Microsoft Dynamics® AX 2009

Understanding Security in Microsoft Dynamics AX 2009

White Paper

Microsoft Dynamics AX 2009 Security includes user authentication, permissions within the application, and may also include security in other applications that interact with AX. While all of these are important, permissions within the application is the primary focus of this document.

Date: September, 2009

Table of Contents

Introduction

Microsoft Dynamics AX 2009 provides three methods for controlling access to features within the AX client. These include: license keys, configuration keys, and security keys. These methods each control a different range of items, from an entire feature set to something as specific as a field on a form.
Another available security option in Microsoft Dynamics AX 2009 is Record Level Security. This allows for data restriction and allows an administrator to control which records are displayed to members of each user group.
Before getting into the configuration of Microsoft Dynamics AX 2009 security, it is best to understand the purpose of each control method and how to manage each. The intent of this document is to provide an understanding of how the granting of permissions within the security framework takes place and how to find the necessary keys related to permissions needed for working with a specific object.

User Groups

Permissions are granted to user groups and not directly to a user. Each AX user is a member of one or more user groups. Users inherit permissions from the groups they belong to. If a user belongs to more than one group, the least restrictive permissions will be allowed for the user.
For example, Group1 has 'view' access to the Sales Order form. Group2 has 'create' access to the Sales Order form. If a user belongs to both Group1 and Group2, they would be granted the 'create' access because it is the least restrictive level of access set in the groups they belong to.

The Admin User and Administrators Group

There is one super user account, which has unrestricted rights to everything within the application. This is the Admin account. The user that performs the installation will automatically be set as the Admin user, but this can be changed.
The Administrators group is very similar to the Admin user. This group also has unrestricted access to all objects within the application. Adding users to the Administrators group makes them almost the same as the Admin user. The only difference is that permissions cannot be revoked from the Admin account, while users can be removed from the Administrator group.
Note that the permissions of the Admin user and Administrators group cannot be changed within the AX application. These users automatically have the maximum allowed access to every object, so it is also important to note that the maximum allowed access could restrict these users to a level of control lower than 'Full Control.'

Domains

In Microsoft Dynamics AX 2009, domains represent a company or collection of companies. These can then be used to grant permissions specifically on the companies that belong to the domain. By default one domain exists, which is the Admin domain. The Admin domain

includes all company accounts. Using domains gives administrators the ability to give a group of users a different set of permissions in different companies.

User Authentication

In Axapta 3.0 usernames, passwords, and user information were stored in the Axapta database. When a user launched the Axapta client, they were prompted for a username and password. Axapta then authenticated the provided credentials against those stored in its database.

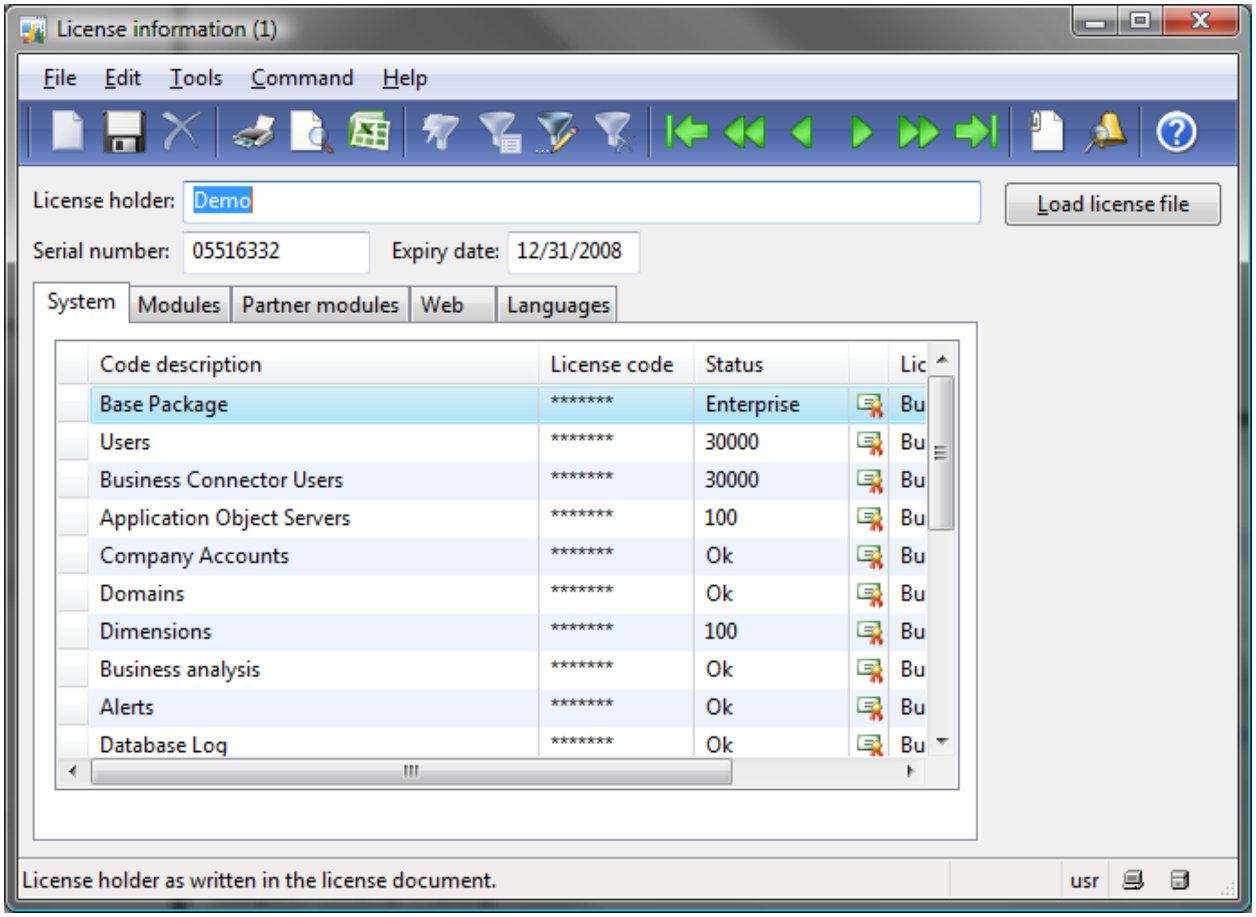
In Microsoft Dynamics AX 4.0 and later, users are authenticated against Active Directory. Information about Active Directory users is stored in the UserInfo table when added as AX users. When logging into the AX client, users are then authenticated by comparing their windows credentials to this stored information. After a user is authenticated, AX checks user permissions based on their user group membership.

License Keys

License keys control access to entire modules within Microsoft Dynamics AX 2009. If a license key is not present, then the related features are not included in the application. This means that no one will have access to the features that belong to that license key.

To check which license keys are in use, navigate to the License Information form: **Administration** > **Setup** > **System** > **License Information form**. Generally, license keys will not be touched unless a new license to add extra functionality has been purchased.

