ListPermissionsUP for SharePoint

USER GUIDE

TABLES OF CONTENTS

Introduction....3

Deployment and licensing....4

Required components checking....5

Deployment....6

Deployment steps....6

Updating....7

Updating steps....7

Removal....8

Removal steps....8

Migration....9

Licensing....10

Product usage....11

Introduction....11

Limitations....12

Feature activation....13

Activation with web-inteface....13

Activation with command line....13

Permissions setting....14

Fields / list views permissions setting (SharePoint 2007)....14

Fields / list views permissions setting (SharePoint 2010)....24

The trial: features ans recommendations....34

Troubleshooting....35

INTRODUCTION

This user guide is developed by Speals company and contains important information for successful deployment and usage of ListPermissionsUP for SharePoint solution in your environment. We recommend to review this guide carefully before product deployment and usage. Additional information regarding the solution can be found at the product homepage:

http://www.speals.com/products/listpermissionsup/default.aspx

DEPLOYMENT AND LICENSING

The product distributive is zip-archive, contains the following files:

- **deployment.en.txt** – brief deployment manual.
- **license.en.txt** – EULA (plain-text).
- **SpealsListPermissionsUP.wsp** – solution' file.
- this guide in **PDF** and **MHT**.

The solution from **SpealsListPermissionsUP.wsp** is deployed by standard way.

Administrative utility – **stsadm.exe** - must be used for deployment. This utility can be found in the following folders:

- Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007
  C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\BIN
- SharePoint Foundation 2010 or Microsoft SharePoint Server 2010
  C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN

To process the deployment successfully you need to have administrator' permissions for the whole SharePoint farm and for specified server where the product will be installed.

REQUIRED COMPONENTS CHECKING

The set of installed components is required for the product functioning. Set the components in compliance with the list below.

- Microsoft .NET Framework 3.5 with Server Pack 1.
  Download from Microsoft Download Center
- One of the following SharePoint line products:
  - Windows SharePoint Services 3.0
  - Microsoft Office SharePoint Server 2007
  - SharePoint Foundation 2010
  - Microsoft SharePoint Server 2010

DEPLOYMENT

The solution' deployment procedure is the same for all SharePoint-line products.

To process the deployment successfully you need to have administrator' permissions for the whole SharePoint farm and for specified server where the product will be installed.

DEPLOYMENT STEPS

1. Extract files from **SpealsListPermissionsUP.zip** to any folder on any SharePoint farm server.
2. Add **SpealsListPermissionsUP.wsp** to the solution storage with the following command:
   `> stsadm -o addsolution -filename SpealsListPermissionsUP.wsp`
3. Deploy added solution with the command below:
   `> stsadm -o deploysolution -name SpealsListPermissionsUP.wsp -allowgacdeployment -allcontenturls -immediate`
4. Wait successful finish of deployment. To check the final status of deployment you can use the command:
   `> stsadm -o displaysolution -name SpealsListPermissionsUP.wsp`
   The result should contain **`<Deployed>`** parameter, which value is **TRUE**.

When the deployment has been successful finished, you could start to activate and set up the product as it described in Usage section. If any errors appear, view Troubleshooting section.

UPDATES

The update procedure for the solution is the same as for all SharePoint-line products.

To realize update procedure successfully you need to have administrator' permissions for whole SharePoint farm and for specified server where the product will be deployed.

It is not required any additional actions to update the solution.

UPDATE STEPS

1. Extract files from **SpealsListPermissionsUP.zip** any folder on any SharePoint farm server.
2. Update the solution with the following command:
   `> stsadm.exe -o upgradesolution -name SpealsListPermissionsUP.wsp -filename SpealsListPermissionsUP.wsp -allowgacdeployment -immediate`
3. Wait successful finish of updating. To check the final status of update you can use the command:
   `> stsadm -o displaysolution -name SpealsListPermissionsUP.wsp`
   The result should contain **`<Deployed>`**, parameter, which value is **TRUE** and **`<LastOperationResult>`** parameter with **`DeploymentSucceeded`** value.
4. We recommend to restart **Windows SharePoint Services Timer** (**SharePoint 2010 Timer**)) service on each server in the farm when the updating procedure is completed.

REMOVAL

The removal procedure for the solution is the same as for all SharePoint-line products.

To realize update procedure successfully you need to have administrator' permissions for whole SharePoint farm and for specified server where the product will be deployed.

Product settings are saved in additional SharePoint databases after removal, so removal and further re-deployment procedures for the solution can be processed without any additional background.

REMOVAL STEPS

1. Removal is initiated with the following command:
   `> stsadm -o retractsolution -name SpealsListPermissionsUP.wsp -allcontenturls -immediate`
2. Wait successful finish of removal. To check the final status of removal you can use the command:
   `> stsadm -o displaysolution -name SpealsListPermissionsUP.wsp`
   The result should contain **`<Deployed>`**, parameter, which value is **FALSE** and **`<LastOperationResult>`** parameter with **`DeploymentSucceeded`** value.
3. Remove the solution from SharePoint solutions storage:
   `> stsadm -o deletesolution -name SpealsListPermissionsUP.wsp`
4. We recommend to restart **Windows SharePoint Services Timer** (**SharePoint 2010 Timer**) service on each server in the farm, when the removal procedure is completed.

MIGRATION

In a case of SharePoint web-sites content transfer between different farms, the product' settings will be transferred automatically, with all other content. So, to continue using the product after web-site content' transferring or restoring, it is enough just deploy it on a new SharePoint farm as it is described in Deployment section. The priority of web-sites data collections transferring and SpealsListPermissionsUP.wsp deployment is not important.

LICENSING

ListPermissionsUP for SharePoint has 30-day trial for testing and evaluation of the solution in your environment. There are not any functional limitations in the trial.

You need to register the product and purchase the additional numbers of licensing keys when trial is expired. Otherwise, you need to stop using the product and remove it from SharePoint farm as it is described in Removal section.

To purchase the licensing key(s) (license the product) you need to visit Speals web-site:

http://www.speals.com/purchase/default.aspx

When you have got the licensing key(s), it is required to enter it to SharePoint farm. It can be done with the following command:

```
> stsadm -o slprmsregister -key XXXXXXXXXXXXXXXXXXXX
```

Insert received licensing key instead XXXXXXXXXXXXXXXXXXXX. If you need to enter several licensing keys, so repeat this command several times with a new key for each time.

When licensing key(s) is entered, all trial limitations will be removed.

If the trial is expired, the product will be functioned in normal mode. It guarantees that hidden columns and fields cannot be viewed by users without appropriate permissions. However the possibility to change permission settings in the product will be blocked in this case. The usage of the product in 'expired trial' mode is illegal. Active columns and fields protection in 'expired trial' mode just provides the informational security in your environment.

PRODUCT USAGE

INTRODUCTION

ListPermissionsUP for SharePoint provides extended possibilities for SharePoint lists protection.

The product allows to set up the following permissions:

- Permission/prohibition to view list item field.
- Permission/prohibition to edit list item field.
- Permission/prohibition to display List View.

Previously mentioned permissions/prohibitions can be set up for both separate users and user groups.

The permissions are formed at SharePoint web-sites level.

The user-interface is organically integrated in existed SharePoint web-sites interface. You need a minimum time to understand the product and start work with it.

LIMITATIONS

The permissions are operated by ListPermissionsUP can be divided into two groups: view permissions and edit permissions.

Edit permissions for list content is realized in full size. It means if the administrator prohibits to edit any list item field, so the product guarantees that nobody from target user group can perform this operation.

Unfortunately, view permissions for list item fields and list views cannot be realized in full size by the by objective reasons.

The list of cases in which protected content cannot be hidden:

1. Data View Web Part content.
2. Document' metadata in a case when the document is viewed through additional applications such as Microsoft Word, Microsoft Excel, etc.
3. View form of Wiki library pages.
4. RSS content.
5. Search results content. The standard protection is used during searching. ListPermissionsUP for SharePoint does not impact to the content of search results.
6. ListPermissionsUP for SharePoint hides fields content for standard items only. Original forms, web-parts, controls content cannot be modified (forms created with InfoPath, items modificated with SharePoint Designer, etc.).
7. Any permissions created with the product cannot be applied to users who have Site collection administrator rights. This limitation can be turned off for more convenient testing (see Trial: features and recommendation section).
8. Calendar and Gant list views. If some user does not have view permission for any list' field, so all view will be hidden from this user. The page with notification regarding access limitation will be shown to user in this case.
9. 'Title', 'Last Modified', 'Modified by' fields content. These fields cannot be hidden in the following cases:
    a. these fields content in SharePoint notifications, distributed by e-mail or SMS.
10. Permissions list created with ListPermissionsUP for SharePoint cannot be saved when list template is created. A new list, created with such template, will have default permission settings.
11. SharePoint notifications content when additional templates have been changed.

FEATURE ACTIVATION

To start working with the product you need to activate **ListPermissionsUP for SharePoint** feature.

The mentioned feature can be activated by two ways: with SharePoint web-site interface or with command line through **stsadm.exe** utility.

ACTIVATION WITH WEB INTERFACE

1. Open SharePoint web-site using **site-collection administrator account**.
2. Choose **Site Settings** option in **Site Action** menu.
3. Choose **Manage site features** in **Site Actions**.
4. Activate **ListPermissionsUP for SharePoint** feature.

ACTIVATION WITH COMMAND LINE

To activate the feature, run the command below:

```
> stsadm -o activatefeature -name SpealsColumnPermissionsFeature -url <url>
```

To deactivate:

```
> stsadm -o deactivatefeature -name SpealsColumnPermissionsFeature -url <url>
```

Indicate web-site address instead **<url>**. For example: http://speals.com/catalog.

PERMISSIONS SETTINGS

The permissions system in ListPermissionsUP for SharePoint is created similarly native permissions system in SharePoint.

The permissions are set separately for each specified field or list view.

User must have the following access rights to operate with ListPermissionsUP for SharePoint permissions:

1. **Enumerate Permissions - Enumerate permissions on the Web site, list, folder, document, or list item.**
   This permission allows to get information about current status of access rights for field or list view. However, it is not enough to make and changes to the permissions list.

2. **Manage Lists - Create and delete lists, add or remove columns in a list, and add or remove public views of a list.**
   User with this access rights can change permissions.

To change permissions, user must have both access rights at the same time.

Initial status of the fields and list views permissions is based on existing list permissions (i.e. native SharePoint permissions). Till the initial permissions status has not been changed, the permissions are inherited from native SharePoint permissions, so the product does not provide any changes to regular functioning of SharePoint web-site.

To change the fields / list view permissions, the permissions inheritance can be break. In this case the list permissions don't affect on the fields / list views permissions.

It is possible to stop permissions inheritance anytime and restore default permissions.

