

Plan authentication methods (SharePoint Server 2010)

Updated: 2009-11-12

[This article is pre-release documentation and is subject to change in future releases.]

This article describes the authentication methods that are supported by Microsoft SharePoint Server 2010. Authentication is the process of validating a user's identity. After a user's identity is validated, the authorization process determines which sites, content, and other features the user can access.

In this article:

[Supported authentication methods](#)

[Configure authentication](#)

[Plan authentication for crawling content](#)

[Choose methods of authentication allowed in your environment](#)

[Planning zones for your authentication design](#)

[Choose methods of authentication allowed in your environment](#)

Supported authentication methods

SharePoint Server 2010 provides a flexible and extensible authentication system, which supports authentication for identity management systems that are based or are not based on the Microsoft Windows operating system. By integrating with ASP .NET pluggable authentication, SharePoint Server 2010 supports a variety of authentication scenarios, including:

Using standard Windows authentication methods.

Using a simple database of user names and passwords.

Connecting directly to an organization's identity management system.

Using two or more methods of authentication for accessing partner applications (for example, connecting to your partner company's identity management system for authenticating partner employees while using Windows authentication methods to authenticate your internal employees).

The following table lists the supported authentication methods:

| Authentication method | Description | Examples |
|-----------------------|--|----------------|
| Claims | Claims authentication for SharePoint Server 2010 is built on the Windows Identity Foundation, which is a set of .NET Framework classes that are used to implement claims-based identity. | Not applicable |

| | | |
|----------------------------------|---|---|
| Windows | The standard IIS Windows authentication methods are supported. | <p>Anonymous</p> <p>Basic</p> <p>Digest</p> <p>Certificates</p> <p>Kerberos (Integrated Windows)</p> <p>NTLM (Integrated Windows)</p> |
| Forms-based authentication (FBA) | SharePoint Server 2010 adds support for identity management systems that are not based on Windows by integrating with forms-based authentication. Forms-based authentication enables SharePoint Server 2010 to work with identity management systems that implement the MembershipProvider interface. You do not need to rewrite the security administration pages or manage shadow Active Directory directory service accounts. | <p>Lightweight Directory Access Protocol (LDAP)</p> <p>SQL database or other database</p> <p>Other forms-based authentication solutions</p> |

Authentication of system accounts

Forms-based authentication can be used to authenticate only user accounts. The process accounts used to connect to Microsoft SQL Server database software and run the farm must be Windows accounts, even when using alternative methods of authentication to authenticate users.

SharePoint Server 2010 supports SQL Server authentication and local computer process accounts for farms that are not running Active Directory Domain Services (AD DS). For example, you can implement local accounts by using identical user names and passwords across all servers within a farm.

[Claims-based authentication vs. classic-mode authentication](#)

In SharePoint Server 2010, you can choose between claims-based authentication or classic mode authentication when you create a Web application.

[Claims-based authentication](#)

The claims-based authentication model for SharePoint Server 2010 is built on the Windows Identity Foundation (WIF). Claims-based authentication in SharePoint Server 2010 enables authentication across Windows-based systems and systems that are not Windows-based. Claims-based authentication supports delegation of user identity between applications. Using claims-based authentication, you can implement multiple forms of authentication on a single zone.

Classic-mode authentication

Classic-mode authentication refers to the Integrated Windows authentication model supported in Windows SharePoint Services 3.0. In classic-mode authentication, no claims augmentation is performed and the new claims authentication features are not supported. Using classic-mode authentication, you can implement all of the previously supported forms of authentication with a limit of one form of authentication for each zone.