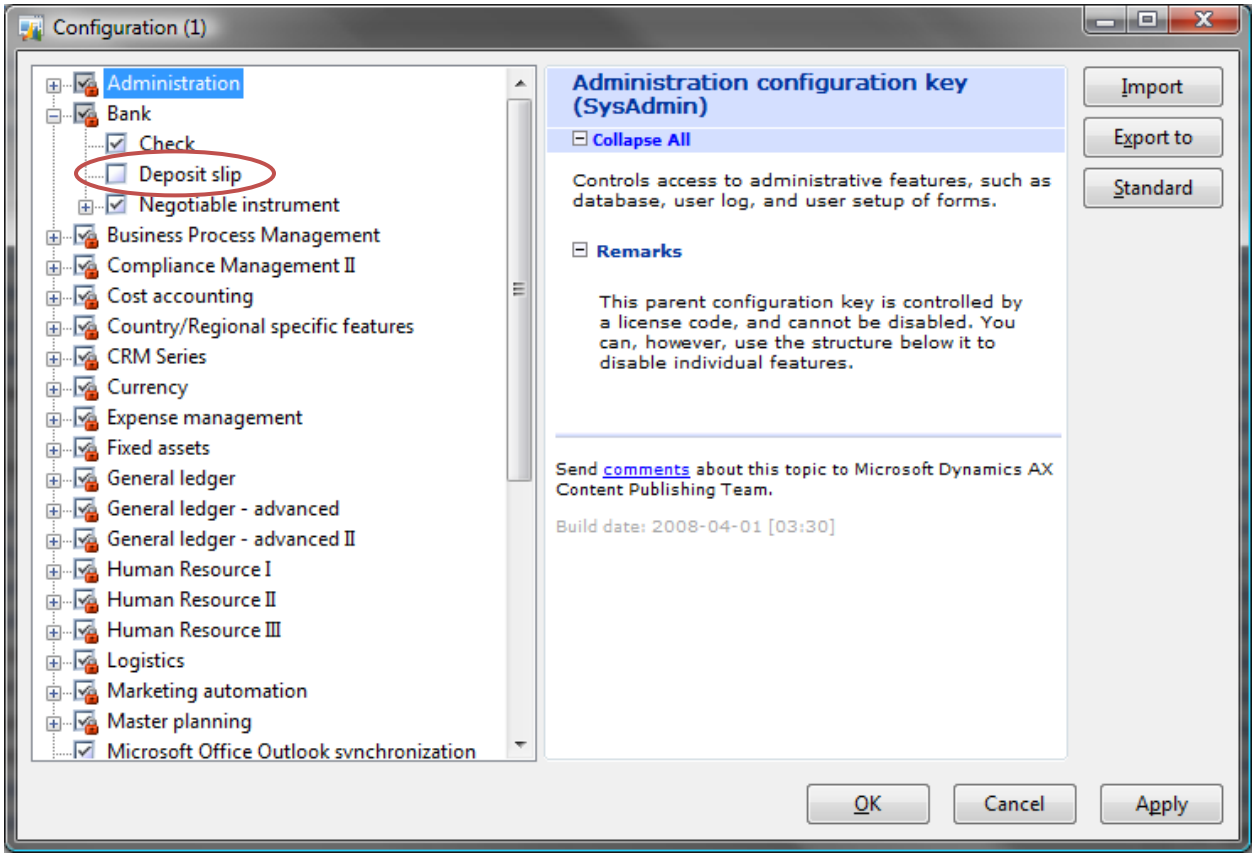
NOTE: A valid license key will display as '*******' in the license code column. If values in the column are showing in plain text, such as 'ABC123', the key is invalid and the feature will not be available.


License information (1)
File Edit Tools Command Help
License holder: Demo
Load license file
Serial number: 05516332
Expiry date: 12/31/2008
System Modules Partner modules Web Languages
Code description License code Status Lic
Base Package ******* Enterprise Bu
Users ******* 30000 Bu
Business Connector Users ******* 30000 Bu
Application Object Servers ******* 100 Bu
Company Accounts ******* Ok Bu
Domains ******* Ok Bu
Dimensions ******* 100 Bu
Business analysis ******* Ok Bu
Alerts ******* Ok Bu
Database Log ******* Ok Bu
License holder as written in the license document.
usr

Configuration Keys

Modules within Microsoft Dynamics AX 2009 have features that are linked with configuration keys. There are around 100 configuration keys in the AX application. If a module is licensed, one or more features within the module could be disabled through configuration if desired. Turning off a configuration key completely removes the functionality from the application. No one would have access to the features if the configuration key is disabled.
For example, the 'Deposit slip' feature which is part of the 'Bank' module could be disabled. To do so use the following steps.

1. Open the 'Configuration' form (**Administration** > **Setup** > **System** > **Configuration**).
2. Expand the 'Bank' node.
3. Uncheck the 'Deposit Slip' option.
4. Click OK to save settings.



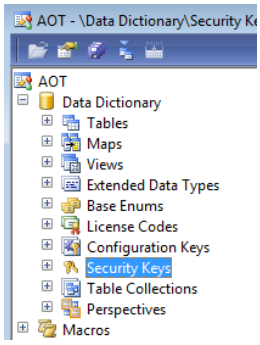
Security Keys

Security keys are by far the most commonly used items for restricting access in the Microsoft Dynamics AX 2009 application. By using these keys, access can be restricted or granted to almost any item within the application. This includes menu items, forms, and tables.
Other objects, such as classes and reports, are not directly controlled by security keys. These objects can only be directly called from a menu item. This means that security for these items is set on the corresponding menu items.
Security keys are used in conjunction with user groups to set specific limitations on which data operations are available to users. Domains can be setup to grant access to features by company or by a group of companies.
Each key has up to five levels of access available. By default new groups will have 'No Access' set on all security keys.

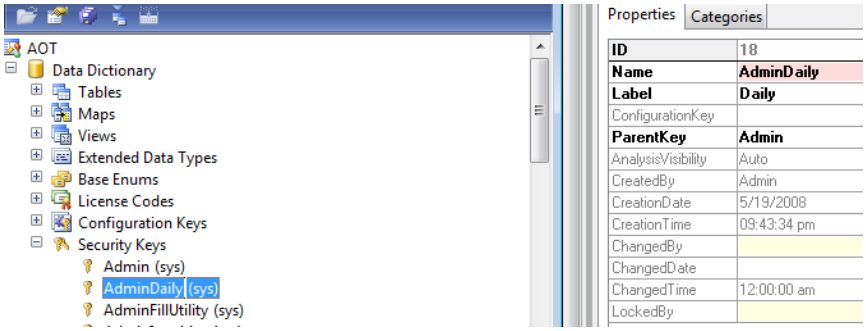
Five Levels of Access

- No Access —the user cannot access these items
- View— user can only view items
- Edit ——the has access to edit items
- Create— the user can create new items
- Full Control— able to create and delete items

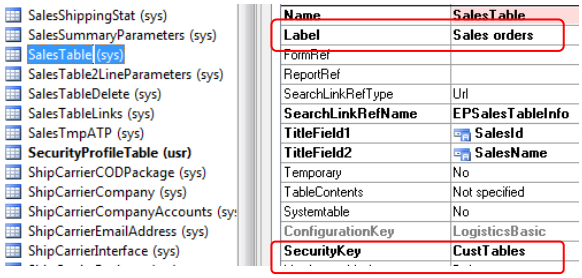
Security keys are maintained in the AOT\Data Dictionary. Security keys have parent-child relationships which are based on the ParentKey property.



The following example illustrates that the Admin security key is set as the parent of AdminDaily. These relationships help organize objects into functional areas.



