Using RPC over HTTP with Exchange Server 2003 SP1

Author: Bill Boswell

Bill Boswell Consulting, Inc.
www.billboswellconsulting.com
bill@billboswellconsulting.com

RCP over HTTP has a *lot* of moving parts and it can be a frustrating experience to get it working the first time. Exchange 2003 SP1 simplifies the process in several important ways:

- A new property page in Exchange System Manager makes it quick and easy to identify servers as back-end (mailbox and public folder) servers or front-end (RPC over HTTP Proxy) servers.
- An Exchange 2003 SP1 server automatically discovers and configures the RPC service ports used by back-end servers, eliminating a tedious and error-prone step in the original release of Exchange 2003.
- A front-end server can now proxy directory service requests to a Global Catalog server on behalf of incoming clients, eliminating the need to run RPC over HTTP on Global Catalog servers.

Even with these changes, setting up a production environment in support of RPC over HTTP is quite an exercise. This document contains a simple configuration you can set up in a lab to demonstrate how the various moving parts fit together:

- RPC over HTTP on the front-end server
- Front-end and back-end server selection in ESM
- SSL on the front-end server
- Outlook 2003 client proxy configuration

Don't let the length of this document discourage you from giving RPC over HTTP a try. Once you get the knack, it's fairly simple to work with. Really.

Prerequisites

Before getting started, run your thumb down the following list of prerequisites to make sure you meet the minimum conditions to use RPC over HTTP for Outlook. Remember that production deployments would include at least one firewall with a DMZ containing a hardened ISA server.

DNS -- Most Exchange problems are caused by an incorrect DNS configuration. Before starting to configure RPC over HTTP, make absolutely sure that your Exchange servers, Outlook client desktops, and Active Directory domain controllers and Global Catalog servers can all ping each other using fully qualified DNS names and flat names.

Distributed architecture -- The RPC over HTTP improvements in Exchange Server SP1 assume that you have at least one front-end server that stands proxy for all incoming and outgoing e-mail requests from suitably configured Outlook 2003 clients. It's possible to use RPC over HTTP to connect directly to a mailbox server (a so-called *back-end* server) , such as you might have for Small Business Server 2003, but you'll need to do additional configuration. My suggestion is that you get the feature working using the suggested architecture in your lab so you can see how everything fits together. Then try your hand at making it work with a single Exchange server.

Server operating system -- RPC over HTTP is a feature of the operating system, so you must run Exchange 2003 on Windows Server 2003 to use this feature. The domain controllers used by Exchange must also be running Windows Server 2003. You can use Windows Server 2003 Standard Edition or Enterprise Edition.

Exchange version -- The front-end server must be running Exchange Server 2003 SP1. You can use the Standard Edition or Enterprise Edition of Exchange 2003.

Back-end servers can run Exchange Server 2003 without a service pack, however, it's not a good idea to have a mix of service packs in an organization. Apply the service pack to the back-end servers, as well.

(Note: Before installing SP1, you'll need to install Hotfix 831464. This fixes an issue with HTTP compression. Download the fix from http://support.microsoft.com/?kbid=831464.)

Outlook clients -- The only e-mail client that supports RPC over HTTP is Outlook 2003, and only when running on XP SP1 with Hotfix 331320 or XP SP2. (You can also install Outlook 2003 on Windows Server 2003, but this would not be a suggested practice for a production system.)

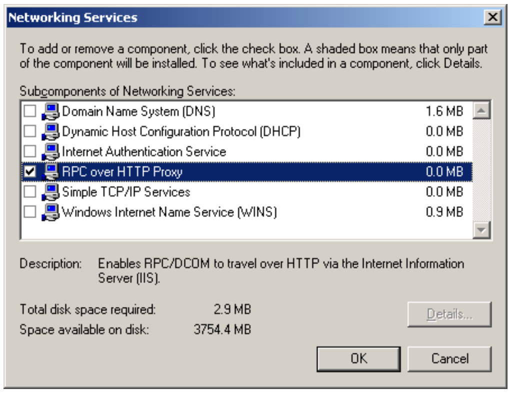
Clusters -- The front-end RPC over HTTP proxy server cannot be a cluster. The back-end servers can be clusters.

Install the RPC over HTTP Proxy Service on the Front-end Server

The Exchange front-end server accepts RPC over HTTP traffic from Outlook 2003 clients, extracts the messages inside, and forwards the messages to the mailbox (back-end) servers. It also accepts GAL lookups (more formally called Name Server Provider Interface, or NSPI, requests) from Outlook clients and proxies them to a Global Catalog server.

Only the front-end server needs to run the RPC over HTTP Proxy service. This is the major advantage of a distributed architecture. Install the service as follows:

1. Open the Control Panel and launch the Add/Remove Programs applet.
2. Click Add/Remove Windows Components.
3. Highlight the Networking Services option and click Details. This opens the Networking Services window.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☐	Domain Name System (DNS)	1.6 MB
☐	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☐	Internet Authentication Service	0.0 MB
☑	RPC over HTTP Proxy	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☐	Windows Internet Name Service (WINS)	0.9 MB

Description: Enables RPC/DCOM to travel over HTTP via the Internet Information Server (IIS).

Total disk space required: 2.9 MB

Space available on disk: 3754.4 MB

Install RPC over HTTP proxy

4. Select the RPC over HTTP Proxy option and click OK to save the change then click Next at each window that follows to apply the change.

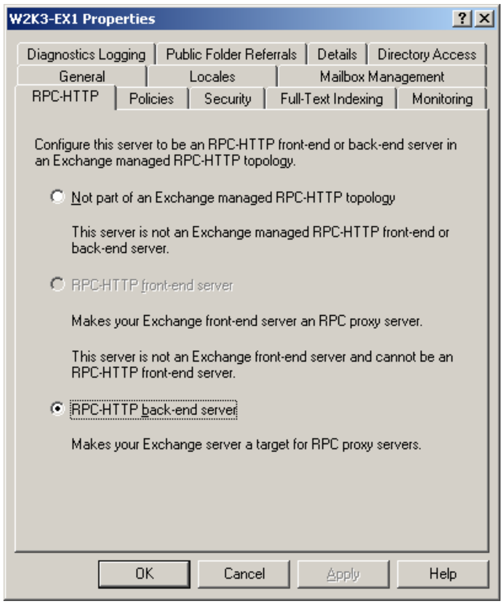
Identify Back-end Exchange Servers in ESM

In a standard distributed architecture Exchange topology, there is no need to identify back-end servers, the assumption being that any server that's not a front-end server is a back-end server.

But an RPC over HTTP front-end server needs to know which servers are willing to accept proxied message traffic so it can determine the RPC ports on which each back-end server is listening for HTTP requests. Recall that RPC services don't necessarily use the same port on each server.

The initial release (pre-SP1) of Exchange Server 2003 requires you as the administrator to find the RPC ports on the back end servers and Global Catalog servers and put them in the Registry of the front-end server. Exchange Server 2003 SP1 automates the process by querying each designated back-end server to discover the ports used for RPC over HTTP communication then writing this information into the Registry. For this reason, it's important that you configure the back-end servers first in ESM.

1. Open Exchange System Manager (ESM) and drill down to the server icons.
2. Open the Properties window for a back-end server and select the RPC-HTTP tab.



