**SharePoint Permission and Security Mechanisms**

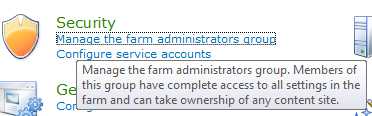
From time to time, our customers ask us about how SharePoint security and permission features work, and how should they be utilized. In this post we try to walk through the basic permission and security features of SharePoint. This post is not intended to be a complete description of every security and permission related feature in SharePoint, but we try to gather all the essential pieces here. We took many screenshots to illustrate what each setting or feature means in practice, enjoy the ride, ;-) !

Additional Resources:

* [Basics: What are permissions?](http://office.microsoft.com/en-us/sharepoint-server-help/basics-what-are-permissions-HA101810704.aspx)

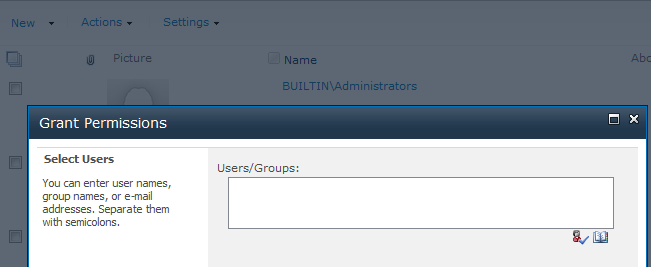
**Farm Administrators**

Farm Administrators group is a group that is managed centrally via SharePoint Central Administration web-site:

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/farm-admins-1.png)

Farm Administrators include by default SharePoint Farm -account, SharePoint installation account and BUILTIN\Administrators group. Farm Administrators have basically “all rights” in SharePoint Farm (or at least they have the ability to get them).

You can give Farm Administration rights to AD groups and AD users:

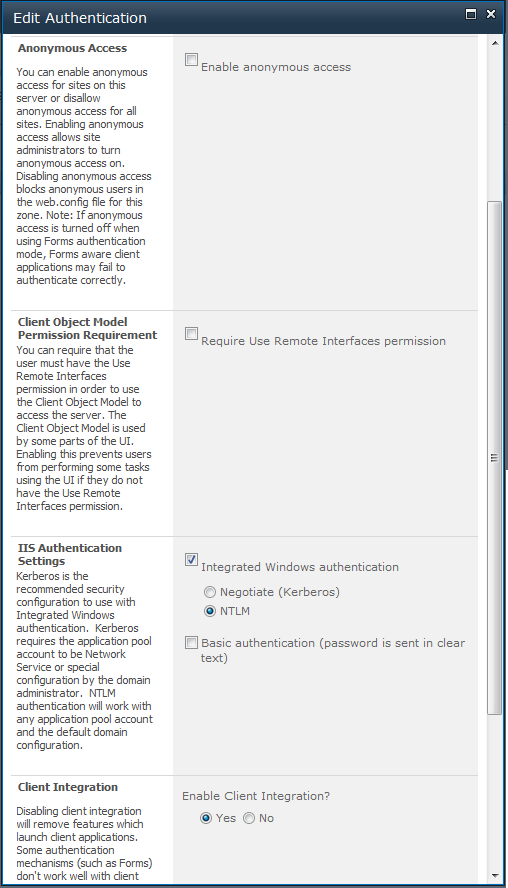
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/farm-admins-2.png)

Additional Resources:

* [Choose administrators and owners for the administration hierarchy (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc263291.aspx)

**Authentication Providers**

With authentication providers you can control how you would like to have your users authenticated in a web application. You can also enable/disable anonymous access and client integration and control client object model permission requirements among others:

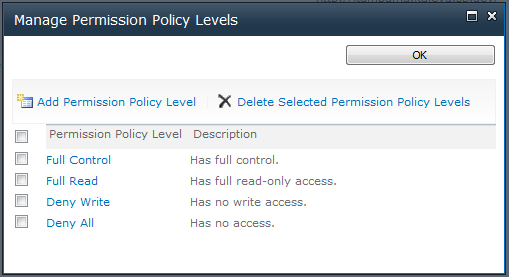
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/misc-auth.png)

Additional Resources:

* [Plan authentication methods (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc262350.aspx)

