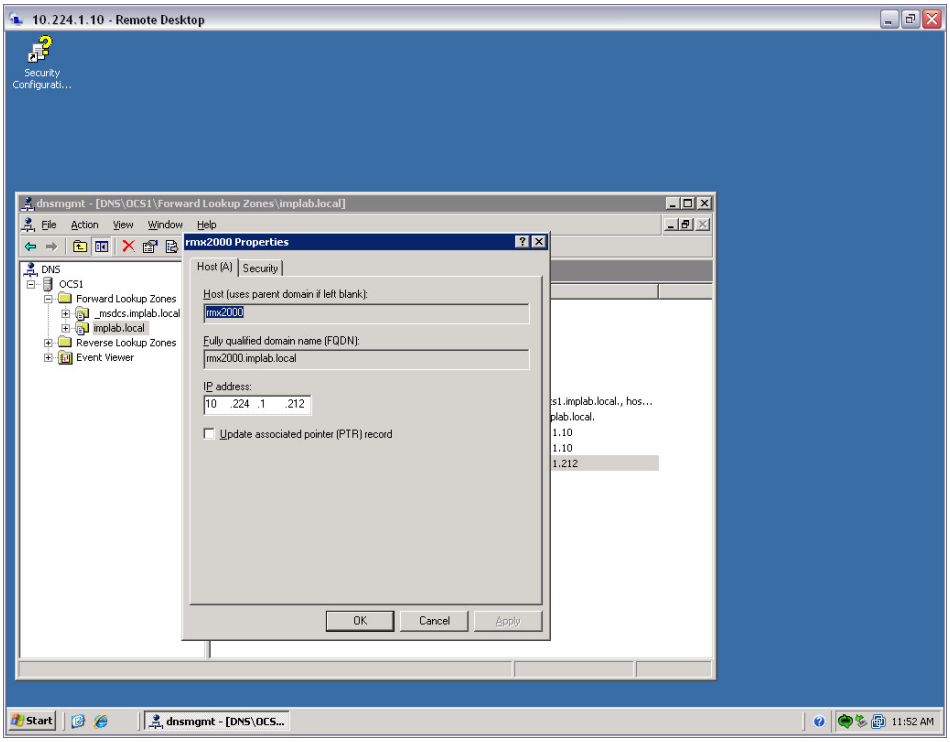
RMX Setup with OCS

Items needed :

1.) FQDN for the RMX

FQDN for RMX Signaling Host	

2.) DNS A record to resolve FQDN to the Signalling IP of the RMX



3.) List of DNS servers to enter into RMX

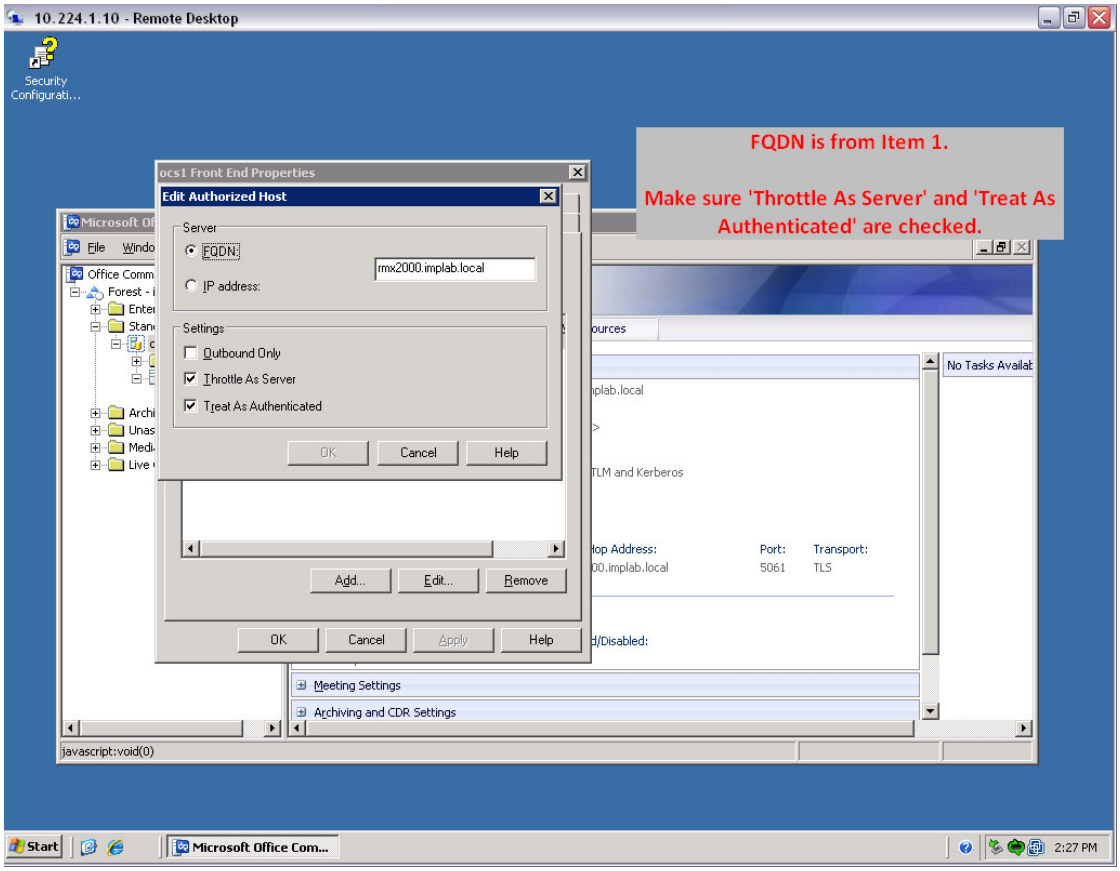
Primary DNS Server	
Secondary DNS Server	
Tertiary DNS Server	

4.) Certificate created for the RMX with the FQDN as the Subject line. This should be a Microsoft .pfx file or the rootca.pem, cert.pem, privkey.pem also the password that was used to export cert put in a file named 'certPassword.txt' case sensitive filename

See APPENDIX A.