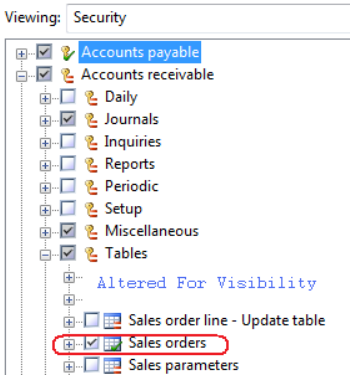
There is also a parent-child relationship between security keys and the objects within Microsoft Dynamics 2009 AX. Each object can have a security key assigned to it. The assigned key will then group the object with any others that have been assigned to the same key in the User Group Permissions form. In the permissions form, objects are all grouped based on their parent key/security key setting and their Label property.
For example, the SalesTable is a member of the CustTables security key and has a label of 'Sales orders'. This can be found by looking at the table's properties in the AOT. NOTE: To view properties, right click on the table and choose Properties.



Looking at the CustTables security key in the AOT, it has a label of Tables and also has Cust as a parent key.

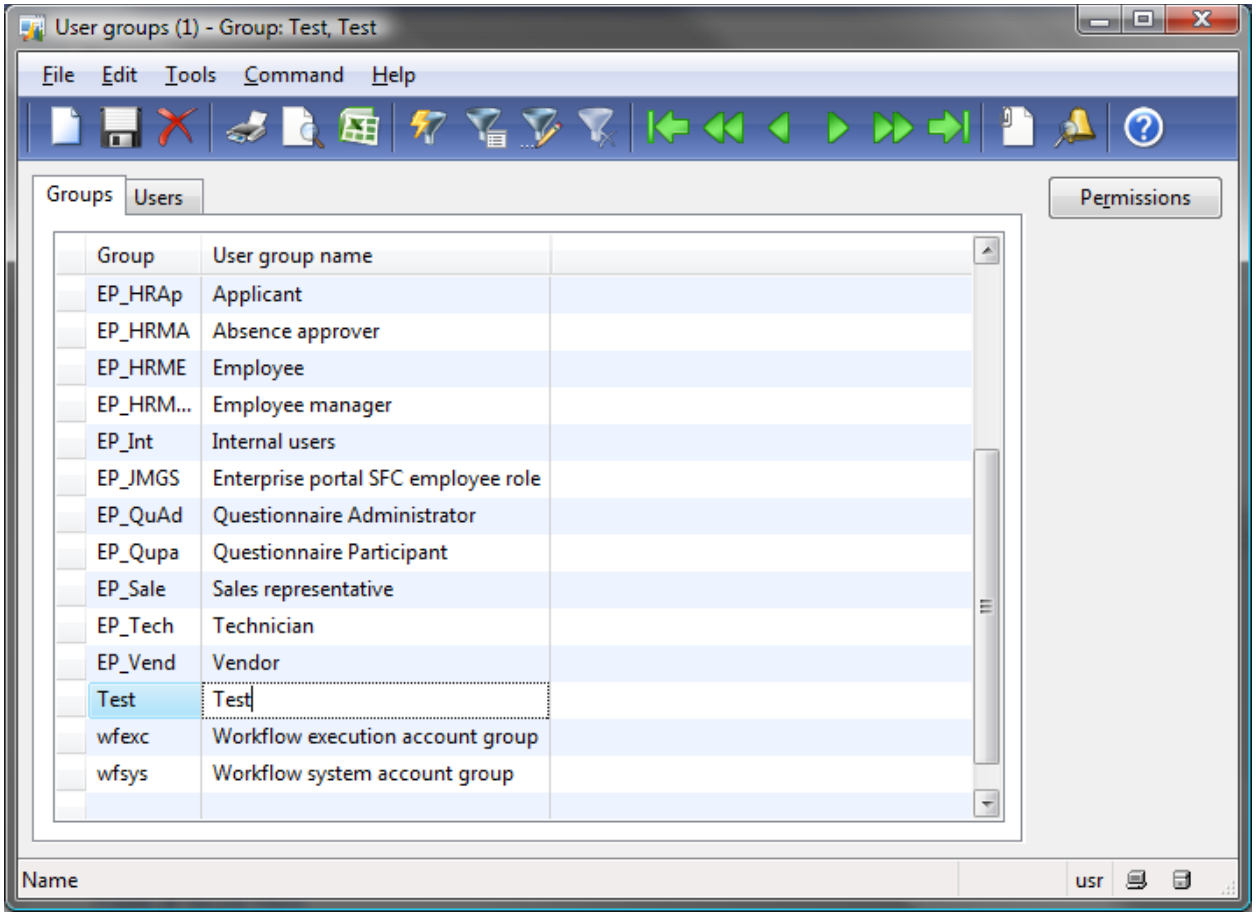
Finally, looking at the Cust security key, it does not have a parent key and has a label of Accounts Receivable.

This means that in the User Group Permissions form, this object's permissions will be found by navigating to **Accounts Receivable** > **Tables** > **Sales orders.**



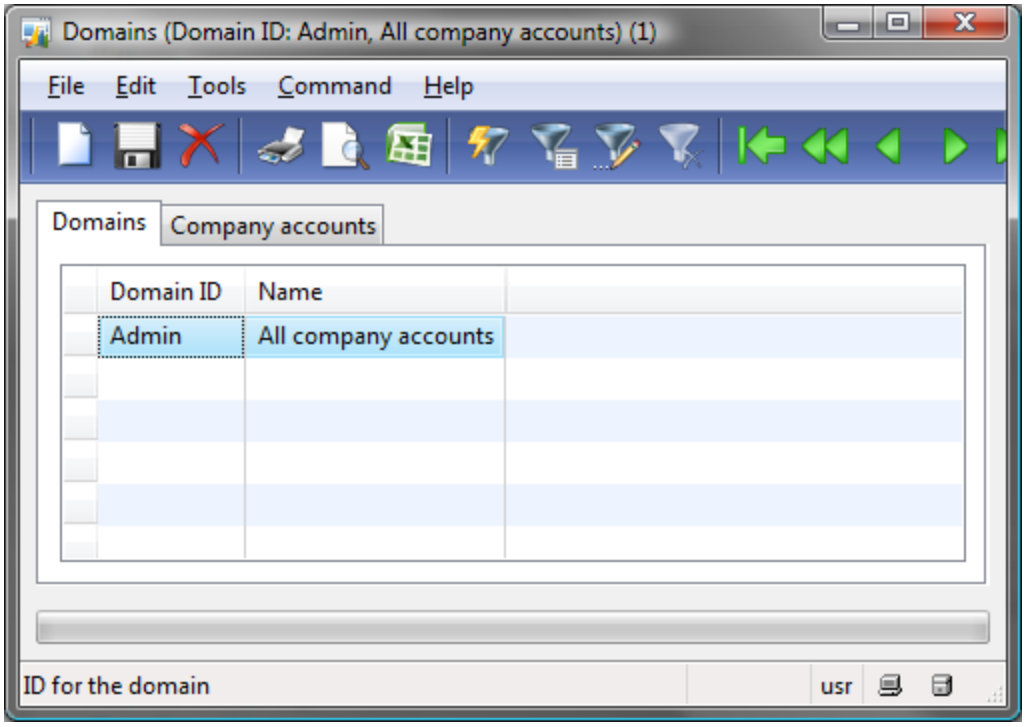
Managing User Groups

User groups are managed from the User groups form which is found by navigating to **Administration** > **Setup** > **User groups**. This form can be used to add and remove groups, and to control the members of each group. By selecting a group on this form and clicking the Permissions button a new form for managing the permissions of the selected group will open as well.



