Xerox Multifunction Devices

Customer Tips

dc07cc0420
June 5, 2007

... for the user

Xerox Network Scanning – HTTP/HTTPS Configuration using Microsoft IIS

This document applies to these Xerox products:

X	**WC Pro 232/238/245/ 255/265/275**

Purpose

This document contains the procedure to configure a Xerox multifunction device and an internet server using IIS (Internet Information Services) to enable network scanning using the HTTP and HTTPS protocols.

Background

HTTP (Hypertext Transfer Protocol) is an industry standard protocol that enables the exchange of information over the internet. HTTPS (Hypertext Transfer Protocol Secure) is the secure version of the HTTP protocol that allows for secure data transfer using SSL (Secure Socket Layer).

Configuring the Xerox multifunction device for network scanning using HTTP/HTTPS

Verify Device Settings via Configuration Report

At the WorkCentre/Pro

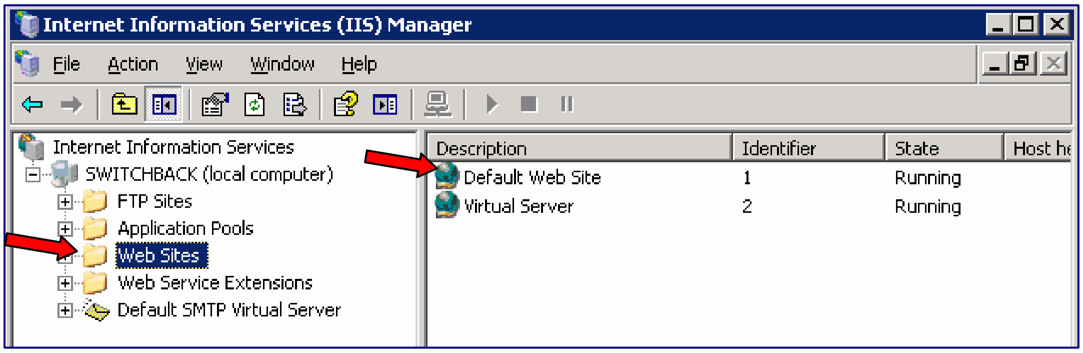
1. Press the **[Machine Status]** button.
2. Touch the **[Print Reports]** button.
3. Touch the **[Configuration Report]** button.
4. On the configuration report verify that within the:
   - **TCP/IP Settings** section that **TCP/IP** is **Enabled**, that a **Host Name** has been entered, and an **IP Address** exists.
   - **DNS Setting** section that a Domain Name exists.
   - **HTTP Setting** section that HTTP or HTTPS is enabled. ***(To enable HTTPS on the WorkCentre/Pro see the 'Enabling HTTPS' section on page 6.)***

ⓘ ***Retain the Configuration Report as the IP address will be used in subsequent steps.***

On the Web Server

1. On the web server create a folder that will be used as the scan repository. Even though we will be using C:\Scans in this example, the repository can reside anywhere on the server.

2. Within IIS Manager ensure that the ‘Default Web Site’ is running. Note the IP address or host name of the server as you will need that information in subsequent steps.

