How to set up access rights for site collections

[*Click here for an overview of available languages of this document*](http://sp-appl-bbs.bayer-ag.com/sites/010024/Pages/training%20material.aspx?View=%7b50F2E62A-7AB4-4590-9B36-8FD839A2A60C%7d&FilterField1=CatalogID&FilterValue1=223)

Within the Bayer Intranet, you should open your SharePoint Site to the maximum number of users whenever this is possible from a data security point of view and the content is of general interest.

However sites may contain content that should not be available to all users.

Regarding the Bayer Extranet, only grand selected external users access to SharePoint Sites and their content.

With access rights you control the access to sites and site content. This How to describes the management of access rights for sites and site content and provides considerations for implementing your permission structure.

**In this How to:**

[How to control access](#_Toc318448304)

[About permission inheritance](#_Toc318448305)

[Plan site and content access](#_Toc318448306)

[Which permissions are available by default?](#_Toc318448307)

[How can permissions be customized](#_Toc318448308)

[Assigning permissions](#_Toc318448309)

[Assigning permissions to external users](#_Toc318448310)

[Further exceptions regarding external user’s permissions](#_Toc318448311)

1. How to control access

You can control access to sites and site content by assigning permissions to users or groups for a specific site or site content at the following levels within a site collection:

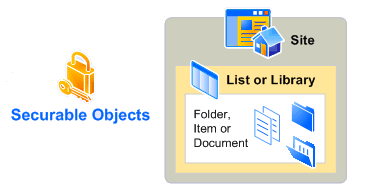
• Site

• List or Library

• Folder

• Document or item

**Note:** It is recommended to limit the depth of your permission assignments to site level or at most to list or library level. This will help to keep your permission management simple and manageable.



A site collection is a group of SharePoint sites that have the same owner and share administration settings, i.e. permissions.

* 1. About permission inheritance

Permissions on securable objects within a site are inherited from the parent site collection by default. You can break inheritance and use unique permissions on the list or library, folder, or item or document level but it is recommended to do this **only as an exception, as it leads to a very complex permission management.**

Stopping inheriting permissions copies the groups, users, and permission levels from the parent object to the child object, and then breaks the inheritance. When permission inheritance is broken, all permissions are explicit and any changes to parent object do not affect the child object. If you restore inherited permissions, the child object will inherit its users, groups, and permission levels from the parent again, and you will lose any users, groups, or permission levels that were unique to the child object.

* 1. Plan site and content access

Before developing your plan for site and content access, you should consider the following question:

To what granularity do you want to control permissions for the site or site content? It is recommended practice to control access at the site level, thus providing for example read or contribute access to the whole site and not to individual objects.

1. Which permissions are available by default?

Permission levels are collections of permissions that allow users to perform a set of related actions. Permissions can be included in multiple permission levels. Unless you have very specific permission configuration requirements, avoid assigning individual permissions and use the available default levels.

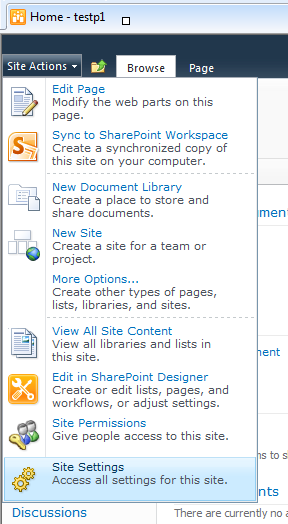
The following table displays the default permission levels and the SharePoint groups (roles) that are assigned with these levels by default.

|  |  |  |  |
| --- | --- | --- | --- |
| Permission Level | Description | Default Group |  |
| Full Control | Has full control | Owners | **Do not assign to external users!** |
| Contribute | Can view, add, update, and delete list items and documents | Members |  |
| Read | Can view pages and list items and download documents | Visitors |  |

1. How can permissions be customized

In case that there is a need for a specific permission configuration that isn’t available by default, you can create your own customized permission level.

