BARNOWL

Security and Permissions

Introduction

1. **Basic vs NT Authentication**
   - Setting Password Security
2. **Capturing System Users**
   - Manual Capture of Users
   - Importing Users
   - Synchronising LDAP with BarnOwl
3. **Creating User Groups**
4. **Assigning Permissions**
   - User Permissions
   - Group Permissions
   - Unit Permissions
   - Field Level Permissions

BARNOWL

Basic vs NT Authentication

- **Basic Authentication**
  - This method of authentication requires users to type in a username and password when logging into the system
- **NT Authentication**
  - This method of authentication uses the Windows or Network credentials, so users to do not need to specify a user name and password.

Password Security

- **If the Basic Authentication method is to be used, administrators are able to specify the following optional security settings:**
  - Min & max password length required
  - Password strength using point structure for weak, medium and strong passwords
  - Number of unique passwords before a password is allowed to be reused
  - Password expiration period
  - Conditions for suspended user accounts
  - Automatic log off timings

For more information, see Password Security

Capturing System Users

- Users can be manually captured in the **Server Manager Console (SMC)** application.
  (See Capturing a New User)

- Users can also be imported into BarnOwl by importing the active directory. A setting can be set to synchronize the active directory with BarnOwl.
  (See Importing the Active Directory)

Note:

A user account must be created for each user who will access BarnOwl. This includes access to the BarnOwl web interface, even if no license is required.

Importing Users

- In the **SMC** application the **LDAP Integrator** can be used to import Windows Active Directory users into BarnOwl

- Access the LDAP integrator by clicking on **SMC > File > LDAP Integrator**

- Users can also be imported into the system by means of the **Import Utility**. This method requires a **BarnOwl Template Spreadsheet** to be populated with all the relevant user details. A copy of this template can be generated in the Import Utility.

- Access the Import Utility by clicking on **SMC > File > Access Import Utility**, and opt to import users

Manual Capture of Users

- Users can be captured manually in the **SMC** application by clicking on the “**New**” button under **Security > Security Members > Users**

- Type in the required user information such as the user’s name, surname and email address and the account status. Upon completion click on the “**Save**” button

Synchronizing LDAP with BarnOwl

- BarnOwl can be set to be kept in sync with the LDAP directory.
  - This means that if a new user is created in the active directory, the user will automatically be pulled through to BarnOwl.
  - If a user is deleted from the active directory, the user will not be deleted from BarnOwl, but will be marked as "Suspended".
- The system can also be set to automatically attempt to map manually captured users in BarnOwl to the LDAP directory based on the user's email address
- To specify system settings for the desired LDAP integration functionality, click on **SMC > Security > LDAP Integration**, and select the desired settings (See Synchronising Users with the Active Directory)

Creating User Groups in BarnOwl

- Groups of users can be captured to categorise users into their various functions. A user can belong to multiple groups.
- All the permissions that can be set on a user level can be set on a group level. This is the preferred method of managing user permissions.

(See Capturing a New User Group)

Creating User Groups in BarnOwl

- To create a new user group, go to **SMC > Security > Security Members > Groups.**

- Click on the “**New**” button located on the top part of the screen.

- In the “**Group**” capture screen, type in a title, code and description for the new user group, then click “**Save**”.

Assigning Permissions

- Specific permissions can be assigned to users of the system.

- Permissions can be set for users and groups. User permissions take preference over group permissions. It is therefore recommended that if a user is allocated to a group, the security properties tab is left blank on the user profile, as these settings will override the group settings.

- Setting the security properties in the Server Management Console is equivalent to setting the user permissions at the "Root" level of the organizational structure. This means that the settings are applied to all units across the organizational structure. It is recommended that if you have unit level security (for example, users can be restricted to certain unit's data), that these settings are set up at individual units on the Organisational Structure tree rather than in the Server Management Console.

