Telia Mobil Mail Enterprise Edition

(Microsoft Exchange)
Release 5.2

User Guide

Installation and administration Guide
Document version 1.4

Table of Contents

Table Of Figures

1 Introduction

Welcome to ”Telia Mobil Mail”, which offers you the chance to transfer the key features of Microsoft Outlook and Lotus Notes from your desktop straight to your phone. This allows you to move freely, but still keep up with all of your important email accounts, calendar appointments and contacts. This Installation and Administration Guide presents the setup process for the corporate administrator and basic functions of the software. Please read these instructions carefully before utilising your ”Telia Mobil Mail”.

1.1 How ”Telia Mobil Mail” works

”Telia Mobil Mail” is designed to connect mobile device users easily and securely to enterprise groupware systems. The figure below picture describes the ”Telia Mobil Mail” Push components to give you an overview of the whole framework.

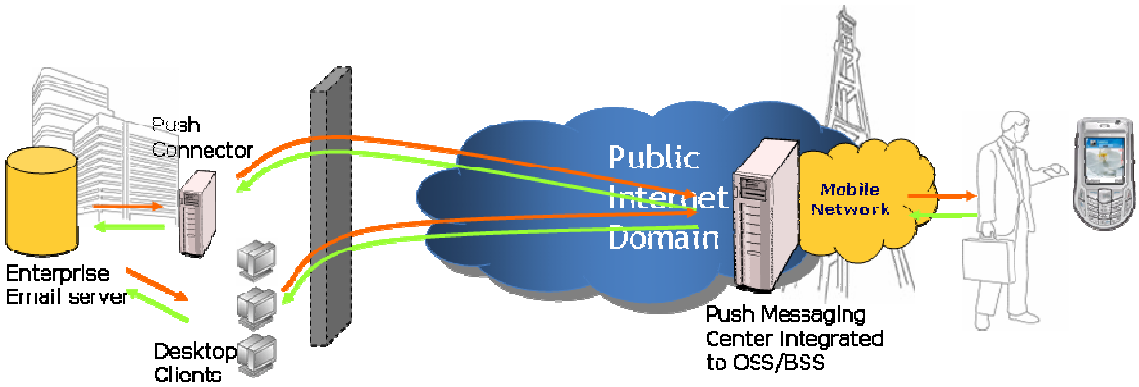


Figure 1. Solution Overview

The ”Telia Mobil Mail” Push Connector monitors mailboxes to mirror any changes to the mobile client. It is designed for deployment on a computer situated on a corporate network, and run by the IT administrator of an organisation. The Push Connector includes several features that enable administrators to tailor the ”Telia Mobil Mail” service to your individual needs.

The ” Telia Mobil Mail” Relay Server is designed to enable Push Connectors to connect to the ”Telia Mobil Mail” Client, which is otherwise not addressable due to corporate firewall and the dynamic nature of mobile device’s IP address and network availability.

The Push Client resides on the mobile device, and maintains a connection to the Relay Server using TCP/IP over a packet data (e.g. GPRS, 3G) network. This enables True Push from the Relay Server once a new email arrives or a change in the calendar notes occurs.

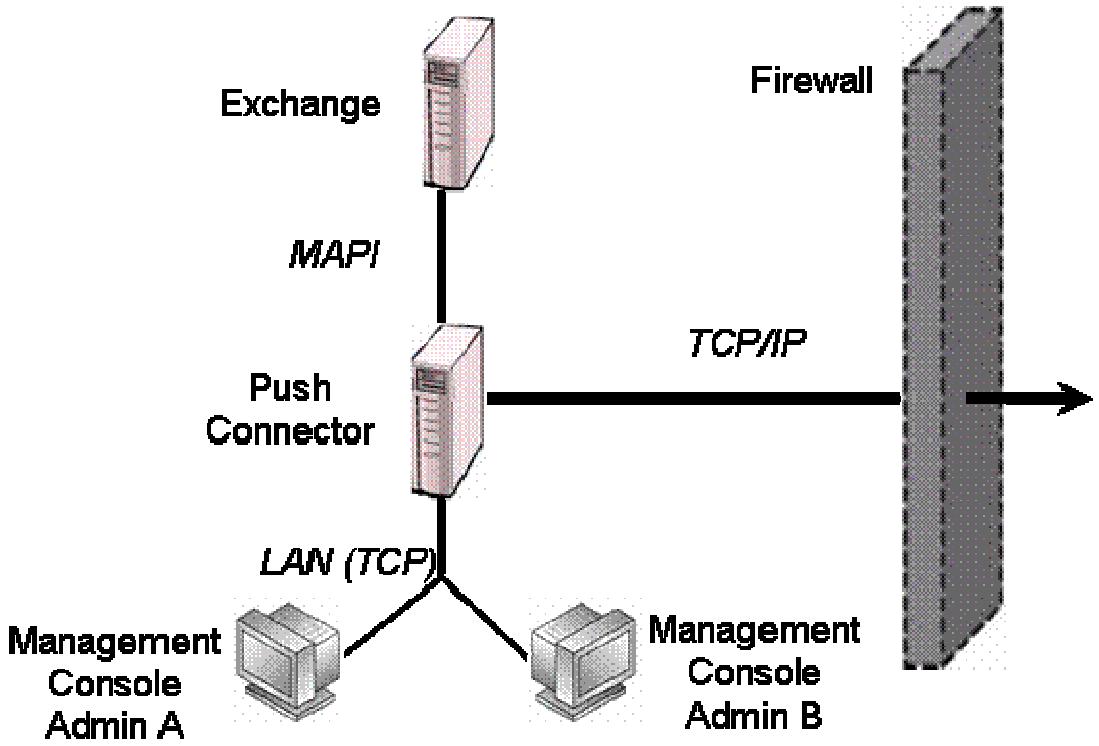


Figure 2. Push Connector in the corporate network

Inside the corporate LAN, the Push Connector connects to the Exchange Server using MAPI. It can be administered remotely from any computer in the corporate LAN through the Push Connector Management Console. The outward connection to the Relay Server is via TCP/IP.

1.2 How Push Connector Works

The Push Connector runs as a Windows service on a Windows Server machine in the LAN and constantly monitors multiple user mailboxes. Push connector must be located close to the email server in the network so that the network latency and bandwidth are sufficient to manage multiple mailboxes at the same time.

Push Connector administration is performed remotely from a Management Console program, which runs on a PC machine in the same LAN. Administrators can manage many push connectors from the same console. Also, there may be many management consoles installed to manage the same connectors.

Push Connector constantly monitors only the mailboxes of active users. All events in a user's mailbox are signalled to the Push Client immediately when the event happens. Also, all the events communicated by the Push Client are immediately applied in the user's mailbox.

Push Connector requests user connectivity status information from Relay Server once an hour, by default. So, if user has been disconnected from the Relay Server an hour or more then Push Connector will notify this, set user into Inactive, state and stop monitoring the user's mailbox. Push Connector keeps communicating events to the mobile device until it notices that the client is disconnected from Relay Server. Thus, Relay Server needs to store those messages in

its message queue to wait until the device connects again. The messages in queue are stored in encrypted format.

When device connects again, Relay Server will first push all queued messages to the device and immediately notify the connector that the device is active again. After this event, Push Connector compares the current mailbox state and the state when user was last connected, and replicates the current state to the device.

If a mobile device is disconnected for a long time and there are queued messages in the Relay Server message queue, then Relay Server clears old messages from the queue automatically and they will never be delivered to the device. By default, Relay Server clears queued items older than 5 days.

1.3 Secure Communications via Relay Server

The protocol used in communication between the Push Connector and Relay Server uses standard FIPS compliant AES encryption. The primary transport protocol to Relay Server is a plain TCP connection. TCP connections from Push Connector through the Firewall are only opened towards the Relay Server and therefore there is no need to open any ports in the Firewall for inbound connections. The Push Connector only uses outbound connections and never acts as a server towards the Internet.

TCP connection is established only after a successful challenge-response authentication between Push Connector and the Relay Server. Both Relay Server and Push Connector store a connector specific authentication key for this purpose. Also the Push Clients use the same challenge-response authentication towards Relay Server, but the authentication key is, of course, unique for each device.

Third party VPN solutions can be used between Relay Server and the Push Connector to bring additional security but this is not necessary as the application protocol is end-to-end secured.

All application data delivered between mobile devices and connectors is end-to-end encrypted using 128 bit AES encryption. These packages are communicated via Relay Server in a secure way but Relay Server is, of course, not able to see the content of the data being transported.

2 Push Connector Installation

2.1 Installation Quick Steps

This section provides a list of steps to successfully install the Push Connector.

1. Make sure your system meets the software and hardware requirements as described in section 2.2.
2. Create a Windows user account with sufficient permissions. This is described in section 2.3. Please note that without sufficient permissions the service cannot run.
3. Install the Push Connector with Push Connector Manager as described in sections 2.4 - 2.5.
4. Optionally install further Push Connector Management Consoles for remote administration as described in section 2.6.
5. Enable service(s) for users using the Push Connector Manager as described in section 3.7.

2.2 System requirements

The table below specifies the overall system requirements for installing and running the Push Connector.

Machine for the Push Connector installation (Enterprise Server)	Hardware (0-1000 users): • Intel (>1 GHz) CPU • RAM: Min 512 MB. This amount is sufficient for organizations up to 50 000 employees (employees meaning entries in the GAL). For larger organizations the minimum recommendations are as follows: 50 000 - 100 000 in GAL: 1GB RAM 100 000 - <200 k in GAL: 1,5 GB 200 k - <300k in GAL: 2 GB >300k in GAL: ≥2 GB On the minimum configuration you can run up to 250 users (meaning users of the service) on the Push Connector. After that add 256 MB for each 250 users added to the Push Connector. Please note that these recommendations are estimates and may depend on the data in each GAL entry. For better performance it is recommended to add more RAM than the minimum requirement. • It is recommended to have one Push Connector per 1000 users and to balance the users evenly across Connectors • 100 MB free disk space Operating system: • Windows 2000 Server SP3, or higher • Windows 2003 Server • Windows XP Professional Installed additional software: • Microsoft Outlook 2000, or • Microsoft Outlook 2003 **NOTE!** Outlook XP should NOT be used! It is recommended to use English language versions of the operating system and Outlook client software. Microsoft does not recommend running Outlook on the same machine with Exchange or Domain Controller. So, the connector must not be

	installed on the same machine that is running Exchange server or Domain Controller. Support for Languages that require Unicode characters in email messages requires that the default language for non-unicode characters is set in the operating system. See chapter 2.3.1 for more details.
Network Connections	The Push Connector machine needs to have a fixed IP address in the LAN. Public IP address is not required. Constant LAN (>10 Mbps) connection from the Push Connector PC to the Exchange Server with latency less than 10 ms. See chapter 2.2.1 for more details. There should not be any firewalls between the Push Connector and Exchange computers. If there is a firewall between the two computers, it must be configured so that Outlook can access the Exchange server from the Push Connector computer. For more information how to configure these firewalls please consult Microsoft documentation. The Exchange Server must have TCP/IP connectivity and be able to send and receive Internet emails. The Push Connector server must be configured as a **Member Server** on the same domain as the Exchange Server. The firewall must be configured to allow TCP outbound connection from the connector machine to Relay Server (default port 7171). The available ports towards the Relay Server are defined in the connector license file.
Exchange Server	Microsoft Exchange 5.5, or Microsoft Exchange 2000 SP3 with Post-Service Pack 3 Rollup*, or Microsoft Exchange 2003 SP1 and SP2 A new Exchange user account for the Push Connector (the ”Telia Mobil Mail” privileged user account). This account must have an Internet email address (for example, AlwaysOnAdmin@company.com) and access to all of the Exchange mailboxes of the intended ”Telia Mobil Mail” end-users. *Post-Service Pack 3 Rollup fixes problems with message read/unread status for off-line use of Outlook **NOTE!** Environments which are undergoing a migration from Exchange version to another may cause problems to Push Connector. Lost functionality is possible to restore when all mailboxes have been migrated to new server environment, including the Push Connector mailbox.
Windows User Account	The Windows user account used to run the Push Connector service needs **local administrator** rights and **log on as service** rights to the machine where the Push Connector service will be installed and run.

2.2.1 Checking Network Latency to the Email Server

Push Connector requires fast LAN connection to the email server to run properly. Required bandwidth is 10 Mbps and the round-trip time to server should be below 10 ms.

Network latency is checked easily using a ping command on the Push Connector machine as follows:

1. Open Windows command prompt
2. Type ping <email server hostname/IP address>
3. Check the round trip time shown in the command output

If the network latency is too big place the push connector machine closer to the email server in your LAN. If there are many email servers in different geographical locations, each location should have its own Push Connector.

