

SharePoint Security and Permissions Overview

A fundamental responsibility concerning site security is to manage who can access resources on your site. The following outlines specifics and best practices in doing just this.

SECURITY PROCESS OVERVIEW

1. How Group Security Works {the process}

Background

- Permissions levels are assigned to groups, people to groups, and groups to site.
- Typically sites will inherit (so have the same) security as the main site.
- In the event you have different needs at the site level, you then would “break inheritance” and have the site use the base security set up from the main site, but then change the appropriate group permissions on THAT site’s settings.

The Steps (on a new site)

1. Once you ensure your permission levels are correct, you then;
2. Create the groups you need on the main site. (Once you create the group, AND users have fully registered for access to their site) you then;
3. Assign the users to groups
4. Once users are assigned to groups, you can start setting permissions for the site(s)/subsites.
5. In order to do this you would go to the applicable site security settings and follow the instructions as applicable for breaking the inheritance and changing permissions for that group.

The Steps (On existing setups)

1. Assuming that you have permissions and groups already in place
2. Assuming you already have the site not inheriting the main site security
3. You would typically at this point just need to add users to the groups as appropriate!
4. In the case you have a “list” (which can also have independent security), you may need to create a permission level specific for that function, create a group for that list, and add users to the group as needed.

BEST PRACTICE: Remove groups you are not using. Ensure groups are named according to their purpose and make SURE they have the appropriate permissions to the site.

BEST PRACTICE: Assign permissions to groups (NOT to individuals). These should be set up FIRST then assigned to groups as appropriate.

NOTE: DO NOT CHANGE DEFAULT LEVELS!!!

PERMISSIONS LEVELS OVERVIEW

1. SharePoint has various Default levels of Permissions.

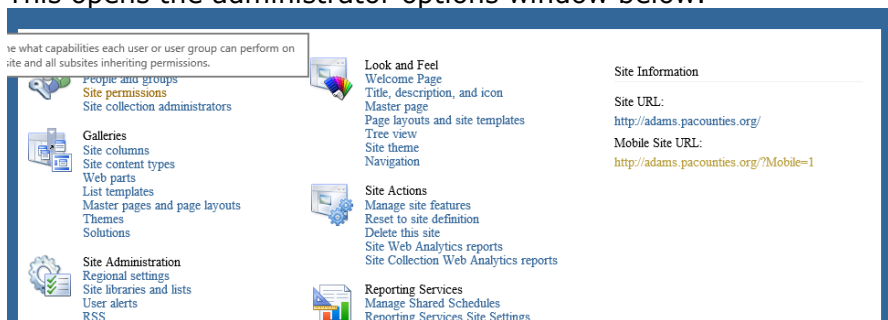
Hint: You may have a need for special permissions (such as “add to list” or “approve” etc. and you can create those here. However, 99% of the time the default (OOTB {out of the box) works fine!

Permission Level	Description
<input type="checkbox"/> Full Control	Has full control.
<input type="checkbox"/> Design	Can view, add, update, delete, approve, and customize.
<input type="checkbox"/> Contribute	Can view, add, update, and delete list items and documents.
<input type="checkbox"/> Read	Can view pages and list items and download documents.
<input type="checkbox"/> Limited Access	Can view specific lists, document libraries, list items, folders, or documents when given permissions.
<input type="checkbox"/> Approve	Can edit and approve pages, list items, and documents.
<input type="checkbox"/> Manage Hierarchy	Can create sites and edit pages, list items, and documents.
<input type="checkbox"/> Restricted Read	Can view pages and documents, but cannot view historical versions or user permissions.
<input type="checkbox"/> View Only	Can view pages, list items, and documents. Document types with server-side file handlers can be viewed in the browser but not downloaded.