Managing Domains

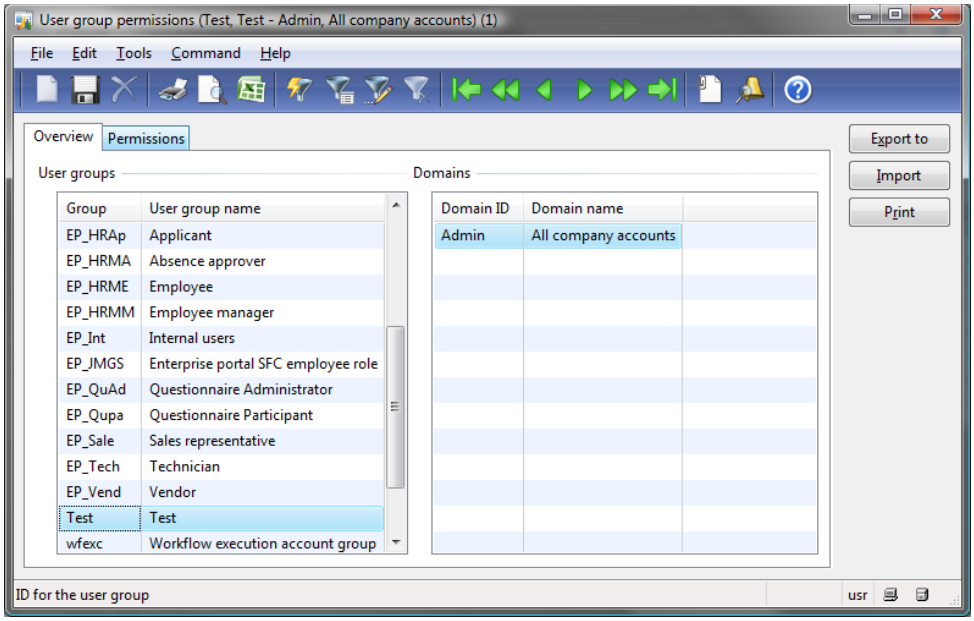
Domains are managed using the 'Domains' form which is found by navigating to **Administration** > **Setup** > **Domains** in the Microsoft Dynamics AX 2009 client.



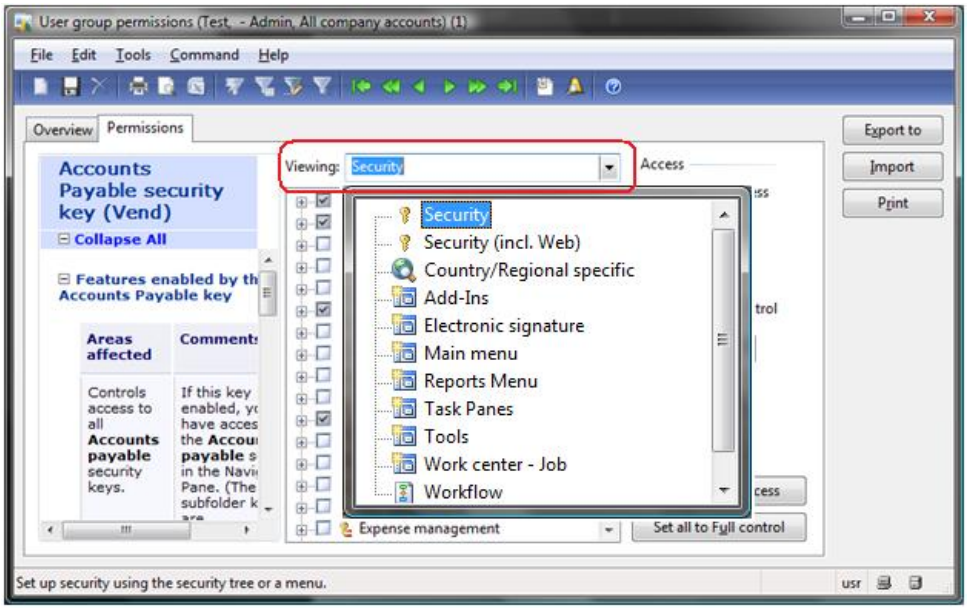
If the application is licensed for domains this form can be used to create a new domain. After domains are created, this form can be used to add/remove company accounts from the domain.
Once created, domains can be used to more precisely define security. Using domains allows administrators to grant user groups different permissions per domain.
For example, CompanyA and CompanyB belong to Domain1. CompanyC is a member of Domain2. Remember all three companies also belong to the Admin domain as well, because the Admin domain automatically contains all company accounts.
A user group has been granted Full Control in Domain1, View in Domain2, and Create in the Admin domain.
In CompanyA and CompanyB the users will all have Full Control because the users have full control in Domain1 and Domain1 includes both CompanyA and CompanyB. Remember that the Full Control is less restrictive than the Create access on the admin domain.
On the other hand, in CompanyC users do have the Create control. In Domain2, they are limited to the View access, but as they have the less restrictive Create access in the Admin domain, the users in CompanyC would, therefore, be given Create access in CompanyC.

Managing User Group Permissions

User group permissions can be managed with the 'User Group Permissions' form which is found by navigating to **Administration** > **Setup** > **Security** > **User group permissions**. On this form, permissions will be set based on the selected User Group and Domain combination.
NOTE: This is the same form that appears when clicking Permissions on the User Group form but in this case all groups are shown, rather than just one selected group. To manage permissions, select the desired group and domain combination and then click on the Permissions tab.



After selecting the Permissions tab on this form there are a number of **views** available for setting permission levels. To switch between views use the Viewing dropdown box.



The default view is the Security view. This is the most common to work with, followed by the Main Menu view.

A list of available views in Microsoft Dynamics AX 2009, some may not be present in previous versions.