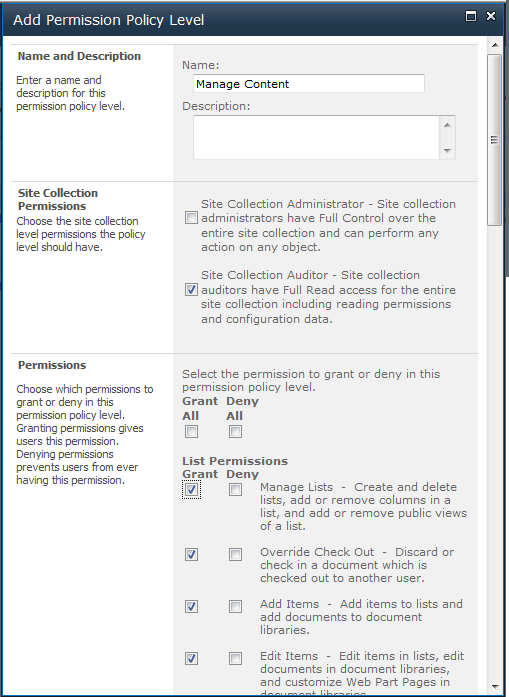
**Web Application Level Permission Policies**

With web application level permission policies you can control centrally, with Central Administration, what kind of permission policies you want to apply to all site collections and sites under specific web application. By default SharePoint gives us four predefined policies:

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/web-app-perm-policy-2.png)

Our recommendation is that you should not edit the default policies, but instead go ahead and create a new policies, if the out of the box policies are not what you are looking for. Policies itself do not grant any permissions unless you attach users or groups to that policy. Policies are just a definitions what the user who has granted the policy can do in the entire web application. With web application policies you can either Grant or Deny the permission.

Here is an example of adding a new web application level permission policy:

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/web-app-perm-policy-3.png)

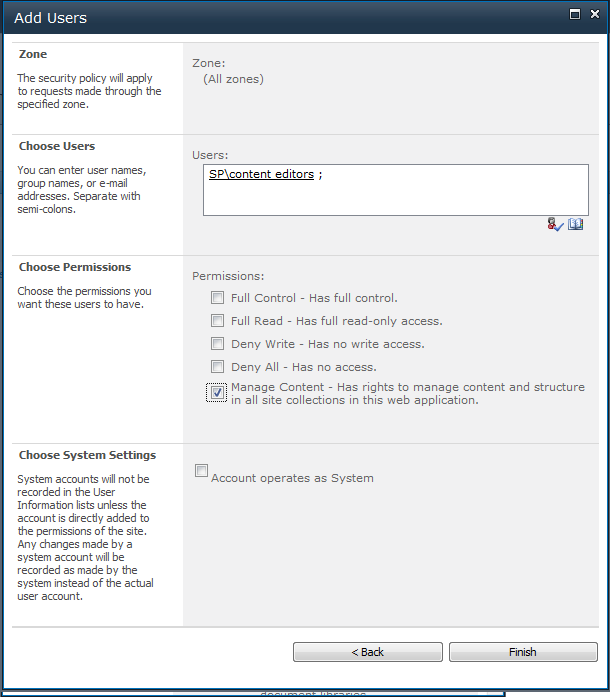
Additional Resources:

* [Manage permission policies for a Web application (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ff608071.aspx)

**Web Application Level User Policies**

User Policy is the place where the magic happens in a web application level. User policy is basically a AD user or AD group mapping to certain Web Application Level Permission policy. You can even define a Zone in which the policy is applied. For example you can use different policy for users who use the SharePoint sites from your internal network (intranet zone), and different policy for those who access the sites through public internet (internet zone), or just apply to “All Zones”. User policies are especially useful for service accounts and in development/integration environments where you probably recreate site collections often (maybe with TFS autobuild scripts).

Here is a screenshot of applying Manage Content -policy to Content Editors AD group:

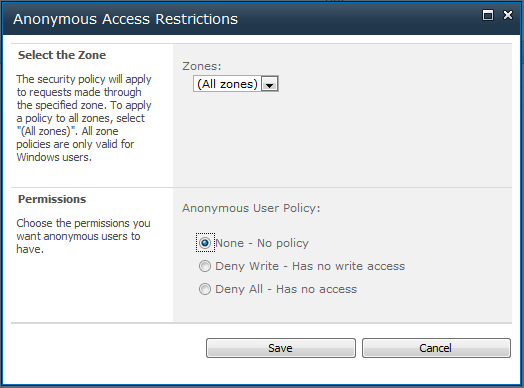
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/web-app-perm-policy-4.png)

Additional Resources:

* [Manage permissions for a Web application (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ff607719.aspx)

**Web Application Level Anonymous Policy**

You can also define web application level anonymous users’ policy through Central Administration -site (but you can only select the policy from a three predefined policies):