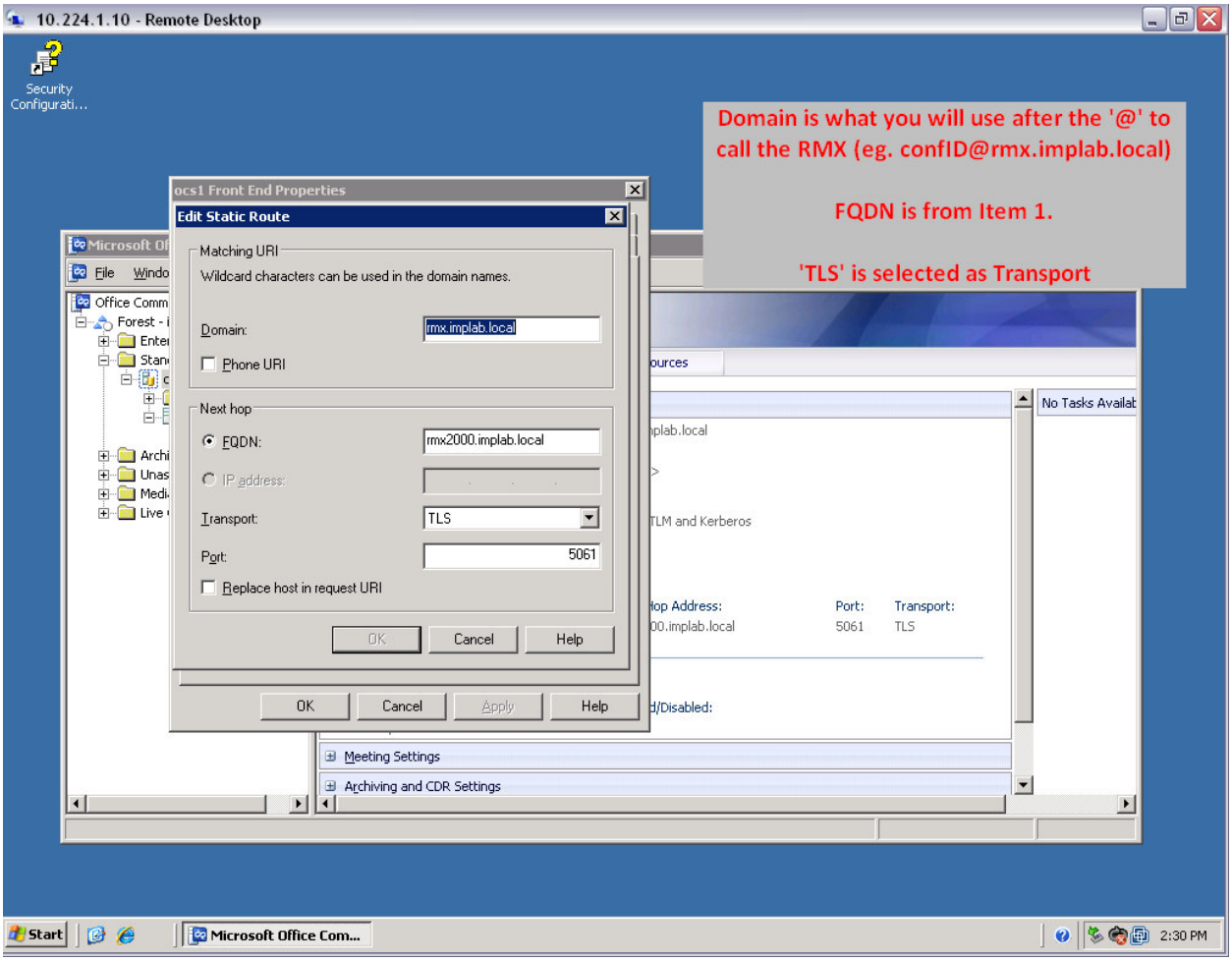
5.) Host Authorization setup in the OCS server for the RMX.

Right click the Front End pool and Select ‘Properties’ then ‘Front End Properties’, Host Authorization tab.

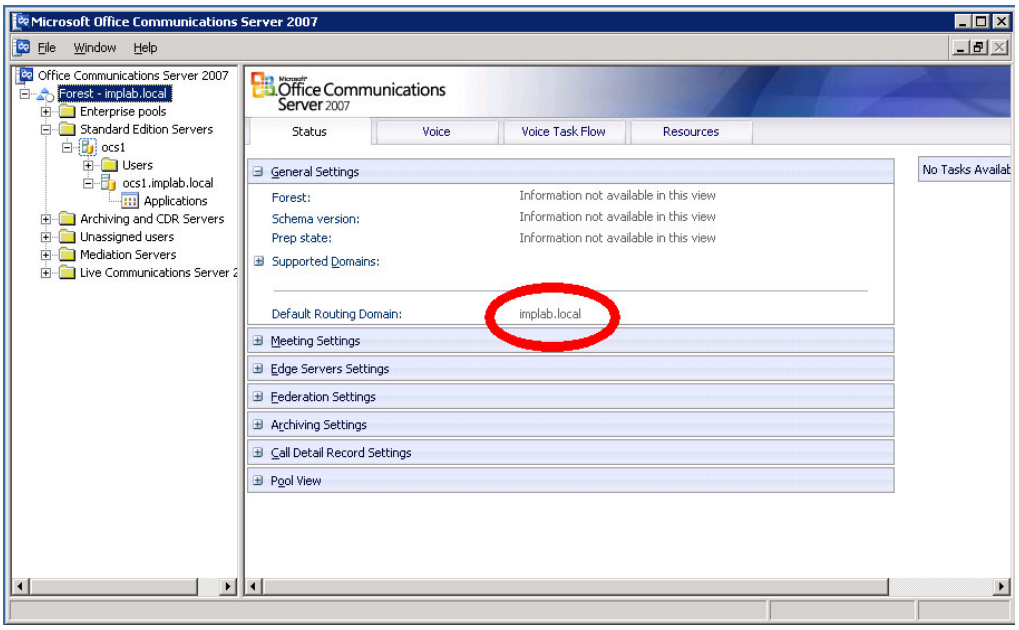


6.) Route setup in the OCS server for the RMX.

Still in the ‘Front End Properties’ select the Routing tab.

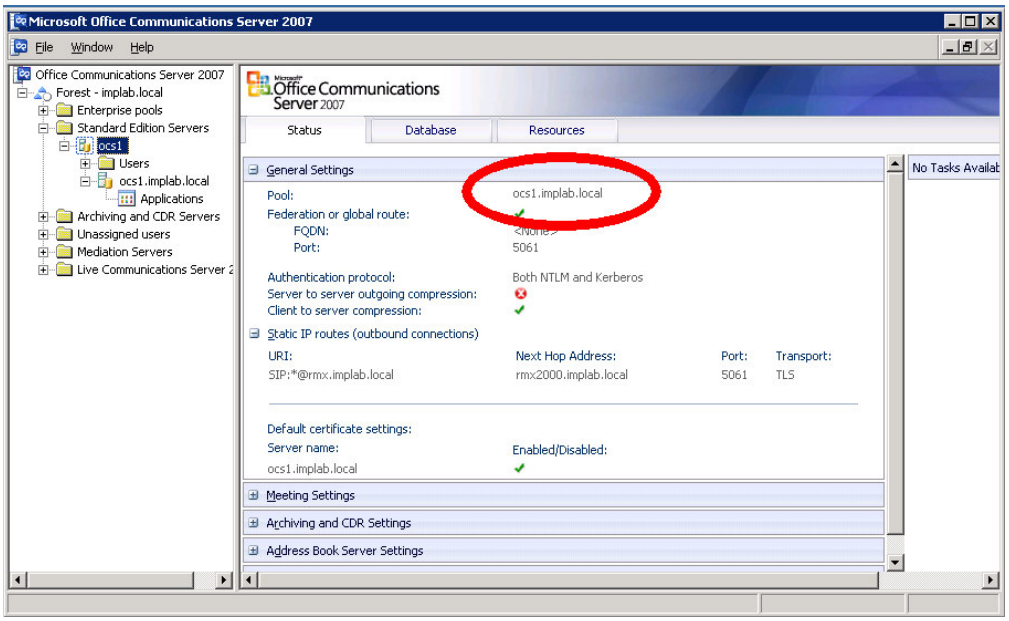


7.) ‘Server Domain Name’ or Sip Domain for the RMX.