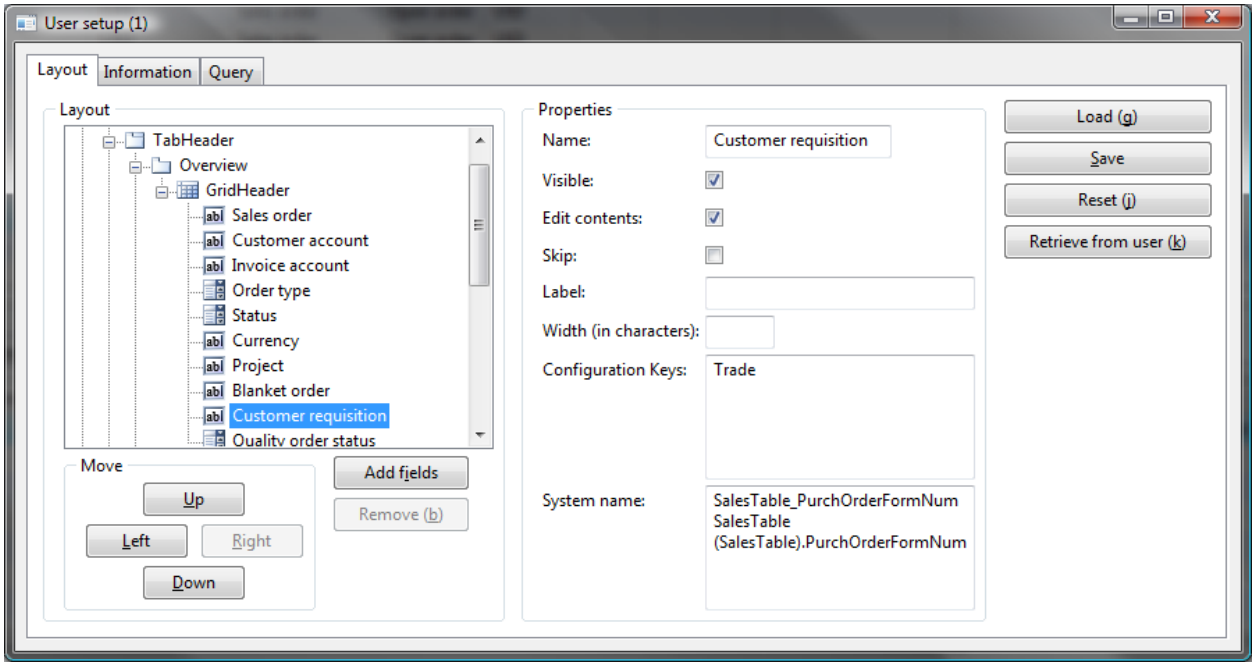
- Security – Displays security elements, grouped by parent/child relationships and sorted alphabetically.
- Security (incl. Web) –This is the same as the 'Security' view, but includes Enterprise Portal related security keys

- Country/Regional specific – Security elements that are relevant for individual countries/regions, sorted alphabetically.
- Add-Ins – Displays some security elements according to the Add-ins menu. This is mostly development related security that would appear when choosing the Add-ins menu within the AOT (right click on an object > Add-ins)
- Main menu – Security elements are displayed according to the layout of the main menu rather than alphabetically. This view does not provide access to parent keys, such as 'Cust' or 'CustTable.'
- Task Panes – Functions that are structured according to the Task panes menu within the Microsoft Dynamics AX 2009 application runtime.
- Tools – Displays security elements related to the Tools menu...
- Work center - Job – Functions that are structured according to the Work center - Job menu within the Microsoft Dynamics AX 2009 application runtime.
- Workflow (Microsoft Dynamics 2009 AX 2009 only) – Functions that sort menu items related to a given workflow with the correct permissions.

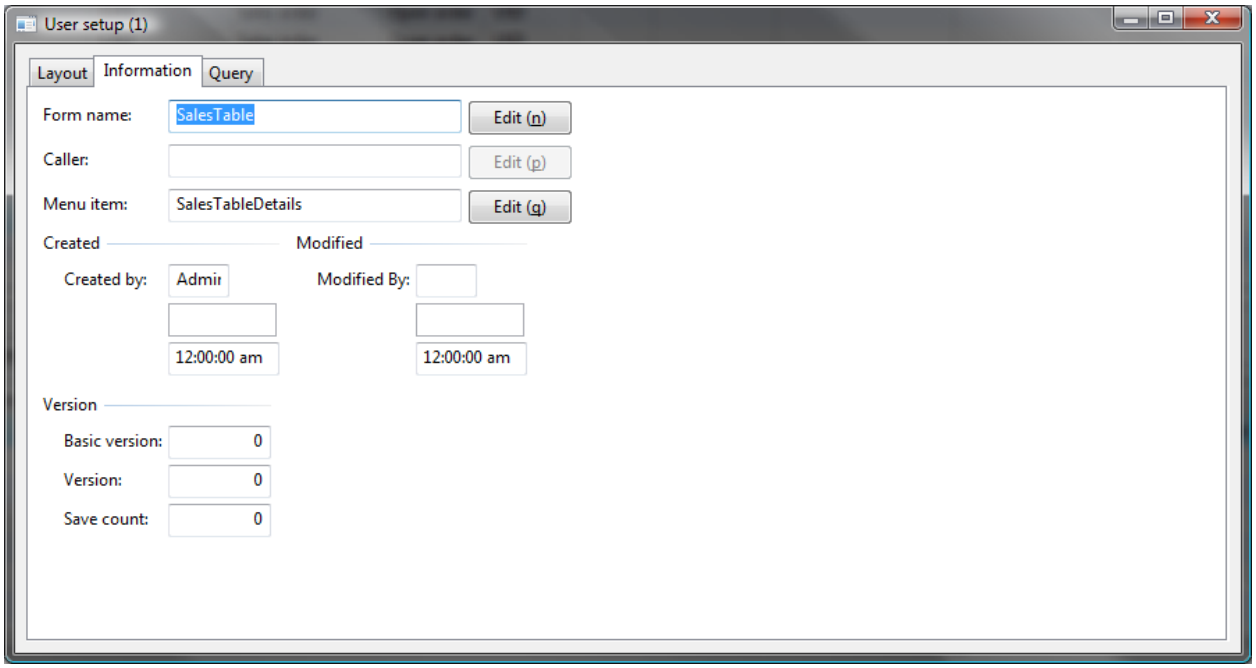
Some of these views provide the means to grant access to very specific areas of the application, such as the Tools or Add-ins view. Others are very similar to one another; they just group the security keys differently, such as the Security and Main menu views.

Finding the Correct Security Key

The most challenging and time consuming task in security setup is that of determining the appropriate security keys to be granted to each user group. Some keys are straight forward based on the structure of the user groups' permission tree. However, others are not as apparent and must be tracked by inspecting the properties within the AOT window. Locating these keys becomes easier as you become more familiarized with the process below.
Often an administrator can begin by simply opening the User Group Permissions form, finding the form (menu item) they want to give access to, and then within the security tree, expand that item to see which other tables, menu items and other objects are required. The more you work with security, the more you are able to accomplish without having to go through the exercise of tracking down a key in the AOT.
When you come across a form, table, button, or tab that you are unsure of, or are unable to find by expanding the user group permission's security tree, the best place to start is by opening the form, or the form that contains the object that users need to access. On any form, an administrator may right click on an object and choose Setup to view more information regarding the form and the object.
When the Setup option is clicked, a User setup form will open showing the layout of the form. In the layout window, the object that was clicked on will be highlighted. In the System name field, information about the selected object is displayed. In many cases, the information in this field can then be used to determine which table or field or menu item a user needs access to.