Configure authentication

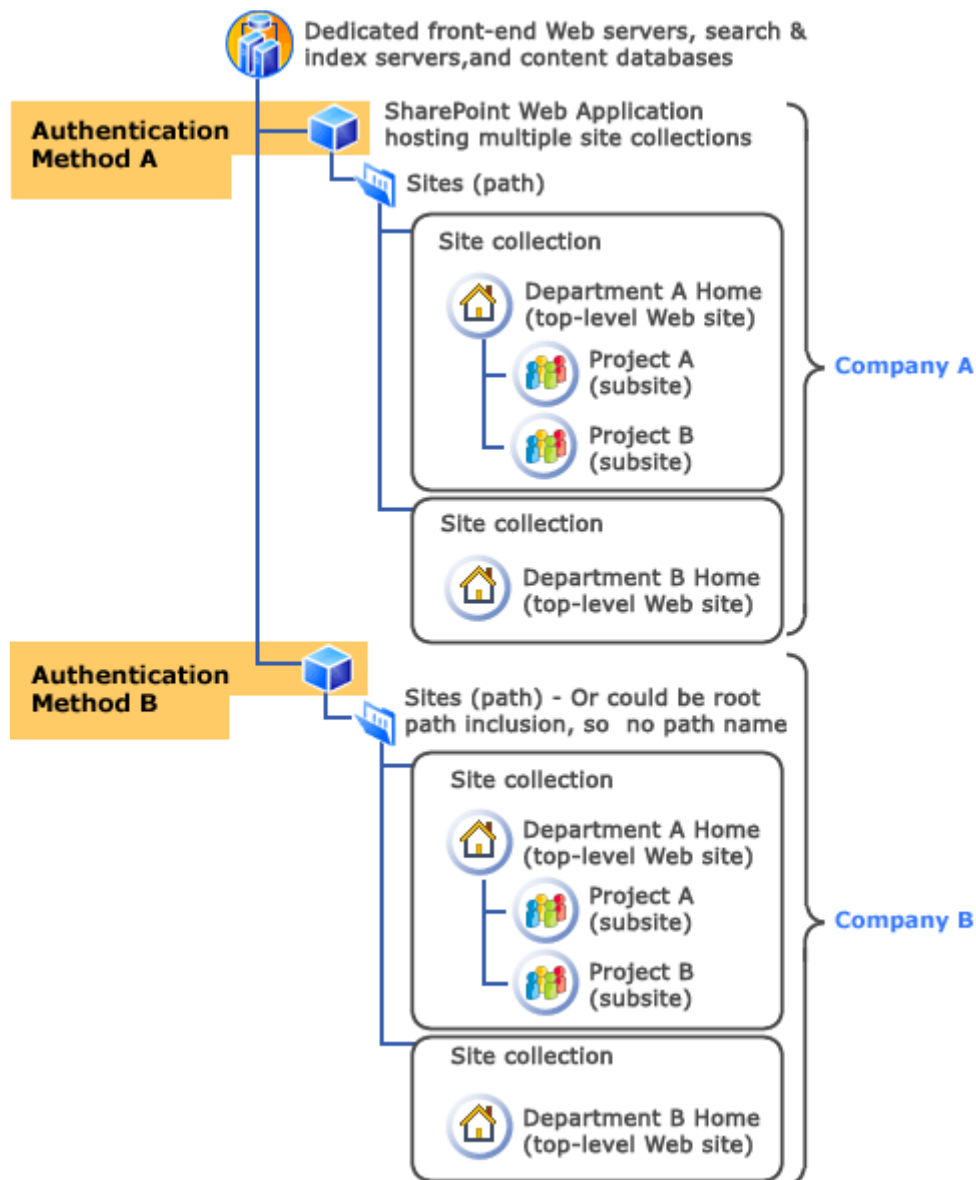
Claims-based authentication introduces new options for configuring authentication for Web applications and zones. This section provides a summary of how authentication is configured in SharePoint Server 2010. This information will help you understand how to put together an authentication strategy for your solution and determine who in your organization needs to be involved in planning for authentication.

Configure claims-based authentication for SharePoint Web applications

Claims-based authentication is initiated with the Integrated Windows sign-in process. After the Windows user **WindowsIdentity** object is created, SharePoint Server 2010 converts the **WindowsIdentity** object to a **ClaimsIdentity** object. The **ClaimsIdentity** object is then used to create a token that is issued by SharePoint Server 2010.

