SharePoint Column Permission

Please note that Column View Permission has to be activated before it can be used. For further reference, please see our Product Installation Guide.

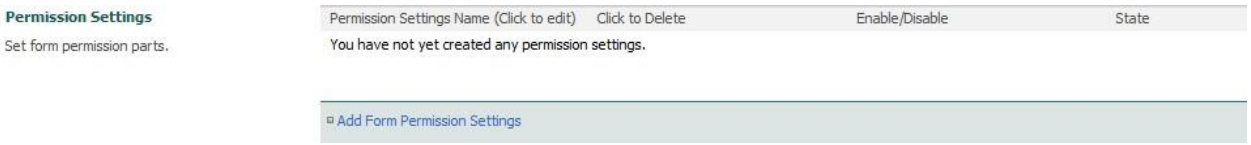
Further information is also available in our FAQ.

Feature Introduction

Column Permission

This function lets the administrator globally enable or disable or Column Permission settings configured with Column Permission in this list.

Permission Settings



The Permissions Settings section gives the administrator an overview over all Column Permission settings already set up. Each settings part can be deleted, or enabled disabled. The status field display whether a settings part is enabled or disabled. To edit a Column Permission settings part click the name of the settings part which will open the settings page for the Column Permission settings part.

To add Column Permission settings, click the “Add Form Permissions Settings” link.

Import/Export Permission Parts

The new version of Column View Permission allows for importing and exporting permission parts. This function is based on XML files. Thus, creating similar permissions for different sites will be easier and less time consuming.

To import settings click the Import button. A popup window will open. There the administrator can either paste the XML file contents into the designated area, or browse for a file and upload it. After uploading the file the contents will be displayed in the area above the upload area. To confirm importing the XML file click the OK button. To abort importing the specified permission settings, click the Cancel button.

To export permission settings click the Export button. A popup window will open and display the XML file contents in the edit area. The administrator can then save the settings to any location and thus make it reusable in other lists. To abort exporting the settings, click the Cancel button.

Permission Settings Name

Name each Column Permission settings part. The settings part will be displayed with this name in the Permission Settings table in the main settings page for View Permission.

User/Group Selection Process

The User/Group selection process has been modified and improved compared to the previous version. One distinctive difference is that administrators are now able to specify in far more detail which users to include and which to exclude from the selection process. It also makes understanding the selection easier as both parts share the same interface.

The first selection lets the administrator decide if he wants to include all users, or if he wants to select a small group of users based on criteria that he specifies below.

Column View Permission now allows for specific selection of users and groups by filtering them by:

a) Including/excluding anonymous users
b) Input of user or group names
c) Selecting user/group columns, as well as relative lookup fields in this list
d) Looking up users from other lists and filter them based on conditions

a) Anonymous Users

This allows the administrator to include anonymous users in the permission settings.

An anonymous user is used for public access to your Web Site.

Anonymous access allows anyone to visit the public areas of your Web sites while preventing unauthorized users from gaining access to your Web server's critical administrative features and private information.

b) Input of user and group names

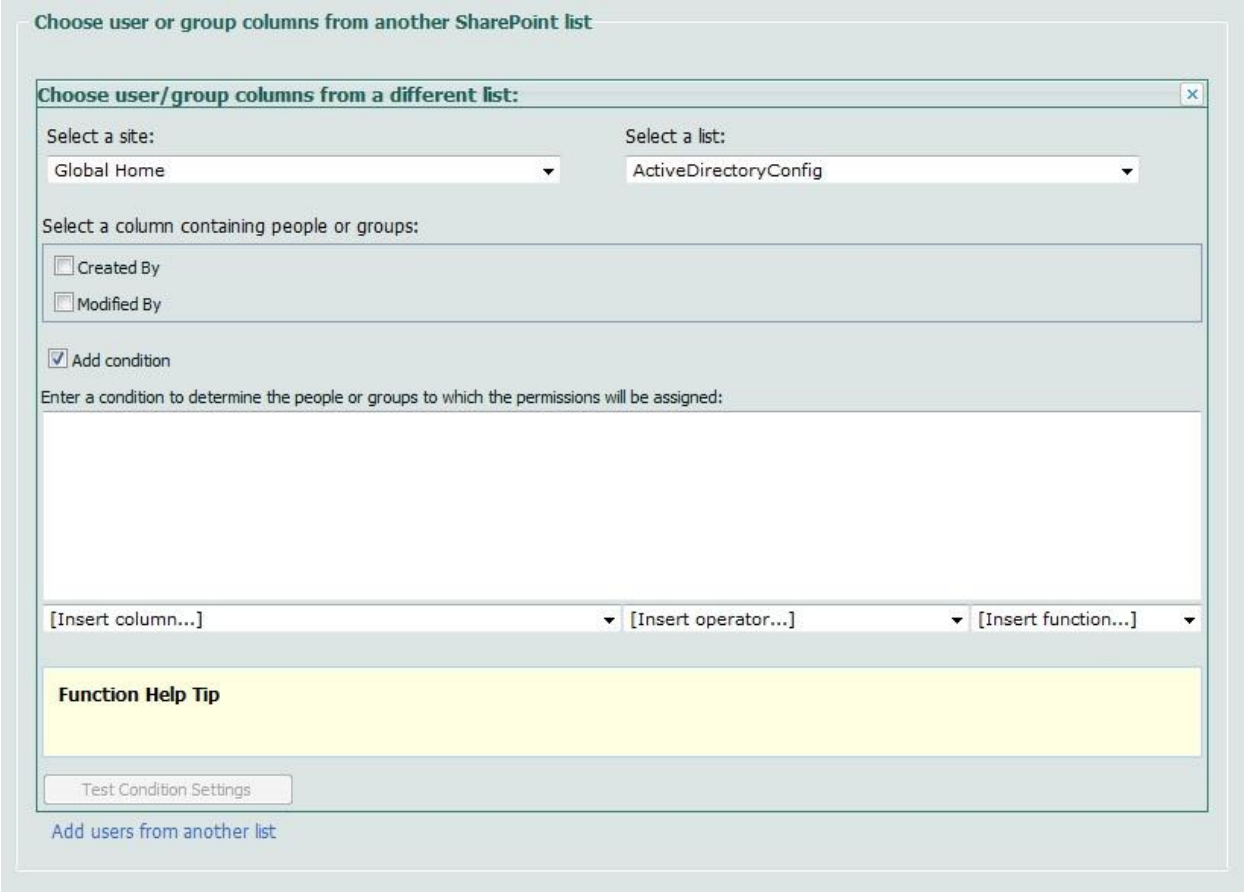
As in previous versions, Column View Permission provides a box to enter any user or group name. It also allows entering multiple users or groups, and as with the default user selection, the administrator can look up names or check the names entered into the box.

c) Selecting user/group columns, as well as relative lookup fields in this list

As in previous versions, Column View Permission provides checkboxes with all User/Group columns available. Checking these checkboxes will result in selecting the users which are contained within the selected column. This selection will filter the values in the column specified with the logged in user. The permissions are only set for items associated with the currently logged in user, but will not affect any other items.

The administrator can also select related columns, if the checkbox to display them is checked. This means that all user/group columns in the list that is looked up from will be available for selection.

d) Looking up users from other lists and filter them based on conditions



The process to select users from another list works in 3 steps:

1. Specify the list to look up from. To do so, the administrator has to firstly select the site on which the list is located. Note that only sites in the same site collection are available. All lists located on this site will be available for selection in another dropdown list.
2. Specify the User/Group columns that will be used to specify the users. These are to be selected through checkboxes, similar to the User/Group column selection in the original list. The difference is that all the users are pulled from the column regardless of the user who has logged in. Thus the settings will be the same for all items. Also, related columns are not available to select in these settings.
3. A final step is the ability to filter the users selected based on conditions.

Specify Selection Criteria Based on Conditions

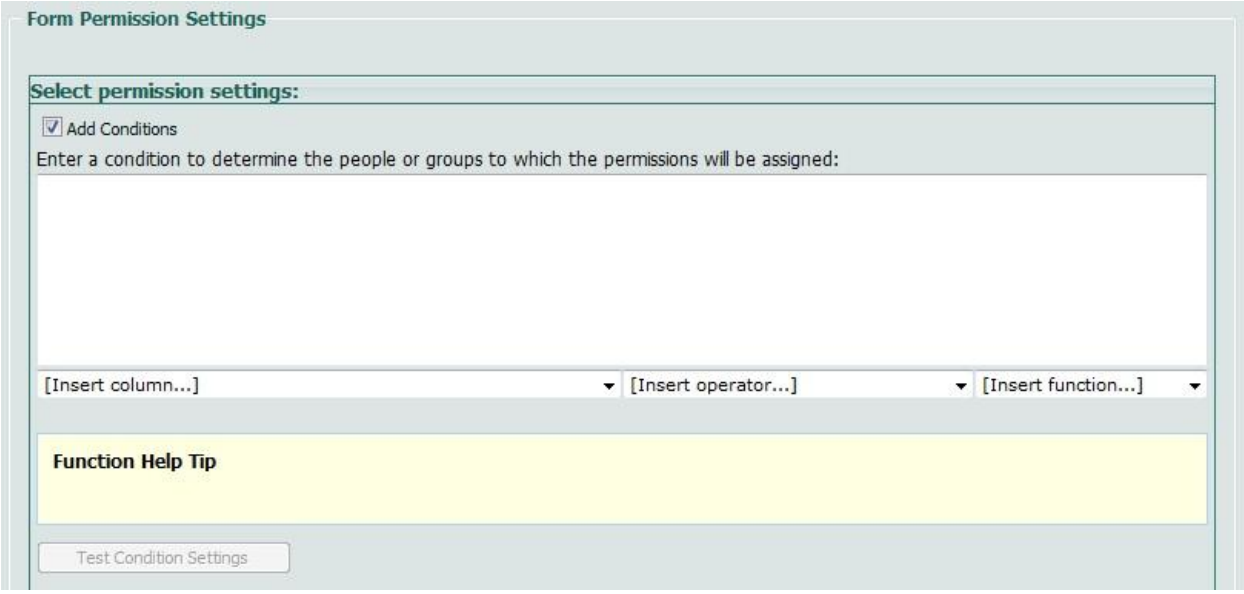
We have introduced conditions to specify user and items even more precise, and thus providing an even more granular approach. The conditions sections have been added in two sections:

a) For filtering users/groups from other sites
b) For specifying the items that will be affected by the permission settings

a) The process to select users from another list works in 3 steps:

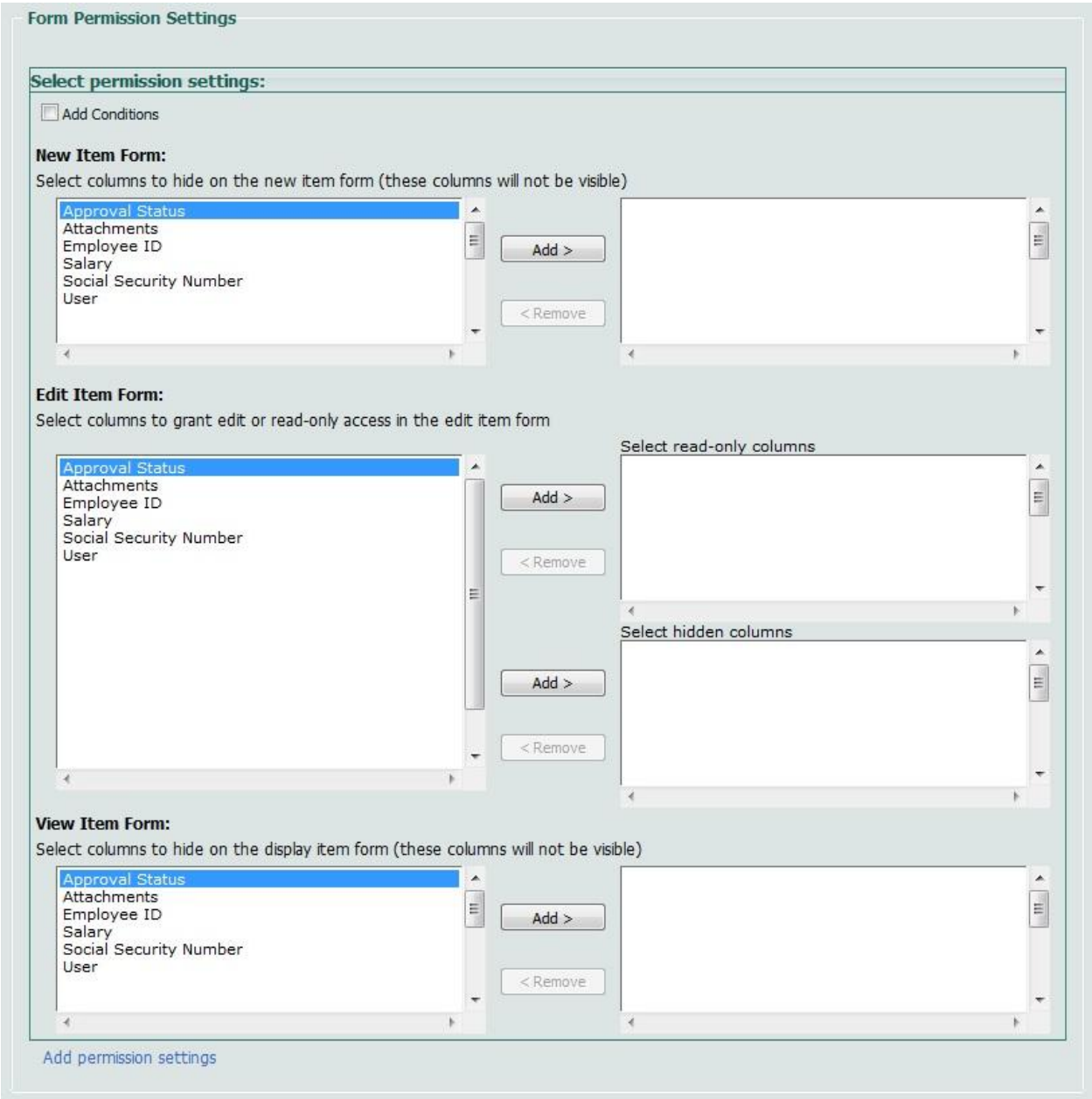
1. Specify the list to look up from. To do so, the administrator has to firstly select the site on which the list is located. Then all lists located on this site will be available for selection in a dropdown list.
2. Specify the User/Group columns that will be used to specify the users. These are to be selected through checkboxes, similar to the User/Group column selection in the original list.
3. Filter the results by specifying conditions. The conditions allow to build relationships between the User/Group columns and any other column existing in the list. This will effectively result in only selecting users who meet the conditions specified.

b) Specifying items that will be affected by the permission settings:



By entering conditions, the administrator can specify for which items the permissions are set. The main difference to the user selection process is that these conditions are only based on the current list. There is no reference to other lists possible. Also, the selection process is not based on any associated columns with the user selection, but it takes direct effect.

