApplicationRealm"/>
```

This ends the changes on DME Server side.

Step 5: Configure and setup at connecter side

At the Client(Connector) destination: perform the following actions. Import server certificate into a client.keystore:

1. Initially – copy the generated Server certificate from DME server to Connectore server in the following location. Copy/transfer the certificate(server.cer) into:
   `/%CONNECTORHOME%/connector/conf/`

2. Then using the keytool again to import the certificate into client.keystore:

```
> %CONNECTORHOME%/connector/conf/
> keytool -import -trustcacerts -alias server -file
server.cer -keystore client.keystore

Enter keystore password:123456
Re-enter new password:123456
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

3. In order to make the DME connector communicate with the DME server, make the following change in the `wrapper.conf` file on all connectors.
   Open `wrapper.conf` file, located `/%CONNECTORHOME%/conf/` in edit mode

   Insert 2 additional java parameters and correct the numbers accordingly (For this example it is number 13 and 14). Full path client.keystore is needed and also the password choosen earlier is needed:

```
wrapper.java.additional.13=-Djavax.net.ssl.trustStore=
/<%CONNECTORHOMEFULLPATH%>/conf/client.keystore
wrapper.java.additional.14=-Djavax.net.ssl.trustStoreP
assword=123456
```

4. Change configurations in the `dme-config.xml` file:
   Open `dme-config.xml` file located:
   `/%CONNECTORHOME%/connectore/conf/` in edit mode

   Add one extra tag `<encrypt>yes</encrypt>` at the bottom at the list like this:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<configuration>
    <jboss>remote://xxx.xxx.xxx.xxx:4447</jboss>
.
.
.
.
.
.
<encrypt>yes</encrypt>
</configuration>
```

Step 6: Finally do a restart of all servers and then afterwards all connectors

Deactivate encryption of traffic between server and connectors

To deactivate the encryption of the communication between the DME Server and the DME Connectors, use the following steps.

Step 1: Stop all servers and connectors

At ALL Server destinations:

Step 2: Update configuration file on DME Server side

Comment in the tag shown below in the file `standalone-full-ha-dme.xml` located:
`/%JBOSSHOME%/standalone/configuration/`

Before:

```
<!-- <connector name="remoting-connector"
socket-binding="remoting"/> -->
```

After:

```
<connector name="remoting-connector"
socket-binding="remoting"/>
```

Comment out this:

```
<connector name="remoting-connector"
socket-binding="remoting"
security-realm="ApplicationRealm"/>
```

Comment out the `<server-identities>` tag in the `ApplicationRealm` like below

```
<security-realm name="ApplicationRealm">
            <!--   <server-identities>
                        <ssl>
                           <keystore path="server.keystore"
relative-to="jboss.server.config.dir" keystore-password="123456"
alias="server" key-password="123456"/>
                        </ssl>
                   </server-identities>  -->
                <authentication>
                    <local default-user="$local" allowed-users="*"
skip-group-loading="true"/>
                    <properties path="application-users.properties"
relative-to="jboss.server.config.dir"/>
                </authentication>
                <authorization>
                    <properties path="application-roles.properties"
relative-to="jboss.server.config.dir"/>
                </authorization>
</security-realm>
```

Step 3: Disable Encryption at Connector side

At ALL Connector destinations:

In the `dme-config.xml` file located:

`/%CONNECTORHOME%/connector/conf/`

Delete or out comment this tag `<encrypt>yes</encrypt>`

In `wrapper.conf` on the Connector – remove/comment out the additional java:

```
#wrapper.java.additional.13=-Djavax.net.ssl.trustStore=/%
CONNECTORHOMEFULLPATH%/conf/client.keystore
#wrapper.java.additional.14=-Djavax.net.ssl.trustStorePas
sword=123456
```

Step 4: Start all servers and then all connectors

Encrypting the database password

To further enhance security on your Linux server, you can encrypt the password used for the DME database.

The following steps describe how to do this.

1. Run the following Java command, which will output an encoded password. The password will be used later in

`standalone-full-ha-dme.xml`. Use the database connection password found in `/etc/init.d/dme_base` instead of `someSecretPassword` used in this example.

