

Configuring Authentication Service on Microsoft Windows 7

John R. Vacca

This appendix describes the configuration of Windows 7 authentication service features that are relevant to IT professionals. The authentication service features included with Windows 7 extend to a strong set of platform-based authentication features to help provide better security, manageability, and user experience.

1. CONFIGURING WINDOWS 7 AUTHENTICATION (WEB SERVER (IIS 7))

Use Windows authentication when you want clients to authenticate using the NT LAN Manager (NTLM) or Kerberos protocols. The default authentication configuration for IIS 7 enables Anonymous authentication only [1].

Windows authentication, which includes both NTLM and Kerberos v5 or higher authentication, is best suited for an intranet environment for the following reasons:

- Client computers and Web servers are in the same domain.
- Administrators can make sure that every client browser is Internet Explorer 2.0 or later versions.
- HTTP proxy connections, which are not supported by NTLM, are not required.
- Kerberos v5 or higher requires a connection to Active Directory, which is not feasible in an Internet environment [1].

Important

Windows Authentication is not supported by Home or Starter editions of Windows Vista[®] and Windows[®] 7. To see which IIS features are supported on your operating system, see one of the following:

- If you are using Windows Vista[®] or Windows Server[®] 2008, see Available Role Services in IIS 7.0 ([http://technet.microsoft.com/en-us/library/cc753473\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc753473(WS.10).aspx)).

- If you are using Windows[®] 7 or Windows Server[®] 2008 R2, see Available Web Server (IIS) Role Services in IIS 7.5 (<http://technet.microsoft.com/en-us/library/cc753473.aspx>) [1].

Windows authentication is not appropriate for use in an Internet environment, because that environment does not require or encrypt user credentials. The default setting for Windows authentication is Negotiate. This setting means that the client can select the appropriate security support provider. To force NTLM authentication, you must change the value of the `<Provider>` element under the `<windowsAuthentication>` element in the `ApplicationHost.config` file [1].

Prerequisites

For information about the levels at which you can perform this procedure, and the modules, handlers, and permissions that are required to perform this procedure, see Authentication Feature Requirements (IIS 7) ([http://technet.microsoft.com/en-us/library/cc755253\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755253(v=ws.10).aspx)) [1].

Exceptions to Feature Requirements

None

Modules

`WindowsAuthenticationModule`: To configure Windows authentication, you can perform this procedure by using the user interface (UI), by running `Appcmd.exe` commands in a command-line window, by editing configuration files directly, or by writing Windows Management Instrumentation (WMI) scripts [1].

User Interface (UI)

To use the UI, open IIS Manager and navigate to the level you want to manage. For information about opening IIS

Manager, see Open IIS Manager (IIS 7) ([http://technet.microsoft.com/en-us/library/cc770472\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc770472(v=ws.10).aspx)). For information about navigating to locations in the UI, see Navigation in IIS Manager (IIS 7) ([http://technet.microsoft.com/en-us/library/cc732920\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732920(v=ws.10).aspx)):

1. In **Features View**, double-click **Authentication**.
2. On the **Authentication** page, select **Windows Authentication**.
3. In the **Actions** pane, click **Enable** to use Windows authentication [1].

Note

*Optionally, you can disable Kernel-mode authentication by clicking **Advanced Settings**. As a best practice, you should not disable this setting if you use Kerberos authentication and a custom identity on the application pool [1].*

Command Line

To enable or disable Windows authentication, use the following syntax [1]:

```
appcmd set config /section:windowsAuthentication /enabled:true | false
```

By default, IIS sets the **enabled** attribute to false, which disables Windows authentication. If you set the attribute to true, you enable Windows authentication. For example, to enable Windows Authentication, type the following at the command prompt, and then press ENTER [1]:

```
appcmd set config /section:windowsAuthentication /enabled:true
```

Optionally, you can force Windows authentication to use NTLM, using the following syntax [1]:

```
appcmd set config /section:windowsAuthentication /-providers.[value = 'Negotiate']
```

For more information about Appcmd.exe, see Appcmd.exe (IIS 7) (<http://msdn.microsoft.com/en-us/library/aa347559.aspx>).

