



# Domino Integration

*DME 5.0 • IBM Lotus Domino*

Document version 1.5

Published 16-05-2018

# Contents

<b>Integration with IBM Lotus Domino .....</b>	<b>3</b>
Authentication and authorization: LDAP .....	4
<i>LDAP identity</i> .....	4
<i>Access groups</i> .....	5
<i>User information retrieval</i> .....	6
<i>Configuration</i> .....	6
<i>Allow users to change passwords</i> .....	7
<i>Server access</i> .....	8
Data retrieval: Remote connector .....	9
<i>Domino CORBA/DIOP basics</i> .....	9
<i>Configuration</i> .....	10
<i>Verifying the CORBA/DIOP setup</i> .....	11
<i>Database access</i> .....	13
<i>Unread marks</i> .....	13
Data retrieval: Notes session using client.....	16
<i>Create proxy user in Domino</i> .....	17
<i>Install Lotus Notes client</i> .....	19
Data retrieval: Domino session using server .....	20
<i>Mail server setup</i> .....	20
<i>Setup on the connector</i> .....	22
Notes encryption .....	22
<i>iNotes</i> .....	23
<i>ID Vault</i> .....	25
Secure push e-mail requirements.....	26
<i>Altering ACL for one mail database</i> .....	26
<i>Altering ACL for multiple mail databases</i> .....	27
Contacts .....	28
<i>Lotus Notes 7.x</i> .....	28
<i>Lotus Notes 8.x</i> .....	29
E-mail search.....	30
Sametime integration .....	32
Personal notebooks (journals) .....	32



Domino integration checklist .....	33
<i>Connections to existing Domino environment</i> .....	33
<i>Tasks/services on the Domino server</i> .....	33
<i>User groups</i> .....	34
<i>Specific Domino setup</i> .....	34

# Integration with IBM Lotus Domino

This section describes the integration between the DME server and IBM Lotus Domino. Please note that all screenshots are taken from various versions of the Domino Administrator; minor differences to your user interface may occur.

The system used for authentication and authorization is the *Domino Directory*. The DME server interfaces with the Domino server using LDAP through one or more *connectors*.

This document provides the information you need for setting up a Domino server to accept connections from the DME connector. In addition, prerequisites and requirements for a successful integration between the DME server and Domino server are discussed. Please note that this document does not cover all aspects of the Domino server's functionality, and the Domino server documentation should be consulted in supplement to this information.

The DME connector connects to the Domino server using the LDAP protocol for user authentication. If the connector is installed on the Domino server (using the Notes session solution), access to Domino data (for instance retrieving mails, calendar information, etc.) is retrieved using the Domino RPC protocol (through port **1352**); otherwise access is secured through the DIIOP protocol. Support for both protocols is built into the Domino server, but the relevant tasks must be loaded on the Domino server, and some configuration may be needed.

For information about firewall rules, see the interactive document "DME Firewall Rules" at the **DME Resource Center**  
**<http://resources.solitonsystems.com/docs/firewall-rules>**.

Please note that DME version 3.0 had support for local connectors - that is, connectors installed directly on the Domino server. Support for this was removed in 3.5. If you need to see documentation for the local connector setup, please refer to the DME Partner site and look for the 3.0 installation documentation.

64-bit connectors are supported with DME 4.1. See **Data retrieval: Domino session using server** on page 20.

## Authentication and authorization: LDAP

---

When logging in to DME on the client, the users will be using the following credentials:

**User name:** The user **short name** or **e-mail address**

**Password:** The user's **Internet password**

The DME server validates these credentials against the LDAP. If you are using a technical user (**DME\_Server**), then this user must have an Internet password as well. See the following section.

### LDAP identity

For the LDAP integration to work correctly, you must specify an LDAP lookup identity.

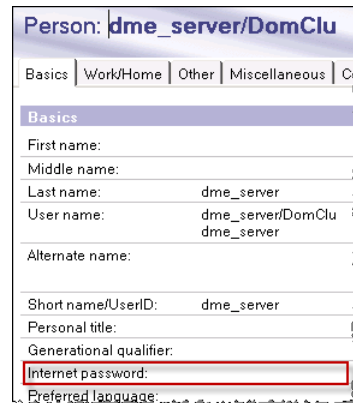
It is recommended that a technical user is created for the purpose of performing LDAP lookups and mail scan (optional; will be described later in this document). The recommended name for the technical user is **DME\_Server/<yourdomain>**, which clearly indicates that it is not a real user. The user must have an Internet password in order to be authenticated.

Please note that throughout this document, references to the user **DME\_Server** are made. The technical user in Domino can have another name. This can be configured in the DME Server Web Administration interface, in the **Domain** setup panel on the setup page for the Domino connector in question (the field **User for domain info queries**).

The **DME\_Server** ID is used for:

- ❖ LDAP integration.
- ❖ Building a group graph.
- ❖ Mail scan (optional).

### Example:



Person: dme\_server/DomClu

Basics | Work/Home | Other | Miscellaneous | C

**Basics**

First name:

Middle name:

Last name: dme\_server

User name: dme\_server/DomClu  
dme\_server

Alternate name:

Short name/UserID: dme\_server

Personal title:

Generational qualifier:

Internet password:

Preferred language:

## Access groups

Access to the DME server is controlled by security groups on the Domino server.

Throughout this document, references to the LDAP groups **DME\_User** and **DME\_Admin** are made. Please note that the actual groups in Domino can have other names, and in that case you must use those group names instead. This can be configured in the **Access rights** group of fields in the **Domain** section of the **Connector** setup page in the DME Server Web Administration interface.

The following 3 groups must be created in the Domino Directory:

#### ❖ **DME\_User**

Add all users synchronizing with DME to the **DME\_User** group.

A user requesting sync operations must be a member of the **DME\_User** group.

#### ❖ **DME\_Admin**

Add all the users who are to have administrative access to DME to this group.

A user accessing the administrative interface with full control must be a member of the **DME\_Admin** group.

#### ❖ **DME\_Superuser**

Add all users that need read access to the administrative interface of DME to this group. Users in the **DME\_Superuser** group cannot change any server settings.

Please note that members of the **DME\_Admin** and **DME\_Superuser** groups do not have the privileges of the **DME\_User** group. If they are also regular users of DME, they must be added to the **DME\_User** group as well.

The group type (**Multi-purpose**, **Mail-only**, etc.) is not important. However, **Multi-purpose** is recommended due to its flexibility.

## User information retrieval

As described, DME connects to the LDAP service on the Domino server to verify user credentials and group memberships. In addition, information regarding the location of the user's mailbox is retrieved (that is, server name and file path). For DME to operate completely integrated into the existing collaboration system, information regarding **Mail server** and **Mail database path** for each user must be available through LDAP (this is the default setting on the Domino server).

**Note:** The user name used when logging in on the DME client (the device) should be the same as what is stored in the **Short name/UserID** field OR the **Internet address** field (full e-mail address) in the user's person document in the Domino directory. See also **Server access** on page 8.

## Configuration

By default, LDAP runs on port 389 or 636 (secure).

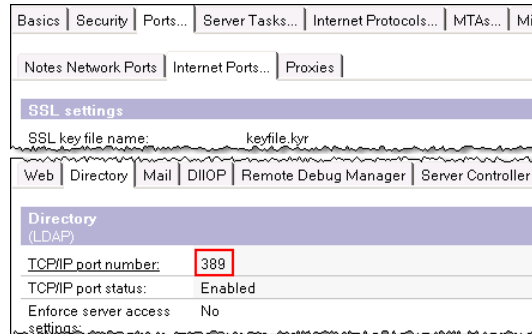
If the Domino server is running on a Windows server which is also running Active Directory (Domain Controller), port 389 is most likely bound to the AD service. In this situation, LDAP must be configured to service on a different port, and this port number must be entered in two fields in the DME Server Web Administration interface:

1. Domino connector setup > **Domain** > **Domain info LDAP server**, and
2. Domino connector setup > **Authentication** > **LDAP server**.