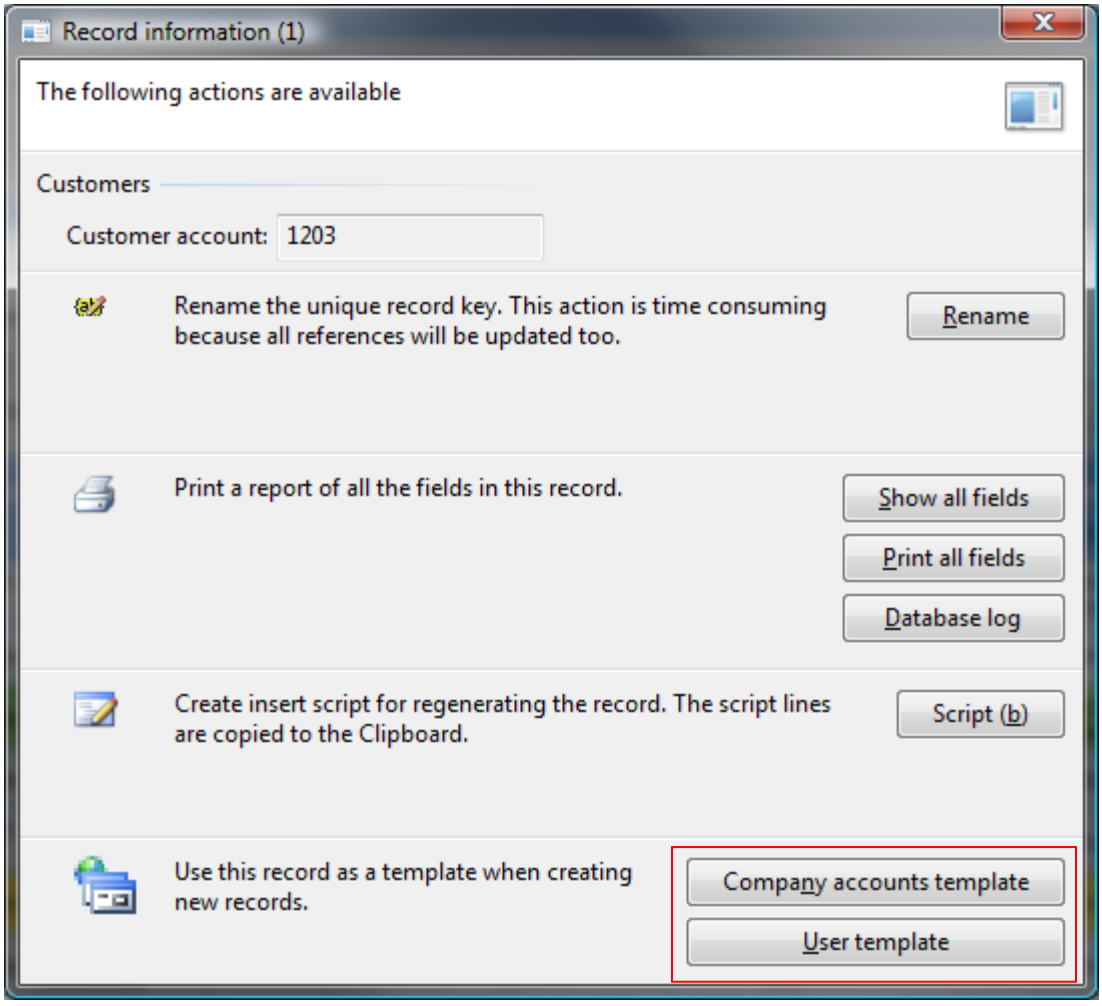


In other cases, it may be a tab or another object on the form that needs to be found. In this case, select the Information tab of the User setup form.

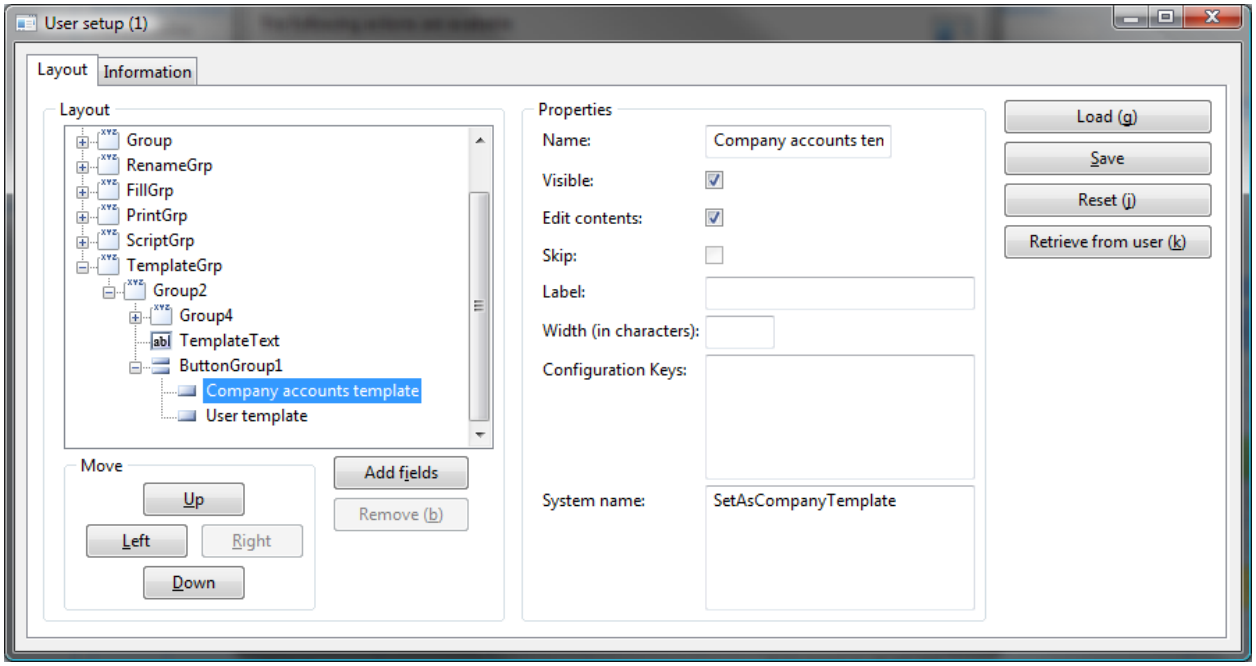


On the Information tab it shows the Menu item used to open the form, or the caller if the form or dialog was opened by a class. It also shows the actual form name. Using the Edit buttons to the right of these fields, you can open an AOT window to inspect the properties of each item.