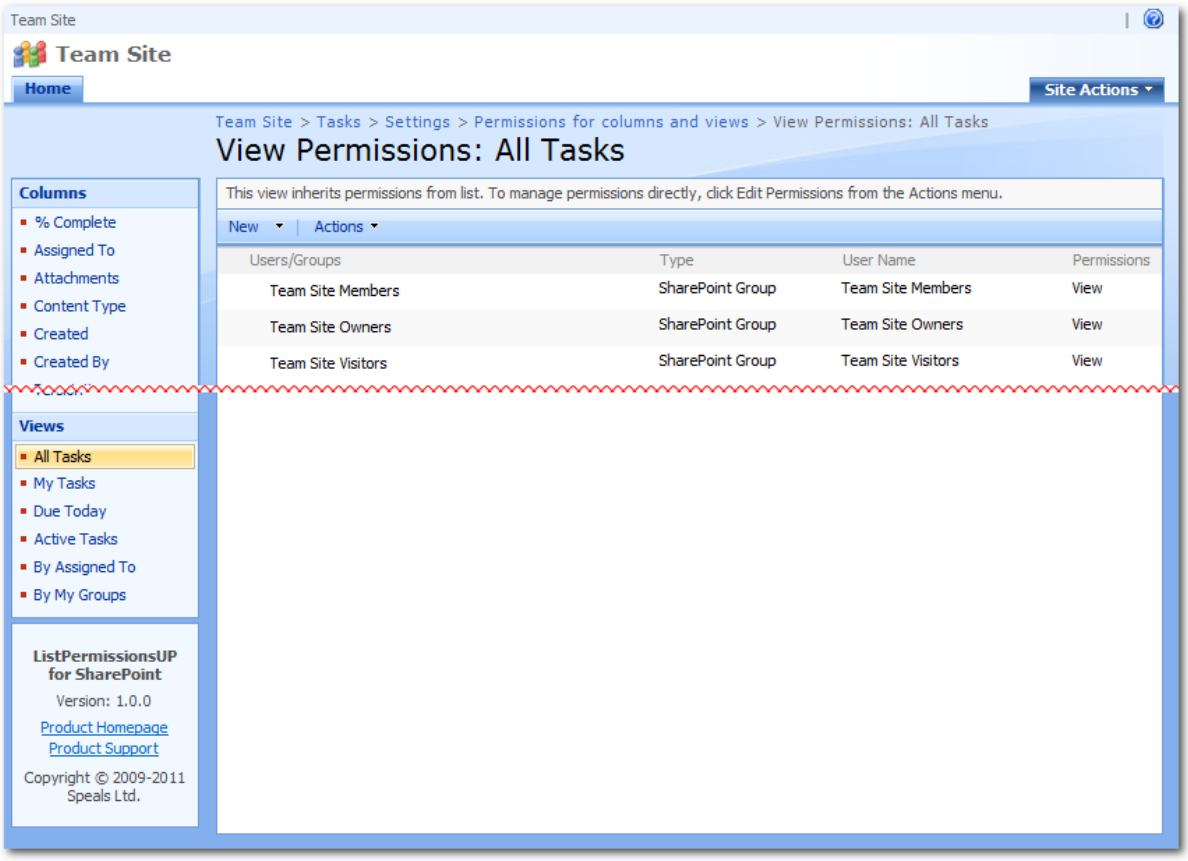
NOTE. The users with web-site collection administrator permissions have special status - there are not any access limitations created by ListPermissionsUP for SharePoint. This model is a standard for all SharePoint-line products. It means these users will see all fields and list views in any case. However, if this fact does not allow you to test the product, it can be changed as described in Trial: features and recommendations section.

Because of SharePoint-line products have different interfaces in different versions, so further description of permissions setting procedure will be separated on 2 sections. The first one will be described setting procedure for SharePoint 2007, the second one – for SharePoint 2010.

FIELDS / LIST VIEWS PERMISSIONS SETTINGS (SHAREPOINT 2007)

PERMISSIONS SETTINGS PAGE

The user interface of fields / list views permissions settings has the following appearance:



The left part of the form contains the list of fields and list views, which permissions can be adjusted.

The right part contains the users / groups list with indication of current permissions for the item from the left listing.

There is a menu with the following options, in the header of users / groups list:

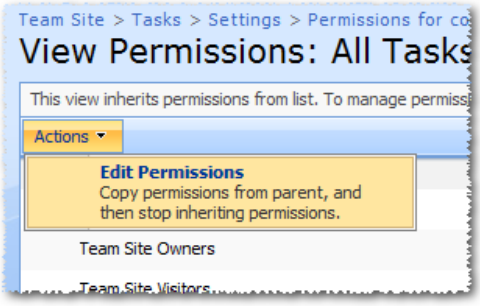
- **New – Add User**
  Add user or group with required permissions to the permissions list.

- **Actions – Remove User Permissions**
  Remove users or groups marked with flags from the permissions list. Removed users will be lost the permissions for editing or viewing field / list view, marked in the left listing.

- **Actions – Edit User Permissions**
  Change the permissions for users / groups marked with the flags in the listing.

- **Actions – Inherit Permissions**
  Restore permissions inheritance. It removes the current permissions list and forms default permissions list on the parent' object basis.

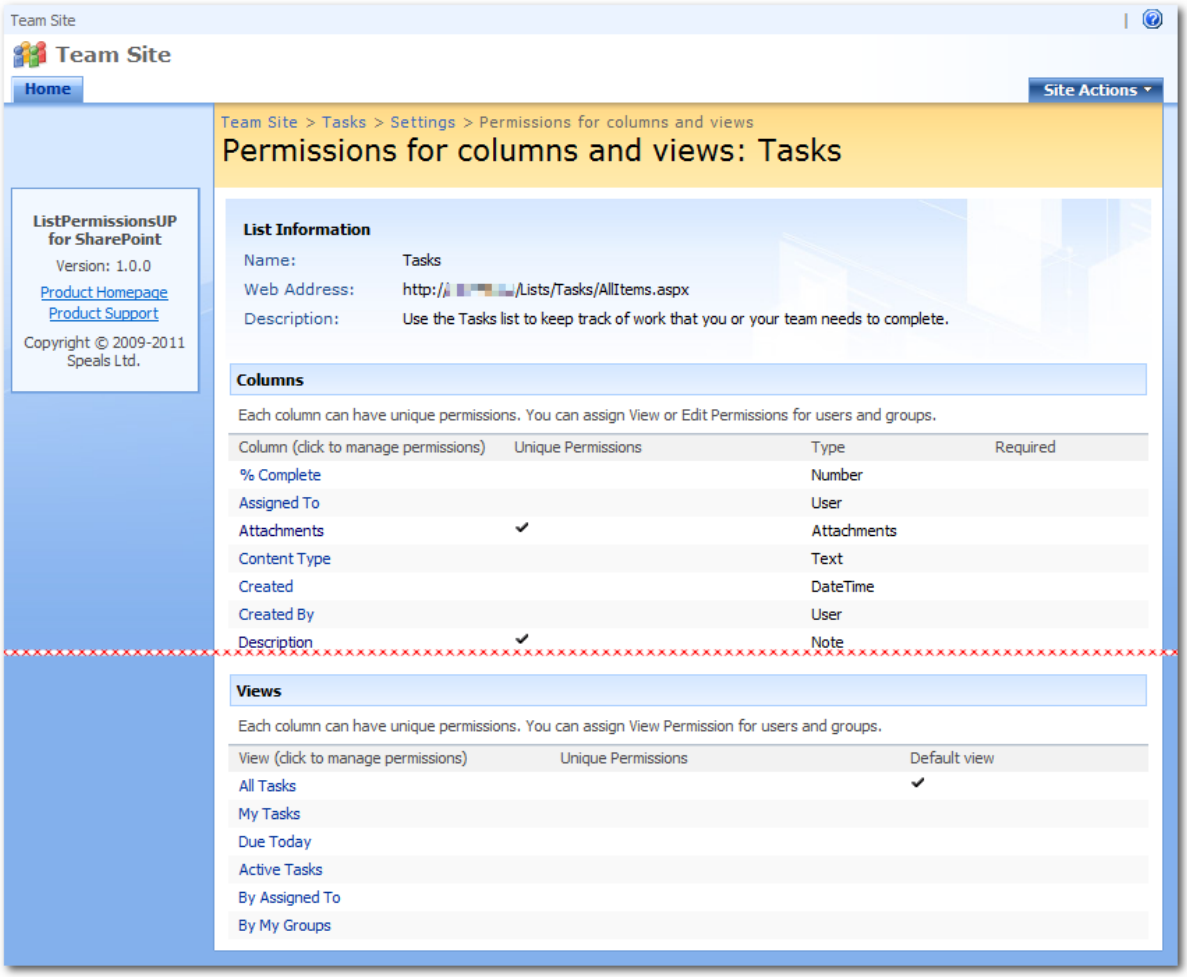
When the permissions inheritance was not break, the menu looks like:



Edit Permissions option allows to break the permissions inheritance and forms required permissions.

CURRENT PERMISSIONS PAGE VIEW

The page has the following appearance:



The page contains tables of the fields (columns) and list views for which the permissions can be configured. There is the following information in the table' columns:

- **Column, View**
  The name of the field (column) or list view. The link allows you to visit the permissions settings page for the chosen field (column) or list view.

- **Unique Permissions**
  The field (column) or list view has the list of changed permissions.

- **Type**
  The data type for the field (column).

- **Required**
  The field (column) must be filled.

- **Default view**
  The list view is used by default.

This page demonstrates the fields and list views which permissions can be changed and processed by ListPermissionsUP for SharePoint.

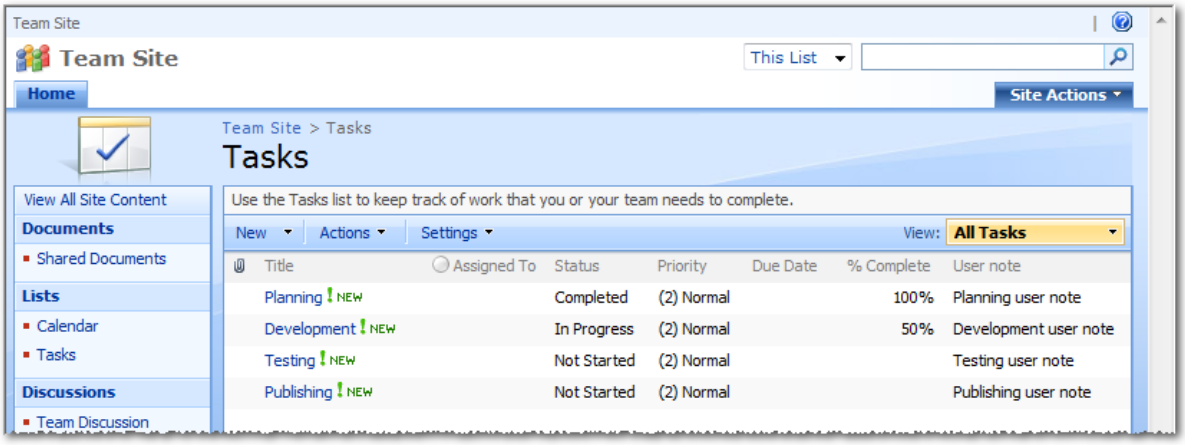
EXAMPLE OF FIELD / LIST VIEW PERMISSIONS SETTING

There is a list of **Tasks**, in which we have **User note** and **Priority** fields. This list has **By Assigned To** List View also.