Configure authentication for SharePoint Web applications

Authentication in SharePoint Server 2010 is configured at the SharePoint Web application level. The following diagram illustrates a Windows SharePoint Services server farm that is configured to host sites for multiple companies. Authentication is configured separately for each company.



Connect to identity management systems that are external or not based on Windows

To use forms-based authentication to authenticate users against an identity management system that is not based on Windows or that is external, you must register the membership provider in the Web.config file. In addition to registering a membership provider, you can register a role manager. SharePoint Server 2010 uses the standard ASP.NET role manager interface to gather group information about the current user. Each ASP.NET role is treated like a domain group by the authorization process in SharePoint Server 2010. You register role managers in the Web.config file the same way you register membership providers for authentication.

If you want to manage membership user or roles from the Central Administration site, you can register the membership provider and the role manager in the Web.config file for the Central Administration site in addition to registering these in the Web.config file for the Web application that hosts the content.

Ensure that the membership provider name and role manager name that you registered in the Web.config file is the same as the name that you entered in Central Administration. If you do not enter the role manager in the Web.config file, the default provider specified in the machine.config file might be used instead.

For example, the following string in a Web.config file specifies a SQL membership provider:

[Copy Code](#)

```
<membership defaultProvider="AspNetSqlMembershipProvider">
```

Integrating with forms-based authentication places additional requirements on the authentication provider. In addition to registering the various elements in the Web.config file, the membership provider, role manager, and HTTP module must be programmed to interact with SharePoint Server 2010 and ASP.NET methods, as indicated in the following table.

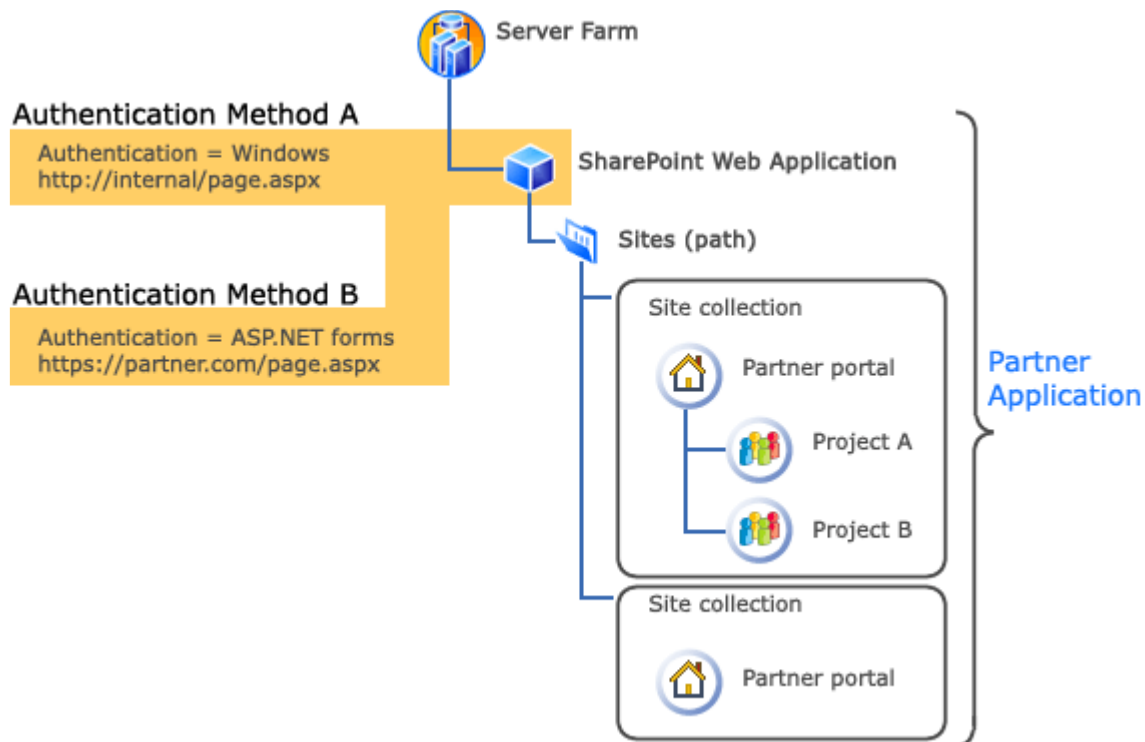
| Category | Description |
|---------------------|--|
| Membership provider | <p>To work with SharePoint Server 2010, the membership provider must implement the following methods:</p> <p>GetUser (String): SharePoint Server 2010 calls this method to resolve user names during invitations and to get the user's display name.</p> <p>GetUserNameByEmail: SharePoint Server 2010 calls this method to resolve user names in invitations.</p> <p>FindUsersByName and FindUsersByEmail: SharePoint Server 2010 calls these methods to populate the user picker control on the Add Users page. If the membership provider does not return any users, the picker will not function and administrators will need to type the user name or e-mail address in the Add User text box.</p> |
| Role manager | <p>The role manager must implement the following methods:</p> <p>RoleExists: SharePoint Server 2010 calls this method during invitations to verify that a role name exists.</p> <p>GetRolesForUser: SharePoint Server 2010 calls this method at access check to gather the roles for the current user.</p> <p>GetAllRoles: SharePoint Server 2010 calls this method to populate the group and role picker. If the role provider does not return any groups or roles, the SharePoint Server 2010 picker will not function and the administrator will need to type the name of the role in the Add User text box.</p> |