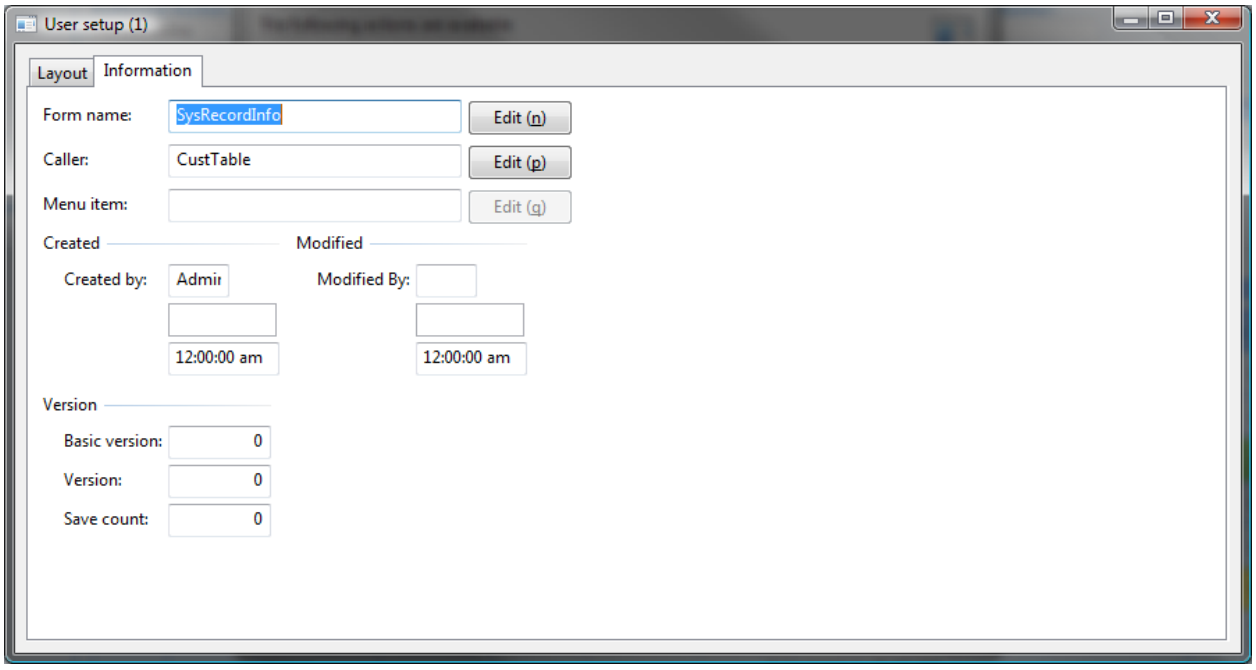
For a Menu item check the SecurityKey property of the menu item, along with the label. These can be used with any parent keys to determine the path to the item within the security permissions tree.
For a form, you need to first review the data sources for the form. Users will most likely need some type of access to each of the tables used as data sources. Note that the data sources themselves do not have a security key, and that you will have to look up each table in the AOT to find the proper security key and label for the tables.
Typically when reviewing a form, a security admin has probably already given access to tables and is looking for something more specific. Such as why a certain object on the form isn't appearing, or perhaps looking for a field group, button or a tab. To find these objects, you need to navigate the design of the form and locate the tab or button. Then review the properties to see if a security key is assigned to the object (usually for tabs). Buttons typically point to a menu item, and this same method can be used to find the menu item type and name. Granting access to the menu item called by a button will allow the button to appear.
For example, one very common security question is how to grant access to the Company accounts template and User Template buttons on the Record information form. This form can be accessed by right clicking on a record and choosing 'Record info.'
NOTE: These buttons do not appear for all record types. On the Sales Order Details, these buttons are not on the Record information, but from Customer Details the template buttons will appear.



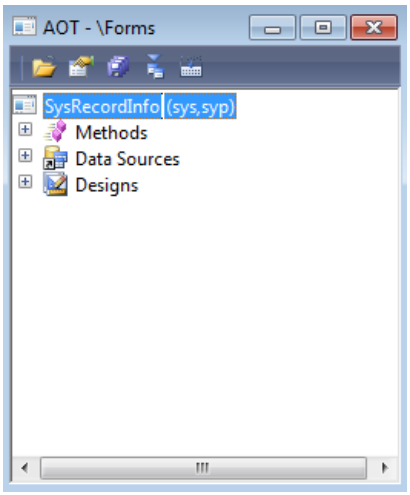
To begin tracking down the keys for these buttons, right click on Company accounts template and choose the Setup option. The User setup form will appear.



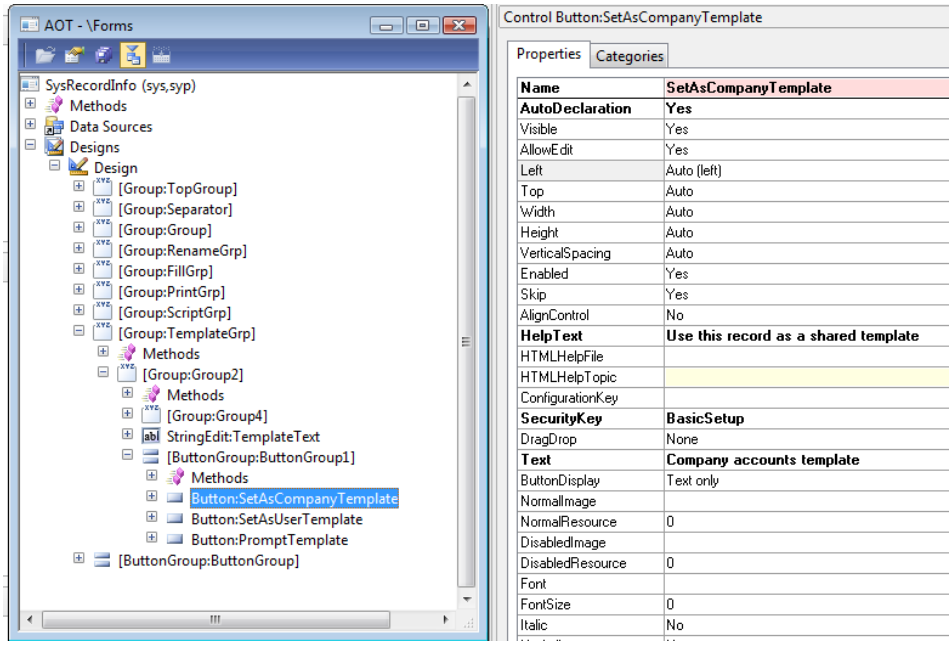
Notice that there is little information in the System name area indicating what menu item may be required for access to the button. Also, note the tree structure in the Layout portion as this will be useful when reviewing the form in the AOT. Select the Information tab and the screen will then look like the image below.



NOTE: The Caller is now the form from which Record info was called (CustTable is the Customer Details form). In this case, click the Edit button next to the Form name, which is SysRecordInfo. An AOT window will open.



Expand the Designs node. Then expand [**Group: TemplateGrp**] > [**Group:Group2**] > [**ButtonGroup:ButtonGroup1**]. Select the Button: SetAsCompanyTemplate, right click on this and choose properties. NOTE: This is the same path that was shown in the Layout section of the User setup form.



Review the SecurityKey property of this button and note that it is the BasicSetup key. Also, note that there is no label for this object. Now select the Button: SetAsUserTemplate and note its security key. There is not one for this object. This may seem odd, as users may not be seeing this button. Go back up and select the different nodes that were expanded to get to the button. Notice that none of the nodes have a security key, until you reach the [Group:TemplateGrp] object. This group has a security key of AdminSetup. This means that in order for a user to see any of the buttons, they must have access to the AdminSetup security key. In addition, they would also have to have the BasicSetup key in order to see

the Company account template button. These two objects are some of the exceptions to the grouping rule.

As seen previously, any object assigned to a security key will be grouped for individual rights as a child of the key. These objects will not appear as children (no label, or being a temporary table is a good indicator that this will be the case). For objects like this, access is truly controlled by access to the key that is assigned. This means users actually must have access to **Admin** > **Setup and Basic** > **Setup** in user group permissions to view these buttons. They do ***not*** need access to any of the children beneath the Setup nodes.

Tips, Tricks, and Exceptions to the Rules

As just seen, security in Microsoft Dynamics 2009 AX doesn't always adhere to the rules. There are a few general exceptions or tricks to know that will speed security setup.