Server Domain Name	

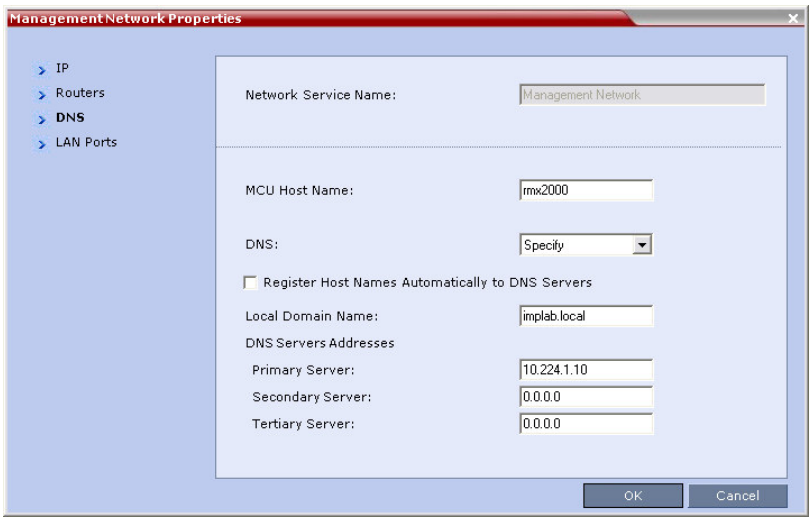
8.) ‘Server IP Address or Name’ for the RMX.



Server IP Address or Name	

Once all the above pieces are in place we can configure the RMX.

In the ‘Management Network’ under the DNS Section:



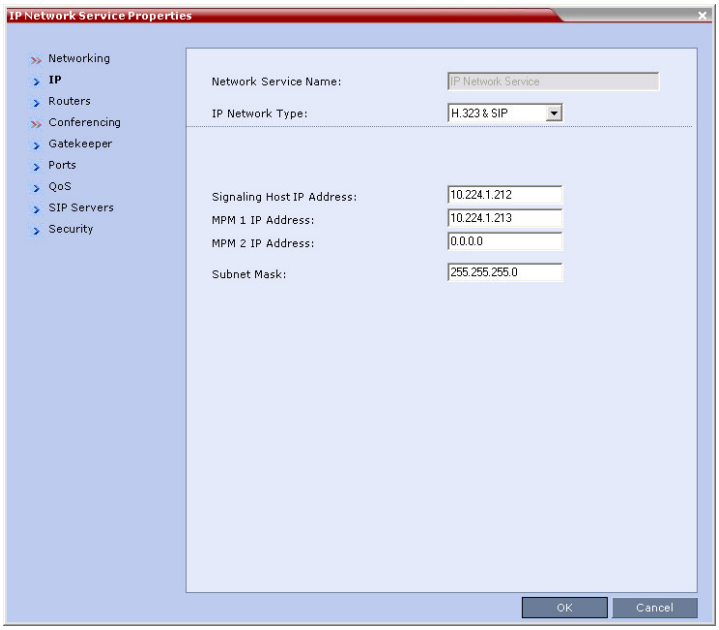
- ‘MCU Host Name’ is the host name portion of the FQDN from item 1.
- Set ‘DNS’ to Specify
- Do Not check ‘Register Host Names Automatically to DNS Servers’
- ‘Local Domain Name’ is the domain portion for the FQDN from item 1.
- ‘DNS Servers Addresses’ are the addresses you gathered in item 3.

Hit ‘OK’ RMX will most likely need to Reset.

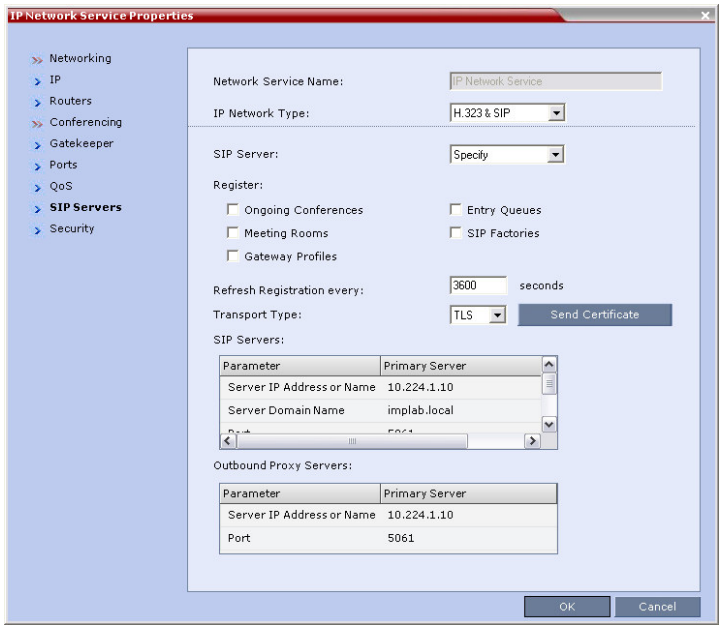
After Reset go into ‘IP Network Service’

In the ‘IP’ Tab:

verify ‘IP Network Type’ is set to ‘SIP’ or ‘H.323 & SIP’



In the ‘SIP Servers’ tab:

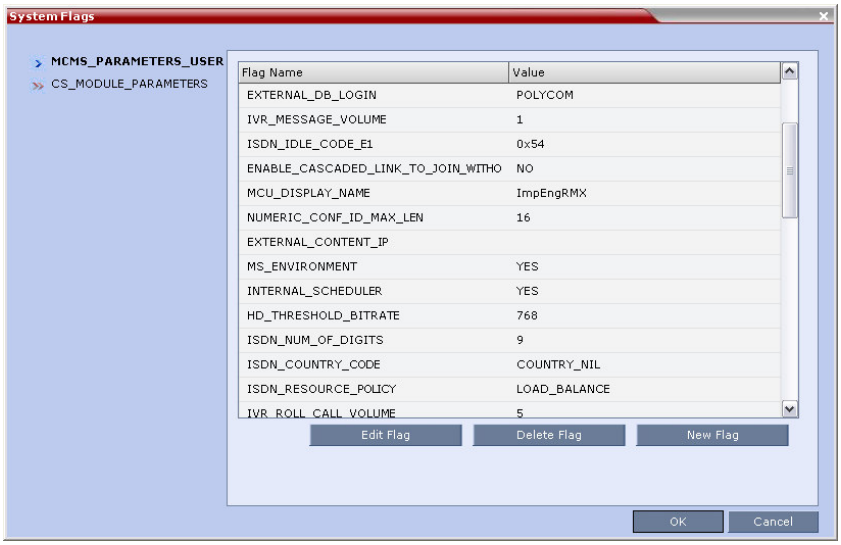


- ‘SIP Server’ set to Specify
- Under ‘Register’ section make sure all boxes are UnChecked.
- ‘Refresh Registration every’ can stay at the default ‘3600’ seconds.
- ‘Transport Type’ should be ‘TLS’
- Under ‘SIP Servers’
    - ‘Server IP Address or Name’ is the IP or FQDN of the OCS Front End Server from Item 8.
    - ‘Server Domain Name’ is the SIP Domain of your company from Item 7.
    - ‘Port’ is 5061 for TLS
- Under ‘Outbound Proxy Servers’
    - ‘Server IP Address or Name’ is the IP or FQDN of the OCS Front End Server from Item 8.
    - ‘Port’ is 5061 for TLS

Then Click ‘Send Certificate’ select all the files from item 4. See APPENDIX B.