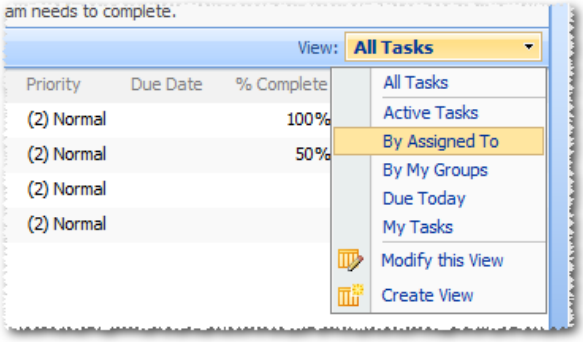
EXAMPLE' TASKS:

1. To hide the **User note** field from all users, excluding users from **Developers** group.
2. To prohibit editing of the **Priority** field for all users, excluding users from **Developers** group.
3. To hide **By Assigned To** List View from all users, excluding users from **Developers** group.

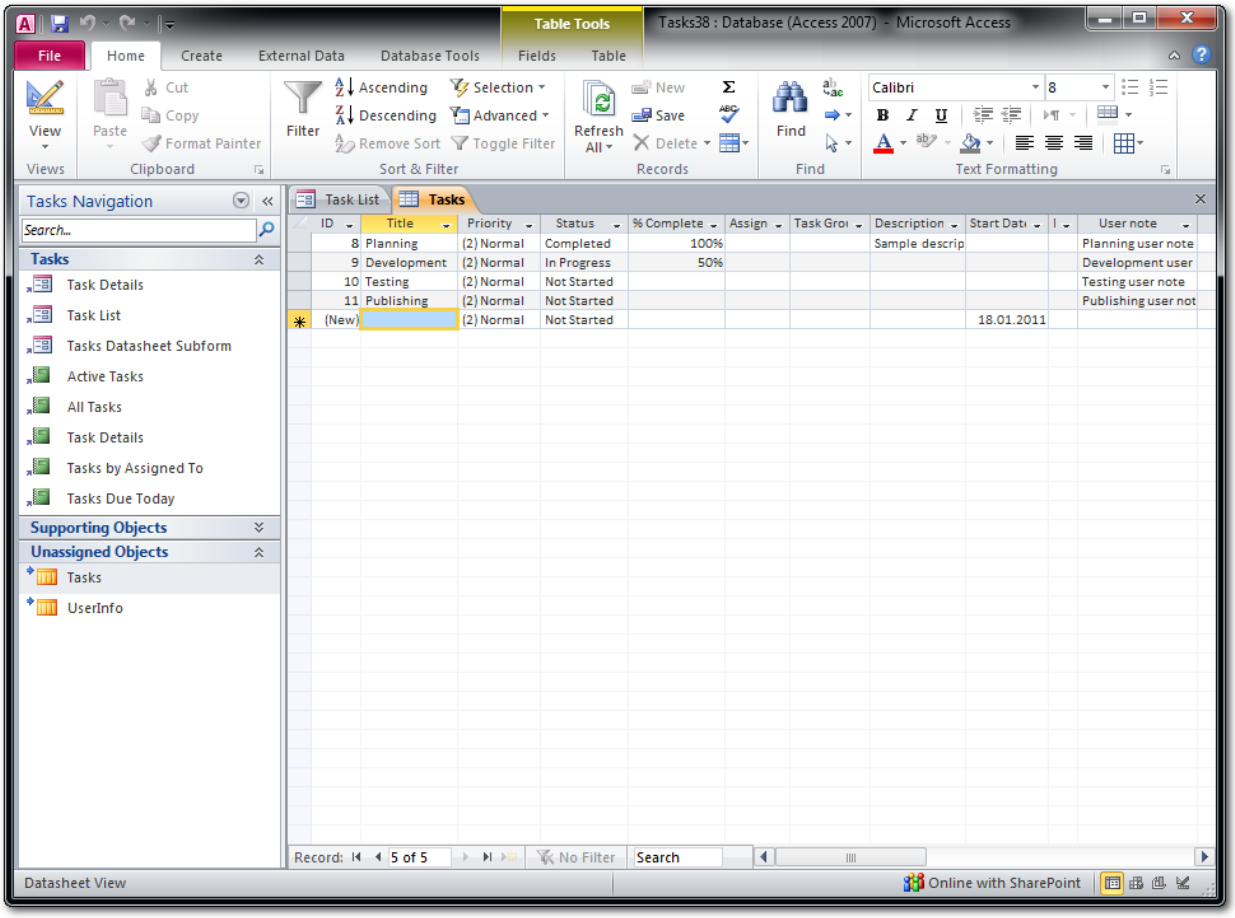
Tasks list has the following appearance in **All Tasks** List View:



It is possible to find all existed List Views list in dropdown menu:

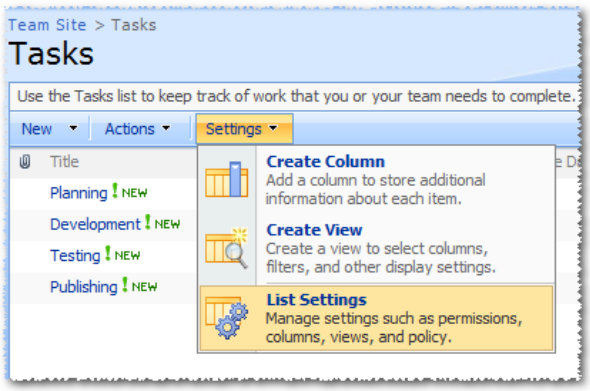


Moreover, it is possible to watch the list content with Microsoft Access:

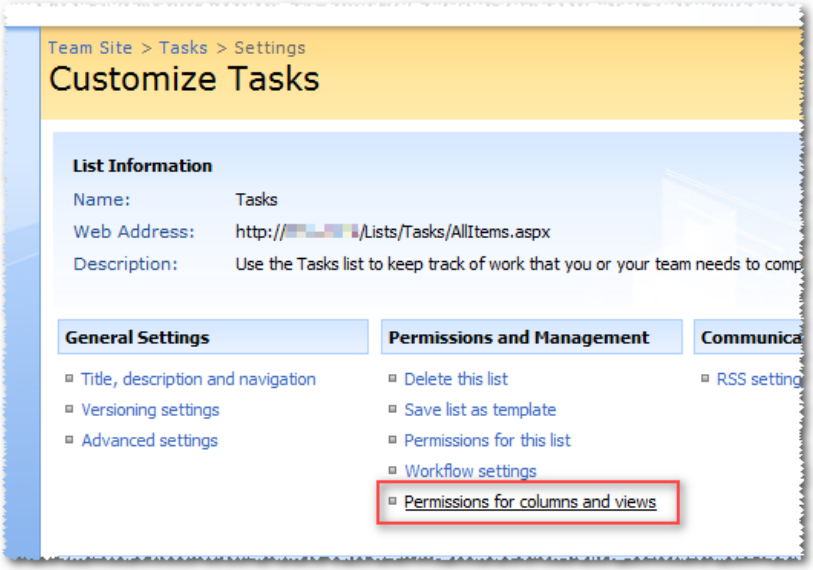


To complete the tasks above, the following actions must be realized:

1. Choose **Settings – List Settings** point in the **Tasks** list header:

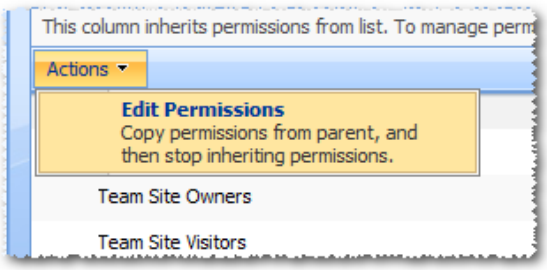


2. Click **Permissions for columns and views** link at the **Customize Tasks** page:

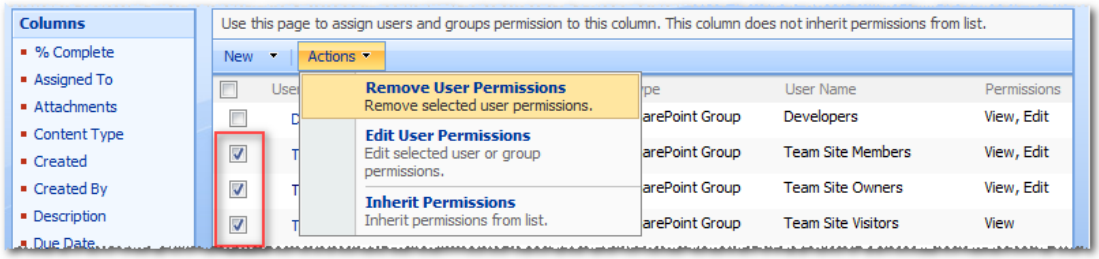


3. Click **User note** link at the **Permissions for columns and views** page.

4. Choose **Actions – Edit Permissions** menu point at the **Column Permissions: User note** page and confirm the creation of customized permissions list:

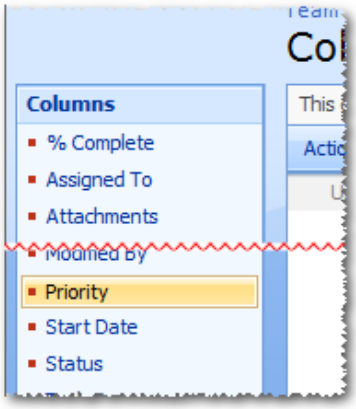


5. Mark with the flags all groups in the list, excluding **Developers** group and click **Remove User Permissions** button[1]:



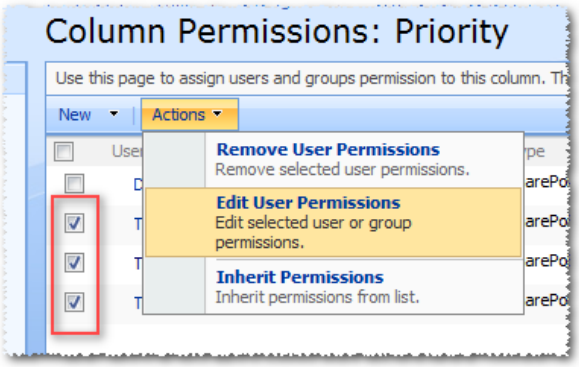
[1] If all groups and users will be removed from permissions list, field or List View will be visible for site-collection administrators only.

