https://web.archive.org/web/20100210125749/https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4beddb35-0cba-424c-8b9b-a5832ad8e208.mspx

Managing WebDAV Security (IIS 6.0)

Archived: 2026-04-06 01:03:04 UTC

The Wayback Machine - https://web.archive.org/web/20100210125749/http://www.microsoft.com:80/technet/prodtechnol/WindowsServer2003/Library/IIS/4be 0cba-424c-8b9b-a5832ad8e208.mspx

This topic provides a brief overview of recommended security practices for remote publishing. It briefly describes how to protect your server and content by authenticating client connections to your server and by controlling access to content on your server. Included in this topic are descriptions of the following:

•	Authenticating Clients
•	Controlling Access

Note

For security reasons and to to enable DAV custom properties, ensure that your publishing directory resides on an NTFS partition. To learn more about NTFS partitions, see Windows Server 2003 family Help.

Authenticating Clients

The best way to configure a WebDAV directory depends on the kind of publishing that you want to do. When you create a virtual directory through IIS, Anonymous and Integrated Windows authentication are both turned on. Although this default configuration works well for clients connecting to your server, reading content on a Web page, and running scripts, it does not work well with clients publishing to a directory and manipulating files in that directory.

IIS offers the following authentication methods:

•	Kerberos is the primary security protocol for authentication within a domain. Kerberos is the best option for WebDAV client authentication and file security.
•	Anonymous authentication grants anyone access to the directory. You should turn off anonymous access to your WebDAV directory. Without controlling who has access, your directory could be attacked by unknown clients.
•	Basic authentication sends passwords over the connection in clear text. Clear text passwords can be intercepted and read. Turn on Basic authentication only if you encrypt passwords by using Secure Sockets Layer.
•	Digest authentication is a good choice for publishing information on a server that is accessed over the Internet and through firewalls because the passwords are sent over the network as an MD5 hash. However, passwords are stored as plain text in Active Directory.

- Advanced Digest authentication is an improvement over Digest authentication because in addition to sending passwords over the network as an MD5 hash, the passwords are also stored in Active Directory as an MD5 hash rather than plaintext. This makes Advanced Digest the best choice for publishing information on a server that is accessed over the Internet and through firewalls.
- Integrated Windows authentication works best when you are setting up a WebDAV directory on an intranet.
- .NET Passport authentication uses cookies to validate user credentials.

Controlling Access

This section describes how you can control access to your WebDAV directory by coordinating IIS and Windows Server 2003 permissions, and how you can protect your script files.

Configuring Web Permissions

The following are various ways to configure Web permissions based on the purpose of the material you are publishing:

- Read, Write, and directory browsing enabled: Turning on these permissions allows clients to see a list of resources, modify them (except for those resources without Write permission), publish their own resources, and manipulate files.
- Write enabled; and Read and directory browsing disabled: If you want clients to publish private information on the directory, but do not want others to see what has been published, set Write permission and do not set Read or directory browsing permission. This configuration works well if clients are submitting ballots or performance reviews.
- Read and Write enabled; and directory browsing disabled: Set this configuration if you want to rely on obscuring file names as a security method. However, be aware that security by obscurity is a low-level security precaution because an attacker could guess file names by trial and error.
- Index this resource enabled: Be sure to enable Indexing Service if you plan to let clients search directory resources.

Controlling Access with DACLs

WebDAV takes advantage of the security features offered by the platform and the Web server, including permissions control and discretionary access control lists (DACLs) in the NTFS file system. When setting up a WebDAV publishing directory on an NTFS file system drive, make sure the **Everyone** group has Read permission only. Then assign Write permission to specific individuals or groups.

Protecting Script Code

If you have script files in your publishing directory that you do not want to expose to clients, you can deny access to these files by verifying that **Script source access permission** is not assigned. Executable files are treated as static HTML files unless **Scripts and Executables** is enabled for the directory.

To prevent .exe files from being downloaded and viewed as HTML files, but to allow .exe files to run, on the **Virtual Directory** property sheet of the publishing directory, change the Execute Permissions to **Scripts and Executables**.

This level of permission makes all executable files subject to the **Script source access** setting. When **Script source access** is selected, clients with Read permission can see all executables; and clients with Write permission can edit them, as well as run them.

With the following permissions, clients can write to an executable file that does not appear in the Application Mapping:

•	Write permission is assigned.
•	Execute Permissions is set to **Scripts only**.

With the following permissions, clients can write to any executable file, regardless of whether it appears in the Application Mapping:

•	**Script source access** is assigned.
•	Execute Permissions is set to **Scripts and Executables**.

Related Information

Source: https://web.archive.org/web/20100210125749/https://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/4beddb35-0cba-424c-8b9b-a5832ad8e208.mspx