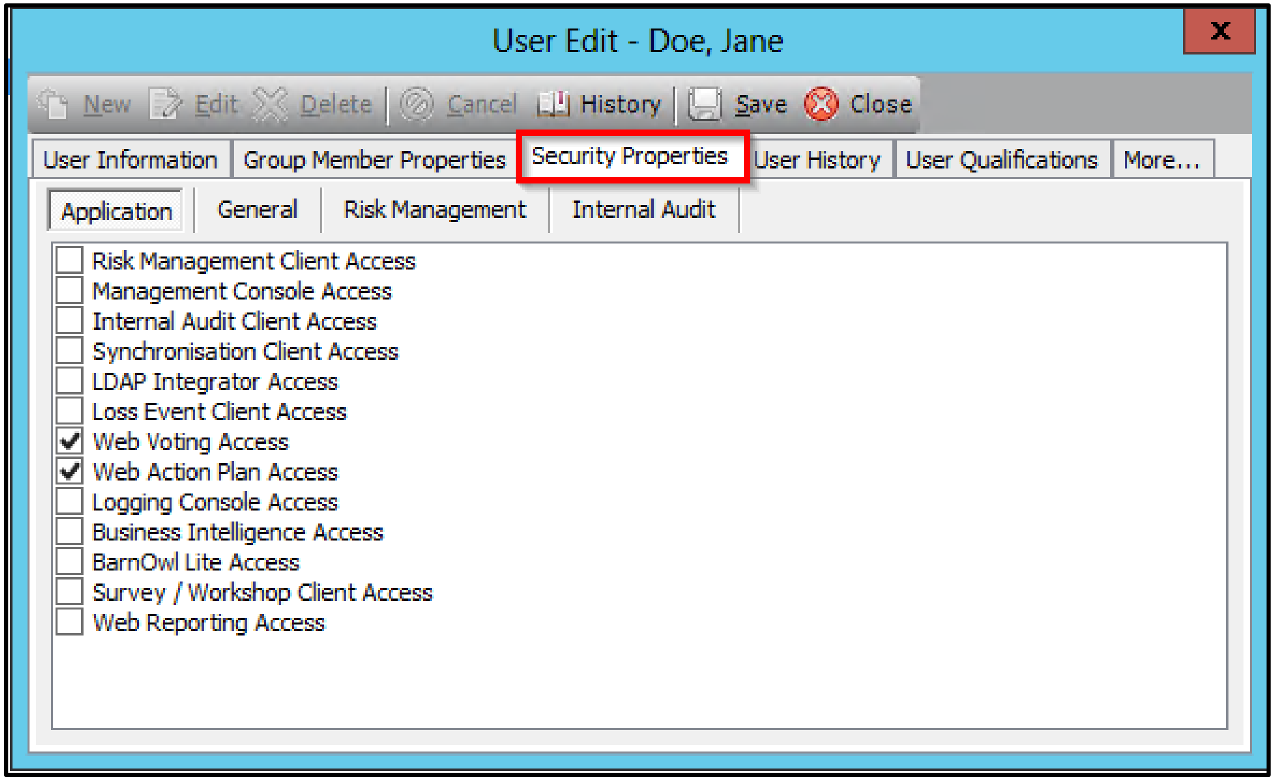
User Permissions

- To set permissions on the user profile, go to **SMC > Security > Security Members > Users**
- Double click on the user profile you wish to set permissions on and click on the **Security Properties** tab

(See Editing an Existing User)

User Permissions

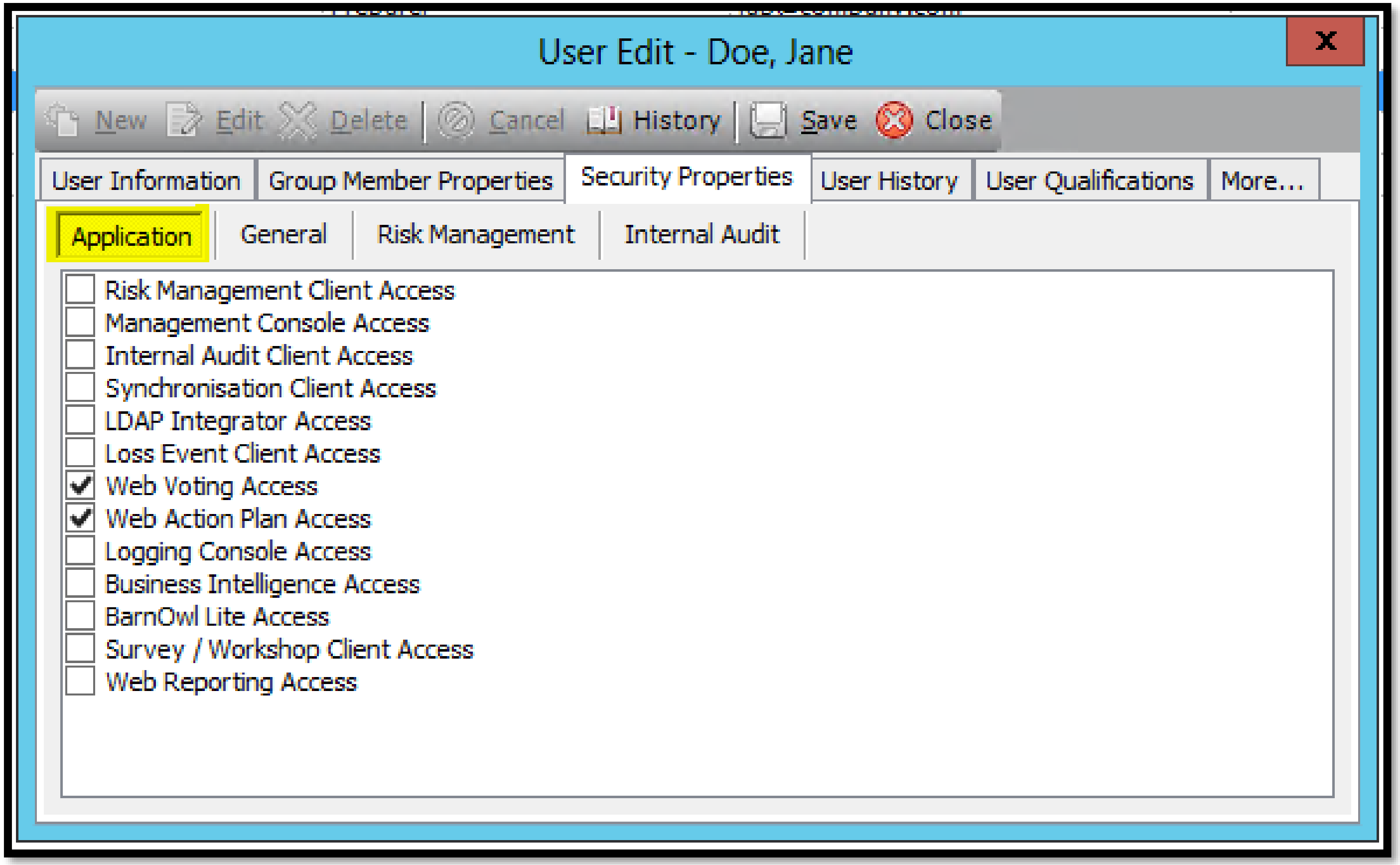
- Double click on the user profile you wish to set permissions on and click on the **Security Properties** tab