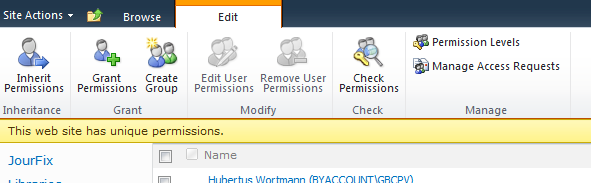
1. While on your site or site collection, click on “Site Actions” followed by “Site Permissions”:



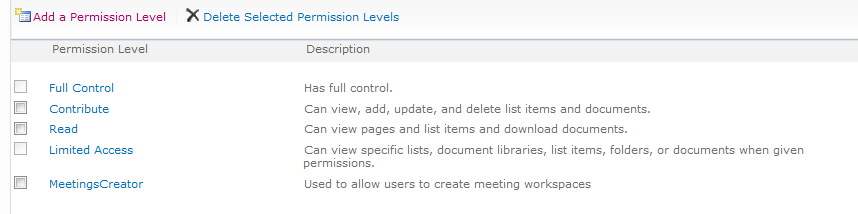
**1**

**2**

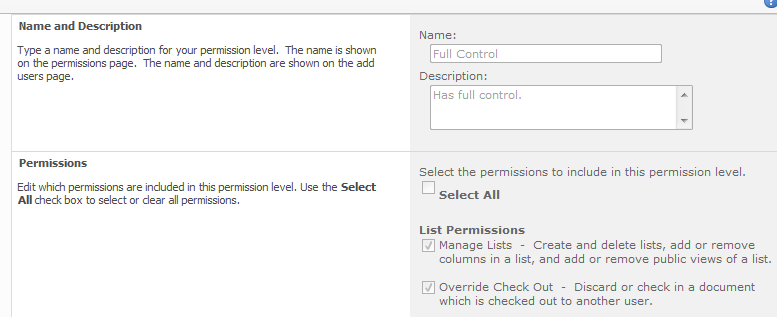
1. Click on “Permission Levels”:



1. You now see an overview of the already existing permission levels.  
   By clicking on “Add a Permission Level” you can create a new one.



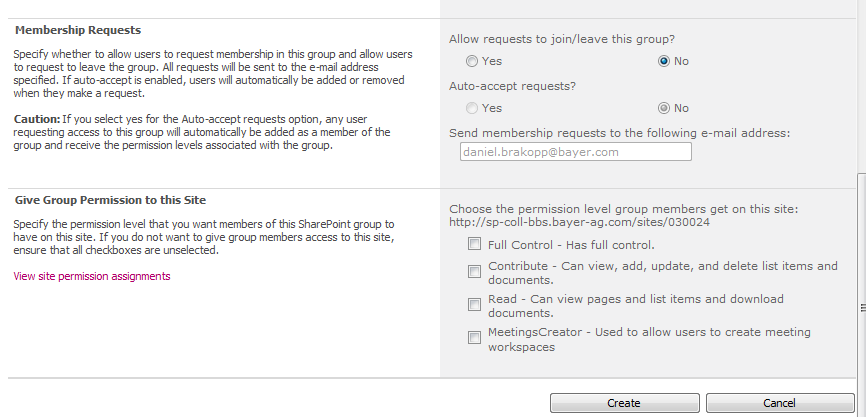
1. Assign an appropriate name, fill in a description and check the permissions that you want to assign to the new permission level.



**+**

**+**

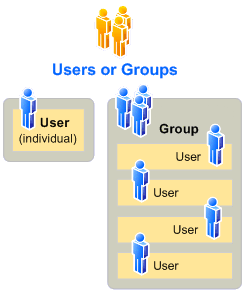
1. After clicking “Create”, the new permission level is ready to be used.



**Important!:** Please Keep in mind that the maximum permission level for external user is Contribute!

1. Assigning permissions

You can assign permission levels either to a group or a single user.