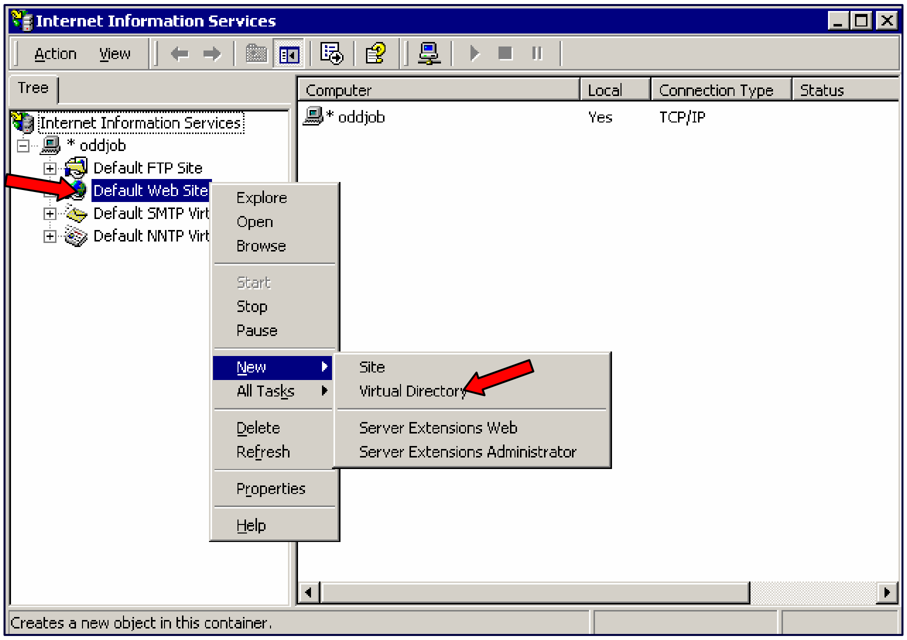

Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
SWITCHBACK (local computer)
FTP Sites
Application Pools
Web Sites
Web Service Extensions
Default SMTP Virtual Server

Description	Identifier	State	Host he
Default Web Site	1	Running	
Virtual Server	2	Running	

3. Create a Virtual Directory within IIS Manager by doing the following:

   a. Open IIS and right click on the ‘Default Web Site’ and select **[New, Virtual Directory]**.

   b. The Virtual Directory Creation Wizard will appear. Click **[Next]**.



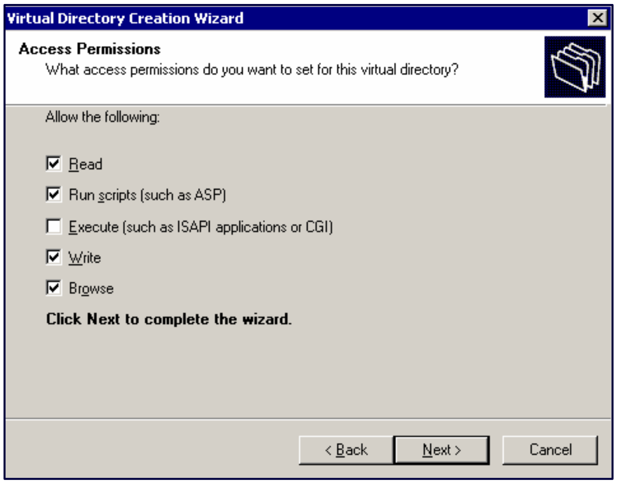
Computer	Local	Connection Type	Status
* oddjob	Yes	TCP/IP	

Creates a new object in this container.

   c. In the Virtual directory Alias window enter an ‘Alias’ name and click **[Next]**.

   d. In the Web Site Content Directory window browse to the folder that was created in step 2 and click **[OK, Next]**.

e. In the Access Permissions window check **[Read, Run Scripts, Browse, Write]**, ensure that Execute is NOT selected.



Virtual Directory Creation Wizard

Access Permissions

What access permissions do you want to set for this virtual directory?

Allow the following:

☑ Read

☑ Run scripts (such as ASP)

☐ Execute (such as ISAPI applications or CGI)

☑ Write

☑ Browse

Click Next to complete the wizard.

f. Click **[Next, Finish]**.

