



# Sitecore CMS 6.0-6.4

# Sitecore Security Hardening Guide

*Recommendations for making Sitecore more secure*

## Table of Contents

Chapter 1	Introduction.....	3
1.1	Secure Software.....	4
1.1.1	General Recommendations .....	4
Chapter 2	Security Settings .....	5
2.1	Security Settings .....	6
2.2	Limiting Access to .XML, .XSLT, and .MRT Files .....	7
2.3	Protecting Folders in the IIS.....	8
2.3.1	Folder Structure.....	8
	The /data Folder .....	8
2.3.2	Limiting Access to Anonymous Users.....	9
2.4	Turn off Auto Complete of Username in the Login Page .....	12
2.5	Controlling File Upload.....	13
2.5.1	Deny Execute Permissions on the Upload Folder .....	13
	Denying Execute Permission in IIS 6 .....	13
	Denying Execute Permission in IIS 7 .....	13
2.5.2	Disabling the Upload Watcher.....	14
2.5.3	The Upload Filter Tool.....	15
	Installing the Upload Filter Tool.....	15
	Configuring the Upload Filter Tool .....	15
2.6	Security and Client RSS Feeds.....	17
2.6.1	Disabling Client RSS Feeds.....	17
2.7	Recommended Reading .....	18
2.7.1	Other Resources .....	18

# Chapter 1

## Introduction

This introduction explains the aim and scope of this security hardening guide.

This chapter contains the following sections:

- Secure Software

## 1.1 Secure Software

This document is designed to help you make your Sitecore installation as secure as possible. Sitecore is of course subjected to rigorous testing before each release and any bugs or security threats that may exist are fixed and removed as soon as they are discovered. We also release updates and service packs whenever necessary.

However, the way you implement your Sitecore installation has a significant effect on the security of your Web site.

This document contains details of our best practices and recommendations for ensuring that your Sitecore installation is as secure as possible.

Sitecore is not responsible for the security of any other software products that you use with your Web site. We strongly recommend that you install *every* available service pack and update for *all* of the software products that you use.

It is important to remember that secure software is a goal that we are constantly trying to achieve but may never reach.

Security is risk management; it is about understanding the risks and concrete threats to your environment and mitigating against them. You must analyze the threats and risks that your installation faces and then do your utmost to secure your installation against these threats.

This document does not describe the Sitecore Security system. For more information about the Sitecore security system, see the *Security Administrators Cookbook*.

### 1.1.1 General Recommendations

Although Sitecore can run on several different operating systems, we recommend that you use the newest operating systems with the most up-to-date security features. Use the Windows update / Automatic update service to keep all your client computers and servers up-to-date with the most recent security updates and service packs.

You should also create a disaster recovery plan to ensure the rapid resumption of services should a disaster occur. The recovery program should include:

- A plan for acquiring new or temporary equipment.
- A plan for restoring backups.
- Testing the recovery plan.

## Chapter 2

# Security Settings

This chapter describes some of the settings that you should apply in your Sitecore installation.

This chapter contains the following sections:

- Security Settings
- Limiting Access to .XML, .XSLT, and .MRT Files
- Protecting Folders in the IIS
- Turn off Auto Complete of Username in the Login Page
- Controlling File Upload
- Security and Client RSS Feeds
- Recommended Reading

## 2.1 Security Settings

When you use the installation program to install Sitecore, all of the appropriate security settings are set. However, if you install Sitecore from a zip file or if you install a Web site on a server without running the setup.exe, there are a number of settings that you will have to set manually.

These settings are described in detail in the Sitecore CMS 6.1 Installation Guide in sections 3.5 to 3.6.5.

Furthermore, if you are updating from an earlier version to Sitecore 6.1, you must edit the appropriate config files.

These changes are described in detail in the Sitecore Developer Network at <http://sdn5.sitecore.net/Products/Sitecore%20V5/Sitecore%20CMS%206/ReleaseNotes/webConfig.aspx>

## 2.2 Limiting Access to .XML, .XSLT, and .MRT Files

To improve the security of your Sitecore installation, you must edit the `web.config` file. This file is stored in the `\WebSite` folder of your installation, for example at

`C:\inetpub\wwwroot\YourWebsite\WebSite`

To limit access to `.XML`, `.XSLT`, and `.MRT` files:

1. Open the `web.config` file.
2. Add the following lines to the `<system.webServer><handlers>` section:

```
<system.webServer>
  <handlers>

    <!-- Add managed handler for IIS7 Classic Mode in order to prevent access to files
    Notice: Must correspond to the handlers defined in <httpHandlers> section -->
    <add path="*.xml" name="xml Handler (classic)" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll"
resourceType="Unspecified" precondition="classicMode, runtimeVersionv2.0" />
    <add path="*.xslt" name="xslt Handler (classic)" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll"
resourceType="Unspecified" precondition="classicMode, runtimeVersionv2.0" />
    <add path="*.config.xml" name="config.xml handler (classic)" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll"
resourceType="Unspecified" precondition="classicMode, runtimeVersionv2.0" />
    <add path="*.mrt" name="mrt handler (classic)" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll"
resourceType="Unspecified" precondition="classicMode, runtimeVersionv2.0" />

    <!-- Prevent files from being served in IIS7 Integrated Mode -->
    <add path="*.xml" verb="*" type="System.Web.HttpForbiddenHandler" name="xml (integrated)"
preCondition="integratedMode"/>
    <add path="*.xslt" verb="*" type="System.Web.HttpForbiddenHandler" name="xslt (integrated)"
/>
    <add path="*.config.xml" verb="*" type="System.Web.HttpForbiddenHandler" name="config.xml
(integrated)" precondition="integratedMode"/>
    <add path="*.mrt" verb="*" type="System.Web.HttpForbiddenHandler" name="mrt (integrated)"
preCondition="integratedMode"/>
```

3. Add the following lines to the `<system.web><httpHandlers>` section:

```
<system.web>
  <httpHandlers>

    <!-- Prevent files from being served in IIS6 and in IIS7 Classic Mode -->
    <add path="*.xml" verb="*" type="System.Web.HttpForbiddenHandler" validate="true" />
    <add path="*.xslt" verb="*" type="System.Web.HttpForbiddenHandler" validate="true" />
    <add path="*.config.xml" verb="*" type="System.Web.HttpForbiddenHandler" validate="true" />
    <add path="*.mrt" verb="*" type="System.Web.HttpForbiddenHandler" validate="true" />
```

### Internet Information Services 6

If you are using IIS6, you must map these file extensions to the `aspnet_isapi.dll` to allow the ASP.NET framework to block requests for these file types.

## 2.3 Protecting Folders in the IIS

You can improve security by preventing anonymous users from accessing certain key folders and by placing other folders in more secure locations.

You should ensure that the following folders are placed outside the website root folder:

- /data
- /indexes

You should prevent anonymous users from accessing the following folders:

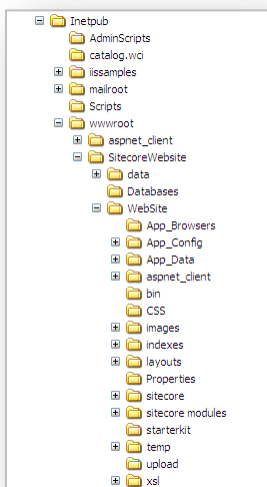
- /App\_Config
- /sitecore/admin
- /sitecore/debug
- /sitecore/shell/WebService

### 2.3.1 Folder Structure

You must ensure that certain folders are stored in the recommended location.

#### The /data Folder

The /data folder should be placed outside the /Website folder. You must edit the `web.config` file to point to the new location of the /data folder. You also must configure permissions for ASP.NET requests. For more information about that, see section 4.2.2 File System Permissions for ASP.NET requests in the *CMS Installation Guide*.



There are two ways to install Sitecore — you can use

- The installation program.
- A .zip file.



## Using the Installation Program

If you use the installation program to install Sitecore, the `/data` folder is created in the correct location and the `web.config` file is edited to point to this location.

This is the recommended configuration and you don't need to make any changes.

## Using a .zip File

If you use a `.zip` file to install Sitecore, the `data` folder is created in the correct location but the `web.config` file is not edited to point to this location. When you run Sitecore for the first time, it creates another `data` folder in the `/WebSite` folder.

We therefore recommend that you edit the `web.config` file to point to the correct location.

