

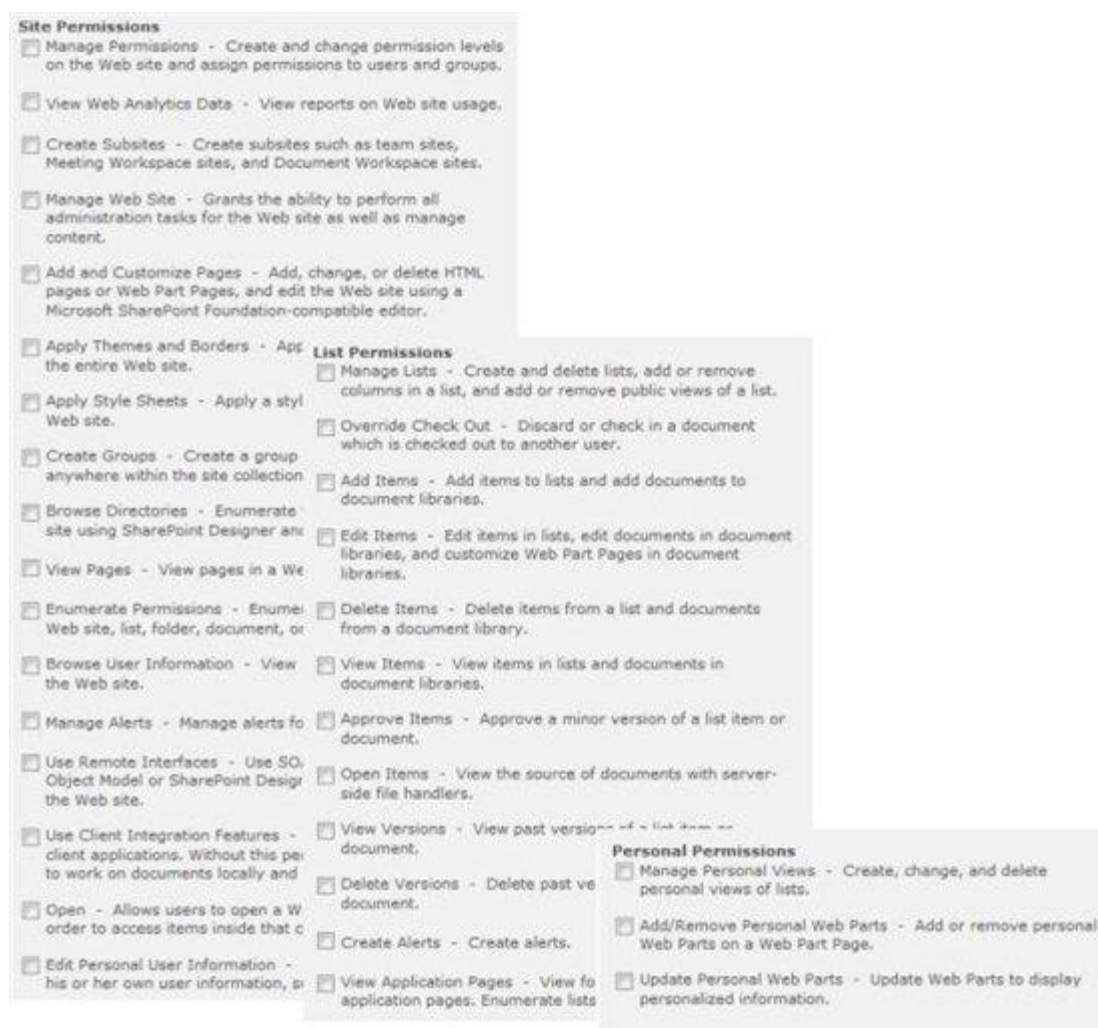
An overview of site permissions

Three concepts

Permissions

Permissions (also called individual permissions or base permissions) grant a user the ability to perform specific actions, such as viewing pages, opening items, and creating subsites. However, unless you are going to add a custom permission level, you have little chance of dealing with these individual permissions (Figure 1).