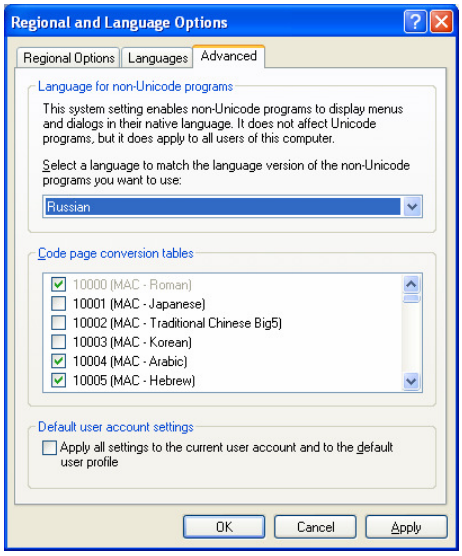
Having small bandwidth or big latency to the email server may cause Push Connector to go in error state for one or more users time to time.

2.3 Preparations for Installing the Push Connector

A successful installation of ”Telia Mobil Mail” Push Connector requires that a service account with suitable permissions is created for the service. Without adequate permissions the service cannot run properly. Creating the privileged user account is described in the following chapters. You must have an Exchange server installed in order to install the Push Connector. If you plan to install several Push Connectors, one service account for each Push Connector is required. Service account names should be unique across domains.

2.3.1 Setting non-unicode Language

The default language for non-unicode programs must be configured in the operating system that runs the Push Connector if the service will be used to deliver messages with characters that require unicode support, such as Cyrillic characters.



Instructions:

1. Open Control Panel => Regional and Language Options
2. Open 'Advanced' tab
3. Select the used language from the drop-down list in 'Language for non-Unicode programs'
4. Click OK

If this setting is not set, the messages sent through the service may have '?' characters replacing original ones.

2.3.2 Creating a service account (privileged user)

Please note that granting the privileged connector account appropriate privileges is the most important step of installation and granting insufficient privileges will cause problems later when running the service. The service is designed to perform operations such as reading, sending and deleting emails and needs permissions to do so. Shortcuts and workarounds such as granting delegate access from the Outlook client do not work.

Creating the push connector service account is done as follows:

1. Log on to the computer running Exchange as Administrator.
2. Go to **Start> All Programs> Microsoft Exchange> Active Directory Users and Computers**.
3. Select the **Users** folder, and on the **Action** menu select **New>User**. The New Object–User dialog will appear.
4. Enter details of the privileged user account, for example, **privuser** in the **First name** and **User log on name** fields. Click **Next**.

Figure 3. Creating New User Account for the Push Connector

5. Enter the password and tick the **Password never expires** box. Make sure that all other boxes are unchecked. Click **Next**.

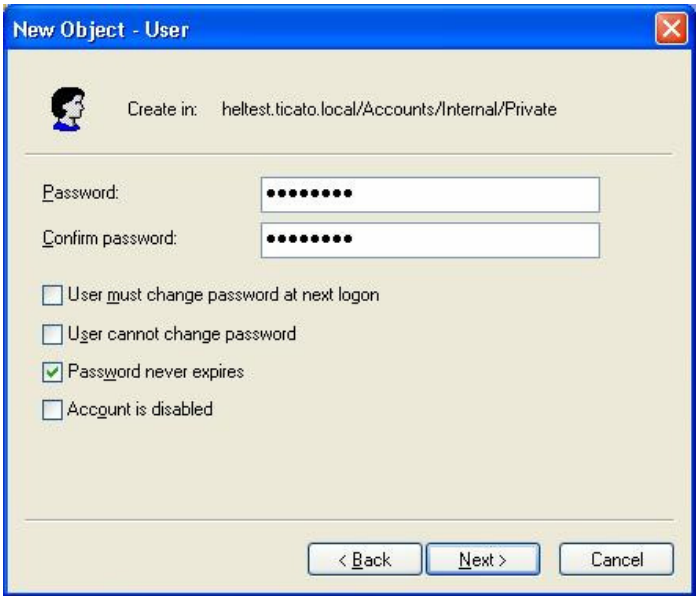


Figure 4. Set Password

6. Leave all the fields with default values and make sure that the **Create an Exchange mailbox** is ticked. Click **Next**.

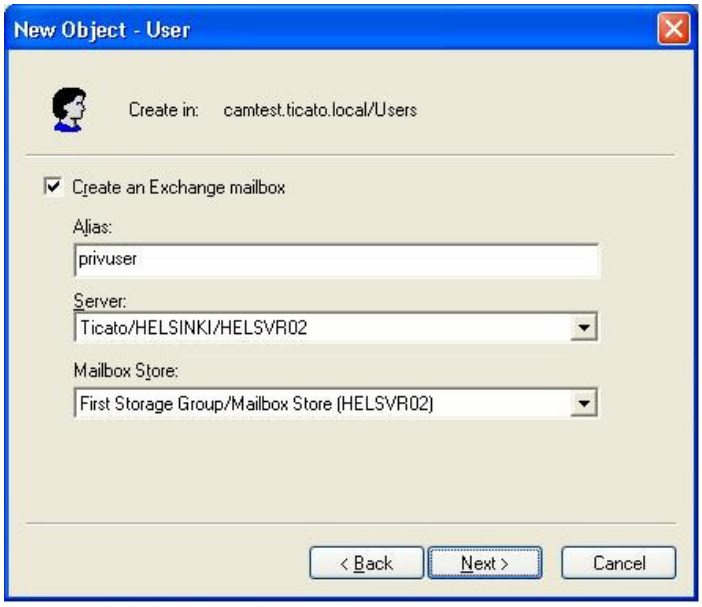


Figure 5. Creating an Exchange Mailbox

7. Click **Finish** to create the new account.
8. In the Active Directory Users and Computers screen, right click on the privileged user account just created and select **Properties**.
9. Fill the General tab **Description** field with something like **"Telia Mobil Mail" privileged user account**.

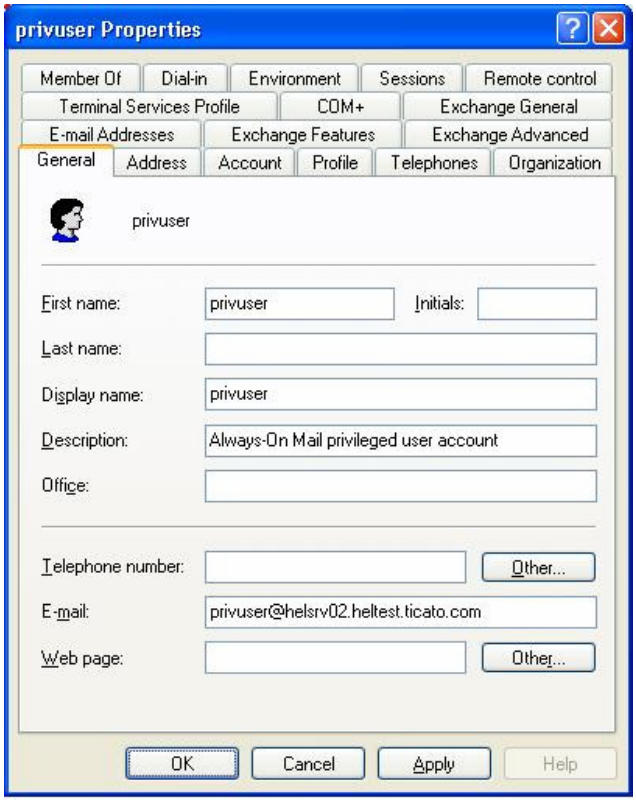


Figure 6. Privileged Connector User Account Properties

10. Click the Member Of tab, and click **Add**. The Select Groups screen will appear.

11. Add the **Exchange Enterprise Servers** group. Click **OK**. This gives mailbox access to all mailboxes in the system and is the recommended option. If you are running Exchange 2003, or if you want to give mailbox access "user by user", see chapter 2.3.4. For instructions how to check that you have sufficient privileges see section 2.4.1.

NOTE!
Make sure that the privileged user is not a member of the **Domain Admins** group, or adding users to the server will fail later on.

In some cases, there can be conflicting access rights due to different settings on a higher level. Privilege defaults may also change between mail server versions, so when you upgrade, always check the privileges. In Exchange 2003, please ensure that the privileged user account has the following rights to each user's mailbox that will be using the "Telia Mobil Mail" service:

- **Administer Information Store**
- **Send As**
- **Receive As**

Check this by the following procedure:
1. Open **Start**>**All Programs**>**Microsoft Exchange**>**System Manager**
2. Open **Servers**>[Your Server]. If you are using several Administrative groups, you find this setting under **Administrative groups**>[Your Group].
3. Right click on [Your Server] and select **Profiles**
4. On the **Security tab** select the user or group
5. Verify that the appropriate privileges, (see above) are checked as 'allow'

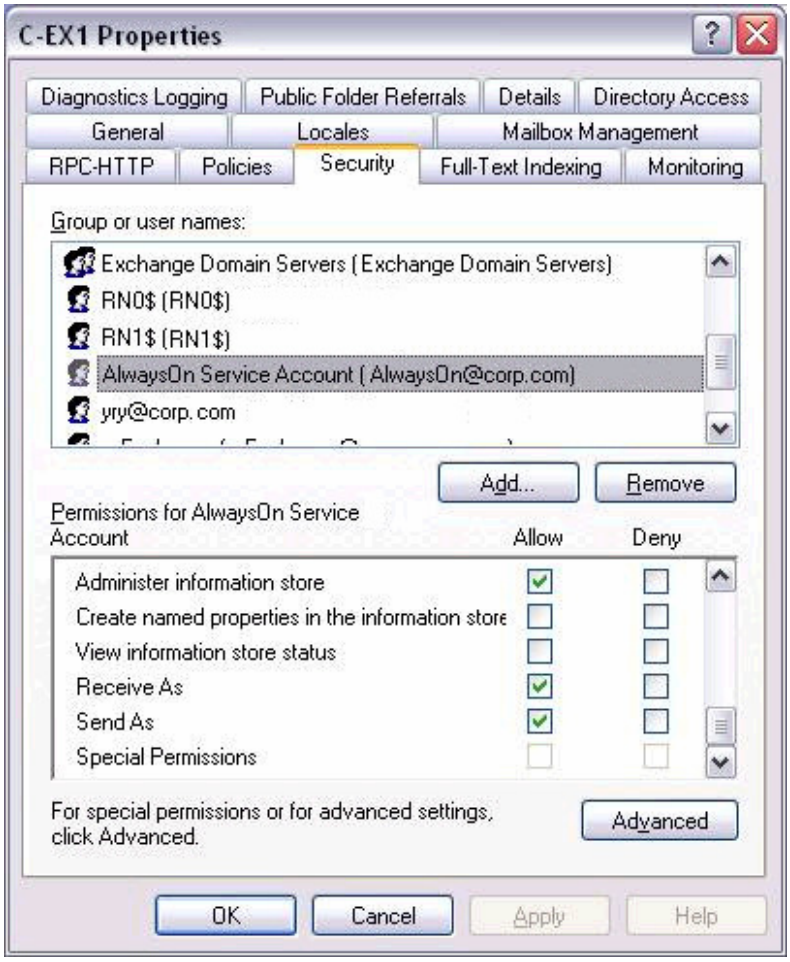


Figure 7. Account Privileges

12. Go to section 2.3.3 to give the privileged user account the **Log on as a service** rights. If this is not set, the installation program will report an error stating '…could not start system services…'. You can then also ignore this error and set these permissions from Windows Services properties.

2.3.3 Running the Push Connector as a Service

You now have to make sure that the created privileged user account has the **Log on as a service** rights on the Windows 2003 server (the server that used to install and run the "Telia Mobil Mail" Push service). This is done as follows:

1. Grant the privileged user local administrator permissions. Using an account with local administrator permissions (for example, the local Administrator account or an account which is a member of the Domain Admins group), log on to the server where you plan to install the "Telia Mobil Mail" Push service.
2. Go to **Start>Control Panel>Administrative Tools>Computer Management**.
3. Select **System Tools>Local Users and Groups>Groups**.