Configure this server to be an RPC-HTTP front-end or back-end server in an Exchange managed RPC-HTTP topology.

○ Not part of an Exchange managed RPC-HTTP topology

This server is not an Exchange managed RPC-HTTP front-end or back-end server.

○ RPC-HTTP front-end server

Makes your Exchange front-end server an RPC proxy server.

This server is not an Exchange front-end server and cannot be an RPC-HTTP front-end server.

● RPC-HTTP back-end server

Makes your Exchange server a target for RPC proxy servers.

Back-end server configuration

3. Click OK to save the change. If you forgot to install the RPC over HTTP Proxy service on the server, you'll get an error message.

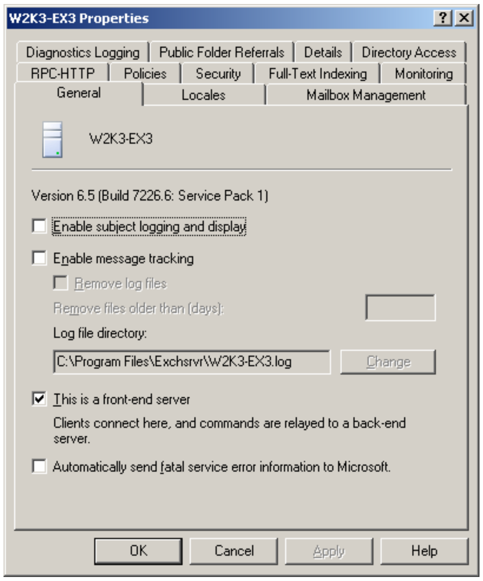
4. Repeat this procedure for each back-end server. Remember, the front-end server can route mail to a back-end server on behalf of an RPC over HTTP client unless you configure the back-end server to accept RPC over HTTP requests.

You may want to wait until this information has replicated out to all domain controllers used by Exchange servers. Then proceed to the next section to configure the front-end servers.

Configure Front-end Server

An RPC over HTTP front-end server must also be configured as a standard Exchange front-end server. This makes changes in the Exchange configuration to support pass-through authentication and direct message delivery to other Exchange servers. Ordinarily, a front-end server would not have mailboxes or public folders. If your budget won't permit you to install a front-end server, you can configure RPC over HTTP directly on your Exchange server. You'll lose the automatic configuration and NSPI proxy capabilities in SP1, though, so you'll need to make these settings yourself.

1. In ESM, open the Properties window of the server you've decided to use as an RPC over HTTP front-end server. Select the General tab.



W2K3-EX3

Version 6.5 (Build 7226.6: Service Pack 1)

☐ Enable subject logging and display

☐ Enable message tracking

☐ Remove log files

Remove files older than (days):

Log file directory:

C:\Program Files\Exchsrvr\W2K3-EX3.log Change

☑ This is a front-end server

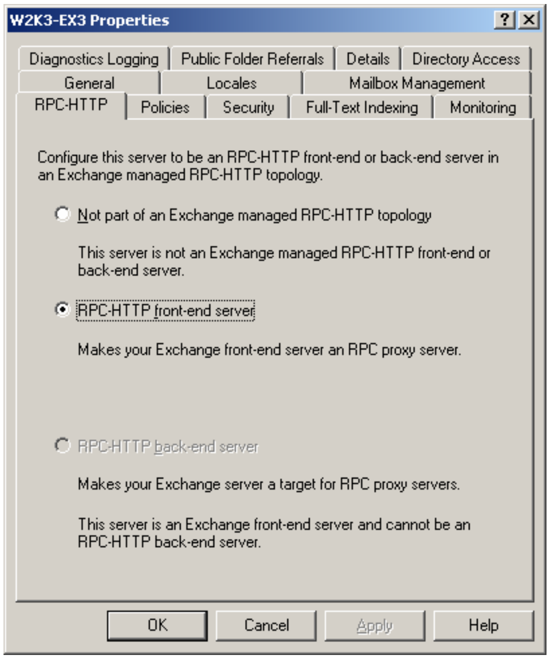
Clients connect here, and commands are relayed to a back-end server.

☐ Automatically send fatal service error information to Microsoft.

Front-end primary configuration

2. If the server is not already a front-end server for other purposes, select the option *This is a front-end server* and click Apply to save the change.

3. Now select the RPC-HTTP tab and select the *RPC-HTTP front-end server* radio button.



Configure this server to be an RPC-HTTP front-end or back-end server in an Exchange managed RPC-HTTP topology.

○ Not part of an Exchange managed RPC-HTTP topology

This server is not an Exchange managed RPC-HTTP front-end or back-end server.

● RPC-HTTP front-end server

Makes your Exchange front-end server an RPC proxy server.

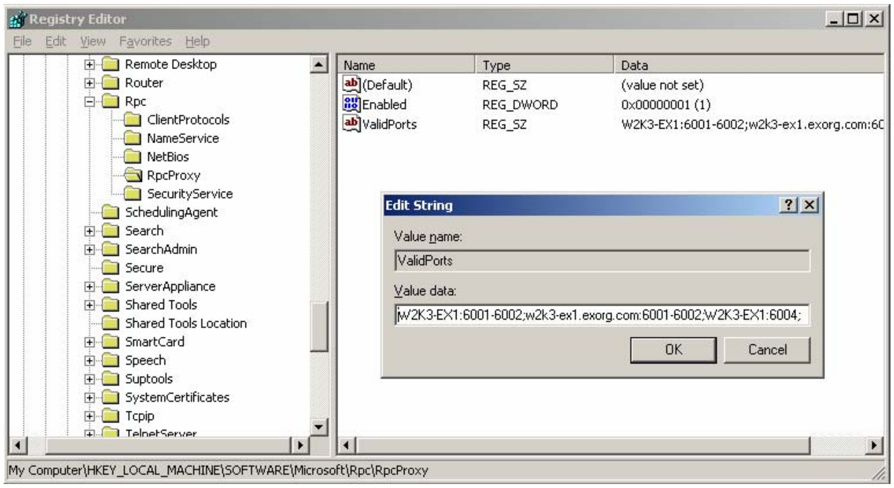
○ RPC-HTTP back-end server

Makes your Exchange server a target for RPC proxy servers.

This server is an Exchange front-end server and cannot be an RPC-HTTP back-end server.

Front-end server RPC-HTTP configuration

4. Click OK to save the change.



Name	Type	Data
(Default)	REG_SZ	(value not set)
Enabled	REG_DWORD	0x00000001 (1)
ValidPorts	REG_SZ	W2K3-EX1:6001-6002;w2k3-ex1.exorg.com:60

Value name: ValidPorts

Value data: W2K3-EX1:6001-6002;w2k3-ex1.exorg.com:6001-6002;W2K3-EX1:6004;

My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy

Registry entries for valid ports

Here's where the magic happens. The newly configured Exchange front-end server now sweeps the back-end servers looking for the port used to make HTTP connection to the Information Store. It then writes this name and port information into the Registry. You should check this key to make sure it has entries.

Here's an example showing the port settings for a back-end server called w2k3-ex1.exorg.com:

```
Key: HKLM | Software | Microsoft | Rpc | RpcProxy
Value: ValidPorts
Data: W2K3-EX1:6001-6002;w2k3-ex1.exorg.com:6001-6002;W2K3-EX1:6004;w2k3-
ex1.exorg.com:6004
```

At this point, the distributed architecture of the Exchange organization in support of RPC over HTTP has been configured. You're not quite ready to go yet, though, because RPC over HTTP requires SSL at the front-end server.

