Introduction

Microsoft SharePoint is a platform for building and deploying collaborative solutions. It is a centralized web portal that tracks content and documents as well as users, audiences and teams. One of the major challenges for the SharePoint IT administrator is to understand and effectively manage SharePoint user access along with the multiple directory services that co-exist within the corporate network, including numerous web applications, sites, and multiple authentication servers. Since an increasing number of companies are deploying SharePoint on a global enterprise network, connecting a large number of users and in the process creating a structure of corporate hierarchy-based users as well as a formidable social network, user access must be regulated and managed effectively.
This article provides a detailed look at how users and security are managed and configured within SharePoint. It will give you a systematic overview of SharePoint architecture, user authentication configurations, and user security groups and permissions, and explain the differences between Microsoft Office SharePoint Server (MOSS) and Windows SharePoint Services (WSS). This article is written for the latest SharePoint version 3 release.

**SharePoint Architecture**

User Management in SharePoint with different options and architecture is a very complex subject, and thus it will be worthwhile for us to discuss and understand the out-of-the-box SharePoint user management, security and architecture. The chart in Figure 1 represents the logical SharePoint technology architecture. SharePoint is in its third major release and is comprised of Windows SharePoint Services (WSS) version 3.0 and Microsoft Office SharePoint Server (MOSS) 2007. WSS v3 is a free add-on to the Windows 2003 Server, running on top of SQL Server, Windows 2003 Server and ASP.NET 2.0. MOSS is available in various editions (Standard vs. Enterprise) and options (Excel Services, Content Management, etc.), and runs on top of WSS.

![Figure 1: SharePoint Architecture Overview](image)

Since MOSS is built on Windows SharePoint Services (WSS), they share similar architecture and foundations. MOSS provides more application level features and services. It also has different and more extensive User Profile management than WSS. The important point about this architecture is that SharePoint relies on many user management and security principles from the Network Operating system, Microsoft Internet Information Services (IIS) and ASP.Net foundation. In the rest of this section we will take a look at:

- WSS and MOSS architecture
- SharePoint Security (Authentication and Authorization)
- SharePoint User Profiles in MOSS and WSS
Windows SharePoint Services Architecture

WSS is the core platform for SharePoint services. WSS is a logical three-tier that contains a Front End Web Server, a Search and Index server and a Database Server (see Figure 2).

![Figure 2: WSS Architecture](image)

WSS is essentially a web-based ASP.NET application that extends an IIS web site processing HTML requests through a set of ASP.NET (.aspx) pages, .Net application programming interface (API), and XML web services. It processes and executes the business logic using a combination of .Net and SharePoint objects assemblies. The data is stored in the backend SQL database. SharePoint presents the information to end users in the standard HTML format compatible with most web browsers. An IIS web site that has been extended with WSS is called a **Web Application** *(virtual server in previous WSS versions)*. SharePoint Web Applications use an HttpModule and an HttpHandler to re-route incoming traffic to the SharePoint business logic, thus enabling the SharePoint Web Application to coexist with other IIS web applications. Note that this architecture also allows SharePoint and other web applications to share the same user security infrastructure, mainly Windows Server and ASP.NET.

The Search and Index server is an executable (MSSearch.exe) that is installed as web services in Windows Server. Its primary job is to index the content of the database to enable searching on SharePoint lists, documents, and files. Note that MOSS uses entirely different search architecture than WSS.

WSS uses Microsoft SQL Server to store both the configuration and the content in the databases. When WSS is installed it creates a configuration database that stores the metadata, physical configuration and information about every web application that has been extended, as well as all the servers and their roles in the farm. WSS also create an Admin database that stores the content of the Central Administrator toll. In addition, for every extended virtual server, WSS creates a Content Database that stores the actual site content. Note that WSS stores the user information in its content database.

![Figure 3: WSS Farm Provision](image)

WSS is also designed to be scalable. In a large or medium server farm, you can assign a multiple cluster database backend and install load balanced architecture for the front end web server as shown in Figure 3. Note that there is only a single Configuration database for all SharePoint servers in the farm.