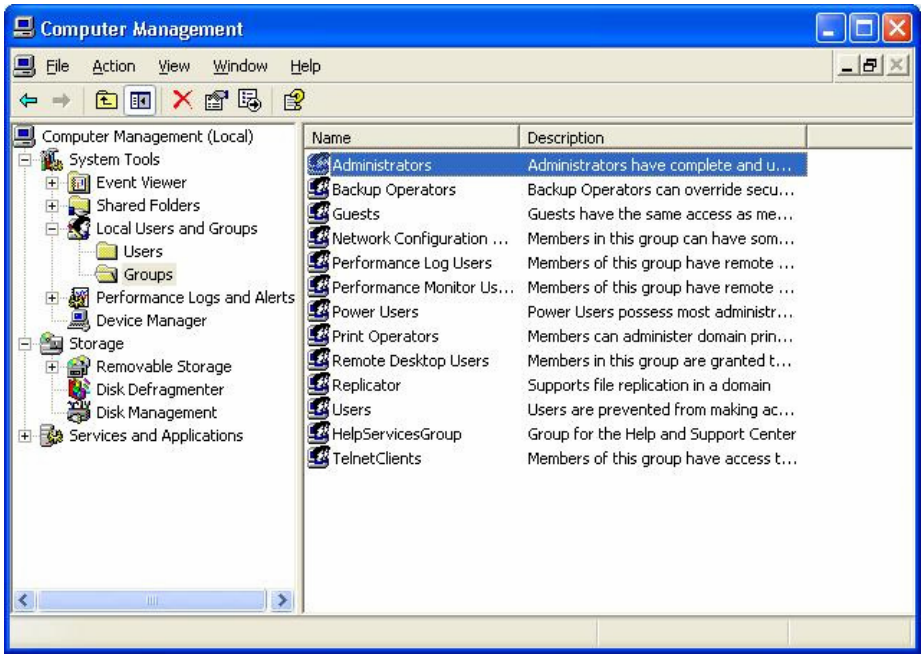


Figure 8. Local Users and Groups

4. Double click the **Administrators** group. The Administrators Properties screen will appear.
5. Click **Add**.
6. In the **From this location** text field, select your domain. In the **Enter the object names to** select text field, add the user account you created and click **Check Names**. Click **OK** to confirm.

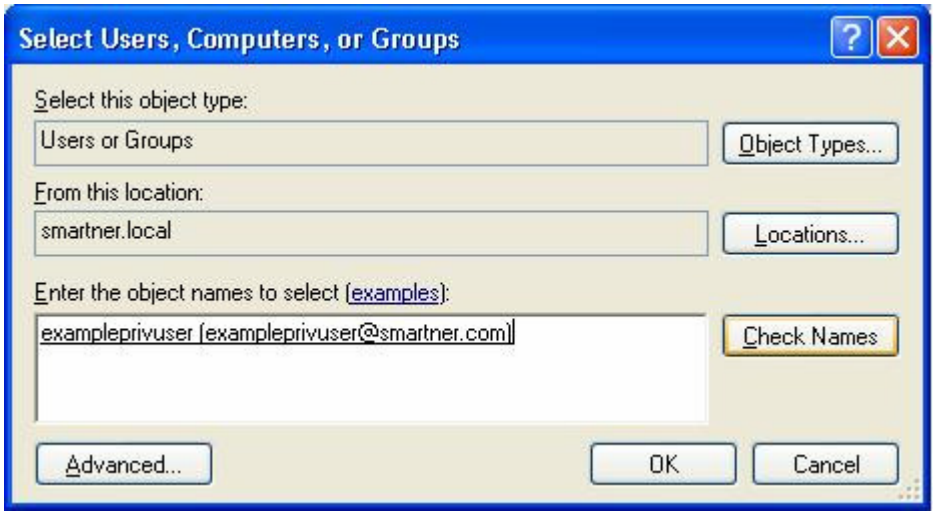


Figure 9. Select Users, Computers or Groups

7. Grant the privileged user the **Log on as a service** rights. Go to **Start>Control Panel>Administrative Tools>Local Security Policy** and select **Security Settings>Local Policies>User Rights Assignment.**

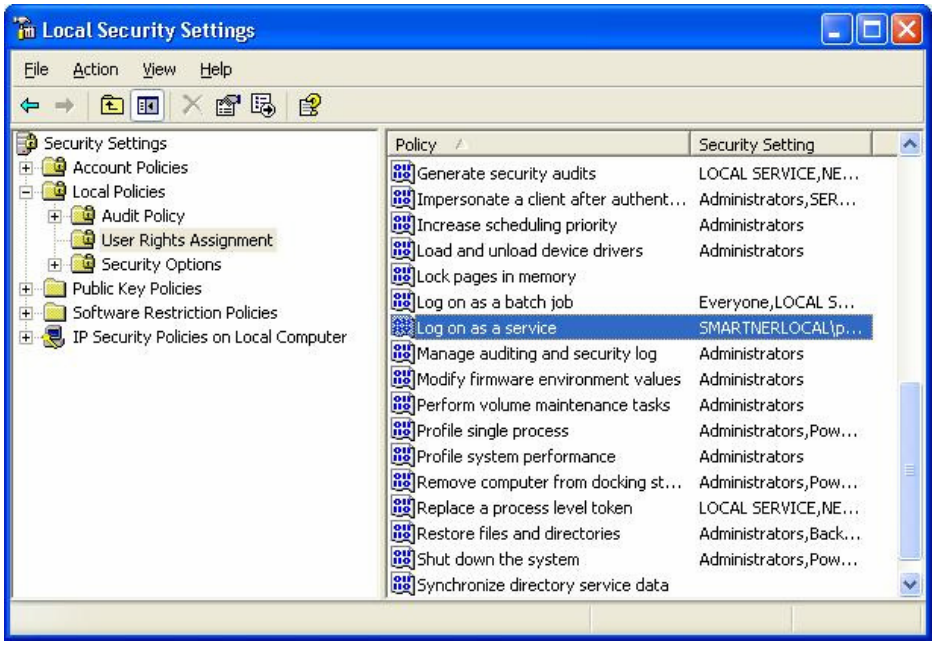


Figure 10. Group Policy

8. Double click the **Log on as a service** entry. A Properties dialog with security setting tab will appear.
9. Click **Add user or Group**. The Select Users, Computers or Groups dialog will appear.
10. In the **Enter the object names to select** text field, add the user account you created and click **Check Names**. Click **OK** to confirm.

Figure 11. Select Users or Groups

You are now ready to install the ”Telia Mobil Mail” Push Connector as specified in chapter 2.4.

2.3.4 Granting Mailbox Access User by User

This section is optional and you only need to make the changes explained here if you were not able to give privileges as outlined in section 2.3.2. As described there, the default access rights

configuration for the privileged connector user account grants connector the access to all mailboxes in Exchange. Thus, no additional access rights configurations are required when adding new users to the connector. However, in Exchange 2003 environments the full mailbox access permission is disabled by default and unless you can override this mailbox right otherwise you need to grant the rights user by user.

So, if required, it is also possible to grant the privileged user such user rights that it cannot access all the mailboxes and grant access to the mailboxes user by user as they are added to the service.

The following instructions can be used to grant connector the necessary access rights to one mailbox.

1. Open Active Directory user list
2. Select the user to be added in the connector
3. Open its properties and select 'Exchange Advanced' page
4. Click 'Mailbox Rights…'
5. Add the privileged user account (connector account) in the list and grant 'Full mailbox access' to this user (see the picture below)
6. Click 'Apply'

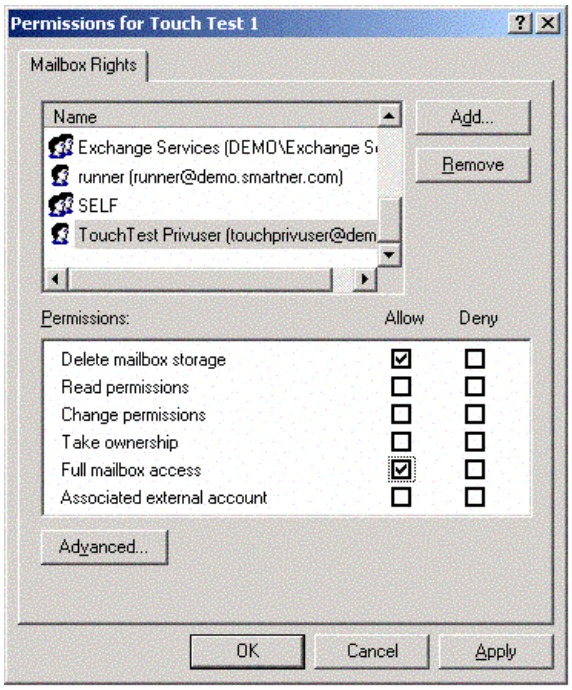


Figure 12. Mailbox permissions

NOTE! Check that there are no conflicting access rights blocking the mailbox access on a higher level in the Active Directory hierarchy.

2.4 Installing the Push Connector

Before you install the Push Connector, please contact your "TELIA MOBIL MAIL" Reseller to get your **license file**. You will be prompted for the license file when you run install the Push Connector Manager.

2.4.1 Prerequisites for Installing the Push Connector

Important Prerequisites!

1. **Privileged user**
   Make sure that you are logged onto the Windows 2003 server where you plan to install the ”Telia Mobil Mail” Push Connector as the privileged user.

2. **User account access**
   Make sure that you have access to all email accounts on the domain using MS Outlook. To verify this, open Outlook. If this is the first time Outlook has been run under the privileged user account, you will have to follow a series of prompts:
   1. Select Corporate or Workgroup mode and open the mailbox of the privileged user.
   2. Once Outlook has been opened, select **File**>**Open**>**Other User’s Folder**.
   3. Select the inbox of any intended ”Telia Mobil Mail” end-user and click **OK**.

   If the user’s inbox can be accessed, then you have successfully configured the privileged user account.

3. **Log on as a service**
   Make sure that that you have **Log on as a service** rights. To confirm this:
   1. Go to **Start>Settings>Control Panel>Administrative Tools>Local Security Policy**. The Microsoft Management Console for the Local Security Settings will appear.
   2. Select **Local Policies>User Rights Assignment**, and double click **Log on as a service**. The Local Security Policy Settings screen will appear.
   3. Make sure that the privileged user account that you have added has a tick in both, the Local Policy Setting and Effective Policy Setting, boxes.

4. **Verify TCP connection to Relay Server**
   Make sure that you have a TCP connection to the Relay Server. You can find the Relay Server IP address in the licence file. You can verify the connection, for example, via trying to open a telnet connection from the connector machine to the Relay Server as follows:

   Example, Telnet to relay server port 7171 using command line command: *telnet relayserver.com 7171.*

2.4.2 Defining Outbound Connection Port

The license file may include more than one port that the push connector can use to connect to the relay server. You can remove some of the options to force the Push Connector to use a certain port only. Please note that you cannot add ports to the list, as the ports are defined in the Relay Server.

So, if the license file defines Relay Server ports 7171, 9191, and 80, then the connector will try each one of these ports until it gets a direct TCP connection to Relay Server. It will choose the first port which enables connection to Relay Server.

2.4.3 Push Connector Installation

”Telia Mobil Mail” Push Connector is installed as a service on its host computer. Once ”Telia Mobil Mail” is installed, the Windows services manager will administer it.

To install the Push Connector files, follow these steps:

1. Run the connector installation program (the **.msi** file)
2. The InstallShield Wizard screen will appear. Click **Next**.
3. Once you have read and agreed to the license agreement, click **Next**.

Figure 13. Access configuration

4. An access configuration screen will appear. Enter the password of the privileged user in the fields provided and click **Next**.

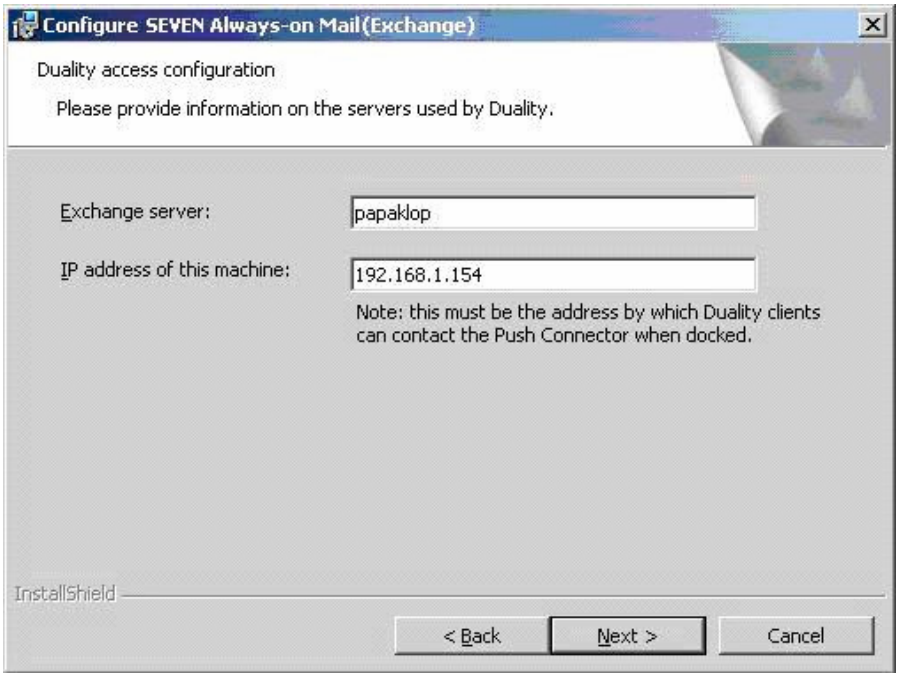


Figure 14. Email server configuration

5. Enter the IP address of the Exchange Server Host machine and the name of the Exchange Server in the fields provided, and click **Next**. This information is required for when Windows Mobile clients connect to the Push Connector when they are cradled.