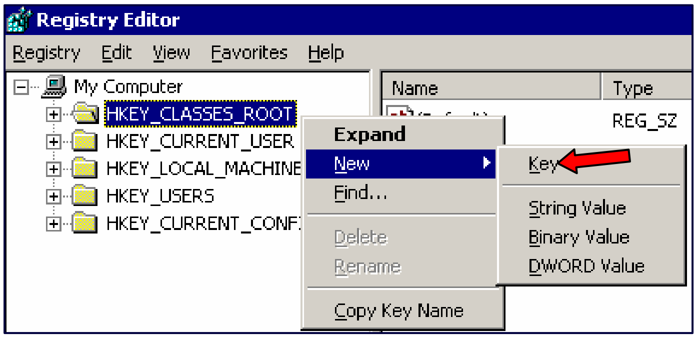
4. Create a MIME type for the file type **.xst** within the Windows Registry

   (Warning: Serious problems might occur if the registry is modified incorrectly.)

   a. Open the registry editor by selecting **[Start, Run]** and type **regedit**, click **[OK]**.

   b. Right click on [**HKEY_CLASSES_ROOT]**.

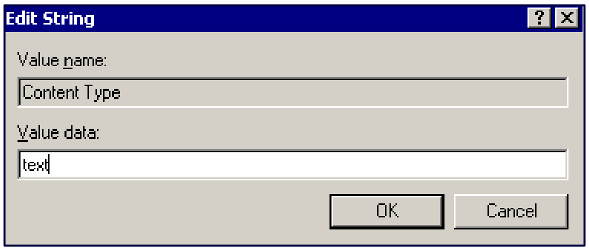
   c. Select **[New, Key]** and rename it to **[.xst]** (include the leading dot) and click anywhere on the screen to save the changes.



   d. Right click on the new key and select **[New, String Value]**.

   e. Rename the new string value to **[Content Type]** and click anywhere on the screen to have the changes take hold.

   f. Right click on **[Content Type]** and select **[Modify]** and type **[text]** in the Value Data type field, click **[OK]** and close the regedit window.

