

Securing IIS 5.0/5.1 Guidelines:

1. **Do NOT install IIS on a Windows Domain Controller.**
2. **Follow applicable guidelines for securing OS.**
3. **Download the appropriate security cumulative patch before installing IIS.**
You will only need this patch for IIS 4. (The contents of this patch are already included in Windows 2003, Windows 2000 Service Pack 4 or greater, and XP Service Pack 1 or greater). If using IIS on NT4, the latest IIS rollup patch can be found at:
<http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b811114>
4. **Install IIS.** Once IIS is installed, backup the IIS Metabase – a database that stores IIS configuration parameters. The metabase can become corrupted, so it is important to save a backup. To back up the metabase, right click on the icon for your web server and select *Backup/Restore Configuration*. Click on *Create Backup* and enter a meaningful name. Click on *Ok* to complete the process.
5. **Determine if WebDav will be used to update your pages.** If so, apply the following patch (warning, if your operating system is Windows 2000 and you are running certain post-service pack 2 patches, this may cause a “blue screen of death”):
<http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>

If not using WebDav, manually disable it through a registry setting or by using the IIS Lockdown Tool. Additional information about the IIS Lockdown tool is located in step 13 of this document. Instructions on manually changing the registry setting to disable WebDav can be found at:

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B241520>

6. **Do not store your web page in the default location (C:\inetpub\wwwroot).** If possible, place your data on a separate partition (e.g. on D:) in a folder that describes your web page content. For example, since my office is named SOS (Security Operations and Services), I might create a folder D:\SOS\ to store my web content. Next, use the ISM to link the folder to your web site. To do so, right-click on the icon for your server and select *New*, then choose *Site*. You will need to enter a descriptive name of your web site, IP Address and port settings properties (the default settings should be fine as long as you disable the “default” IIS site that is installed with IIS), and then you will need to browse to the location of your content (e.g. D:\SOS\). Next, you will need to choose whether you wish to permit anonymous access to the site, and what types of permissions you wish the users to have (e.g. Read, Run Scripts, Execute, Write, and Browse).
7. **Select authentication means of users connecting to your web site.** If you want to have anonymous access to your site, you do not need to change anything. If you want to restrict access to your site by means of a username and password, right click on your web site and click on the *properties* button. Select the *directory security* tab. Click on the *Edit* button next to *Anonymous access and authentication control*. Uncheck the box for *Anonymous access*. You will then need to supply your users with a Windows username and password to access the content off of your server.

8. **Set IP/DNS Address restrictions for your web site if you wish to filter which IP Addresses can access your site.** To do so, right click on your site and choose *properties*. Click the *directory security* tab. Click the *Edit* button next to *IP Address and domain name restrictions*. You can specify who can be granted or denied access by address or domain name.
9. **Set maximum number of connections.** By default, the number of connections to your web server is unlimited, which can lead to extremely poor performance or even denial of service. To limit the maximum number of connections, right click on your web site and click on the *properties* button. Click on the *web site* tab and change the radio button from *unlimited* to *limited to*: Type in the desired maximum number of connections (the default is 1000). Change the *Connection Timeout* to 300 seconds.
10. **Determine if it is acceptable for pages to be cached on your clients' machines or if a new version of the pages should be downloaded every time.** The default setting is for pages to be cached indefinitely on remote computers. If your web site is unavailable and the page is cached on the remote user's machine, it will open up the cached version. To change the cached pages setting, right click on your web site and choose *properties*. Choose the *HTTP Headers* tab and check the box next to *Enable content expiration*. You can then choose the length of content expiration (e.g. daily, weekly, every time, etc).
11. **If you are hosting sensitive information, secure the connection by using SSL.** You will need to request a certificate from the built in certificate server (to issue your own certificates – for an intranet type of environment) or request one from a public certification authority such as Verisign (<http://digitalid.verisign.com>) or Thawte (<http://www.thawte.com>). After creating a digital certificate, to set up SSL, right click on your web site and choose *properties*. Next, click on the *directory security* tab. Under *Secure Communications*, click on the *Server Certificate* button to install the certificate. Next, on the main *Directory Security* tab of your web site, click on the *Edit* button under *Secure Communications*. Check the box for *Require secure channel (SSL)*.
12. **Extended Logging Properties should be enabled for your website and/or FTP server.** To check your current logging configuration, right click on your web site choose *properties* and click on the *web site* tab. Towards the bottom of the page, you will see a check box for *enable logging*, which should be checked, and the format should be *W3C Extended Log File Format*. If this is not the current method of logging, use the drop down menu to change to W3C logging. By default, the logs are saved in GMT format. Check the box *Use local time for file naming and rollover* so that log files are kept in local system time. Check the Next, click on the *properties* button located beside the format and choose the *extended logging properties* tab to make sure that it includes Date, Time, Server IP, Client IP, URI Stem, and URI Query so that you can fully log every access to your web site.
13. **Change the location of IIS log files and set log file permissions.** The logfiles are located by default in C:\winnt\system32\LogFiles). It is recommended that you store the log files in another location, both for security and for space concerns. To change the location of the log files, right click your web site and choose *properties*. Click on

the web site tab and click the properties button next to the format. At the bottom of the screen, type in the new location for the log file location, or browse to select the desired directory. Next, use Windows Explorer or My Computer to browse to the location of the log folder. Right click on the folder and choose properties, and then select the security tab. Make sure administrators and system have full control and that authenticated users and the IUSR_Computername account have RWC permissions.