6. Choose **Priority** field in the left list:

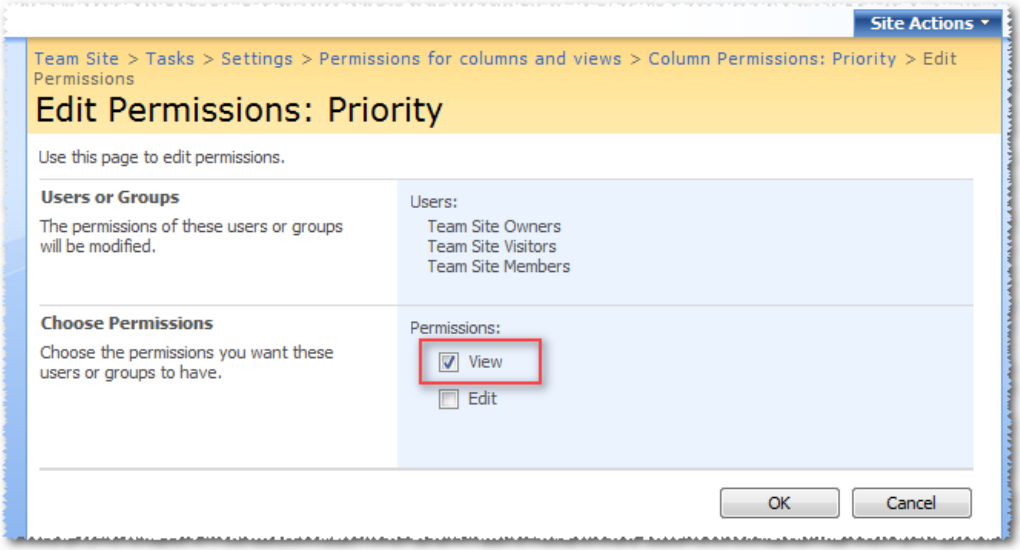


7. Choose **Actions – Edit Permissions** menu point at the **Column Permissions: Priority** page and confirm the creation of customized permissions list.

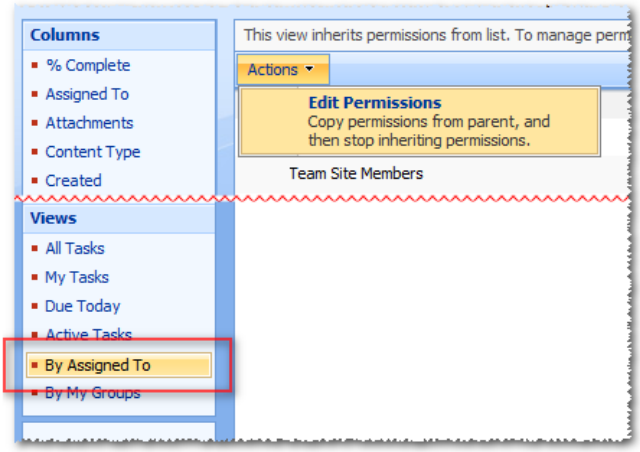
8. Mark with the flags all groups in the list, excluding **Developers** group and choose **Actions – Edit User Permissions** menu point:



9. Set up **View** flag at the **Edit Permissions: Priority** page and click **Ok** button:



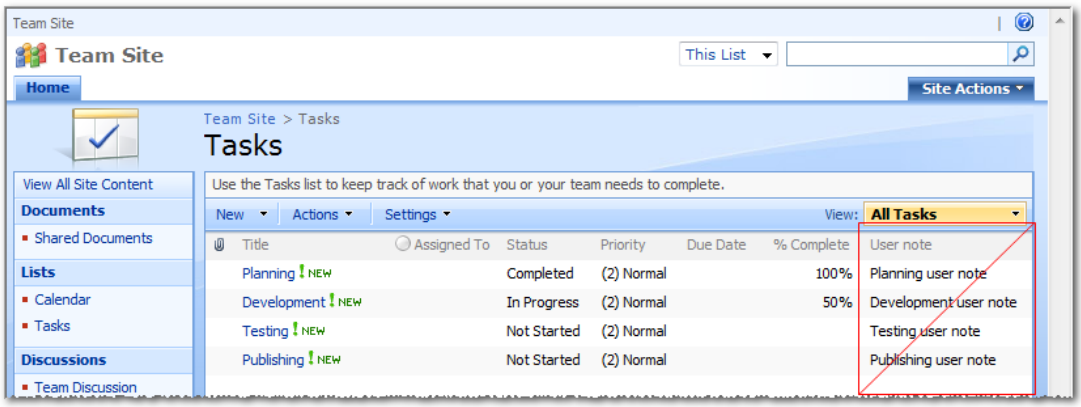
10. Choose **By Assigned To** View in the left part of the list and click **Edit User Permissions** button:



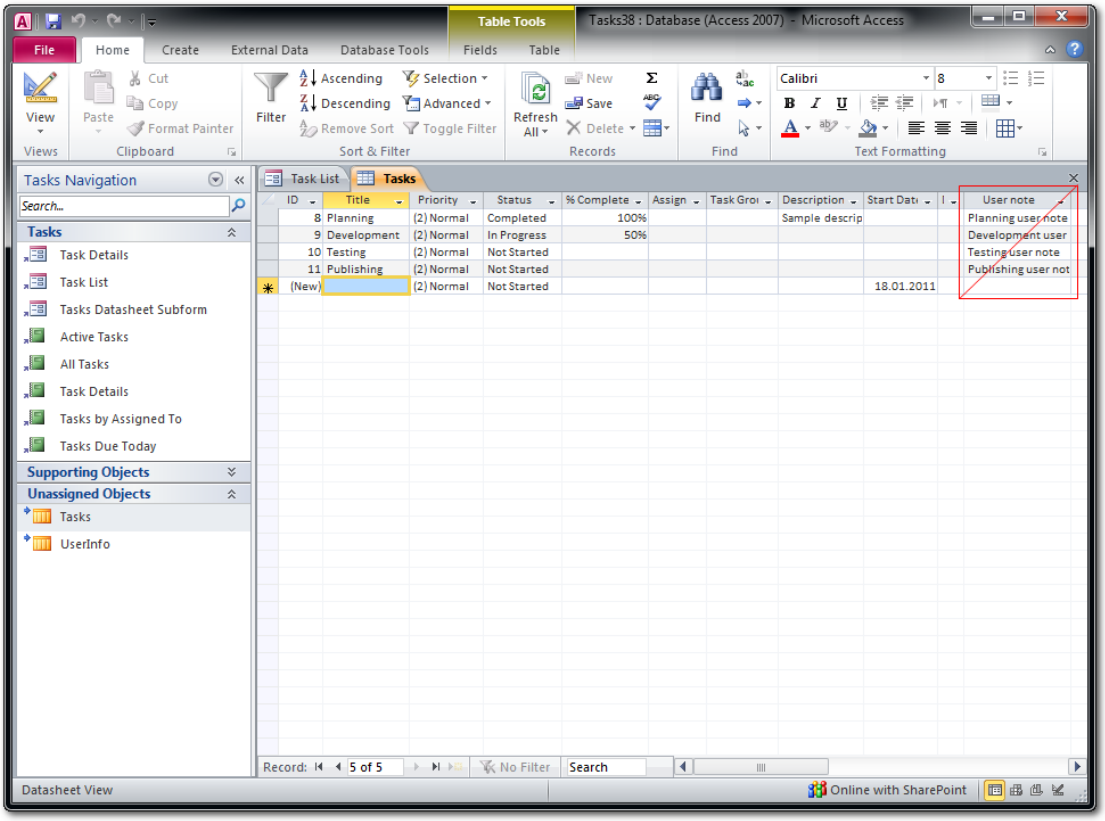
11. Choose **Actions – Edit Permissions** menu point at the **View Permissions: By Assigned** page and confirm the creation of customized permissions list.
12. Mark with the flags all groups in the list, excluding **Developers** group and choose **Actions – Remove User Permissions** menu point.
13. The permissions settings are finished. The changes will be active in 5 minutes after they were completed.

The **Task** list will have the following appearance after the actions above:

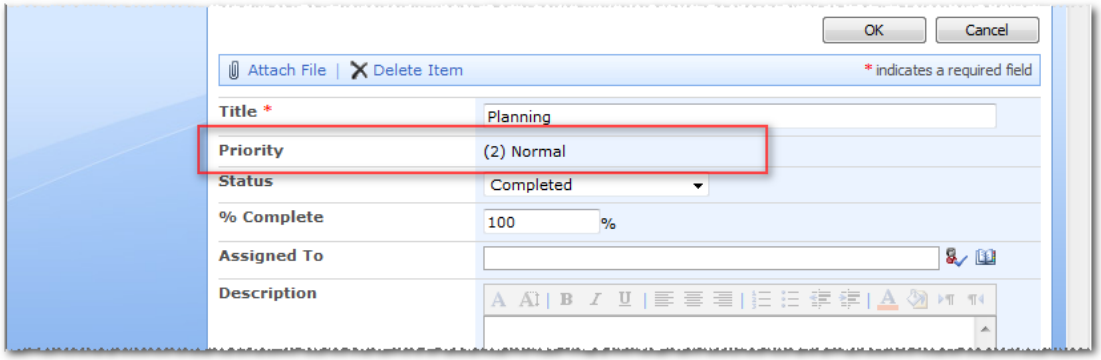
1. B The column **User note** is hidden in **All Tasks** table view. The appropriate field is hidden in the standard forms of this list.



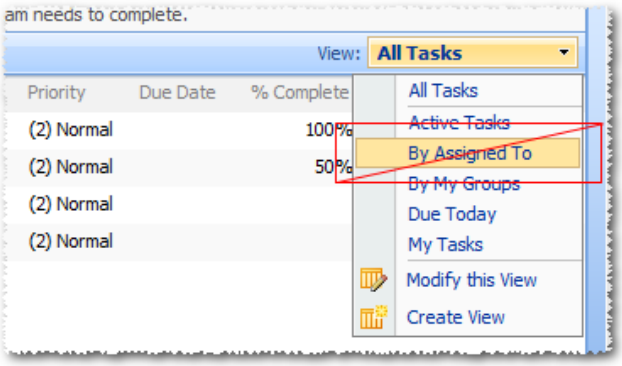
2. **User note** field is hidden in **Microsoft Access**:



3. **Priority** field is inaccessible for editing:



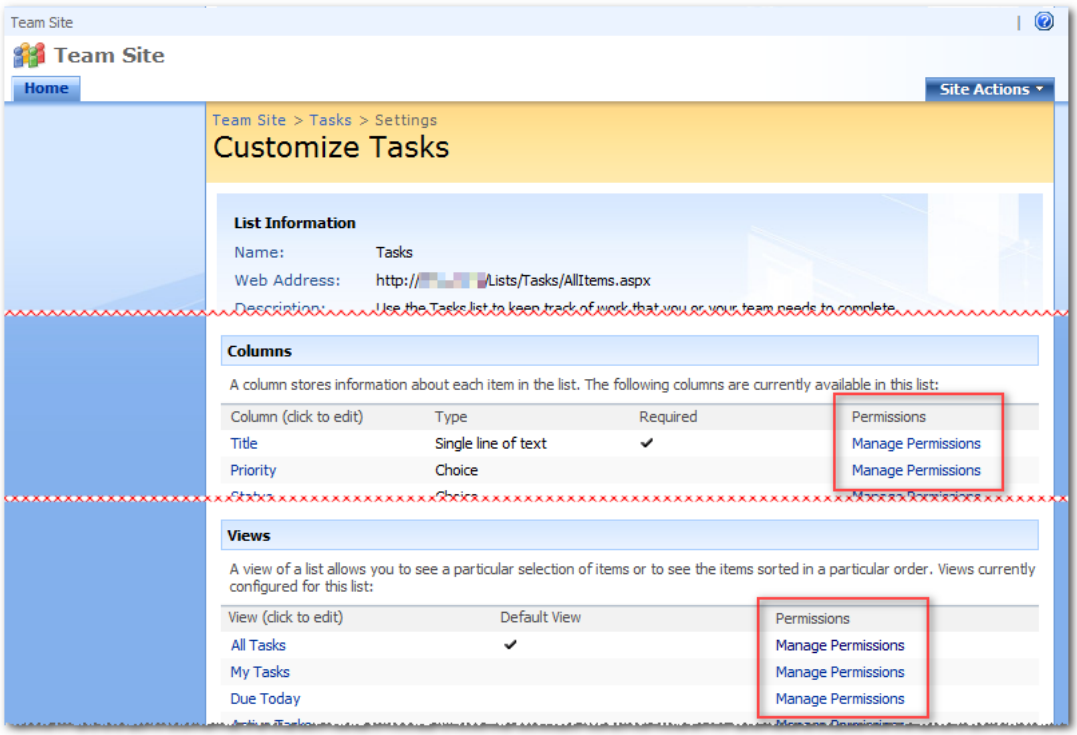
4. **By Assigned To** view disappears from accessible views list. In addition, this view page cannot be opened with a direct link.