Form Permission Settings



In the new version of Column View Permission the administrator has the option to not only set the permissions for columns, but instead can specify what columns are accessible in what way for each form.

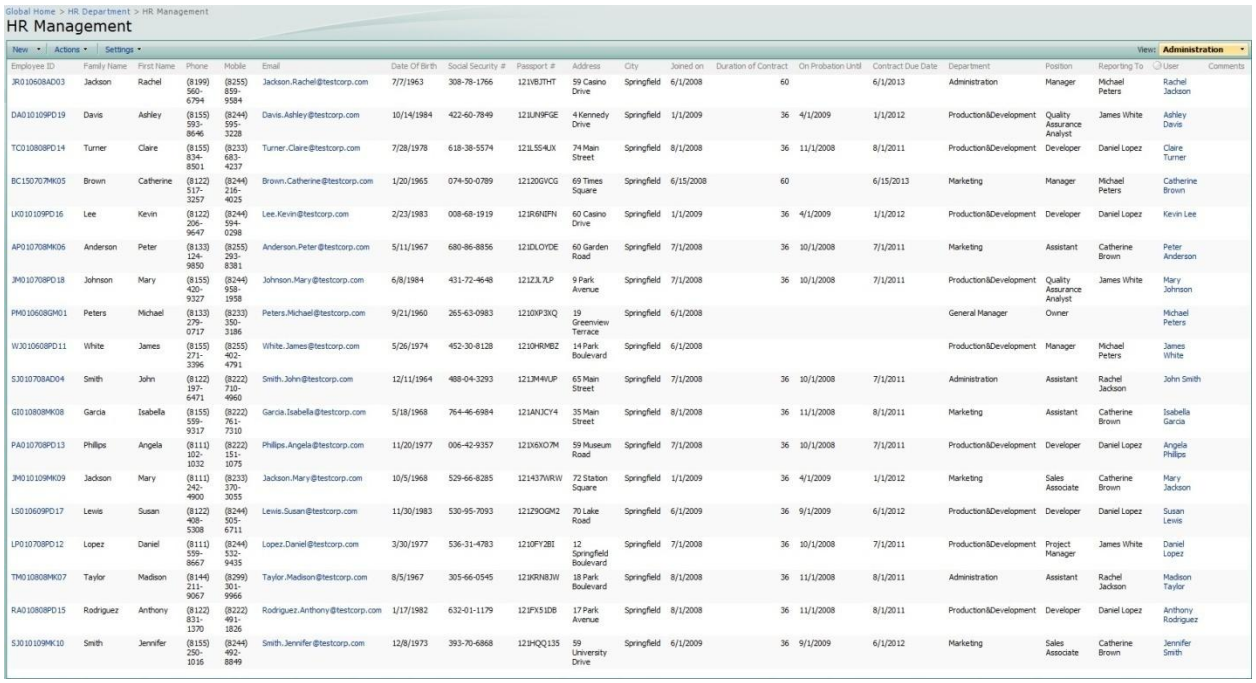
To set columns read-only, they have to be set as read-only in the Edit Item Form.

To set columns hidden, they have to be set as hidden in all three forms, meaning the New Item Form, the Edit Item Form and the View Item Form.

Column Permission and View Permission are working closely together. This means that columns hidden from certain users will have to be removed from a view if these users should be able to access this view. If a view contains these columns it will not be accessible to the users.

Example

In a list that keeps confidential information on HR, most companies will have to restrict access to certain fields.