Configuration

The procedure in this topic affects the following configuration elements [1]:

```
<windowsAuthentication>
```

For more information about IIS 7 configuration, see IIS 7.0: IIS Settings Schema (<http://msdn.microsoft.com/en-us/library/aa347559.aspx>) on MSDN [1].

WMI

Use the following WMI classes, methods, or properties to perform this procedure [1]:

WindowsAuthenticationSection class

For more information about WMI and IIS, see Windows Management Instrumentation (WMI) in IIS 7 ([http://technet.microsoft.com/en-us/library/cc771707\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc771707(v=ws.10).aspx)). For more information about the classes, methods, or properties associated with this procedure, see the IIS WMI Provider Reference (<http://msdn.microsoft.com/en-us/library/Aa347459>) on the MSDN site [1].

2. CONFIGURING AUTHENTICATION IN IIS 7

Authentication helps you confirm the identity of clients who request access to your sites and applications. IIS 7 supports Anonymous and Integrated Windows authentication by default [2].

IIS 7 supports both *challenge-based* and *login redirection-based* authentication methods. A challenge-based authentication method, for example, Integrated Windows authentication, requires a client to respond correctly to a server-initiated challenge. A login redirection-based authentication method, for example, Forms authentication, relies on redirection to a login page to determine the identity of the user. You cannot use both a challenge-based authentication method and a login redirection-based authentication method at the same time [2].

IIS 7 also supports client certificate authentication, which requires that Secure Sockets Layer (SSL) be configured for the site. For more information about client certificates, see Configuring Server Certificates in IIS 7 ([http://technet.microsoft.com/en-us/library/cc732230\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732230(v=ws.10).aspx)) [2].

Prerequisites

For information about the levels at which you can perform these procedures, and the modules, handlers, and permissions that are required to perform these procedures, see Authentication Feature Requirements (IIS 7) ([http://technet.microsoft.com/en-us/library/cc755253\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc755253(v=ws.10).aspx)) [2].

Procedures

This task includes the following procedures [2]:

- Configure the Anonymous Authentication Identity (IIS 7) [[http://technet.microsoft.com/en-us/library/cc770966\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc770966(v=ws.10).aspx)]
- Configure ASP.NET Impersonation Authentication (IIS 7) [[http://technet.microsoft.com/en-us/library/cc730708\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730708(v=ws.10).aspx)]
- Configure Basic Authentication (IIS 7) [[http://technet.microsoft.com/en-us/library/cc772009\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc772009(v=ws.10).aspx)]

- Configure Client Certificate Mapping Authentication (IIS 7) [[http://technet.microsoft.com/en-us/library/cc732996\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732996(v=ws.10).aspx)]
- Configure Digest Authentication (IIS 7) [[http://technet.microsoft.com/en-us/library/cc754104\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754104(v=ws.10).aspx)]
- Configuring Forms Authentication (IIS 7) [[http://technet.microsoft.com/en-us/library/cc753252\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc753252(v=ws.10).aspx)]
- Configure Windows Authentication (IIS 7) [[http://technet.microsoft.com/en-us/library/cc754628\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754628(v=ws.10).aspx)]
- Configure Extended Protection in IIS 7.5 [[http://technet.microsoft.com/en-us/library/ee909472\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee909472(v=ws.10).aspx)]

REFERENCES

- [1] Configure Windows Authentication (IIS 7), Microsoft TechNet, © 2013 Microsoft Corporation. All rights reserved. Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, 2013.
- [2] Configuring Authentication in IIS 7, Microsoft TechNet, © 2013 Microsoft Corporation. All rights reserved. Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, 2013.