The `web.config` file should look like this:

```
<sitecore database="SqlServer">
  <sc.variable name="dataFolder" value="C:\inetpub\wwwroot\SitecoreWebsite\data\" />
  <sc.variable name="mediaFolder" value="/upload" />
  <sc.variable name="tempFolder" value="/temp" />
</sitecore>
```

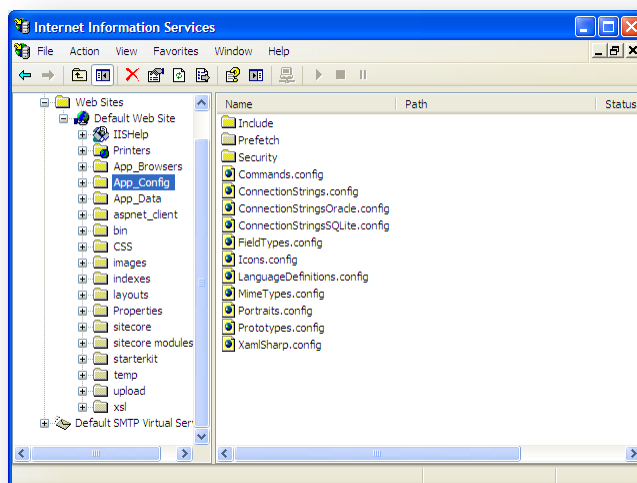
## 2.3.2 Limiting Access to Anonymous Users

You should prevent anonymous users from accessing the following folders:

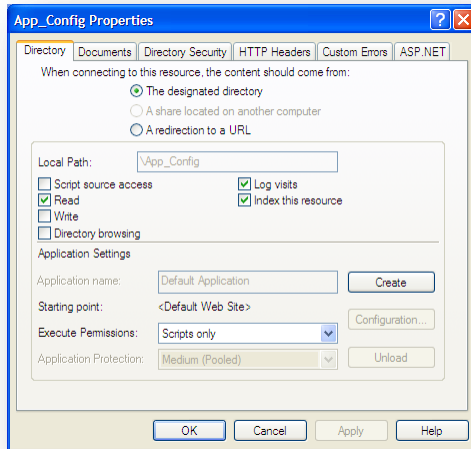
- `/App_Config`
- `/sitecore/admin`
- `/sitecore/debug`
- `/sitecore/shell/WebService`

To limit anonymous access to the `/App_Config` folder:

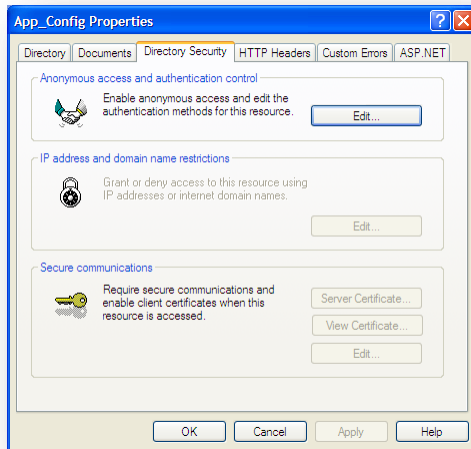
1. Open the IIS.
2. Navigate to the `Web Sites\Default Web Site\App_Config` folder.



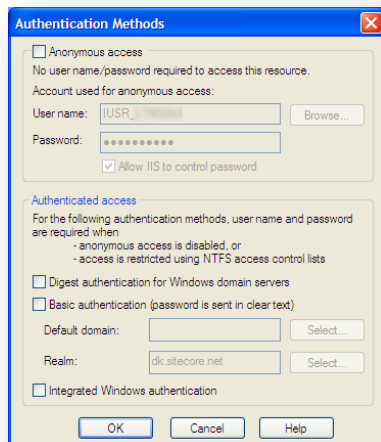
- In the **Internet Information Services** window, right-click the `App_Config` folder and click **Properties**:



- In the **App\_Config Properties** window, click the **Directory Security** tab.



5. In the **Anonymous access and authentication** control section, click Edit.



6. In the **Authentication Methods** window, ensure that the **Anonymous access** check box is cleared.
7. Restart the IIS.

Repeat this process for the `/sitecore/admin`, `/sitecore/debug` and `/sitecore/shell/WebService` folders.

#### Note

If you have upgraded to Sitecore 6 from an earlier version and followed the upgrade instructions, you should have removed all the obsolete files. However, if you did not follow the upgrade instructions, you should prevent anonymous access to the `rest.aspx` file. This file is stored in the `/sitecore` folder.

## 2.4 Turn off Auto Complete of Username in the Login Page

You can also improve the security of your Sitecore installation by specifying that Sitecore should not automatically complete the username of users when they log in.

