How To Secure Default IIS Site & Enable Windows Authentication

blog.netwrix.com/2022/10/21/enable-windows-authentication-iis

Joe Dibley

By default, when you create a new Internet Information Services (IIS) website, it's open to everyone with anonymous access enabled — anyone can access and view the data being hosted by that site. Obviously, this is a security concern for most organizations. Indeed, I'm often asked by clients and colleagues how to lock down an IIS site so only the desired people can access it.

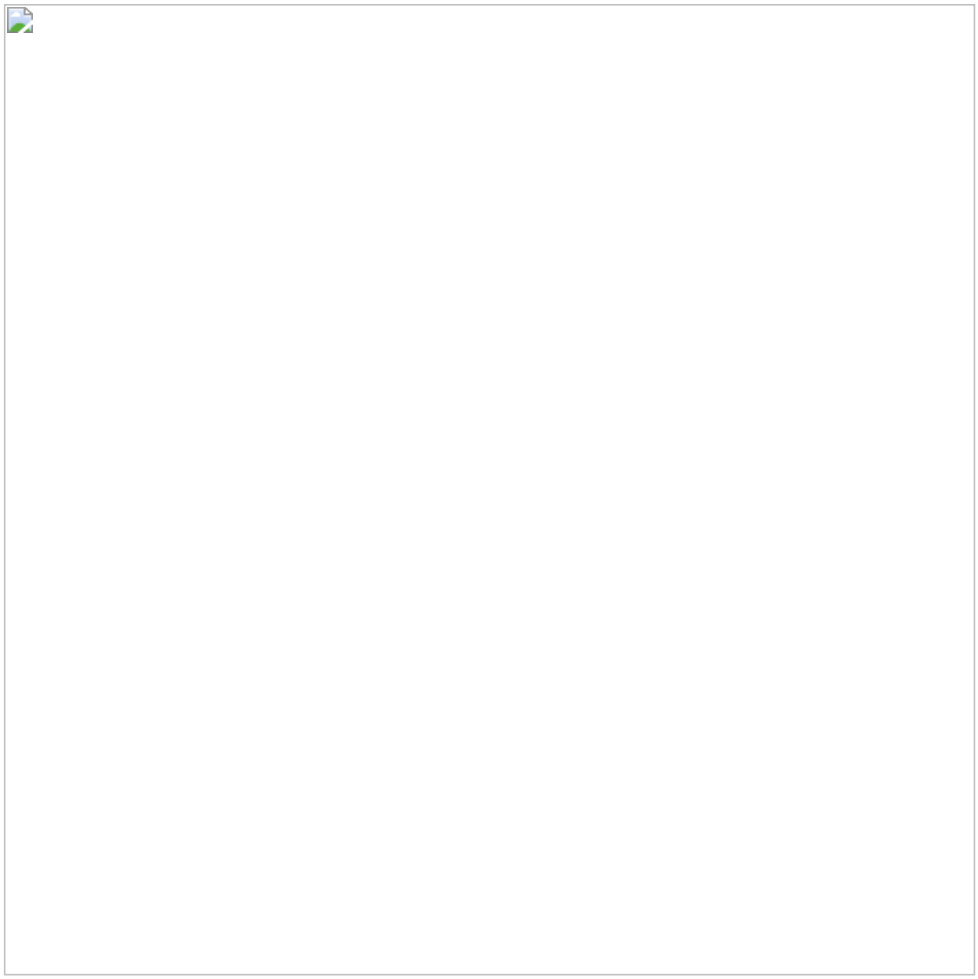
Handpicked related content:

Windows Server Security Best Practices

The answer is pretty simple: In order to secure an IIS site, all one needs to do is change the default permissions, enable Windows Authentication for user accounts, and disable Anonymous Authentication in IIS Manager. Here are the steps:

How to secure your IIS site

1.Select your site and click "Authentication", In the screenshot below, you can see that I have many IIS sites, including one named "Default Web Site".