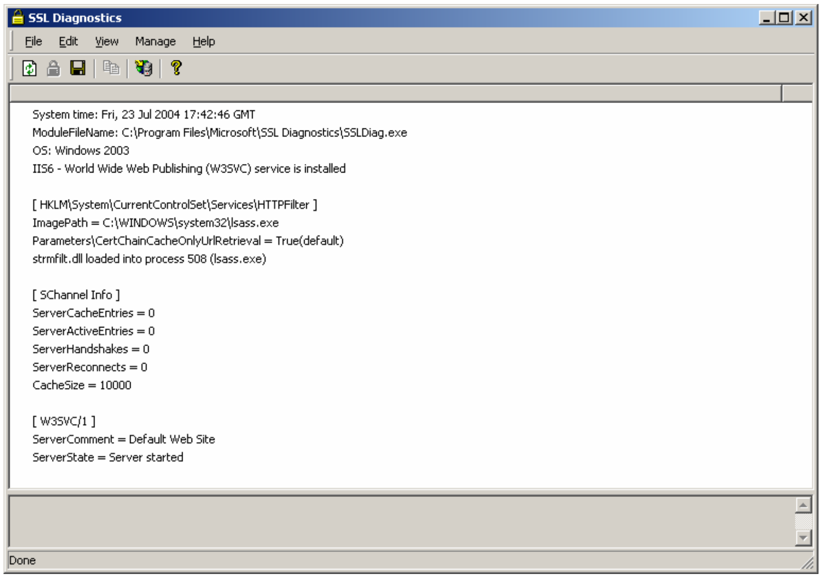
If you configure the front-end first, or you add more back-end servers at a later time, you can simply select the *Not part of an Exchange managed RPC-HTTP topology*, apply the change, then go back to the original *RPC-HTTP front-end server* setting. This clears out the Registry entry and rediscovers the back-end servers.

Configure SSL on Front-End Server

RPC over HTTP, as implemented in Outlook and Exchange, requires SSL. You cannot make a connection, even for testing, using standard HTTP. This can cause you some problems if this is the first time you've worked with installing an SSL certificate on a web server. The configuration isn't all that difficult, but the trick is to get a copy of the certificate (or the certificate of the issuing Certification Authority) onto the client machines so that they trust the SSL connection offered by the front-end server.

For lab testing, I recommend using a self-signed certificate. Microsoft provides a free utility called SSLDiag that generates the self-signed certificate, assigns it to the IIS server, and verifies that the server uses the certificate for an SSL connection. (This makes SSLDiag much more convenient to use than the SelfSSL utility in the IIS 6.0 Resource Kit.) Download SSLDiag from http://snipurl.com/7zmz.

The first time you run SSLDiag, you'll get a text listing that describes your current web configuration.

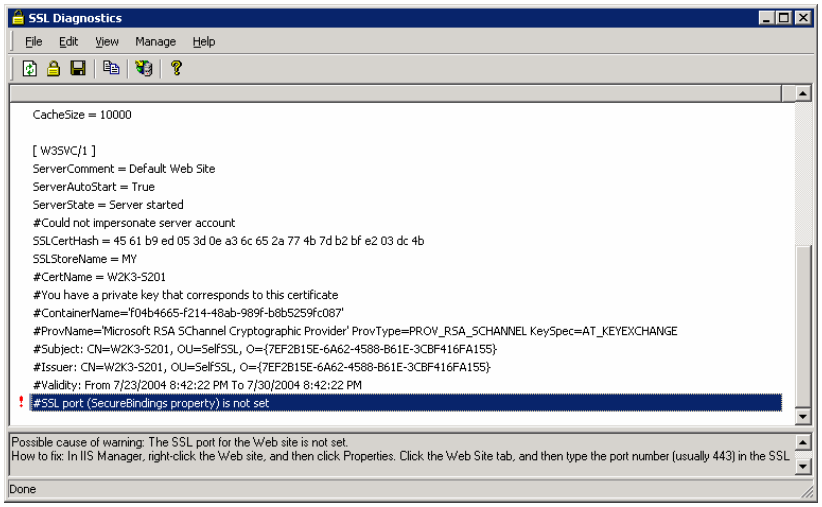


```
System time: Fri, 23 Jul 2004 17:42:46 GMT
ModuleFileName: C:\Program Files\Microsoft\SSL Diagnostics\SSLDiag.exe
OS: Windows 2003
IIS6 - World Wide Web Publishing (W3SVC) service is installed

[ HKLM\System\CurrentControlSet\Services\HTTPFilter ]
ImagePath = C:\WINDOWS\system32\lsass.exe
Parameters\CertChainCacheOnlyUrlRetrieval = True(default)
strmfilt.dll loaded into process 508 (lsass.exe)

[ SChannel Info ]
ServerCacheEntries = 0
ServerActiveEntries = 0
ServerHandshakes = 0
ServerReconnects = 0
CacheSize = 10000

[ W3SVC/1 ]
ServerComment = Default Web Site
ServerState = Server started
```

SSLDiag initial configuration window

Right-click the [W3SVC/1] line and select Create New Cert from the flyout menu. This one little action does the following:

- Creates a self-signed certificate
- Installs the certificate in the default web site
- Puts a copy of the certificate in the Trusted Root Servers repository so that it's trusted by the local machine
- Gives a full report of the operation, including the names and keys used by the certificate.



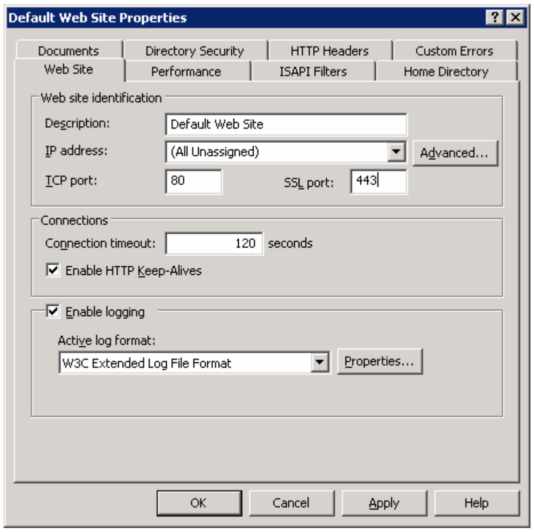
```
CacheSize = 10000

[ W3SVC/1 ]
ServerComment = Default Web Site
ServerAutoStart = True
ServerState = Server started
#Could not impersonate server account
SSLCertHash = 45 61 b9 ed 05 3d 0e a3 6c 65 2a 77 4b 7d b2 bf e2 03 dc 4b
SSLStoreName = MY
#CertName = W2K3-S201
#You have a private key that corresponds to this certificate
#ContainerName='f04b4665-f214-48ab-989f-b8b5259fc087'
#ProvName='Microsoft RSA SChannel Cryptographic Provider' ProvType=PROV_RSA_SCHANNEL KeySpec=AT_KEYEXCHANGE
#Subject: CN=W2K3-S201, OU=SelfSSL, O={7EF2B15E-6A62-4588-B61E-3CBF416FA155}
#Issuer: CN=W2K3-S201, OU=SelfSSL, O={7EF2B15E-6A62-4588-B61E-3CBF416FA155}
#Validity: From 7/23/2004 8:42:22 PM To 7/30/2004 8:42:22 PM
! #SSL port (SecureBindings property) is not set
```