☐ Risk Management Client Access
☐ Management Console Access
☐ Internal Audit Client Access
☐ Synchronisation Client Access
☐ LDAP Integrator Access
☐ Loss Event Client Access
☑ Web Voting Access
☑ Web Action Plan Access
☐ Logging Console Access
☐ Business Intelligence Access
☐ BarnOwl Lite Access
☐ Survey / Workshop Client Access
☐ Web Reporting Access

Application Permissions

- The permissions specified here apply to application permissions.(See Application Permissions)



☐ Risk Management Client Access
☐ Management Console Access
☐ Internal Audit Client Access
☐ Synchronisation Client Access
☐ LDAP Integrator Access
☐ Loss Event Client Access
☑ Web Voting Access
☑ Web Action Plan Access
☐ Logging Console Access
☐ Business Intelligence Access
☐ BarnOwl Lite Access
☐ Survey / Workshop Client Access
☐ Web Reporting Access

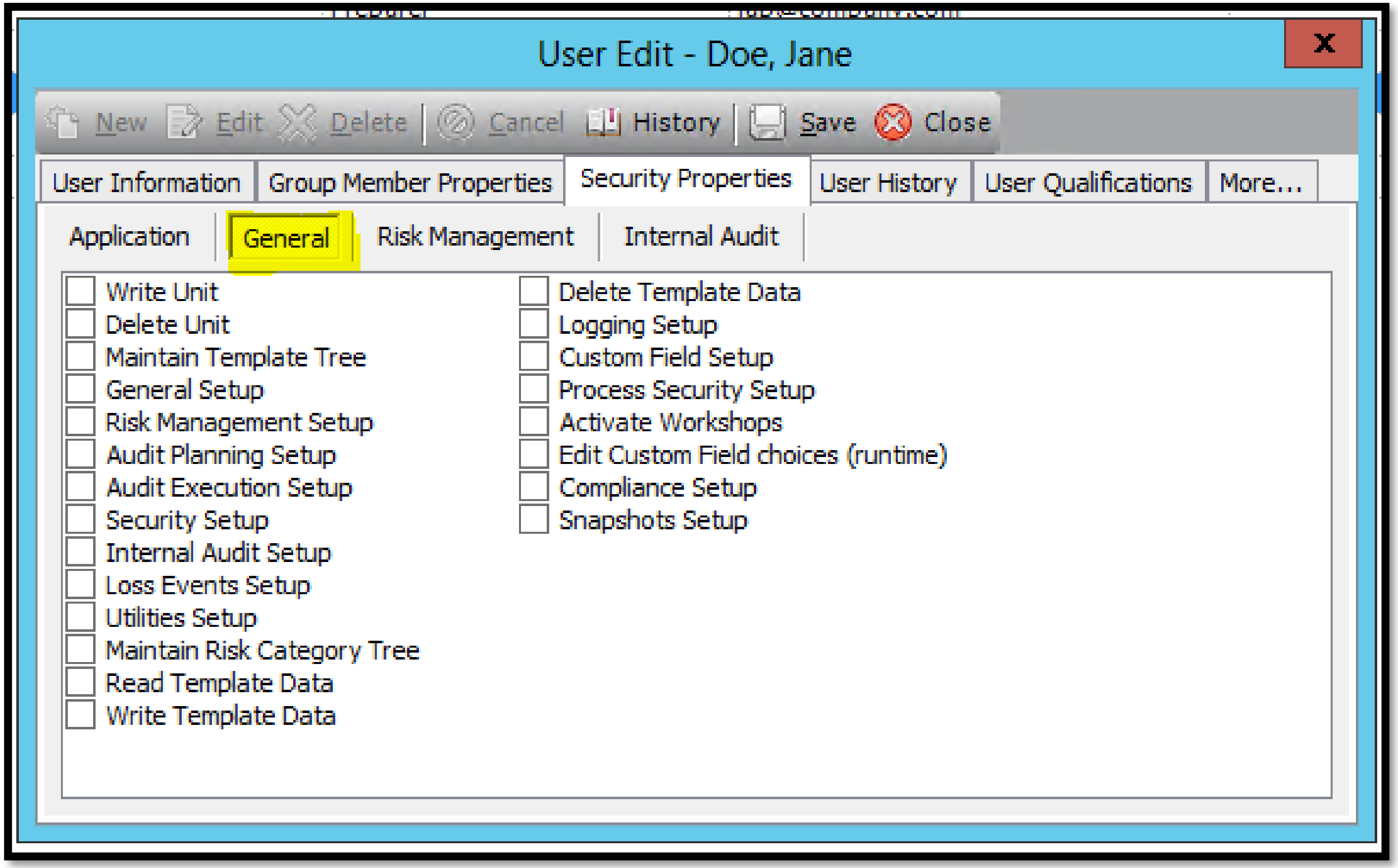
Application Permissions

- This table provides an overview of what each permission allows a user to access:

Permission	Description
Risk Management Client Access	Allows users to access the Risk Management client.
Management Console Access	Allows users to access the Server Management Console.
Internal Audit Client Access	Allows users to access the Internal Audit client
Synchronisation Client Access	Allows users to access the Synchronisation client.
LDAP Integrator Access	Allows users to access the LDAP Integrator client.
Loss Event Client Access	Allows users to access the loss event client. This feature is obsolete, and this permission will have no impact on the BarnOwl system.
Web Voting Access	Allows users to access the web voting.
Web Action Plan Access	Allows users to access the web action plan.
Logging Console Access	Allows users to the logging console
Business Intelligence Access	Allows users to access the BarnOwl Business Intelligence section where the user can populate the BI Warehouse
BarnOwl Lite Access	Allows user to access the web based BarnOwl Lite Module
Surveys Client Access	Allows user to access the Surveys Client

General Permissions

- The permissions specified here apply to general permissions (system permissions) (See General Permissions)



□ Write Unit
□ Delete Unit
□ Maintain Template Tree
□ General Setup
□ Risk Management Setup
□ Audit Planning Setup
□ Audit Execution Setup
□ Security Setup
□ Internal Audit Setup
□ Loss Events Setup
□ Utilities Setup
□ Maintain Risk Category Tree
□ Read Template Data
□ Write Template Data
□ Delete Template Data
□ Logging Setup
□ Custom Field Setup
□ Process Security Setup
□ Activate Workshops
□ Edit Custom Field choices (runtime)
□ Compliance Setup
□ Snapshots Setup