Page 3 of 17
MOSS Architecture

Although MOSS runs on top of the WSS platform, MOSS provides a number of extended applications and features, such as: Advanced content management and publishing sites, the ability to search the contents of external databases, and more site templates and workspaces.

Instead of running the Search and Index on the same box as WSS, MOSS uses another application server called Shared Services. This is a collection of application servers (a set of services) that can be configured on one server and shared across many different MOSS portal sites and WSS sites. The services on these servers include enterprise level applications such as Search, Index, User Profile, Content Management, My Sites, Business Data Catalogue, Form Services, Excel Services, Job Scheduling and Usage Reporting.

Another important architectural difference from WSS is the Search database is created for each Shared Services Provider (SSP) database in the farm. The SSP Search database contains search related information such as crawl properties, document properties and propagation properties.

From the user management perspective, MOSS also has several additional services that differentiate it from WSS: Audience, User Profiles database, and Single-Sign-On (SSO). The SSP database contains important data such as the Business Data Catalogue, Site Usage data, BI information and several tables for user management:

- User Profile information that is imported from a directory service such as Active Directory.
- Audiences and organizational hierarchies.
- Security information.

SharePoint Hierarchy

Another important topic that you need to understand related to SharePoint user management is the hierarchy, or scope of the SharePoint architecture. The security and user permissions are applied based on the scope. SharePoint uses the following hierarchy:
1. **Farm**: This is the highest available level, and refers to all SharePoint installations within a server farm. It can contain multiple servers, but each farm has a single configuration database.

2. **Web Application**: A Web Application is the container for all sites on a particular server, on a specified IP address and port. Web applications map to one IIS web site, which also map to exactly one SSP. This is what was called Virtual Server in SPv2. As previously mentioned, this is an IIS site that is extended to work with SharePoint.

3. **Site Collection**: A site collection is a top level site where all sites within a particular web application are grouped. Each site collection has the same content database.

4. **Web**: Refers to an individual site within a site collection. This is the lowest available level.

**SharePoint User Authentication**

SharePoint security consists of two main parts: Authentication and Authorization. This section will focus on the Authentication process, which determines how user identity is verified before allowing access to SharePoint sites.

SharePoint itself does NOT handle user authentication, but relies on Windows, ASP.NET and IIS to perform that function. Authentication in WSS v3 has been redesigned on top of the new authentication provider infrastructure introduced with ASP.NET 2.0. SharePoint is shipped out of the box to work with Windows Authentication, but also allows users the capability to work with SQL Server based form authentication. The following identity management systems are supported:

- **Windows**: All Microsoft Internet Information Services (IIS) and Windows authentication integration options, including Basic, Digest, Certificates, Windows NT LAN Manager (NTLM), and Kerberos. Windows authentication allows IIS to perform the authentication for Windows SharePoint Services.

- **ASP.NET Forms**: A non-Windows identity management system that uses the pluggable Microsoft ASP.NET form-based authentication system. This mode allows Windows SharePoint Services to work with a variety of identity management systems, including externally defined groups or roles such as Lightweight Directory Access Protocol (LDAP) and light-weight database identity management systems. Forms authentication allows ASP.NET to perform the authentication for Windows SharePoint Services, often involving redirect to a log-on page.

- **Delegated**: A system for delegating end-user credentials from a trusted system to Windows SharePoint Services. This allows trusted services to pass user identities to Windows SharePoint Services for authorization, conveying who the current user is without requiring that Windows SharePoint Services have that user's credentials.

Note: In this article we use the terms Authentication Provider or Service (frequently used with Active Directory), User Identity Management (frequently used with a custom system), User Authentication System, and User
Membership Provider (frequently used to refer to the LDAP provider) interchangeably depending on the context of the topic. In all cases, the term refers to the system that keeps the user information and also provides access permission to SharePoint sites.

Using Multiple Authentication Methods to Access a SharePoint Web Application

You can configure SharePoint Web Applications for access by up to five different authentication methods, thus allowing content of the same web sites to be accessed and authenticated by different target users. For example, employees can be authenticated by using one of the standard Windows authentication methods, which can be Windows integrated login (NTLM) behind the firewall and SSL outside of the firewall. Partners or customers can be authenticated against a simple SQL database Form Authentication or even their own identity management system.

