

About controlling access to sites and site content

As a site owner, when you create the permission structure for your site or grouping of sites, you should balance ease of administration with the need to control specific permissions for individual securable objects. With any Web site, it is also important to follow the principle of least privilege when authorizing access to the site.

For easiest administration, begin by using the standard SharePoint groups (which are *Site name* Owners, *Site name* Members, and *Site name* Visitors) and assigning permissions at the site level. We recommend that you make most users members of the *Site name* Visitors or *Site name* Members SharePoint groups. Do not add every user as a member of the *Site name* Owners SharePoint group. By default, site members can contribute to the site, adding or removing items or documents, but cannot change the structure of the site or change site settings or appearance. You can create additional SharePoint groups and permission levels if you need finer control over the actions that your users can take.

If there are particular lists, libraries, folders within a list or library, list items, or documents that contain sensitive data that must be even more secure, you can use fine-grained permissions to grant permissions to a specific SharePoint group or individual user. Note, however, that managing fine-grained permissions can be a very time-consuming task.

How security elements are assigned to a securable object

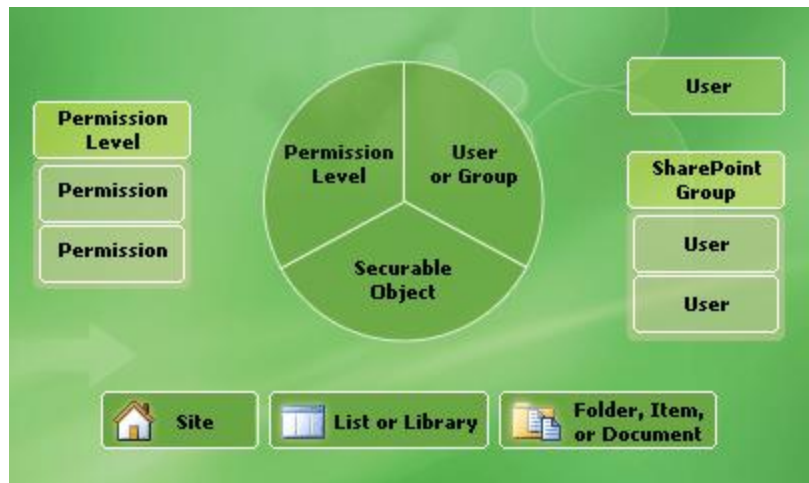
You can grant specific permissions to users and SharePoint groups (that contain users) for a securable object, such as a site, list, library, folder within a list or library, item, or document. Because it is inefficient to maintain user accounts directly, use SharePoint groups as much as possible to manage users.

The following figure illustrates how users and SharePoint groups are assigned specific permission levels on a site or a securable object in a SharePoint site.

* A single user can be directly assigned without needing to be a member of a SharePoint group.

Note that a permission assignment is created on a particular securable object. This permission assignment includes a user or SharePoint group and a permission level. Each permission level has a specific set of permissions.

You can assign different users and SharePoint groups different permission levels for a specific site, list, library, folder within a list or library, list item, or document. Individual users or SharePoint groups can have different permission levels for different securable objects.



Anyone with the Manage Permissions permission can create SharePoint groups

and assign permission levels for the site as a whole. Note, however, that they may not be able to add or remove users or domain groups to or from a SharePoint group. Site collection administrators and site owners have this permission, by default.

List or library administrators can specify more or less restrictive permissions for their list or library (or a folder within the list or library) by adding or removing users or SharePoint groups, or changing the permission levels for users or SharePoint groups.

List item or document creators can specify more or less restrictive permissions for an item or document by adding or removing users or SharePoint groups, or by changing the permission levels for users or SharePoint groups.

Hierarchy and inheritance

By default, permissions on lists, libraries, folders within lists and libraries, items, and documents are inherited from their parent site. However, you can break this inheritance for any securable object at a lower level in the hierarchy by editing the permissions (that is, creating a unique permission assignment) on that securable object. For example, you can edit the permissions for a document library, which breaks the inheritance from the site.

Web sites are themselves a securable object on which permissions can be assigned. You can configure subsites to inherit permissions from a parent site or break the inheritance and create unique permissions for a particular site. Inheriting permissions is the easiest way to manage a group of Web sites. However, if a subsite inherits permissions from its parent, that set of permissions is shared.