General Permissions

- This group of permissions applies to overall permissions and access:

Permission	**Description**
Write Unit	A user with "Write Unit" permissions is able to capture or edit any unit across the organizational structure in Risk Management. You can also specify Write Unit at unit permission level.
Delete Unit	A user with "Delete Unit" permissions is able delete any unit across the organizational structure in Risk Management. Write and Delete permissions for specific units can be set at Unit level.
Maintain Template Tree	Enables a user with this permission to access and view the Template tree.
General Setup	A user with "General Setup" is able to access the General Setup tab from within the Server Console. A user must have this permission in order to view this tab. This permission also grants the user permission to run the System User Report from within the server console
Risk Management Setup	A user with "Risk Management Setup" is able to access the Risk Management tab from within the Server Console. A user must have this permission in order to view this tab.
Audit Planning Setup	This permission has been replaced by the "Internal Audit Setup" permission as indicated below.

General Permissions

Permission	Description
Audit Execution Setup	This permission has been replaced by the “Internal Audit Setup” permission as indicated below.
Security Setup	A user with “Security Setup” is able to access the Security tab from within the Server Console. A user must have this permission in order to view this tab. The user will be able to add and delete users as well as add / delete groups and add members to groups. However, unless the user is an administrator, he/she will not be able to add another user to the administrators group. Users also require this permission to view the BarnOwl user reports in the sever console.
Internal Audit Setup	A user with “Internal Audit Setup” is able to access the Internal Audit tab from within the Server Console. A user must have this permission in order to view this tab.
Loss Events Setup	A user with “Loss Events Setup” is able to access the Loss Event tab from within the Server Console. A user must have this permission in order to view this tab.
Utilities Setup	A user with “Utilities Setup” is able to access the Utilities tab from within the Server Console. A user must have this permission in order to view this tab.
Maintain Risk Category Tree	In order for a user to access the Risk Category panel from within Risk Management, he/she must have this permission. If the user does not have this permission they may not access this panel.