Enabling anonymous access

You can enable anonymous access for a Web application in addition to configuring a more secure authentication method. With this configuration, administrators of sites within the Web application can choose to allow anonymous access. If anonymous users want to gain access to secured resources and capabilities, they can click a logon button to submit their credentials.

Using different authentication methods to access a site

You can configure Web applications in SharePoint Server 2010 to be accessed by up to five different authentication methods or identity management systems. The following figure illustrates a partner application that is configured to be accessed by users from two different identity management systems. Internal employees are authenticated by using one of the standard Windows authentication methods. Employees of the partner company are authenticated against their own company's identity management system.



To configure a Web application to be accessed by two or more different authentication systems, you must configure additional zones for the Web application. Zones represent different logical paths of gaining access to the same physical application. With a typical partner application, employees of a partner company access the application through the Internet, while internal employees access the application directly through the intranet.

To create a new zone, extend the Web application. On the Extend Web Application to Another IIS Web Site page, in the **Load Balanced URL** section, specify the URL and zone type. The zone type is simply a category name applied to the zone and does not affect the configuration of the zone.

After extending the Web application, you can configure a separate authentication method for the new zone. The default zone is the zone used by internal employees. The Internet zone is configured for partner access and uses forms-based authentication to authenticate partner employees against the partner identity management system.

Plan authentication for crawling content

To perform successful crawls of content in a Web application, you must understand the authentication requirements of the index component of the search server (also known as the *crawler*). This section describes how to configure authentication for Web applications to ensure that the content in those Web applications can be successfully crawled.

When a farm administrator creates a Web application by using all default settings, the default zone for that Web application is configured to use NTLM. The farm administrator can change the authentication method for the default zone to any authentication method supported by SharePoint Server 2010.

The farm administrator can also extend a Web application one or more times to enable additional zones. Up to five zones can be associated with a particular Web application, and each zone can be configured to use any authentication method supported by SharePoint Server 2010.

Order in which the crawler accesses zones

When planning the zones for a Web application, consider the polling order in which the crawler accesses zones when attempting to authenticate. The polling order is important, because if the crawler encounters a zone configured to use basic, digest, or Kerberos authentication, authentication fails and the crawler does not attempt to access the next zone in the polling order. If this occurs, the crawler will not crawl content on that Web application.