Hit ‘OK’ RMX will most likely need to reboot.

After reset go into ‘System Configuration’



Make sure ‘MS_ENVIRONMENT’ exists and is set to ‘YES’

If you had to add or change hitting ‘OK’ will cause another RESET of the RMX.

Appendix A:

Creating the Security (TLS) Certificate in the OCS and Exporting the Certificate to the RMX Workstation

To enable the TLS transport, certificate files *rootCA.pem*, *pkey.pem* and *cert.pem* must be sent to the RMX unit. These files can be created and sent to the RMX in two methods:

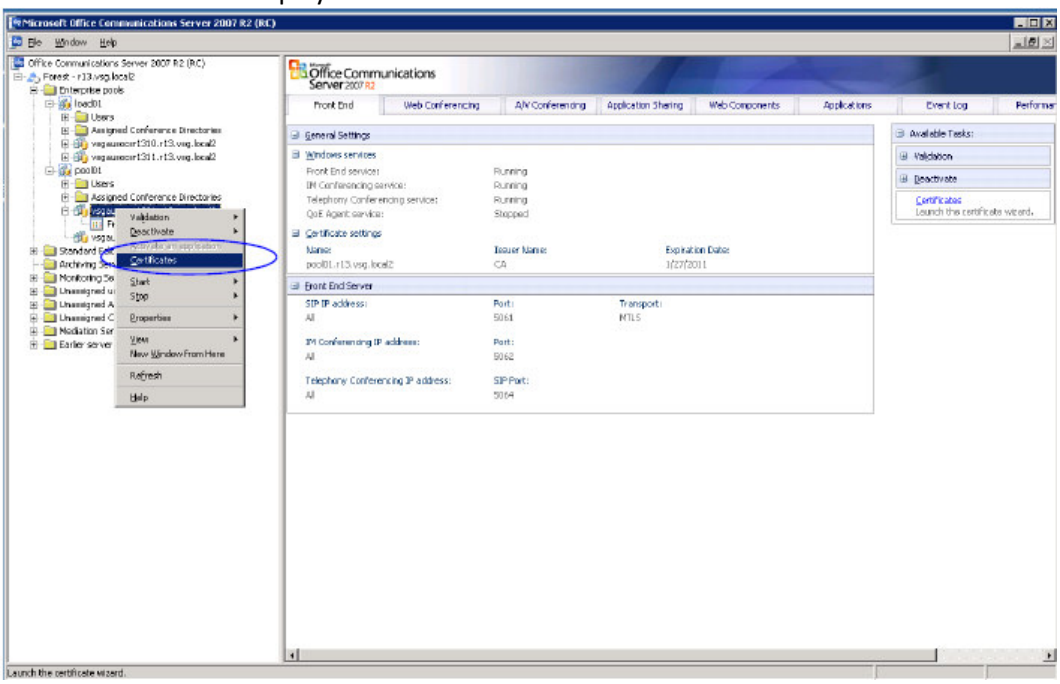
• The files *rootCA.pem*, *pkey.pem* and *cert.pem* are provided by a Certificate Authority and are sent independently or together with a password file to the RMX. This is the recommended method.

• Alternatively, the TLS certificate files are created internally in the OCS and exported to the RMX workstation from where the files can be downloaded to the RMX. If the certificate is created internally by the OCS, one **.pfx* file is created. In addition, a text file containing the password that was used during the creation of the **.pfx* file is manually created. Both files can then be sent from the RMX workstation to the RMX unit. When the files are sent to the RMX, the **.pfx* file is converted into three certificate files: *rootCA.pem*, *pkey.pem* and *cert.pem*.

Sometimes, the system fails to read the *.pfx file and the conversion process fails. Resending *.pfx file again and then resetting the system may resolve the problem.

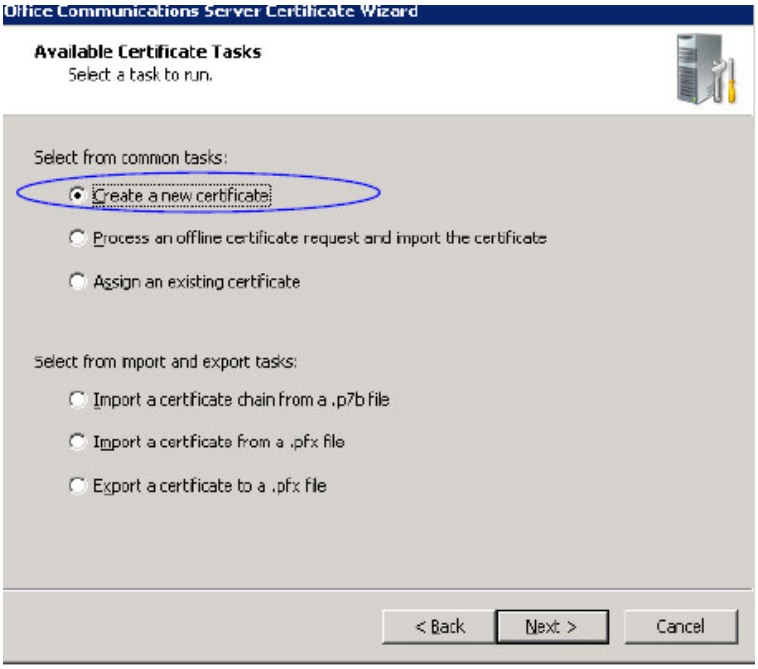
To create the TLS certificate in the OCS:
1 In the OCS *Enterprise Pools* tree, expand the Pools list and the *server pool* list. If a Load Balancer is used in Microsoft R1environment, the transport type may be set to TCP or TLS.

2 Right-click the pool *Front End* entity, and click **Certificate**. The *Office Communicator Server Wizard Welcome* window is displayed.



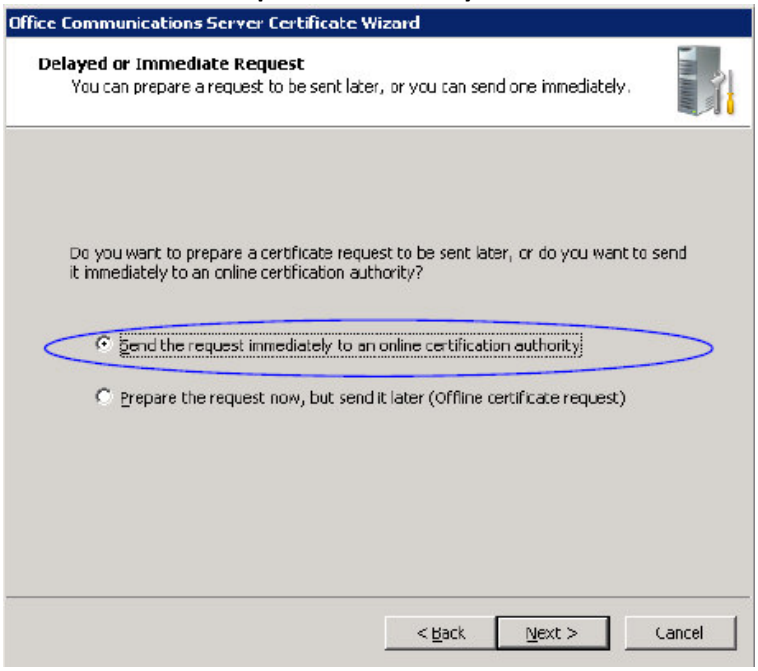
3 Click **Next**.
The *Available Certificate Tasks* window appears.