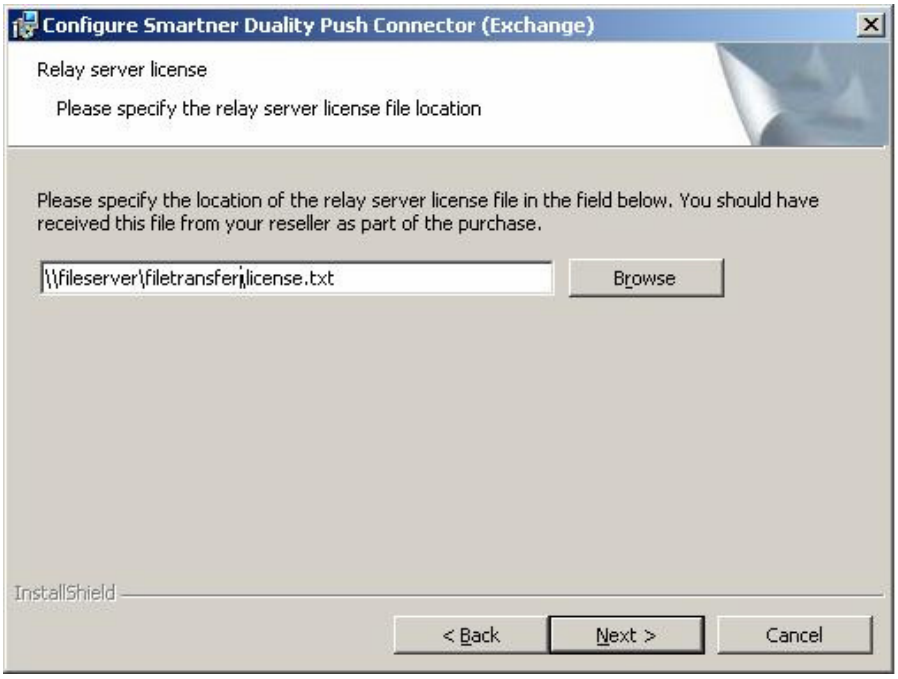


Figure 15. License file location

6. In the Relay server license screen, browse to the location of the license file you received when you purchased the licences and click **Next**. At this stage a TCP connection to the Relay Server is created.
7. Click **Install** to begin the installation.
8. The Installing ”Telia Mobil Mail” Push Connector screen will appear.
9. When the installation is finished, the InstallShield Wizard Completed screen will appear.
10. Click **Finish** to complete the installation.

2.5 Upgrading the Push Connector

This section describes how to upgrade the Push Connector if you have a previous version installed. If you are using 4.0, a prerequisite for the upgrade is that you acquire a new license file from your reseller. New license is not required if you are installing on version 5.0 or 5.2.

End-users may be in any state in the service during the upgrade.

Existing users can use the new features only after the client application on the mobile device is updated as well.

Steps to perform the Push Connector 5.2 (Enterprise Server) upgrade:

1. Log on to the connector computer as the Windows user that is running the connector. (You can check this by opening the ”Telia Mobil Mail” Connector Manager program from the Start Menu. If the program starts, you are logged in as the correct user)

2. Start the installation program of the ”Telia Mobil Mail” 5.2 Push Connector. Installation program will update all relevant components and keep existing users and settings.
3. You will be prompted for a license key if upgrading from a pre 5.0 version.
4. Check that the upgraded connector services are up and running after the upgrade.

NOTE! Automatic upgrade is not possible if Push Connectors have different branding, i.e. product name. You must upgrade the Push Connector with a newer push connector having the same product name, or perform the upgrade so that the new connector is installed parallel to the old one and users are removed from the old one and added to the new connector when they upgrade the client software.

2.6 Installing Push Connector Management Consoles

The Push Connector Management Console can be installed on separate PCs from the Push Connector to enable remote management of the server. The main benefits are:

- The Push Connector can be remotely administered by the administrators from any location on the corporate LAN
- The Push Connector Management Console can be used to administer several different Push Connector instances
- Management rights can be delegated through standard Windows Domain user rights management
- The Push Connector administrator does not need to have access to the emails in the Exchange server (through the privileged user). This permission is restricted to the Push Connector service only.

The Management Console is installed automatically on the Push Connector Server. To install the Push Connector Management Console on other computers follow these steps:

1. Log on to the Push Connector with the Push Connector service account (privileged user).

2. On the **Push Connector Server**, go to **Start>”TELIA MOBIL MAIL” Push Connector>Access Manager**.

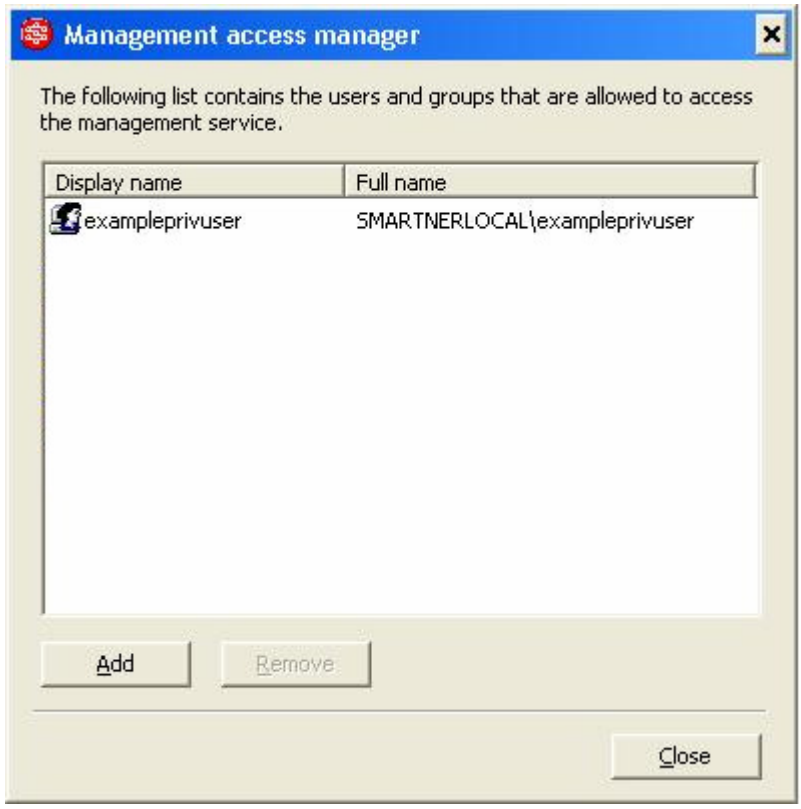


Figure 16. Access manager

3. Add the User or Group that needs access to the Push Connector. Hint: For easier administration it may make sense to create an Active Directory group e.g. PushConnectorAdmins. Then you need to add the users who need access to Push Connector only into this group in Active Directory.
4. Log in to another computer as one of the users to whom you gave access to the Push Connector.
5. Run the Management Console Setup program.
6. Once you have read and agreed to the license agreement, click **Next**.
7. Select the installation directory and click **Next**.
8. Select the program folder for the Start menu icon and click **Next**.
9. In the Ready to Install screen click **Install**.
10. If the installation was successful, the InstallShield Wizard Completed screen will appear.
11. Click **Finish** to complete the installation.

Once installed, the Management Consoles are automatically updated when a new version of the Push Connector is installed.

3 Push Connector Administration

3.1 Launching the ”Telia Mobil Mail” Push Connector Manager

When you have installed the Push Connector Management Console, it can be opened from the Start menu.

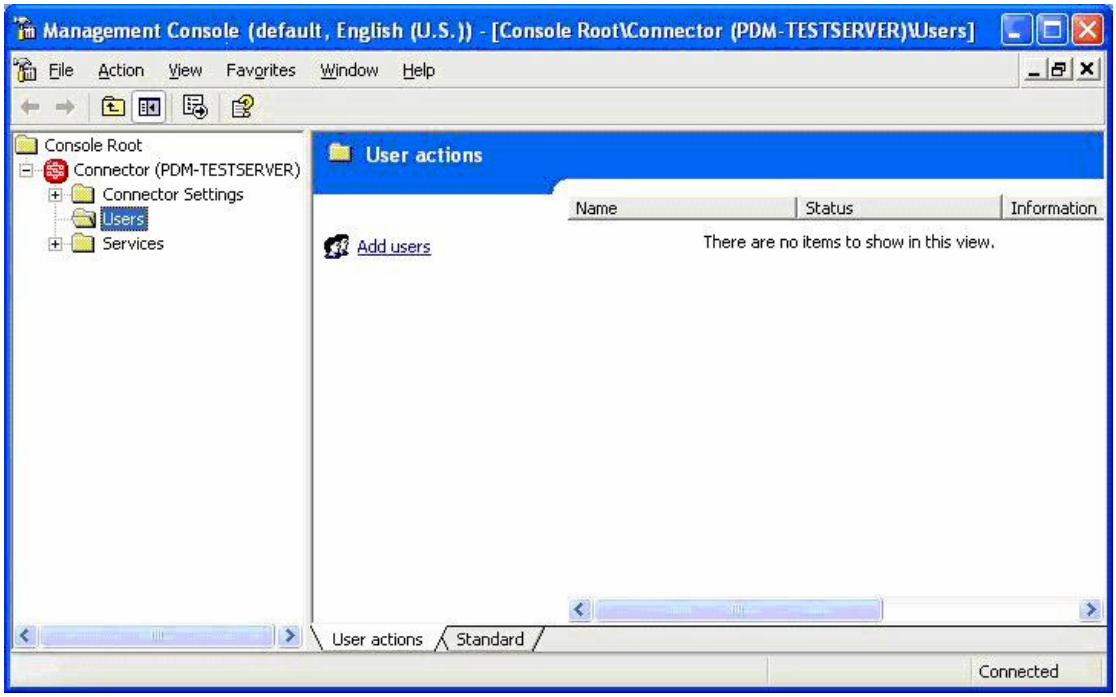


Figure 17. Push Connector Manager

You are now ready to use the Push Connector.