It is highly recommended to use Active Directory (AD) groups to assign permissions to users instead of providing them directly to individual users in order to keep your permission management as simple as possible and therefore manageable.

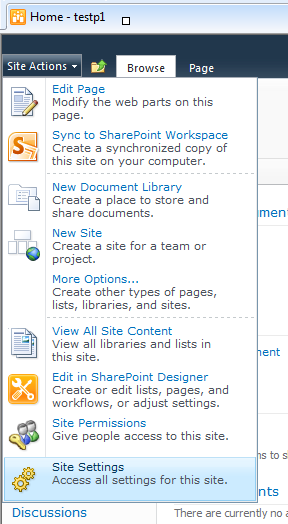
Active Directory groups have the advantage to be available within the whole Bayer structure and are updated when for example a user changes the business unit and should no longer have access to the respective site. SharePoint groups with individual users will be only available within the site collection they are created in and will always require manual maintenance in case of changes.

It is recommended to use the SharePoint groups (roles) that are assigned to the default permission levels as a root group and add Active Directory groups to them as required.

Please consult your local O&I in order to find out what is the preferred structure of AD groups in your organization.

Follow the next steps to assign the required permission level to your groups:

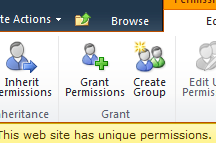
1. You can assign permissions to AD groups or users by clicking on “Site Actions” followed by “Site Permissions”, while on your site or site collection.



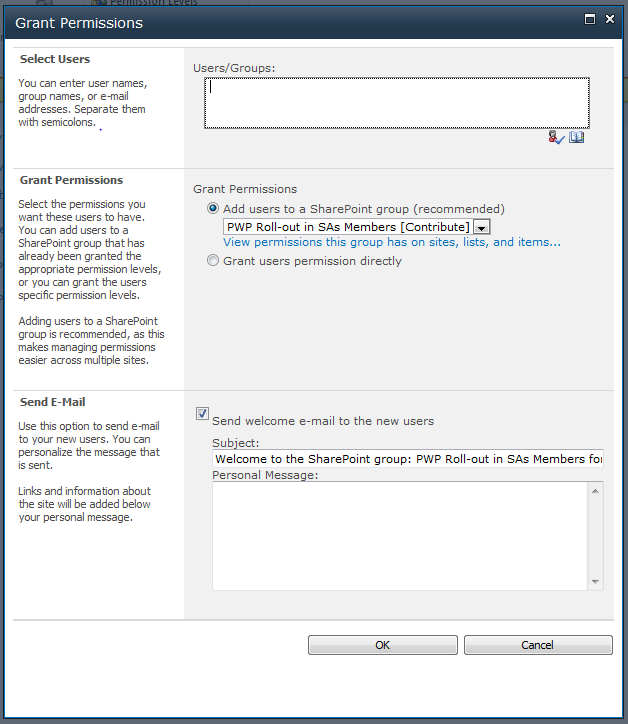
**1**

**2**

Click on “Grant Permissions”:



1. Add users or AD groups (in order to grant access to external users, you need to fill in the full email address) and select the SharePoint group with the permission you want to assign. It is recommended not to assign the Group “All Authenticated User” on a SharePoint that is accessible to external users.