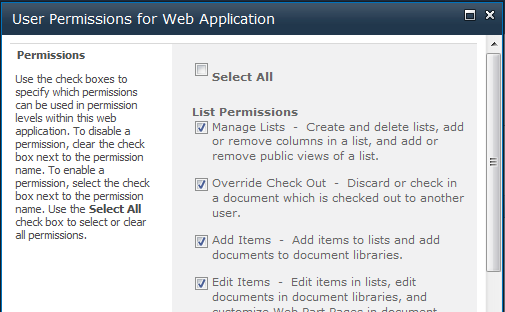
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/web-app-perm-policy-5.png)

Additional Resources:

* [Manage permissions for a Web application (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ff607719.aspx)

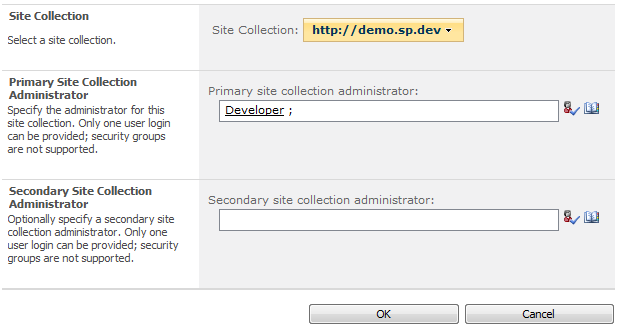
**Web Application Level User Permissions**

This is just a checkbox list from where you can manage what kind of permission levels can be used in a web application and site collections (by default all check boxes are checked, and in general we rarely need to modify the selections):

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/web-app-perm-policy-6.png)

**Site Collection Administrators**

Site Collection Administrators have full control of a specific SharePoint site collection. You can only use AD users (not AD groups, at least with the UI) as site collection administrators (We don’t actually know why it is like that, do you?). With Central Administration site, you can define two users as site collection administrators, but in site collection settings you can add more site collection administrators. Here is a screenshot of Central Administration site collection administrators settings page:

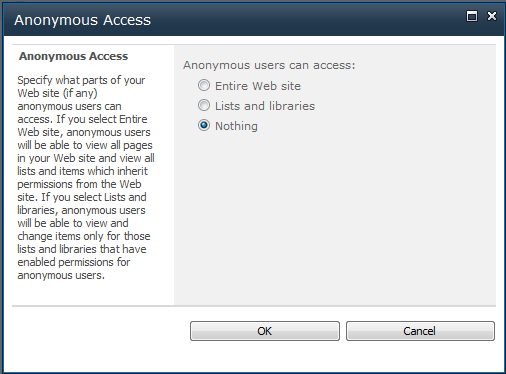
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/sitecol-admin-1.png)

Additional Resources:

* [Add or remove site collection administrators (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ff631156.aspx)
* [Choose administrators and owners for the administration hierarchy (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc263291.aspx)
* [Permissions for site collection administrators](http://office.microsoft.com/en-us/sharepoint-server-help/permissions-for-site-collection-administrators-HA101943260.aspx)

**Anonymous Access Permissions**

You can control what parts of your site the Anonymous users can access with Anonymous Access Setting:

[](http://www.sharepointblues.com/wp-content/uploads/2010/09/site-anon.png)

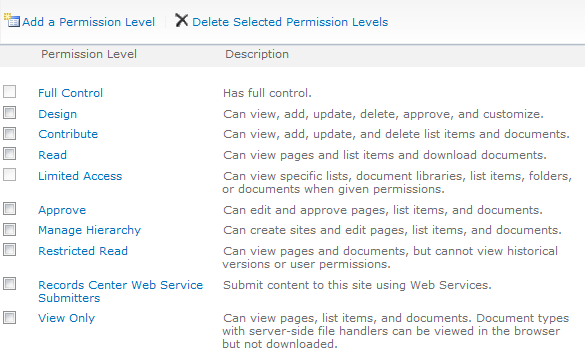
Anonymous access can further be restricted by enabling View Form Pages Lock Down -feature. Our advice is to enable this feature in every public SharePoint site. More about this feature and some other anonymous access suggestions, please consult the following article:

* [Plan security for an external anonymous access environment (Office SharePoint Server)](http://technet.microsoft.com/en-us/library/cc263468(office.12).aspx)

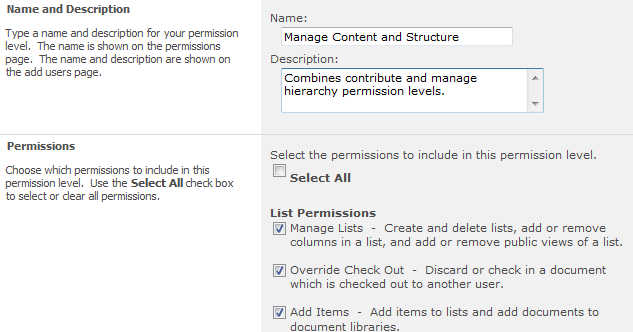
**Site Collection Level Permission Levels**

Like in Web Application level permission policies, these are the actual permissions that SharePoint will check when user accesses resources in a SharePoint site. This time we have Grant only abilities (in Web Application Level Permission Policies you could use Grant and Deny). In itself permission levels are only definitions that group the more fine grained permissions together in a more useful entity.

