Configuring RPC Over HTTP

Because email has grown to be one of the primary methods of business communication, enabling users to access their email remotely has become a priority. With an updated version of Outlook Web Access (OWA), users have a rich email client that is approaching the full set of features and functionality found in Outlook 2003. However, some features are available only in the full Outlook client.

The good news is that with Exchange 2003 and Remote Procedure Call (RPC) over HTTP, you can allow remote users to use the full Outlook 2003 client to access their email without setting up a VPN or other facility.

RPC is one of the protocols that Exchange supports for client connections. To use RPC over HTTP, you need to configure one of your Exchange front-end servers to act as an RPC proxy server.

You can then expose this server to the outside world and allow users to connect through it. Alternatively, you can use Microsoft ISA Server to route requests through your firewall or perimeter network.

MICROSOFT ISA SERVER
For more information on installing and configuring Microsoft ISA Server, check out `http://www.microsoft.com/isa`.

Outlook 2003 supports RPC over HTTP. However, you need to upgrade your user's operating system to Windows XP, SP1 and apply Windows Update 331320 (available from `windowsupdate.microsoft.com`) to use this feature.

To configure RPC over HTTP using your existing Exchange front-end servers, follow these steps:

1. From the Control Panel, select Add/Remove Programs and then Add/Remove Windows Components. From Networking Services, install the RPC over HTTP protocol.
2. In the IIS Manager, locate the RPC virtual directory and select its properties from the shortcut menu.
3. Open the Directory Security property page and edit the Authentication and Access Control settings to select Basic Authentication.
4. Edit the registry and locate the HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\RpcProxy key.
5. Modify the ValidPorts key and add the following identifiers and ports, separated by a semicolon as shown here:

```
ExchangeServer:593;
ExchangeServerFQDN:593;
ExchangeServer:6001-6002;
ExchangeServerFQDN:6001-6002;
ExchangeServer:6004;
ExchangeServerFQDN:6004;
GlobalCatalogServers:593;
GlobalCatalogServersFQDN:593;
GlobalCatalogServer:6004;
GlobalCatalogServerFQDN:6004
```

CONFIGURING PORTS

Replace the previous placeholders with the name and fully qualified domain name of the servers in your Exchange topology.

6. On your Global Catalog Server, edit the registry and locate the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters key.
7. Add a new key (multistring) and name it `NSPI interface Protocol Sequences`.
8. Modify the key you have just created and add the value `ncacn_http:6004`.

To configure Outlook 2003 to communicate via RPC over HTTP, follow these steps:

1. From the Control Panel, open the Mail control panel. Then create a new profile.
2. Add a new email account, selecting Exchange as your server type. Enter the name of your Exchange back-end server (*not* your Exchange front-end server).
3. Click the More Settings button and select the Connection property page. Then select the option Connect to My Exchange Mailbox Using HTTP.

4. Select the Exchange Proxy Settings property page. Under Connection Settings, enter the name of your Exchange front-end server in the text box marked Use This URL.

5. Check the options for Connect Using SSL Only and Mutually Authenticate.

6. In the text box marked Principle Name for Proxy Server, enter the fully qualified domain name of your Exchange front-end server, prefixed by `msstd:` (that is, `msstd:exch.orion`.com).

7. Change Proxy Authentication Settings to use basic authentication.

Your Outlook client is now ready to communicate with Exchange using RPC over HTTP.

WORKING WITH MICROSOFT ISA SERVER

Microsoft ISA Server can be implemented alongside Exchange to increase security in two critical areas. The first area is RPC over HTTP, which was already examined. You can place an ISA Server within the demilitarized zone (DMZ) or outside your firewall to handle RPC requests, and route these requests back to your Exchange front-end servers.

Second, for securing OWA implementations, you can configure ISA as a proxy to an Exchange front-end server, eliminating the need to expose a front-end server to the rest of the world. Using ISA Server, you can use a special publishing wizard for OWA to configure a proxy to your Exchange front-end servers. This eliminates the need to open multiple ports to the outside world and provides a more secure implementation method for OWA.