4 Select **Create a New Certificate** and click **Next**.



The *Delayed or Immediate Request* window appears.

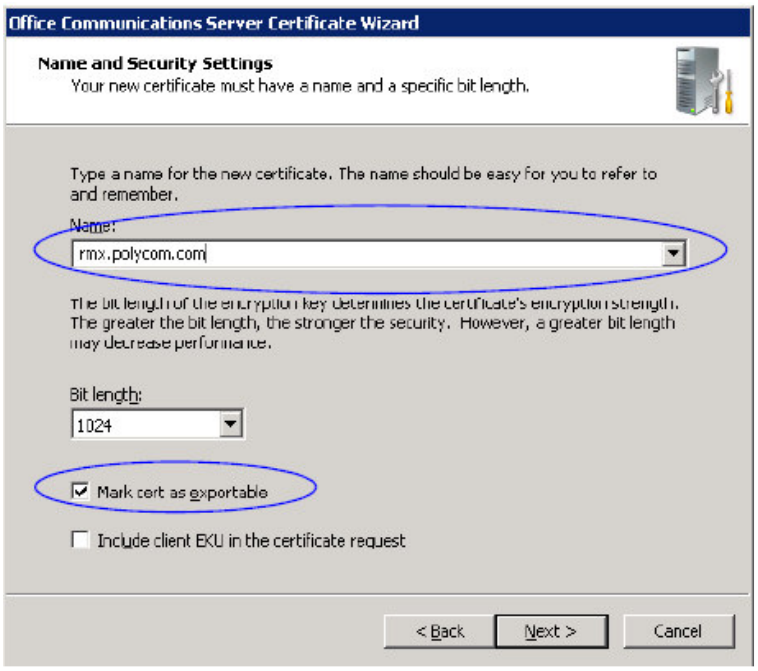
5 Select **Send the Request immediately to an online certificate authority** and click **Next**.



The *Name and Security Settings* window appears.

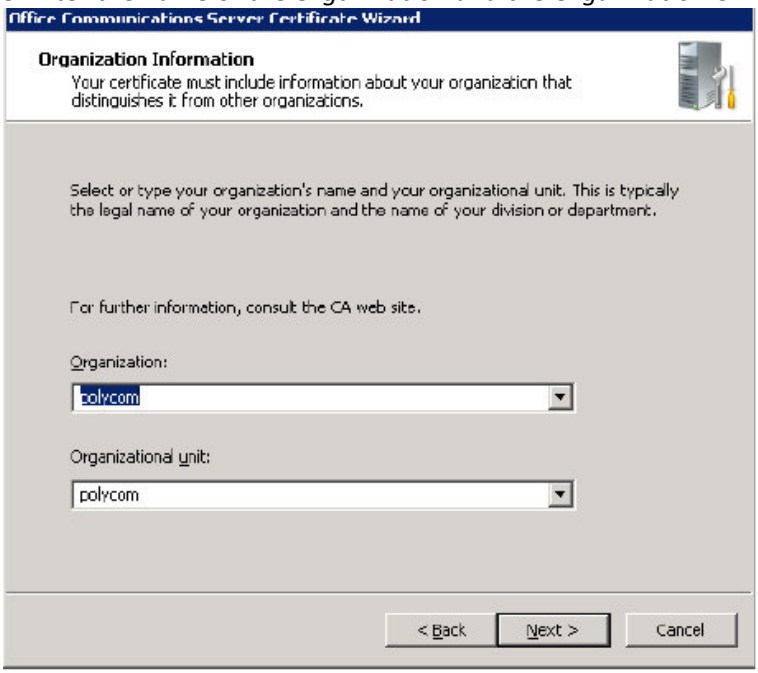
6 In the *Name* field, select the RMX name you entered in the *FQDN* field when defining the trusted host or as defined in the DNS server.

7 Select the **Mark cert as exportable** check box.



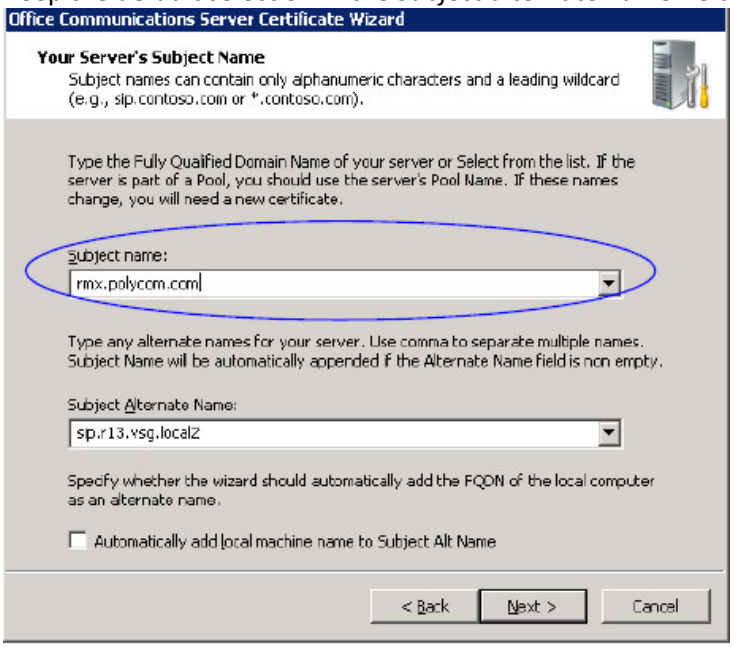
8 Click **Next**.
The *Organization Information* window appears.

9 Enter the name of the *Organization* and the *Organization Unit* and click **Next**.



Your Server's Subject Name window appears.

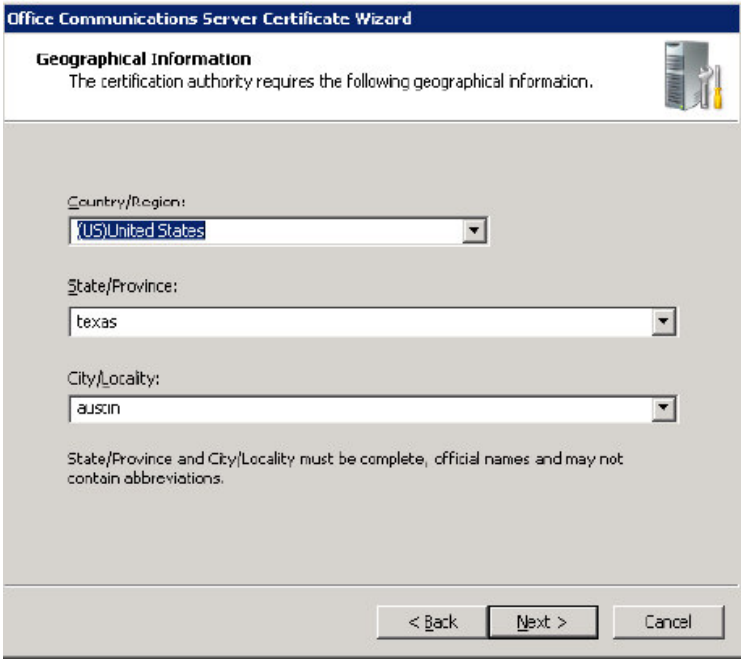
10 In the *Subject name* field, select the *FQDN* name of the RMX from the list or enter its name. Keep the default selection in the *Subject alternate name* field and click **Next**.