3.2 Connecting to Push Connector server

This section describes connecting to the server when using a remote ”Telia Mobil Mail” Management Console. If you are using the Management Console locally on the Push Connector, it is automatically connected. To connect to the server, follow these steps:

1. Right click on the **Connector** and select **Properties**.

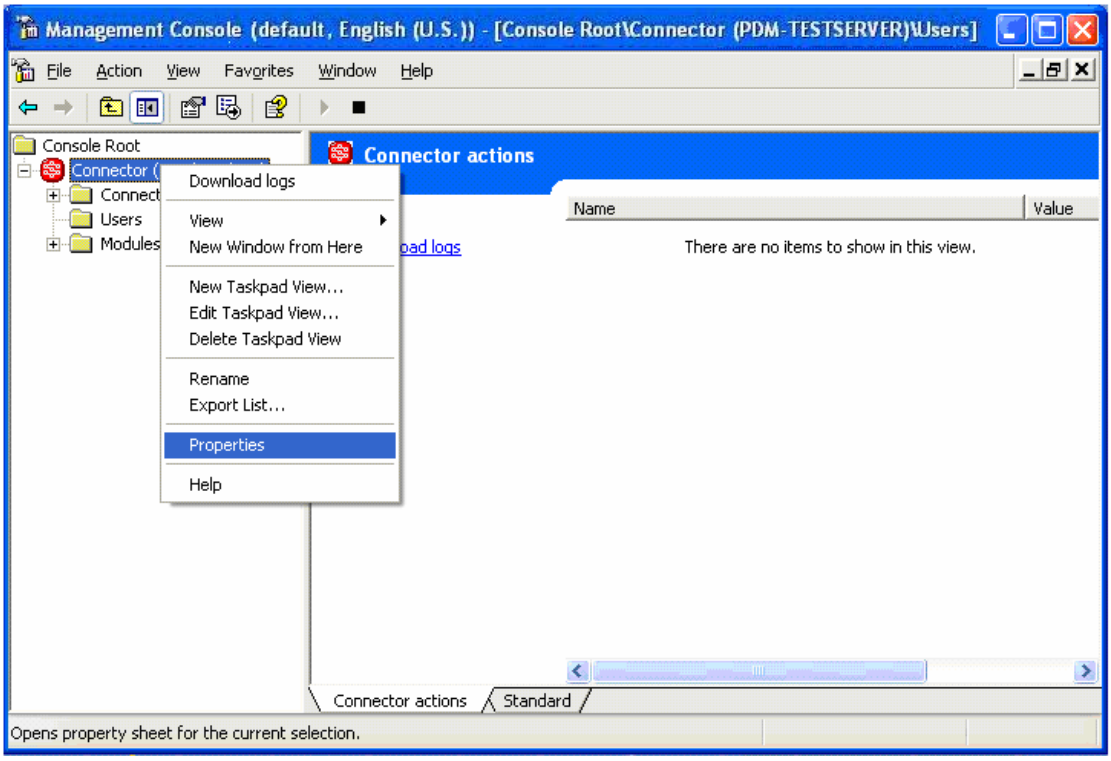


Figure 18. Connector Properties menu

2. In the **Properties** dialog select **Another Computer** and **Browse** to the Push Connector computer.

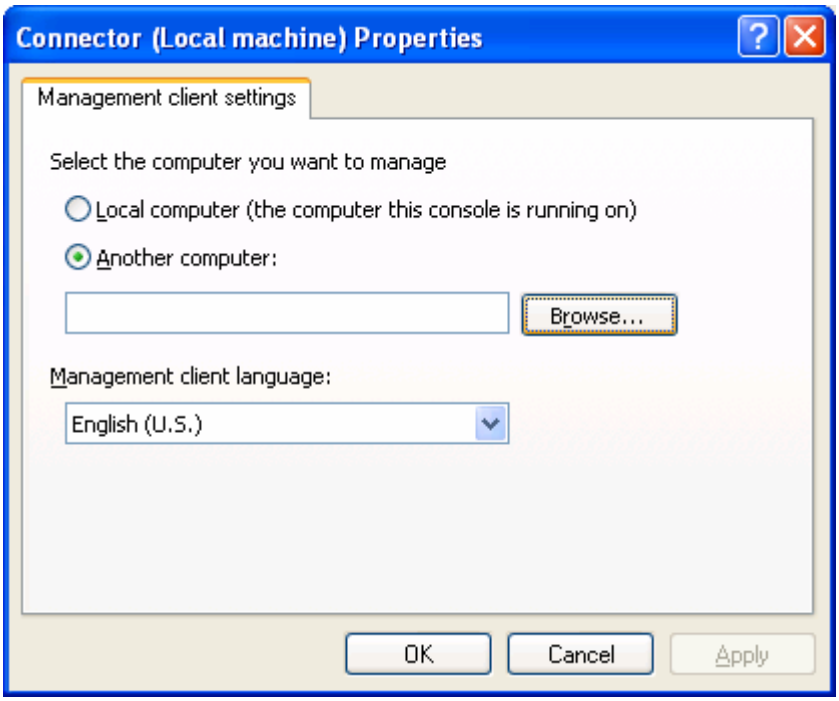


Figure 19. Connector Properties dialog

3. Click on **OK** and the Management Console connects to the Push Connector. Make sure you have given the user sufficient privileges as described in section 2.6, or the connection will fail.

3.3 Reloading Cached User List from Email Server

Push Connector loads the Global Address List from the Exchange Server to its cache which is used to add users and to perform remote recipient address search from Push Clients.

The cached list is reloaded daily but it can be reloaded manually also selecting the connector icon on to Management Console, clicking the right mouse button and selecting 'Reload user list from email server' action.

3.4 Reinstallation of Push Connector

Reinstalling Push Connector can be done using the same license file on condition that the Push Connector has been uninstalled. If the Push Connector has not been uninstalled (or if uninstallation failed to free the licenses on the service provider server), the service provider can reset the license manually on the Relay Server. Note that reinstalling means that all users are removed from the Push Connector.

If the Push Connector is not uninstalled, a new license file or license reset is required because the Authentication Key contained in the original license file is not valid anymore. Push Connector uses the Authentication Key in the License File only during the first connection to Relay Server and then Relay Server and the Push Connector negotiate a new Authentication Key that is used for all new connections. So, if you reinstall a connector with the same License Key, Relay Server detects that the connector is trying to perform challenge-response authentication with wrong key and rejects connection attempts.

When you request your Relay Server service provider to reset your connector license and provide a new one, the Relay Server and connector have the same key in use for authentication.

3.5 Connector Settings

Under Connector Settings you find a number of settings to control the operation of the Push Connector. There are three pages of settings: **General Settings**, **Watchdog Settings** and **Logging Settings**.

3.5.1 Connector Information

Click on the **Connector** item in the left hand side tree view to see information about the status of the Connector. The following information is available:

Service status	This shows if the server is running or if there is a problem.
Server version	This shows the build number of the Server.
Total number of users	This shows how many users have been added to the push connector.
Maximum users	This shows the maximum number of users in the license.

Connector extra information	This indicates any available troubleshooting information. There may be several issues indicated if there are many internal problems, so you may need to scroll to see them all.
Relay Server connection status	This shows if the Push Connector is connected to the Relay Server using a direct TCP connection.

3.5.2 General Settings

Click on **Connector Settings** and **General Settings** in the left hand side tree view to access the General Settings. The following settings are available:

System Language	Sets the default language of the system
Automatic recovery interval.	This setting controls how often the connector checks for users in error state and attempts to reset them in case they are in error state. The user may go to error state for instance when the email quota is exceeded.
Default synchronisation interval	This setting controls how often the Push Connector checks for new email. With the default setting of 5 seconds, there will be an average delay of 2.5 seconds before new email in the Exchange server is sent to the device.
Default synchronisation interval for over 50/100/200 users	You can set a different synchronisation interval as the number of users grows. Normally this would not be required in an Exchange environment.
User inactivity threshold	This setting controls after which period of client inactivity the Push Connector stops forwarding emails to the Relay Server for the user. The default is 60 minutes.
Docking address (connector IP)	This setting tells where Pocket PC devices should dock when docked into cradle. This should be the IP of the Push Connector inside the corporate LAN.
Primary mail server	This is the mail server address.
Relay server e-mail address	This setting is the email address of the Relay Server. Normally this is automatically filled in during installation and does not need to be changed.
Relay server IP address	This setting is the IP address of the Relay Server. Normally this is automatically filled in during installation and does not need to be changed.
Relay server port	This setting is the port through which the Push Connector communicates to the Relay Server using direct TCP connection.

3.5.3 Watchdog Settings

The watchdog is a monitoring process that monitors the status of and restarts the Push Connector if necessary. Click on **Connector Settings** and **Watchdog Settings** in the left hand side tree view to access the General Settings. The **Watchdog** is a service which checks to see that the Push Connector is running. If the Push Connector causes an exception, the watchdog can restart it. The following settings are available under Watchdog Settings:

Time to keep service on hold after exception limit has been	The time the watchdog waits before restarting the server after too many instant exceptions.

exceeded	
Running time after which an exception is not an instant exception	If the server halts due to an exception before it has been alive for the time defined by this setting, the exception is registered as an instant exception. Zero value means no instant exception counting.
Maximum number of consecutive instant exceptions before putting service on hold	This setting specifies the maximum amount of consecutive instant exceptions before a recovery wait is performed.
Maximum service memory usage	This setting specifies how much memory the Push connector service can use. If the limit is exceeded the server is restarted.
Ping interval	This specifies how often the watchdog pings the Push Connector.
Maximum time to wait for ping response	This setting specifies the time within which the server must respond to the ping request. The server will be restarted if this time limit is exceeded. Zero value means no pinging.
Maximum number of consecutive ping failures	When the number of consecutive timed out pings reaches this value the server is shut down forcefully.
Maximum time to wait for the service to stop gracefully	The time in which the server must exit as a response to the stop message from the watchdog. The server will be shut down forcefully if this time limit is exceeded.
Maximum running time for the service	If this time limit is exceeded the server is restarted. Zero value indicates no limit.
Preferred hour of day to restart the service	The default value -1 specifies to reset at any time.

3.5.4 Logging Settings

The Push Connector writes a number of logs while operating. The following settings are available under Logging Settings:

Log level	This setting defines which events are written into the log file. The finer the log level the larger the number of events that are written. A fine log level leads to log files of significant size, consumes resources and slows down program operation because writing to the hard disk takes time. For this reason it is recommended to use the fine levels only when investigating problems. The following values are selectable: • Fatal errors – events which stop the program from functioning or a permanent loss of data. • Errors – events that may cause a loss of service • Warnings - events that affect the user but do not cause any loss of service • Information - events that are useful for an administrator or support person to know but is not a warning or an error • Data dump – events that may be useful to an administrator and definitely useful to ”TELIA MOBIL MAIL” Support: Data dump, UT packets, PEC data, MAPI/Notes • Debugging messages - events that are typically only useful to a developer • Fine debug – finer granularity developer events • Tick debug – This is the finest level of logging.
Log directory	Allows you to specify the directory (folder) for saving the Push Connector logs.

3.6 Push Connector Logs

Log files are useful for troubleshooting and monitoring how the connector is operating. The log files should always be sent as part of support requests if there are problems with the Push Connector service. You can also follow up the operations the push connector users perform.

The log files are by default located in the \logs subfolder on the Push Connector computer. In order to view them remotely from a Management Console they must first be downloaded by selecting the **Connector** in the tree view and selecting **Download logs** from the **Action** menu. The logs are saved as compressed files in '.zip' format.

3.6.1 Used Log Files and their Location

Push Connector uses the following log files:

- **EnterpriseServerLog.txt**: this is the main log written by the Push Connector service. Push Connector writes its events and errors in this log file.
- **WatchdogLog.txt**: this log is written by a special monitor process that monitors the performance of the Push Connector and restarts Push Connector if necessary. Automatic restarts and recoveries are reported into this file.
- **GalProviderServer.txt**: this is the log file for the Global Address List Provider. This process is for keeping the address list up-to-date. By default, the address list is updated once every 24 hours.
- **ManagementServerLog.txt**: this log contains management server events, such as user activities and debugging information.
- **ManagementServerLog audit.txt**: this log contains audit information such as user logins. The following events are logged: Login, Login failure, Logout, AddUser, ActivateUser, ActivateUserEmail, ClearError, ResetUser, ClearDevice, RemoveUser, StopConnector, StartConnector, UpdateProperty

These log files are all written in the working directory of the Push Connector, which is normally under C:\Program Files\"TELIA MOBIL MAIL"\Always-On Mail Push Connector.

Management Console uses the following log file:

- **ManagementClientLog.txt**: this log is written by the Management Console. The activities and errors of the Management Console are written into this file.

3.6.2 Archival of Log Files

Each log file is archived every time the Push Connector service restarts. The log files written before the restart are archived by adding the date and time to the filename 'EnterpriseServerLog [2005-12-31 18.42].zip' to them. Note that the timestamp comes from the time when the file was backed up (i.e. when the server started up again), not from the last line written to the file. At start up log files with a timestamp older than 15 days are deleted.

3.6.3 Archival of Logs Files if Push Connector Fails To Respond

In the event of an unexpected Push Connector exception, its main log file EnterpriseServerLog.txt log is archived automatically for troubleshooting with timestamp information in the file name.

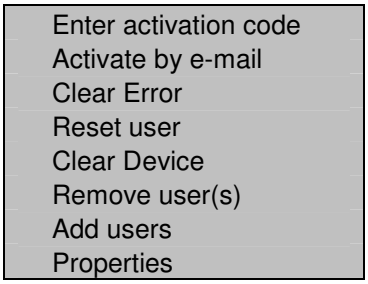
As an example, if the Push Connector causes an exception on November 12, 2005 at 16.12 PM, the log file written by that is automatically copied and named as 'EnterpriseServerLog [2005-11-12 16.12] wd.zip'.

Thus, it is easy to collect the log files containing activities before each exception situation just by collecting the log files with similar timestamp in the file name.

3.7 User Administration

This section describes the user actions that can be performed with the Push Connector.

The following actions are available in the **Action** menu:



3.7.1 Adding a user

Push Connector adds users from a cached user list (Global Address List) which is loaded from Exchange Server. If you have added new users to the server but they are not visible in the cached user list, reload the user list from server.