The port number is entered on the form

**domino\_server:portnumber**, for instance **dom\_server:400**.

To configure the LDAP task, open the Domino server document, and go to **Ports > Internet Ports > Directory** (please refer to your Domino server documentation).



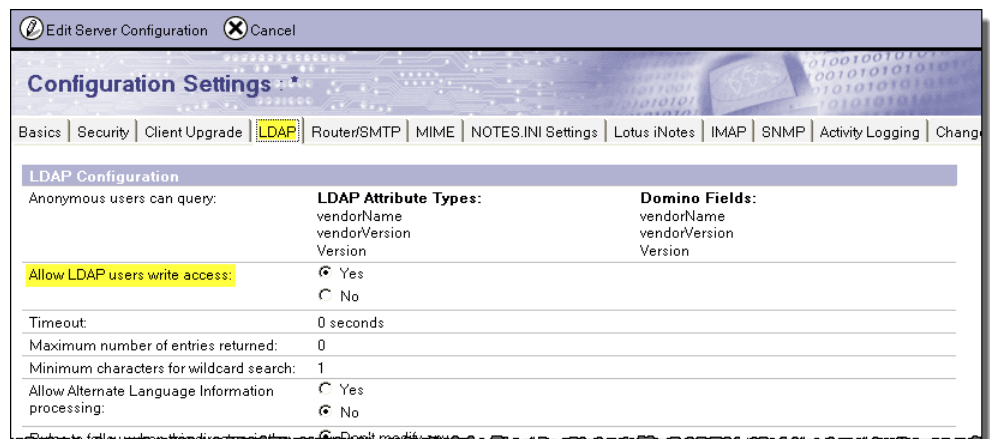
To ensure that the LDAP task is loaded every time the Domino server is started, add LDAP to the **ServerTasks** parameter in the `notes.ini` file (please refer to your Domino server documentation for details regarding this). For example:

```
ServerTasks=Replica,Router,Update,DIIOp,HTTP,LDAP
```

## Allow users to change passwords

To enable users to change their password (when the client setting **Allow change password** is **Enabled**), you need to give users write access to the LDAP.

To do this, open the Configuration Settings document for your Domino server, and select the LDAP tab.



Select **Yes** in the field **Allow LDAP users write access**, and save your changes.



## Server access

Before a user can connect to a Domino server through DME, the user must be granted access to the Domino server.

The user must be allowed to access the server in the same way as through a Notes client. To verify that users can access the server, please locate the **Server Access Who can** - section, located on the Server document, **Security** tab. Here you will find the field **Access server**. Normally, the field **users listed in all trusted directories** will be marked. If this field is marked, you normally do not have to include the **DME\_User** in the **and** field; otherwise insert the **DME\_User** and the **DME\_Server** users in the **and** field.

This must be done on all servers containing users that will use the DME client.

Server access:

Server Access	Who can -
Access server:	<input checked="" type="checkbox"/> users listed in all trusted directories
	and
	<input type="checkbox"/> DME_User

To allow DME users to authenticate (log in to DME on their devices) using their short name, set **Internet Access > Internet Authentication** to **More name variations with lower security**:

Internet Access
Internet authentication:
More name variations with lower security

If you want the setting to be **Fewer name variations with higher security**, you can let the users authenticate with their e-mail address. This option became available in DME 3.0 Service Pack 3. Please note that changing this setting in Domino and letting users log in using their full e-mail address on an *existing DME system* will have some consequences, most notably the following. When the user **JS** starts logging in to the DME client as **John.Smith@example.com**:

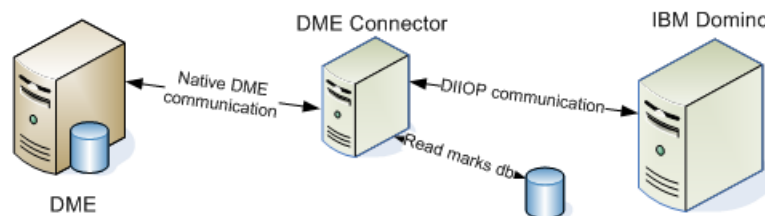
- ❖ The DME client will regard the change from using **JS** to using **John.Smith@example.com** as login name as a change of users. The client will delete all DME data from the client before letting the "new user" log in.
- ❖ On the DME server, the "new user" will appear in the list in the **Devices** tab. Each real user will exist in two variations, for instance **JS** and **John.Smith@example.com**.
- ❖ All statistics, device histories, etc. related to **JS** will not be transferred to **John.Smith@example.com**.

Changing this setting on existing systems must therefore be considered carefully.

One more thing to consider is usability - if the device setting **Show username on logout** is **Disabled**, John Smith might get tired of having to type **John.Smith@example.com** in the login screen every time he wants to log in to DME.

## Data retrieval: Remote connector

If you have chosen to access Domino data (e-mails, calendar entries, contacts, etc.) through a connector, which is not installed locally on the Domino server, you can do so via the CORBA/DIOP interface. The Domino server offers the CORBA service through the DIOP task, which must be loaded on the Domino server, as illustrated here:

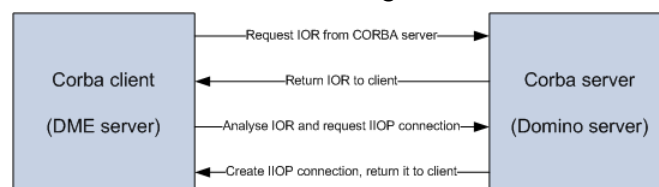


## Domino CORBA/DIOP basics

CORBA is a specification created to support interoperability between software applications, regardless of operating system, programming language, and network specific details. With regard to DME, the CORBA session created between the DME server and a Domino server allows the DME server to create objects and call methods on those objects, but leaving the processing to the Domino server.

To create a CORBA (IIOP) session, the CORBA client retrieves an IOR (Interoperable Object Reference) that contains information about how to create the session (for instance, internet address of the CORBA server and port number on which the CORBA server is listening). Using the information encapsulated in the IOR, the CORBA session is created. For a successful CORBA session to be created, the information in the IOR must be correct.

*Schematic overview of creating a CORBA session:*



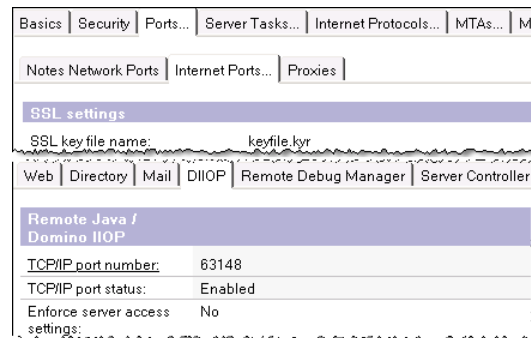
By default, the host IP Address encoded into the IOR is the one that is provided by the TCP/IP network on the Domino server. The Domino server will attempt to resolve the fully qualified Internet host name stored on the **Basic** tab of the Domino server document; that is, it will query the underlying OS for an IP address. If, for any reason, this operation does not return the correct IP, or the DME server should connect using a different IP, the correct IP can be entered in the **Internet Protocols > DIIOIP** section. An invalid IP address encoded in the IOR is a more common problem than one should expect!

## Configuration

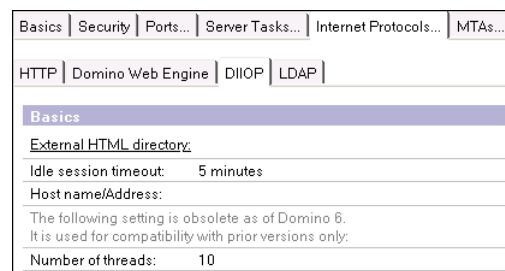
The CORBA task can be configured in the Domino server document. Choose

- ❖ **Ports > Internet Ports > DIIOIP**  
to specify port number and authentication options.
- ❖ **Internet Protocols > DIIOIP**  
to specify idle session time-out, host name/IP.