Figure 1



Permission levels

Permission level is a collection of individual permissions that are bundled together to allow users to perform a set of related tasks. One or more permission levels can be assigned to a user or group.

When we say grant permissions to users or groups, we actually mean grant permission levels to users or groups. Don't be confused by **Grant Permissions** (Figure 2) and **Grant users permission directly** (Figure 3) in the UI; again, permissions here all equal to permission levels. For more information about each permission and permission level, see [User permissions and permission levels \(SharePoint Foundation 2010\)](#) and [User permissions and permission levels \(SharePoint Server 2010\)](#).

Figure 2

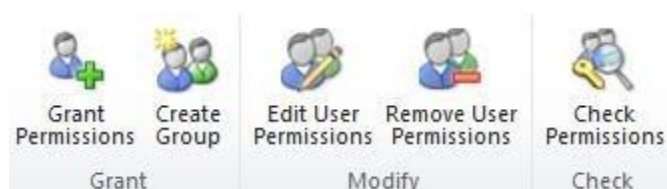
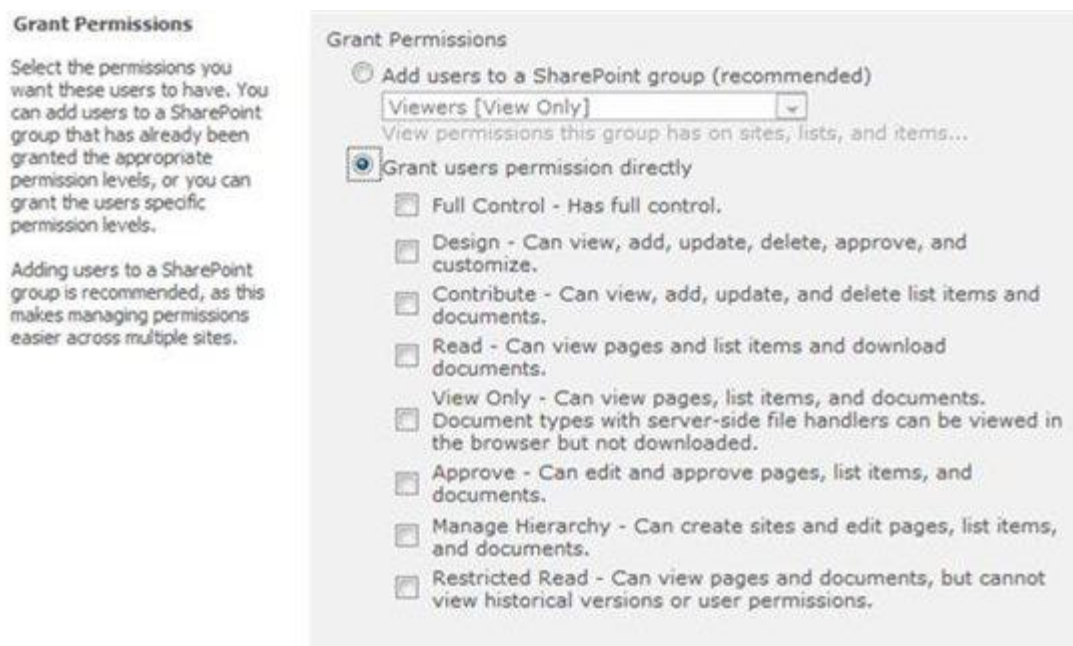


Figure 3



Fine-grained permissions

Site administrators control access to sites and site content by assigning permission levels to users or groups. Permission (level) assignment can happen at any level of a site hierarchy: top-level site, site, subsite, list or library, folder, item or document. If you are assigning permission (level) to a lower level as granular as a list or library, folder, or item or document, we call these permissions (level) *fine-grained permissions*. In some topics, fine-grained permissions are also referred to as "list-level permissions" or

"item-level permissions". For more information about fine-grained permission, download the white paper [Best practices for using fine-grained permissions \(SharePoint Products and Technologies\)](#).