Global Home > HR Department > HR Management

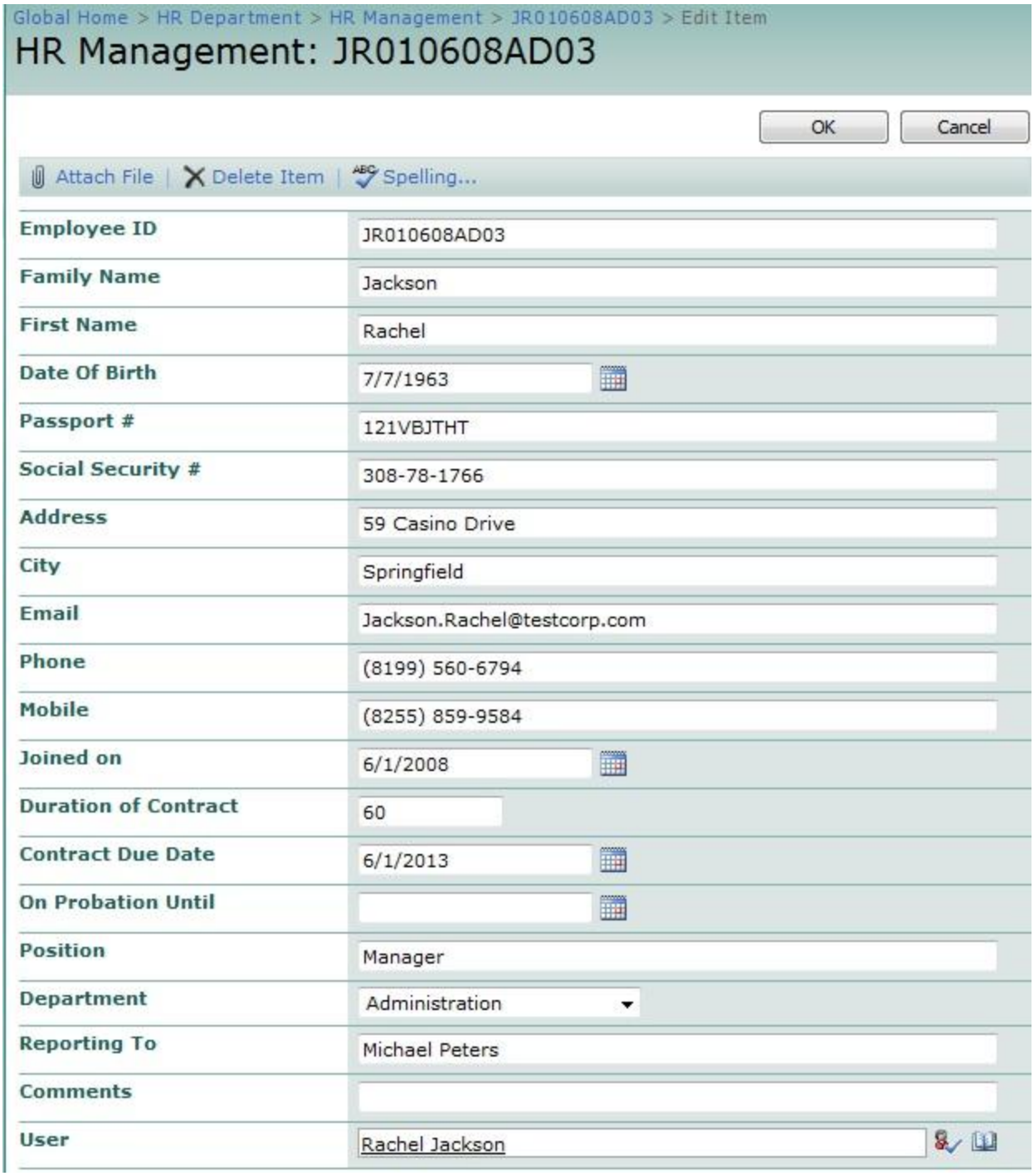
HR Management

New | Actions | Settings — View: Administration

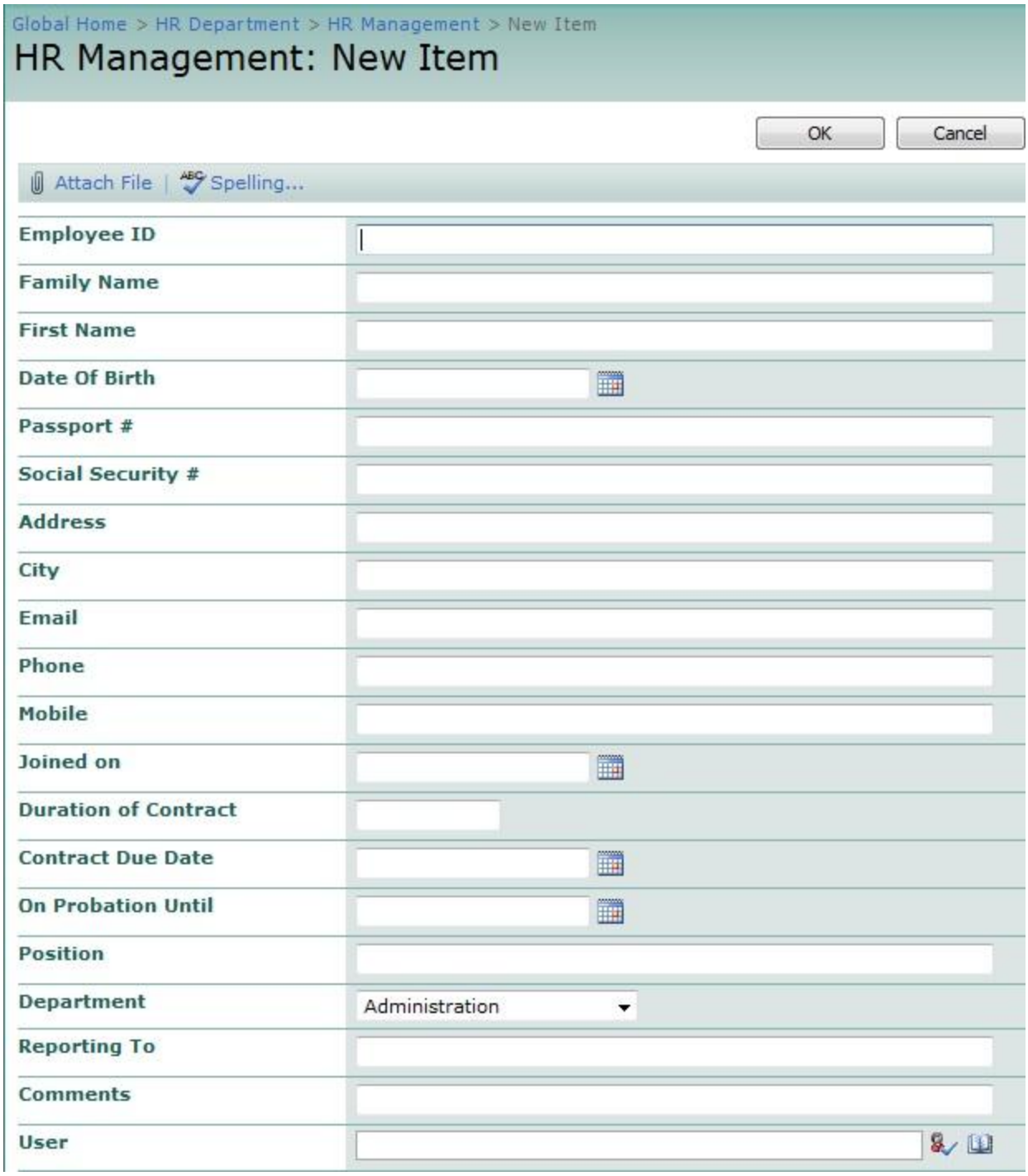
Employee ID	Family Name	First Name	Phone	Mobile	Email	Date Of Birth	Social Security #	Passport #	Address	City	Joined on	Duration of Contract	On Probation Until	Contract Due Date	Department	Position	Reporting To	User	Comments
JR010608AD03	Jackson	Rachel	(8199) 560-6794	(8255) 859-9584	Jackson.Rachel@testcorp.com	7/7/1963	308-78-1766	121VBJTHT	59 Casino Drive	Springfield	6/1/2008	60		6/1/2013	Administration	Manager	Michael Peters	Rachel Jackson	
DA010109PD19	Davis	Ashley	(8155) 593-8646	(8244) 595-3228	Davis.Ashley@testcorp.com	10/14/1984	422-60-7849	121UN9FGE	4 Kennedy Drive	Springfield	1/1/2009	36	4/1/2009	1/1/2012	Production&Development	Quality Assurance Analyst	James White	Ashley Davis	
TC010808PD14	Turner	Claire	(8155) 834-8501	(8233) 683-4237	Turner.Claire@testcorp.com	7/28/1978	618-38-5574	121LSS4UX	74 Main Street	Springfield	8/1/2008	36	11/1/2008	8/1/2011	Production&Development	Developer	Daniel Lopez	Claire Turner	
BC150707MK05	Brown	Catherine	(8122) 517-3257	(8244) 218-4025	Brown.Catherine@testcorp.com	1/20/1965	074-50-0789	12120GVCG	69 Times Square	Springfield	6/15/2008	60		6/15/2013	Marketing	Manager	Michael Peters	Catherine Brown	
LK010109PD16	Lee	Kevin	(8122) 206-9647	(8244) 594-0298	Lee.Kevin@testcorp.com	2/23/1983	008-68-1919	121R6NIFN	60 Casino Drive	Springfield	1/1/2009	36	4/1/2009	1/1/2012	Production&Development	Developer	Daniel Lopez	Kevin Lee	
AP010708MK06	Anderson	Peter	(8133) 124-9850	(8255) 293-8381	Anderson.Peter@testcorp.com	5/11/1967	680-86-8856	121DLOYDE	60 Garden Road	Springfield	7/1/2008	36	10/1/2008	7/1/2011	Marketing	Assistant	Catherine Brown	Peter Anderson	
JM010708PD18	Johnson	Mary	(8155) 420-9327	(8244) 958-1958	Johnson.Mary@testcorp.com	6/8/1984	431-72-4648	121ZJL7LP	9 Park Avenue	Springfield	7/1/2008	36	10/1/2008	7/1/2011	Production&Development	Quality Assurance Analyst	James White	Mary Johnson	
PM010608GM01	Peters	Michael	(8133) 279-0717	(8233) 350-3186	Peters.Michael@testcorp.com	9/21/1960	265-63-0983	1210XP3XQ	19 Greenview Terrace	Springfield	6/1/2008				General Manager	Owner		Michael Peters	
WJ010608PD11	White	James	(8155) 271-3396	(8255) 402-4791	White.James@testcorp.com	5/26/1974	452-30-8128	1210HRMBZ	14 Park Boulevard	Springfield	6/1/2008				Production&Development	Manager	Michael Peters	James White	
SJ010708AD04	Smith	John	(8122) 197-6471	(8222) 710-4960	Smith.John@testcorp.com	12/11/1964	488-04-3293	121JM4WUP	65 Main Street	Springfield	7/1/2008	36	10/1/2008	7/1/2011	Administration	Assistant	Rachel Jackson	John Smith	
GI010808MK08	Garcia	Isabella	(8155) 599-9317	(8222) 761-7310	Garcia.Isabella@testcorp.com	5/18/1968	764-46-6984	121ANJCY4	35 Main Street	Springfield	8/1/2008	36	11/1/2008	8/1/2011	Marketing	Assistant	Catherine Brown	Isabella Garcia	
PA010708PD13	Phillips	Angela	(8111) 102-1032	(8222) 151-1075	Phillips.Angela@testcorp.com	11/20/1977	006-42-9357	121X6XO7M	59 Museum Road	Springfield	7/1/2008	36	10/1/2008	7/1/2011	Production&Development	Developer	Daniel Lopez	Angela Phillips	
JM010109MK09	Jackson	Mary	(8111) 242-4900	(8233) 370-3055	Jackson.Mary@testcorp.com	10/5/1968	529-66-8285	121437WRW	72 Station Square	Springfield	1/1/2009	36	4/1/2009	1/1/2012	Marketing	Sales Associate	Catherine Brown	Mary Jackson	
LS010609PD17	Lewis	Susan	(8122) 408-5308	(8244) 505-6711	Lewis.Susan@testcorp.com	11/30/1983	530-95-7093	121Z9OGM2	70 Lake Road	Springfield	6/1/2009	36	9/1/2009	6/1/2012	Production&Development	Developer	Daniel Lopez	Susan Lewis	
LP010708PD12	Lopez	Daniel	(8111) 559-8667	(8244) 532-9435	Lopez.Daniel@testcorp.com	3/30/1977	536-31-4783	1210FY2BI	12 Springfield Boulevard	Springfield	7/1/2008	36	10/1/2008	7/1/2011	Production&Development	Project Manager	James White	Daniel Lopez	
TM010808MK07	Taylor	Madison	(8144) 211-9067	(8299) 301-9966	Taylor.Madison@testcorp.com	8/5/1967	305-66-0545	121KRN8JW	18 Park Boulevard	Springfield	8/1/2008	36	11/1/2008	8/1/2011	Administration	Assistant	Rachel Jackson	Madison Taylor	
RA010808PD15	Rodriguez	Anthony	(8122) 831-1370	(8222) 491-1826	Rodriguez.Anthony@testcorp.com	1/17/1982	632-01-1179	121FX51DB	17 Park Avenue	Springfield	8/1/2008	36	11/1/2008	8/1/2011	Production&Development	Developer	Daniel Lopez	Anthony Rodriguez	
SJ010109MK10	Smith	Jennifer	(8155) 250-1016	(8244) 492-8849	Smith.Jennifer@testcorp.com	12/8/1973	393-70-6868	121HQQ135	59 University Drive	Springfield	6/1/2009	36	9/1/2009	6/1/2012	Marketing	Sales Associate	Catherine Brown	Jennifer Smith	

The screenshot above illustrates this issue; here a lot of information is included that normal employees should not be able to change. Column View Permission is designed to provide a way to manage permissions for forms. It also provides the option to hide columns, or to set them as read-only.

So for the Edit Item Form all values can be changed, even though the user should not be able to see or changed all the information in this form.



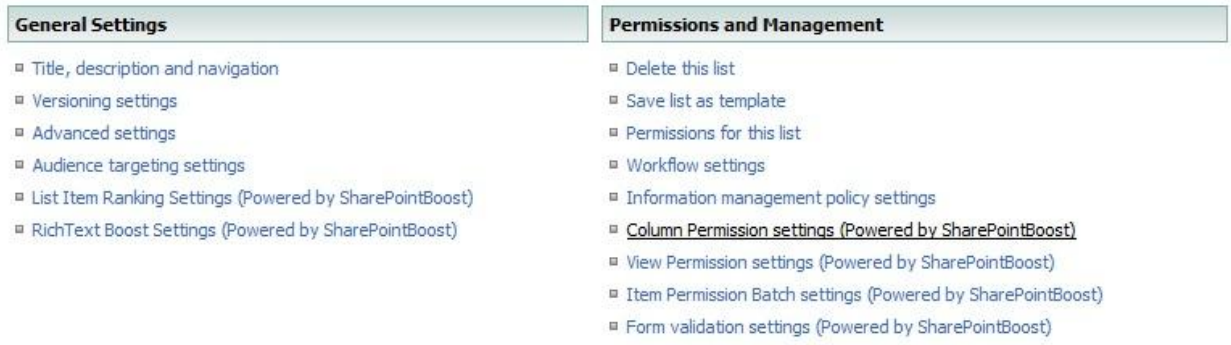
The same issue exists for the New Item Form. Not every user should be able to add information to the list, or enter values for all columns.



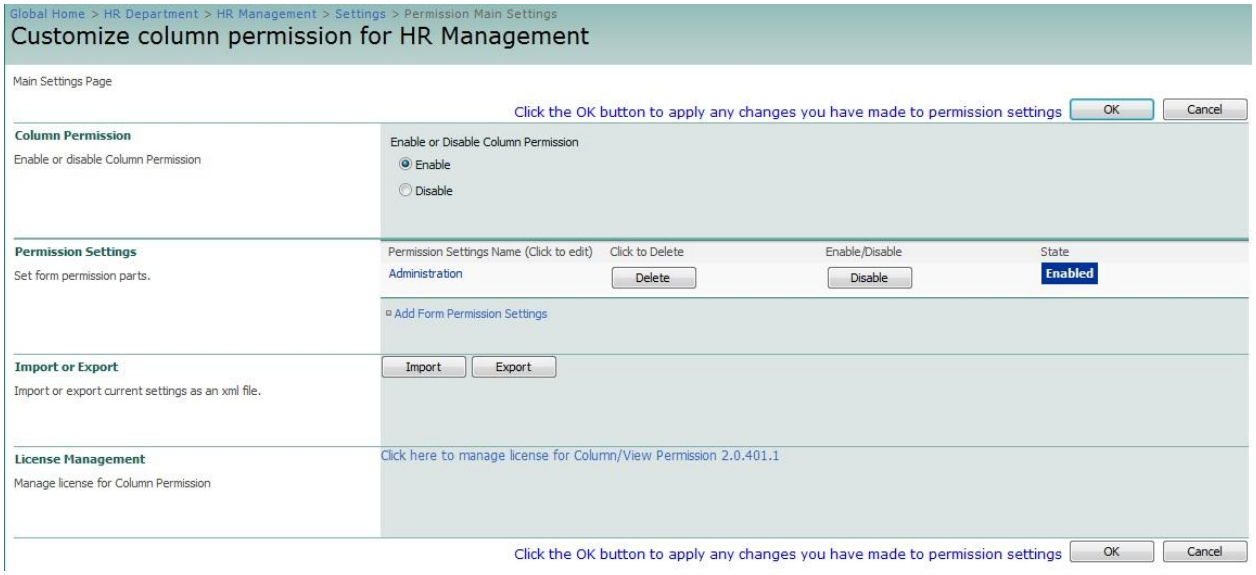
In the View Item Form, most often, companies would want to hide certain information from users. With default settings however the View Item Form looks like the one below.

To change this behavior, navigate to the Column Permission Settings. To do so, enter the List Settings page.

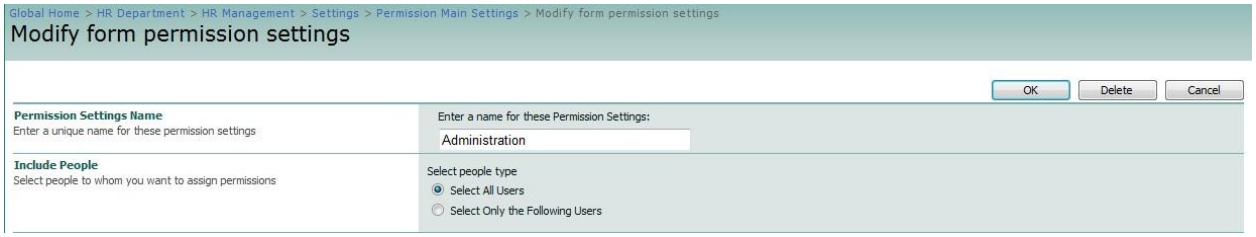
There click the Column Permission settings link.



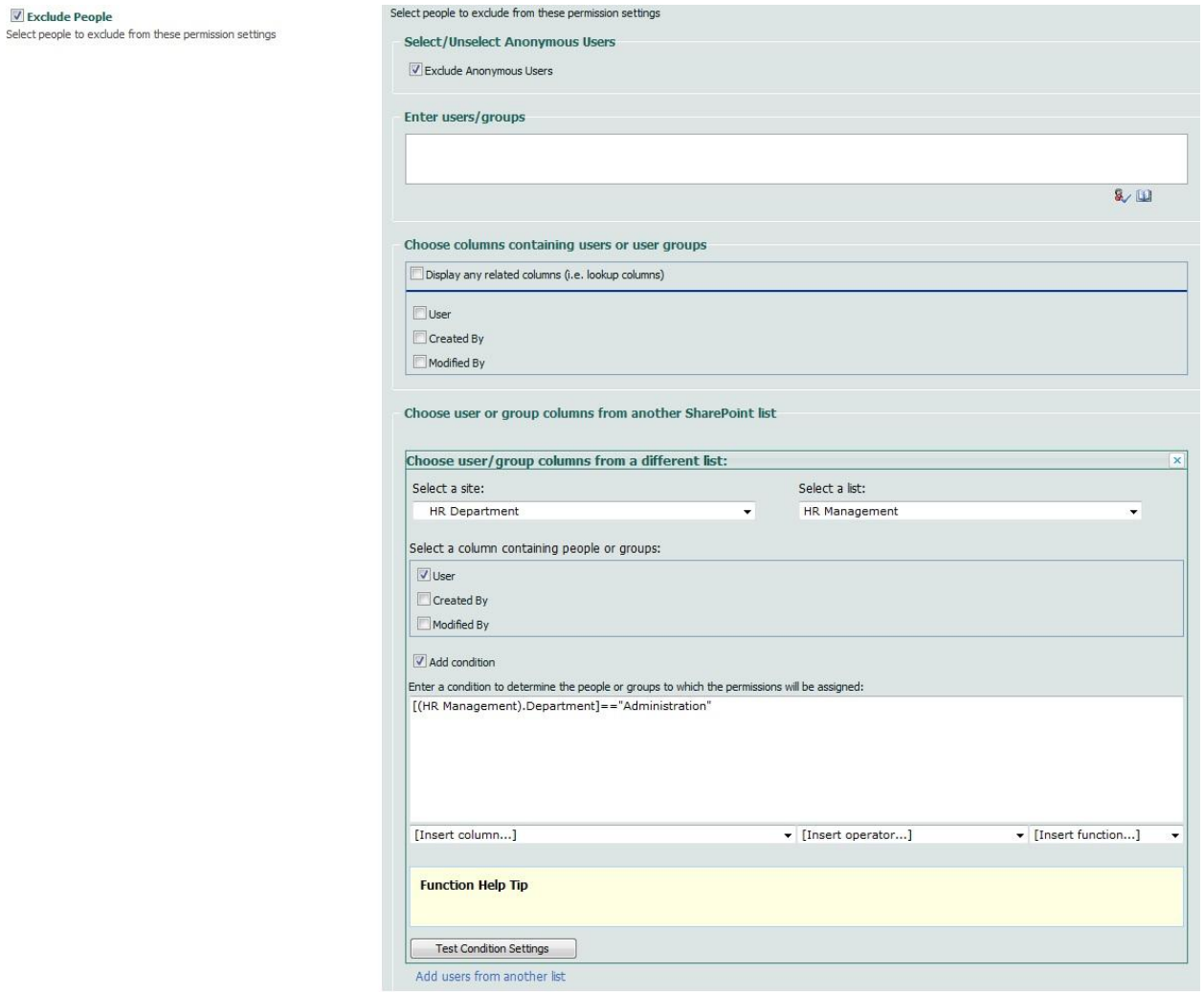
This will direct you to the Column Permission Main Settings page. Here click Add Form Permission Settings.