*CORBA/DIIOIP port and authentication setup:*



*CORBA/DIIOIP session and connection setup:*



**Note:** If you are using Internet Sites documents, you must define both a LDAP and IIOIP internet site document to enable DME to access these services.

To ensure that the DIIOP task is loaded every time the Domino server is started, add DIIOP to the **ServerTasks** parameter in the `notes.ini` file (please refer to your Domino server documentation for details regarding this). For example:

```
ServerTasks=Replica,Router,Update,DIIOP,HTTP,LDAP
```

## Verifying the CORBA/DIIOP setup

After setting up the DIIOP task, the actual setup can be verified by using one of the following two Domino server commands:

```
tell diiop show config
```

or

```
tell diiop dump config
```

These commands provide a list of the configuration data that DIIOP is using from the Domino Directory. If you use the `dump` command, the configuration is written to the file `diiopcfg.txt` in the server's data directory. If you use the `show` command, the configuration is displayed on the server console.

The most important parameter returned by the `tell diiop dump/show config` command is the **Public Host Name/Address** parameter. This parameter indicates the IP address to which the CORBA client will attempt to create a CORBA connection. It is very important to understand that the value of the **Public Host Name/Address** parameter is the one that DME must use to connect to the Domino server. If the Domino server has one IP address on the Internal LAN and another in the DMZ, the value must be that of the DMZ (if the DME connector is located in the DMZ).

Sample configuration provided by the command `tell diiop show config`:

```

DomCluster1/DMEUDD: Lotus Domino Server
> tell diiop show config
Dump of Domino IIOP <DIIOp> Configuration Settings

Full Server Name:  CN=DomCluster1/O=DMEUDD
Common Server Name:  DomCluster1/DMEUDD
Refresh Interval:  3 minutes

Host Full Name:  domcluster1.learn.excitor.com
Host Short Name:  domcluster1
Host Address:  172.16.10.21
Public Host Name/Address:  172.16.10.21

TCP Port:  63148  Enabled
SSL Port:  0      Disabled
Initial Net Timeout:  120 seconds
Session Timeout:  60 minutes
Client Session Timeout:  62 minutes

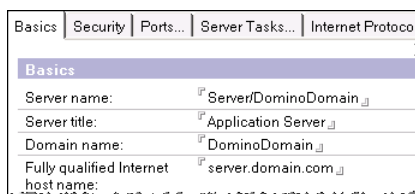
IOR File:  C:\Lotus\Domino\data\domino\html\diiop_ior.txt

Allow Ambiguous Names:  True
Web Name Authentic:  False
User Lookup View:  <$Users>
Allow Database Browsing:  False
TCP Name/Password Allowed:  True
TCP Anonymous Allowed:  True
SSL Name/Password Allowed:  False
SSL Anonymous Allowed:  True
Multi-Server Session Authentication:  Enabled
Multi-Server Session Configuration:  LtpaToken

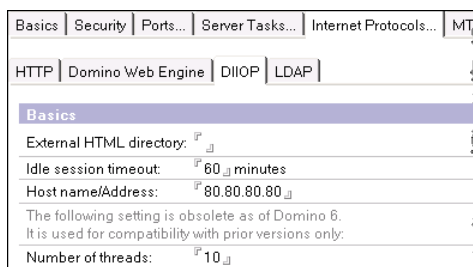
Internet Sites:  Disabled

Single Server Cookies:  Disabled
>
  
```

Parameters on the Domino server document corresponding to the parameters in the DIIOp configuration dump:



Note: In some configurations (where the DME server does not use DNS, but host file) the **Fully qualified Internet host name** must be the **Domino\_server\_name.domain.Top\_Level\_Domain**, and *not* the Windows server name:

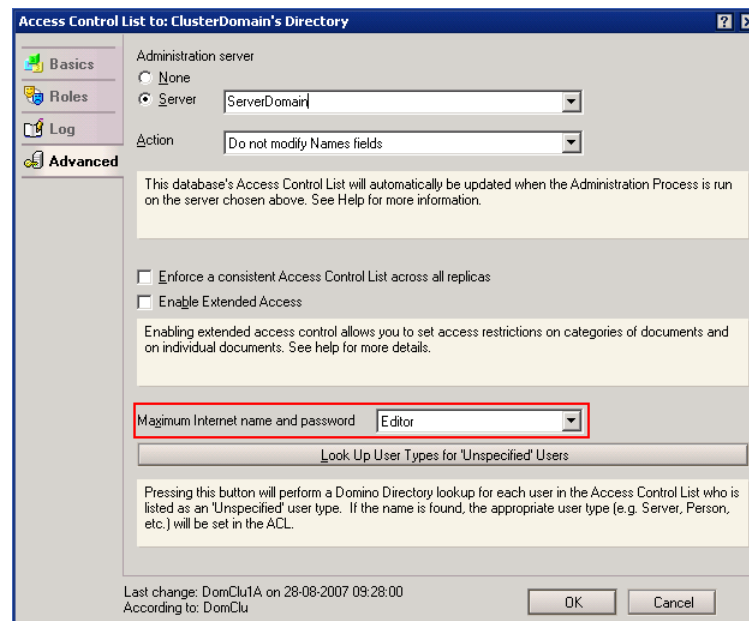


## Database access

Since a CORBA connection is considered an Internet connection, server access (see **Server access** on page 8) and database ACL must be configured accordingly. Please keep this in mind in case of problems regarding insufficient access rights.

As the user connecting to a Notes database through DME is probably the database owner, access control is in many cases set up correctly. However, as DME connects through CORBA through an Internet connection, access to the database from the Internet must be granted. This is done in the **Advanced** options on the database ACL. The access level must be at least **Editor**.

**Maximum Internet name and password** must be set to **Editor** (or higher):



## Unread marks

In order to enable the DME server to synchronize unread marks between the Lotus Notes client mailbox and the DME secure e-mail client, the *DME Marker module* (a Lotus Notes database) needs to be installed on the Domino server. You only need to install this module if you connect using remote CORBA/DIIOP to Domino.

The DME Marker module is not necessary if you connect to Domino using Notes session mode. In fact, if you run Domino 8.x with the connector in Notes session mode, and you specify an unread mark database in the DME web interface, DME will produce an error.

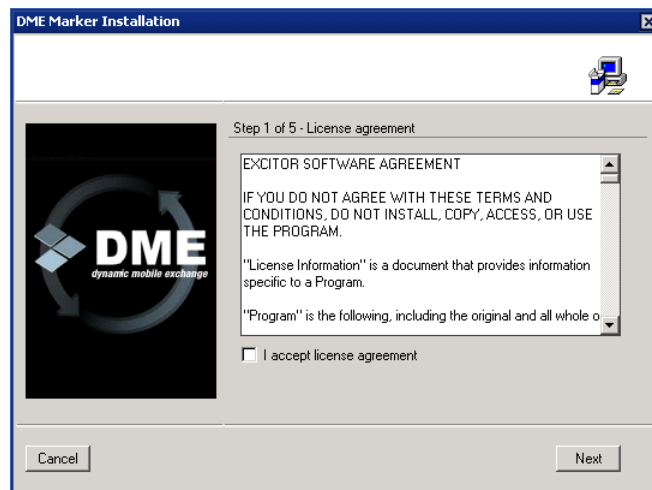
The DME Marker module is supported on all 32-bit Domino versions, and on 64-bit Domino 8.5 and later for Windows servers.

Before the installation, make sure that the person who will install the DME marker database is listed (or is member of a group listed) in the **Security Settings** on the Domino server in the field **Run restricted LotusScript/Java agents**.