General Permissions

Permission	Description
Read Template Data	The read template data permission allows users to read data in the template tree. Users that do not have template read permissions will not be able to view data in the template tree. The user will also need the ‘Maintain Template Tree’ (General permissions as per section 3.2) permissions to access the template tree.
Write Template Data	The write template data permission allows users to capture and edit template data. This permission also allows users to apply templates. Users need write permissions to the unit they wish to apply the template to. Users will also need ‘Maintain Template Tree’ permission to access the template tree.
Delete Template Data	The delete template data permission allows users to delete template data. This permission also allows users to delete templates. Users will also need ‘Maintain Template Tree’ (General permissions as per section 3.2) permission to access the template tree.
Logging setup	The logging setup permission allows a user to set up the logging.
Custom Field Setup	The Custom Field Setup permission allows a user to set up custom fields for BarnOwl objects
Process Security Setup	The process security setup permission allows a user to set up process security for other users in BarnOwl

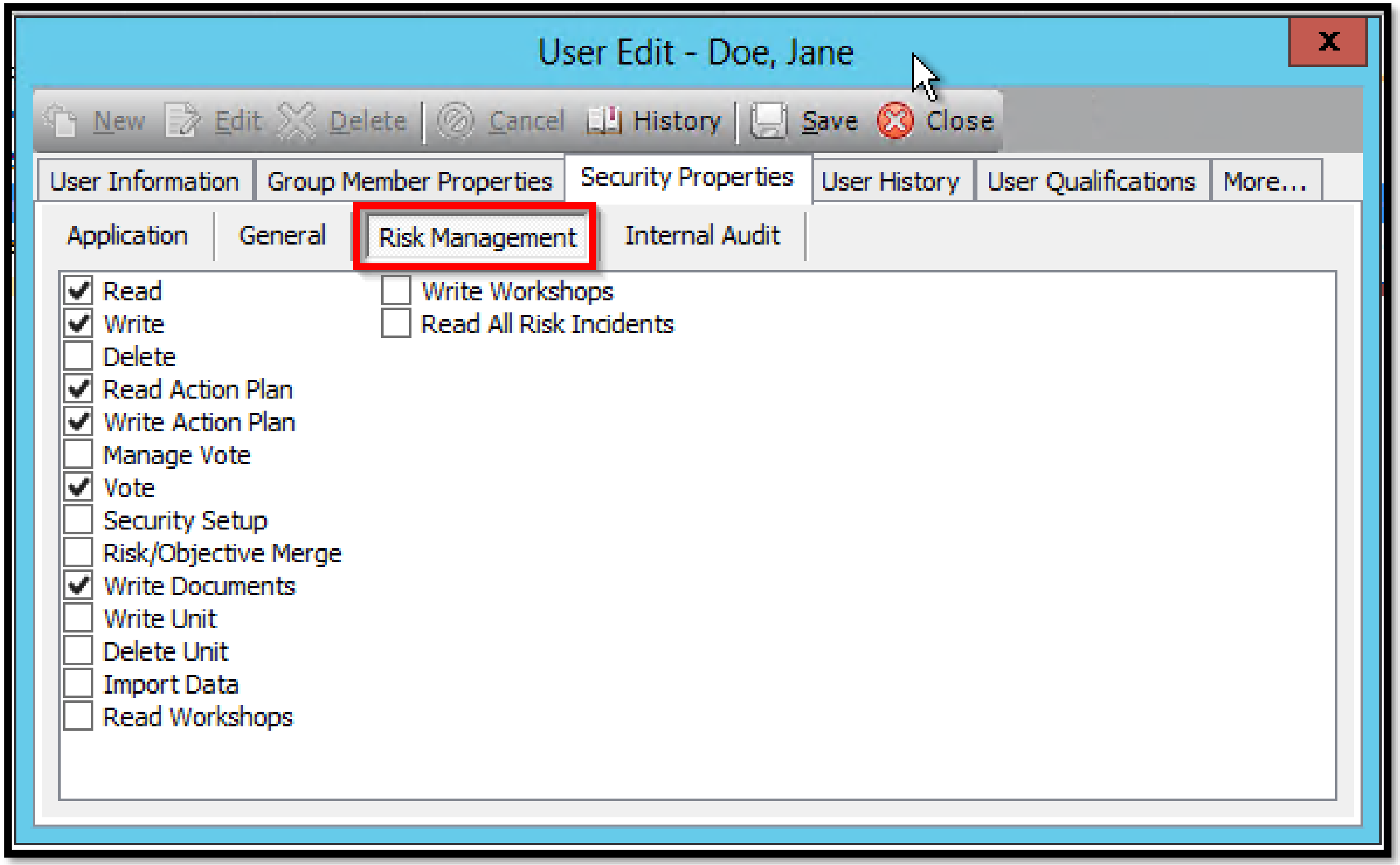
General Permissions

Permission	Description
Activate Workshops	The activate workshop permission allows a user to activate a workshop, deducting a license off the license key (unless the client has purchased unlimited licenses)
Edit Custom Field Choices (runtime)	This permission allows a user to right click on a custom field which has choices (i.e. a combo box or a list view custom field) and modify the choices at time of capture, from within the BarnOwl desktop (“rich”) application.
Compliance Setup	The Compliance Setup permission allows a user to set up compliance settings

Risk Management Permissions

- The permissions specified here apply to the Risk Management functions.