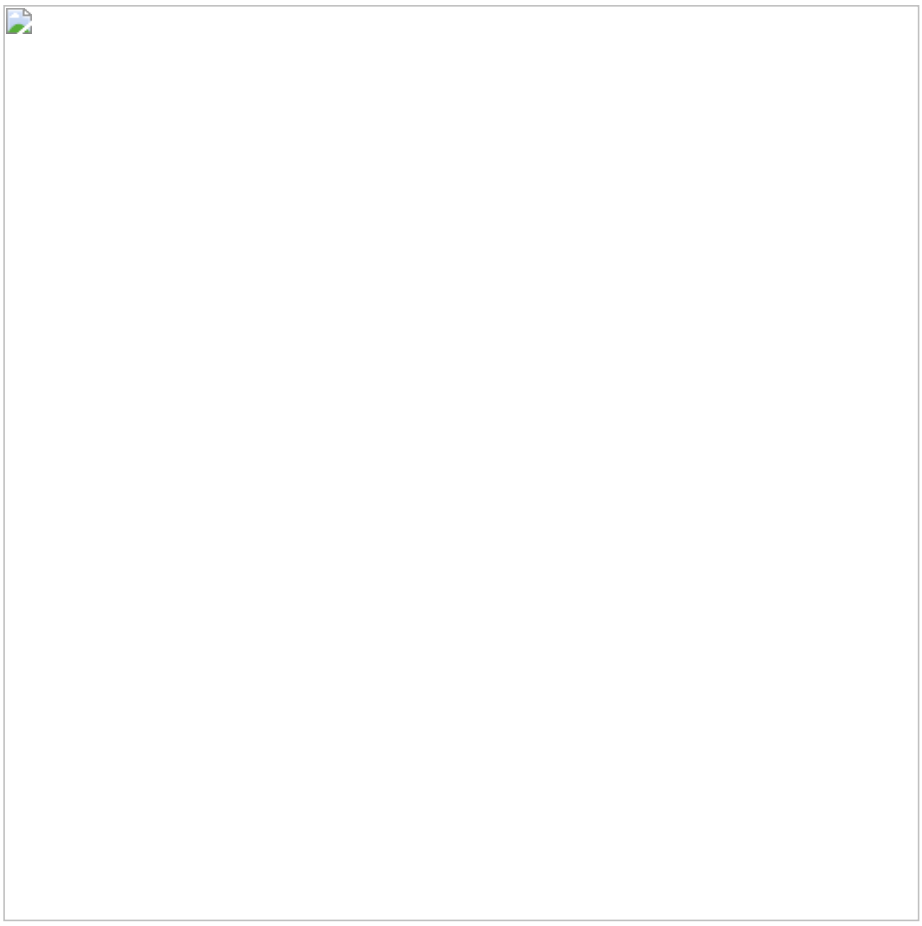


2. If you have Windows Authentication installed for IIS, proceed to step 3. If you don't have Windows Authentication integrated in IIS, add this feature from Server Manager under "Roles / Services" for IIS"EX. IIS Windows Authentication Feature of IIS.

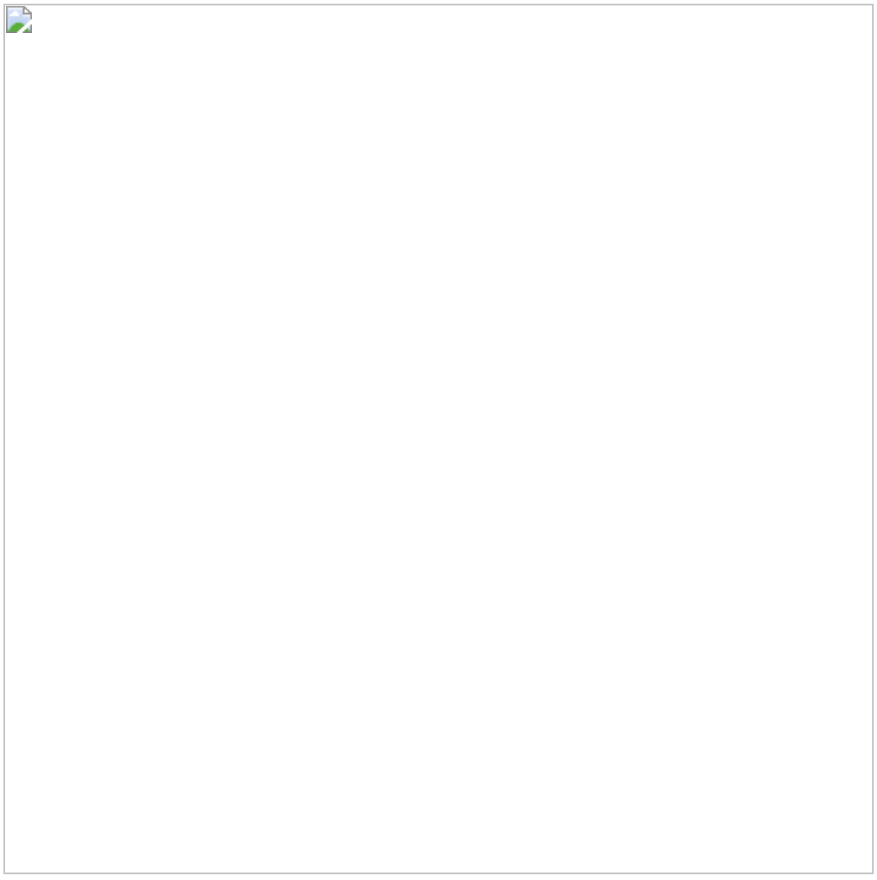
3. Enable the Windows Authentication option for your site:

4. Reconfigure the permissions of the web site. First, we will break inheritance and then we will remove “Users” from having any access:

4.1 Right-click the site select “Edit Permissions”

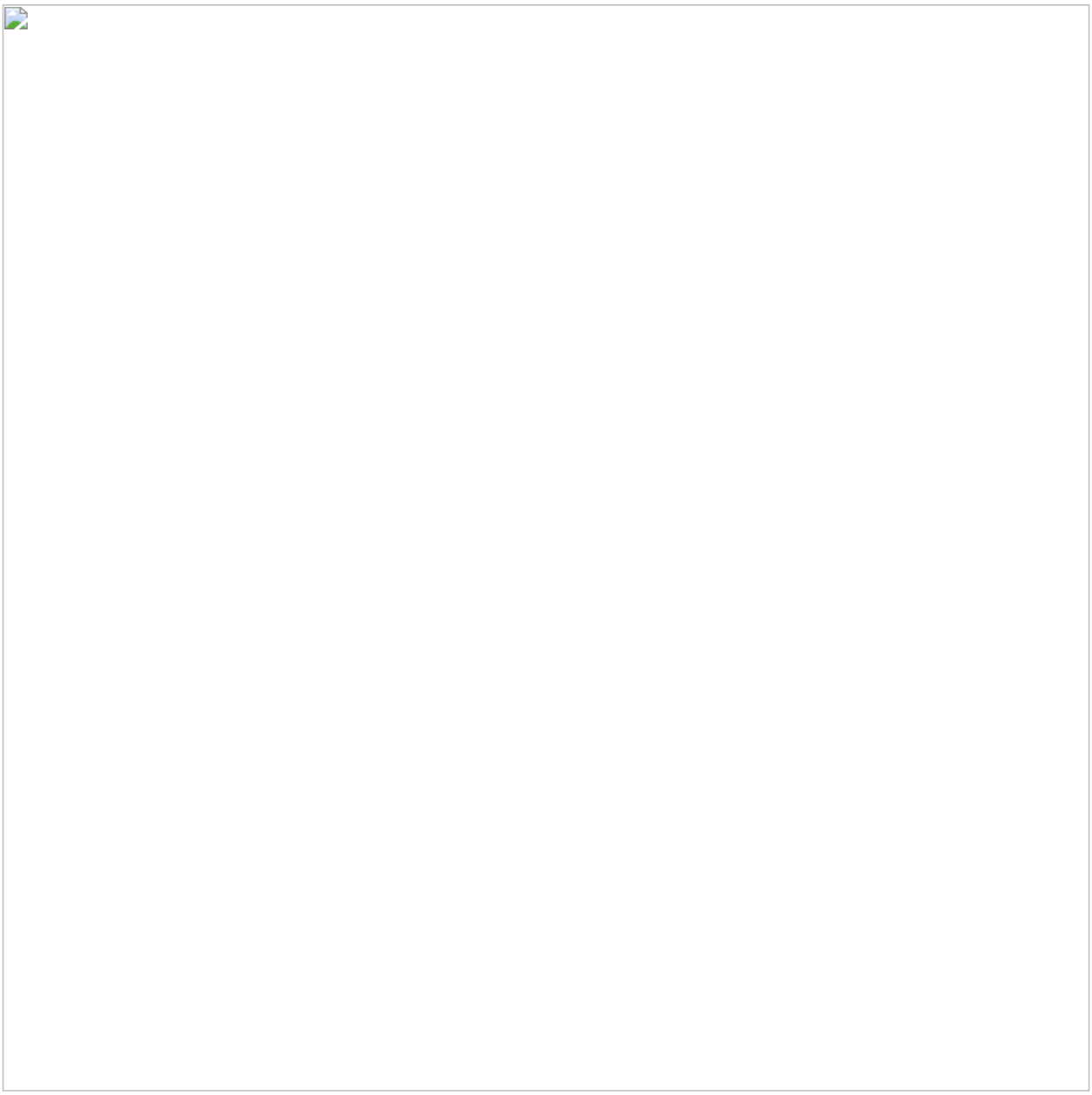


4.2 Click “Advanced.”

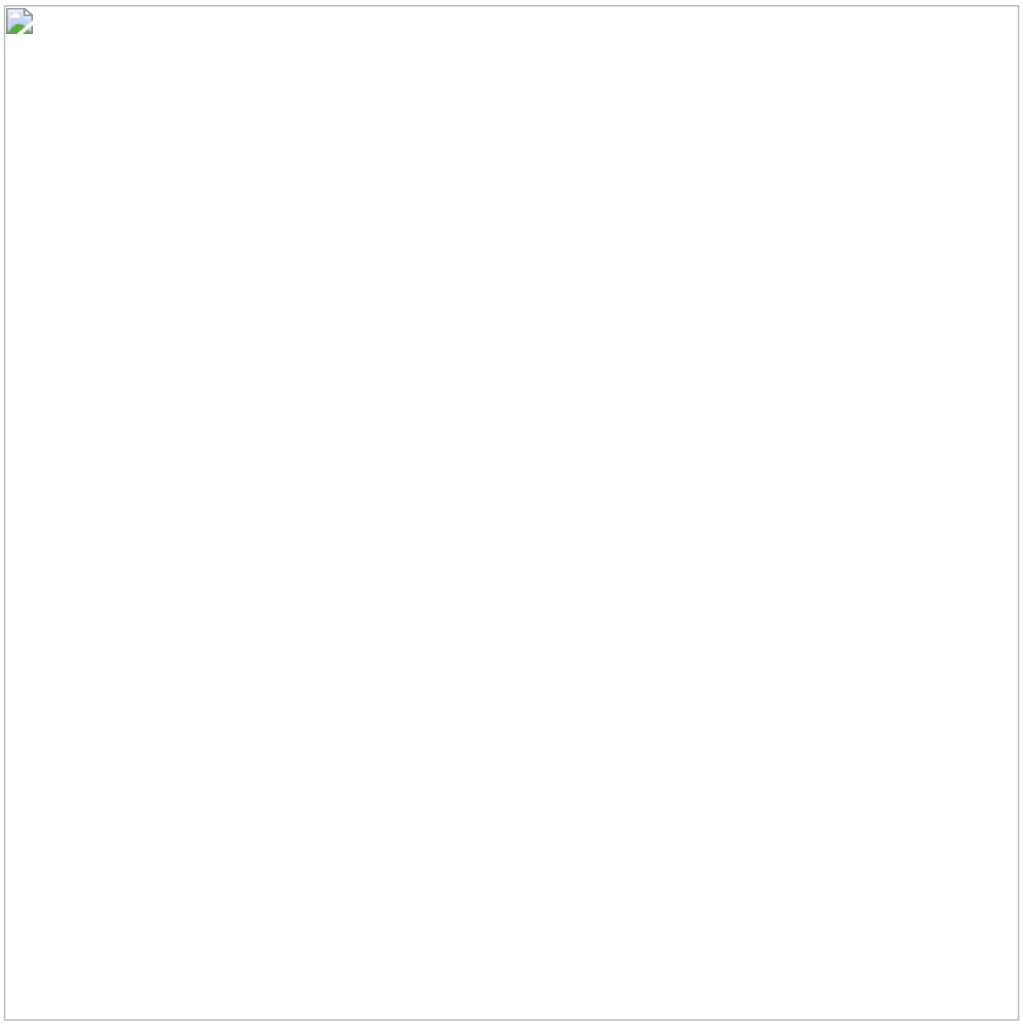


4.3 Click “Change Permissions.”

4.4 Uncheck the box “Include inheritable permissions from this objects parent”. When prompted with a warning**,** select ADD. This simply copies the existing permissions back without inheritance; this is very important as to not break the website for yourself and the system at large.



4.5 Delete the permission for Users. This will disable the ability for any domain users to simply authenticate to your site to view the reports, while allowing local administrators and members of IIS_IUSRS to log in and view reports. (The set of base permissions can vary from OS to OS.) Also make sure that security principals like “Everyone” and “Authenticated Users” do not have any access.



4.6 Last, you can now use the basic “Edit” button to add Read Only access for select users and groups. In my case, I gave Read access to my reports to Frank. For basic site usage, nothing more then Read access is really needed; don’t give anyone Modify or Full Control access unless there is some special need.

Note that I did this testing on Windows 2008 and Win 7, and I did not need to bounce IIS for any of these configuration changes to start working.

How can Netwrix help?

Netwrix StealthAUDIT can help you enhance the security of your Windows infrastructure and minimize the risk of a data breach. It empowers you to:

- Identify vulnerabilities that can be used by attackers to compromise Windows systems and get to your data.
- Enforce security and operational policies through baseline configuration analysis.
- Audit and govern privileged accounts.
- Prove compliance more easily with prebuilt reports and complete system transparency.

FAQ

What is Windows Authentication in IIS?

Windows Authentication in IIS is a secure type of authentication in which user account credentials are hashed before being transmitted over the network.

Is Windows Authentication the same as Active Directory?

No. You can use Windows Authentication even if your server is not a member of an Active Directory domain.

Does IIS Windows Authentication use LDAP?

No. IIS Windows Authentication supports only the Kerberos and NTLM protocols.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.