### Installing on the Domino server

To install the unread marks database on the Domino server, follow the steps below.

- ❖ Open the database `dme_m_setup.nsf` from your Lotus Notes client (accept an execution security alert related to the Development Team signature). The installation wizard will guide you through the rest of the installation process.



- ❖ Accept the license agreement.
- ❖ Specify the server name and file path for the DME marker database. It is highly recommended to keep the default path `dme\dmemarker.nsf` (especially for the enterprise DME solution and load-balancing of the DME marker module).
- ❖ Specify the **Administrators** group (manager rights in ACL of database) (*optional*).
- ❖ Specify post-installation actions: **Open DME marker after installation** and **Put DME Marker icon to workspace** (*optional*).
- ❖ Click **Install**.



Clicking **Count deletion stubs** shows the current number of deletion stubs in the Unread Marker database. Click **Clear deletion stubs** to remove them. Both buttons are only used when debugging.

**Note:** For future ACL changes: if the administrator wishes to restrict access for any user to the DME Marker database, then DME Users must be added in ACL with editor rights (or higher) and must have the **delete documents** property enabled (see **-Default-** ACL settings after installation).

### Further unread mark setup

On the Domino server, make sure that the **DME\_User** is listed (or is a member of a group listed) in the **Security Settings** on the Domino server in the field **Run restricted LotusScript/Java agents**.



When you later set up the Domino connector in the DME Administrator Web Interface, specify the server and database paths to the DME marker module in the **Read marks** group of fields in the **E-mail and PIM > E-mail** section of the connector setup page.

Read marks (if Remote/Corba mode)	
Server *	<input type="text" value="172.16.12.1:63148"/>
Database *	<input type="text" value="dme\dmemarker.nsf"/>

To see if you need to install this database and specify its location, see the following table:

	<u>DIOP (Remote/Corba) mode</u>	<u>Notes/Domino session mode</u>
Domino 7.x	Specify <b>Database</b>	Specify <b>Server</b> and <b>Database</b>
Domino 8.x	Specify <b>Database</b>	Specify <i>nothing</i> (remove any information in the fields)

This means that:

1. If the connector communicates with any supported version of Domino using DIOP, you must specify the name of the **UnreadMark** database in the **Database** field, leaving the **Server** field blank.
2. If the connector is running as a Notes session, AND your Domino version is less than version 8, you must specify the name of the **UnreadMark** database in the **Database** field and the name of the server on which it is installed in the **Server** field.
3. If the connector is running as a Notes session, AND your Domino version is version 8 or above, the **Server** and **Database** fields must both be blank.

For more information, see the Server Administration Reference about setting up the Domino connector.

## Data retrieval: Notes session using client

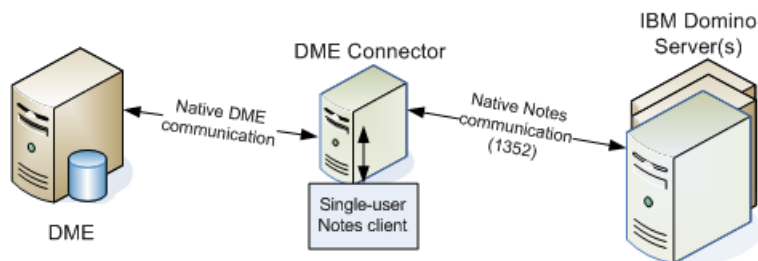
You can install the connector on a machine on which a Notes client is also installed. This is called *Notes Session mode*. There are special requirements for installing a connector in Notes Session mode:

- ❖ The connector machine must run Windows.
- ❖ The connector must run a 32-bit version of Java, as there is no Notes client for 64-bit Java.
- ❖ The Notes client must be version 8 and above.

Check the **System Requirements** document before installing.

Up until DME 4.1, only connectors running 32-bit Java were supported, because the Notes client does not come in a version for 64-bit Java. See **Data retrieval: Domino session using server** on page 20 for information about using 64-bit connectors.

The Notes Session mode solution is illustrated below.



There are a number of advantages to this solution over using Corba/DIOP:

1. The connector will not have to use the DIOP protocol, which is slower than the native Domino connection running on port **1352**.
2. For Domino 8.x servers, no read mark database needs to be configured for helping the DME clients to know which e-mails have been read (for important information about read marks, see **Further unread mark setup** on page 15 above).
3. Using a Notes client version 8.x makes it possible to send and receive Notes-encrypted e-mail in the DME client, also when connecting to Domino 7.x servers.
4. No replication of mail databases is necessary.
5. You can use one proxy user/Notes ID to access all mailboxes.

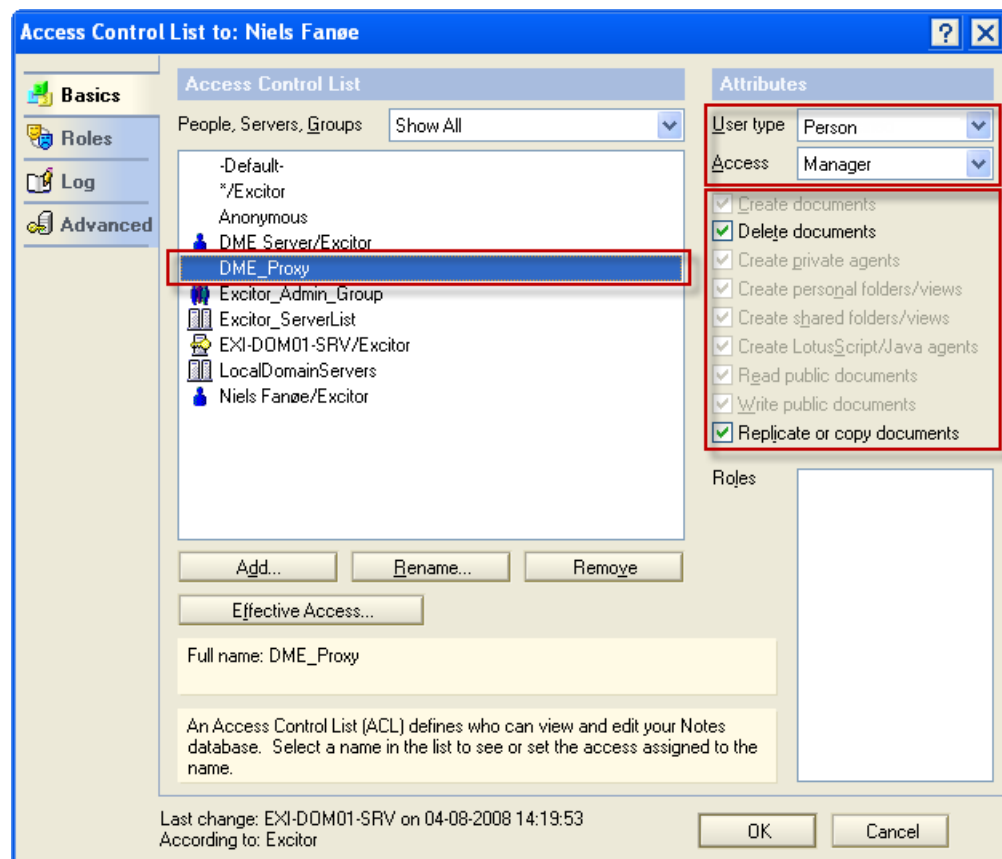
The connector communicates with the DME server using the native DME communication protocol. The connector logs in to Notes as a proxy user, and through Notes gets access to the mailboxes of all DME users in the Domino system.

The following sections describe how to prepare Domino for DME using Notes session.