(See Risk Management Permissions)



☑ Read
☑ Write
☐ Delete
☑ Read Action Plan
☑ Write Action Plan
☐ Manage Vote
☑ Vote
☐ Security Setup
☐ Risk/Objective Merge
☑ Write Documents
☐ Write Unit
☐ Delete Unit
☐ Import Data
☐ Read Workshops
☐ Write Workshops
☐ Read All Risk Incidents

Risk Management Permissions

- This table provides an overview of the Risk Management permissions:

Permission	**Description**
Read	Read permissions allow the user to read data from units. Read permissions allow the user to read all Risk Management objects. User will be able to open registers to view data and on double clicking objects will be able view them in read only view.
Write	Write permissions allow a user to save and edit data. The user will be able to make use of the capture menus and save objects.
Delete	Delete permissions will allow users to delete items from within the Organisational Structure and the Template tree. Users need “read” permissions as well in order to view and access the data before deleting it.

Risk Management Permissions

Permission	Description
Read Action Plan	Users with limited access may be required to view and update their action plans in restricted units. The read action plan permissions will allow users to view details of action plans on units where they have this permission; they will not be able to see any other detail. Should a user have read permissions, these will override read action plan permissions. However, If a user does not have read permissions, read action plan permissions will allow them to read only action plans. A user requires either read action plan or read permissions to be able to access the action plan reports. These users will also be able to view action plans via the web action plan interface.
Write Action Plan	These permissions work in the same way as the read action plan permissions, though they allow users to edit and create new action plans. A user capturing action plans will only be able to capture action plans to the Units since they do not have view rights to any other Risk Management object.

Risk Management Permissions

Permission	Description
Manage Vote	Users will need Manage Vote permissions to be able to create and maintain voting templates. These users would be designated as “vote administrators” and would create and manage voting sessions. They would change voting templates statuses and push the vote results into BarnOwl.
Vote	Users with vote permissions will be able to vote on voting templates via the Voting Website. These users may not have access to the client application access and voting would be their only interaction with BarnOwl.
Security Setup	Security Setup permissions allow users to alter unit security for units on which they have these permissions. Users that have General security setup permissions are allowed to alter unit security in any unit and therefore overwrite Risk Management Security Setup permissions. Users need General Security Setup to draw reports on BarnOwl User and BarnOwl group reports. This permission will not allow users access to these reports.
Risk Merge	Since risk merge is a very specific function, a permission has been created to prevent non-trained users from using it. The risk merge permission allows users to make use of the risk merge functionality in the Risk Register.

Risk Management Permissions

Permission	Description
Write Documents	The "Write Documents" permission will allow a user to attach a document to any item, even if the user does not have permission to edit the item they are attaching the document to.
Write Unit	A user with "Write Unit" permissions on the unit is able to capture any unit below the unit for which this permission is set. Note: If a user has been granted "General" Write/Delete Unit permissions, he will have permission to capture units anywhere on the Organisational Structure.
Delete Unit	A user with "Delete Unit" permissions is able delete any unit below the unit for which this permission is set. Note: If a user has been granted "General" Write/Delete Unit permissions, he will have permission to Delete units anywhere on the Organisational Structure.
Import Data	A user with "Import Data" permissions is able to import data from Excel (in a predefined format) into any unit where this permission has been set.