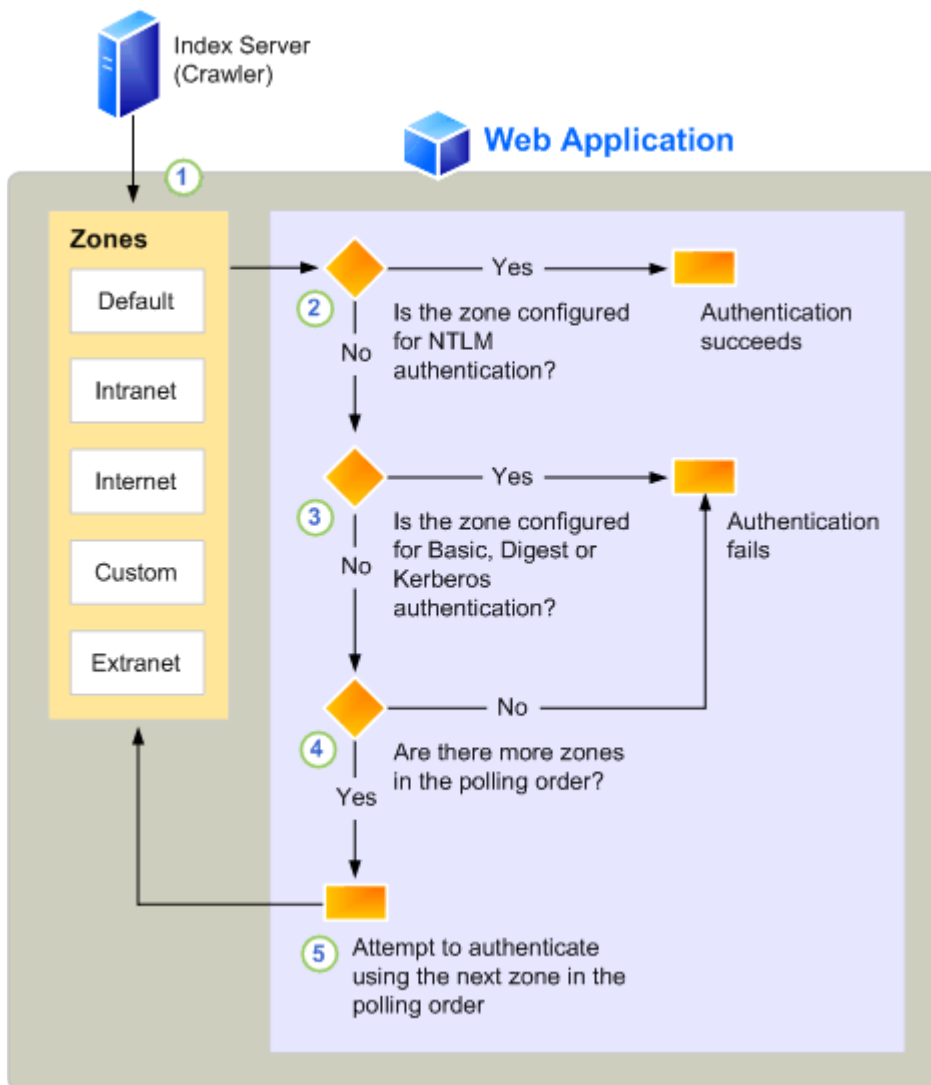
Tip:

Ensure that a zone configured for NTLM is earlier in the polling order than a zone configured for basic, digest, or Kerberos authentication.

The crawler polls the zones in the following order:

- Default zone
- Intranet zone
- Internet zone
- Custom zone
- Extranet zone

The following figure shows the decisions that are made by the authentication system when the crawler attempts to authenticate:



The following table describes the actions associated with each callout in the figure.

| Callout | Action |
|---------|--|
| 1 | Crawler attempts to authenticate by using the default zone. Note: The crawler always attempts to use the default zone first when attempting to authenticate for a particular Web application. |
| 2 | If the zone is configured for NTLM, the crawler is authenticated and proceeds to the authorization phase. |
| 3 | If the zone is configured for basic, digest, or Kerberos authentication, authentication fails and the crawler does not attempt to authenticate by using another zone. This means the content is not crawled. |
| 4 | If there are no more zones in the polling order, authentication fails and the content is not crawled. |
| 5 | Crawler attempts to authenticate by using the next zone in the polling order. |

If you configure the Default zone to use an authentication method that the crawler does not support — for example, forms-based authentication — you must create at least one additional zone and configure this zone to use NTLM authentication. Consider the following scenario.