```
java -cp
/usr/local/jboss-eap-6.4/modules/system/layers/base/.o
verlays/layer-base-jboss-eap-6.4.13.CP/org/picketbox/m
ain/picketbox-4.1.3.Final-redhat-1.jar:/usr/local/jbos
s-eap-6.4/modules/system/layers/base/org/jboss/logging
/main/jboss-logging-3.1.4.GA-redhat-2.jar
org.picketbox.datasource.security.SecureIdentityLoginM
odule someSecretPassword
```

or run `encryptedpassword.sh` and type your `someSecretPassword`

Note that the java command must be entered on one single line. The command will respond with the encoded password, for example:

```
Encoded password:
-48403a759da375b2d7857b9c0660fa38612116 1fb6881cc
```

2. Search “`security-domain`” from `/usr/local/jboss-eap-6.4/standalone/configuration/standalone-full-ha-dme.xml` and add the following to `/usr/local/jboss-eap-6.4/standalone/configuration/standalone-full-ha-dme.xml`

   Change `USERNAME` to the database user name (default base). Change `PASSWORD` to the encoded/encrypted password from the java command above. It should look something like this (note: no line breaks between similar tags!):

   ```
   <!-- snip -->
   <security-domain name="EncryptDBPassword"
   cache-type="default">
   <authentication>
   <login-module
   code="org.picketbox.datasource.security.SecureIdentity
   LoginModule" flag="required">
   <module-option name="username" value="USERNAME"/>
   <module-option name="password" value="PASSWORD"/>
   </login-module>
   </authentication>
   </security-domain>
   <!-- snip -->
   ```

3. Replace the `user-name` and `password` tags with the `security-domain` tag in `/usr/local/jboss-eap-6.4/standalone/configuration/standalone-full-ha-dme.xml`

```
<security>
<!-- snip -->
<!--<user-name>${jboss.datasource.security.username:ba
se}</user-name>
<password>${jboss.datasource.security.password:somepas
sword}</password>-->
<security-domain>EncryptDBPassword</security-domain></
security>
<!-- snip -->
```

4. Restart the DME server

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

Using a proxy

In order to provide push functionality for iOS and Android devices (Apple Push and Google Cloud Messaging), the DME server connects to `cs.excitor.com` on port `443` using a web service.

If a web proxy is used to connect from the DME server, which is typically located in the DMZ, to `cs.excitor.com`, then you need to add some JBoss parameters to allow the connection.

Edit the DME startup script `etc/init.d/dme_base`, and find the following section:

```
JAVA_OPTS="$JAVA_OPTS -XX:MaxPermSize=${PERMMAX}m"
JAVA_OPTS="$JAVA_OPTS
-XX:ThreadStackSize=${THREADSIZE}"
JAVA_OPTS="$JAVA_OPTS -Djava.net.preferIPv4Stack=true"
```

Add the following on separate lines below the above section:

```
JAVA_OPTS="$JAVA_OPTS -Dhttps.proxyHost=<proxyIP or
DNS>"
JAVA_OPTS="$JAVA_OPTS -Dhttps.proxyPort=<port number>"
JAVA_OPTS="$JAVA_OPTS -DproxySet=true"
```

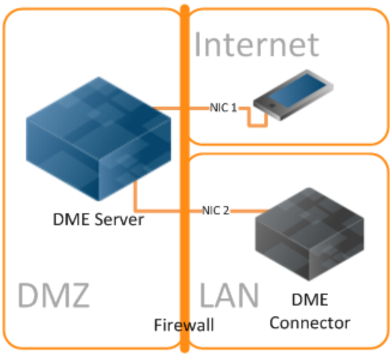
Enter the correct proxy host instead of the text `<proxyIP or DNS>`, and the port number instead of `<port number>`.

Restart the DME server. The server will now connect to `cs.excitor.com` using the proxy.

> Please note that DME currently only supports anonymous proxy due to a JBoss limitation.

Using two NICs

It is possible to use two different Network Interface Cards for DME traffic. This way you can use one NIC for device connections (outbound), and another for connector traffic (inbound), like this:



The JBoss server must respond on the "connector network" (through NIC 2 in the graphic above). You can then configure JBoss to use NIC 1 to communicate with the DME devices. To achieve this, do the following:

1. Open the JBoss configuration file **`server.xml`**, which is located in

   ```
   /var/dme/instances/<instance>/etc/jboss/server.xml
   ```

   - on the DME server.
2. In the **`server.xml`** file, find the place where a bind address for the sync. port is defined:

   ```
   port="5011"
   address="${jboss.bind.address}"
   ```

3. Change this to the fixed IP address of **NIC 1** from the graphic above, for example:

   ```
   port="5011"
   address="172.16.10.12"
   ```

4. Save the **`server.xml`** file, and restart the DME service.

> Make sure the default gateway on the DME server machine is set to use the internet NIC (**NIC 1** above). Otherwise, push notifications for the devices will not work.

DME administration web interface

After installing the DME server and connector, you need to set them up in the DME Administration Web Interface. For information about how to perform the initial setup, please see the integration guides for Exchange and Domino at the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/docs/checklist***.

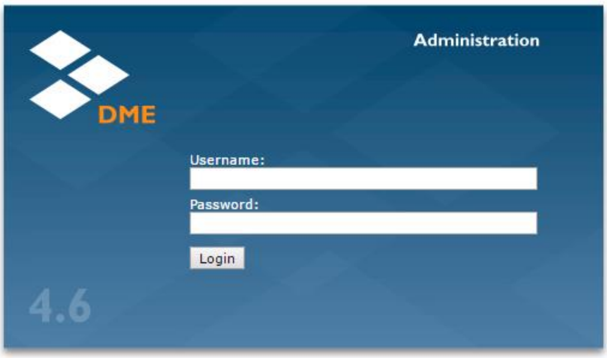
➢ ***Logging in to DME***

1. To administer the DME server, open a browser window, and enter the DME server path including connection port as the URL, for instance **https://dme.company.com:8080**

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

2. Accept the warning.

   The DME server login screen is shown:



3. The first time you log in, use the following credentials:

   Username: SYSADM

   Password: HeraterSol55 (case sensitive)

You can now configure the server and connectors as described elsewhere, notably in the DME Server Administration Reference (click ? in the DME web interface) and the Domino and Exchange integration guides, which can be found online at the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/docs/checklist*** site.

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

➢ ***Changing SYSADM password***

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**.

Upgrading

This section describes how to upgrade the DME server and connectors.

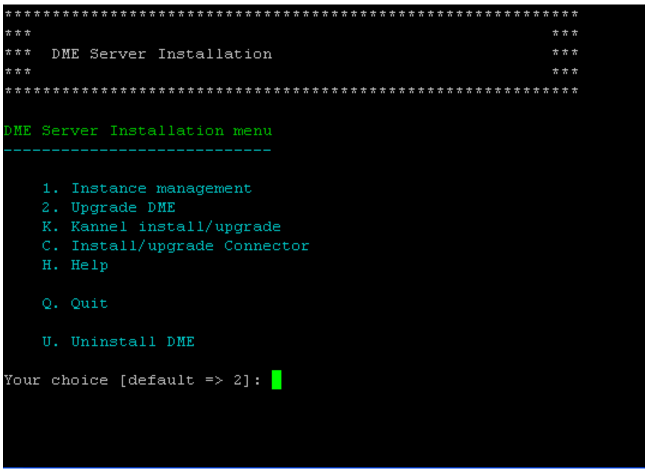
> **Important**
>
> Make sure to upgrade the server before any connectors. If you upgrade the connectors first, remember to restart the connectors after eventually upgrading the server.

Upgrading the DME server

➢ ***Upgrading a DME server***

To upgrade to the latest server release, do the following:

1. Back up your DME database.
2. Download the installer and run the upgrade through the installer as described in ***Getting the installation files*** on page 7.
3. Log in.
4. Choose the default item **2 - Upgrade DME** in the 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]:
```

You will be informed about making a database backup if you choose to upgrade DME. If you forgot to do so, press **R** return to the main menu, and start again from item 1 above.

5. Otherwise press **C** to continue with the upgrade.

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, a message will inform you that there are no newer versions of DME, and you will be returned to the main menu.

6. Choose the version of DME you want 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.

   The installer will now perform the following operations:

   - 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 you upgrade a DME server, the original configuration and SSL encryption files are not touched.

When the upgrade is finished, you may need to update the database schema.

1. If you are running *MySQL on localhost*, the database update is automatic.
2. If you are running MySQL on a remote host or MS SQL Server, you need to update the database schema on the remote database server.

