[**Editor's Note:** The following content was excerpted from the free eBook *The Tips and Tricks Guide to Securing Windows Server 2003* (Realtimepublishers.com) written by Roberta Bragg and available at http://www.netiq.com/offers/ebooks.]

Q: We do not allow users to store data on their hard drives. They are provided a place on a file server. I can protect this area with discretionary access control lists, but how do I protect data during transport from client to file server?

A: There are several ways to secure data in flight, including using virtual private networks (VPNs), IPSec, and the Secure Sockets Layer (SSL). VPNs are usually the methodology of choice when transferring data across the WAN, while transport-mode IPSec, explained in Question 8.5, is preferred for transferring files on the LAN. However, another methodology exists for protecting files in transport on the intranet, WebDAV over SSL.

WebDAV is the Microsoft implementation of the Distributed Authoring and Versioning extension to HTTP/1.1. You can read about DAV in Request for Comments (RFC) 1518. It was originally designed as an alternative to using FTP to publish files to a Web server, but can also be used as an alternative to SMB. If the Web client is installed, Internet Explorer (IE), Microsoft Office applications, and the Windows Desktop can be used to read and write files to a WebDAV-enabled folder. Office applications can also directly open files from and save files to the Web folder, much as they would use a regular local folder or shared folder on a file server. To use WebDAV securely requires securing the IIS Server, the Web folders and the Web site that hosts them. Our focus here is securing data in flight, but we'll start with a secure implementation of WebDAV.

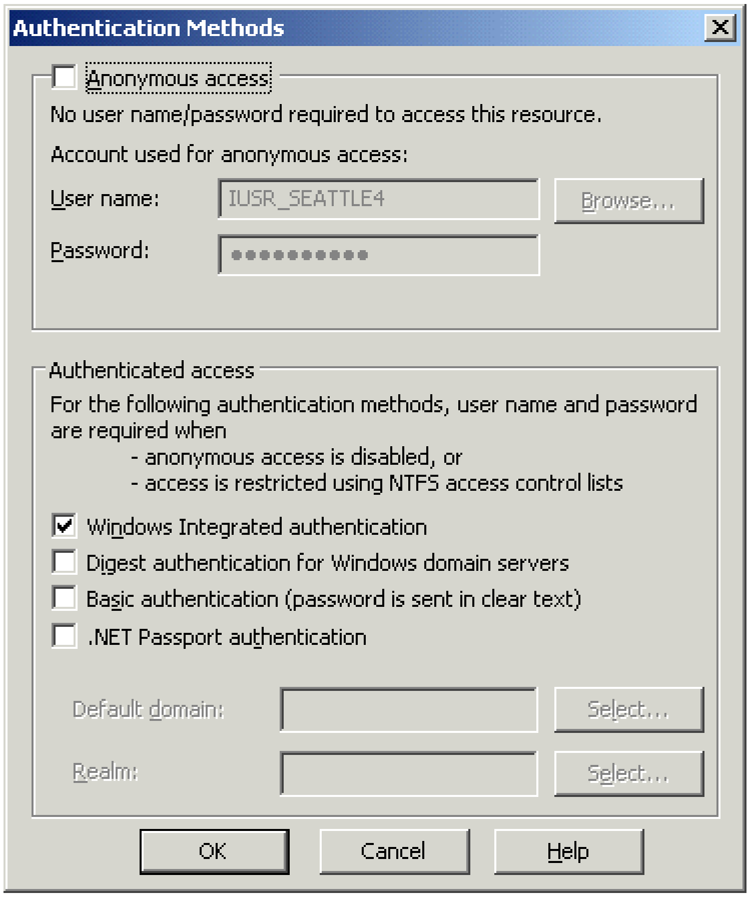
To use WebDAV in Windows Server 2003, you must WebDAV enable the IIS 6.0 Web server and create Web folders on it. (Web folders and WebDAV can also be used with IIS 5.0 and Windows 2000—Win2K.) Then, using the Web client, files can be transferred from the client computer to the Web folder using HTTP. No file share is necessary on the Web server. WebDAV itself does not provide any mechanism for protecting data in transport. However, you can protect data during transfer to the Web folders by establishing and using SSL—after authenticating the connection with the Web server, all data is encrypted during transport. Files saved in the WebDAV folders are not encrypted.