## Create proxy user in Domino

To prepare Domino for DME using Notes session, you must perform the following steps in Domino:

1. Create a proxy user, for instance called **DME\_Proxy**.  
The mailboxes of all DME users are accessed through this user.
2. The proxy user must fulfill the following criteria:
  1. The user must be a full Notes user with a Notes ID.
  2. The user must have a Notes password.
  3. The user must have a mailbox (even though it will not be used actively).
3. The proxy user must have access to the following:  
*DME users' mailboxes.* Apply **Manager** rights for the **DME\_Proxy** user to the mailboxes of all DME users in the Domino system by altering the ACL of each DME user's mailbox. Follow a procedure similar to the one described elsewhere in this document (see **Altering ACL for multiple mail databases** on page 27) to assign the following attributes to the **DME\_Proxy** user:
  1. **User type: Person**
  2. **Access: Manager.** Only Managers can read the unread marks of other users.
  3. Select **Delete documents** and **Replicate or copy documents**. The proxy user may need to delete or replicate/copy the documents of other users. All checkboxes in the **Attributes** group of fields should be selected.



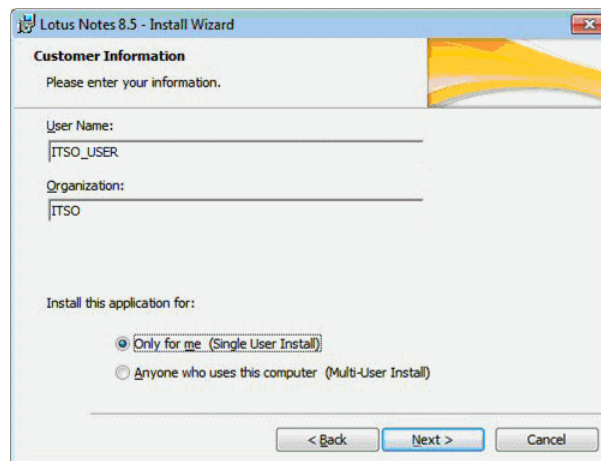
See also **Notes encryption** on page 22 for information about possibly giving access to the users' ID storage databases.

**DME users' notebooks.** If you want to synchronize Domino notes/journals to the clients, the **DME\_Proxy** user must have **Manager** access to the notebook database of the users. Grant access in the same way as for mailboxes. See also **Personal notebooks (journals)** on page 32.

## Install Lotus Notes client

When the DME proxy user has been created with adequate rights as described above, install a Lotus Notes client on the server used for accessing Domino.

1. Install a Lotus Notes 8.5.x Basic client for Windows.  
This must be a Notes 8.5.x client (even if you are running an earlier version of Domino). This client is used for routing the DME users' requests to Domino on the native port **1352**.
2. The Notes client must be installed with the **Only for me (Single User Install)** option selected.



3. Configure the client to use the DME proxy user (**DME\_Proxy** created earlier).
4. Open the DME Administrator Web Interface, and
  1. Go to the **Connector** tab.
  2. Click the Domino connector you want to configure.
  3. Click **E-mail and PIM**.
  4. In the **General (Domino)** subtab, select the field **Using Notes session**.
  5. in the **Notes ID password** field, enter the password of the **DME\_Proxy** user which you created in Domino.
5. Click **Save**.

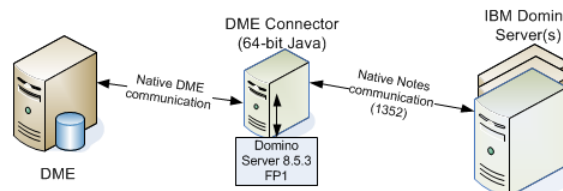
The Notes client now handles the *Notes session* used to communicate with DME and Domino.

## Data retrieval: Domino session using server

Domino session is similar to Notes session, but uses a Domino server instead of a Notes client. Domino servers can run on 64-bit Java, thus making full use of 64-bit server hardware. Support for Domino session mode was introduced in DME version 4.1. The following sections list the special setup required to run Domino connectors running on 64-bit Java.

The advantages of this solution over the Corba/DIOP solution are the same as for 32-bit connectors, with the added advantage that the solution runs on 64-bit Java. For information about Notes session using a Notes client on 32-bit connectors, see **Data retrieval: Notes session using client** on page 16.

To run the DME connector in Domino session mode, install a Domino server on the connector machine. The *Domino Session mode* solution for 64-bit servers is illustrated below.



The following version of Domino is required:

**Domino Server 8.5.3 FP1 - 8.5.3 FP6 or 9.0.1 highly recommended**

Install the server as a Messaging Server.

Note that in Fix Packs FP3 and below, the formatting of HTML e-mails may be broken. Therefore we strongly recommend using at least Domino 8.5.3 FP6.

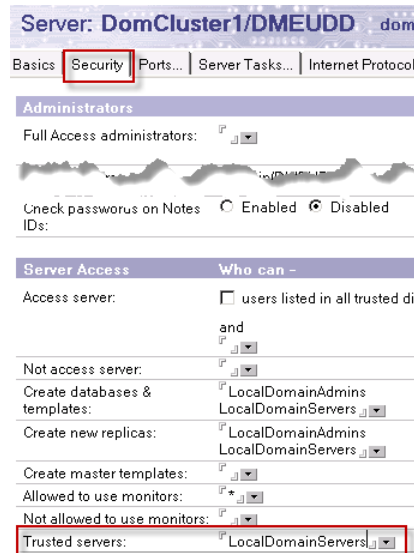
## Mail server setup

After installing the Domino server on the connector, perform the following setup on the Domino mail server:

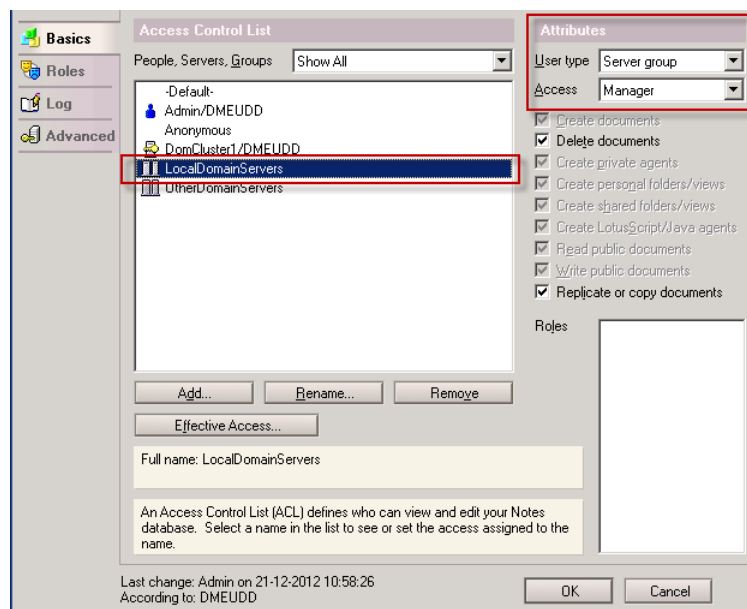
- I. Create a new server.

This server will represent the Domino server which you will install on the connector. You may call it anything you like - in this text, we call it **DMEConn**.

2. Add the **DMEConn** server to the **LocalDomainServer** group on the mailserv (this will often be default).
3. Make sure that the LocalDomainServer group is added as **Trusted servers** in the **Security** page of the mail server document:



4. Allow the **LocalDomainServer** group **Manager** access to the users' mailboxes. Make sure to assign the attribute **Server group** as **User type**.



You can follow the description in ***Altering ACL for multiple mail databases*** on page 27 to see how to assign this attribute to multiple user databases.

Then move back to the connector to complete the final setup.