![SharePoint Authentication Zones Diagram](image)

To configure a SharePoint Web Application for access by two or more different authentication systems, you configure additional zones by extending the Web Application in the Central Administrator. SharePoint Zones represent different logical paths of gaining access to the same physical application (see Figure 6). After extending the Web application, you can configure a separate authentication method for the new zone. The available zones are: Default, Intranet, Internet, Custom, and Extranet.

SharePoint User Management

Since SharePoint uses an external user identity provider, its user operation is very simple. The fact that SharePoint can be provisioned in many different ways, and the overlap between WSS and MOSS tends to confuse most users on how it actually works. Here are some of the important points to remember:

- **Creating users:** You do NOT create a user in SharePoint. Users are created in a user directory provider. You can then add or invite a new user to SharePoint.

- **Adding 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, Windows SharePoint Services 3.0 resolves the user name against the following sources in the following order:
  - The UserInfoList table stored by WSS v3. User information is 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, WSS v3 first checks this associated membership provider.
  - All other authentication providers.
- **Deleting users**: User accounts are marked as deleted in the WSS v3 database. However, the user record is not removed.

- **Managing users**: 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.

Some user authentication systems behave differently within WSS v3, depending on the authentication provider. Figure 7 highlights several common user account tasks that differ depending on the authentication method that is implemented.

<table>
<thead>
<tr>
<th>Function</th>
<th>Active Directory</th>
<th>LDAP</th>
<th>Form Authentication</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Users</td>
<td>AD Console</td>
<td>LDAP Console</td>
<td>Form Console</td>
<td>Custom method</td>
</tr>
<tr>
<td>Add Users to SharePoint</td>
<td>SharePoint Top Site Collection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Users</td>
<td>You can remove users from SharePoint. Use the membership console to delete users.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Password</td>
<td>AD or Windows</td>
<td>LDAP Console</td>
<td>Form Console</td>
<td>Custom method</td>
</tr>
<tr>
<td>Change User Profile</td>
<td>Change user profile in MOSS’s Central Admin</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 7: User Authentication Methods Comparison**

Note also that MOSS does NOT provide any user management functionalities. Although MOSS provides a User Profile database, MOSS uses WSS to handle user management. We will address the differences between User Management and User Profile Management in the next section.

**User Profile Management**

When you are using just WSS, the user management situation is pretty simple as shown in Figure 8. WSS has a People and Groups feature that keeps track of user information. The user information is managed by:

1. When you add a user to WSS, the system adds a limited number of properties from the user authentication provider (e.g. Active Directory) to the WSS Content database’s User Info table. This is a one-time sync between the User Directory provider to the WSS database as shown in path 1 in Figure 8. WSS tries to map as much information from the User Directory Services to the UserInfo table as possible on the initial sync.
2. You can add extra columns to the user info list, but they must be updated manually and are not synced with the User Directory services as shown in path 2 in Figure 8.

3. This user information is stored per site (remember, this is not per SharePoint Web, it is the top site collection). Clicking on the "My Settings" link takes you to a page where this information can be maintained.

MOSS, on the other hand, is a little confusing. MOSS has a User Profile database that is stored in the SSP database. It provides a much more extensive User Profile feature that allows for scheduled synchronization from one or more User Directory Services, which could be AD/LDAP/BDC/Custom, at regular intervals. You can also define properties and set various policies on how data is imported from various User Directory Services.

As you can see in Figure 9, there are more complex conditions in MOSS when dealing with user management. The user information is propagated between various databases.

Figure 9: MOSS User Profiles

1. Since MOSS is based on WSS, it also lets WSS manage its own user information. When you add a user to a MOSS site, such as a Team Site, WSS still copies a subset of the user information from the User Directory Services (AD) to the UserInfo table in the content database, as shown in path 1 in Figure 9.

2. At the same time, when you add a user to MOSS, it also checks to see if that user already has a record in its User Profile database. If a record does not exist, it creates a record in the User Profile table.