Preparing and Securing Web Folders for WebDAV

First, you must enable WebDAV, create and secure the Web folder. To do so, create a folder on the Web server, and apply NTFS file permissions to limit its access to the Windows groups that should use it. This first folder will be the location for the Web site. Next, open the Internet Information Services Console, right-click the Default Web Site (or Web site you have created), and select New, then Virtual Directory. Click Next on the New Virtual Directory Creation Wizard Welcome page. Give the virtual directory an alias to be used for accessing it (for this example, I'll name it Stuff), then click Next. Enter the path to the new folder or use the Browse button to browse to its location, then click Next. Set folder permissions.

Because this folder will be the root for the WebDAV folders, you might want to set it with run scripts and read permission. I added write permission so that approved users can save files to the folder, and browse (Directory Browsing) so that users can see the files that are stored there. The appropriate permissions to set will depend on your implementation. You might not want, for example, users to see the files available or you might even want users to only be able to write files but not read them. Keep in mind these are virtual directory folder permissions. The underlying NTFS permissions further control who can do what with the files.

Click Next, then click Finish to complete the creation of the virtual directory. Set authentication. On a static Web server, anonymous connections are allowed; however, they are not a good idea when enabling folders for WebDAV. No one should be allowed to access a Web folder for reading or writing without proper identification. A good choice for Web-based authentication on the intranet is Windows integrated (see Figure 2.10). The dialog box that Figure 2.10 shows can be located on the property pages of the Web site. It is reached by clicking Edit at the top of the Directory Security page. Basic authentication means passwords are passed in the clear, which might be OK if you will also use SSL.



Authentication Methods

□ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

User name: IUSR_SEATTLE4

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

☑ Windows Integrated authentication

□ Digest authentication for Windows domain servers

□ Basic authentication (password is sent in clear text)