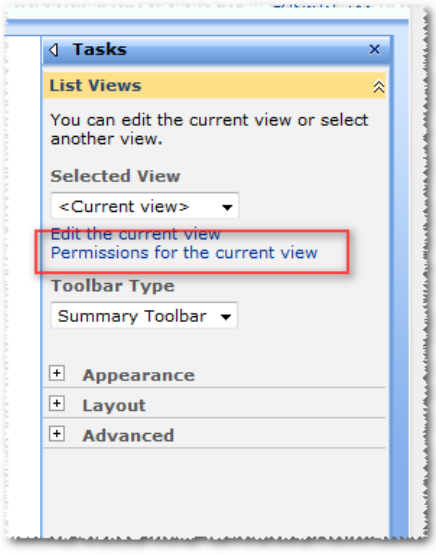
ADDITIONAL FEATURES

For convenient usage, links to permission settings pages are placed in the following SharePoint web-site areas:

- Additional **Manage Permissions** links at **List Settings** page:



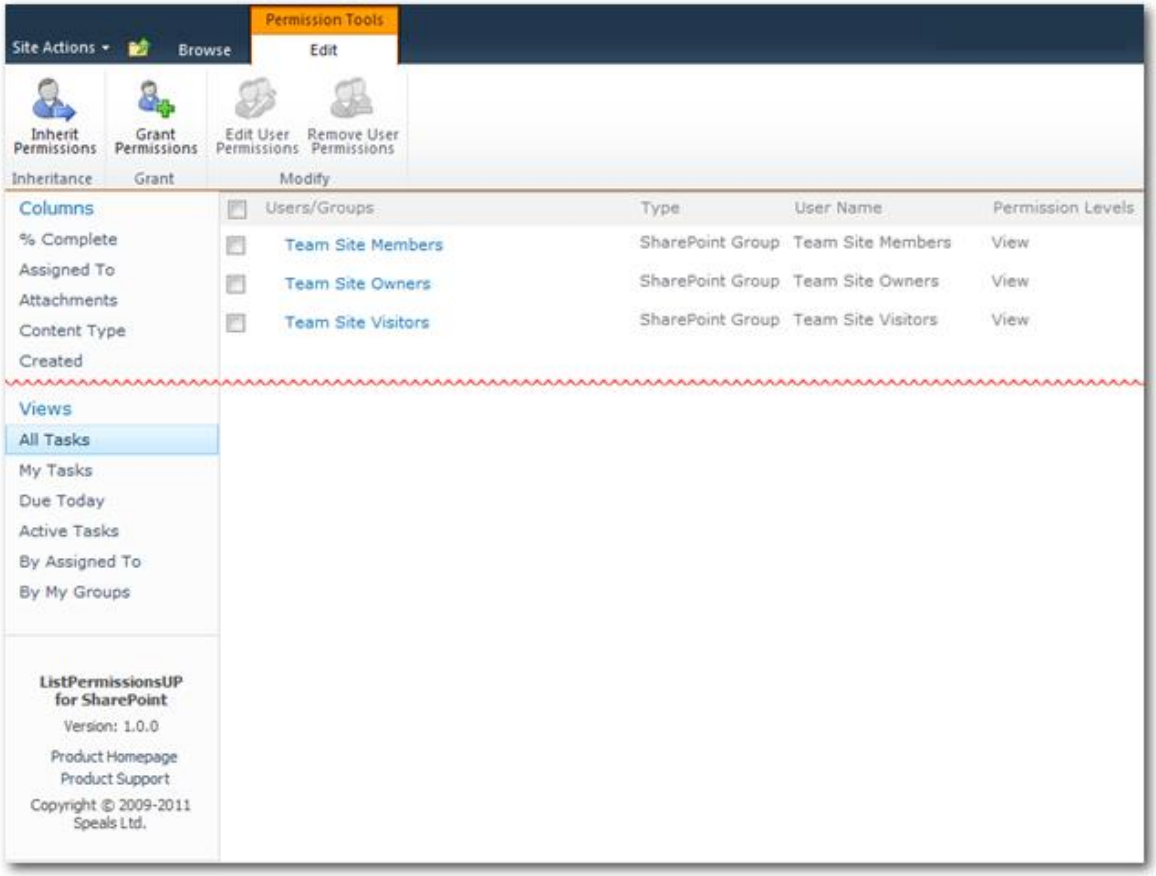
- **Permissions for the current view** link at **List Views** web-part settings:



FIELDS / LIST VIEWS PERMISSION SETTINGS (SHAREPOINT 2010)

PERMISSION SETTINGS PAGE

The user interface for the fields / list views permission settings has the following appearance:



The information 'How to access at the permission settings page' will be available in the The example of field / list view permission settings section.

The left part of the form contains the list of fields and list views for which the permissions can be set up.

In the right part there is the list of users and user groups with indication of current permissions status for the chosen item in the left part.

In the form header, there is the main control element – the ribbon with the following buttons:

- **Inherit Permissions**
  Restore permissions inheritance. It removes the current permissions list and forms default permissions list on the parent' object basis.

- **Grant Permissions**
  Add user or group with required permissions to the permissions list.

- **Edit User Permissions**
  Change the permissions for users / groups marked with the flags in the listing.

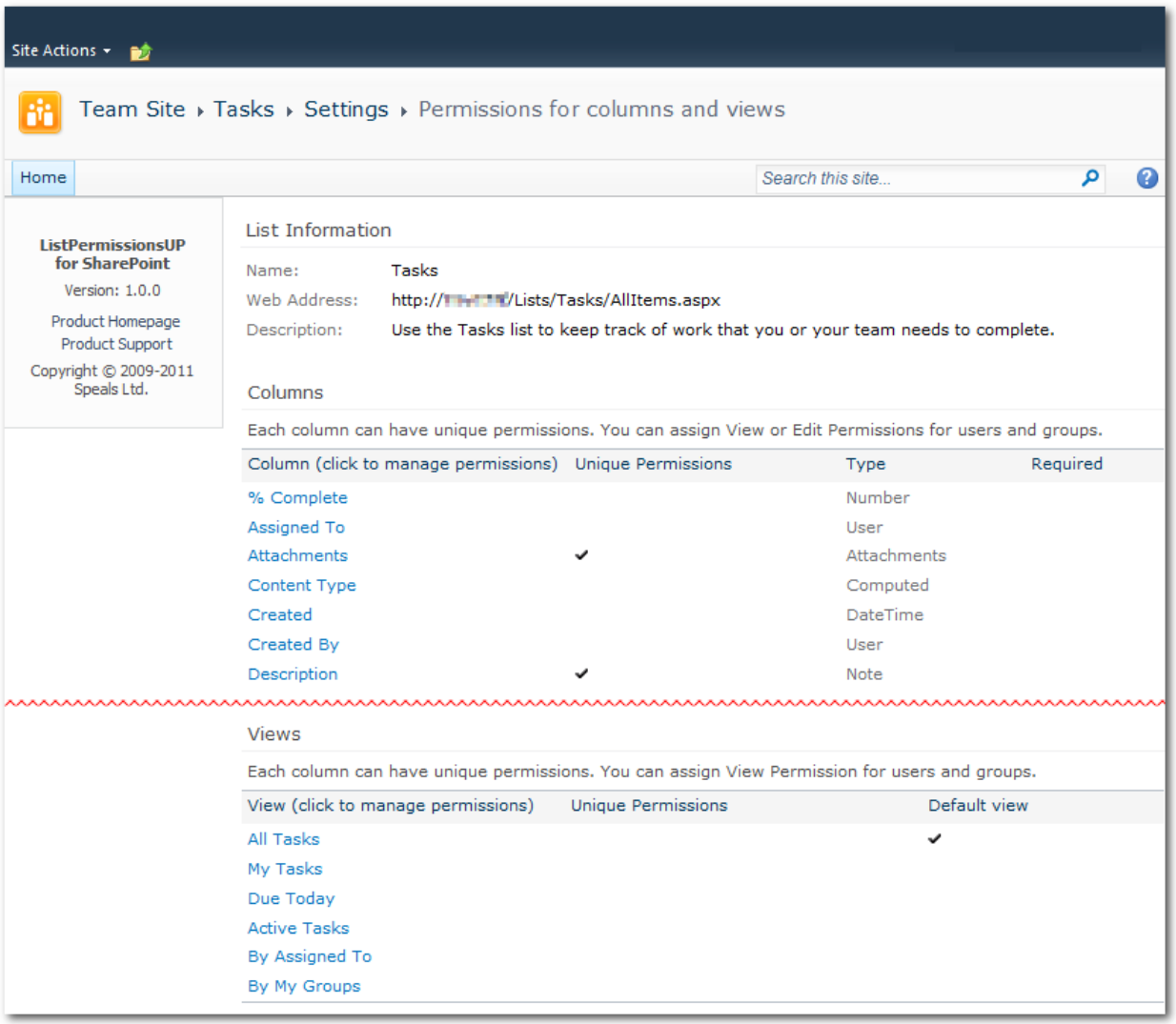
- **Remove User Permissions**
  Remove users or groups marked with flags from the permissions list. Removed users will be lost the permissions for editing or viewing field / list view, marked in the left listing.

When the permissions inheritance was not break, the ribbon has the following appearance:

Just **Edit Permissions** button allows to break the permissions inheritance and creates the required permissions.

CURRENT PERMISSION STATUS VIEW PAGE

The page has the following appearance:



The page contains fields (columns) / view tables, for which the permissions can be set up. There is the following information:

- **Column, View**
  The field (column) or view' name. The link allows to visit permissions editing page for chosen field (column) / view.