Here, firstly specify the name of the permissions part, here it is called "Administration".



In the Include People section the checkbox is set to Select All Users. In this Permission part the users affected are specified by excluding users, thus the selection is actually made in the Exclude People part.



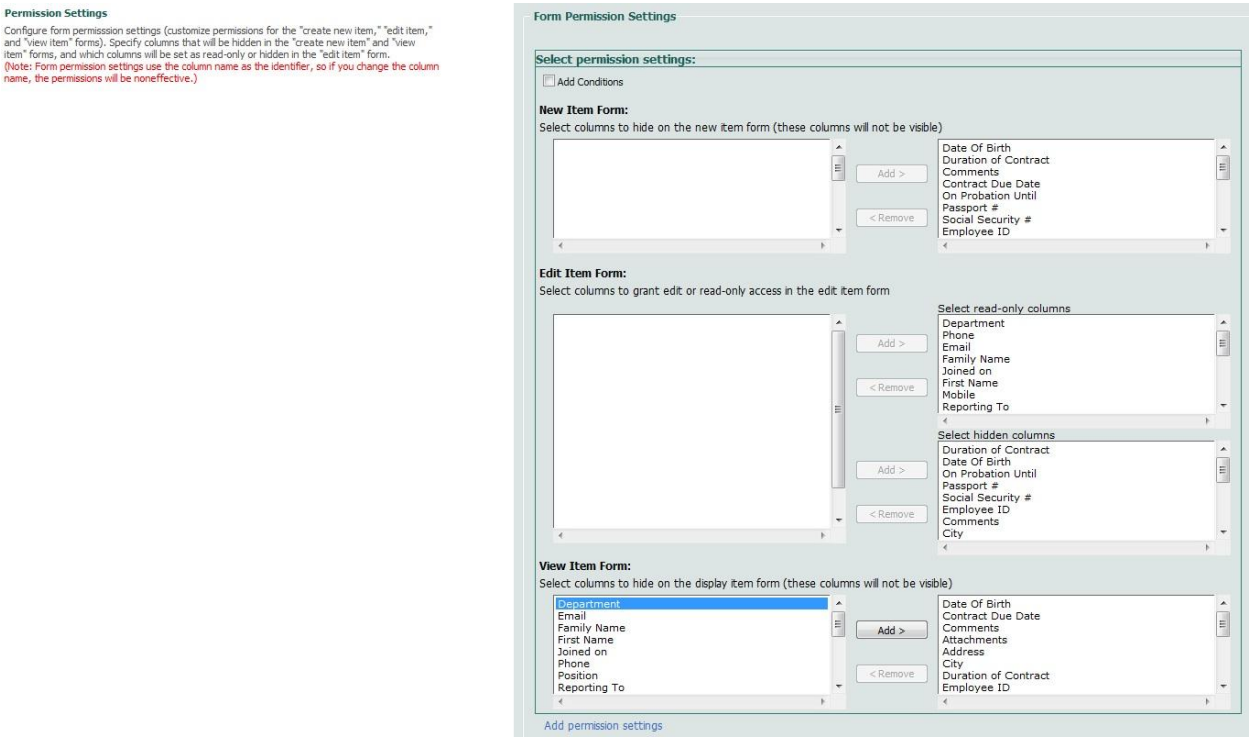
Firstly, the Anonymous Users are excluded from the selection. Furthermore, this settings part should only affect all users except employees in the "Administration" department. To exclude these users, the "Choose user or group from another SharePoint list" section can be used to filter users. To do so you have to specify the site and list to lookup from. In this case, this is actually the same list, so it is the HR Department site, and the HR Management list. After that, a column has to be selected from which the users or groups are pulled from. The "User" column contains all the users in the company; therefore this information has to be filtered. For filtering this information Column Permission provides condition settings. The condition in this case is:

[(HR Management).Department]=="Administration"

This condition specifies that only users working in the "Administration" department will be selected.

Looking at the whole user selection, this part specifies that only users should be affected by these settings who are not an anonymous user, and whose value in the Department field is not "Administration".

To complete the settings you have to specify what permissions the users should have for which form.



These permissions reflect the permissions for all users except the "Administration" department employees.

For the New Item Form, these users should not be able to add any information. Therefore all the columns are set to be hidden.

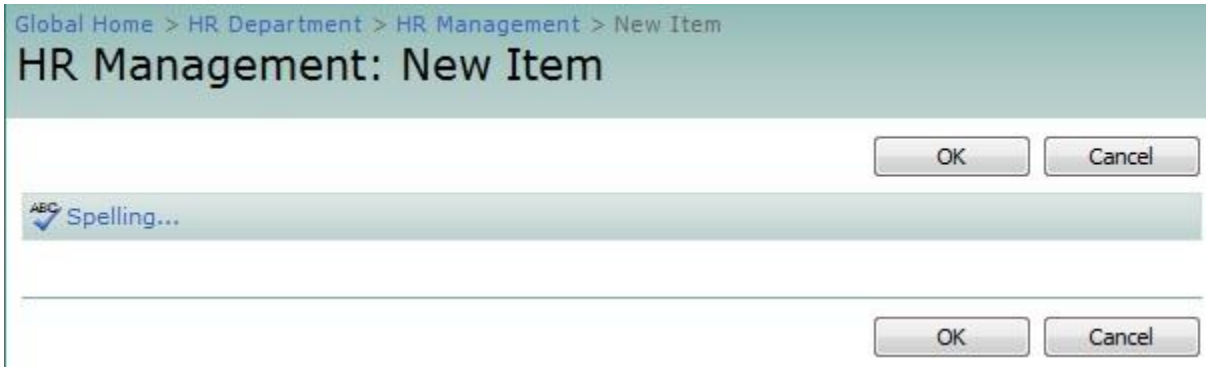
For the Edit Item Form, you can choose to set columns either as read-only, or as hidden. Information in columns like First Name, Family Name, Email, Department, Reporting to, and Phone should be visible, but not changeable for these users.

The permission settings for the View Item Form should reflect the settings in the read-only section for the Edit Item Form. This means that all other columns will be set invisible for this form.

After all settings have been made, confirm by clicking OK. Please note that you also have to click OK in the Column Permission main settings page to confirm any changes made.

Looking in as a user who is not working in the "Administration" department will change the forms displayed.

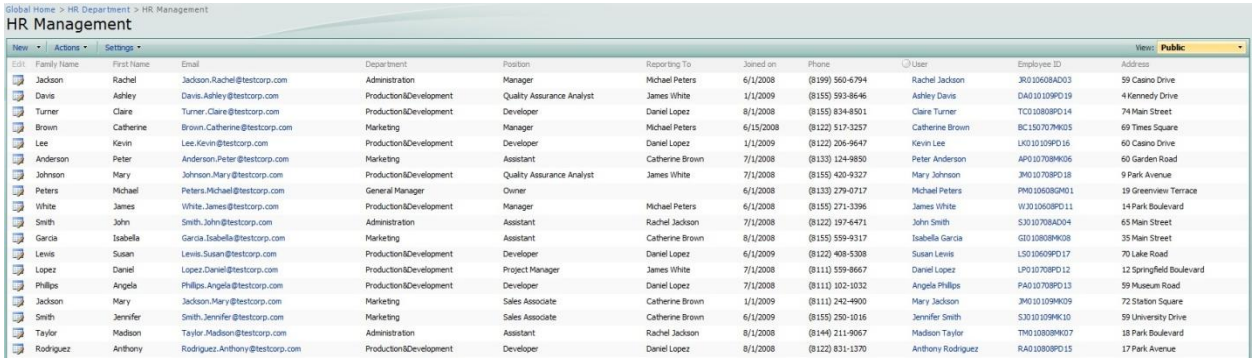
The New Item Form now does not display any column to edit, it is completely empty.



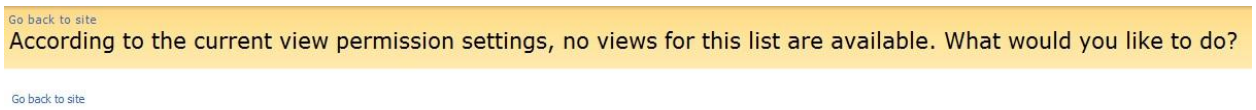
In the Edit Item Form only the columns set as read-only are displayed, all others are not shown anymore. The columns displayed cannot be edited at all, they behave like in the View Item Form.

The View Item Form is also only displaying the columns not set as hidden.

As Column Permission is linked with SharePointBoost's View Permission, views containing columns that are hidden from users will be not accessible.



So in this case while Administration staff can see the Public view with the Address column included, this will throw an error message.



SharePoint-list-items-view.jpg

SharePoint list items view that cannot be seen

However, the view is accessible if the column is removed from this view.

SharePoint View Permission

Please note that Column View Permission has to be activated before it can be used. For further reference, please see our Product Installation Guide.

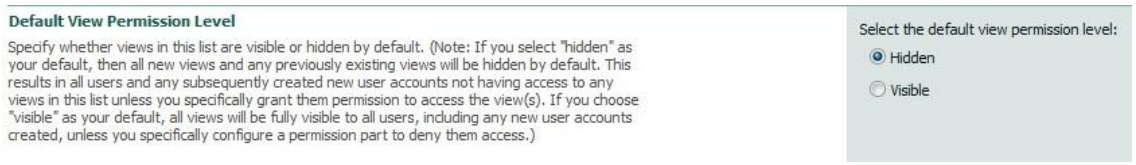
Further information is also available in our FAQ.

Feature Introduction

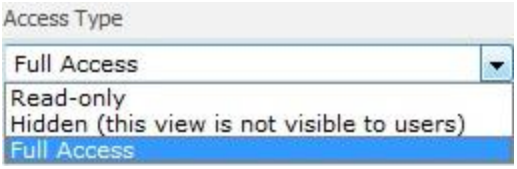
View Permission

This function lets the administrator globally enable or disable or View Permission settings configured with View Permission in this list.

Default View Permission Level



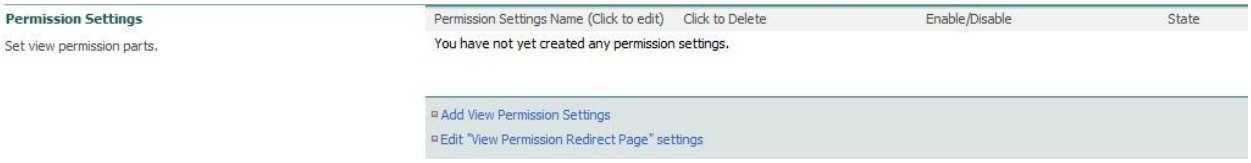
This function defines the default behavior for View Permissions. If the default level is set as “Hidden” then new users will not be able to access any views affected by View Permission settings, unless the administrator specifically grants them access to these view. Setting the default to be “Visible” will thus allow all new users access to all views, unless they specifically denies them access by creating separate View Permission settings.



These settings also have another effect on the View Permission settings. Depending on the value set here, the default value in the Access Type menu in specific View Permission Settings will change. If the default value is “Hidden” then the default in the Access Type menu will also be “Hidden (this view is not visible to users)” However, if the default value is set to be “Visible” then the default in the Access Type menu will change to “Full Access”.

These are important settings if you will lists with a large number of views. Selecting a good default value will set the Access Type for all views, so that the administrator does not have to change these settings. Also, for each new view this value will be set by default, so the administrator can save a lot of time with choosing the appropriate default value.

Permission Settings

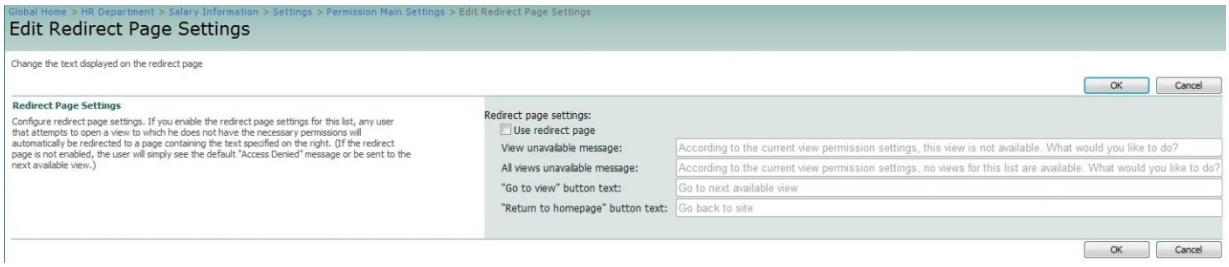


The Permission Settings section gives the administrator an overview over all View Permission settings already set up. Each settings part can be deleted, or enabled disabled. The status field display whether a settings part is enabled or disabled. To edit a View Permission settings part click the name of the settings part which will open the settings page for the View Permission settings part.