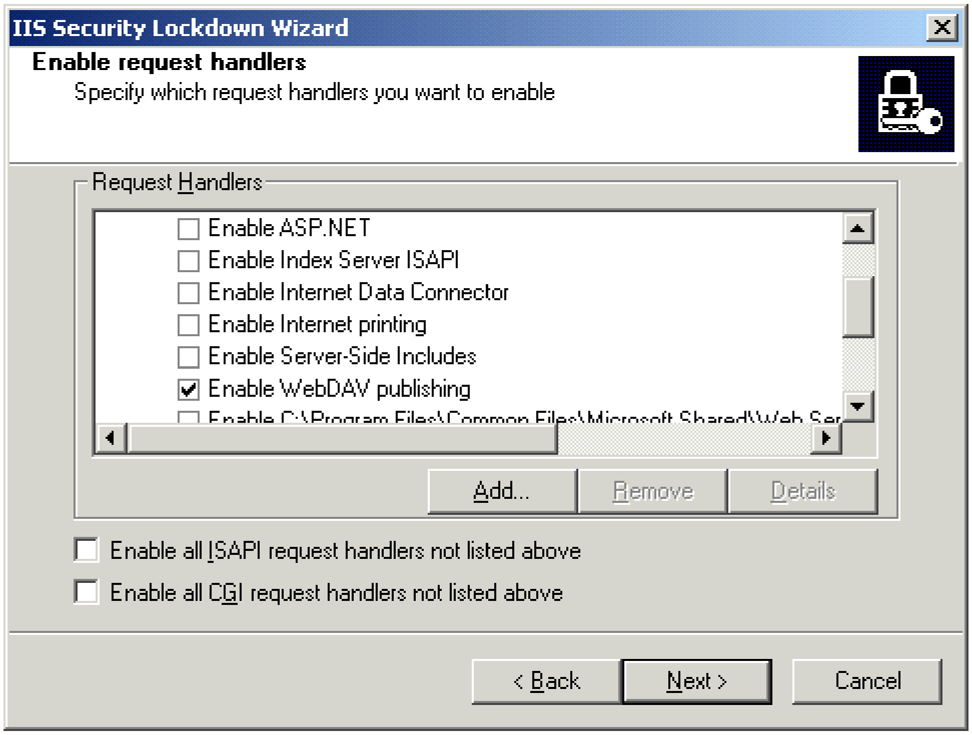
□ .NET Passport authentication

Default domain:

Realm:

Figure 2.10: Set authentication methods.

Next, enable WebDAV by right-clicking in the IIS console on the local computer, and selecting Security. Doing so runs the IIS Security Lockdown Wizard. Click Next twice to advance to the Enable Request Handler's page. Scroll down and select the Enable WebDAV Publishing check box, as Figure 2.11 shows, click Next, then click Finish to complete the wizard.



IIS Security Lockdown Wizard

Enable request handlers

Specify which request handlers you want to enable

Request Handlers

- ☐ Enable ASP.NET
- ☐ Enable Index Server ISAPI
- ☐ Enable Internet Data Connector
- ☐ Enable Internet printing
- ☐ Enable Server-Side Includes
- ☑ Enable WebDAV publishing
- ☐ Enable C:\Program Files\Common Files\Microsoft Shared\Web Ser

☐ Enable all ISAPI request handlers not listed above

☐ Enable all CGI request handlers not listed above

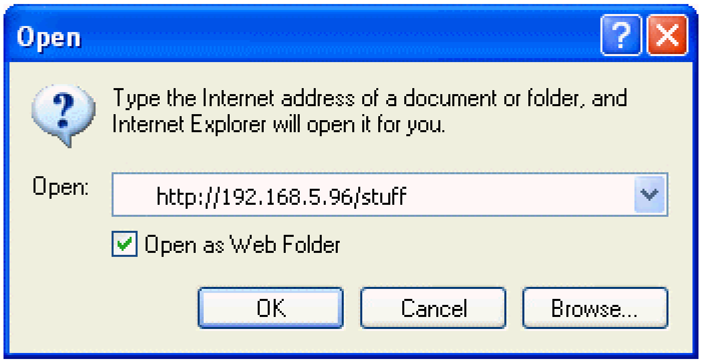
Figure 2.11: WebDAV is disabled by default. To enable it, run the Security Lockdown Wizard.

The WebDAV ISAPI request handler is not enabled by default to prevent its malicious use. Before you enable WebDAV, you should thoroughly consider the additional risk it entails. Remember, WebDAV enables access to documents using Microsoft Office, many versions of IE, and other products that meet the HTTP/1.1 WebDAV specification. It does so over port 80. Therefore, unlike file sharing, which can be blocked at the firewall, WebDAV manipulation of this data can be accomplished across a port commonly open on the firewall. If your intention is to allow such access, you must ensure that other controls are in place. If you will merely be using WebDAV on your intranet, you must still take the appropriate action to block external access to port 80 of the WebDAV-enabled IIS server on your internal network. Security controls for WebDAV are summarized later.

Before setting up SSL, it's wise to test the Web folder for accessibility. To do so, make sure that your Windows XP client has the Web Client service enabled and started (you can check and also enable it if it is disabled by going to the Start menu, selecting Administrative Tools, then selecting Services). You will also need the appropriate URL. For this example, I used the IP address of the Web site, followed by the alias assigned to the virtual directory. Then, to test, try one of these options:

- Any Office product should be able to save or open files saved to the Web folder as if the folder existed on the local hard drive. Instead of using a local drive path or mapping a network drive, simply save to My Network Places, and select the correct Web folder or type the URL.
- Open My Computer, and select My Network Places, double-click *Add a new Network Place*, and enter the URL. A file can be dragged from the desktop or Explorer window to the Web folder.