14. Install the IIS Lockdown tool, or follow guidelines below to manually secure IIS.

The IIS Lockdown tool can be downloaded from:

<http://www.microsoft.com/technet/security/tools/tools/locktool.asp>. The lockdown tool runs as a wizard to secure IIS by disabling unnecessary script mappings, sample folders, changing permissions on vulnerable executables, removing access to unneeded directories, and can install a program named URLScan, which restricts the type and content of harmful HTTP requests your web server processes. It is highly recommended that you run URLScan in conjunction with your web server.

If you do not install the IIS Lockdown tool, manually set the following options:

1. **Change permissions on the following Windows executables, located in %Systemroot/Windows/System32 or %Systemroot/Winnt/System32.** (Everyone has read and execute permissions on these files by default. The IUSR_Computername account is included as part of that everyone group, and thus can execute these commands). Change permissions to only include Authenticated users rather than everyone. Also, ensure that administrators and system have full control.
 - a. Command.com
 - b. Cmd.exe
 - c. ftp.exe
 - d. regedit.exe
 - e. regedt32.exe
 - f. telnet.exe
 - g. tftp.exe

You can also change permissions on all files in the system32 folder using the *CACLS* command from a command prompt rather than changing settings manually. For example, to grant Full Control to the System and Administrator, and no control to all other users, you would type the following command: *Cacls %systemroot%*.exe /T /G System:F Administrators:F*

2. **Remove IIS Samples and Documentation.** Open up the ISM and double click the default web site to expand its contents. Highlight the virtual directories entitled *IISamples* and *IISHelp* and delete them if present.
3. **If upgrading from IIS4 to IIS5, also remove the IISADMPWD virtual directory,** which allows you to reset Windows passwords
4. **Remove or stop the IIS Administration web site** if you do not wish to make configuration changes to your IIS server over the internet.
5. **Try to group all scripts, executables, etc. together.** For example, create one directory for .asp files, create another for executables, etc). Navigate to this directory and change its permissions to Administrators and System having full control and the IUSR_Computername account having only the execute permission. Grant appropriate permissions to anyone else who needs to access the files.
6. **Similarly, attempt to place static content for a web site in the same place** (graphics, plain .html files, documents, etc). Grant the IIS_Computername read only permissions, and Administrators and System full control. Again, grant appropriate permissions for other necessary users.
7. **Remove unnecessary script mappings.** Open up the ISM, right click on the web server and select properties. Choose Master Properties from the menu. Select WWW service and select edit, and then chose HomeDirectory and finally configuration. It is suggested that you remove the following entries:
 - a. .ida, .idq, and .htw if you are not using the Index Server feature of IIS.
 - b. .htr if you do not wish to use the web-based password reset feature.
 - c. .printer if you do not wish to support internet printing from the server
 - d. .stm, .shtm, and .shtml if you are not using Server-Side includes.
 - e. .idc if you are not using database applications.

8. **Disable Parent Paths**, which allow Active Server Pages to use relative file paths (e.g. ../directory/file.html instead of c:/directory/file.html). To disable parent paths, right click on your machine name and choose to edit the WWW properties. Next, open up the Home Directory tab. Click on the configuration button in the bottom right hand side. Next, click on the App Options tab. Uncheck enable parent paths.

If FTP is installed:

1. **Check the permissions of the default FTP folder** (C:\Inetpub\ftproot), which may be set to Everyone has Full Control. If your FTP server allows uploads, specify who may upload.
2. **If you don't require anonymous uploading**, it is suggested that you do not check the box to allow anonymous access in the *Security Accounts* tab of your FTP site.
3. **If you are hosting an FTP server on the same machine as a web server, change the account that is used to anonymously access the FTP resource.** Right click on your Ftp site and choose *properties*. Click on the *Security Accounts* tab and use the browse feature to change the account from IUSR_Computername to another local user. Follow good password guidelines for this account.
4. **If you wish to allow only downloads, make sure that the IUSR_Computername does not have Write ACLs set.** Right click on the FTP site and choose I. Click on the *Home Directory* tab and ensure that the Write attribute is not checked.
5. **Whenever possible, place your FTP content on a different volume than the operating system.** Right click on the FTP site and choose *properties*. Click on the *Home Directory* tab and enter the location of the FTP folder or browse to it in the *FTP Site Directory* box.
6. **Set IP/DNS Address restrictions.** To do so, right click on your site and choose *properties*. Click the *directory security* tab. Click the *Edit* button next to *IP Address and domain name restrictions*. You can specify who can be granted or denied access by address or domain name.
7. **Limit number of connections.** Right click on your FTP site and choose *properties*. Click on the *FTP Site* tab and change the radio button from *Unlimited* to *Limited to:* and type in the number of maximum connections you will allow. Change the *Connection Timeout* to 300 seconds.
8. **Give a welcome banner and message that indicates restricted use of the FTP server.** Right click on the FTP site and choose *properties*. Click on the *Messages* tab and enter an appropriate message in the box.

If SMTP is installed:

1. **Check the permissions of the default SMTP folder** (C:\Inetpub\mailroot), which may be set to Everyone has Full Control.
2. **Limit number of messages sent per message** To do so, right click on your SMTP server and choose *properties*. Click the *messages* tab. *Limit the number of recipients per message* to a smaller number than the default, which is 100.