- **Unique Permissions**
  The field (column) or list view has the list of changed permissions.

- **Type**
  The data type of the field (column).

- **Required**
  The field (column) must be filled in.

- **Default view**
  The list view is used by default.

This page presents the fields and views with permissions which are changed and processed with ListPermissionsUP for SharePoint.

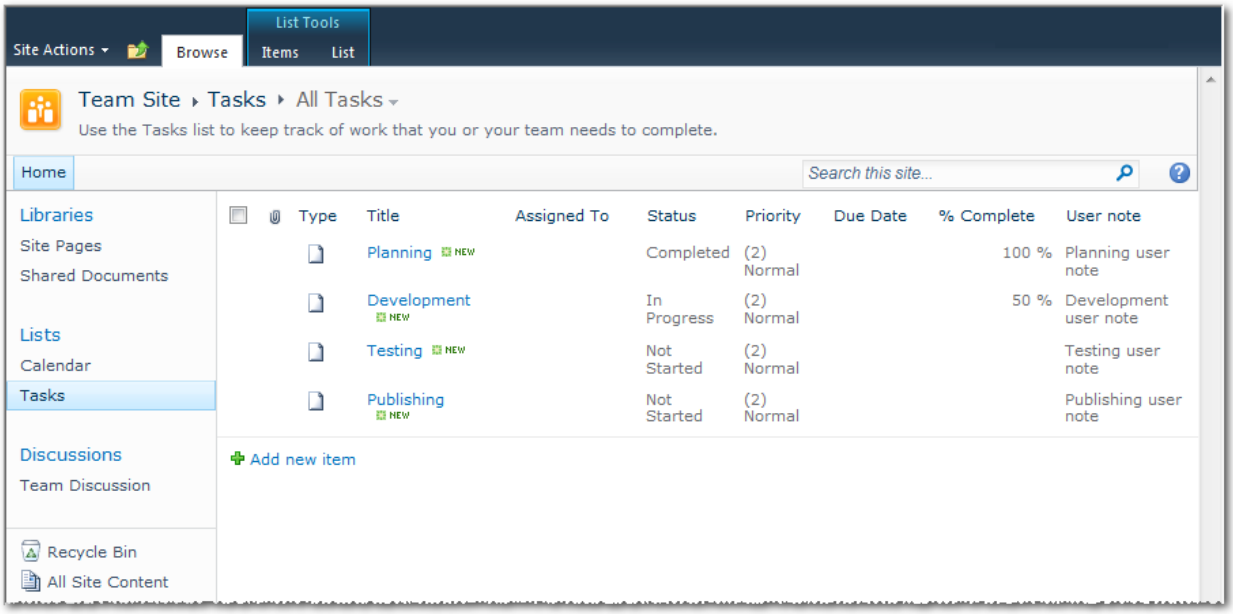
EXAMPLE OF FIELD / LIST VIEW PERMISSIONS SETTING

There is a **Tasks** list, in which we have **User note** and **Priority** fields. This list has **By Assigned To** List View also.

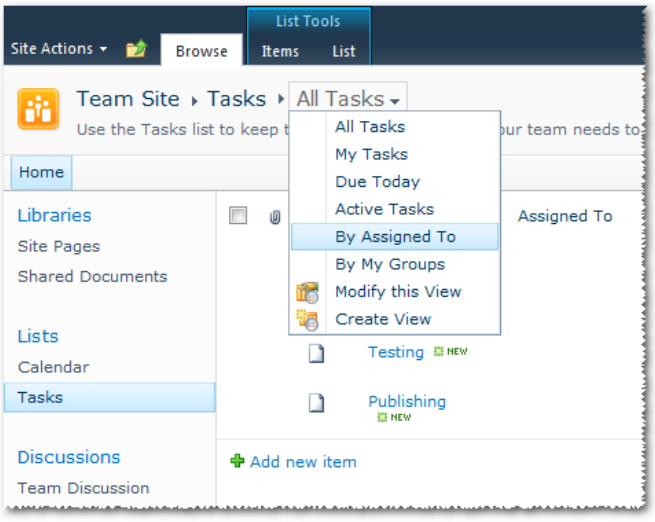
EXAMPLE' TASKS:

1. To hide the **User note** field from all users, excluding users from **Developers** group.
2. To prohibit editing of the **Priority** field for all users, excluding users from **Developers** group.
3. To hide **By Assigned To** List View from all users, excluding users from **Developers** group.

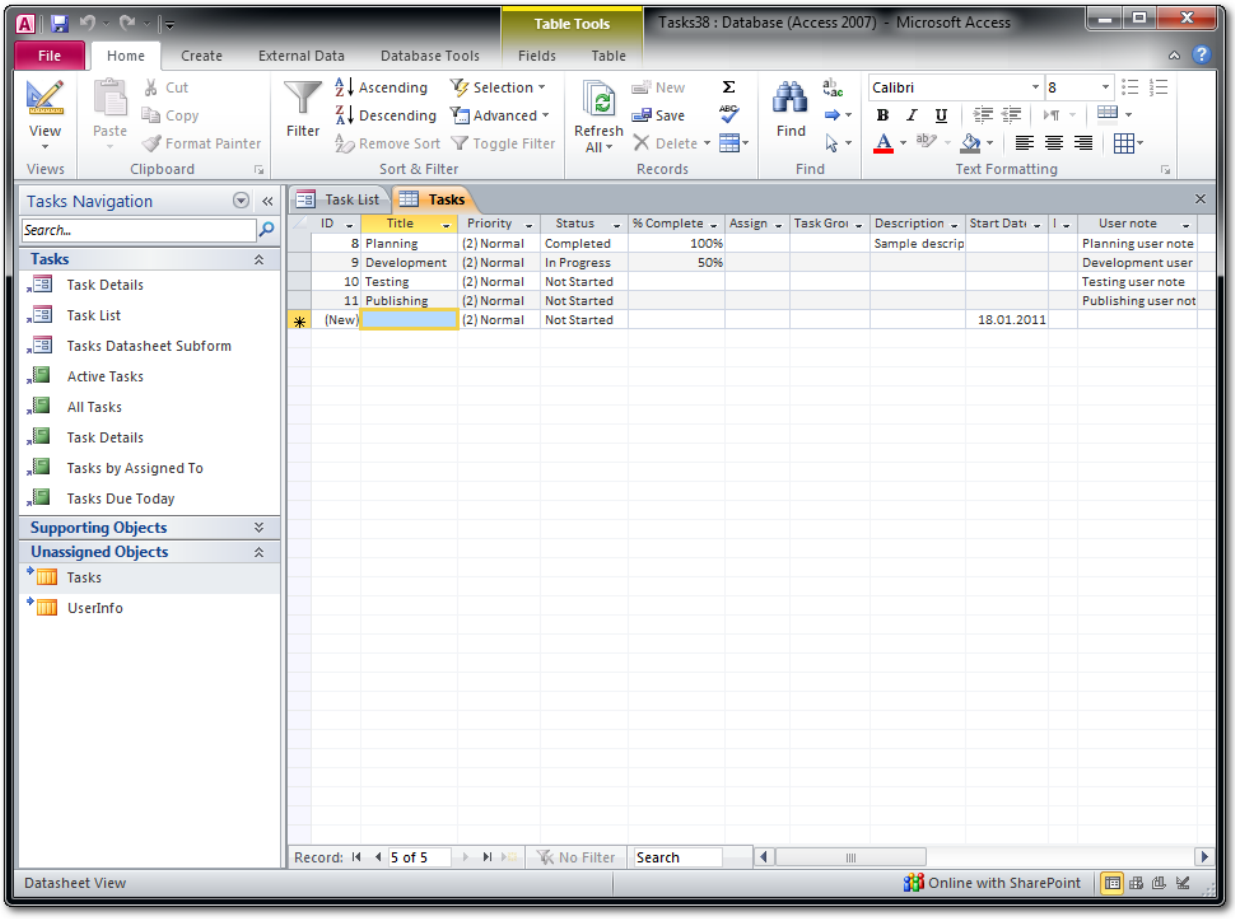
Tasks list has the following appearance in **All Tasks** List View::



It is possible to find all existed List Views list in dropdown menu:

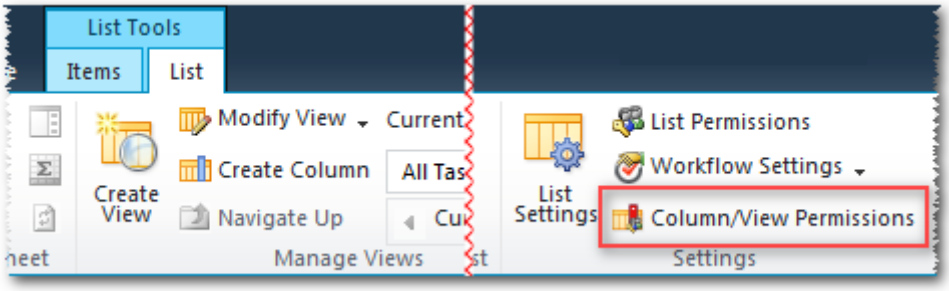


Moreover, it is possible to watch the list content with Microsoft Access:



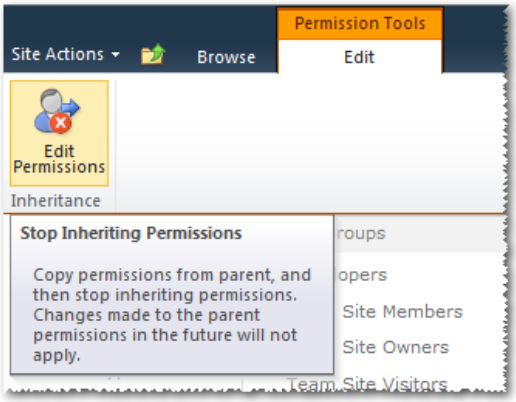
To complete the tasks above, the following actions must be realized:

1. Open **List** bookmark in the ribbon. Click **Column/View Permissions** button:

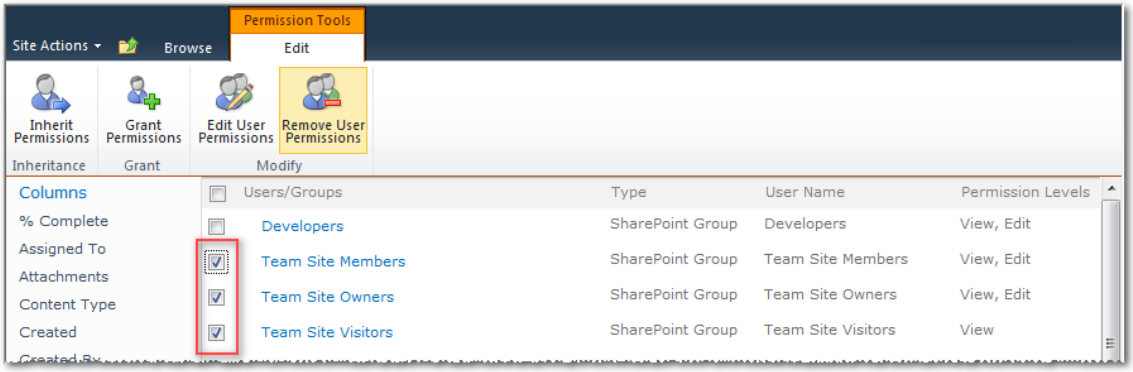


2. Click **User note** link at the **Permissions for columns and views** page.

3. Click **Edit Permissions** button at the **Column Permissions: User note** page and confirm the creation of customized permissions list:

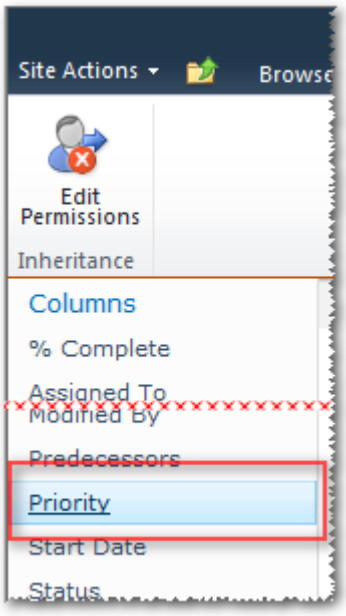


4. Mark all groups in the list with the flags, excluding **Developers** group and click **Remove User Permissions** button[2]:



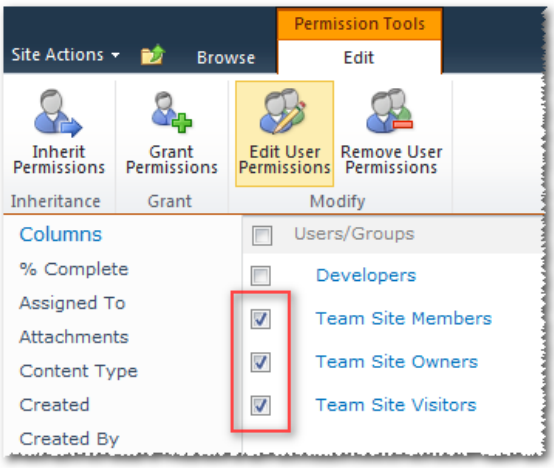
[2] If all groups and users will be removed from permissions list, field or List View will be visible for site-collection administrators only.

5. Chose **Priority** field in the left listing:

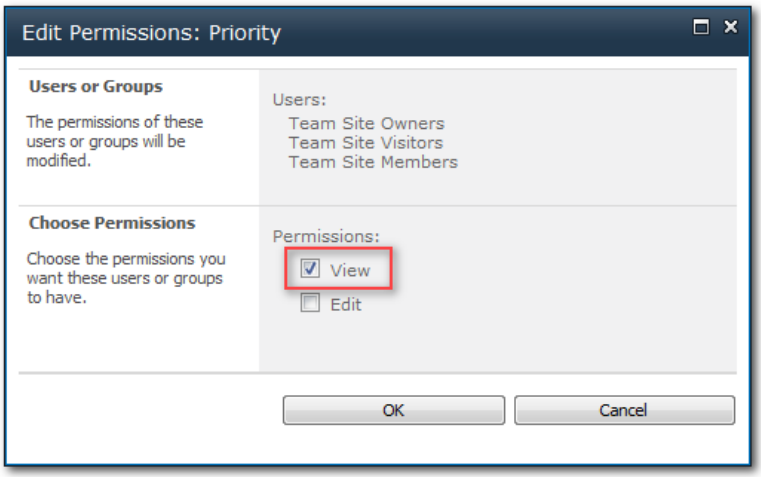


6. Click **Edit Permissions** button at the **Column Permissions: Priority** page and confirm the creation of customized permissions list.

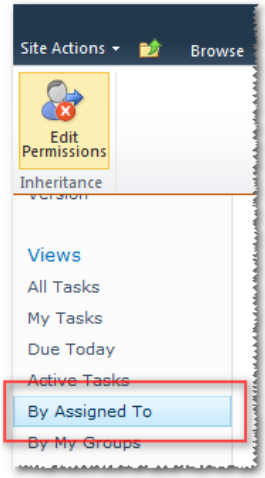
7. Mark with the flags all existed groups, excluding **Developers** group and click **Edit User Permissions** button:



8. Set the **View** flag in **Edit Permissions: Priority** dialog window and click **Ok**:



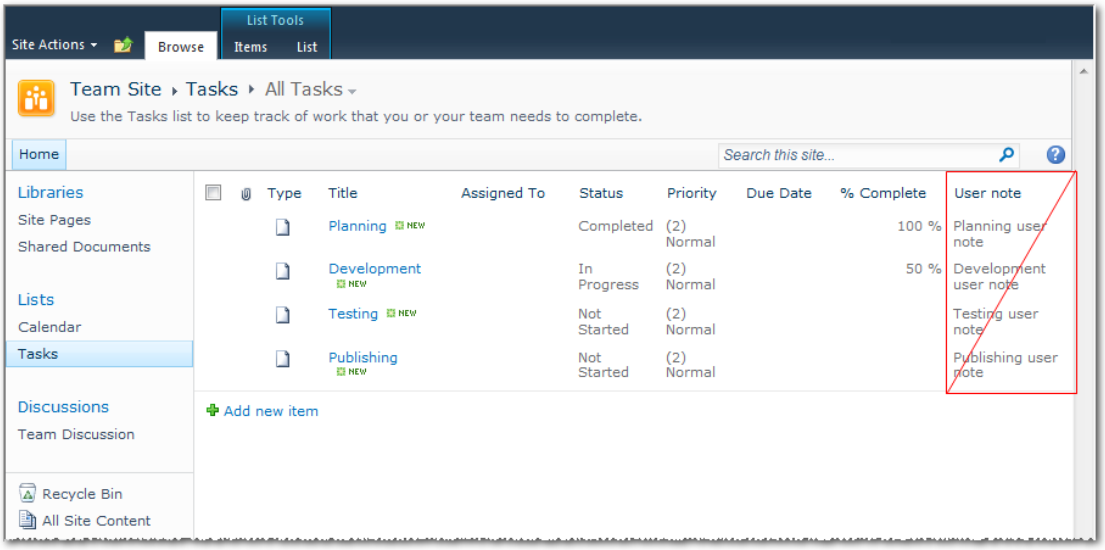
9. Choose **By Assigned To** view in the left listing and click **Edit User Permissions** button:



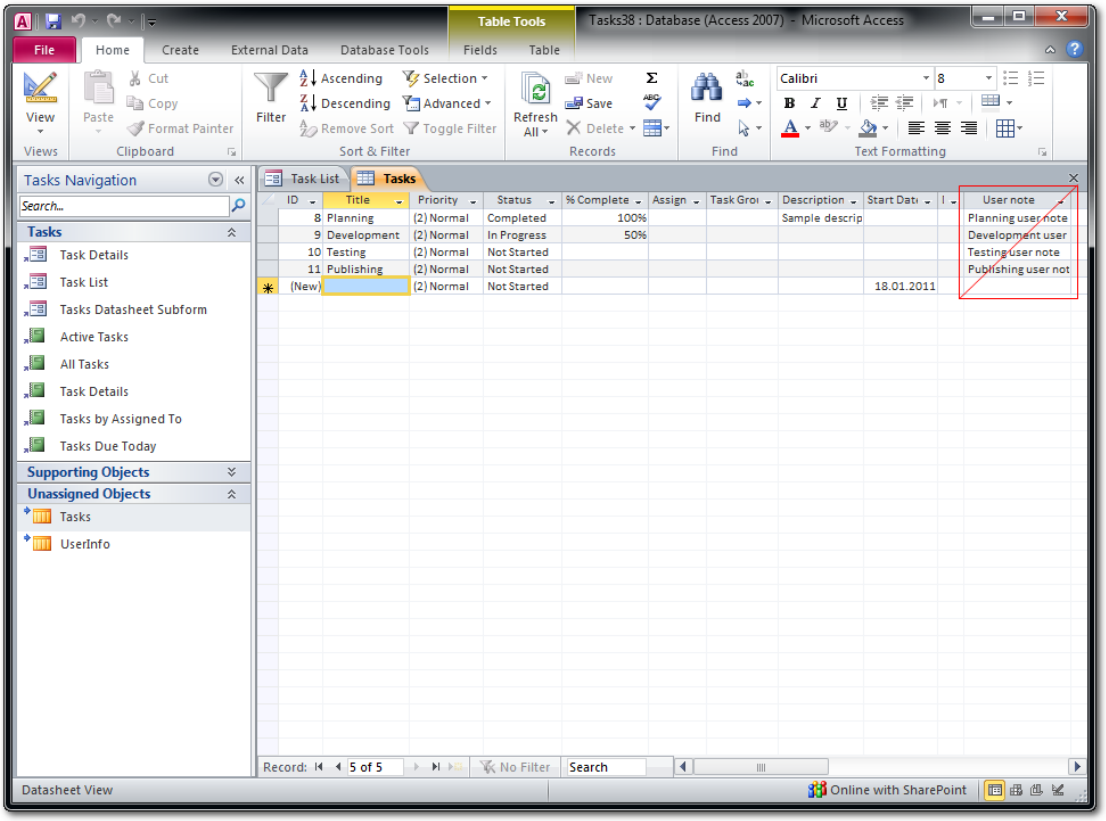
10. Click **Edit Permissions** button in the ribbon at the **View Permissions: By Assigned To** page and confirm the creation of customized permissions list.
11. Mark with the flag all groups in the list, excluding **Developers** group and click **Remove User Permissions** button.
12. The permissions settings are finished. The changes will be active in 5 minutes after they were completed.