The same cached user list is used also to search recipient addresses for emails as a remote search from clients.

To add a user, do the following:

1. Select the **Users** item in the left hand pane.
2. Select the **Add users** from the **Action** menu.
3. Select the user(s) from the Global Address list and click **OK**. Repeat the procedure for all users you wish to add.

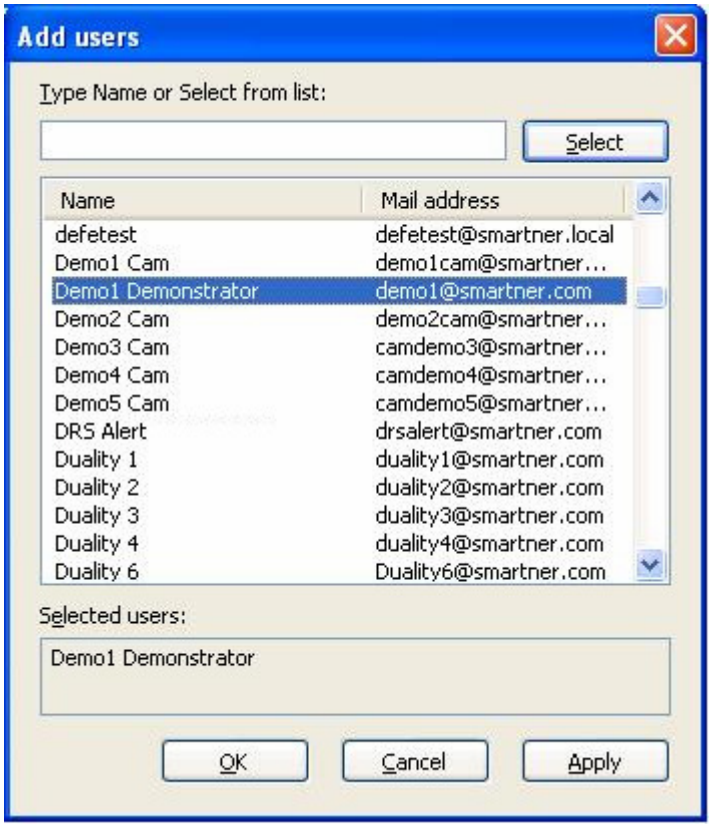


Figure 20. Add users

When you press **OK** the status of the operation will be shown in the Management Console window. It should go from 'Adding User to relay server' to 'Adding user' to 'Ready to install'.

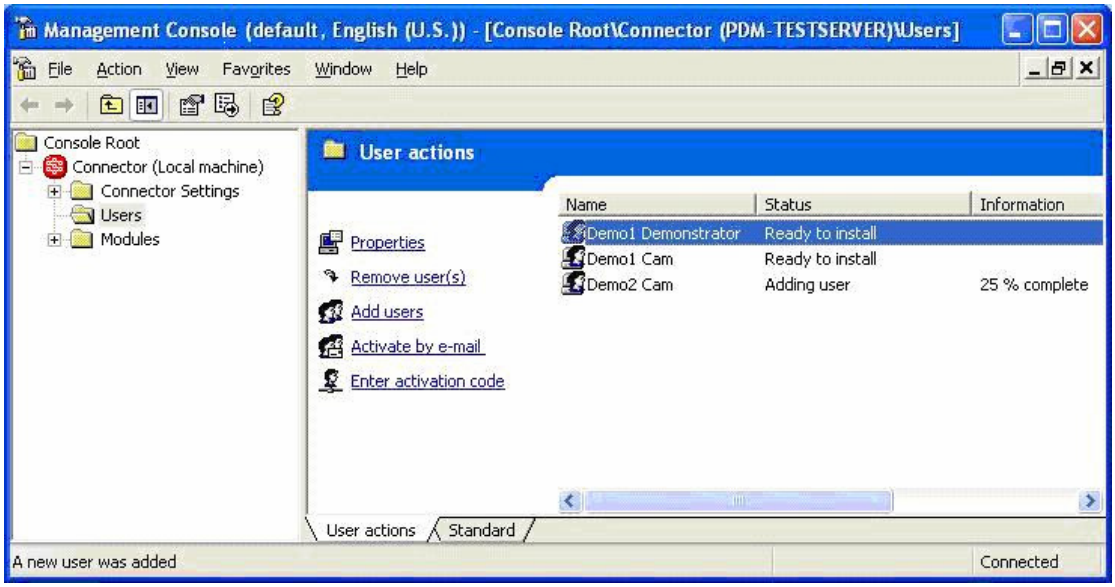


Figure 21. Users in Management Console

NOTE!
If a user has a large amount of email in their Outlook Inbox and Calendar events, the state may remain as **Adding User** for several minutes until the Push Connector has finished processing the existing email. The time that the state remains as **Adding User** will depend on the size of the user's Inbox. You must not install the user's Push Client until that user's state has changed to **Ready to Install**.

4. The user or users have now been added to the Push Connector. The user's state will remain as **Ready to Install** until the Push Client is installed to their mobile device. Installing and activating the client on a mobile device is explained in chapter 4.

5. When the Push Client has been installed and activated, the user's state will change to **Enabled**.

3.7.2 Clearing an error state

The **Clear error** action lets you reset the error state of a user. An error state might occur for instance when a user exceeds their mailbox size limit. Errors are also automatically cleared at a set interval by the server.

3.7.3 Resetting users

The **Reset user(s)** action allows you to reset the user defaults, such as they are when the user is added to the server. This feature should be used for instance when re-installing the mobile client software for an existing user. Resetting a user changes a user's state to **Ready to Install**.

To reset a user, do the following:

1. Select the user or users that you wish to reset.
2. Select **Reset User** from the **Action** menu.
3. Re-install the client to the device.

3.7.4 Clearing a device

The **Clear device** is an action to be used when the device has been lost or stolen to minimise the security risk. This action deletes all the data that has been synchronised to the device such as emails, calendar entries and contacts. This action also deletes the encryption key from the device.

NOTE!
Using the **Clear device** action deletes all synchronised data including emails, calendar entries and contacts from the device as well as the encryption key. After performing this action, the client software needs to be reinstalled for the service to continue.

Steps to clear a device:

1. Select the user or users for whom the device should be cleared.
2. Select **Clear Device** from the **Action** menu, and click **OK** to confirm.

The Push connector will then send out a protocol signal to command the push client to clear device data.

3.7.5 Locking a Device

Remote locking is currently available only for devices using Symbian S80 client software, such as Nokia 9300 and Nokia 9500. If a user is using Symbian S80 type of push client, then the Push Connector shows **Lock Device** option in the action list. When the device is locked remotely the user can not use the device at all before a pre-defined lock code is entered.

Locking of device from Push Connector requires that user has set the lock code in his device. This is done in Device security settings (Control Panel => Security => Device security) changing the 'Lock code' value for the device.

Assuming that user has set the lock code of the device, then the device can be locked remotely as follows:

1. Select the user whose device should be locked
2. Select **Lock Device** from the **Action** menu, and click **OK** to confirm

The Push connector will then send out a protocol signal to command the push client to lock the device. Device will be locked immediately when the message arrives to the device.

3.7.6 Removing a user

The **Remove user** action allows you to permanently remove a user from the service(s).

To remove a user, do the following:

1. Select the user or users that you wish to remove.
2. Select **Remove User** from the **Action** menu, and click **OK** to confirm.
3. The user has now been permanently removed from the Push Connector.

3.7.7 Viewing and editing user properties

The **Properties** contain a number of basic read-only and editable settings for the user. Multiple users can be edited at a time. The properties dialog is opened by selecting the user and selecting **Properties** on the **Action** menu. The following settings are available:

General

- **Display name**. This is the name of the user shown in Push Connector user list.
- **Mail address**. This field shows the user's email address.
- **Client ID**. This is a unique identifier by which the Relay Server identifies the client. It is used for support purposes.

- **Device Type**. This is an informational field which shows the type of mobile device being used. The field is automatically filled.
- **Client version**. This field shows the SW version on the mobile device.
- **User language**. Select one of the languages to be used as default for Push Connector generated strings.

Statistics

- **Data last received**. This shows when the Push Connector has last received data (email, calendar or contact data) from the client.
- **Data received this month**. Shows how much data has been received by the Push Connector from the device during this month.
- **Data received last month**. Shows how much data has been received by the Push Connector from the device during last month.
- **Data last sent**. Shows when data has last been sent to the device.
- **Data sent this month**. This field shows how much data has been sent to the device during this month.
- **Data sent last month**. This field shows how much data has been sent to the device during the previous month.

Services

- On the **Services** tab you can select whether **Calendar** and **Contacts** should be synchronised. **Email** is always on.

Email

- On the **Email** tab, the **Truncate messages larger than** means the size limit at which emails will be cut when sent to the device. It is set to 10k by default. This means that emails larger than 10k will appear truncated on the device, and the user will need to request the rest of the email before it is downloaded.
- The **Don't synchronize mails older than** sets a limit for when emails are propagated to the device. If you select e.g. 2 days, it means mails from the current date and one day in the past are handled (mails from 'today' and 'yesterday'). The Push Connector does not forward emails older than this to the device, so if the device is off for 3 days, the mails from the first day will not be forwarded when the device is turned back on.
  Note that there is a related setting on the device called 'Days to store emails'. The device setting controls how old emails are deleted from the device to save memory.

3.7.8 Changing User's Mobile Device

When a user wants to change their mobile device and start using the "Telia Mobil Mail" service on the new device, the user account in the Push Connector needs to be reset and activated again with an activation code from the new client installation. A new activation code is required to minimize the risk of possible denial of service attacks and enforce strong security practices.

Please, read chapter 3.7.3 for instructions to reset a user account.

3.8 Changing the Content of Automatic Email Messages Sent to End-users

The Push Connector sends preformatted emails directly to end-users in certain situations. The content of these email messages can be changed easily in order to inform the users about what to do in a specific situations.

Preformatted email messages are stored in RTF format in the Templates directory of the Push Connector (\Program Files\”TELIA MOBIL MAIL”\Push Connector\Templates). The content of the emails can be easily updated by editing these files with a normal document editor supporting RTF format.

The predefined automatic email files are:

- Welcome.rtf: this message is sent to each end-user after successful service activation.
- Activation.rtf: this message is sent to an end-user if the connector is ordered to ask for the client activation code from the end-user via email.
- ActivationBadCode.rtf: this message is sent to end-users who respond to activation message with an invalid activation code.
- ActivationFailed.rtf: this message is sent to end-user whose client activation via email has failed.

3.9 Creating and Restoring a Backup of User Accounts

Push Connector stores the user account information in the Windows Registry and partially also in the Push Connector Maps directory.

A backup of the data on the Push Connector is done by copying all user and server specific data. The user account information from the Windows Registry also needs to be exported. Note that when the accounts are restored, any emails pushed after the backup are pushed to the device again. These instructions can be used to extract user accounts from an existing connector.

Backup users from the Push Connector:

1. Log on to the Push Connector machine containing the user accounts with the Push Connector Windows user account
2. Stop the Push Connector services
3. Export windows registry branch '\HKEY_CURRENT_USER\Software\”TELIA MOBIL MAIL”\Always-On Mail Push\' to a file using Windows Regedit application.
4. Copy the user account files from the Push Connector \Maps directory to your backup location. The Maps directory is Program Files\”TELIA MOBIL MAIL”\Always-On Mail Push connector\Maps.

Restore user accounts to Push Connector:

1. Log on to the Push Connector using the Windows account used for the service
2. Stop the Push Connector services if running
3. Import the windows registry files (.reg) back to the location '\HKEY_CURRENT_USER\Software\”TELIA MOBIL MAIL”\Always-On Mail Push'
4. Copy the user account files from your backup location to the Push Connector \Maps directory. The Maps directory is Program Files\ ”TELIA MOBIL MAIL”\Always-On Mail Push connector\Maps.
5. Restart the Push Connector services

3.10 Moving a Push Connector to another Server

It is possible to move all the users on one Push Connector to another clean installation. This is useful for instance when you wish to upgrade to a more powerful computer.

To move a connector from server A to server B, please follow these steps:

1. Setup the new server (server B)

   - Log on to the server B using the same Windows domain account that is running the Push Connector service on server A
   - Install the connector with a test license, not with the production license that you have used before!
   - Stop the Push Connector services

2. Log on to the server A and stop Push Connector services

3. Backup users from server A (Push Connector stores the user account information in the Windows Registry and partially also in the Push Connector Maps directory):

   - Log on to the Push Connector machine containing the user accounts with the Push Connector Windows user account
   - Stop the Push Connector services
   - Export windows registry branch '\HKEY_CURRENT_USER\Software\"TELIA MOBIL MAIL"\Always-On Mail Push\' to a file using Windows Regedit application.
   - Copy the user account files from the Push Connector \Maps directory to your backup location. The Maps directory is Program Files\"TELIA MOBIL MAIL"\Always-On Mail Push connector\Maps or similar.