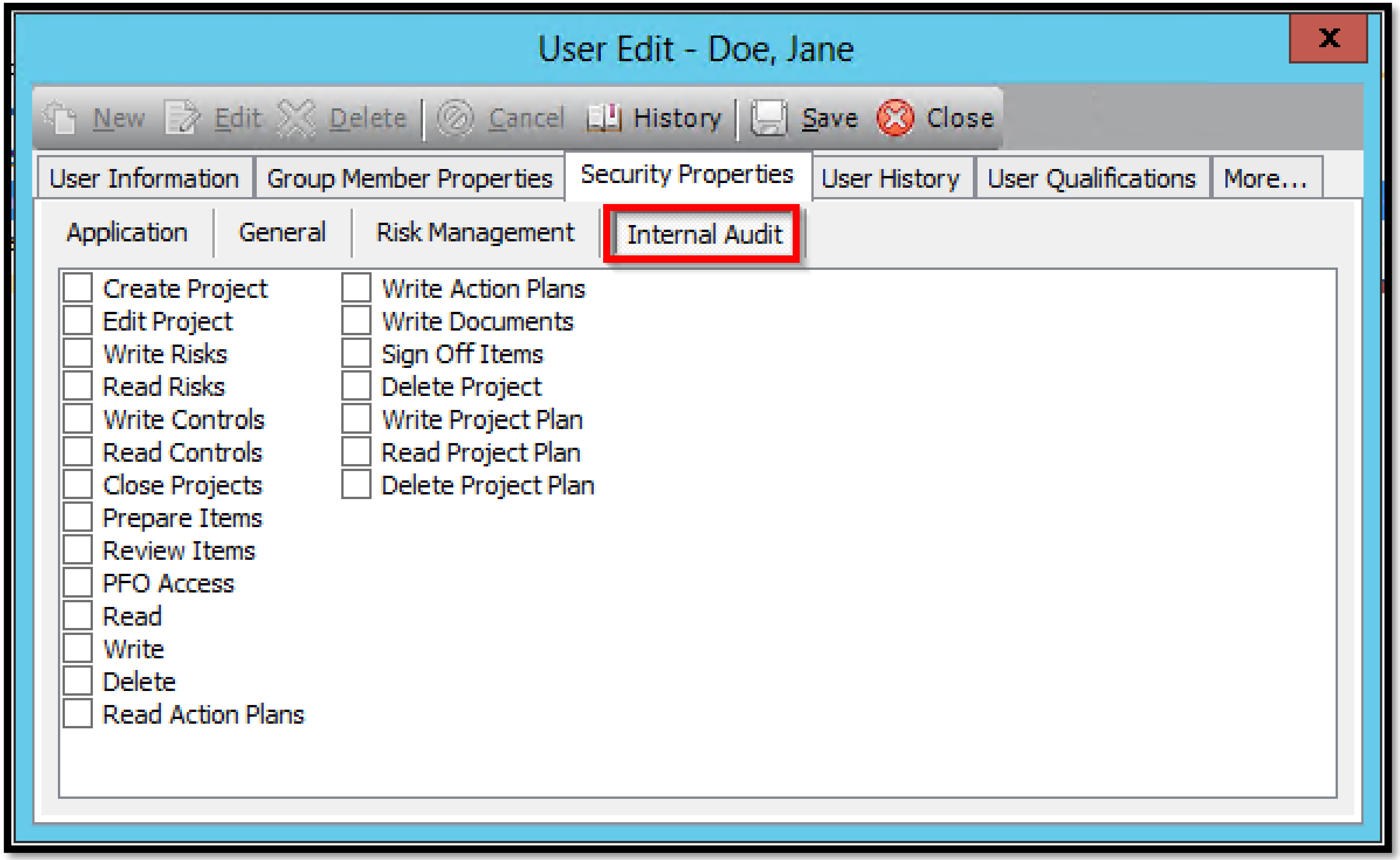
Risk Management Permissions

Permission	**Description**
Read Workshops	Users with limited access may be required to still view and update their workshops in restricted units. The read workshop permissions will allow users to view details of workshops on units where they have this permission; they will not be able to see any other detail. Should a user have read permissions these will override read workshop permissions. Though should a user not have read permissions, read workshop permissions will allow them to read only workshops.
Write Workshops	These permissions work in the same way as the read workshop permissions, though they allow users to edit and create new workshops. A user capturing workshops will only be able to capture workshops to the Units since they do not have view rights to any other Risk Management object.
Read All Risk Incidents	By default, users can only view risk incidents to which they are an allocated user (owner or originator). When this permission is granted, a user can view all risk incidents.

Audit Permissions

- The permissions specified here apply to Audit functions.

(See Audit Permissions)



□ Create Project
□ Edit Project
□ Write Risks
□ Read Risks
□ Write Controls
□ Read Controls
□ Close Projects
□ Prepare Items
□ Review Items
□ PFO Access
□ Read
□ Write
□ Delete
□ Read Action Plans
□ Write Action Plans
□ Write Documents
□ Sign Off Items
□ Delete Project
□ Write Project Plan
□ Read Project Plan
□ Delete Project Plan

Audit Permissions

- This table provides an overview of the different permissions and their functions:

Permission	Description
Create Project	A user with “Create Project” permissions is able to create an Internal Audit project for the unit which this permission is granted to.
Edit Project	A user with “Edit Project” permissions is able to edit the following items from within Internal Audit: •Anything from within the Project detail Figure •Actual Hours •Tasks •Resources •Resource Allocation •Assign status flag/resource on Risk/Control/Recommendation This user will also be able to delete the above items. In order to edit these items the user must have this permission granted to them, regardless of whether they have Write permissions.
Write Risks	A user with “Write Risks” is able to capture and edit risks from within Internal Audit. The user can capture/edit risks from both the Risk Register (providing they have Read permissions to view the register) and from the Capture menu. The “Write” permission overrides this permission. Therefore if a user does not have “Write Risks” permission but has “Write” permissions, they will be able to capture/edit risks.

Audit Permissions

Permission	Description
Read Risks	A user with “Read Risks” is able to view the risk register. The “Read” permission overrides this permission. Therefore if a user does not have “Read Risks” permission but has “Read” permissions, they will be able to view this register.
Write Controls	A user with “Write Controls” is able to capture and edit controls from within Internal Audit. The user can capture/edit controls from both the Control Register and Risk Register (providing they have Read permissions to view the registers) as well as from the Capture menu. This permission also allows you to capture/edit Audit Control Effectiveness and Audit Control Adequacy. The “Write” permission overrides this permission. Therefore if a user does not have “Write Controls” permission but has “Write” permissions, they will be able to capture/edit controls.
Read Controls	A user with “Read Controls” is able to view the control register. The “Read” permission overrides this permission. Therefore if a user does not have “Read Controls” permission but has “Read” permissions, they will be able to view this register.
Close Projects	A user must have the “Close Projects” permission in order to be able to close the project from the Capture -> Project Detail Figure.