11 If an error message is displayed, click **Yes** to continue.

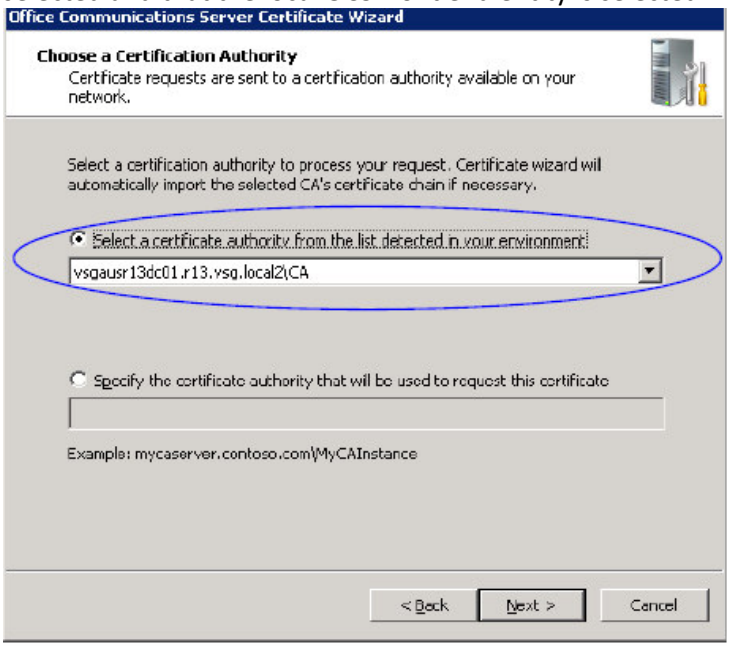
The *Geographical Information* window appears.

12 Enter the geographical information as required and click **Next**.



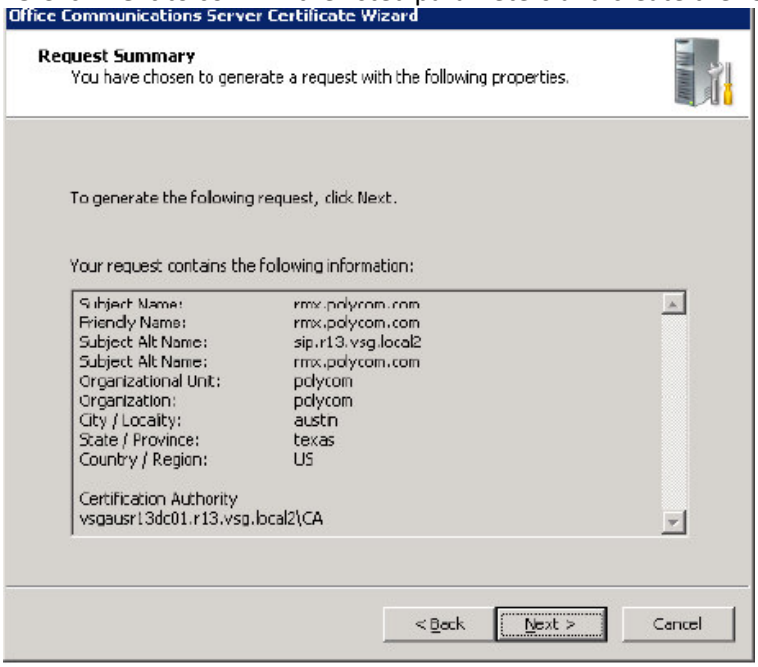
The *Choose a Certification Authority* window appears.

13 Ensure that the **Select a certificate authority from the list detected in your environment** option is selected and that the local OCS front end entity is selected.



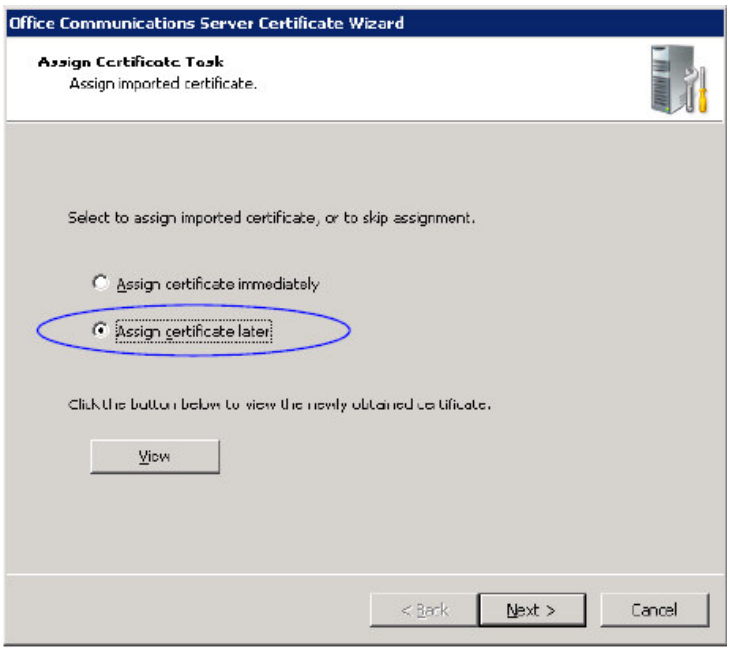
14 Click **Next**.
The *Request Summary* window appears.

15 Click **Next** to confirm the listed parameters and create the requested certificate.



The *Assign Certificate Task* window appears.

16 Select **Assign certificate later** and click **Next** (MS R2).
Select **Assign certificate later** and click **Finish** (MS R1).



The *Certificate Wizard Completed* window appears (MS R2).

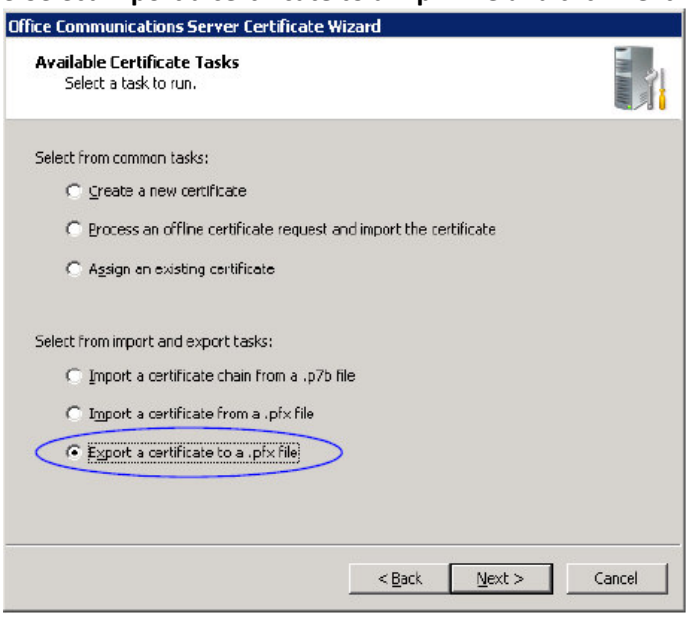
17 Click **Finish** (MS R2).