To add View Permission settings, click the “Add View Permissions Settings” link.

The “Edit ‘View Permission Redirect Page’ settings” directs the administrator to a site to configure notifications for users if they do not have sufficient permissions to access a view.

Edit "View Permission Redirect Page" settings



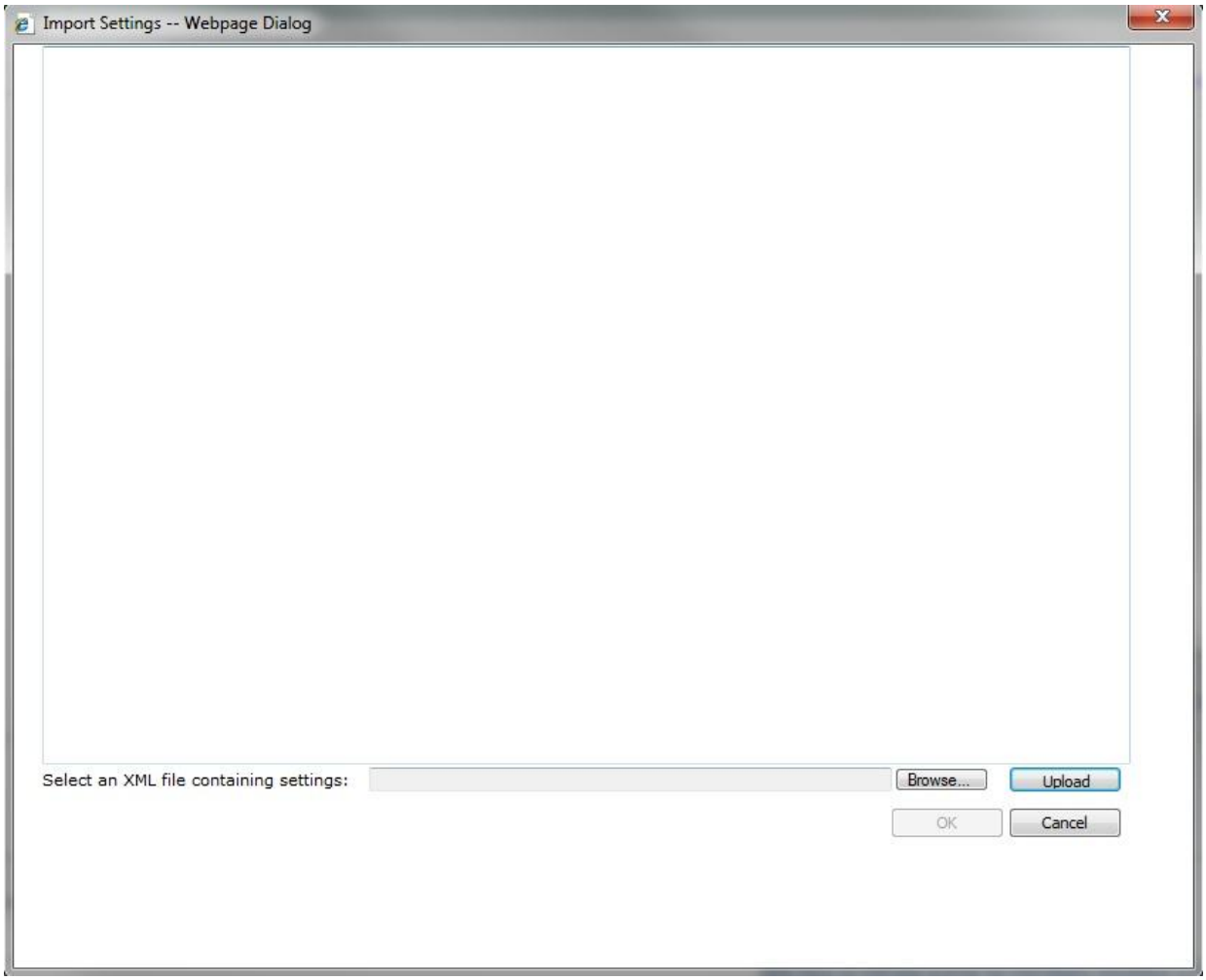
These settings have been newly introduced to Column View Permission. They give the administrator the option to configure notifications if views are unavailable to users. Check the "Use redirect page" to use this feature. If activated, any users without sufficient permissions will be directed to a page presenting him with the following options.

There are four messages that can be configured. However, for each message a default message is preset. So activating this feature does not require to enter any messages, if the default messages meet the requirements of the administrator.

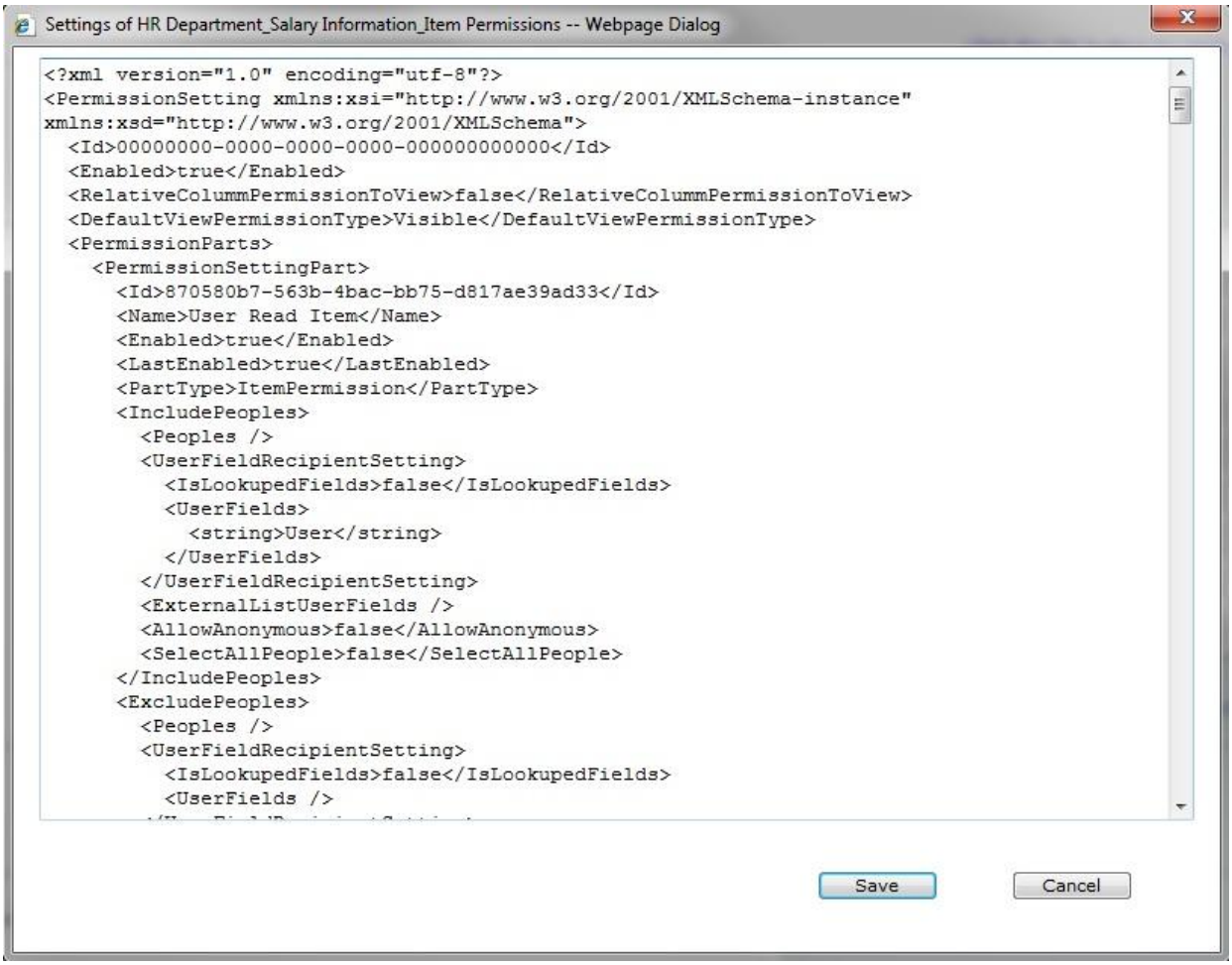
1. The "View unavailable message": This message will be displayed if the user does not have sufficient permissions to access the view selected.
2. The "All views unavailable message": This message will be displayed if the user does not have sufficient permissions to access any view for this list.
3. The "'Go to view' button text": This message will be displayed on the face of the 'Go to view' button, to direct the user to the next available view.
4. The "'Return to homepage' button text": This message will be displayed on the face of the 'Return to homepage' button to direct the user from this list.

Import/Export Permission Parts

The new version of Column View Permission allows for importing and exporting permission parts. This function is based on XML files. Thus, creating similar permissions for different sites will be easier and less time consuming.



To import settings click the Import button. A popup window will open. There the administrator can either paste the XML file contents into the designated area, or browse for a file and upload it. After uploading the file the contents will be displayed in the area above the upload area. To confirm importing the XML file click the OK button. To abort importing the specified permission settings, click the Cancel button.



To export permission settings click the Export button. A popup window will open and display the XML file contents in the edit area. The administrator can then save the settings to any location and thus make it reusable in other lists. To abort exporting the settings, click the Cancel button.

Permission Settings Name

Name each View Permission settings part. The settings part will be displayed with this name in the Permission Settings table in the main settings page for View Permission.

User/Group Selection Process

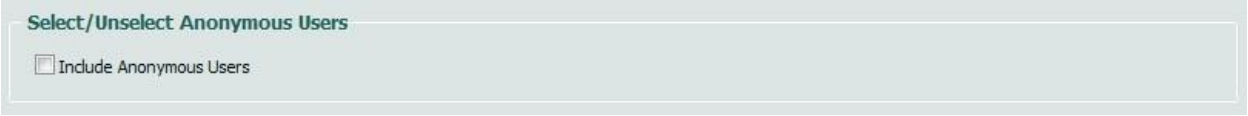
The User/Group selection process has been modified and improved compared to the previous version. One distinctive difference is that administrators are now able to specify in far more detail which users to include and which to exclude from the selection process. It also makes understanding the selection easier as both parts share the same interface.

The first selection lets the administrator decide if he wants to include all users, or if he wants to select a small group of users based on criteria that he specifies below.

Column View Permission now allows for specific selection of users and groups by filtering them by:

e) Including/excluding anonymous users
f) Input of user or group names
g) Looking up users from other lists and filter them based on conditions

e) Anonymous Users



This allows the administrator to include anonymous users in the permission settings.

An anonymous user is used for public access to your Web Site.

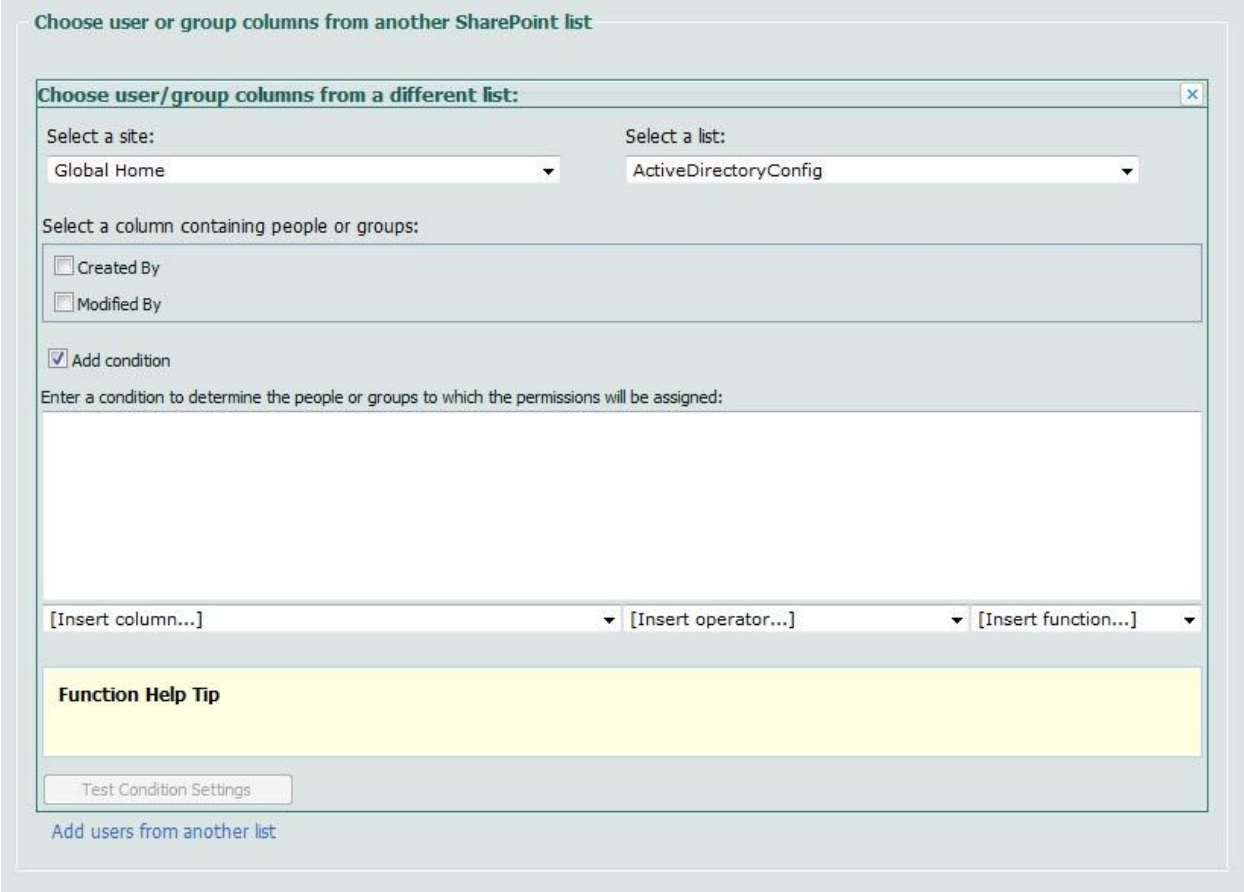
Anonymous access allows anyone to visit the public areas of your Web sites while preventing unauthorized users from gaining access to your Web server's critical administrative features and private information.

f) Input of user and group names

As in previous versions, Column View Permission provides a box to enter any user or group name. It also allows entering multiple users or groups, and as with the default user selection, the administrator can look up names or check the names entered into the box.