Possible cause of warning: The SSL port for the Web site is not set.
How to fix: In IIS Manager, right-click the Web site, and then click Properties. Click the Web Site tab, and then type the port number (usually 443) in the SSL

SSLDiag report following self-signed certificate creation

You'll notice a red exclamation point next to *#SSL port (SecureBindings property) is not set.* This is because the utility doesn't put a value in the SSL port configuration for the default web site. You'll need to do that manually. Also, the utility only makes SSL available, it does not *require* the use of SSL. You'll need to lock down the RPC virtual folder in the default web site to only accept SSL connections. Correct both of these issues as follows:

1. From the main SSLDiag menu, select Manage | Open IIS Manager.
2. Drill down to the Default Web Site and open the Properties window. Select the Web Site tab. In the *SSL Port* field, enter 443.



Web site identification

Description: Default Web Site

IP address: (All Unassigned)

TCP port: 80 SSL port: 443

Connections

Connection timeout: 120 seconds

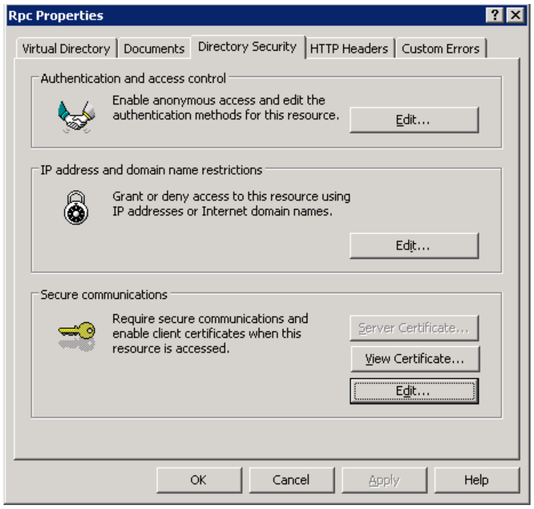
☑ Enable HTTP Keep-Alives

☑ Enable logging

Active log format: W3C Extended Log File Format

Web site properties showing SSL port

3. Click OK to save the change and return to the main IIS management console.
4. Drill down to the RPC folder, open the Properties window for the folder, and select the Directory Security tab.



Authentication and access control

Enable anonymous access and edit the authentication methods for this resource.

IP address and domain name restrictions

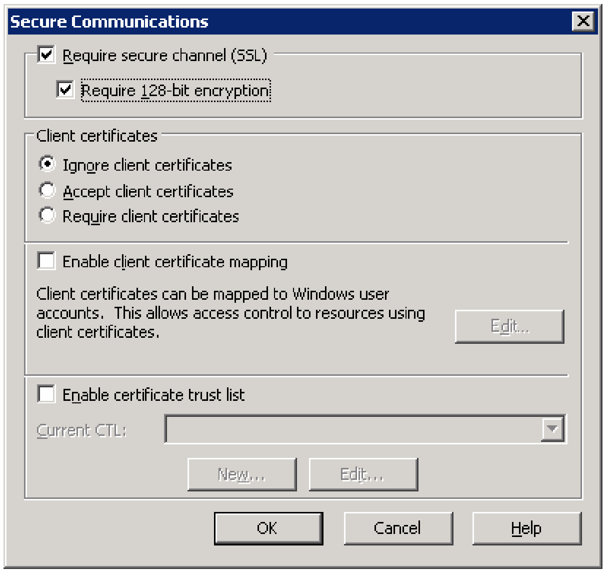
Grant or deny access to this resource using IP addresses or Internet domain names.

Secure communications

Require secure communications and enable client certificates when this resource is accessed.

Web site properties - Directory Security tab

5. In the Secure Communications area, click *Edit*. This opens the Secure Communications window.



Secure Communications

☑ Require secure channel (SSL)

☑ Require 128-bit encryption

Client certificates

● Ignore client certificates

○ Accept client certificates

○ Require client certificates

□ Enable client certificate mapping

Client certificates can be mapped to Windows user accounts. This allows access control to resources using client certificates.

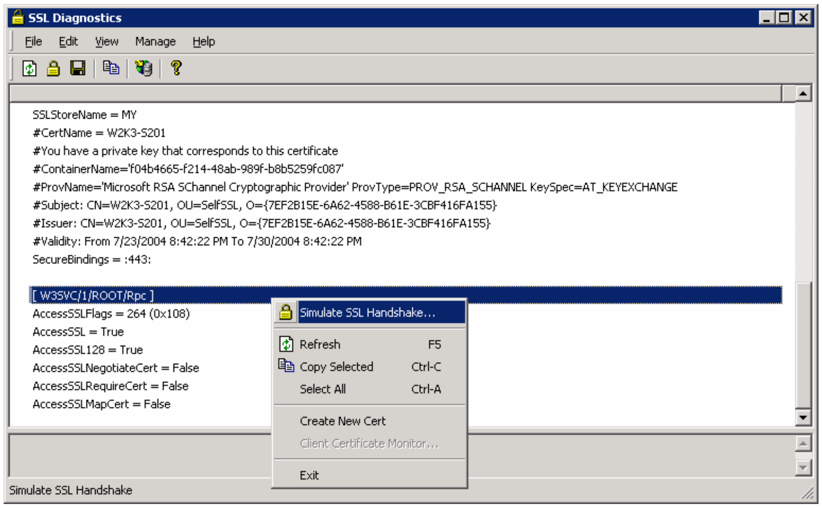
□ Enable certificate trust list

Current CTL:

Secure Communications window showing secure channel requirement

6. Select both *Require Secure Channel (SSL)* and *Require 128-bit Encryption*. Click OK to save the change then close the IIS management console and return to the SSLDiag window.

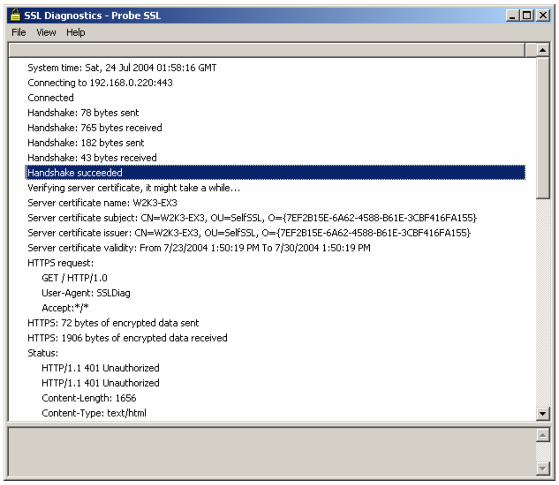
7. Test the SSL connection by right-clicking the [W3SVC/1/ROOT/Rpc] line and selecting *Simulate SSL Handshake* from the flyout menu.



```
SSLStoreName = MY
#CertName = W2K3-S201
#You have a private key that corresponds to this certificate
#ContainerName='f04b4665-f214-48ab-989f-b8b5259fc087'
#ProvName='Microsoft RSA SChannel Cryptographic Provider' ProvType=PROV_RSA_SCHANNEL KeySpec=AT_KEYEXCHANGE
#Subject: CN=W2K3-S201, OU=SelfSSL, O={7EF2B15E-6A62-4588-B61E-3CBF416FA155}
#Issuer: CN=W2K3-S201, OU=SelfSSL, O={7EF2B15E-6A62-4588-B61E-3CBF416FA155}
#Validity: From 7/23/2004 8:42:22 PM To 7/30/2004 8:42:22 PM
SecureBindings = :443:

[ W3SVC/1/ROOT/Rpc ]
AccessSSLFlags = 264 (0x108)
AccessSSL = True
AccessSSL128 = True
AccessSSLNegotiateCert = False
AccessSSLRequireCert = False
AccessSSLMapCert = False
```