Retrieving the Certificate from the OCS to the RMX Workstation

1 In the OCS *Enterprise Pools* tree, expand the *Pools* list and the *Server Pool* list.

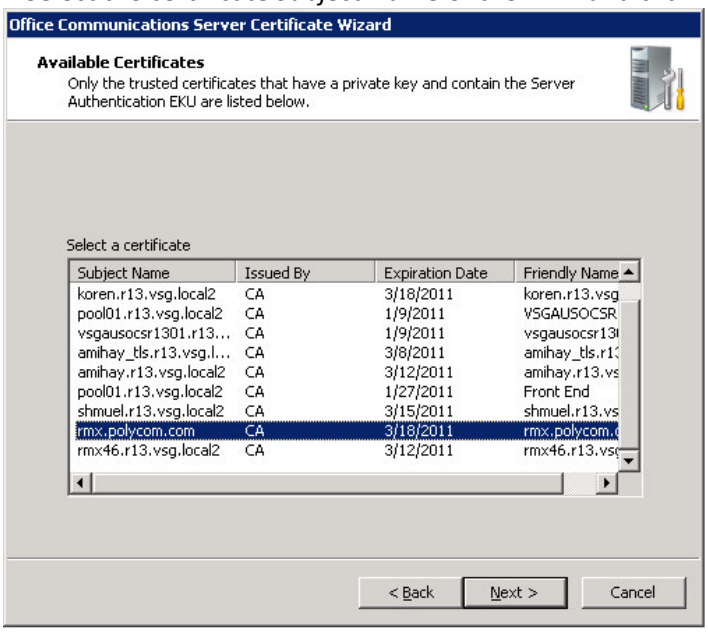
2 Right-click the *pool Front End* entity, and select **Certificate**.
The *Available Certificate Tasks* window appears.

3 Select **Export a certificate to a *.pfx file** and click **Next**.



The *Available Certificates* window appears.

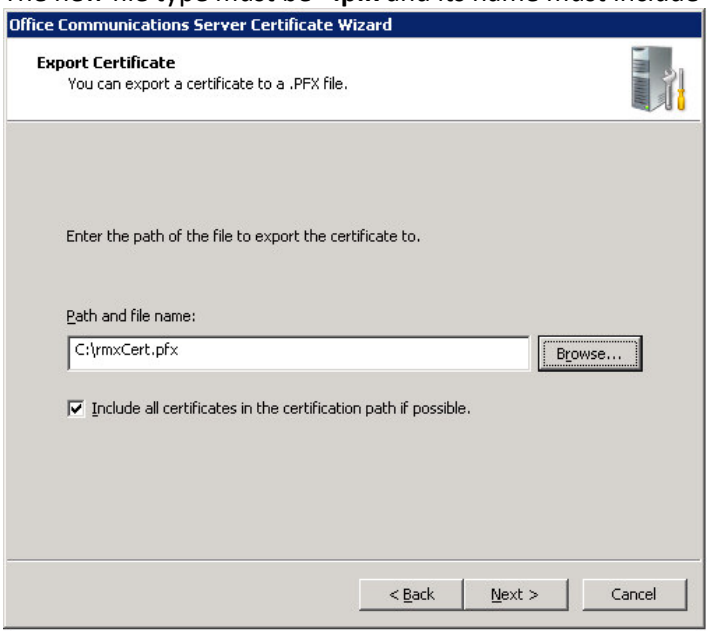
4 Select the certificate *Subject Name* of the RMX and click **Next.**



The *Export Certificate* window appears.

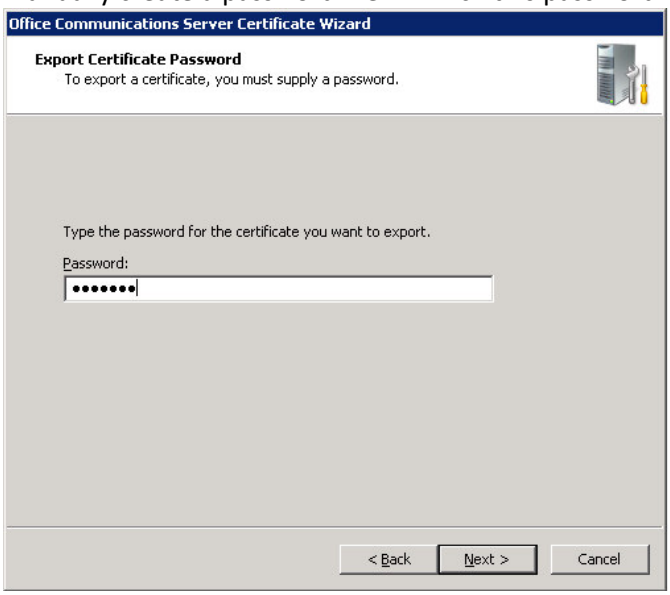
5 Enter the path and file name of the certificate file to be exported or click the **Browse** button to select the path from the list.

The new file type must be ***.pfx** and its name must include the **.pfx** extension.



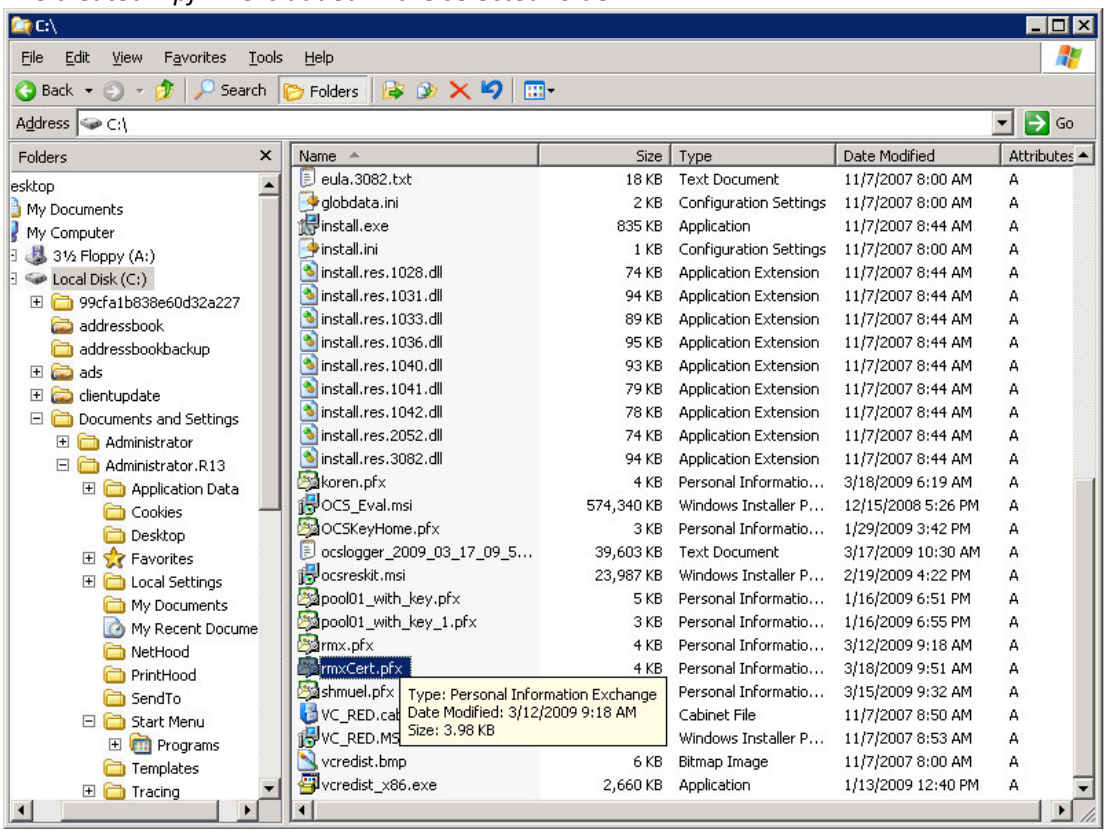
6 Select the **Include all certificates in the certification path if possible** check box and then click **Next**.
The *Export Certificate Password* window appears.

