**Reference:**

[**http://support.microsoft.com/kb/324069**](http://support.microsoft.com/kb/324069)

**How To Set Up an HTTPS Service in IIS**

**HTTPS is a secure communications channel that is used to exchange information b...**

HTTPS is a secure communications channel that is used to exchange information between a client computer and a server. It uses Secure Sockets Layer (SSL). This article describes how to configure the SSL/HTTPS service in Internet Information Services (IIS) and compares this process to the similar process in Apache.

**Configuring Your Web Server for SSL**

To enable SSL in IIS, you must first obtain a certificate that is used to encrypt and decrypt the information that is transferred over the network. IIS includes its own certificate request tool that you can use to send a certificate request to a certification authority. This tool simplifies the process of obtaining a certificate. If you use Apache, you must obtain the certificate manually.   
  
In both IIS and Apache, you receive a certificate file from the certification authority, which you must configure on the computer. Apache reads the certificate from its source file by using the SSLCACertificateFile directive. However, in IIS, you can configure and manage certificates by using the **Directory Security** tab of the Web site or folder properties.   
  
You can migrate certificates from Apache to IIS; however, Microsoft recommends that you re-create or obtain a new certificate for IIS.

**Configure Folder or Web Site to Use SSL/HTTPS**

This procedure assumes that your site has already has a certificate assigned to it.

1. Log on to the Web server computer as an administrator.
2. Click **Start**, point to **Settings**, and then click **Control Panel**.
3. Double-click **Administrative Tools**, and then double click **Internet Services Manager**.
4. Select the Web site from the list of different served sites in the left pane.
5. Right-click the Web site, folder, or file for which you want to configure SSL communication, and then click **Properties**.
6. Click the **Directory Security** tab.
7. Click **Edit**.
8. Click **Require secure-channel (SSL)** if you want the Web site, folder, or file to require SSL communications.
9. Click **Require 128-bit encryption** to configure 128-bit (instead of 40-bit) encryption support.
10. To allow users to connect without supplying their own certificate, click **Ignore client certificates**.  
      
    Alternatively, to allow a user to supply their own certificate, use **Accept client certificates**.
11. To configure client mapping, click **Enable client certificate mapping**, and then click **Edit** to map client certificates to users.   
      
    If you configure this functionality, you can map client certificates to individual users in Active Directory. You can use this functionality to automatically identify a user according to the certificate they supplied when they access the Web site. You can map users to certificates on a one-to-one basis (one certificate identifies one user) or you can map many certificates to one user (a list of certificates is matched against a specific user according to specific rules. The first valid match becomes the mapping).
12. Click **OK**.

**For additional information about how to set other preferences for log files in I...**

For additional information about how to set other preferences for log files in IIS, click the article number below to view the article in the Microsoft Knowledge Base:

[310178](http://support.microsoft.com/kb/310178/EN-US/)  (http://support.microsoft.com/kb/310178/EN-US/ ) How To Install Imported Certificates on a Web Server in Windows 2000

For additional information about securing IIS for a migration from UNIX to Windows, click the article number below to view the article in the Microsoft Knowledge Base:

[324216](http://support.microsoft.com/kb/324216/EN-US/)  (http://support.microsoft.com/kb/324216/EN-US/ ) How To Secure IIS in a UNIX-to-Windows Migration