- Open IE, from the File menu select open, input the URL, and select the *Open as a Web folder* check box. A file can be dragged from the desktop or Explorer window to the Web folder (see Figure 2.12).



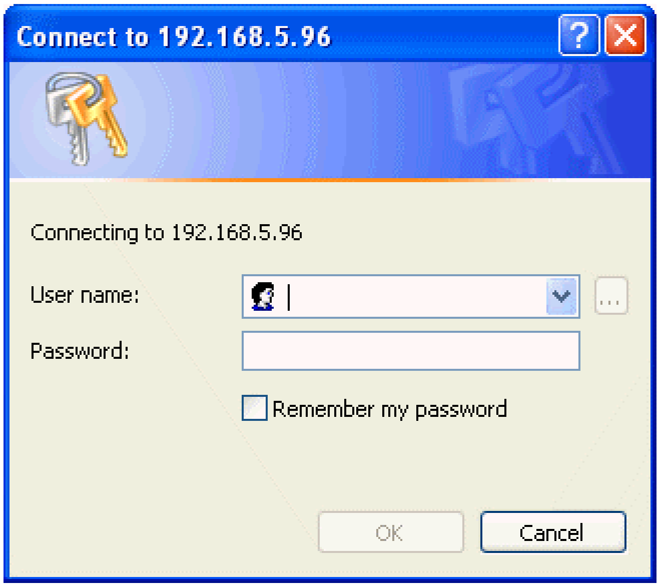
Type the Internet address of a document or folder, and Internet Explorer will open it for you.

Open: http://192.168.5.96/stuff

☑ Open as Web Folder

Figure 2.12: Use the IE File menu's Open dialog box to open a Web folder.

If your logon does not match the NTFS permissions set on the underlying folders, you will be prompted for a user ID and password, as Figure 2.13 shows.



Connecting to 192.168.5.96

User name:

Password:

□ Remember my password

Figure 2.13: The site doesn't allow anonymous connection, so you might need to enter a user ID and password.

Using SSL to Transfer Files to Web Folders

Setting up SSL for use with Web folders is simple and straightforward. The basic process is the same as for setting up SSL for other purposes. You must decide where the certificate should come from and where it should be installed? Because our example is an intranet Web site, the steps which follow obtain the certificate from an internal Windows Server 2003 Certificate Authority (CA). If you choose, you might obtain a certificate from one of the commercial CAs.

IIS offers several locations where the certificate might be installed. It can be installed at the Web site level, and all connections to the Web folders can be required to use SSL. It can be installed on a Web folder. In this manner, connections elsewhere on the site do not have to use SSL. It can also be installed at a subfolder level. Our example consists of a Web site set up specifically for WebDAV, so the certificate will be installed at the Web site level.

To require SSL for Web folder access, you must request a certificate, install it, and require SSL. To request a certificate, in the Internet Information Services console, right-click the Web site, and select Properties, then select the Directory Security tab. Click Server Certificate in the Secure Communications area of the page, click Next on the wizard welcome page, select *Create a new Certificate*, and click Next. Select *Send the Request immediately to an on-line certification authority*, and click Next. (If you must obtain your certificate from a third-party CA, you will need to create a request for forwarding to the authority, then install the certificate when you receive it.)