SSLDiag - SSL handshake

8. This opens an SSL Probe window that shows the (hopefully successful) results of the SSL handshake, including the reply from the web site.



```
System time: Sat, 24 Jul 2004 01:58:16 GMT
Connecting to 192.168.0.220:443
Connected
Handshake: 78 bytes sent
Handshake: 765 bytes received
Handshake: 182 bytes sent
Handshake: 43 bytes received
Handshake succeeded
Verifying server certificate, it might take a while...
Server certificate name: W2K3-EX3
Server certificate subject: CN=W2K3-EX3, OU=SelfSSL, O={7EF2B15E-6A62-4588-B61E-3CBF416FA155}
Server certificate issuer: CN=W2K3-EX3, OU=SelfSSL, O={7EF2B15E-6A62-4588-B61E-3CBF416FA155}
Server certificate validity: From 7/23/2004 1:50:19 PM To 7/30/2004 1:50:19 PM
HTTPS request:
   GET / HTTP/1.0
   User-Agent: SSLDiag
   Accept:*/*
HTTPS: 72 bytes of encrypted data sent
HTTPS: 1906 bytes of encrypted data received
Status:
   HTTP/1.1 401 Unauthorized
   HTTP/1.1 401 Unauthorized
   Content-Length: 1656
   Content-Type: text/html
```

Probe SSL -- handshake succeeds

Trusting a Certificate

At this point, you have confidence that the SSL configuration at the front-end server is correct. However, at this point, the SSL certificate used by this web server is not trusted by another other machine. This will cause SSL connection warnings. You'll need to add the self-signed certificate used by the Exchange front-end server to the Trusted Root Servers repository on the Outlook client desktop.

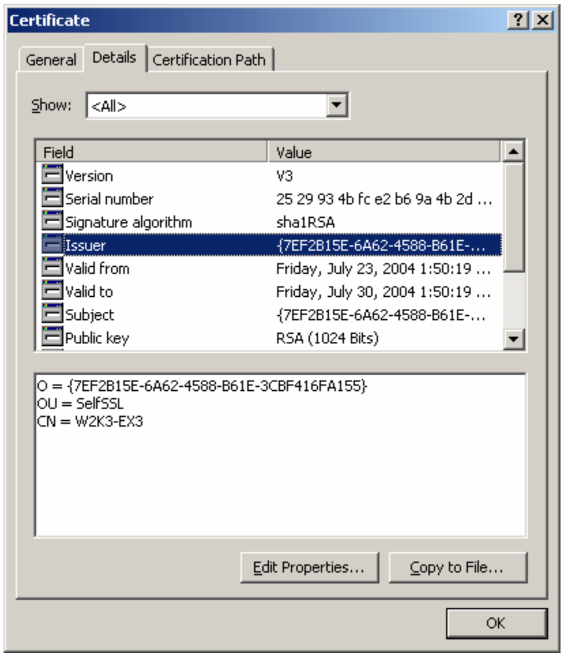
(Note: In a small network where you can easily get a copy of the self-signed certificate into each desktop, then you don't need to spend any money to purchase a third party certificate for your Exchange server. However, if it will be a logistical problem to distribute the certificate, then you should consider purchasing a certificate from a well-known vendor that already has a Root Certification Authority certificate in the Windows trusted root repository.)

Exporting an SSL Certificate

Before you can import the server's SSL certificate into your client desktop, you'll need to export the certificate to a file. There are several ways to do this. Here's a way that uses the IIS management console:

1. Open the IIS management console and drill down to the Default Web Site.
2. Open the Properties window for the Default Web Site and select the Directory Security tab.
3. In the Secure Communications area, click View Certificate. This opens the certificate viewer.

4. Select the Details tab.



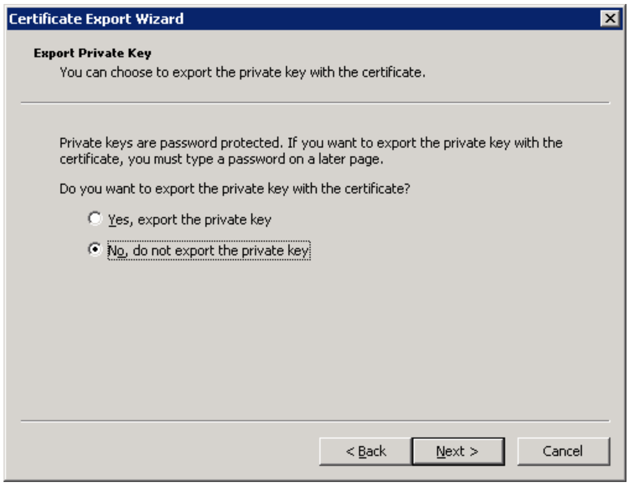
Show: <All>

Field	Value
Version	V3
Serial number	25 29 93 4b fc e2 b6 9a 4b 2d ...
Signature algorithm	sha1RSA
Issuer	{7EF2B15E-6A62-4588-B61E-...
Valid from	Friday, July 23, 2004 1:50:19 ...
Valid to	Friday, July 30, 2004 1:50:19 ...
Subject	{7EF2B15E-6A62-4588-B61E-...
Public key	RSA (1024 Bits)

```
O = {7EF2B15E-6A62-4588-B61E-3CBF416FA155}
OU = SelfSSL
CN = W2K3-EX3
```

SSL certificate details

5. Click *Copy to File*. This launches the Certificate Export Wizard. Click Next at the Welcome window to get the Export Private Key window.



Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

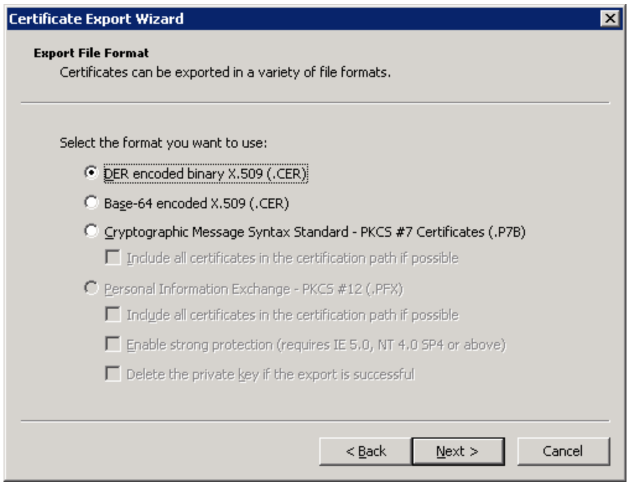
Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Certificate export wizard - don't export private key

6. Leave the radio button on *No, do not export the private key* and click Next to open the Export File Format window.



Certificate Export Wizard

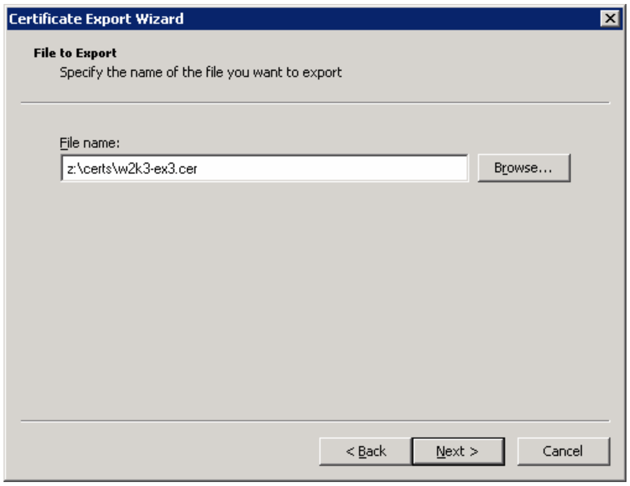
Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
  - □ Delete the private key if the export is successful

Certificate export wizard - export file format

7. Leave the radio button on *DER encoded binary X.509 (.CER)* and click Next to open the File to Export window.



Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name: z:\certs\w2k3-ex3.cer

Certificate export wizard - file name

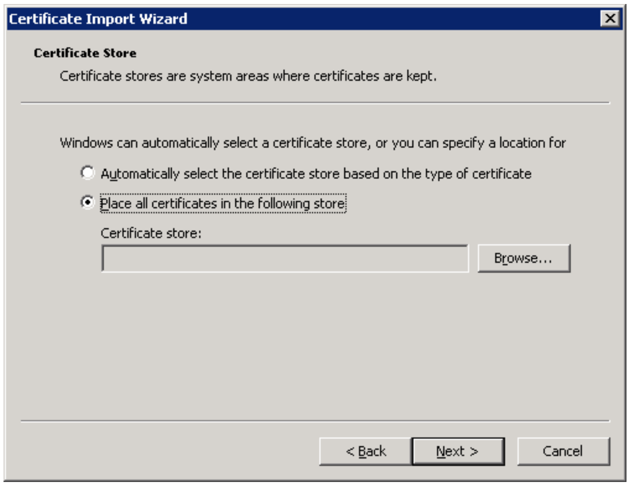
8. Save the file in a convenient location that's accessible from the Outlook client desktop. There are no secrets in this certificate, so you don't need to worry about leaving it on the drive.

Importing the SSL Server's Certificate

You're just about finished. You now need to import the certificate at the client and put it in a special place in the Registry set aside for certificates from trusted sources.

1. Locate the certificate (cer) file in Explorer. (You may need to map a drive to the location where you saved it at the server.)

2. Double-click the file to open the Certificate Import wizard. All the windows in this wizard are self-explanatory except for the Certificate Store window.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

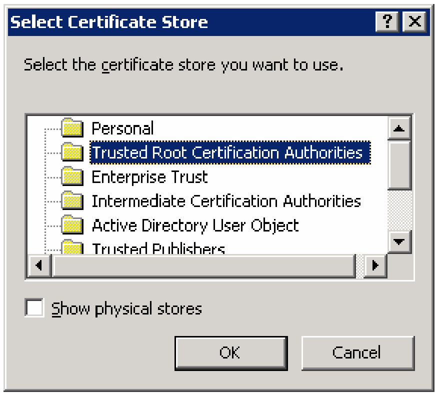
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Certificate import wizard - Certificate Store

3. Select the *Place all certificates in the following store* radio button and click Browse. This opens the Select Certificate Store window.



Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

Certificate import wizard - select cert store - trusted root

4. Select the Trusted Root Certification Authorities folder and click OK.

5. Continue through the remaining windows in the wizard, clicking Next at each window.

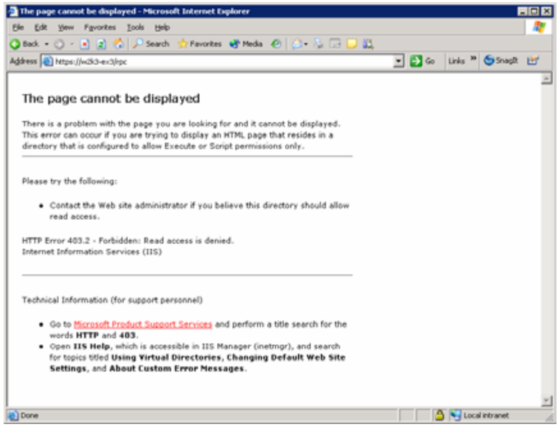
Testing the Certificate Trust

At this point, the client now "trusts" the SSL certificate used by the front-end server. It's time to test the SSL connection from the client to the Exchange front-end server. *Don't skip this step*. If you can't make a clean SSL connection to the server, then Outlook won't be able to make an RPC over HTTP connection.

Open a browser at the client desktop and point it at the Rpc virtual folder on the front-end Exchange server, specifying *https*:// as the connection protocol. Here's an example for a server named W2K3-EX3:

https://w2k3-ex3/rpc

You should get a 403.2 (Forbidden) page in reply. This shows that you made a successful SSL connection and that the Rpc virtual folder is available but it does not permit read access.


The page cannot be displayed - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://w2k3-ex3/rpc
Go Links SnagIt
Done
Local intranet

The page cannot be displayed

There is a problem with the page you are looking for and it cannot be displayed. This error can occur if you are trying to display an HTML page that resides in a directory that is configured to allow Execute or Script permissions only.

Please try the following:

- Contact the Web site administrator if you believe this directory should allow read access.

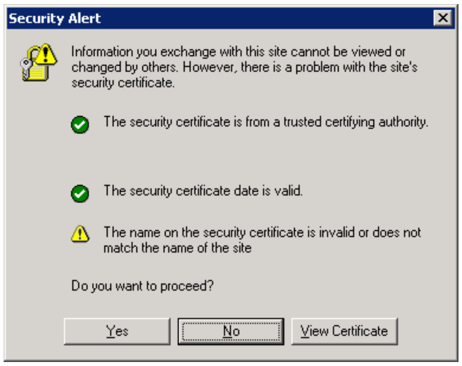
HTTP Error 403.2 - Forbidden: Read access is denied.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **403**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Using Virtual Directories**, **Changing Default Web Site Settings**, and **About Custom Error Messages**.

Browser test succeeds - 403.2 page

If, on the other hand, you get a Security Alert window, then you have a configuration error of some sort.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate is from a trusted certifying authority.

The security certificate date is valid.

The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Security alert - certificate not trusted

The most common error at this point is a warning in the third item, *The name on the security certificate is invalid or does not match the name of the site.* You'll get this error if the name format you specified in the browser does not match the name format in the SSL certificate.

This is very important. **The name format you use in the browser (and in the RPC over HTTP configuration in Outlook 2003) must match the name format in the certificate.** For example, if the server name in the certificate is W2K3-EX3, then you'll get a warning if you specify the Fully Qualified Domain Name (FQDN) in the browser address. The same is true in the opposite situation, where the certificate uses the FQDN and you specify a flat name. (The names are not case sensitive.)