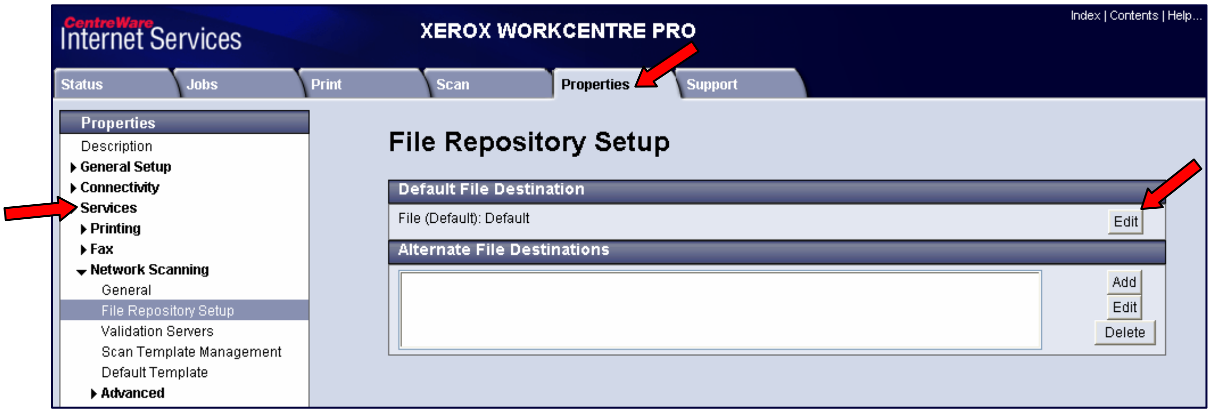


Edit String

Value name: Content Type

Value data: text

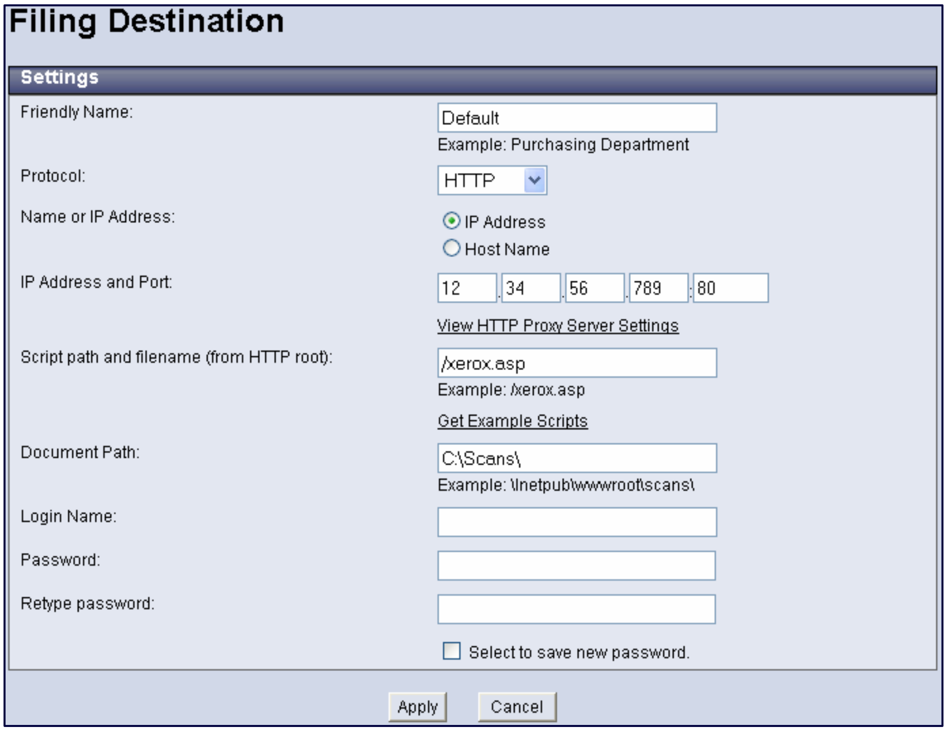
5. In your web browser enter the IP address of the WorkCentre/Pro that you want to configure which will cause the Xerox CentreWare Internet Services site to appear.



File (Default): Default

6. Select the ‘Properties’ tab then **[Services, Network Scanning, File Repository Setup]**.

7. In the Default File Destination section click **[Edit]** which will cause the ‘Filing Destination’ page to appear.



Friendly Name: Default
Example: Purchasing Department

Protocol: HTTP

Name or IP Address: ● IP Address ○ Host Name

IP Address and Port: 12 . 34 . 56 . 789 : 80

Script path and filename (from HTTP root): /xerox.asp
Example: /xerox.asp

Document Path: C:\Scans\
Example: \Inetpub\wwwroot\scans\

Login Name:

Password:

Retype password:

□ Select to save new password.

8. *Optional:* Within the ‘Filing Destination’ window enter a name in the ‘Friendly Name’ field to describe the destination.

9. Select HTTP or HTTPS in the **[Protocol]** pull-down menu.

10. Select either **[Host Name]** or **[IP Address]** and enter the associated information in the field below.

11. In the **Script path and filename (from HTTP root)** section select **[Get Example Scripts]**

12. In the Filing Destination window choose a file that corresponds with the scripting language supported on your server. In this example we will be using ASP.