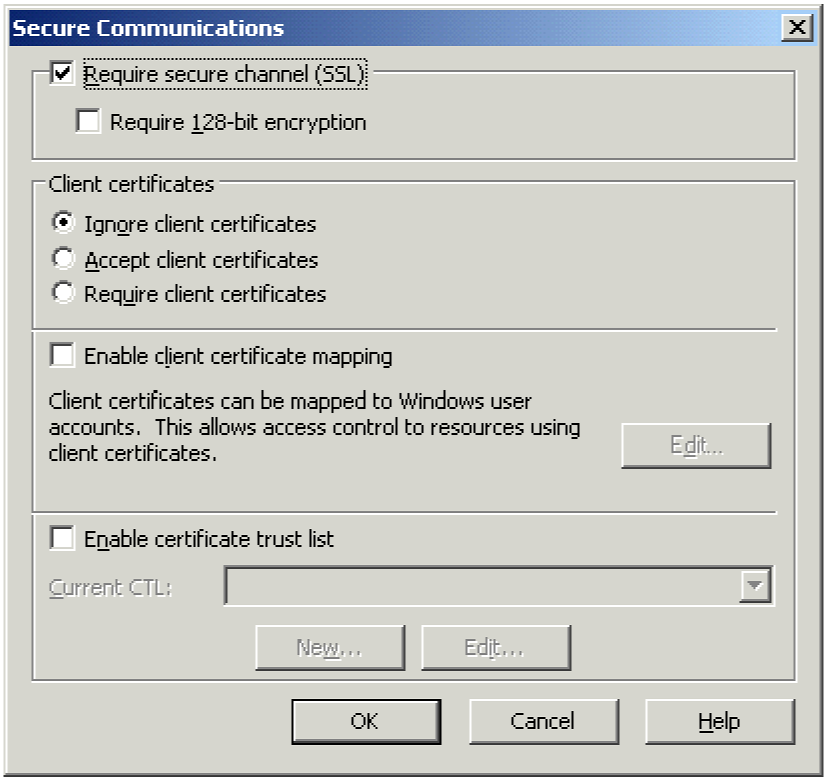
Next, you'll need to enter a name for the new certificate. Change the bit length if you desire stronger security. In general, the longer the bit length of the key, the better the security but the worse the performance. Click Next. Enter the legal name of the organization in the Organization text box, enter the departmental name in the organizational unit (OU) text box, and click Next. The NetBIOS name of the site (the server name) will appear in the Common Name text box. You might replace it with the fully qualified domain name (FQDN) or, because this is strictly planned for intranet access, leave the NetBIOS name. In this example, the FQDN was entered. Click Next.

In the next step, enter the city and state location of the Web server, and click Next. Select a CA, then click Next. All online CAs should be available in the drop-down box. Review the settings on the Certificate Request Submission, and click Next. Click Finish on the notice that the certificate has been installed, select the Web Site tab, enter the port number for SSL (the standard port number is 443), and click Apply.

Return to Directory Security page, and click Edit in the Anonymous Access and Authentication Control section. Change authentication method to Basic Authentication if desired. The SSL connection will occur before authentication and thus the entered user ID and password will be encrypted.

Click View Certificate to review the certificate details and verify that a Web Server certificate has been installed. The designation of the type of certificate is found by examining the Certificate Template Name on the Details page. The specified use of the certificate—Server Authentication—can be found on the General page. Click OK to close the view, then click OK to close the properties page.

After the certificate is installed, HTTPS can be used to access the server and ensure encryption of the entire communication between the client and the server. However, ordinary HTTP can also be used. To ensure that all communication is encrypted, you must configure the Web server to only accept SSL. To do so, return to the Directory Security properties page for the Web site, click Edit on the Secure Communications section of the page, and on the Secure Communications dialog box, select Require Secure Channel. If all clients are capable of 128-bit encryption, select this option as well (see Figure 2.14). Click OK to close the window and apply the setting. Now all clients will be required to use HTTPS to connect.



☑ 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.