The self-signed certificates generated by SSLDiag use the server's flat name (example, W2K3-EX3), not the fully qualified DNS name (example, w2k3-ex3.exorg.com). If you obtain a certificate from some other source, then the name format in the certificate might be the flat name or the Fully Qualified Domain Name (FQDN). You'll need to look at the certificate to make sure. The certificate viewer in Windows will show the name in the first window.

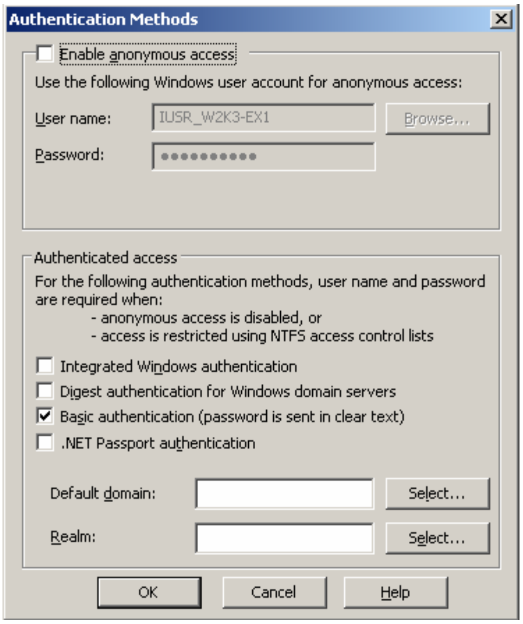
Also, if you plan on using a DNS alias to specify the name of the Exchange server, then you'll need to use the alias name for the SSL certificate.

Configure Web Authentication On Front-End Server

In RPC over HTTP, the Outlook client connects to the World Wide Web service (W3SVC) at the front-end server rather than connecting directly to the Exchange Information Store service. This means that the W3SVC service must authenticate the user before it permits access to the Rpc virtual folder.

The Outlook client connects using SSL, so it's permissible to use Basic authentication for the initial web connection. The plain text password is protected inside the encrypted SSL connection. All other forms of authentication should be disabled for the Rpc service.

1. Open the IIS management console and drill down to the Rpc folder under the Default Web Site. Open the Properties window and select the Directory Security tab.
2. In the Authentication and Access Control area, click Edit to open the Authentication Methods window.



Authentication Methods

☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_W2K3-EX1

Password: ••••••••••

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☑ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

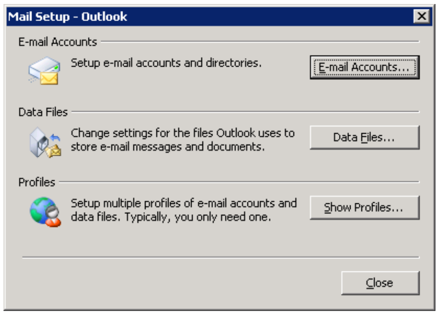
Authentication methods window in IIS

3. Uncheck all options except for *Basic authentication*.
4. Click OK to save the change then close all other IIS management console windows.

Configure Outlook to Use RPC over HTTP Proxy

It's finally time to configure the Outlook client to use RPC over HTTP.

1. Close Outlook if it's open and then open the Mail applet in the Control Panel to configure the account settings.



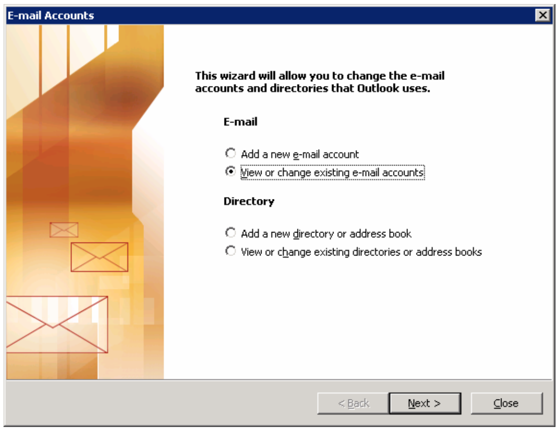
Setup e-mail accounts and directories.

Change settings for the files Outlook uses to store e-mail messages and documents.

Setup multiple profiles of e-mail accounts and data files. Typically, you only need one.

Outlook Mail setup - E-mail accounts

2. Click *E-mail Accounts*. This opens the E-mail Accounts wizard.



This wizard will allow you to change the e-mail accounts and directories that Outlook uses.

E-mail

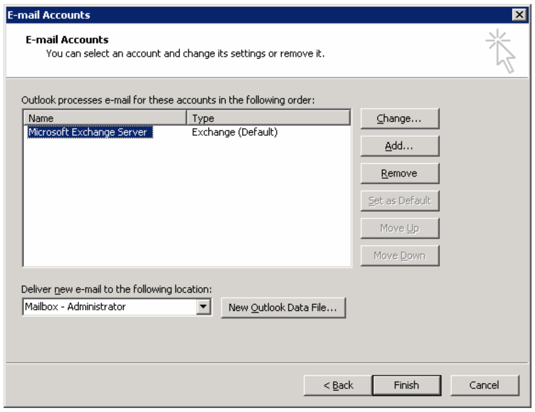
○ Add a new e-mail account
● View or change existing e-mail accounts

Directory

○ Add a new directory or address book
○ View or change existing directories or address books

Outlook Mail setup - view or change existing account

3. Leave the radio button on *View or change existing e-mail accounts* and click Next.



E-mail Accounts

You can select an account and change its settings or remove it.

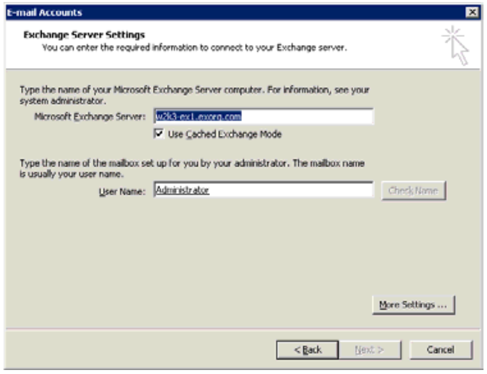
Outlook processes e-mail for these accounts in the following order:

Name	Type
Microsoft Exchange Server	Exchange (Default)

Deliver new e-mail to the following location: Mailbox - Administrator

Outlook E-mail Setup - e-mail accounts

4. Highlight the Microsoft Exchange Server option and click *Change*.



Exchange Server Settings

You can enter the required information to connect to your Exchange server.

Type the name of your Microsoft Exchange Server computer. For information, see your system administrator.

Microsoft Exchange Server: w2k3-ex1.exorg.com

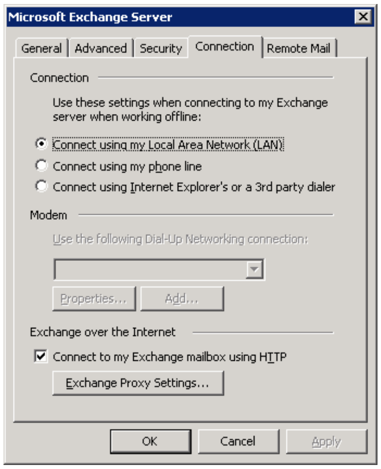
☑ Use Cached Exchange Mode

Type the name of the mailbox set up for you by your administrator. The mailbox name is usually your user name.