4. Disconnect server A from network

5. Change server B IP address to server A's IP address (necessary for Windows Mobile client docking functionality)

6. Restore users to server B:

   - Log on to the server B using the same Windows domain account that is running the Push Connector service on server A
   - Install the connector with a test license, not with the production license that you have used before!
   - Stop the Push Connector services
   - Import the windows registry files (.reg) back to the location '\HKEY_CURRENT_USER\Software\"TELIA MOBIL MAIL"\Always-On Mail Push\'
   - Copy the user account files from your backup location to the Push Connector \Maps directory. The Maps directory is Program Files\ "TELIA MOBIL MAIL"\Always-On Mail Push connector\Maps or similar.
   - Restart the Push Connector services

- If you get authentication failed errors after starting the new machine, please check that the following key is the same on both the old and the new machine:

\HKEY_CURRENT_USER\Software\ ”TELIA MOBIL MAIL”\Always-On Mail Push\Global\RelayServerKey

7. Uninstall connector from server A (make sure server A is not connected to network)

Please note that moving single or groups of users to another Push Connectors is not supported and may cause problems.

3.11 Increasing the Amount of Licences

Push Connector checks the available number of licenses from the Relay Server every time when a new user is added.

If you have activated the number of users allocated to your license, please contact your ”Telia Mobil Mail” reseller to purchase further licenses. License handling is on the Relay Server, no modifications to Push Connector are required to increase the amount.

4 Installing Push Clients

This chapter describes a step list for installing the ”Telia Mobil Mail” Push Clients. More information is available in the device specific user guides.

4.1 Installation Packages

”Telia Mobil Mail” Push Client for devices running the Windows Mobile operating system is delivered as a standard Windows installation (.CAB) file.

”Telia Mobil Mail” Push Client for devices running the Symbian OS is delivered as a standard Symbian installation (.SIS/.SISX) file.

”Telia Mobil Mail” Push Client for Java 2 Mobile Edition devices is delivered as standard JAD and JAR files.

4.2 Client Installation and Activation Process

Detailed step lists for installing the different clients are available in the User Guides for each mobile device type. At the end of the device installation process an Activation Code will be displayed. The Activation Code that should be sent as a response to the activation email or entered for this user in the Push Connector Manager.

To manually enter the user specific Activation Code to the Push Connector, do the following:

1. Select the user and select **Enter activation code** on the **Action** menu. The following screen will appear:

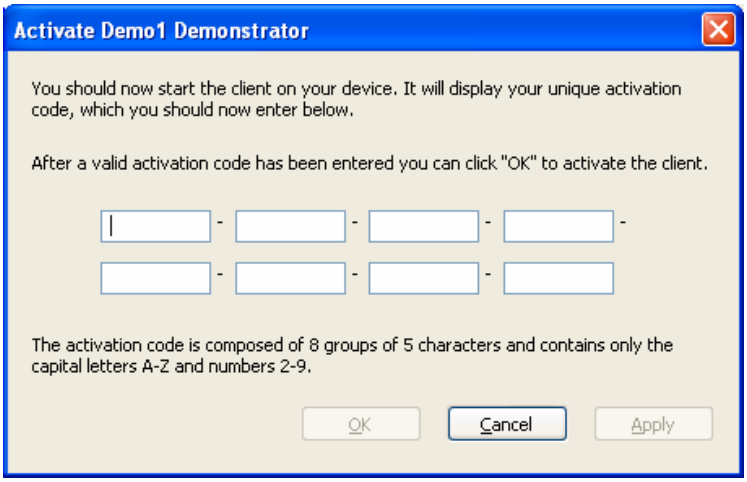


Figure 22. Activating user

2. Select “**I would like to activate by entering the activation code now**” and type in the Activation Code that is shown on the mobile device screen.

The **Activate by email** action allows you to send an activation email to a user. The email prompts the user to install the client (if not already done) and to reply to the message with the activation code. To request for the Activation Code directly from the user by email, do the following:

1. Select the user in the Push Connector Users view and select **Activate by email** from the **Actions** menu
2. A dialog will appear requesting the validity period during which the user must reply with the Activation Code in order for the Activation to be successful.

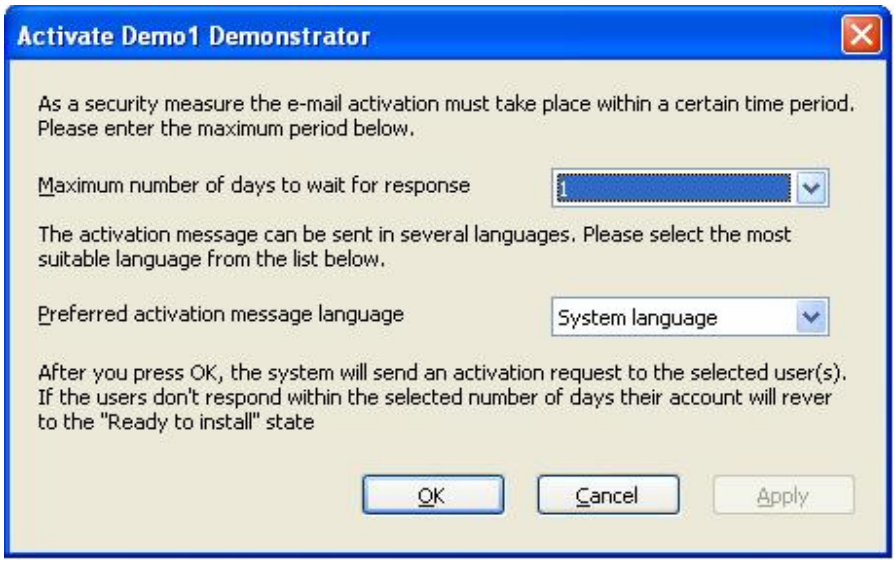


Figure 23. Email activation settings

3. Select the amount of time in days that the user has time to reply with the Activation Code and the preferred language and click **OK**.

The user will now receive an email requesting the Activation Code along with instructions on how to respond to it.

a. If the user responds within the set time with the valid Activation Code, the user state is automatically changed into **Started,** and they can immediately start using the service. The ”Telia Mobil Mail” user interface on the mobile device will no longer show the Activation Code. The current status of the application is shown instead.
b. If the user responds with an invalid Activation Code, a new email is sent to the user describing the error, and requesting the user to reply to the email with the correct Activation Code.

4.3 Cloning Mobile Device Installations

”Telia Mobil Mail” clients can be preinstalled on many devices by cloning one non-activated installation to many devices. In this way, the application is easier to distribute. So, the Push Client application is installed only to one device and then that device installation cloned to other devices using third party mobile device management tools.

It is important to clone the application in the right state. The client can not be fully activated and installed before cloning because then all the devices have the same user profile. The right cloning stage for Symbian and PocketPC clients is different:

- Symbian: Device cloning should be done right after the client installation program finishes. The Push Client application itself must not be started at all before copying the application to other devices.
- Windows Mobile: Device cloning should be done after you have run the client installation program until the License screen shows up. Choose not to accept the licence and then it is ready for cloning.

4.4 Upgrading from Previous Versions

This chapter describes how to perform an upgrade from a previous ”Telia Mobil Mail” installation.

4.4.1 Client Upgrade Compatibility

The table below describes how the upgrade can be done from earlier versions of ”Telia Mobil Mail”.

”Telia Mobil Mail” Version	Upgrade to ”Telia Mobil Mail” Enterprise Edition 5.2
V 5.0	The new version can be upgraded on top of the existing installation. Existing 5.0 clients will work, but clients should be upgraded to 5.2 to benefit from the new features. It is recommended to activate only 5.2 clients to the Push Connector.
V 4.0	The new version can be upgraded on top of the existing installation. Existing 4.0 clients will work, but clients should be upgraded to 5.0 to benefit from the new features. All new clients activated to the push Connector must be newer clients. Push Connector does not accept activation codes from 4.0 or older clients. **NOTE!** Clients and connectors are upgradeable only using the same branding (product name). If you have version 4.0 client with brand X and 5.0 with brand Y then you can not upgrade directly and will need to reinstall.

4.4.2 Upgrading the ”Telia Mobil Mail” Push Client

The client upgrade process will differ slightly depending on the used mobile device. Please follow the instructions below to upgrade the client software.

The recommended option to deliver the clients are to either download them from a web site, or by sending the new client installation as an email attachment. For details, please see the client user guides.

4.4.2.1 Upgrading Push Client on Symbian Devices

Symbian clients can be upgraded by running the .SIS./SISX installation file on the phone. It will automatically update all necessary files while keeping existing settings.

4.4.2.2 Upgrading the Windows Mobile client

Windows Mobile / Pocket PC client can be upgraded by running the new .CAB installation file on the phone. It will automatically update all necessary files while keeping existing settings.

4.4.3 Uninstalling the client

Please check the device specific documentation for uninstall instructions.

5 Troubleshooting

This chapter describes basic troubleshooting instructions in some typical problem cases.

5.1 General Problem Situations

The following subchapters provide information about common problem situations and how to resolve them.

5.1.1 Relay Server connection status is 'Not connected' in the Push Connector

This means that Push Connector is using direct TCP connectivity to Relay Server, but currently the connection is not available.

Typically, the reason is that the connector has been disabled from Relay Server or there is a temporary outage in the network, or the firewalls are blocking the connection.

Resolution:

1. Restart the Push Connector and check the connection status again to see if this recovered the connection. If not, continue to perform the checks listed below.
2. Check the used Relay Server IP address and port from general settings (3.5.2)
3. Login to Push Connector machine (machine where the actual Push Connector service is running) and open Windows command prompt (Run… => cmd).
4. Try to open a telnet connection from connector machine to the Relay Server connector port with following command: *telnet <relay server IP> <port>*
    a. If the telnet connection is established the telnet shows an empty screen for a while, this means that the connectivity to the Relay Server is in place. If the connector is still not able to establish a connection, then the Relay Server is not accepting connection from your connector and you must contact your Relay Server service provider.
    b. If connection is not possible then there is a network problem or firewalls blocking the traffic from Push Connector to this port at Relay Server. You must check the network configurations in the LAN and possible firewalls in between.

5.1.2 User account stays in 'Adding User to relay server' state in the Push Connector

This state means that Push Connector is communicating with Relay Server in order to check the license quota for the company and to get unique device ID and Relay Server authentication information for the new user.

Normally 'Adding user to relay server' should take only a few seconds to complete, but if it stays in this state for many minutes then there is most probably a connection problem to Relay Server.

Resolution:

1. Check the 'Relay Server connection status' from Push Connector Management Console (see chapter 3.5.1).
    a. If it says 'Connected', the connection is OK
    b. If it says 'Not connected' then you need to verify TCP connection to Relay Server (see chapter 2.4.1).
2. After you have fixed the connectivity to Relay Server, restart the connector so that it tries to resend the request to Relay Server again.
3. If the user account goes to 'Ready to install' state in a minute then the issue is resolved. If not, then the connectivity to Relay Server is not corrected yet and you must continue troubleshooting the connection.

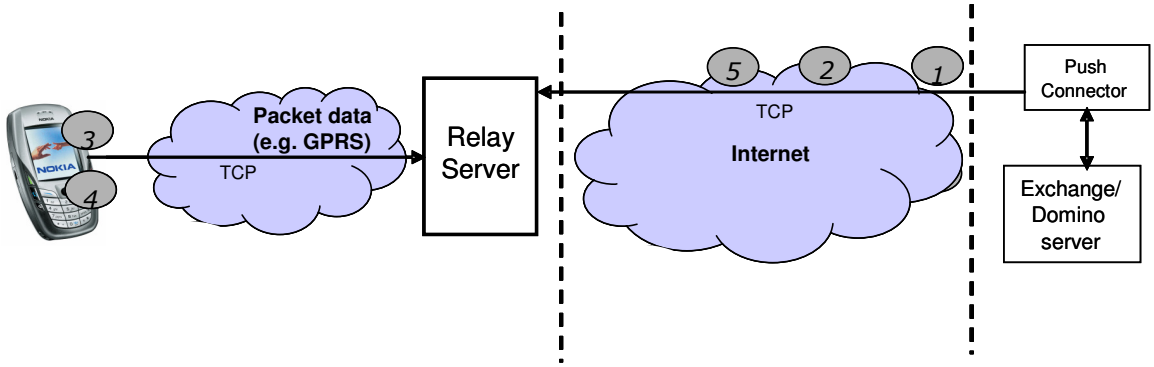
5.1.3 User account stays in 'Installing' state in the Push Connector

Sometimes, after activating a new user account in the Push Connector, the user account stays in 'Installing' status for a long time. This user status means that the connector has sent a Provisioning Message to the Push Client and waits for a Provisioning Response Message from the client. Connector goes to 'Started' state only after it has received the Provisioning Response message back from the client.