2. To access the Permission levels, you:

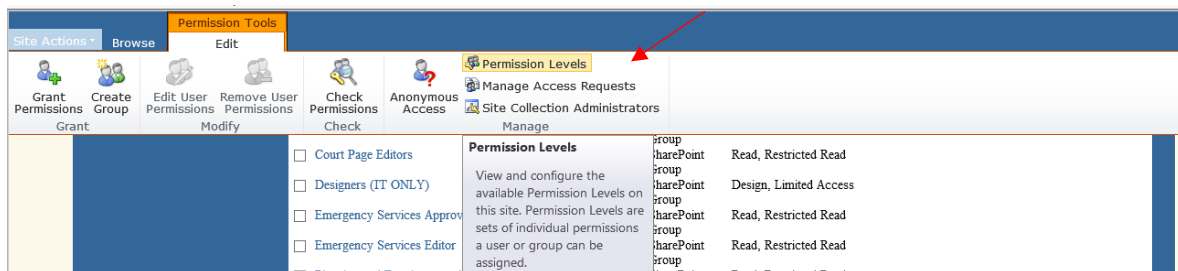
1. Login to the site
2. Click on **Site Actions** -> **Site Settings**

This opens the administrator options window below.



3. Click on **Site Permissions**

4. Now you will see a Ribbon, you select **Permission Levels** on the ribbon



5. You can create custom levels; however, the defaults usually suffice.



6. If you plan on furthering restrictions to your end users, generally this would warrant the creation of a new permission level. (I.E. A level that you can add to a list but not do any other tasks.)
7. These permission levels are the base of the security that you will assign to groups.

SHAREPOINT PERMISSIONS

The following table lists the default permission levels for team sites in SharePoint Server 2010.

Permission level	Description	Permissions included by default
Limited Access	Allows access to shared resources in the Web site so that the users can access an item within the site. Designed to be combined with fine-grained permissions to give users access to a specific list, document library, folder, list item, or document, without giving them access to the entire site. Cannot be customized or deleted.	<ul style="list-style-type: none"> • View Application Pages • Browse User Information • Use Remote Interfaces • Use Client Integration Features • Open
Read	View pages, list items and download documents.	<ul style="list-style-type: none"> • Limited Access permissions, plus: • View Items • Open Items • View Versions • Create Alerts • Use Self-Service Site Creation • View Pages
Contribute	View, add, update, and delete items in the existing lists and document libraries.	<ul style="list-style-type: none"> • Read permissions, plus: • Add Items • Edit Items • Delete Items

		<ul style="list-style-type: none"> • Delete Versions • Browse Directories • Edit Personal User Information • Manage Personal Views • Add/Remove Personal Web Parts • Update Personal Web Parts
Design	View, add, update, delete, approve, and customize items or pages in the Web site.	<ul style="list-style-type: none"> • Approve permissions, plus: • Manage Lists • Add and Customize Pages • Apply Themes and Borders • Apply Style Sheets
Full Control	Allows full control of the scope.	All permissions

If you use a site template other than the team site template, you will see a different list of default SharePoint groups. For example, the following table shows additional permission levels provided with the publishing template.

Permission level	Description	Permissions included by default
Restricted Read	View pages and documents. For publishing sites only.	<ul style="list-style-type: none"> • View Items • Open Items • View Pages • Open

Approve	Edit and approve pages, list items, and documents. For publishing sites only.	<ul style="list-style-type: none"> • Contribute permissions, plus: • Override Checkout • Approve Items
Manage Hierarchy	Create sites; edit pages, list items, and documents. For Publishing sites only.	<ul style="list-style-type: none"> • Design permissions minus the Approve Items, Apply Themes and Borders, and Apply Style Sheets permissions, plus: • Manage permissions • View Web Analytics Data • Create Subsites • Manage Alerts • Enumerate Permissions • Manage Web Site

User permissions

SharePoint Server 2010 includes 33 permissions, which are used in the five default permission levels. You can change which permissions are included in a particular permission level (except for the Limited Access and Full Control permission levels), or you can create a new permission level to contain specific permissions.

Permissions are categorized as list permissions, site permissions, and personal permissions, depending on the objects to which they can be applied. For example, site permissions apply to a particular site, list permissions apply only to lists and libraries, and personal permissions apply only to things such as personal views, private Web Parts, and more. The following tables describe what each permission is used for, the dependent permissions, and the permission levels in which it is included.