For more information about downloading and running the database upgrade scripts, go to the ***DME Resource Center https://resources.solitonsystems.com/dl/database-scripts*** and navigate to **Downloads** > **Database scripts**. Click the relevant section (**Scripts for MS SQL Server** or **Scripts for MySQL**), find and download the correct script. You only need to run the script pertaining to the version you are upgrading **to**. This script will include all the database changes that have occurred since your current DME version (it is *cumulative*).

To run the script for *MS SQL Server*:

1. Open the SQL Server Management Studio on a Windows machine.
2. Connect to the database server.
3. Select the DME database.
4. Open a new **Query** window.
5. Paste the content of the script you want to run into the query window.

6. Click **Execute** in the toolbar.

To run the script for *MySQL Server*, see the MySQL documentation.

For more information, see the section **Database setup** at the ***DME Resource Center*** see DME Resource Center - ***http://resources.solitonsystems.com/docs/checklist***.

You can also choose to do this before launching the DME installer.

Upgrading the DME connector

Before upgrading a connector, make sure that the server has been upgraded first. See ***Upgrading the DME server*** on page 51. If you do upgrade the connectors first, make sure to restart the connector service after upgrading the DME server.

➢ ***Upgrading a connector***

1. **Caution:** First consider whether you are affected by either of these scenarios:
   1. *Are you running SSL between server and connector?* Then you *must secure the traffic again* as described in ***Securing the traffic between server and connector(s)*** on page 40.
   2. *Are you using custom contact mapping?* See ***Contact mapping files*** on page 54 for *important information* about how to handle contact mapping files in connection with upgrades.
2. After reviewing the items above, download the installer as described in ***Getting the installation files*** on page 7.

   Make sure 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.
3. Run the connector installer as `root` on the server that needs to be upgraded, as described in ***Installing the DME connector*** on page 32.

   Be sure to select the Service Pack level that matches the DME server.
4. After the installation, restore any required backup files related to contact mapping *before* starting the `dmeconnector` service. See ***Contact mapping files*** on page 54.

5. Enable any secure traffic setup between server and connector. See ***Securing the traffic between server and connector(s)*** on page 40.

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.

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's `conf` directory for the selected collaboration system **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 was 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.

Path to contact mapping files:

Domino: `dmeconnector/domino_collaborator/conf`

Exchange: `dmeconnector/exchange_collaborator/conf`

If the connector upgrade fails

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.

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.

Backup

To prepare for a successful disaster recovery, keep an up-to-date backup of the DME server and connector folders:

From the DME server machine:

`<DME_HOME>` is the DME installation directory (typically `/var/dme/instances/base/`):

Back up the entire folder structure. Note that this includes any connectors that are installed on the DME server machine.

From the DME connector machine(s):

`<CON_HOME>` is the DME installation directory (typically `/var/dme/instances/<connector-name>/`):

Back up the entire folder structure.

DME database:

Make a complete backup of the DME database.

With **MS SQL Server**, use your preferred MS SQL Server backup program.

With **MySQL**, 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 Soliton Systems. 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.

   If you are using a Windows MS SQL Server database, make a connection to the old DME database.

   If you are using a Remote MySQL database, make a connection to the old database.

   If you are using MySQL on localhost, restore the database dump created previously using:

   ```
   mysql -u root -p[root_password] base <
   /var/dme/backup/<date>/dme_mysqldump.sql
   ```

   Do not start the DME server!
3. Restore the backup of the complete DME server folder structure into `<DME_HOME>` (typically `/var/dme/instances/base/`).
4. Start the DME server, and log in.

Restoring DME connectors:

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

   Do not start the DME connector!
2. Restore the backup of the complete DME connector folder structure into `<DME_HOME>` (typically `/var/dme/instances/<connector-name>/`).
3. Start the connector.

The system is now operational again.

List of procedures

- Getting the installation files 8
- Installing the DME server 11
- Installing MySQL or MariaDB 16
- Converting PEM certificate file to binary format, and enabling it 23
- Generating and installing commercial certificate 24
- Creating a new DME instance 27
- Connector installation 32
- Connector removal 34
- Updating Java 38
- Logging in to DME 49
- Changing SYSADM password 50
- Upgrading a DME server 51
- Upgrading a connector 53