## Setup on the connector

When Domino has been set up correctly, do the following:

1. Install the 64-bit **Domino Server 8.5.3 FP6** (or higher) as a Messaging Server on the 64-bit connector.
2. Use the ID file for the **DMEConn** server created previously in Domino.
3. Allow the server to run until all configuration items are replicated.
4. Shut down the Domino server as this must not be running when used by the DME Connector.
5. Set the Domino Windows Services to **Manual** (the Domino server must not run again when restarting Windows in the next step).
6. Restart Windows.
7. Install the DME Connector service according to the installation guide.
8. Configure the connector to use Domino session. Open the DME Administrator Web Interface, and
  1. Go to the **Connector** tab.
  2. Click the Domino connector you want to configure.
  3. Click **E-mail and PIM**.
  4. In the **General (Domino)** subtab, select the field **Using Notes session** (this covers Domino session, too).
  5. In the **Notes ID password** field, **DO NOT** enter anything. The field must be blank, as the Domino server handles the exchange of data, not a proxy user as in the case of a Notes session.
9. Click **Save**.

The connector is now ready to service DME users.

## Notes encryption

In order to enable Notes encryption without requiring a Notes ID file to be stored on each device, you can choose between two separate methods:

1. Using standard Domino iNotes.
2. Using Domino ID Vault.

See the following sections for a description of each method.

Notes encryption is only possible on connectors running in Notes session mode (using a Notes client (32-bit Java) or a Domino server (64-bit Java)).

When using a Domino Server as basis for a DME Connector, and using encryption, there can be a issue where the local Domino Server on Connector don't get a updated names.nsf adressbook fil.

The workaround to ensure that the adressbook always will know the valid certificate is to do the following:

- ❖ Stop DME Connector
- ❖ Start Domino Server
- ❖ Replicate names.nsf
- ❖ Start Connector

Or as an alternative:

- ❖ Stop Connetcor
- ❖ Copy as file the updated names.nsf to connector server
- ❖ Start Connector

## iNotes

When using the iNotes method to enable Notes encryption, each user must use the iNotes webmail interface to upload his or her user ID file. The file is uploaded to the user's mail file in Domino, and DME will look for it there when it is required for encrypting or decrypting an e-mail. Once uploaded, Domino will also handle any changes in the users' passwords.

First ensure that the Domino connector is prepared to get user ID files from iNotes. This is done in the DME Administrator Web Interface:

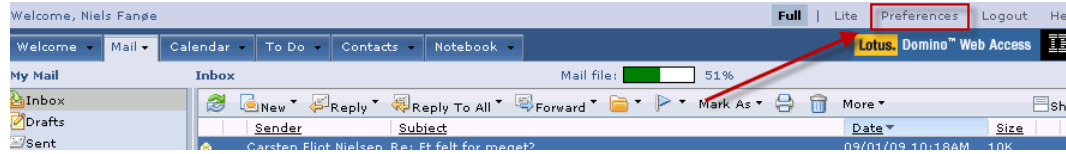
1. Go to the **Connector** tab
2. Click the Domino connector you want to configure
3. Click **E-mail and PIM**
4. In the **General (Domino)** subtab, select the field **Get user ID files from iNotes** in the **Notes encryption** group of fields
5. Click **Save**.

Then instruct the users to upload their ID file in the following way:

1. Open iNotes.



2. Click **Preferences**.

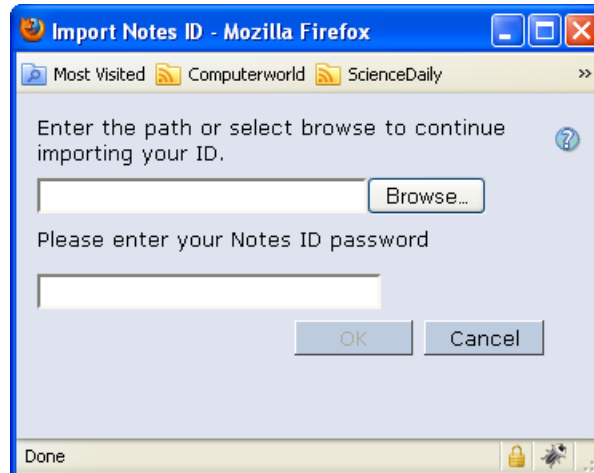


3. If the message "Your mail file DOES NOT CONTAIN a Notes ID" is shown, click **Security > Import Notes ID**.



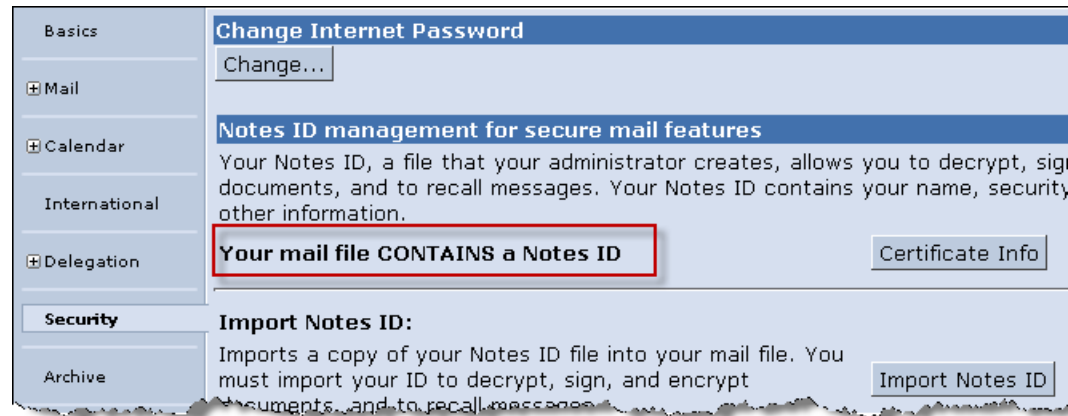
Otherwise, your Notes ID file is already uploaded, and you can click **Cancel** and ignore the next steps.

The following window is shown:



4. Browse to the location of your Notes ID (typically `c:\Program Files\IBM\Lotus\Notes\Data\user.id`), and click **Open**.

- The iNotes application imports the file, and reports that your mail file does contain a Notes ID:



- In the DME client application, open **Tools > Settings > Security**, and enter the password for your Notes ID file in the field **Private key password**.

The user is now ready to receive and send encrypted e-mail on the device.

## ID Vault

The Notes ID Vault was introduced in Domino 8.5. It is a server-based database that holds protected copies of Lotus Notes user IDs. This allows administrators and users to easily manage Notes user IDs. Users are assigned to a vault through policy configuration, and copies of user IDs are uploaded to a vault automatically once the policy has taken effect.

The ID Vault option is a superior replacement for the **IDStorage** database solution previously provided by DME.

When the ID Vault has been set up according to specifications in the IBM administration documentation, you need to tell the DME connector to use the ID Vault. This is done in the DME Administrator Web Interface:

- Go to the **Connector** tab
- Click the Domino connector you want to configure
- Click **E-mail and PIM**
- In the **General (Domino)** subtab, select the field **Get user ID files from ID Vault** in the **Notes encryption** group of fields
- Click **Save**.

The DME client user can then enter the password for his or her ID file in the field **Private key password** in **Security settings** on the device, and he or she is ready to receive and send encrypted e-mail on the device.

## Secure push e-mail requirements

The DME server supports two modes of e-mail scan:

1. *Using the users' own user name and password*

If the option **Store user password (encrypted)** is selected in the section **Server configuration > Authentication** in the DME Server Administration Web Interface, the user's ID and password will be used for mail scanning. The user password is encrypted on the DME server.