By Default SharePoint has these permission levels defined in site collections (levels can be a little bit different depending on what features have been enabled in a site collection):

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/perm-levels-1.png)

You can also define your own permission levels, if predefined levels do not match the requirements. As a general principle, it’s not a good idea to modify predefined permission levels (it will only cause confusion). Own permission levels can be created in similar fashion as web application level permission policies:

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/perm-levels-2.png)

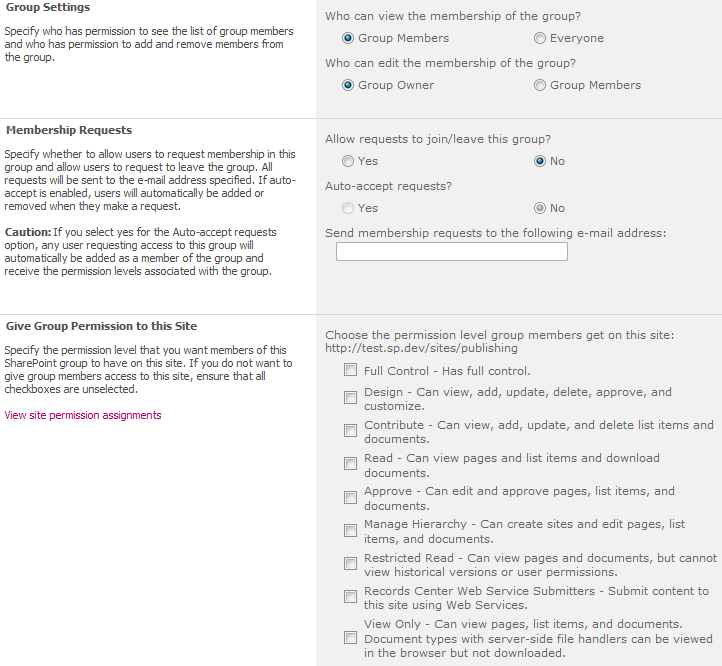
Additional Resources:

* [User permissions and permission levels (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc721640.aspx)
* [Determine permission levels and groups (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc262690.aspx)
* [Edit, create, and delete permission levels](http://office.microsoft.com/en-us/sharepoint-server-help/edit-create-and-delete-permission-levels-HA101805381.aspx?CTT=5&origin=HA101794118)
* [Download a chart of default groups and permission levels](http://office.microsoft.com/en-us/sharepoint-server-help/download-a-chart-of-default-groups-and-permission-levels-HA101994009.aspx)

**SharePoint Groups**

SharePoint groups are a little bit like AD groups, but these groups are managed in SharePoint instead of Active Directory. SharePoint groups can be used to delegate rights management for the site owners instead of system administrators. Whether this is a good thing or not… well it depends on what you want to archive. SharePoint groups are global to the whole site collection. You cannot specify SharePoint group that exists only in a (sub-)site level. SharePoint groups cannot be used over the site collections. One thing SharePoint groups do support that AD groups do not, is membership requests. You can control SharePoint groups’ permission levels whenever you want to use that group. Basically SharePoint group is just a collection of AD groups and AD users with attached permission level(s). While permission level can change for the group the members are globally defined (site collection wide).

Here is a small clipping of Group creation settings (not all settings are visible, but you get an idea):

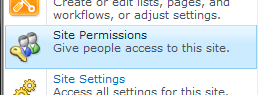
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/group-1.png)

SharePoint Groups do no directly give any rights to ad users or ad groups (unless you use some predefined group that already has for example site level permissions attached to it). You have to use that group somewhere. Next we walk through all the places where you can use SharePoint Groups, AD Groups and AD users to actually give the permissions.