Two factors

In addition to individual permissions, permission levels and fine-grained permissions, there are two key factors related to permission management: permission inheritance and group creation.

Permission inheritance

By default, all sites and content inherit permissions from the parent object above it, all the way up to the top-level site in the site collection (for example, a list item --> folder --> list --> site --> top-level site). Therefore, if you do not break any permission inheritance within a site, the permissions are inherited and shared. However, it is not realistic that all sites and content share the same permissions. SharePoint provides mechanisms to break this inheritance at any site or content level and then to add custom permissions. Figure 4 shows the **Inheritance** group, which can be used to manage permission inheritance.

Figure 4



Note: For ease of management, arrange sites, subsites, lists and libraries so that they can share most of the permissions. Separate sensitive data into their own lists, libraries, or subsites and assign unique permissions there.

Group creation

A SharePoint group is a collection of users that can share the same permissions on a specific site or content. When you create a group, you always bundle a specific permission level to it. Afterwards, when you want to assign someone that specific permission level, simply add the user to the group.

Moreover, you can nest Active Directory groups (to be specific, security groups) in SharePoint groups, which makes permission management much easier. When users come or leave the company, you don't have to manage individual users within the AD group; AD DS (Active Directory Domain Services) manages the users for you. This becomes obvious when you have multiple SharePoint groups that include AD

groups. For more information about recommendations for using security groups, see [Choose security groups \(SharePoint Foundation 2010\)](#) and [Choose security groups \(SharePoint Server 2010\)](#).

Figure 5 shows the **Grant** group, which can be used to create SharePoint groups.

Figure 5



SharePoint groups are usually created at site collection level. If you create a group at a site level (which inherited permissions from its parent site), you cannot grant permission levels to the group directly at that site. Figure 6 shows the resulting message if you try to grant permissions to a group at the site where the group has been created. You can go to its parent site and grant permission level to the group there.

Figure 6



For more information about the three permission concepts and two permission management related factors, see [Plan site permissions \(SharePoint Foundation 2010\)](#) and [Plan site permissions \(SharePoint Server 2010\)](#).

Two new features

The permission features in SharePoint 2010 didn't change much from SharePoint 2007. The following are two main new features I would like to introduce for SharePoint 2010.

Check permissions

Check permissions is a new feature available in SharePoint 2010.

By clicking the **Check Permissions** button (Figure 7), you can determine a user or group's permissions on all site collection resources. You can find the user's directly assigned permissions and the permissions assigned to any groups to which the user belongs (Figure 8).

Figure 7

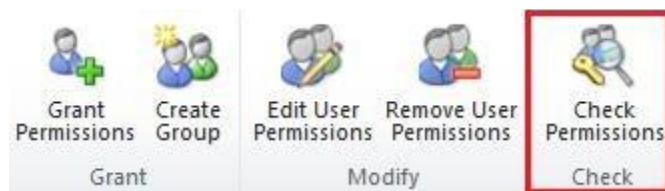



Figure 8

Check Permissions

To check permissions for a user or group, enter their name or e-mail address.

User/Group:  

Permission levels given to Monica Xie (C:\Program Files\Internet Explorer\monica.x)

Limited Access	Given directly
View Only	Given through the "Viewers" group.
Full Control	Given through the "Administrators" Owners" group.
Contribute	Given through the "Administrators" Members" group.
Limited Access	Given through the "Style Resource Readers" group.
Design, Limited Access	Given through the "Designers" group.
Manage Hierarchy	Given through the "Hierarchy Managers" group.
Approve	Given through the "Approvers" group.
Restricted Read	Given through the "Restricted Readers" group.
View Only	Given through the "Monica Group" group.

Inheritance alert bar

Another new feature is the yellow alert bar that indicates the secured content that has unique permissions in a site (Figure 9). You can check that content by clicking the **Show me uniquely secured content** link. The alert bar also indicates the parent site from which you inherited permissions.

Figure 9