User Name: Administrator

Outlook E-mail Setup - Exchange server settings

5. Click the More Settings button in the lower right corner to open the Microsoft Exchange Server window then select the Connection tab.



Connection

Use these settings when connecting to my Exchange server when working offline:

● Connect using my Local Area Network (LAN)

○ Connect using my phone line

○ Connect using Internet Explorer's or a 3rd party dialer

Modem

Use the following Dial-Up Networking connection:

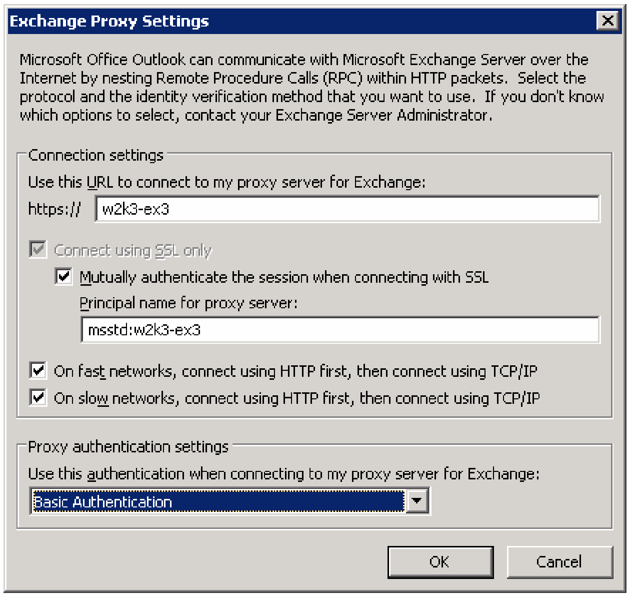
Exchange over the Internet

☑ Connect to my Exchange mailbox using HTTP

Outlook account connection configuration

6. Select the *Connect to my Exchange mailbox using HTTP* option then click Exchange Proxy Settings.

7. You now arrive at one of the most finicky Windows configuration window I've ever encountered. The format for each entry is absolutely critical to the success of the RPC over HTTP connection.



Exchange Proxy Settings

Microsoft Office Outlook can communicate with Microsoft Exchange Server over the Internet by nesting Remote Procedure Calls (RPC) within HTTP packets. Select the protocol and the identity verification method that you want to use. If you don't know which options to select, contact your Exchange Server Administrator.

Connection settings

Use this URL to connect to my proxy server for Exchange:

https:// w2k3-ex3

☑ Connect using SSL only

☑ Mutually authenticate the session when connecting with SSL

Principal name for proxy server:

msstd:w2k3-ex3

☑ On fast networks, connect using HTTP first, then connect using TCP/IP

☑ On slow networks, connect using HTTP first, then connect using TCP/IP

Proxy authentication settings

Use this authentication when connecting to my proxy server for Exchange:

Basic Authentication

Exchange proxy settings in Outlook

8. For the setting titled *Use this URL to connect to my proxy server for Exchange*, enter the name of the front-end server. If the SSL certificate contains a flat name, then enter the flat name. If the SSL certificate contains an FQDN, then enter the FQDN. You've already verified the name using a browser, so enter the same format.

9. Leave the *Connect Using SSL Only* option selected. Exchange will reject any attempt to use simple HTTP to connect to the front-end server, even if you configure the Rpc virtual server to accept non-SSL connections.

10. Check the option titled *Mutually authenticate the session when connecting with SSL.* This assures that the client trusts the SSL certificate. The format for the entry is:

    msstd:servername

    The msstd: identifies a special RPC handler. Don't put a double-slash after the colon. Use the same name format that you used in the previous field.

11. The next two options work together. Under normal circumstances, you would leave the option titled, *On slow networks, connect using HTTP first, then connect using TCP/IP*, checked and the partner entry unchecked. However, for testing, select both options so you can view the connection while you're at your workbench.

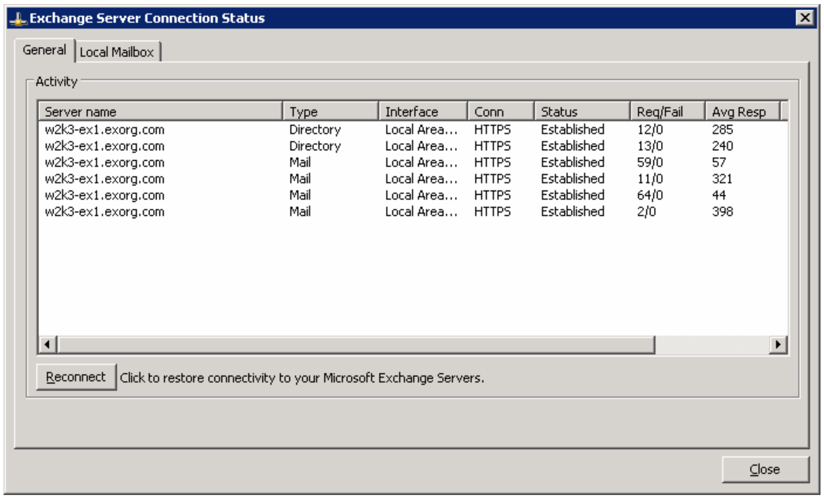
12. In the Proxy Authentication Settings field, select Basic Authentication. This parallels the configuration option you selected for the Rpc virtual folder.

13. Click OK to save the changes then close the rest of the windows.

14. Launch Outlook. After a few seconds, you'll be prompted for credentials. Enter your user name in the domain\name format.

When the Outlook window opens, the status notifications in the lower right corner should eventually show *Connected*. If you stay disconnected, then you have a problem with the configuration.

Take a look in the Notification Area (formerly known as System Tray) for the Outlook icon. Hold the Ctrl key down, click the icon, and select Connection Status from the menu.



Server name	Type	Interface	Conn	Status	Req/Fail	Avg Resp
w2k3-ex1.exorg.com	Directory	Local Area...	HTTPS	Established	12/0	285
w2k3-ex1.exorg.com	Directory	Local Area...	HTTPS	Established	13/0	240
w2k3-ex1.exorg.com	Mail	Local Area...	HTTPS	Established	59/0	57
w2k3-ex1.exorg.com	Mail	Local Area...	HTTPS	Established	11/0	321
w2k3-ex1.exorg.com	Mail	Local Area...	HTTPS	Established	64/0	44
w2k3-ex1.exorg.com	Mail	Local Area...	HTTPS	Established	2/0	398

Reconnect
Click to restore connectivity to your Microsoft Exchange Servers.
Close

Outlook connection status

The Connection Type column should show HTTPS for each connection. If it shows TCP/IP, you may have forgotten to select the option to use HTTP for high speed networks. You also might have not completely configured SSL, in which case a locally connected client will fall back on TCP/IP.

Notice that the Directory connections appear to originate at the back-end e-mail server. That's an artifact of the way the front-end server proxies NSPI requests.

And in the end…

If you just can't get the darned thing to work no matter what you do, e-mail me with your symptoms. I'm putting together a FEP (Frequently Encountered Problem) list for RPC over HTTP and once we work together to figure out the problem, I'll add it to the list.

Good luck and happy messaging…

Windows® and Exchange® are trademarks of Microsoft, Inc.