Additional Resources:

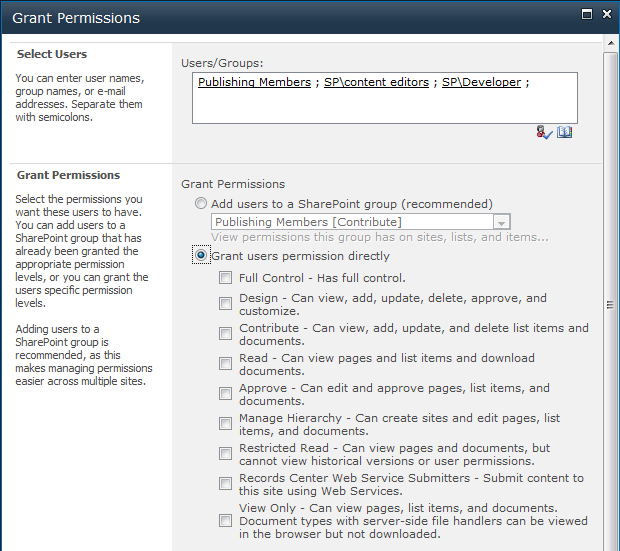
* [Determine permission levels and groups (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc262690.aspx)
* [Manage membership of security group](http://office.microsoft.com/en-us/sharepoint-server-help/manage-membership-of-security-groups-HA101794106.aspx?CTT=5&origin=HA101794118)
* [About security groups](http://office.microsoft.com/en-us/sharepoint-server-help/about-security-groups-HA101794114.aspx)
* [Download a chart of default groups and permission levels](http://office.microsoft.com/en-us/sharepoint-server-help/download-a-chart-of-default-groups-and-permission-levels-HA101994009.aspx)

**Site Permissions**

[](http://www.sharepointblues.com/wp-content/uploads/2010/09/site-perms-2.png)Site permissions is where all the permission management begins. More specifically the root site permissions (root site is the top site in a site collection). These are the permissions that all sub-items (sub-sites, libraries and lists, folders and document sets, documents and items) will inherit. That’s why it is important to carefully design the site permissions as the whole site will use these by default (unless the inheritance chain is broken). Our advice is to try to find some general permissions so that you do no need to break inheritance chain too often.

When you grant site permissions you can use AD groups, AD users and SharePoint groups. You can either add users to some of SharePoint groups or grant the permissions directly (aka attach permission level to user or group). I’m not sure why Microsoft recommends granting permissions though SharePoint Groups, because in many cases it makes a little sense. Probably because of in-built functionality that is attached to SharePoint groups or that when using SharePoint groups, you are able to move your site more easily to different domain (for example from development to cloud service, BPOS anyone?). Our advice is that go with SharePoint groups or grant directly, but try not to overuse SharePoint Groups as it only causes confusion in the end.

Here is a screenshot of SharePoint site level permission granting screen (this exact same functionality is also used in other levels described below):

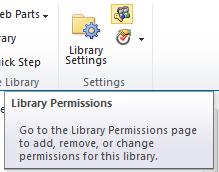
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/site-perms.png)

Each sub site can break the permissions inheritance chain and specify their own permissions, just like you specify them in a root site.

Additional Resources:

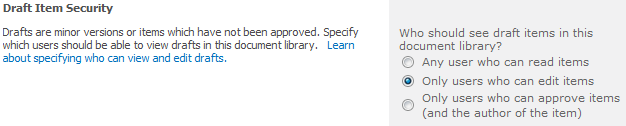
* [Plan site permissions (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc262778.aspx)
* [Roadmap: Grant permissions for a site](http://office.microsoft.com/en-us/sharepoint-server-help/roadmap-grant-permissions-for-a-site-HA101794118.aspx)
* [About permissions inheritance](http://office.microsoft.com/en-us/sharepoint-foundation-help/about-permissions-inheritance-HA101805371.aspx?CTT=5&origin=HA101794118)

**Library or List Permissions**

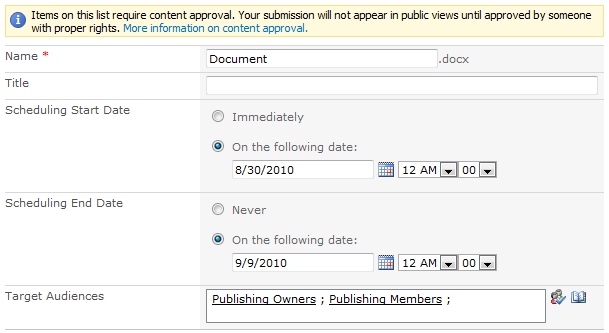
[](http://www.sharepointblues.com/wp-content/uploads/2010/09/list-perms-1.png)Library and List permissions can be managed though list settings. Basically the management works exactly the same as with Site permissions. First you break the inheritance chain and then you start to manage individual list’s or library’s permissions. You can grant rights for AD users, AD groups and SharePoint Groups. By default libraries and lists inherit their permissions from parent site.

With lists and libraries you have also some other security related features.