3. The User Profile table is stored in the Shared Services Provider (SSP) database. Remember that SSP is independent of any front-end Web Application, thus it can manage the users within a farm that has multiple Web Applications.

4. The SSP User Profile database is updated from the profile information in the User Directory services via a scheduled update. This is done in the Central Admin site of the SharePoint Farm. You can specify when this import runs, and what properties are imported to SSP. This is path 2 in Figure 9.

5. MOSS replicates the profile information in the SSP database to the individual content database’s UserInfo table via a scheduled update. This timer runs every hour and copies properties, such as picture,
With a MOSS installation, you also need to be aware of several differences from a WSS-only installation:

1. The most confusing factor for some people is how MOSS displays user information. When you view an item’s CreatedBy and ModifiedBy, those fields came from the UserInfo table in the content database. But when you view information in My Site, that information comes directly from SSP’s User Profile database. If you update a user profile in MOSS, there might be some delay in propagating this information from the SSP database into the UserInfo table and thus create lots of confusion.

2. Since SSP-based User Profile information exists, if you edit MySettings at a SharePoint site collection, it actually edits the User Profile information in the SSP database. This is different from a normal WSS mode where My Settings updates the information in the UserInfo table.

3. Individual users can manage their information in the UserInfo table via the MySettings link, which is either the standard display form (userdisp.aspx), or the edit form (useredit.aspx). This information is overridden by the User Profile database in the SSP.

To make it even more confusing, if your SharePoint installation has My Sites enabled, things are more convoluted. In MOSS, My Sites are special SharePoint sites that are personalized for each user. My Sites are enabled by default, and every user in an organization has a unique My Site. The reason that site personalization is stored in SSP is so that larger organizations that have multiple Web Applications and Portal sites can reference ONE personalization site.

As soon as the My Site feature is activated, any User Profiles from an existing installation of WSS are replaced by the public profiles that are part of My Site. A My Site link is added to the top menu bar for all sites in the site collection, along with the My Links menu. In other words:

1. If My Sites is enabled, the user has to manage their profile information via their My Site link. The link at My Settings in this configuration is read-only.

2. If My Sites is enabled, then administrators can and should manage User Profile information via the SSP profile database, or My Settings for the user being edited.

Lastly, deletion of a user profile also has implications in MOSS. When you delete a User Profile in MOSS, the profile record is moved from the UserProfile table in SSP to the DeleteUsers table, and the deleted user’s My Site becomes inaccessible. This way, if the user is re-imported in at a later date, some information such as Document Libraries and the My Site can be reactivated.

User Profile Information from Business Data Catalog
Business Data Catalog (BDC) is a feature in MOSS that allows users to create an interface to external information systems (databases) without writing any code. You can also import external User Profile information from a BDC.
interface into the MOSS User Profile database. A real world example is to set up a BDC interface to your company payroll or financial system to import employees’ Social Security Numbers into their MOSS User Profiles. This capability also provides some misconceptions on how BDC plays into the overall SharePoint user management capability.

- Although you can import user information from a BDC interface into a MOSS User Profile, similar to how you import data from Active Directory, BDC can NOT act as an authentication provider.
- Although you can import data from a BDC catalog, this can only act as a supplemental import. Another primary user authentication provider (i.e., Active Directory or LDAP) has to be configured as the primary source before you can use BDC. This has implications when you use SQL Forms as your primary authentication provider: you will not be able to set up the automatic import from that source and thus you will also not be able to import supplemental data from a BDC catalog.

**SharePoint Authorization**

Once a user has been authenticated for access to a SharePoint site, the SharePoint authorization process determines which objects in the system a user can access and perform actions on. With the latest release of MOSS 2007, permissions are handled strictly at the WSS platform level.