Planning zones for your authentication design

If you plan to implement more than one authentication method for a Web application by using zones, use the following guidelines:

Use the Default zone to implement your most secure authentication settings. If a request cannot be associated with a specific zone, the authentication settings and other security policies of the default zone are applied. The Default zone is the zone that is created when you initially create a Web application. Typically, the most secure authentication settings are designed for end-user access. Consequently, end users are likely to access the Default zone.

Use the minimum number of zones that is required by the application. Each zone is associated with a new IIS site and domain for accessing the Web application. Only add new access points when these are required.

If you want content within the Web application to be included in search results, ensure that at least one zone is configured to use NTLM authentication. NTLM authentication is required by the index component to crawl content. Do not create a dedicated zone for the index component unless necessary.

Choose methods of authentication allowed in your environment

In addition to understanding how authentication is configured, planning for authentication includes:

Considering the security context or environment of your Web application in SharePoint Server 2010.

Evaluating the recommendations and tradeoffs for each method.

Understanding how user credentials and related identity data are cached and consumed by SharePoint Server 2010.

Understanding how user accounts are managed.

Ensuring that authentication methods are compatible with browsers that are used by your users.

Recommendations for specific security environments

Your choice of authentication methods will primarily be driven by the security context of your application. The following table provides recommendations based on the most common security environments.

| Environment | Considerations |
|-------------------------------|--|
| Internal intranet | At a minimum, protect user credentials from plain view. Integrate with the user management system that is implemented in your environment. If Active Directory Domain Services (AD DS) is implemented, use the Windows authentication methods built into IIS. |
| External secure collaboration | Configure a separate zone for each partner company that connects to the site. If a contributor is no longer employed by a partner company, the contributor cannot continue to gain access to your partner application. |
| External anonymous | Enable anonymous access (no authentication) and allow Read-Only permissions for users who connect from the Internet. If you want to provide targeted or role-based content, you can use forms-based authentication to register users by using a simple database of user names and roles. Use the registration process to identify users by role (such as doctor, patient, or pharmacist). When users log on, your site can present content that is specific to the user role. In this scenario, authentication is not used to validate credentials or to limit who can access the content; the authentication process simply provides a method of targeting content. |

Recommendations and tradeoffs for authentication methods

Understanding the advantages, recommendations, and tradeoffs for each specific authentication method can help you to determine which methods to use in your environment. The following table highlights the recommendations and tradeoffs for each authentication method. For more information about each of the Windows authentication methods supported by IIS, see [IIS Authentication](http://go.microsoft.com/fwlink/?LinkId=78066&clcid=0x409) [<http://go.microsoft.com/fwlink/?LinkId=78066&clcid=0x409>] (<http://go.microsoft.com/fwlink/?LinkId=78066&clcid=0x409>).

| Authentication method | Advantages and recommendations | Tradeoffs |
|-----------------------|---|--|
| Claims | Claims authentication is implemented as a collection of assertions that are encapsulated in security tokens that determine if a user is permitted to access various network resources. Assertions can include a user name, a role, an employee ID, and a variety of other attributes that can be used to determine authorization and permission levels. | Configuration and management requires additional planning and training. |
| Windows | <p>Authenticate by using your existing Active Directory accounts.</p> <p>Simplify user management.</p> <p>Take advantage of Active Directory groups when configuring SharePoint Server 2010 authorization.</p> | Some IIS authentication protocols are not supported by all Web browsers. |

| | | |
|----------------------------|---|---|
| Forms-based authentication | Avoid writing custom code. | <p>Requires customization of the Web.config file.</p> <p>Subject to replay attacks for the lifetime of the cookie, unless using SSL Transport Layer Security (TLS).</p> |
| | <p>Set up SharePoint Server 2010 in an environment that does not use AD DS (does not require Windows accounts).</p> <p>Authenticate against two or more different identity management systems when creating partner applications.</p> <p>Implement a custom authentication scheme using arbitrary criteria.</p> <p>Authenticate users coming from the Internet.</p> | |

Management of user identity information

How user credentials and other identity information is processed and used by SharePoint Server 2010 can influence your decision about which authentication option is best for your intended purpose. This section details how user identity information is processed in the following categories:

Binary IDs: How user binary identifiers (IDs) are created or used by SharePoint Server 2010.