List permissions

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Lists	Create and delete lists, add or remove columns in a list, and add or remove public views of a list.	View Items, View Pages, Open, Manage Personal Views	Design, Full Control
Override Check Out	Discard or check in a document that is checked out to another user without saving the current changes.	View Items, View Pages, Open	Design, Full Control

Add Items	Add items to lists, and add documents to document libraries.	View Items, View Pages, Open	Contribute, Design, Full Control
Edit Items	Edit items in lists, edit documents in document libraries, and customize Web Part Pages in document libraries.	View Items, View Pages, Open	Contribute, Design, Full Control
Delete Items	Delete items from a list, and documents from a document library.	View Items, View Pages, Open	Contribute, Design, Full Control
View Items	View items in lists, and documents in document libraries.	View Pages, Open	Read, Contribute, Design, Full Control
Approve Items	Approve minor versions of list items or documents.	Edit Items, View Items, View Pages, Open	Design, Full Control
Open Items	View the source of documents with server-side file handlers.	View Items, View Pages, Open	Read, Contribute, Design, Full Control
View Versions	View past versions of list items or documents.	View Items, Open Items, View Pages, Open	Read, Contribute, Design, Full Control
Delete Versions	Delete past versions of list items or documents.	View Items, View Versions, View Pages, Open	Contribute, Design, Full Control
Create Alerts	Create e-mail alerts.	View Items, View Pages, Open	Read, Contribute, Design, Full Control
View Application Pages	View forms, views, and application pages. Enumerate lists.	Open	All

Site permissions

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Permissions	Create and change permission levels on the Web site and assign permissions to users and groups.	View Items, Open Items, View Versions, Browse Directories, View Pages, Enumerate Permissions,	Full Control

		Browse User Information, Open	
View Usage Data	View reports on Web site usage.	View Pages, Open	Full Control
Create Subsites	Create subsites such as team sites, Meeting Workspace sites, and Document Workspace sites.	View Pages, Browse User Information, Open	Full Control
Manage Web Site	Perform all administration tasks for the Web site, and manage content.	View Items, Add and Customize Pages, Browse Directories, View Pages, Enumerate Permissions, Browse User Information, Open	Full Control
Add and Customize Pages	Add, change, or delete HTML pages or Web Part pages, and edit the Web site by using a Windows SharePoint Services-compatible editor.	View Items, Browse Directories, View Pages, Open	Design, Full Control
Apply Themes and Borders	Apply a theme or borders to the entire Web site.	View Pages, Open	Design, Full Control
Apply Style Sheets	Apply a style sheet (.css file) to the Web site.	View Pages, Open	Design, Full Control
Create Groups	Create a group of users that can be used anywhere within the site collection.	View Pages, Browse User Information, Open	Full Control
Browse Directories	Enumerate files and folders in a Web site by using Microsoft SharePoint Designer 2010 and Web DAV interfaces.	View Pages, Open	Contribute, Design, Full Control
Use Self-Service Site Creation	Create a Web site by using Self-Service Site Creation.	View Pages, Browse User Information, Open	Read, Contribute, Design, Full Control
View Pages	View pages in a Web site.	Open	Read, Contribute, Design, Full Control
Enumerate Permissions	Enumerate permissions on the Web site, list, folder, document, or list item.	Browse Directories, View Pages, Browse User Information, Open	Full Control

Browse User Information	View information about users of the Web site.	Open	All
Manage Alerts	Manage alerts for all users of the Web site.	View Items, View Pages, Open	Full Control
Use Remote Interfaces	Use SOAP, Web DAV, or SharePoint Designer 2010 interfaces to access the Web site.	Open	All
Use Client Integration Features	Use features that start client applications. Without this permission, users must work on documents locally and then upload their changes.	Use Remote Interfaces, Open	All
Open	Open a Web site, list, or folder to access items inside that container.	None	All
Edit Personal User Information	Users can change their own user information, such as adding a picture.	Browse User Information, Open	Contribute, Design, Full Control

Personal permissions

Permission	Description	Dependent permissions	Included in these permission levels by default
Manage Personal Views	Create, change, and delete personal views of lists.	View Items, View Pages, Open	Contribute, Design, Full Control
Add/Remove Personal Web Parts	Add or remove personal Web Parts on a Web Part page.	View Items, View Pages, Open	Contribute, Design, Full Control
Update Personal Web Parts	Update Web Parts to display personalized information.	View Items, View Pages, Open	Contribute, Design, Full Control