For example you can control Draft Item Security:

[](http://www.sharepointblues.com/wp-content/uploads/2010/09/lists-draft.png)

You can also control item/document scheduling, enable audience targeting and content approval (with or without workflows):

[](http://www.sharepointblues.com/wp-content/uploads/2010/09/lists-scheduling-audiences1.png)

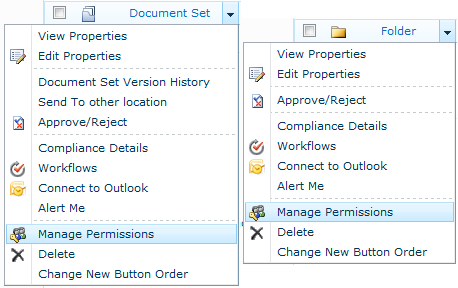
Additional Resources:

* [Control access for a specific piece of content](http://office.microsoft.com/en-us/sharepoint-server-help/control-access-for-a-specific-piece-of-content-HA101805400.aspx)
* [What is uniquely secured content?](http://office.microsoft.com/en-us/sharepoint-server-help/what-is-uniquely-secured-content-HA101808707.aspx)
* [Plan content approval and scheduling](http://technet.microsoft.com/en-us/library/cc263156.aspx)

**Folder or Document Set Permissions**

Like with library and site permissions, folders and document sets can be granted with their own permissions by breaking the permissions inheritance chain.

Document Set and Folder permissions can be accessed from drop-down menu:

[](http://www.sharepointblues.com/wp-content/uploads/2010/09/folderdocset-perms-1.png)

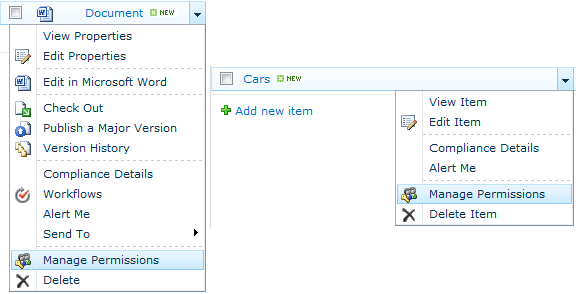
Additinal Resources:

* Consult the links provided in Library or List Permissions

**Document or Item Permissions**

Last level in SharePoint site structure hierarchy is document or item. Document and item permissions can also be granted just like you did with structures above that (folders, libraries, sites…).

You can access document and item level permission settings page directly from the object you are interested in:

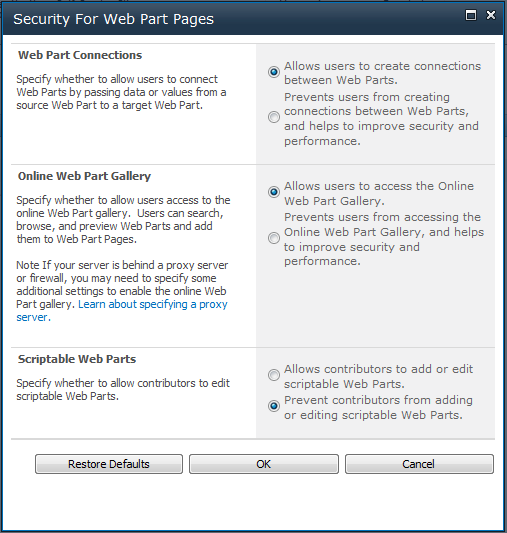
[](http://www.sharepointblues.com/wp-content/uploads/2010/09/docitem-perms-1.png)

Additinal Resources:

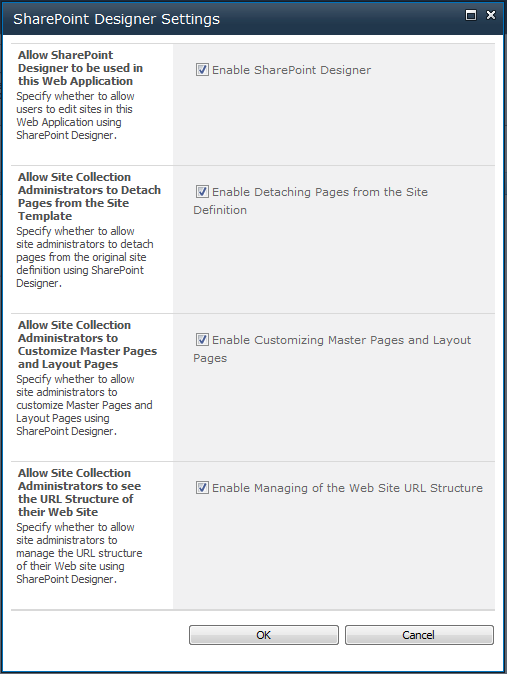
* Consult the links provided in Library or List Permissions