Possible reasons for staying long in "Installing" status are:

1. Push Connector is not connected to Relay Server and can not send the Provisioning Message to Relay Server immediately.
2. Provisioning Message is on its way to Relay Server. So, Relay Server has not received the message and can not push it to the Push Client.
3. The client is not connected to Relay Server (check that it shows the Activation Code on its screen). So, the Relay Server is not able to Push the message to the client.
4. The client is connected, but to a wrong Relay Server instance. So, the correct Relay Server instance can not push the message to the client.
5. The client has received the Provisioning Message but Provisioning Response is still on its way to Push Connector. So, everything is OK on the client side, but the connector does not know it, yet.

The picture below illustrates these problem areas.



5.1.4 Delays in Message Delivery

If the service works well and the Push Client and the Push Connector are directly connected via TCP to the Relay Server, the messages from client to connector should go in seconds.

The table below presents the most common reasons and resolutions for delay problem.

Reason	Resolution
Push connector has internal errors or problems with connectivity to Email server and thus is not able to provide messages as fast as it should.	Check that the end-user account is not in 'Error' state in the push connector. (resolving Errors state is described in other chapter) Check that the network to email server is fast enough (see system requirements) and see the log file for possible errors. Restart the connector to recover from errors caused by the native email server protocol.
The Push Client or the Push Connector has lost its connection to Relay Server.	Pause and resume the client to verify that it is able to connect to Relay Server. If not, then it is a network problem or the user has been disabled from the service on the Relay Server side. Check the Relay Server connection status from the Push Connector management console. If it is not connected there may be a firewall blocking the connection. Restart Push Connector to verify that it can connect.
There is a big queue of messages for the user or for the connector on the Relay Server side.	This is possible if the client or connector has been disconnected from the Relay Server for a long time. This solution will resolve itself as Relay Server processes the message queue soon after the connection is available again.

5.1.5 Characters not shown correctly in the messages

This usually means that the default language for non-unicode characters is not set at all or not set correctly. In this case, characters are usually shown as question '?' marks in the text.

See chapter 2.3.1 for more information.

5.1.6 User Accounts going into Error state in Push Connector

User accounts listed in Push Connector may go into Error state for many reasons. The table below presents the most common reasons and resolution.

Reason	Resolution

User's mailbox session has internal problems.	The most typical reason is that the connection to user's mailbox may get stuck due to network errors between the Push Connector and the email server. Push Connector tries to recover these errors automatically, but if it can't recover automatically, restart the connector. Check also the network quality to the email server (see system requirements)
Permissions to read mailboxes are changed so that connector is not able to access user's mailbox anymore	Access rights may be changed by someone else, which may cause this kind of problems. To resolve this issue check the mailbox access rights for the user mailbox which is in Error state.
The quota of the user's mailbox has been exceeded	If user's mailbox quota is exceeded it usually causes an error in the Push Connector. This is resolved by archiving or deleting items from the end-users mailbox in the email server.
Invalid message in user's mailbox	This means that the user has some item in the mailbox which is has a special format which the Push Connector is not able to interpret without errors. Sometimes special message formats may cause an error state in Push Connector. The item causing this problem may be identified by looking the Push Connector log file but also looking user's mailbox directly and trying to identify special looking emails or other items. Suspected items can be moved to folders which are not monitored by the Push Connector to resolve this case.

5.1.7 Push Connector stops working after the password for the connector user account (privileged user) is changed

If the password for Push Connector user (privileged user) is changed then the password must be changed to all the Windows services that run as a part of the Push Connector.

To resolve this situation open 'Services' list from the Control Panel of the Push Connector machine and reset the new password to all Push Connector services found in the list. Then restart the services.

5.1.8 Management Console opens empty after Push Connector installation

This may happen if you have many user accounts in the system having similar name as the privileged user account created for the connector.

Check EnterpriseServerLog.txt and GalProviderServerLog.txt files for the mention of error 80040700. This error happens if there are usernames which begin with the same characters. E.g. if you are attempting to use 'privuser' and Exchange already has 'privuser2' and 'privuser3' defined.

To resolve this issue use another username for the connector user account.

5.1.9 Management Console is not Starting

Push Connector authenticates all Management Console users against the Active Directory using connection to domain controller. If this connection is not available then the Management Console can not be used unless the authentication is disabled.

To resolve this issue connectivity from the Push Connector machine to the domain controller should be checked and resolved.

If this can not be done, the authentication can be disabled from the Push Connector by disabling Kerberos authentication from the registry settings of the Push connector machine. This is done by setting /Global/Management/Security Provider Configuration/127.0.0.1/Authentication value empty.

5.1.10 Uninstalling Push Connector leaves old settings in the Registry

This may happen if uninstallation is done with different user account that was used to install the push connector.

Make sure you are logged in with the same user with which you installed the push connector when uninstalling.

Old settings can also be removed from the registry manually under the current user's registry settings.

5.1.11 Server Information in the License key do not match

The Push Connector performs a DNS lookup for the Relay Server host name when installing the Push Connector and compares the resolved IP address to the IP address used in the Push Connector.

This causes problems if the DNS used at the Push Connector returns different IP address than the Relay Server's public IP address.

To resolve this, check the Relay Server IP address host name in the Push Connector license file and perform nslookup command on the push connector machine. If the returned IP address is different than the one in License File, change DNS registry or make the correct DNS mapping in local host file.

5.2 Generic Check Procedures for a Push Connector Installation

The following table show general checks that verify if the connector is installed correctly.

What to Check? Problem area.	How to Check?	What to do if check not passed?

Windows account running the Push Connector	Logon to the connector machine using the connector user windows account. Check that the ”TELIA MOBIL MAIL” Push Connector Access Manager and Management Console Programs are available the start menu and that the user account running the Push Connector service is the one you used to logon to the connector machine (Check by pressing CTRL + ALT + Delete and see the logon information).	Logon with a different windows user account. Most probably the connector was not installed using the windows account you are using. If the correct account cannot be used, reinstall the connector and be sure to use the privileged user account during the installation.
Check that the Push Connector is running	Open Windows Services and check that the ”TELIA MOBIL MAIL” Push Connector service is ‘Started’. Try to restart the service and check that it restarts without errors.	Start connector service. If you get a logon permission failure, reset logon username and password to the service and try starting again.
Outlook installation and default connector mailbox	Stop the Push Connector Service. Open the Outlook client on the connector machine. Check that it opens directly to the connector mailbox using Outlook profile name ‘Outlook’ (or ‘MS Exchange Settings’ in Exchange 2000). Check that the Outlook version is correct by opening About window and checking the requirements from the installation guide.	Configure the connector mailbox as the default mailbox for the Outlook with profile name ‘Outlook’. If it does not help, re-install Outlook (check that it is the correct version).
Check connector access to other user’s mailboxes	Open the Outlook client and try to open some end-user’s mailbox by selecting File>Open… >Other User’s folder. Then select inbox folder and Open. If you cannot open the inbox, the connector user does not have correct access rights.	Configure active directory settings as instructed in the installation guide.
Check that the Push Connector Manager’s operating system is correct version	Open Control Panel>System>General and check that the operating system is the same as required in the installation guide.	Install the correct version of the operating system.
Check that the connector machine has fixed IP address	Check this from the computer’s network settings in Control Panel.	Reconfigure TCP/IP networking settings.
Check that the connector machine has sufficient resources	Check system information and ask the IT administrators what the machine specs are. Check that they correspond to the requirements set in the installation guide.	Upgrade the system as required.

Check that network connection to Exchange server is good and reliable	Get the network configurations from the network administrators. Check that the connector is in the same LAN (> 10 Mbps) with Exchange server and that the Exchange is not far away geographically. Check that there are no packet losses (ping) in between connector machine and the Exchange. Check that ping round trip time is less than 10ms to the server.	Move the connector machine closer to the Exchange in the network.
Language setting for non-unicode programs	Check that language setting for non-unicode programs is set correctly opening Control Panel => Regional and Language Settings => Advanced	Select the language that is used in this service.

5.3 Exchange Environment Specific Error Situations

5.3.1 Upgrading from Exchange 2000 to 2003 causes MAPI errors in user accounts

The default active directory security settings change from Exchange 2000 to Exchange 2003.

Check Active Directory privileges for the Service Account (privileged user). The original privileges may have been changed when upgrading Exchange.

For more information, see end of chapter 2.3.2, which describes setting access rights to the connector user account.

5.4 Troubleshooting Push Clients

Please, see the End-user Guide document for instructions to troubleshoot operations in Push Clients.

6 Additional Support and FAQs

6.1 Frequently asked questions

Q. When I add a new user to the Push Connector the user's status does not change to "Started".
A. A possible reason for this is that the "Telia Mobil Mail" Client on the mobile device is not running, or the mobile device is out of packet data coverage. Also, if the activation email is not in ASCII ('Plain text only') format, the provisioning email may be rejected.

Q. Why do emails not always arrive to my mobile device immediately when they come to my corporate mailbox even though the client is up and running without showing any warnings?
A. There are usually two reasons that occasionally may cause delays in the service. 1. The email routing from your corporate email server to "TELIA MOBIL MAIL" Relay Server has delays. This is typical for email routing systems especially when there is a lot of email traffic in the network. 2. Your mobile device has gone out of packet data coverage temporarily and the "Telia Mobil Mail" Client has not yet recovered it automatically.

Q. During Installation of "Telia Mobil Mail" Push Connector I get an error saying, "Please check that the MAPI profile you specified is correct."
A. Please make sure that the MAPI profile name on your Exchange setup is 'Outlook' (or 'MS Exchange Settings' in Exchange 2000). If it is something else, please rename it to 'Outlook' to overcome the problem.

Q. I'm trying to verify that user permissions for the privileged user account have been set up correctly. When I try to open user's Inbox as the privileged user by using Outlook on the Push Connector computer I get an error saying "Unable to open the folder. Cannot find the folder Inbox". What's wrong?
A. The privileged user has not been granted sufficient rights to access other users mailboxes. Please refer to installation chapters for instructions how this can be done.

Q. User's status in the "Telia Mobil Mail" Push Connector is in Warning state, what does it mean?
A. The service is working normally, typically the reason for warning is that some items could not be read from the Exchange or user's quota is exceeded. The service will automatically recover from these incidents once the initial reason is resolved.

Q. When I use the Management Console in another language than English, I still get some error messages in English. Is this normal?
A. Error messages derived from host system error messages are displayed in English.

Q. Why do the emails not disappear immediately from the outbox of mobile device even if the "Telia Mobil Mail" client is connected and running well?
A. Emails disappear from the outbox after the mail has been delivered to the Push Connector and it has informed the Relay Server about this. Thus, the delays of email routing between the Relay Server and the corporate email server may cause the emails to stay in the outbox for a long time.

Q. I'm using MS Exchange 2003 server and adding users causes some users to go into error state.
A. This is known problem in Microsoft Exchange 2003 and MAPI connections prior to the latest patches. Please, see chapter 2.2 and upgrade to the specified version.

6.2 Additional support

If you are experiencing problems with ”Telia Mobil Mail”, please contact your ”TELIA MOBIL MAIL” reseller for additional support.

When submitting a support request, please include the following information in the request to enable us to help you faster:

- Your name
- Company name
- Reseller/operator name (if applicable)
- Privileged user email address
- Environment information
    - Exchange/Domino server version
    - Outlook/Notes version used on the connector server
    - ”Telia Mobil Mail” edition and version
    - Mobile device type and version
    - Affected user(s) email address(es)
- Description of the problem
    - Is this a new or existing installation?
    - What happened (detailed steps)?
    - What did you expect to happen?
    - When did the problem occur?
    - Email, appointment subject where the problem occurred
    - How to reproduce the problem?
    - What works?

Please include also log files from the connector and clients if possible:

Push Connector	See section 3.6 for information about the Push Connector log file locations.
Windows phones	Windows phones have the log file(s) in the root directory: ExmController.txt
Symbian phones	The Duality.log.txt can be seen by viewing the settings in your phone's Duality client or selecting Menu>Tools. Choose View log. You can view, copy, read, save or beam the log to another machine.