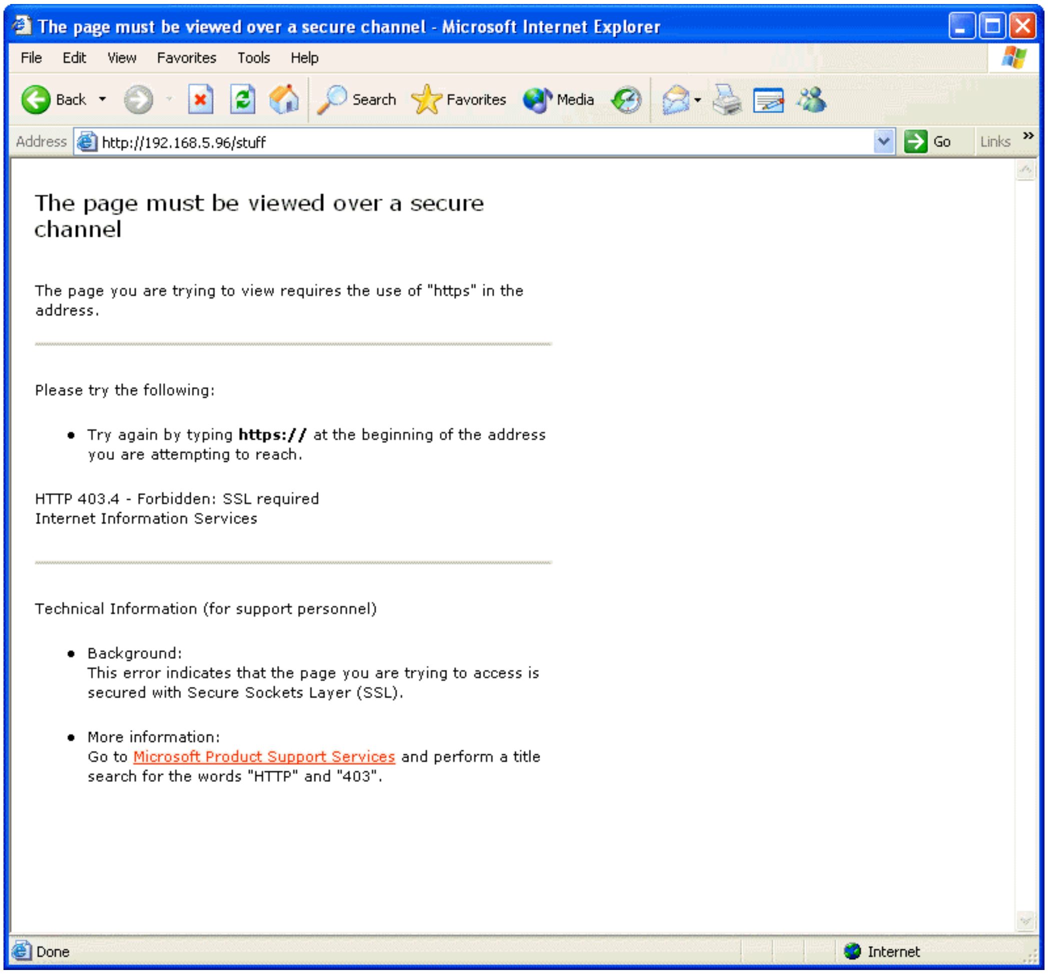
□ Enable certificate trust list

Current CTL:

Figure 2.14: Require SSL, as clients will not remember to request it.

Click OK to close the Properties pages. To test, return to the client and enter the URL to access the Web folder. If you use HTTP, it will not work and provide an error message. Modify the URL to use HTTPS and access is allowed. Note that the failure came before the request to enter a user ID and password, thus showing that the SSL connection will occur before logon. Even use of the basic authentication clear-text password will actually be encrypted when using SSL.

Be sure to retest connections using HTTPS. If you forget, you will be warned, as Figure 2.15 shows.


The page must be viewed over a secure channel - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
http://192.168.5.96/stuff
Go
Links
Done
Internet

The page must be viewed over a secure channel

The page you are trying to view requires the use of "https" in the address.

Please try the following:

- Try again by typing **https://** at the beginning of the address you are attempting to reach.