As in previous versions, Column View Permission provides checkboxes with all User/group columns available. Checking these checkboxes will result in selecting the users which are contained within the selected column. The administrator can also select related columns, if the checkbox to display them is checked. This means that all user/group columns in the list that is looked up from will be available for selection.

g) Looking up users from other lists and filter them based on conditions



The process to select users from another list works in 3 steps:

4. Specify the list to look up from. To do so, the administrator has to firstly select the site on which the list is located. Note that only sites in the same site collection are available. All lists located on this site will be available for selection in another dropdown list.
5. Specify the User/Group columns that will be used to specify the users. These are to be selected through checkboxes, similar to the User/Group column selection in the original list. However, no related columns are available to select in this selection.

6. A final step is the ability to filter the users selected based on conditions.

Specify Selection Criteria Based on Conditions

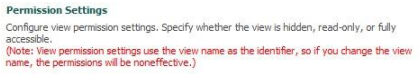
We have introduced conditions to specify user and items even more precise, and thus providing an even more granular approach. In View Permission conditions are used for filtering users/groups from other sites.

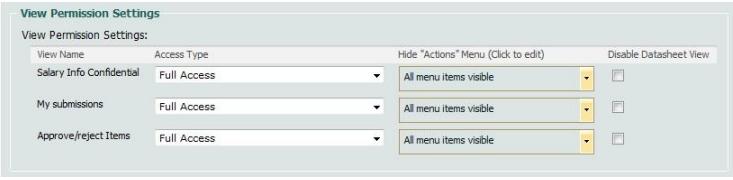
The process to select users from another list works in 3 steps:

1. Specify the list to look up from. To do so, the administrator has to firstly select the site on which the list is located. Then all lists located on this site will be available for selection in a dropdown list.
2. Specify the User/Group columns that will be used to specify the users. These are to be selected through checkboxes, similar to the User/Group column selection in the original list.
3. Filter the results by specifying conditions. The conditions allow building relationships between the User/Group columns and any other column existing in the list. This will effectively result in only selecting users who meet the conditions specified.

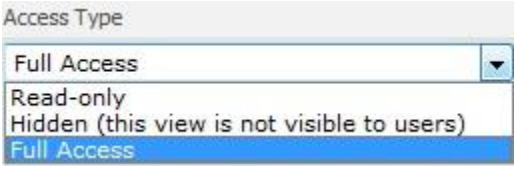
View Permission Settings

In the View Permission Settings the administrator can specify the permission level that the selected users will have for each of the views in a list.

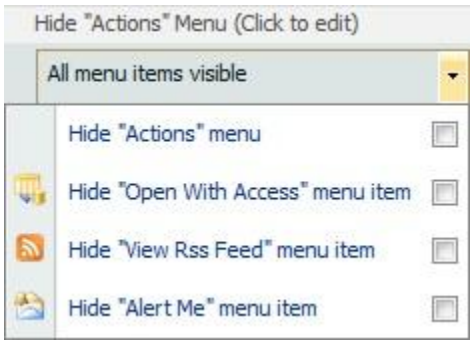




The Access Type defines whether the view should be fully accessible, read-only, or hidden for the selected users. The default for these settings can be changed in the Default View Permission Level settings (see above for further information).



The ‘Actions’ menu configures which options in the ‘Actions’ menu should be visible to the user. Selecting the first option (“Hide ‘Actions’ menu”) will make the whole Actions menu completely invisible in the view, and thus disable all the options available in it. The administrator can also specify single menu items to be hidden from users.



The Datasheet View can be disabled by checking the checkbox in the ‘Disable Datasheet View’ column for each view. This will not only make the Datasheet View ‘Actions’ menu item invisible, but will also disable the URL to access the Datasheet View.

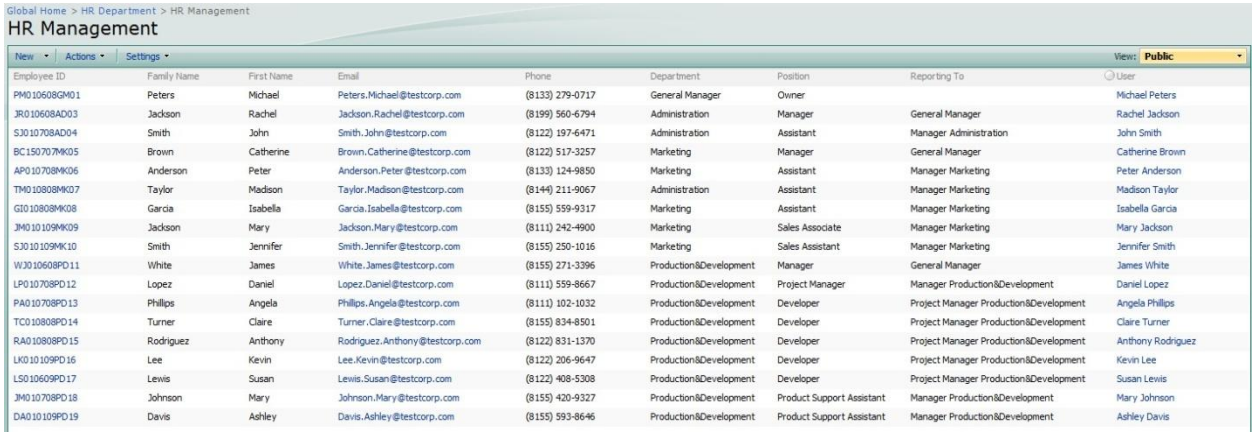
Example

In companies there is information that should only be accessible to certain people. So only staff in the Administration department has to be able to read and modify private information of employees. Other employees should not be able to access this kind of information. So information like address, social security number, etc should be hidden from any employee, except employees working for Administration.

Less sensitive information on the other hand like the department employees are working in, whom they are reporting to, etc is information that should be shared, however, it should only be read-only.

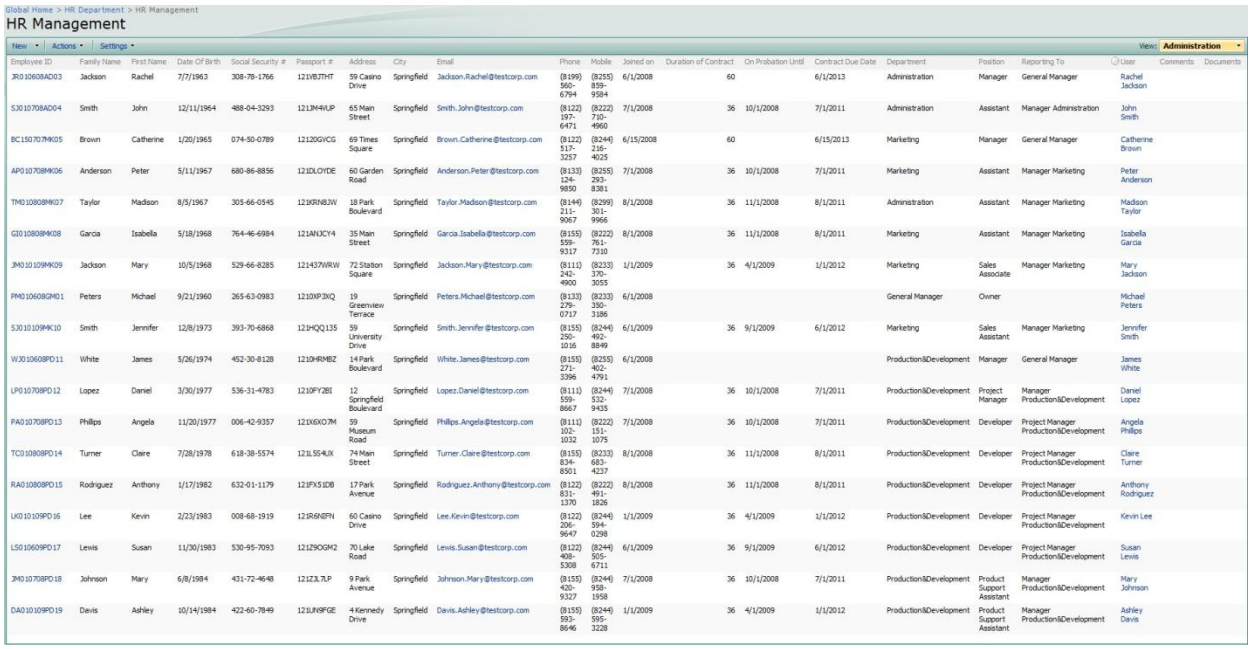
A way to achieve this goal is to define views that include the necessary information for its target audience, and then restrict the access level with SharePointBoost View Permission.

Firstly, create a view that should be accessible by all employees. This view is called "Public".

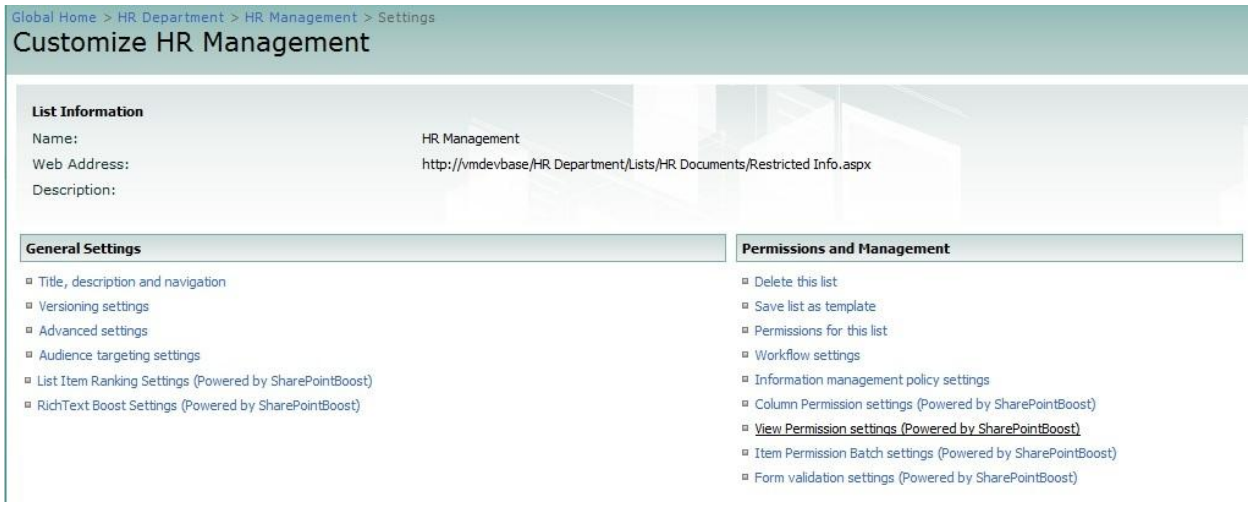


Employee ID	Family Name	First Name	Email	Phone	Department	Position	Reporting To	User
PM010608GM01	Peters	Michael	Peters.Michael@testcorp.com	(8133) 279-0717	General Manager	Owner		Michael Peters
JR010608AD03	Jackson	Rachel	Jackson.Rachel@testcorp.com	(8199) 560-6794	Administration	Manager	General Manager	Rachel Jackson
SJ010708AD04	Smith	John	Smith.John@testcorp.com	(8122) 197-6471	Administration	Assistant	Manager Administration	John Smith
BC150707MK05	Brown	Catherine	Brown.Catherine@testcorp.com	(8122) 517-3257	Marketing	Manager	General Manager	Catherine Brown
AP010708MK06	Anderson	Peter	Anderson.Peter@testcorp.com	(8133) 124-9850	Marketing	Assistant	Manager Marketing	Peter Anderson
TM010808MK07	Taylor	Madison	Taylor.Madison@testcorp.com	(8144) 211-9067	Administration	Assistant	Manager Marketing	Madison Taylor
GI010808MK08	Garcia	Isabella	Garcia.Isabella@testcorp.com	(8155) 559-9317	Marketing	Assistant	Manager Marketing	Isabella Garcia
JM010109MK09	Jackson	Mary	Jackson.Mary@testcorp.com	(8111) 242-4900	Marketing	Sales Associate	Manager Marketing	Mary Jackson
SJ010109MK10	Smith	Jennifer	Smith.Jennifer@testcorp.com	(8155) 250-1016	Marketing	Sales Assistant	Manager Marketing	Jennifer Smith
WJ010608PD11	White	James	White.James@testcorp.com	(8155) 271-3396	Production&Development	Manager	General Manager	James White
LP010708PD12	Lopez	Daniel	Lopez.Daniel@testcorp.com	(8111) 559-8667	Production&Development	Project Manager	Manager Production&Development	Daniel Lopez
PA010708PD13	Phillips	Angela	Phillips.Angela@testcorp.com	(8111) 102-1032	Production&Development	Developer	Project Manager Production&Development	Angela Phillips
TC010808PD14	Turner	Claire	Turner.Claire@testcorp.com	(8155) 834-8501	Production&Development	Developer	Project Manager Production&Development	Claire Turner
RA010808PD15	Rodriguez	Anthony	Rodriguez.Anthony@testcorp.com	(8122) 831-1370	Production&Development	Developer	Project Manager Production&Development	Anthony Rodriguez
LK010109PD16	Lee	Kevin	Lee.Kevin@testcorp.com	(8122) 206-9647	Production&Development	Developer	Project Manager Production&Development	Kevin Lee
LS010609PD17	Lewis	Susan	Lewis.Susan@testcorp.com	(8122) 408-5308	Production&Development	Developer	Project Manager Production&Development	Susan Lewis
JM010708PD18	Johnson	Mary	Johnson.Mary@testcorp.com	(8155) 420-9327	Production&Development	Product Support Assistant	Manager Production&Development	Mary Johnson
DA010109PD19	Davis	Ashley	Davis.Ashley@testcorp.com	(8155) 593-8646	Production&Development	Product Support Assistant	Manager Production&Development	Ashley Davis