CAUTION Owners of subsites that inherit permissions from the parent site can edit the permissions of the parent. Ensure that any changes you make to the permissions on the parent site are appropriate for the parent site and all subsites that inherit those permissions.

The following figure shows a site collection hierarchy with a top-level Web site and subsites that inherit permissions from their parent site as well as a subsite with unique permissions.

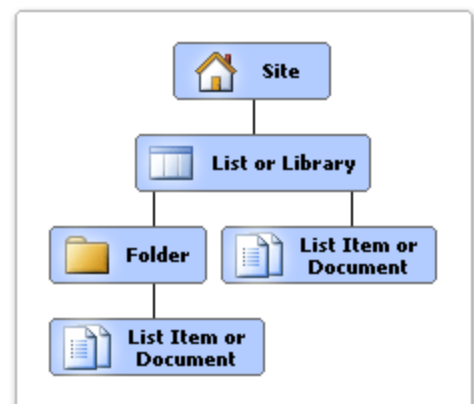
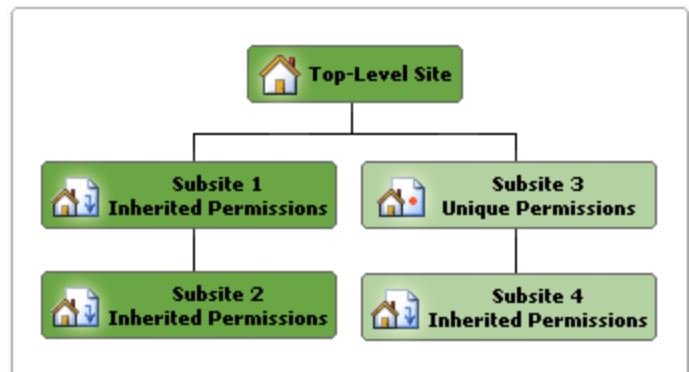
In the figure, subsite 1 inherits permissions from the top-level Web site. This means that changes made to SharePoint groups and permission levels on the top-level site also affect subsite 1.

Subsite 2 is also inheriting permissions from its parent (subsite 1). However, because subsite 1 is also inheriting permissions from its parent, changes made to SharePoint groups and permission levels on the top-level site affect both subsite 2 also. This is because you cannot manage permissions on a subsite that is inheriting permissions. Instead you either manage the permissions of the parent (which is the top-level Web site for subsite 1 and subsite 2) or you can break the inheritance and create unique permissions.

Notice that subsite 3 has unique permissions. This means that it does not inherit permissions from its parent site. Therefore, any changes made to the permission levels and SharePoint groups on subsite 3 do not affect its parent site. Because subsite 4 is inheriting permissions from subsite 3, any changes to permission levels or SharePoint groups on subsite 3 affect both sites.

Each site contains additional securable objects which have a particular position in the site hierarchy, as shown in the following figure.

Lower-level securable objects automatically inherit permissions from their parent. For example, a list or library inherits permissions from the site, and list items and documents inherit permissions from the list, library, or folder that contains them. You can break this inheritance at any point in the hierarchy and assign unique permissions. When you break the inheritance from the parent, the securable object from 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.

Plan for permission inheritance

It is easiest to manage permissions at only the site level, whenever possible. This means you should create your site hierarchy in a way that allows you to assign permissions to sites that are appropriate to all securable objects within the site, such as lists, libraries, folders within lists or libraries, documents, and items. Although you can assign unique permissions on any securable object in the site hierarchy, to do so is more cumbersome than inheriting permissions. It gets more difficult when some lists or libraries within a site have fine-grained permissions applied, and when some sites have subsites with unique permissions and some with inherited permissions. As much as possible, arrange sites, subsites, lists, and libraries so that they can inherit most permissions. Put sensitive data into separate subsites, lists, libraries, and so on.

For example, it is much easier to manage permissions using a hierarchy like the one shown in the following example, rather than mixing sensitive and non-sensitive data in the same sites, lists, and libraries.

Site A Group home page

List A Non-sensitive data (inherited permissions)

Document Library A Non-sensitive data (inherited permissions)

Subsite B Sensitive data (unique permissions)

List B Sensitive data (unique permissions)

Document Library B Sensitive data (unique permissions)

Notice that the list and library in Site A contain non-sensitive data and Subsite B was created below Site A to contain a list and library for storing sensitive data. In this scenario, you can assign permissions to Site A that are appropriate to List A and Document Library A and create unique permissions on Subsite B which are appropriate for List B and Document Library B.