In this section, we will describe several important concepts that make up the authorization process in SharePoint:

- Permissions
- Permission Levels
- Securable Objects
- SharePoint Groups

**Permissions**

Permissions (rights in previous WSS versions) are the rights for a user to perform specific actions such as viewing pages, editing items, and creating sub-sites. WSS provides 33 pre-defined permissions that you can use to allow users to perform specific actions that are grouped into three main categories: List, Site, or Personal. SharePoint permissions are not assigned directly to users or SharePoint groups, but are assigned to one or more permission levels, which are in turn assigned to users and SharePoint groups.

![Figure 11: SharePoint Permission Levels](image)

**SharePoint Permission Levels**

A SharePoint Permission Level (site groups in previous WSS versions) is a group of permissions that can be granted to users or SharePoint groups so that they can perform specific actions on securable objects such as a site, library, list, folder, item, or document on your site. Permission levels allow you to group permissions and apply them to users and SharePoint groups on various sites in your SharePoint installation.

When you create a new SharePoint site, there are five permission levels provided by default:
• **Full Control**: allows users or groups full control over a site. Full Control is the least restrictive permission level. You cannot modify or remove this permission level.

• **Design**: allows users or groups to view, add, update, delete, approve, and customize lists, libraries, and pages on your site, including themes and style sheets.

• **Contribute**: allows users or groups to view, add, update, and delete previously created list items and document libraries.

• **Read**: allows users or groups to read pages on the site including the resource libraries. Read is the most restrictive permission level.

• **Limited Access**: is a permission level that is automatically assigned to a user or group and therefore cannot be directly assigned by the administrator. It is used when you assign the users or groups to a child object of a parent object to which they do not have access. You cannot modify or remove this permission level.

![Permission Levels](image)

**Figure 12: Definition of SharePoint Permission Levels**

**Securable Objects Permission**

SharePoint provides the ability to manage item level permissions on individual objects (such as lists and libraries), even down to the individual folders, documents, and list items within those lists and libraries. These items that you can apply permissions to are called Securable Objects. Each site contains additional securable objects which have a particular position in the site hierarchy, as shown in Figure 13.
Hierarchy and Inheritance

In SharePoint, permissions on any securable object, such as web sites, lists, libraries, folders and documents, are inherited from their parent object. However, you can break this inheritance for any securable object at a lower level in the hierarchy by creating a unique permission on that securable object. For example, you can create a sub-site (Web) and break the permission inheritance from the parent if you want to limit (or expand) the group of users who can have access permission to the site for security reasons. When you break the inheritance from the parent, the securable object to which you broke the inheritance receives a copy of the parent’s permissions. You can then edit those permissions to be unique — meaning that any changes you make to the permissions on that securable object do not affect the parent.

In our example, sub-sites A, B and C inherit permissions from the top-level Web site. This means that changes made to SharePoint groups and permission levels on the top-level site also affect all of those sub-sites. When you make any change in sub-sites A, B or C, you are actually making changes at the parent site, since SharePoint does not allow you to manage permission on a sub-site that is inheriting permissions from its parent site.

Sub-site D has unique permissions, which are not inherited from its parent site. Therefore, any changes made to the permission levels and SharePoint groups on Sub-site D do not affect its parent site.

SharePoint Users and Groups

You can add a user to SharePoint who has a valid account that has been authenticated as mentioned in SharePoint User Authentication. When a user is added to the system, you can assign permissions directly to a securable object (web, list, library, etc.) or indirectly through a SharePoint Group. Using SharePoint Groups is the
recommended practice when managing security since it’s easier to manage changes for a group than for individual users, and apply the same group to different objects across your sites.

A SharePoint Group (cross site group in previous WSS versions) is a logical grouping of users that you can create to manage permissions to the site and to provide an e-mail distribution list for site members. All SharePoint groups are created at the site collection level and are available to all sub-sites in the site collection. You can also create groups that only have permissions to a particular sub-site as shown in path 1 in Figure 15.

SharePoint groups can contain Windows (Active Directory) security groups, ASP.NET Forms authentication groups (using the roles within the role membership provider), and individual users with a user account on the local server or a Windows domain as shown in path 2 in Figure 15.

SharePoint provides three default SharePoint groups with permissions on the top-level site, each with a Site name prefix. These default groups are also provided when a new site with unique permissions is created.