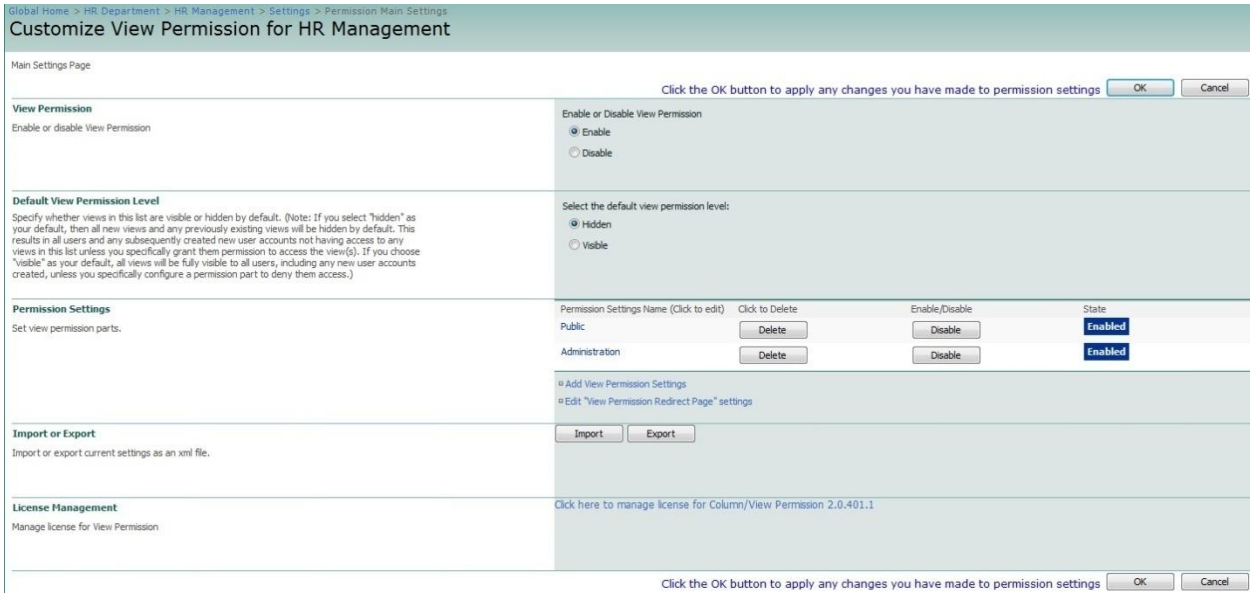
Also, create another view for administrative staff only; this one is the "Administrative" view.



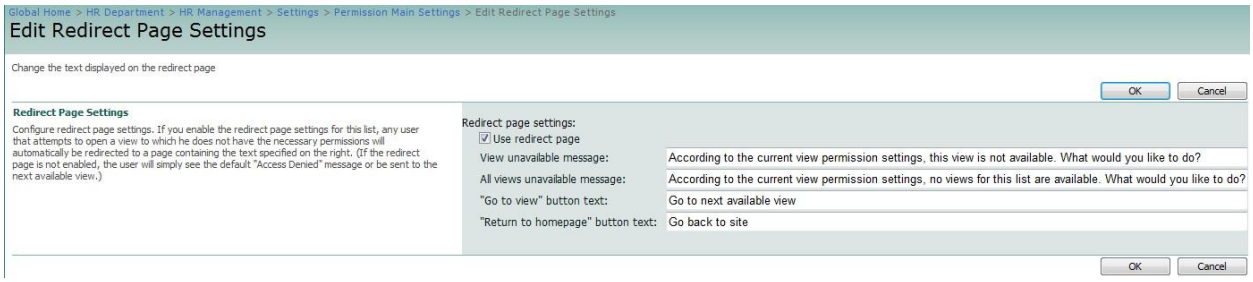
The Public View includes no sensitive information, while the Administrative view displays all fields of interest for the Administration Department. To set permissions for these views, navigate to the View Permission settings page.



In the List Settings page click on the View Permission link to be directed to the View Permission general settings page.



As this information in this list is confidential, the administrator wants the default set to be ‘Hidden’ for new users.

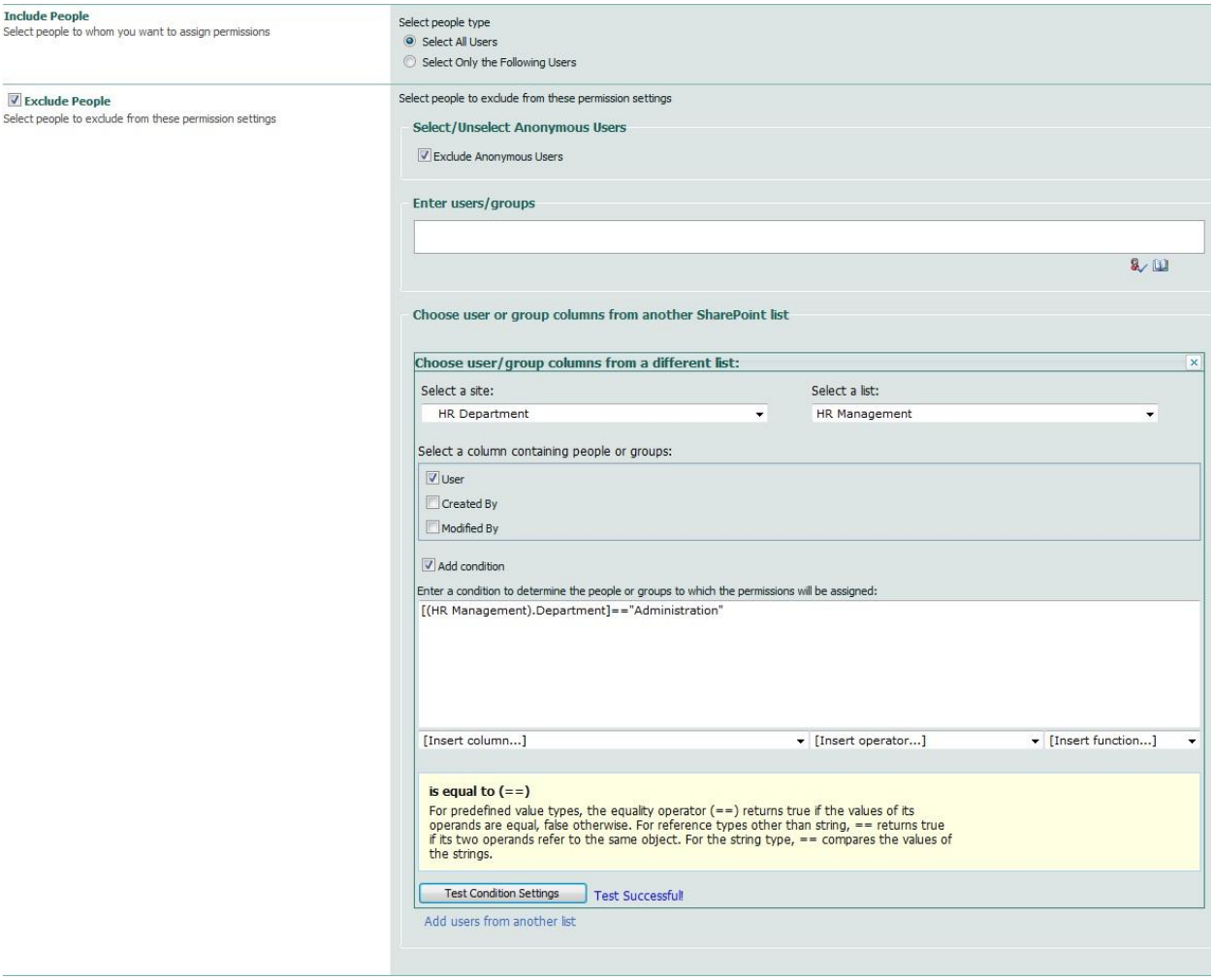


Also, the administrator has activated the Redirect Page; so that users are informed of their choices when they navigate to a view they do not have permissions to.

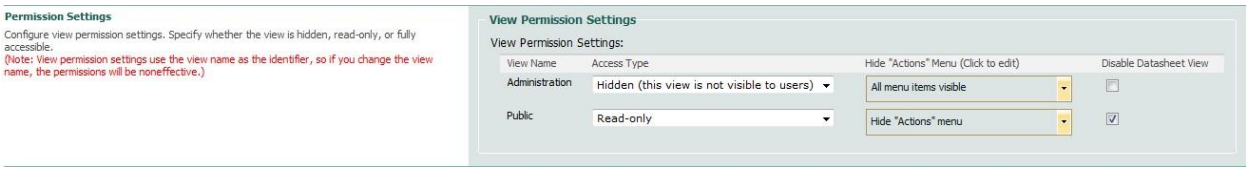
Then navigate back to the View Permission main settings page, and click “Add View Permission Settings”. The administrator creates a settings part that allows users access to the "Public" view, while denying access to other views that contain confidential information. This settings part is called ‘Public’.

Then the administrator has to specify which users will be affected by these view permission settings. As all employees should be able to access this view the administrator just selects the ‘Select all users’ radio button. As external parties should not be able to access this information at all, anonymous users are excluded by checking the Select/Deselect Anonymous Users checkbox. Also, as employees working in the "Administration" department should not be affected, they are excluded as well, using the following condition:

[(HR Management).Department]=="Administration"



Now the administrator has to select what views are available to the employees, and what permissions they have for these views.