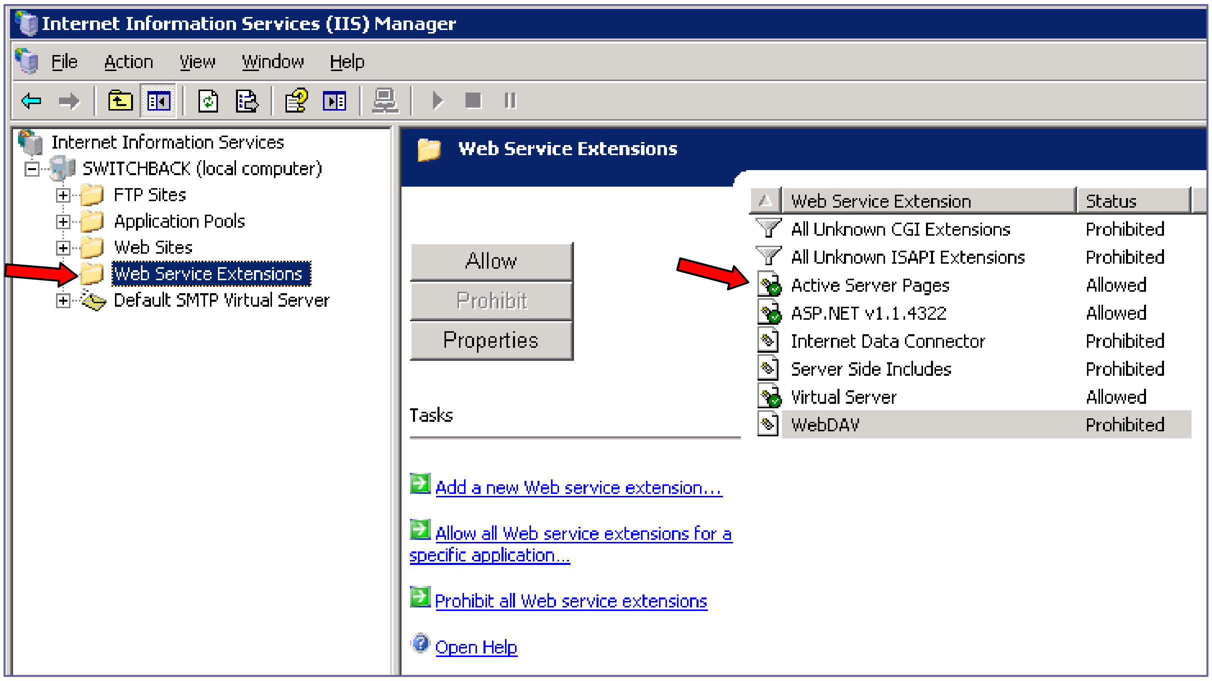
13. Download the chosen file to the <Web Root> directory and extract the file. In this example we will be using the IIS default location which is at C:\Inetpub\wwwroot

14. Enter the path to chosen script, starting at the web root. For example, **C:\wwwroot\xerox.asp** would be entered as **/xerox.asp**.

15. In the Document Path field enter the full path to the location of the scan folder which was created in step 2. In this example it is C:\Scans\.

16. Click **[Apply]** to accept the changes and enter a valid administrator **[User Name]** and **[Password]**. The default is **[admin]** and **[1111]**

Note: Before using an 'Active Server Pages' (.asp) script with version 6 and higher of IIS, 'Active Server Pages' must be allowed within IIS.


Internet Information Services (IIS) Manager
File
Action
View
Window
Help
Internet Information Services
SWITCHBACK (local computer)
FTP Sites
Application Pools
Web Sites
Web Service Extensions
Default SMTP Virtual Server
Web Service Extensions
Allow
Prohibit
Properties
Tasks
Add a new Web service extension...
Allow all Web service extensions for a specific application...
Prohibit all Web service extensions
Open Help

Web Service Extension	Status
All Unknown CGI Extensions	Prohibited
All Unknown ISAPI Extensions	Prohibited
Active Server Pages	Allowed
ASP.NET v1.1.4322	Allowed
Internet Data Connector	Prohibited
Server Side Includes	Prohibited
Virtual Server	Allowed
WebDAV	Prohibited

Scanning a Document

1. At the device, touch **[All Services, Network Scanning]**, then select the desired template. In this example, choose the **[Default]** template.

2. Push **[Start]** on the WorkCentre/Pro. The scan will be delivered to the folder created in step 2.

3. If you receive an error, please verify that you have performed all the steps in the procedure accurately.

Enabling HTTPS

Creation of a Device Digital Certificate

To enable HTTPS on a device, it needs to have its own digital certificate. When clients make a request to the device, it exports the certificate to provide an encrypted channel.