**Miscellaneous Security and Permission Features**

*Web Part security settings can be configured at web application level:*

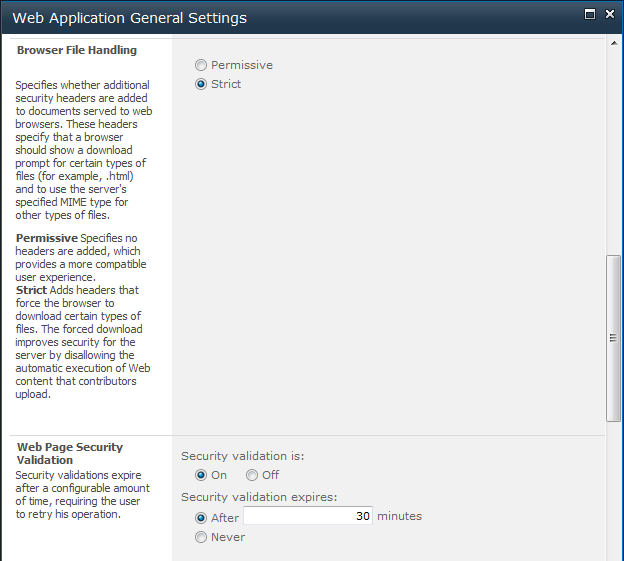
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/misc-webparts.png)

*SharePoint Designer permissions can be controlled with web application level settings:*

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/misc-designer.png)

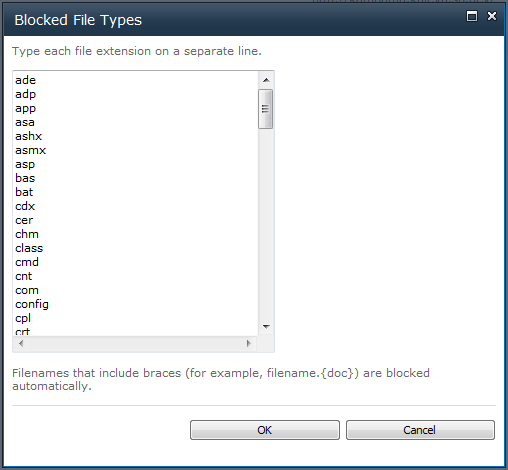
See also: [Managing SharePoint Designer 2010](http://office.microsoft.com/en-us/sharepoint-designer-help/managing-sharepoint-designer-2010-HA101838275.aspx)

*Browser File Handling and Web Page Security validation can be controlled at web application level:*

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/misc-webapp.png)

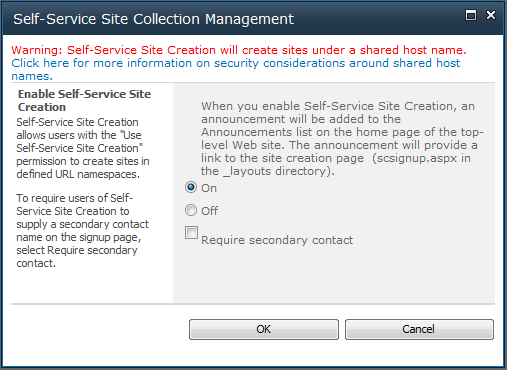
See Also: [Security Validation and Making Posts to Update Data](http://msdn.microsoft.com/en-us/library/ms472879.aspx)

*You can also control blocked file types list (aka restrict of uploading certain file types):*

[](http://www.sharepointblues.com/wp-content/uploads/2010/08/misc-files.png)

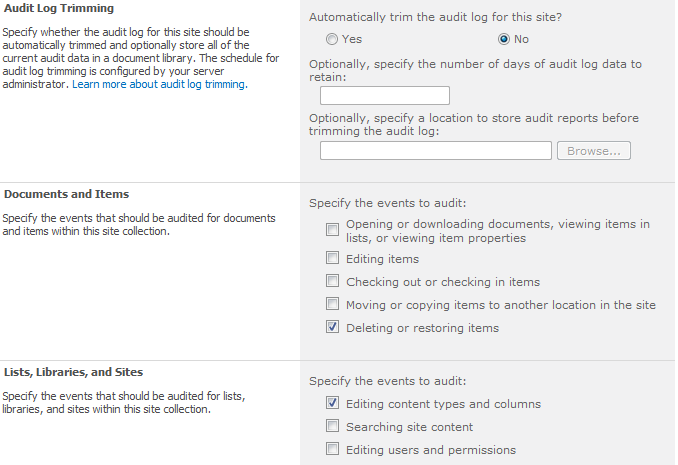
See Also: [Manage blocked file types (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc262496.aspx)