To turn off the auto-completion of user names:

1. Navigate to the `C:\Inetpub\wwwroot\YourWebsite\WebSite\sitecore\login` folder.
2. Open the `default.aspx` file.
3. Locate the `form id="LoginForm"` section
4. Edit this section as follows:

```
<form id="LoginForm" runat="server" autocomplete="off">
```

## 2.5 Controlling File Upload

You can also improve the security of your Sitecore installation by controlling access to uploadable files.

### 2.5.1 Deny Execute Permissions on the Upload Folder

If you allow users to modify the contents of the *upload* folder, you also give them permission to place scripts and executable programs in the folder. Executing these scripts and programs can cause some unexpected behavior on the server. You must therefore prevent an uploaded file from being executed on the server side when a user attempts to download it.

We therefore recommend that deny permission to run scripts and execute files in the *upload* folder.

#### Note

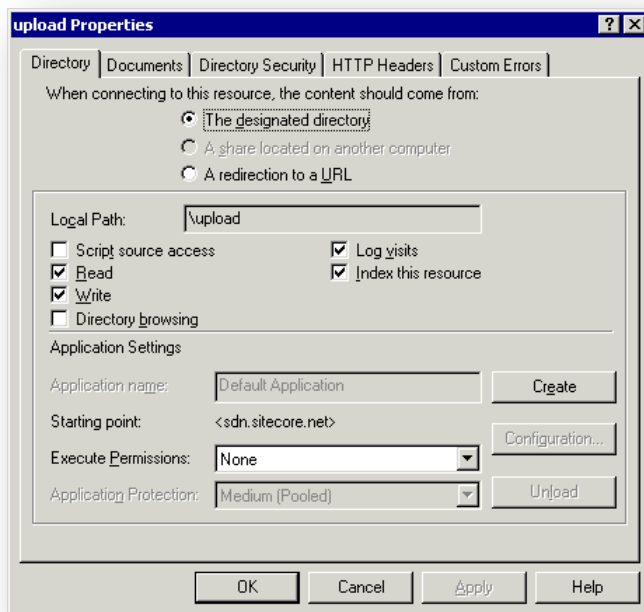
You only need to perform this step if your configuration allows content authors to place files directly into the *upload* folder. For example, if you use a shared directory or FTP server, content authors can quickly place a lot of media in the media library.

For more information about *Execute* permission in IIS, see <http://support.microsoft.com/kb/313075>.

### Denying Execute Permission in IIS 6

If you are running on IIS 6, you must deny *Execute* permission to the *upload* folder.

In IIS 6, select *Properties* for the *upload* folder:



In the **Execute Permissions** field, select *None*.

### Denying Execute Permission in IIS 7

If you are running on IIS 7 you must deny both *Script* and *Execute* permission to the upload folder.



To disable the Upload Watcher, remove the following line from the `<modules>` section of the `Web.config` file.

### IIS7

```
<system.webServer>
  <modules>
    <remove name="ScriptModule"/>
    <add type="Sitecore.Nexus.Web.HttpModule,Sitecore.Nexus" name="SitecoreHttpModule"/>
    <add type="Sitecore.Resources.Media.UploadWatcher, Sitecore.Kernel"
name="SitecoreUploadWatcher"/>
```

### IIS6

```
<httpModules>
  <add type="Sitecore.Nexus.Web.HttpModule,Sitecore.Nexus" name="SitecoreHttpModule"/>
  <add type="Sitecore.Resources.Media.UploadWatcher, Sitecore.Kernel"
name="SitecoreUploadWatcher"/>
```

## 2.5.3 The Upload Filter Tool

However, if you want to have complete control and prevent users from uploading certain file types, you should use the Upload Filter tool.

The Upload Filter tool let's you prevent certain file types from being uploaded for example `.exe`, `.dll`, and so on.

You can download the Upload Filter tool — `Upload Filter-1.0.0.2.zip` — from the Sitecore Developer Network — <http://sdn5.sitecore.net/> — where it is available as a Sitecore package file along with this Security Hardening Guide.

### Important

The Upload Filter tool is only supported on Sitecore CMS 6.1.0 rev. 090630 or later.

The Sitecore package contains the following files:

File Name	Destination Folder
<code>UploadFilter.config</code>	<code>Website\App_Config\Include\</code>
<code>UploadFilter.dll</code>	<code>Website\bin\</code>

## Installing the Upload Filter Tool

You must install the Sitecore package file before you can use the Upload Filter Tool.