Audit Permissions

Permission	Description
Prepare Items	A user with “Prepare Items” permission is able to make himself the preparer of an item. A user must have this permission regardless of their “write” permissions. This permission also allows the user to capture a Finding and Link findings. A user must have either “Prepare Items” or “Review Items” in order to capture/link findings.
Review Items	A user with “Review Items” permission is able to make himself the reviewer of an item. A user must have this permission regardless of their “write” permissions. This permission also allows the user to capture a Recommendation and Link recommendations. A user must have either “Prepare Items” or “Review Items” in order to capture/link recommendations.
PFO Access	A user must have this permission granted in order to access the Project File Organiser. This permission is required regardless of the “Read” permission. It is also required in order to view the Ordered PFO report.
Read	A user who is granted “Read” Permissions is able to view the Risk Register, Control Register, Action Plan register, Review Note Register and Recommendation register. This permission overrides the “Read Risks”, “Read Controls” and “Read Action Plans” permissions. A user with this permission is able to view all reports except for the PFO Report.

Audit Permissions

Permission	Description
Write	A user who is granted “Write” Permissions is able to capture and edit any of the following: •Risks •Controls •Audit Control Effectiveness •Audit Control Adequacy •Action Plans This permission overrides the “Write Risks”, “Write Controls” and “Write Action Plans” permissions.
Delete	A user with “Delete” Permissions is able to delete anything that they have write permissions for, except for the following items which require “Edit Project” permissions: •Anything from within the Project detail Figure •Actual Hours •Tasks •Resources •Resource Allocation •Assign status flag/resource on Risk/Control/Finding
Read Action Plans	A user with “Read Action Plans” is able to view the control register. The “Read” permission overrides this permission. Therefore if a user does not have “Read Action Plans” permission but has “Read” permissions, they will be able to view this register.

Audit Permissions

Permission	Description
Write Action Plans	A user with “Write Action Plans” permission is able to capture and edit action plans from within Internal Audit. The user can edit action plans from both the Action Plan Register and capture them from the Recommendation Register. The “Write” permission overrides this permission. Therefore if a user does not have “Write Action Plans” permission but has “Write” permissions, they will be able to capture/edit action plans.
Write Documents	The “Write Documents” permission will allow a user to attach a document to any item, even if the user does not have permission to edit the item they are attaching the document to.
Sign Off Items	A user with “Sign Off Items” permission is able to sign off an item. A user must have this permission regardless of their “write” permissions.
Delete Project	Permission to delete projects
Write Project Plan	Permission to create and edit project plans (Process security)
Read Project Plan	Permission to read project plans (Process security)
Delete Project Plan	Permission to delete project plans (Process security)

Group Permissions

- After you have created a group, you can assign users to the group, and set permissions for the group.

- To set permissions for a user group, go to **SMC > Security > Security Members > Groups**

- Double click on the user group you wish to set permissions on and click on the **Security** tab

(See Editing an Existing Group)

Unit Permissions

- All permissions set in the Server Management Console are applied to all units across the organizational structure. If you require unit-specific permissions, those permissions need to be setup on individual units on the organizational structure rather than in the Server Management Console.

- Unit security overrules a user’s specific permissions, which enables you to protect sensitive unit information from specific units or unit groups, allowing only the authorized users to access that unit.

- To set unit security permissions, right-click on a unit in the organizational structure, and from the menu that appears, select “**Unit Security**”.

(See Unit Security)

Unit Permissions

- To set unit security permissions, right-click on a unit in the organizational structure, and from the menu that appears, select “**Unit Security**”

- Select the user or user group for which you wish to set unit permissions in the Group or Username section.

- Select or deselect each permission as required, and then click on the “**Save and Close**” button

Field Level Permissions

- Field level permissions are used to restrict certain fields to certain user types
- Field level permissions can be set up on **Risks, Action Plans** and **Risk Incidents** in BarnOwl
- Permissions to change certain fields are setup in the **Server Management Console** and are configured depending on a user's **owner type**

(See Field Level Permissions)

Field Level Permissions

- You need to set access for every field, including the owners tab and the “**More**” section for custom fields. By default, nobody will be able to edit a field until the permissions are set.
- You need to go through every screen type (all Risk Incidents, Risks, and Action Plans) and set up permissions if Field Level Permissions is enabled, otherwise all these fields will be locked.
- The originator will be able to edit all fields regardless of their owner type.

Field Level Permissions

- To restrict the fields which certain users can edit:
  - In the Server Management Console, open General Setup and select the Field Level Permissions node.
  - Select the “**Enable Field Level Permissions in BarnOwl**” checkbox
  - Click the “**Save**” button.
  - Select which item to set field lever permissions on, and then click “**Setup field level permissions**”. This will open the item’s capture screen with lock icons next to each field.
  - For each field, click on the lock icon. This will open a panel on the right hand side of the screen, showing all the available user types.
  - Select the owner type of the owner’s who are permitted to edit this field.
  - Click the green button to accept or the red icon to cancel.
  - Repeat for each field as required.
  - Click the “**Save**” and “**Close**” button.

(For more information, see Field Level Permissions)

Any Questions?

Go to www.barnowl.co.za/support/documentation for the latest version of the Online Help

BARNOWL