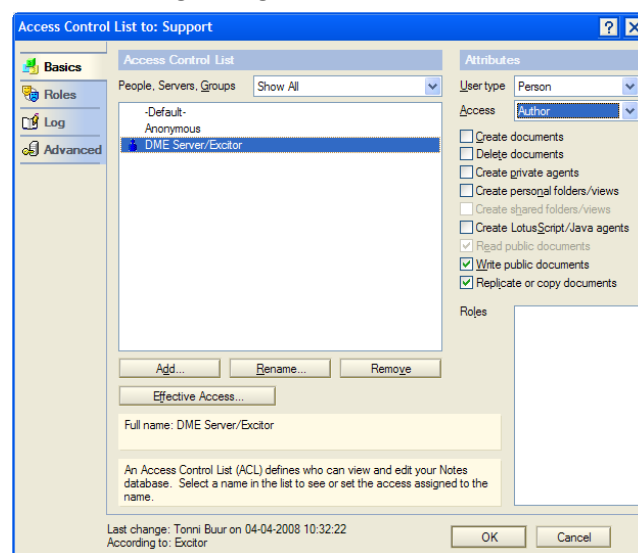
This works without any extra configuration.

2. *Using the technical user (DME\_Server) for all mail scanning*

To enable the DME Server to scan a user's mailbox for new e-mails, the technical user (**DME\_Server**) must be inserted in the ACL of the user's mailbox with at least **Author** privileges.

## Altering ACL for one mail database

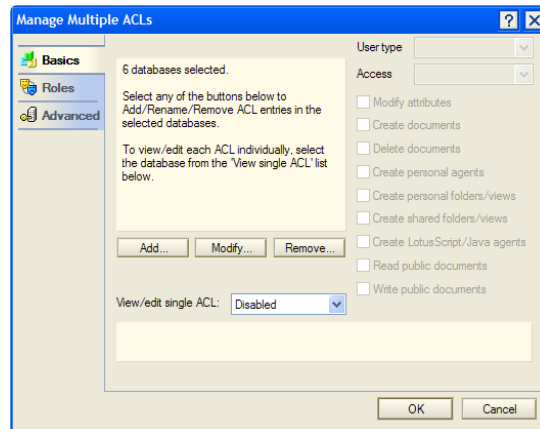
To allow the **DME\_Server** user to perform mail scan for a user, make the following change in the user's ACL:



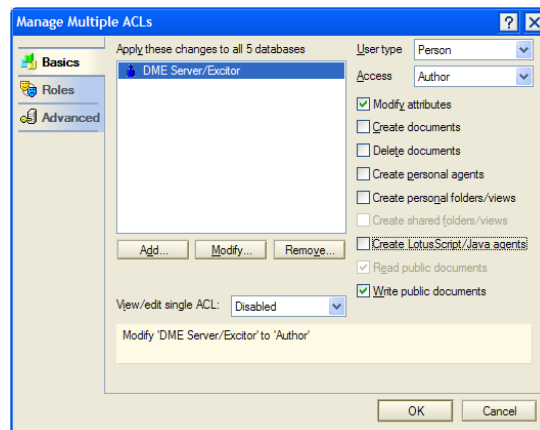
## Altering ACL for multiple mail databases

Using the Domino Administrator, you can change the ACL of multiple databases at the same time. In the **Files** tab, browse to the directory containing the mail databases, and select those that should be scanned by the **DME\_Server** user. Right-click, and select **Access Control > Manage...**, add the LDAP lookup identity, and grant **Author** access.

*Managing multiple ACLs:*

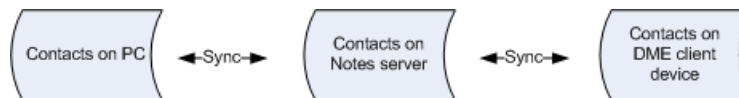


*Mailbox ACL allowing mail scan of multiple databases:*



## Contacts

Personal contacts, which are entered by a user through the Notes interface, are not synchronized with DME clients, unless they are replicated from the personal computer to the Notes server ("iNotes contacts"). DME can only synchronize contacts with the client if they are replicated on the Domino server. See illustration below.

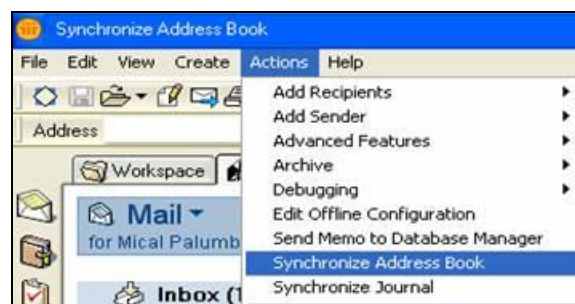


In this respect, Lotus Notes version 7.x and below behaves differently from Lotus Notes 8.x and above.

Note that the following does not apply to *roaming users*. To set up synchronization of personal contacts for roaming users, make sure the field **Use roaming settings if available** is selected in the **Functions** panel of the connector setup page. The location of the personal address book will then be picked up from the **Roaming** settings on the user document of the roaming users.

### Lotus Notes 7.x

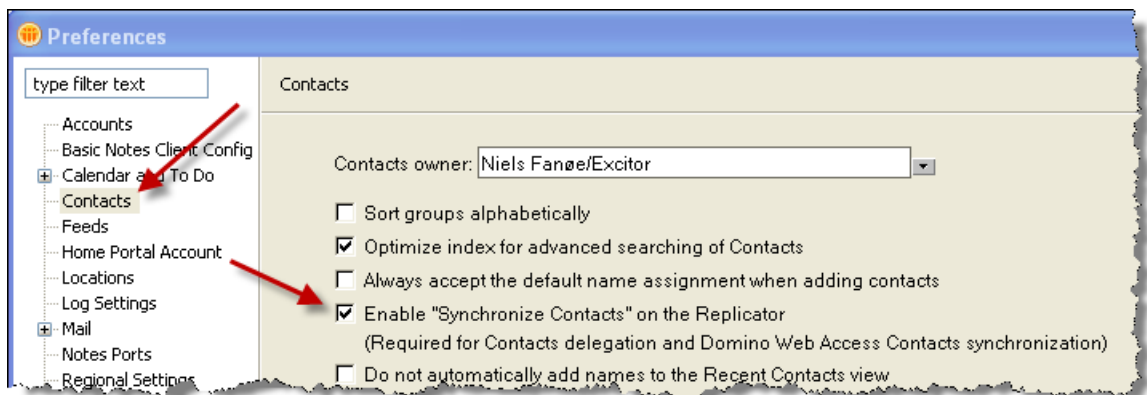
- **To synchronize your local contacts with the Notes server (iNotes) from Notes 7**
  1. Start Lotus Notes, and open your mailbox.
  2. Select **Actions > Synchronize Address Book** from the main menu.



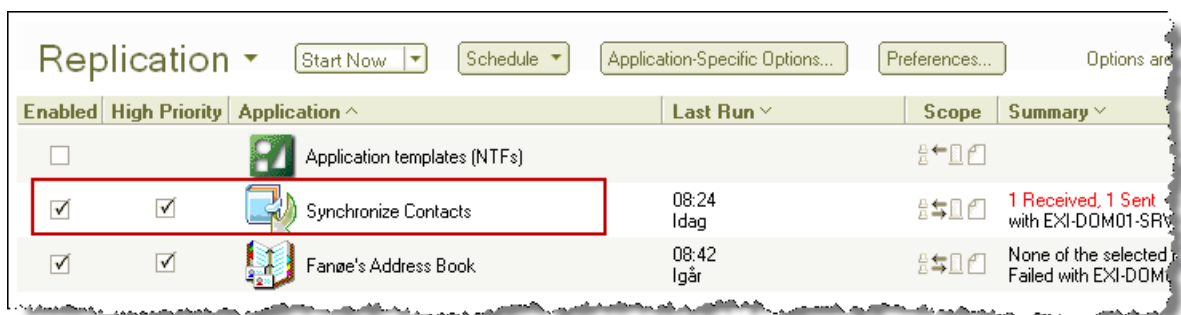
Lotus Notes will compare the contacts stored inside your **names.nsf** file (your local Notes Address Book) and your mail file (iNotes), and synchronize them. Results will be displayed in a dialog. You have to repeat this process each time you add new contacts inside your Notes Address Book, or in iNotes (that is, every time you add contacts on your DME device and synchronize with the DME server).