*Self-Service Site Creation that is basically used for my sites is a way to give users a permission to create a new site collections in certain URL namespaces. This can be controlled through Central Administration -web site and the setting is for a web application:*

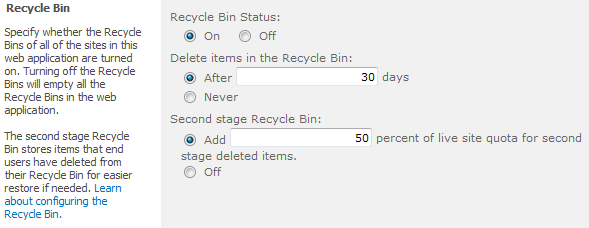
[](http://www.sharepointblues.com/wp-content/uploads/2010/08/misc-self.png)

See Also:[Turn on or turn off self-service site creation (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc261685.aspx)

*With SharePoint auditing features you can gather logs and get reports on what the users have been doing on the site collection:*

*[](http://www.sharepointblues.com/wp-content/uploads/2010/09/auditing.png)*

*This is a little bit unrelated to security, but as a note, SharePoint has also a two level recycle bin:*

*[](http://www.sharepointblues.com/wp-content/uploads/2010/09/recycle.png)*

See also: [Plan to protect content by using recycle bins and versioning (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/cc263011.aspx)

**What Was Not Covered in This Article**

There is also Windows Rights Managements Services integration in SharePoint… let’s discuss about that in a separate article, or give us a link to some article that discusses SharePoint/RMS integration! We could also talk a little bit about SharePoint managed accounts, but those are more of a infrastructure side. And what about security settings that some of SharePoint services contain? As you can see, SharePoint is a very flexible platform in these kind of things, but this flexibility comes with a price. That price is complexity. Hopefully this article clears some of that.

What we also didn’t discuss that are somewhat related to security are for example:

* Quotas and Locks
* Service Application specific security settings
* Code Access Security
* Zones
* Personalized Web Part Zones
* Claim Based Authentication
* SharePoint User Profile Service
* [Microsoft Forefront Thread Management Gateway 2010](http://www.google.fi/url?sa=t&source=web&cd=6&ved=0CEcQFjAF&url=http%3A%2F%2Fwww.microsoft.com%2Fforefront%2Fthreat-management-gateway%2Fen%2Fus%2Fdefault.aspx&ei=EFh-TKOJI9KXOLWrzIIE&usg=AFQjCNEn-j7PSGBDmvhI3-8AitkS4ZLQew&sig2=7CeWsvQDVG-2X3PtkhtLMA)
* [Microsoft Forefront Unified Access Gateway 2010](http://www.google.fi/url?sa=t&source=web&cd=1&ved=0CBoQFjAA&url=http%3A%2F%2Fwww.microsoft.com%2Fforefront%2Funified-access-gateway%2Fen%2Fus%2F&ei=5Fd-TPmnM4SVOKKz3ZoK&usg=AFQjCNFWM3vgm64DrMQ67WT9ajXBPPtLQA&sig2=P_9KbkWlpC1mFsUMx7UjJQ)
* SharePoint Secure Store Service
  + [Plan the Secure Store Service (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ee806889.aspx)
  + [Configure the Secure Store Service (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ee806866.aspx)
* Trust Relationships between farms
  + [Exchange trust certificates between farms (SharePoint Server 2010)](http://technet.microsoft.com/en-us/library/ee704552.aspx)
* Sandboxed Solutions
  + [Developing, Deploying, and Monitoring Sandboxed Solutions in SharePoint 2010](http://msdn.microsoft.com/en-us/magazine/ee335711.aspx)
  + [Sandboxed Solutions](http://msdn.microsoft.com/en-us/library/ee536577.aspx)
* Anything else? Give us feedback?

**Whether to use AD Groups or SharePoint Groups as a Main Mechanism to Grant Rights?**

Well, Everything starts from Active Directory. If Active Directory is a mess, it should be fixed before designing how to manage rights in SharePoint. If Active Directory is well maintained it also benefits the other applications that integrate to AD (for example normal file sharing and NTFS permissions, or systems like Microsoft CRM).

Use SharePoint groups sparingly. Try to utilize the predefined SharePoint groups that are created in SharePoint sites, if possible. Think twice before defining new Web Application policies or Site Collection Permission Levels, and create new ones only if there isn’t better way around it.