There are two options available to obtain a server certificate for the device:

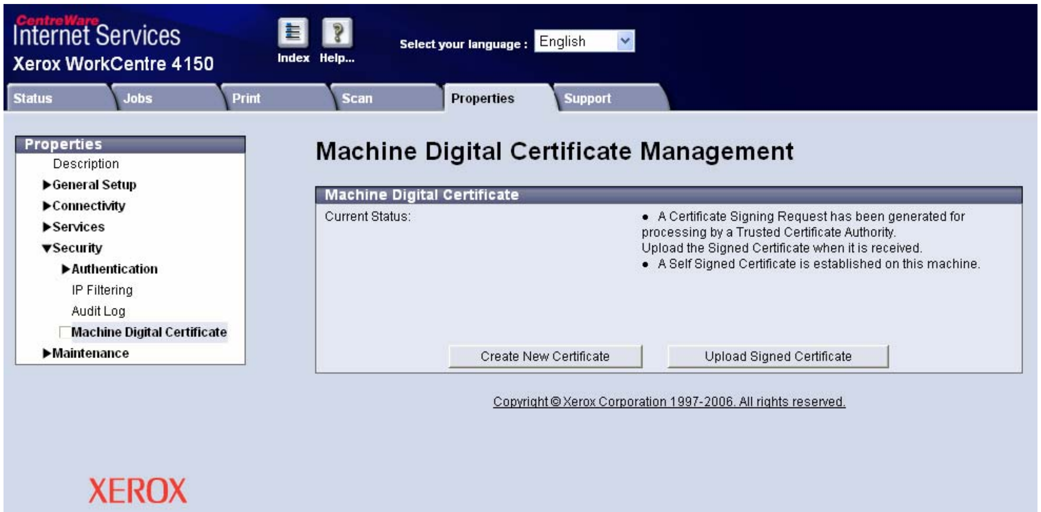
- **Have the device create a Self Signed Certificate**
  - A self signed certificate means that the device signs its own certificate as trusted and creates the public key for the certificate to be used in SSL encryption.
- **Create a request to have a Certificate Authority sign a certificate that can be uploaded to the device**
  - A certificate from a Certificate Authority or a server functioning as a Certificate Authority can be uploaded to the device.

A *separate request is required for each device.*

The Internet Services Machine Digital Certificate Management screen allows you to choose your method to create a new certificate.

Accessing the Machine Digital Certificates Configuration Screen

1. Open your Web browser and enter the TCP/IP address of the WorkCentre in the Address bar. Press **[Enter]**.
2. Click the **[Properties]** tab, select **[Security]** and click on the **[Machine Digital Certificate]** link.
3. Click **[Create New Certificate]**. You have the option to create a self signed certificate for the machine, or download a request for a certificate from a Certificate Authority.



Machine Digital Certificate Management

Machine Digital Certificate

Current Status:

- A Certificate Signing Request has been generated for processing by a Trusted Certificate Authority. Upload the Signed Certificate when it is received.
- A Self Signed Certificate is established on this machine.

Copyright © Xerox Corporation 1997-2006. All rights reserved.

Creating a Self Signed Certificate

1. Click **[Self Signed Certificate]** then **[Continue]**.
2. Complete the Self Signed Certificate form with your 2 Letter Country code, State/Province Name, Locality Name (optional), Organization Name, Organization Unit, E-mail Address and Days of Validity (optional).
3. Click **[Apply]**
4. If prompted, enter the current tools administrator user name and password. The default is **[admin]** and **[1111]**.