## Lotus Notes 8.x

- **To synchronize your local contacts with the Notes server (iNotes) from Notes 8**
- 1. Start Lotus Notes, and select **File > Preferences** in the main menu.
- 2. Browse to the **Contacts** section.
- 3. Make sure the field **Enable "Synchronize Contacts" on the Replicator** is checked.



- 4. Select the **Open** dropdown > **Replication** to open the **Replication** page, and make sure **Synchronize Contacts** is now part of the replication and enabled.



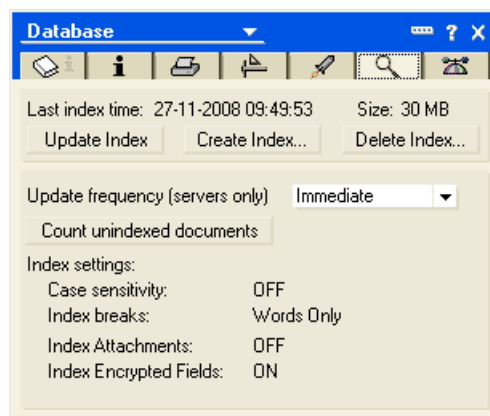
Note that the **Replication** page may also show an entry for your personal Address Book (**Fanøe's Address Book** in the illustration above). This will only happen if your Notes account was enabled for roaming.

## E-mail search

In order to successfully use the **Search e-mail (on server)** feature on the DME clients, the users must have enabled full text indexing of their e-mail database.

It is therefore recommended to enable full text indexing on DME user e-mail databases:

1. Open the **Database** properties for the mailbox in question.
2. Click the **Create Index** button on the tab with the magnifying glass.

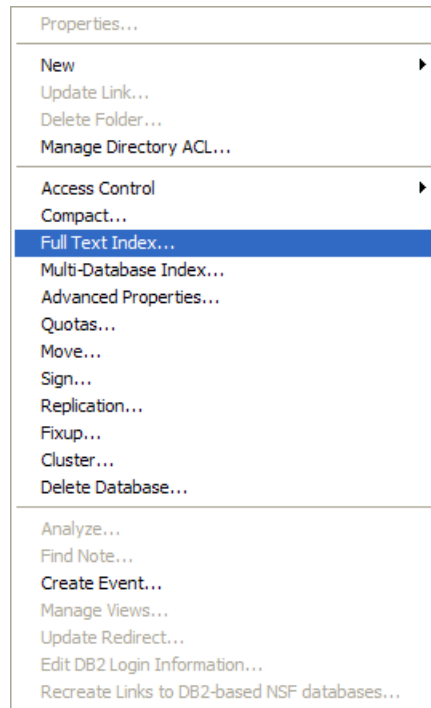


3. Repeat the operation for all DME users.

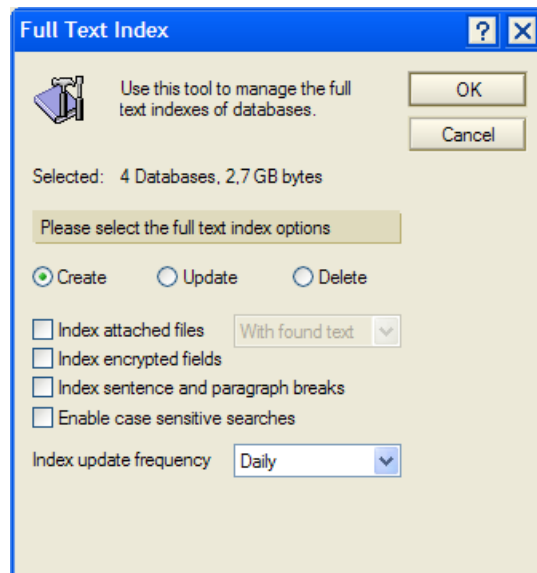
You can also enable full text indexing for several mail databases at the same time:

1. Open the Domino Administrator.
2. Select the mail databases you want to index (using Ctrl+click).

3. Right-click one of the databases, and select **Full Text Index....**



4. Leave the default settings:



-and click **OK** to enable full text indexing of the selected databases.

Please note that the indexing is handled by the Domino server. Depending on the number of databases and their size, this can take some time to finish.



## Sametime integration

*This functionality was removed from DME with DME server 4.1 SPI.*

If you are using Sametime, and you want the DME users to be able to see the Sametime status of their colleagues in DME, you need to create a user for this purpose with default rights.

To connect DME with Sametime, open the DME web interface, and click **Server > Server configuration > Collaboration**.

In the **Instant messaging** section, enter the name of your Sametime server, the name of the Sametime user you just created, and the password of that user as shown below:

Instant messaging	
IM server	<input type="text" value="sametime.excitor.dk"/>
IM username	<input type="text" value="sametime1"/>
IM password	<input type="password" value="*****"/>

DME users running clients set up with network push are now able to see the Sametime status of users on the specified Sametime server.

## Personal notebooks (journals)

As of DME 3.6, it is possible to synchronize users' personal notebooks between Domino and the clients. The Domino *Notebook* feature was called *Journals* in Domino versions before 8.5.

Notebook synchronization is configured in the **Functions** panel of the Domino connector setup page in the DME Administration Interface.

To set up synchronization of personal notebooks for *roaming users*, make sure the field **Use roaming settings if available** is selected. The location of the personal notebook will then be picked up from the **Roaming** settings on the user document of the roaming users.

To set up synchronization of personal notebooks for *non-roaming users*, the notebook databases must be replicated to the Domino server. Then specify the location of the notebooks in the fields **Server** and **Database** in the **Notes** section of the **Functions** panel. Leave the **Server** field blank, if it is the same server as specified in the **Domain** panel of the connector setup page. In the **Database** field, specify the location of the personal notebooks on the form `path\notebookname{0}.nsf`, where {0} is the user's shortname - for instance `journal\notebook_{0}.nsf`.

Keep in mind that the notebook location can also be specified on a per-user basis in the user setup page > **Collab.conf**. A location specified here overrides any other setting.

## Domino integration checklist

This checklist provides an abstract of the information already given. It is meant as a guide to prepare the existing IT environment for the implementation of a DME server.

For more information about firewall settings, see the next section.

### Connections to existing Domino environment

For a successful integration, the following connections must be available. Whether or not firewall rules should be set up depends on your existing environment and the placement of the DME connector (DMZ or internal network).

From	To	Traffic	Port
DME connector	SMTP server	TCP	25
DME connector	Domino server	Corba/TCP	63148 or 60148 (Linux)
DME connector	Domino server	LDAP/TCP	389 or 636 (secure)

Note that if the connector is installed in Notes session mode (Windows only), port 63148 is not necessary.

See also the dynamic Firewall table at the **DME Resource Center** <http://resources.soliton.com/docs/firewall-rules>.

### Tasks/services on the Domino server

For a successful integration, the following Domino tasks must be running:

- ❖ **LDAP**
- ❖ **DIOP/CORBA** (unless the DME connector is running through a Notes session or Domino session)

## User groups

The following groups must be created, and the appropriate users added. Please note that the group names are case sensitive.

Group	Members	Note
<b>DME_User</b>	Regular users	Membership of this group allows a user to connect to the DME Server from a device.
<b>DME_Admin</b>	Administrators of the DME server	Membership of this group allows a user to manage the DME Server and DME users. Membership of this group does not allow connections from a device.
<b>DME_Superuser</b>	Superusers of the DME server	Membership of this group allows a user to have read access to the DME Server. No server settings can be changed by the user, but settings can be set for selected groups of users.

## Specific Domino setup

Review the sections **Contacts** on page 28 and **E-mail search** on page 30 to ensure that contact synchronization and e-mail search will work on the DME clients.