- **Site Owners**: have Full Control permissions in the site.
- **Site Members**: have Contribute permissions.
- **Site Readers**: have Read permissions.

Each of these SharePoint groups is associated with a default permission level, but you can change the permission level for any SharePoint group as needed.
SharePoint Audience

A practical way to apply user profiles out of the box is audience targeting. Audience targeting refers to the ability to create a group of users based on a specific set of rules and then target content to that specific audience. You can target specific content such as a SharePoint List, library items, navigation links, and Web Parts to a specific group of people.

You can create an audience in MOSS using its Central Administration tool. Audiences are created based on a set of rules. The example in Figure 17 shows how an audience of Sport Fans is created by looking for the world "NFL" in the About Me field in their User Profile.

Once the Audience is created, you can enable audience targeting. Select the securable objects for specific audiences using an Audience Targeting column for the library or list containing the items of interest.
MOSS Single-Sign-On

MOSS provides another capability to help with user security management which is called Single-Sign-On (SSO). This is a feature that does not affect the internal operation of MOSS, and actually is not even installed by the default installation program. SSO is a database created in MOSS to keep and manage a set of user names and passwords that can be used to access specific external systems that require access authentication.

An example is if you have a need to crawl and index a backend office system (e.g. SAP or Oracle) to retrieve information that is then made available to the SharePoint enterprise search. These systems might require login
accounts for access, and the accounts’ access information can be retrieved for those purposes. There are several benefits to using SSO; i.e., the access information is encrypted and is more secure, and the account information can be managed by an IT administrator while the Web Parts or code that use the account do not have to know the account details, but just how to use it.

**Summary**

Hopefully, this article provided you with a solid basic understanding of how SharePoint manages its users. Additional information can be found in various books and online articles; please see the Reference section for suggested reading. Given the complexity of managing users in SharePoint, Bamboo Solutions has provided several web parts that are very useful to help you keep the situation under control and create a happy and productive work force. Check these products out on Bamboo Solutions’ web site:

- **User Management Accelerator.** Spend less time managing your SharePoint user accounts. Simply add, edit, move, and clone user accounts and access security in one place.
- **User Account Setup Web Part.** Create new users quickly and easily in both Active Directory (or NT) and SharePoint from one location to save IT Administrator time and effort.
- **Password Reset Web Part.** Allow SharePoint users to reset their Active Directory or NT password without administrator intervention.
- **Password Change Web Part.** Alleviate the workload of SharePoint Administrators by allowing users to change their own passwords while automatically adhering to your security policy.
- **Password Expiration Web Part.** Send your SharePoint users E-mail notifications before their password expires.
- **User Profile Sync.** Synchronize user profile information between your SharePoint Directory and Active Directory databases.

**Reference**

- MSDN Article: [Microsoft Windows SharePoint Authorization and Authentication](#)
- MSDN Article: [User Profiles and Audience Targeting Overview](#)
- Channel 9 Screen Cast: [Forms Authentication with SharePoint, Anonymous Access and Forms Authentication with WSS 3.0](#)
About the author

Lam Le is a member of the Bamboo Solutions Product Team. As a founding member of Bamboo Solutions, Lam Le brings more than 25 years of experience successfully developing and running high technology product organizations. Le previously served as Principal Technology Advisor for Northup Grumman/PRC, where he formed and managed the product development for enterprise-wide document management software, marketed to both commercial and federal industries. Prior to PRC, he was Principal Engineer for Oracle, leading the team responsible for creating business automation software. He has been involved with numerous products and projects involving SharePoint and Collaboration technology. He can be reached via e-mail.

About Bamboo Solutions Corporation

Bamboo Solutions Corporation is a software technology provider specializing in collaborative software solutions built on Microsoft® SharePoint Technology and Services. Our business collaboration solutions are designed for clients who need rapid implementation, quick user acceptance and immediate productivity gains. Bamboo Solutions is a privately held company with headquarters in Reston, Virginia, USA.

Bamboo Solutions Corporation

11417 Sunset Hills Road, Suite 105

Reston, VA 20190, USA

www.bamboosolutions.com