The views of the **Task** list will have the following appearance after the actions above:

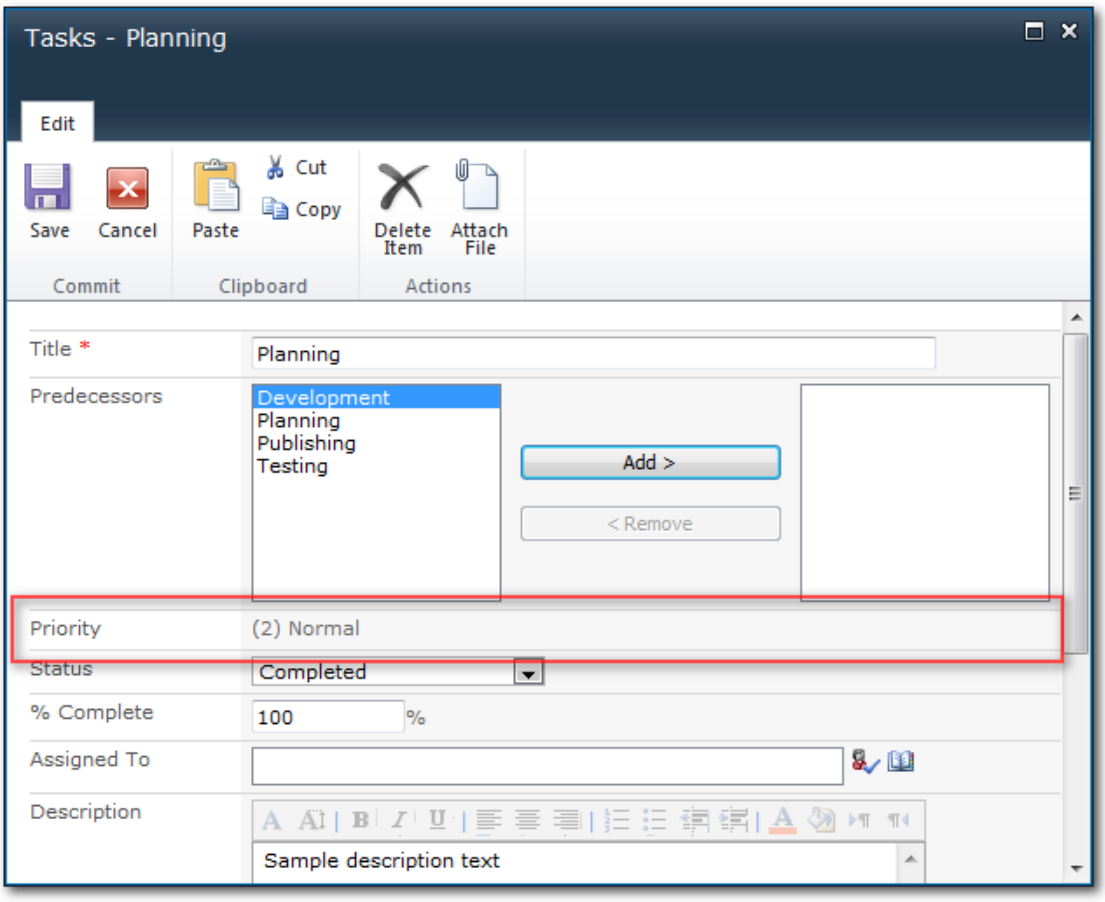
1. **User note** column is hidden in **All Tasks** table view. The appropriate field is hidden in the standard forms of this list.



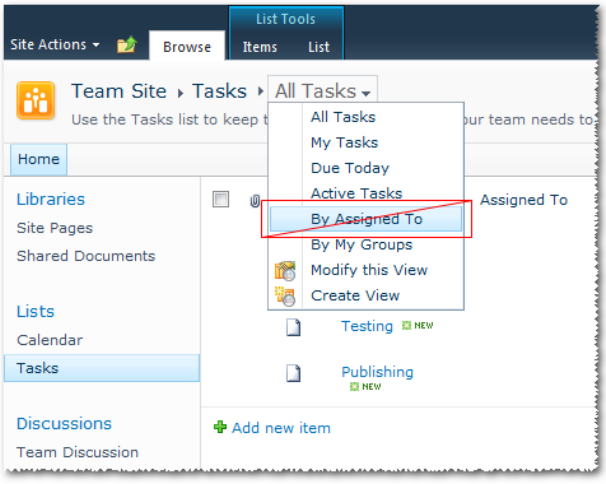
2. **User note** field is hidden in Microsoft Access also:



3. **Priority** field is inaccessible for editing:



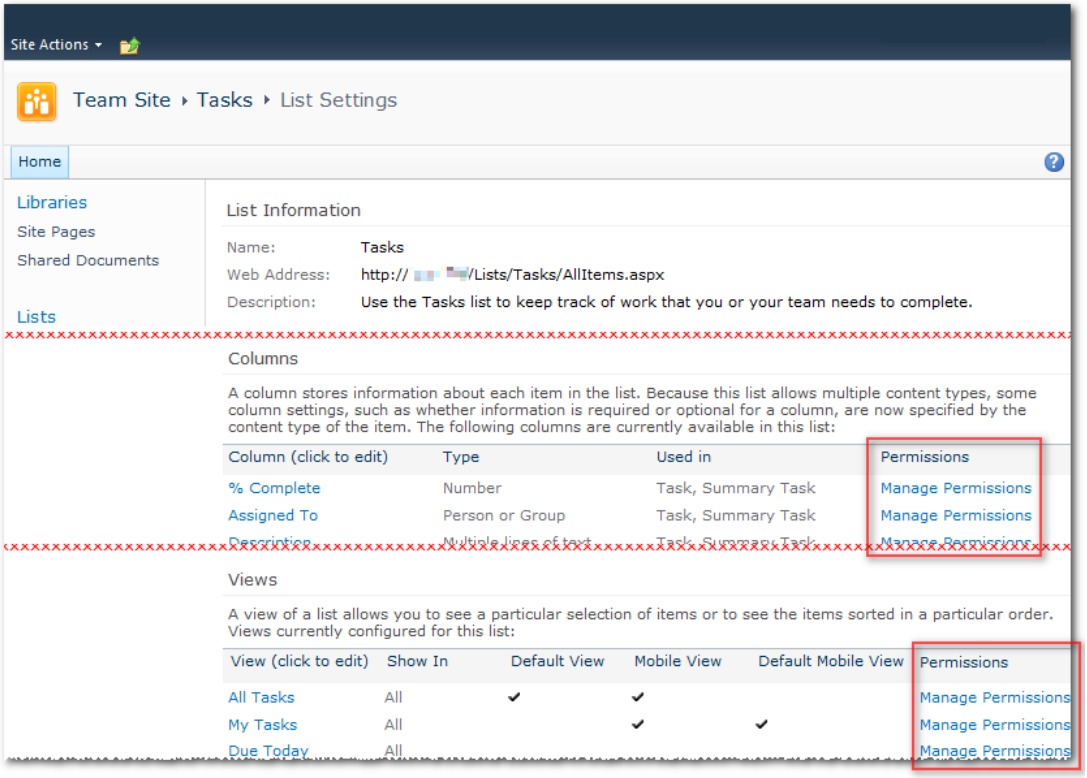
4. **By Assigned To** view disappears from accessible views list. In addition, this view page cannot be opened with a direct link.



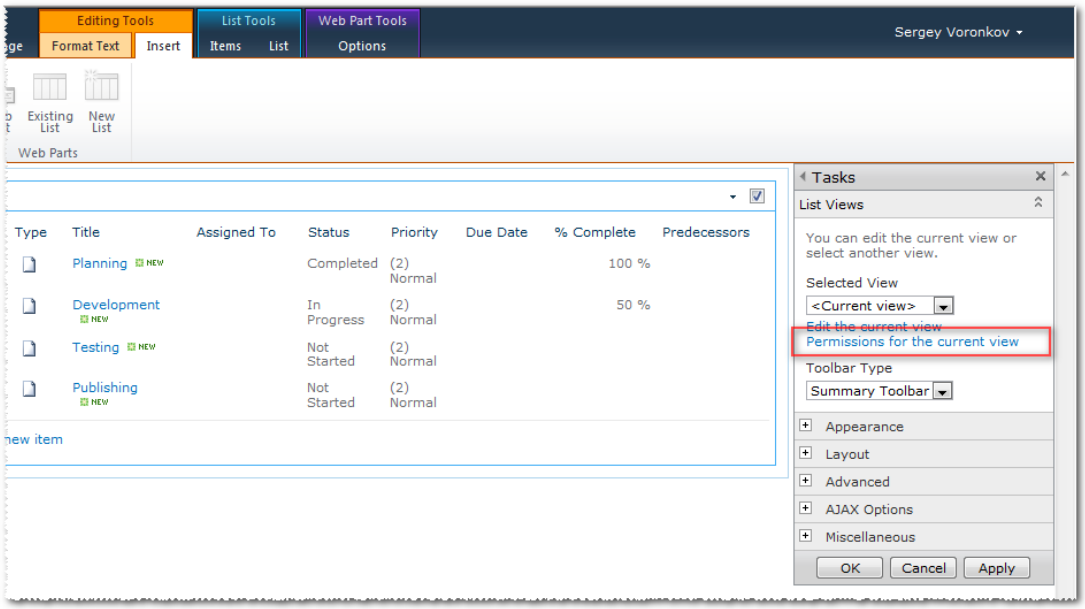
ADDITIONAL FEATURES

For convenient usage, links to permission settings pages are placed in the following SharePoint web-site areas:

- Additional **Manage Permissions** links at **List Settings** page:



- **Permissions for the current view** link at **List Views** web-part settings plane:



THE TRIAL: FEATURES AND RECOMMENDATIONS

ListPermissionsUP for SharePoint has 30-day trial. It is intended specially for the product evaluation in your environment and making a decision regarding applicability for you needs. The product has not any additional limitations during the trial.

Under some technological issues, there are several inconveniences complicate the testing process. These inconveniences are related with two factors:

- Cash-mode for the field items permission table. This mode is required to accelerate the product' functioning and to reduce web-server loading. However, cash-mode also means that the time from permissions changes till changed permissions activation can take up to 5 minutes (default duration of cashed tables storing). It can be inconvenient for instant testing of the product features.

  To exclude the cash-mode influence from the testing process, it is required to switch it off with the following command:

  ```
  > stsadm -o slprmstreatsiteadminregular -enable
  ```

- Web-site users with administrator permissions always have full access to all fields and list views. The SharePoint creators follow the rule: «Site collection administrators always have full access to any content of the data collection ». ListPermissionsUP for SharePoint has the same ideology and it is be subordinated to this rule too. However it is inconvenient for the testing because of the site-collection administrator has a tester role very often. So, the administrator cannot see the results of the product functioning during testing.

  To exclude the administrator' status influence during testing, it is possible to set up special policy with the following command:

  ```
  > stsadm -o slprmscachetimeout -minutes 0
  ```

To return the product in normal mode, the following commands must be realized step by step:

```
stsadm -o slprmstreatsiteadminregular -disable
```

```
stsadm -o slprmscachetimeout -minutes 5
```

All indicated policies will be active up to 5 minutes after the command for its changing.

TROUBLESHOOTING

ListPermissionsUP for SharePoint uses SharePoint native diagnostics system. All errors and other informational messages are placed to SharePoint log files. These files are saved in the following folders::

- Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007
  C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\LOGS
- SharePoint Foundation 2010 or Microsoft SharePoint Server 2010
  C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS

All diagnostics records for ListPermissionsUP for SharePoint have **EventID** parameter with **slcp** value.

Log-files analysis can strongly assist during searching of product' errors and investigation of failures. The great assistance for SharePoint log-files analysis can be provided by the special tools. Particularly, we recommend to use Microsoft utility - **ULS Viewer**, which can be found here http://code.msdn.microsoft.com/ULSViewer.

If you are not able to find the error and fix it, you need to contact Speals support team:

http://www.speals.com/support/

Please, provide the following information (if it is possible) when contact us:

- SharePoint server operational system' version (for example: Windows Web Server R2).
- Exact name and version of installed SharePoint product (for example: Microsoft Office SharePoint Server 2007 SP1).
- Names of third-party web-parts, solutions and tools deployed on SharePoint farm.
- Information from log-files analysis, if you have it.
- Any other information which can be used to resolve your issue.