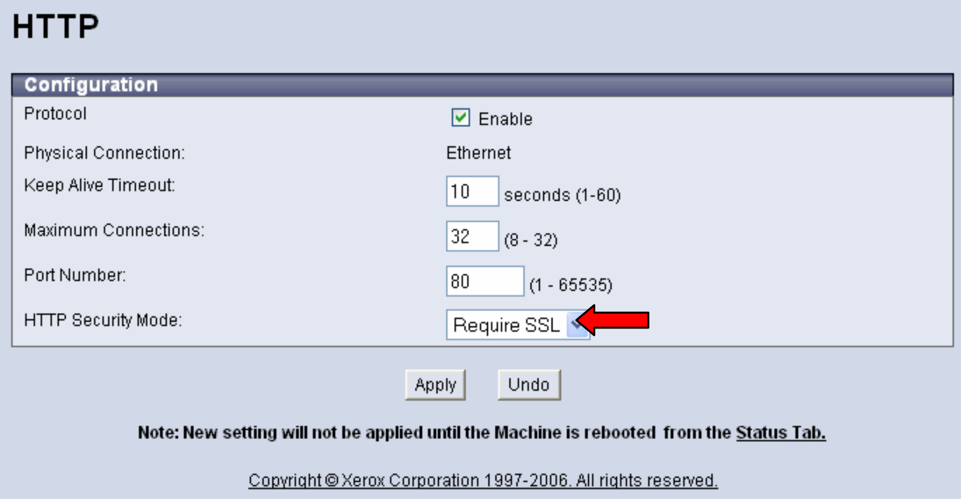
5. If successful, the Current Status will show **A Self Signed Certificate is established on this machine**.

Create a Request for a Certificate from a Certificate Authority

1. In the Machine Digital Certificate screen click **[Certificate Signing Request]**.
2. Click **[Continue]**.
3. Complete the Certificate Signing Request form with your 2 Letter Country code, State/Province Name, Locality Name, Organization Name, Organization Unit and E-mail Address.
4. Click **[Apply]**.
5. If prompted, enter the current tools administrator user name and password. The default is **[admin]** and **[1111]**.
6. The Certificate Signing Request (CSR) form will appear. Click **[Save As...]**.
7. Select the file type for the form. The options are: **X.509** (Privacy Enhanced Mail .pem) or **DER** (Distinguished Encoding Rules).
8. Click **[Save]**.
9. Click **[Save]** and save the file to your PC.
10. Send the request to your Certificate Authority for digital signing.
11. When you receive the signed certificate back from the Certificate Authority, upload the certificate to the device. To do this click the **[Machine Digital Certificate]** link located in the Security menu.
12. Click **[Upload Signed Certificate]**.
13. Browse to the signed certificate file on your PC and click **[Open]**.
14. Click **[Upload Certificate].**
15. If successful, the Current Status will show A Signed Certificate is established on this machine.

Enable the SSL (Secure Socket Layer) protocol

1. In the Internet Services Properties menu, click **[Connectivity, Protocols, HTTP]**.



HTTP

Configuration

Protocol	☑ Enable
Physical Connection:	Ethernet
Keep Alive Timeout:	10 seconds (1-60)
Maximum Connections:	32 (8 - 32)
Port Number:	80 (1 - 65535)
HTTP Security Mode:	Require SSL

Note: New setting will not be applied until the Machine is rebooted from the Status Tab.

Copyright © Xerox Corporation 1997-2006. All rights reserved.

2. In the HTTP Security Mode menu click **[Require SSL]**.

3. Click **[Apply]** and close the acknowledgement window that opens.

Close your web browser and then access the Internet Services screen again. The Security warning will display. Self-signed certificates usually cause browsers to display messages which question the trust of the certificate. Click **[OK]** to continue.

Additional Information

Xerox Customer Support welcomes feedback on all documentation - send feedback via e-mail to: USA.DSSC.Doc.Feedback@mc.usa.xerox.com.

You can reach Xerox Customer Support at 1-800-821-2797 (USA);
TTY 1-800-855-2880 or at http://www.xerox.com.

Other Tips about Xerox multifunction devices are available at the following URL: http://www.office.xerox.com/support/dctips/dctips.html.