Caching: The process of retaining a user's identity for a period of time to avoid repeating the authentication process for each request.

Role and group membership: In addition to determining who users are, the authentication process also determines which groups or roles a user belongs to. This information is used during the authorization process to determine which actions a user has permissions to perform. For the purpose of authorization, SharePoint Server 2010 treats Active Directory groups and ASP.NET roles as the same type of entity.

The following table details how SharePoint Server 2010 manages user binary IDs, cached user data, and role and group membership data depending on which authentication method is used.

| Item | Windows authentication | Forms-based authentication |
|---------------------------|---|---|
| Binary IDs | SharePoint Server 2010 uses the Windows security identifier (SID). | SharePoint Server 2010 creates a unique binary ID by combining the provider name with the user name. |
| Caching | User credentials are cached and managed by IIS, Internet Explorer, and Windows. | ASP.NET uses an encrypted cookie to keep the user's credentials for the duration of a session. |
| Role and group membership | Windows maintains the list of Active Directory domain groups the user belongs to in the access token. SharePoint Server 2010 uses information stored in the access token. | When a role manager is registered, SharePoint Server 2010 uses the standard role manager interface to gather group information about the current user. Each ASP.NET role is treated like a domain group by the authorization process. ASP.NET can cache the roles the user belongs to |

in a cookie, depending on the settings that are configured in the Web.config file.

Management of user accounts

Understanding how SharePoint Server 2010 handles typical user account management tasks can also influence which authentication method you choose. Generally, users who are members of an authentication provider in one zone can manage accounts across all zones as long as they are granted permissions. The information in the following list applies regardless of which authentication method is implemented:

Adding and inviting new users: You can add or invite a new user from any zone and all authentication methods that are configured if the membership provider and role manager are registered in the current Web.config file. When you add a new user, SharePoint Server 2010 resolves the user name against the following sources in the following order:

The UserInfoList table stored by SharePoint Server 2010. User information will be in this list if users have already been added to another site.

The authentication provider that is configured for the current zone. For example, if a user is a member of the authentication provider that is configured for the default zone, SharePoint Server 2010 first checks this associated membership provider.

All other authentication providers.

Deleting users: User accounts are marked as deleted in the SharePoint Server 2010 database. However, the user record is not removed.

Some user account management behaviors within SharePoint Server 2010 differ, depending on the authentication provider. The following table highlights several common user account tasks that differ depending on the authentication method that is implemented.

| Task | Windows authenticated accounts | Forms-based authentication authenticated accounts |
|-------------------------------|---|---|
| Adding and inviting new users | SharePoint Server 2010 validates user identities by using AD DS. | SharePoint Server 2010 calls the membership provider and the role manager to verify that the user and roles exists. |
| Changes to logon names | Updated user names are automatically recognized by SharePoint Server 2010. New entries are not added to the UserInfoList table. | You must delete the old account name and then add the new account name. Permissions cannot be migrated. |
| Logging on | If Integrated Windows authentication (Kerberos or NTLM) is used and the browser is configured to automatically log on, users do not need to manually log on to SharePoint sites. By default, Internet Explorer is configured to automatically log on to intranet sites. If a logon is required (for example, sites that require a different set of credentials), users are prompted only for a user name and password. However, if basic authentication is used, or the user is using a browser that is not configured to automatically log on, users might be prompted for logon credentials when they access a SharePoint site. | SharePoint Server 2010 provides a standard logon page for use with forms authentication. This page includes the following fields: user name, password, sign in automatically (to persist the cookie). You can create your own logon page to add additional logon controls (for example, create a new account, or reset password). |