7 If required, enter any password. For example, *Polycom*. Write down this password as you will have to manually create a password file in which this password will appear.



Click **Next**.
The *Certificate Wizard Completed* window appears.

8 Click **Finish**.
The created **.pfx* file is added in the selected folder.



Optional. Creating the Certificate Password File (certPassword.txt)

If you have used a password when creating the certificate file (**.pfx*), you must create a **certPassword.txt** file. This file will be sent to the RMX together with the **.pfx* file.

To create the certPassword.txt file:

1 Using a text editor application, create a new file.

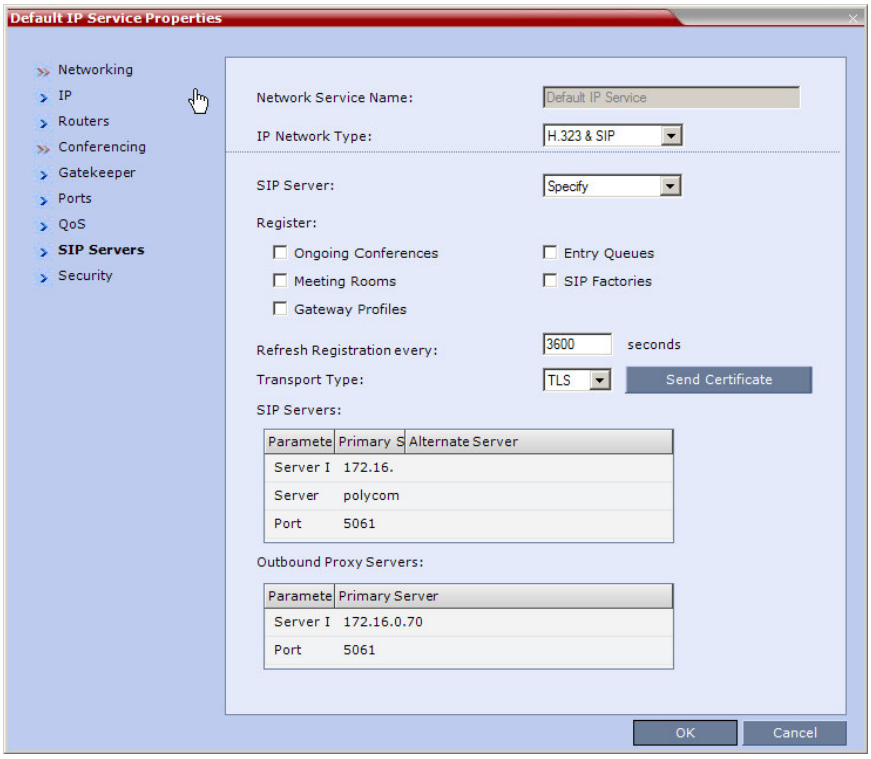
2 Type the password as you have entered when creating the certificate file. For example, enter *Polycom*.

3 Save the file naming it **certPassword.txt** (file name must be exactly as show, the RMX is case sensitive).

APPENDIX B:

Sending the Certificate to the RMX.

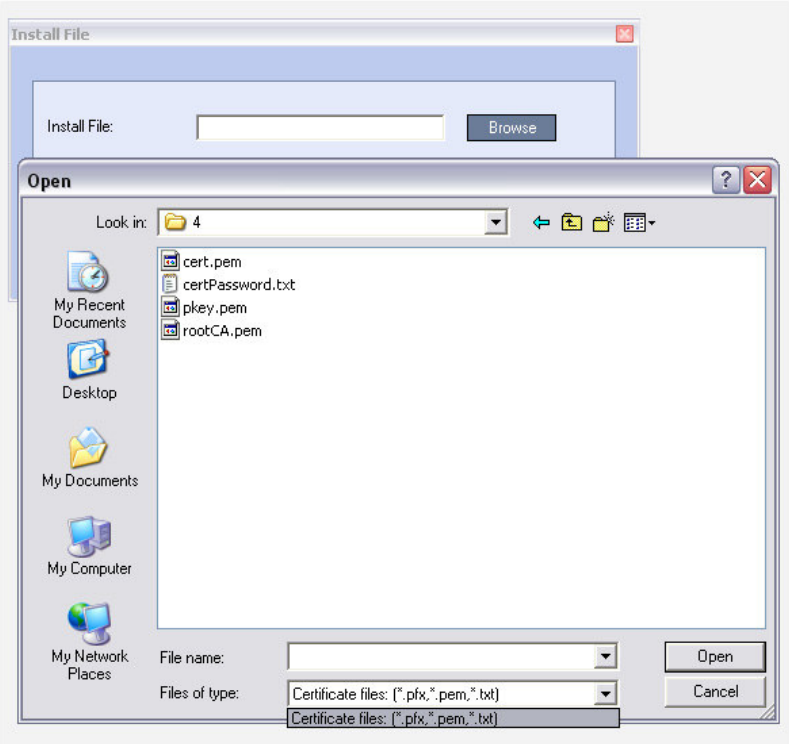
1 Click the **Send Certificate** button.



The *Install File* dialog box opens.

2 Click the **Browse** button.

The *Open* dialog box appears, letting you select the certificate file(s) to send to the MCU.



Depending on the method used when the certificate file(s) were created, send the certificate file(s) to the RMX according to the contents of the file set that was created:

— The certificate files *rootCA.pem, pkey.pem*, *cert.pem* and a *certPassword.txt*. The files were created by a Certificate Authority and are sent as is to the RMX together with the required password contained in the *certPassword.txt* file. This is the recommended method.
— The files *rootCA.pem, pkey.pem* and *cert.pem*. The certificate files were created by a Certificate Authority and are sent as is to the RMX.
— A **.pfx* file and a *certPassword.txt* file. The file c*ertPassword.txt* is manually created if the **.pfx* file was created by the OCS using a password. The **.pfx* file will be converted internally by the RMX using the password included in the certPassword.txt into three certificate files named *rootCA.pem*, *pkey.pem* and *cert.pem*.
— A **.pfx* file if the certificate file was created in the OCS without using a password. The **.pfx* file will be converted internally by the RMX into three certificate files named r*ootCA.pem*, *pkey.pem* and *cert.pem*.

3 In the file browser, select all files to be sent in one operation according to the contents of the set:
— One ***.pfx** file, or
— Two files: one ***.pfx** file and **certPassword.txt**, or
— Three files: **rootCA.pem, pkey.pem** and **cert.pem**, or
— Four files: **rootCA.pem, pkey.pem, cert.pem** and **certPassword.txt**

4 Click **Open**.
The selected file(s) appear in the *Install Files* path.

5 Click **Install**.
The files are sent to the RMX and the *Install File* dialog box closes.