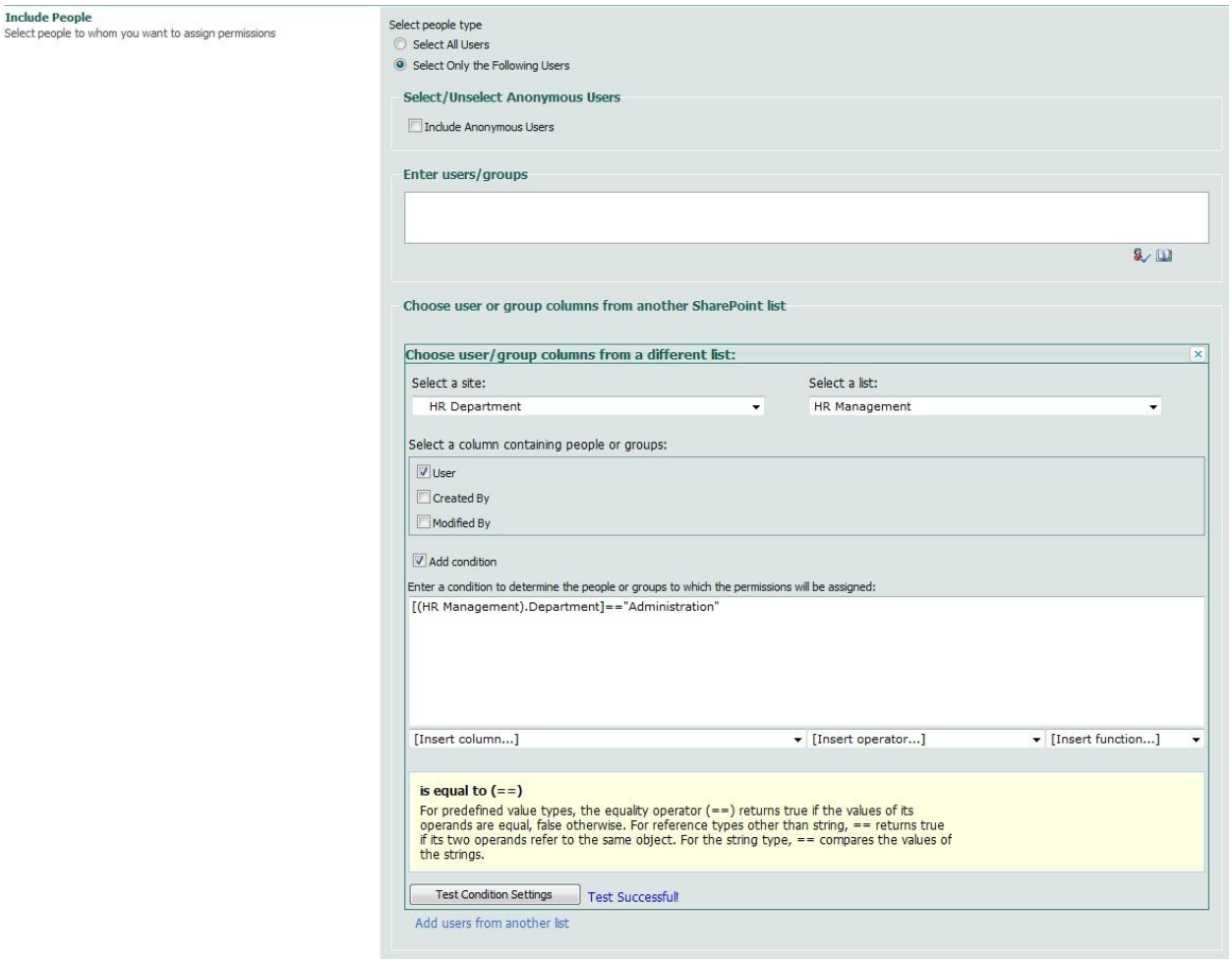
For the ‘Public’ view they should be able to see it, however they should not be able to make any changes, thus selecting read-only access is the right choice. To ensure that they are not able to access the information by exporting the list information, check the administrator can hide the Actions Menu completely. Also, by disabling the Datasheet View, he ensures that the employees cannot access the datasheet view at all, and thus won’t be able to access any information in the datasheet view.

All the other views should be hidden from the employees, thus the administrator just selects the ‘Hidden’ option in the Access Type menu.

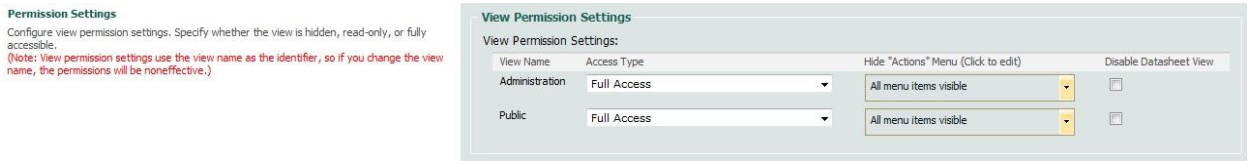
Now, the administrator still has to set up the view permissions for the Administration Department. Firstly, again create a new View Permissions settings part. Name it as ‘Administration’.

Then, select which users to include. To only select employees working in the Administration Department the administrator needs to specify the site and the list from which to look up. Here, this is the same as the existing list. Then specify the ‘User’ column as the column to pull users from. Following he needs to filter for employees in Administration department only. This he can achieve with this condition:

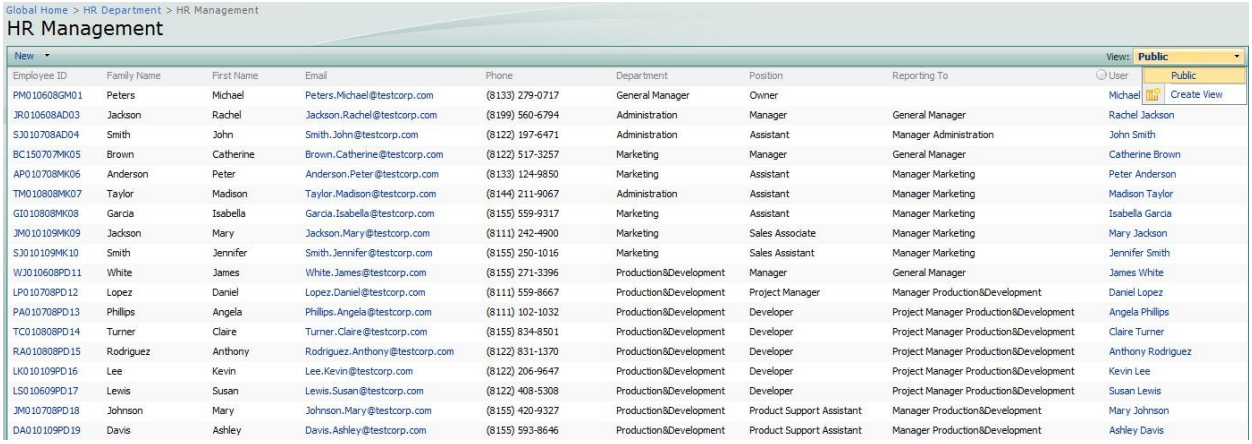
[(HR Management).Department]=="Administration"



Now, the administrator has to specify what access type the administration employees should have for each view. For all views they should have Full Access. So the administrator can just specify full access for all views. Also, the Actions menu and all its options should be visible, and the Datasheet View available.



Logging in as Anthony from the Production & Development department, only the ‘Public’ view is available. Also, the Actions menu is not being displayed.



Global Home > HR Department > HR Management

HR Management

New

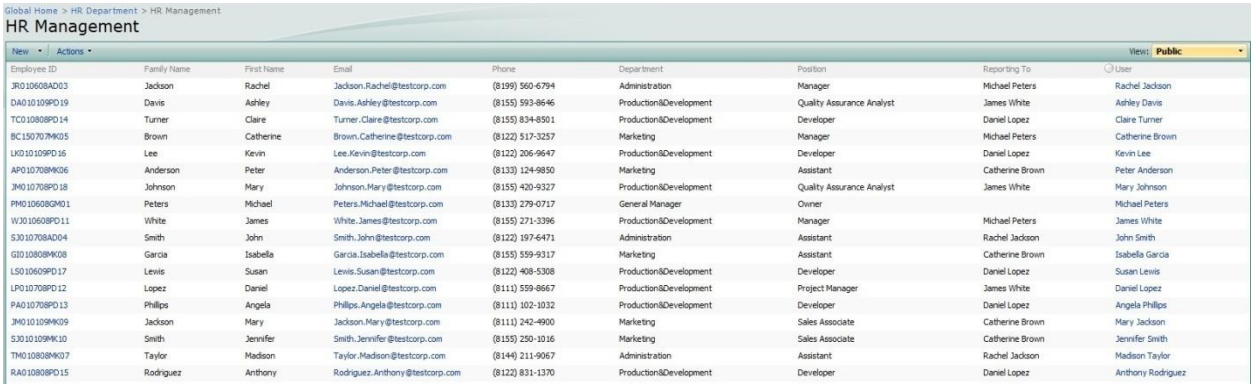
View: Public

Public

Create View

Employee ID	Family Name	First Name	Email	Phone	Department	Position	Reporting To	User
PM010608GM01	Peters	Michael	Peters.Michael@testcorp.com	(8133) 279-0717	General Manager	Owner		Michael
JR010608AD03	Jackson	Rachel	Jackson.Rachel@testcorp.com	(8199) 560-6794	Administration	Manager	General Manager	Rachel Jackson
SJ010708AD04	Smith	John	Smith.John@testcorp.com	(8122) 197-6471	Administration	Assistant	Manager Administration	John Smith
BC150707MK05	Brown	Catherine	Brown.Catherine@testcorp.com	(8122) 517-3257	Marketing	Manager	General Manager	Catherine Brown
AP010708MK06	Anderson	Peter	Anderson.Peter@testcorp.com	(8133) 124-9850	Marketing	Assistant	Manager Marketing	Peter Anderson
TM010808MK07	Taylor	Madison	Taylor.Madison@testcorp.com	(8144) 211-9067	Administration	Assistant	Manager Marketing	Madison Taylor
GI010808MK08	Garcia	Isabella	Garcia.Isabella@testcorp.com	(8155) 559-9317	Marketing	Assistant	Manager Marketing	Isabella Garcia
JM010109MK09	Jackson	Mary	Jackson.Mary@testcorp.com	(8111) 242-4900	Marketing	Sales Associate	Manager Marketing	Mary Jackson
SJ010109MK10	Smith	Jennifer	Smith.Jennifer@testcorp.com	(8155) 250-1016	Marketing	Sales Assistant	Manager Marketing	Jennifer Smith
WJ010608PD11	White	James	White.James@testcorp.com	(8155) 271-3396	Production&Development	Manager	General Manager	James White
LP010708PD12	Lopez	Daniel	Lopez.Daniel@testcorp.com	(8111) 559-8667	Production&Development	Project Manager	Manager Production&Development	Daniel Lopez
PA010708PD13	Phillips	Angela	Phillips.Angela@testcorp.com	(8111) 102-1032	Production&Development	Developer	Project Manager Production&Development	Angela Phillips
TC010808PD14	Turner	Claire	Turner.Claire@testcorp.com	(8155) 834-8501	Production&Development	Developer	Project Manager Production&Development	Claire Turner
RA010808PD15	Rodriguez	Anthony	Rodriguez.Anthony@testcorp.com	(8122) 831-1370	Production&Development	Developer	Project Manager Production&Development	Anthony Rodriguez
LK010109PD16	Lee	Kevin	Lee.Kevin@testcorp.com	(8122) 206-9647	Production&Development	Developer	Project Manager Production&Development	Kevin Lee
LS010609PD17	Lewis	Susan	Lewis.Susan@testcorp.com	(8122) 408-5308	Production&Development	Developer	Project Manager Production&Development	Susan Lewis
JM010708PD18	Johnson	Mary	Johnson.Mary@testcorp.com	(8155) 420-9327	Production&Development	Product Support Assistant	Manager Production&Development	Mary Johnson
DA010109PD19	Davis	Ashley	Davis.Ashley@testcorp.com	(8155) 593-8646	Production&Development	Product Support Assistant	Manager Production&Development	Ashley Davis

On the other hand, if John logs in, she can access all views and has permissions to change or add list entries.



Global Home > HR Department > HR Management

HR Management

New | Actions

View: Public

Employee ID	Family Name	First Name	Email	Phone	Department	Position	Reporting To	User
JR010608AD03	Jackson	Rachel	Jackson.Rachel@testcorp.com	(8199) 560-6794	Administration	Manager	Michael Peters	Rachel Jackson
DA010109PD19	Davis	Ashley	Davis.Ashley@testcorp.com	(8155) 593-8646	Production&Development	Quality Assurance Analyst	James White	Ashley Davis
TC010808PD14	Turner	Claire	Turner.Claire@testcorp.com	(8155) 834-8501	Production&Development	Developer	Daniel Lopez	Claire Turner
BC150707MK05	Brown	Catherine	Brown.Catherine@testcorp.com	(8122) 517-3257	Marketing	Manager	Michael Peters	Catherine Brown
LK010109PD16	Lee	Kevin	Lee.Kevin@testcorp.com	(8122) 206-9647	Production&Development	Developer	Daniel Lopez	Kevin Lee
AP010708MK06	Anderson	Peter	Anderson.Peter@testcorp.com	(8133) 124-9850	Marketing	Assistant	Catherine Brown	Peter Anderson
JM010708PD18	Johnson	Mary	Johnson.Mary@testcorp.com	(8155) 420-9327	Production&Development	Quality Assurance Analyst	James White	Mary Johnson
PM010608GM01	Peters	Michael	Peters.Michael@testcorp.com	(8133) 279-0717	General Manager	Owner		Michael Peters
WJ010608PD11	White	James	White.James@testcorp.com	(8155) 271-3396	Production&Development	Manager	Michael Peters	James White
SJ010708AD04	Smith	John	Smith.John@testcorp.com	(8122) 197-6471	Administration	Assistant	Rachel Jackson	John Smith
GI010808MK08	Garcia	Isabella	Garcia.Isabella@testcorp.com	(8155) 559-9317	Marketing	Assistant	Catherine Brown	Isabella Garcia
LS010609PD17	Lewis	Susan	Lewis.Susan@testcorp.com	(8122) 408-5308	Production&Development	Developer	Daniel Lopez	Susan Lewis
LP010708PD12	Lopez	Daniel	Lopez.Daniel@testcorp.com	(8111) 559-8667	Production&Development	Project Manager	James White	Daniel Lopez
PA010708PD13	Phillips	Angela	Phillips.Angela@testcorp.com	(8111) 102-1032	Production&Development	Developer	Daniel Lopez	Angela Phillips
JM010109MK09	Jackson	Mary	Jackson.Mary@testcorp.com	(8111) 242-4900	Marketing	Sales Associate	Catherine Brown	Mary Jackson
SJ010109MK10	Smith	Jennifer	Smith.Jennifer@testcorp.com	(8155) 250-1016	Marketing	Sales Associate	Catherine Brown	Jennifer Smith
TM010808MK07	Taylor	Madison	Taylor.Madison@testcorp.com	(8144) 211-9067	Administration	Assistant	Rachel Jackson	Madison Taylor
RA010808PD15	Rodriguez	Anthony	Rodriguez.Anthony@testcorp.com	(8122) 831-1370	Production&Development	Developer	Daniel Lopez	Anthony Rodriguez