HTTP 403.4 - Forbidden: SSL required
Internet Information Services

Technical Information (for support personnel)

- Background:
  This error indicates that the page you are trying to access is secured with Secure Sockets Layer (SSL).
- More information:
  Go to Microsoft Product Support Services and perform a title search for the words "HTTP" and "403".

Figure 2.15: If properly configured, any attempt to access the Web folders without using HTTPS will fail.

Fortunately, entering HTTPS and repeating the operation will get you to the Web folder, as Figure 2.16 shows.

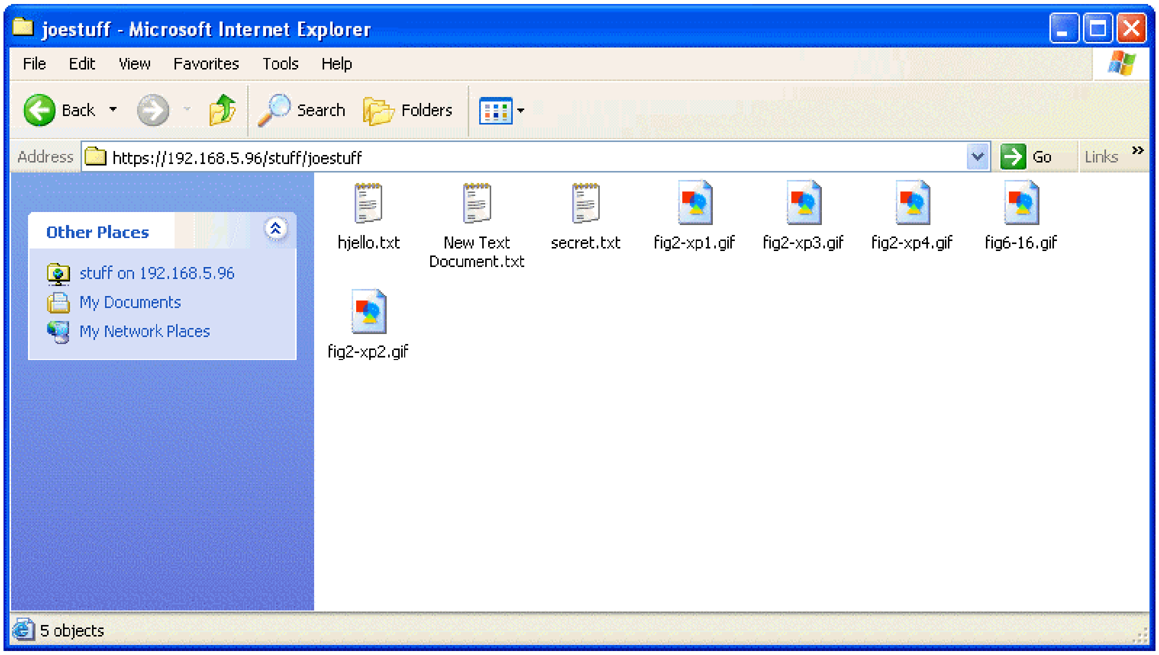


Figure 2.16: After authentication, the Web folder is ready for use in reading and saving files.

> When securing your Web folders with SSL, it is wise to understand that a certificate used by this purpose must be from a trusted CA or you will receive warnings when first attempting access. On an intranet using an internal CA, it is likely that trust of the CA, and thus the certificate issued for the Web server, will already be established. However, if a Windows Server 2003 standalone CA is used, or if clients not joined in the domain of an Enterprise CA are used, you might need to acquire a copy of the CA certificate and place it in the Certificate store of the client system. You can do so during the first access to the Web server, if users are properly instructed.

[**Editor's Note:** This content was excerpted from the free eBook *The Tips and Tricks Guide to Securing Windows Server 2003* (Realtimepublishers.com) written by Roberta Bragg and available at http://www.netiq.com/offers/ebooks.]