To install Upload Filter Tool:

1. In the **Sitecore Desktop**, click **Sitecore, Control Panel**.
2. In the **Sitecore Control Panel**, click **Administration, Install a Package**.
3. The wizard will guide you through the installation process.

## Configuring the Upload Filter Tool

After you install the package, you must configure the tool.

To configure the Upload Filter tool:

1. Open the `UploadFilter.config` file.

```
<processors>
```

```
<uiUpload>
  <processor mode="on" type="Sitecore.Pipelines.Upload.CheckExtension,
Sitecore.UploadFilter" patch:before="*[1]">
    <param desc="Allowed extensions (comma separated)"></param>
    <param desc="Blocked extensions (comma separated)">exe,dll</param>
  </processor>
</uiUpload>
</processors>
```

2. In the `Allowed extensions` parameter, enter a comma separated list the file extension types that can be uploaded.

Or

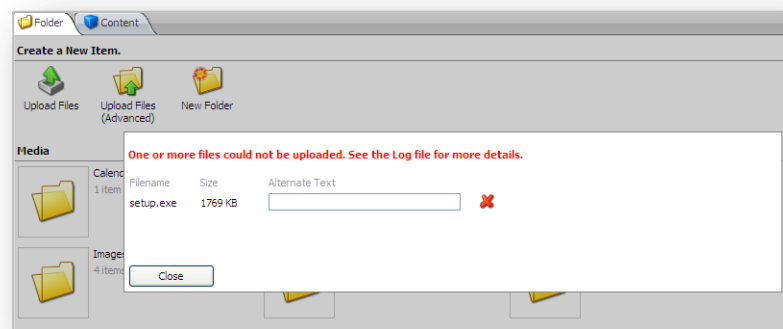
In the `Blocked extensions` parameter, enter a comma separated list the file extension types that cannot be uploaded.

You must enter the file extension without the dot.

### Important

If you set the `Allowed extensions` parameter, the `Blocked extensions` parameter is ignored.

3. If you try to upload a file type that is on the blocked list, you see the following message:





## 2.6 Security and Client RSS Feeds

RSS technology is designed so that users who follow an RSS link can come directly to the item specified in the URL of the RSS feed. Most RSS readers do not support authentication. This means that users who subscribe to Sitecore client RSS feeds have direct access to the item specified in the URL of the RSS feed and do not have to identify themselves to the Sitecore security system when they view the RSS feed. However, the Sitecore security system verifies that they are authorized users when they try to perform any actions associated with the client feed.

If someone else gains access to the URL of the RSS feed:

- They *can* follow the link and view all the content contained in the RSS feed even though their own security permissions do not give them access to this item.
- They *cannot* perform any actions on the content.
- They *cannot* view any other content.
- They *cannot* gain access to the username or password of the original owner of the RSS feed.
- They *cannot* modify the link to gain access to any other content.

### Important

Sitecore users should not share RSS feeds.

### 2.6.1 Disabling Client RSS Feeds

If your Sitecore installation contains sensitive information that you want to protect, you can disable Sitecore client RSS feeds.

To disable Sitecore client feeds:

1. Open the `web.config` file.
2. Locate the `<httpHandlers>` section. Depending on your IIS pool this section may be called `Handlers`.
3. Remove the following handler:

```
<add verb="*" path="sitecore_feed.ashx"  
type="Sitecore.Shell.Feeds.FeedRequestHandler, Sitecore.Kernel"/>
```

Removing this handler disables all the client feeds that are available inside Sitecore. However, any public RSS feeds that you have created are still available to Web site visitors.

## 2.7 Recommended Reading

For information about how to make Sitecore more secure, we recommend that you read the following documents:

- Sitecore Installation Guide.  
<http://sdn.sitecore.net/Products/Sitecore%20V5/Sitecore%20CMS%206/Installation.aspx>  
Read the installation guide for the Sitecore version you are using.
- The upgrade instructions for the Sitecore version you are upgrading from.
- The `web.config` changes documentation for the Sitecore version you are upgrading to.

### 2.7.1 Other Resources

For more information about SQL Server security, visit:

<http://technet.microsoft.com/en-us/library/bb545450.aspx>

<http://www.microsoft.com/sqlserver/2005/en/us/security.aspx>

For more information about security in general, visit the Microsoft Security TechCenter:

<http://technet.microsoft.com/en-us/security/default.aspx>