**1**

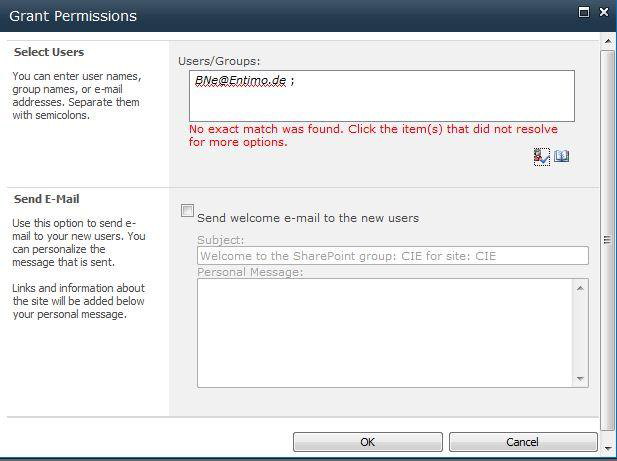
**2**

**3**

1. Assigning permissions to external users

The procedure of assigning permission to external users is in general similar to that of internal users as described in section 3, with one exception:  
To add an external user as described in point 2., you will have to enter the full email address. Using the CWID or ‘People Picker’ isn’t possible in this situation.

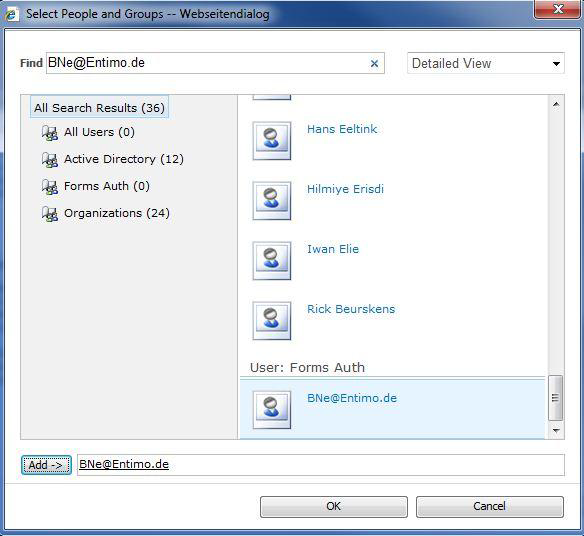
It is possible that SharePoint does not immediately accept the e-mail address [1].  
In that case, you will need to either click on the underlined e-mail address and then select ‘More Names’ or simply click the little address book icon [2].



**1**

**2**

Search for the e-mail address [1] and you will find the user at the bottom of the list under ‘User: Forms Auth’ [2]. Double click the e-mail address or click ‘Add ->’ and then click ‘OK’.



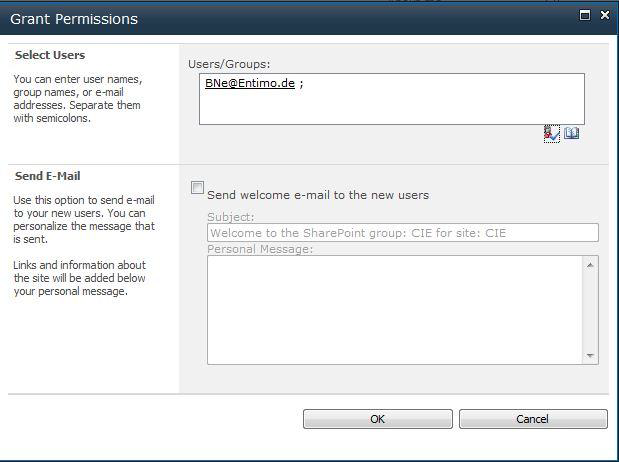
**2**

**1**

**3**

**4**

The ‘Grant Permissions’ dialog now has the Partner ID in the correct format [1] and you can click ‘OK’ [2] to grant the permissions.



**2**

**1**

**Alternatively**, you can also enter the e-mail address directly by prefixing it with ‘ExtranetADUserMembershipProvider:’.

For the example user, you would enter

‚ExtranetADUserMembershipProvider:BNe@Entimo.de‘.

1. Further exceptions regarding external user’s permissions

* Please only assign the absolutely required permission level to external users:
  + If the user only needs to view information: ‘Read’ permission level
  + If the user also needs to change information: ‘Contribute’ permission level
  + Never grand ‘full control’ permission level to external users
* Never assign the Group “All Authenticated User” on a SharePoint that is accessible to external users.