- Items without labels and temporary tables are generally not listed as children of a key. Permissions for these objects are granted by assigning permissions directly to the assigned key.
- Security is set on Menu Items not forms. Often you may think they are setting access to a form, however this is misleading. The same form can be called by multiple menu items. CustTable for example can be opened using the CustTableDetails menu item, and the CustTableEdit menu item. If security on one menu item is set to view, and security on the other is set to full control, the permissions users are granted on the form will depend on which of the menu items were used to open it.
- Restricting access to a field is done on tables, not forms. If you want to make the AccountNum field of the Sales Order form read only, this will be done on the SalesTable. Often people would attempt to find or add a key to the field on the form, but the easiest solution is to find the Table in security, expand it and then set the AccountNum field as view only. This also has the benefit of limiting access on all forms that use the SalesTable as a data source.
- A field on a table **cannot** be set to a level higher than that of the table. If a table is set to View, all fields must be View or lower (No Access). In order to allow only one field on a table to be modified (edit permissions), such as AccountNum, the table must be set to 'Edit' and then all fields *other* than AccountNum must be set to View only.
- The 'Cascade' button: This button offers fairly limited functionality as it does not always cascade as far down the security tree as possible. Usually, if you expand all children nodes, then click expand, permissions will cascade further. Keep this in mind when using the cascade feature.
- Keep in mind that methods in tables, forms, and classes could be checking security behind the scenes. For example the paymentTermsListPage method of the CustTrans table has a line that checks: hasSecuritykeyAccess(securitykeynum(ProjTables), AccessType::View). Basically, this code snippet is checking whether a user has View access to the ProjTables key. In this case the client would return an infolog message if the user did not have access
- While out of the scope of this document. NOTE:Other tables, forms, and classes may perform other security checks, not involving the hasSecurityAccess() method to check security keys. The aosValidate method of AifMessageLog, for example, will validate that the user is a valid user in Active Directory, as well as checking other setup regarding record ownership and configuration.

Security Profiler

There is a Microsoft Dynamics AX 2009 Security Profiler tool that is available for use in test systems. This tool provides a way to perform a security trace. Admin users can open the profile tool and begin tracing. Then in their client simply navigate to and open forms, reports, buttons, and other objects that they wish to grant access to.
Once this is completed, the admin can stop the trace and review the results. The results page lists which keys were required for the actions that they took during the trace. This is an excellent tool to help uncover some keys that are not always obvious, and to speed security setup. It is not a perfect tool, as there are some security calls that it is unable to catch, so the results are not 100% accurate. It is simply an aid in the security setup and troubleshooting process.
This tool isn't publicly available for download. If you would like to obtain the tool please open a request with Microsoft Dynamics AX 2009 support. Keep in mind this tool is for Test environments only and should never be imported into a production environment.

Record Level Security

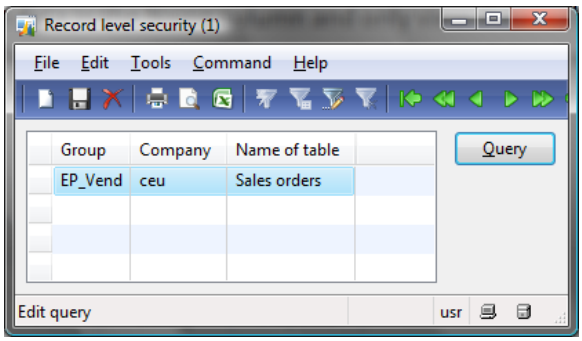
Record Level Security (RLS) is used to restrict the data that a User Group is able to view based on a query. For example, imagine an Excel spreadsheet. While security can be used to restrict access to data in specific columns, RLS can be used to restrict access to the rows of data displayed.
Example: Consider the following table. With security, users could be setup so that they had access to edit data in the Name column and only view data in the Salary column. With RLS, a query could be used so that users could only see records where the ID is between 3 and 10. When viewing this table those users would only see the information for John and Judy.

ID	Name	Salary
1	Jane	40,000
2	Jim	50,000
3	John	60,000
4	Judy	70,000

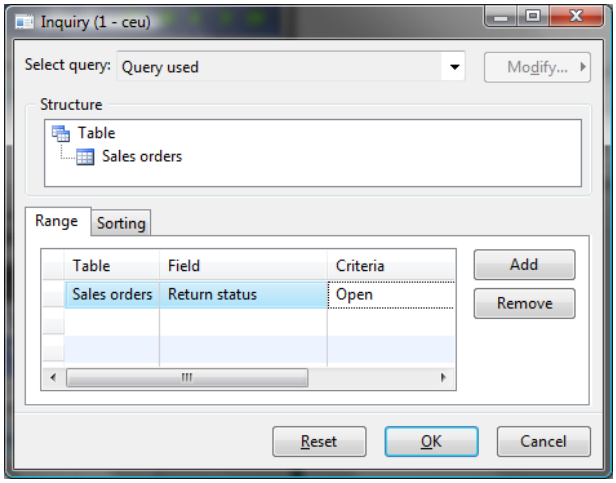
NOTE:RLS filters the records users can see or create, and is an all or nothing for the records it filters. Users will either be able to see the data, or they won't. RLS can be used in conjunction with user group permissions to restrict which records are displayed and which operations users can perform on data.

Configuring Record Level Security

Record Level Security is setup from **Administration** > **Setup** > **Security** > **Record Level Security** in the client. When a new record is created on this form a wizard will walk through selecting the user group, company and table for which to apply security. In the example given, this record would limit access to the data in the Sales orders table for any user logged into the CEU company if they were a member of the EP_Vend group.



After defining the group/company/table combination, the query must still be specified. Without specifying the query, users would still see all data. On the Record level security form , clicking the Query button will open the Inquiry form.



On this form, a query is built based on one or more fields from the specified table. The query defines which data users are permitted to access. In the example given, this query will limit users to only seeing Sales orders with an Open return status. Note that RLS cannot have more than one table per query.

Approaches to Granting Security

There are a few things to consider when approaching security. For some it is best to begin with the highest permissions level and restrict access to specific objects. For others, it is best to begin with the lowest level and grant access to objects. The best approach may vary for each user group.

The advantage to starting will the highest level and then restricting specific objects is that it leaves permission granted to the parent keys, such as the "Accounts Receivable" key. On its own, this key grants nothing to a user that they can see in the application, but for some operations the inherited pieces may be necessary.

Alternatively, starting with the least access and granting has the advantage of keeping the application as locked down as possible. The disadvantage here is that when a parent key is needed, it must be turned on. This will grant access to all child keys. This means that you must go back and restrict access again, and essentially doubles the effort in a case that the need for a parent key is found.

Secondly, you should first determine your overall approach to security groups. Will each security group represent a role within the company, such as an account receivable clerk, or will each group be designed to grant rights to a specific object or two? In the first scenario, most users will belong to only one or two groups, while in the second scenario a user could potentially belong to hundreds of groups.

Most often a combination of these approaches will be used. When deciding on the approach to giving permissions keep in mind that each time a user opens an item in Microsoft Dynamics AX 2009, the client must go through each group to check security. The more groups a user belongs to, the more likely they are to run into performance issues and/or experience unexpected behavior.

Testing Security

For testing the security permissions, an administrator will need a test account. This could be an account created specifically for testing, or any existing domain user, as long as the admin knows the username and password for the account.

In order to test, the administrator will assign the test user to whichever group is to be tested and then login with this user account. To connect to Microsoft Dynamics 2009 AX with the test user there are two options; using a runas command, or logging onto a machine with the test account and then launching the client.

The more convenient option is to use the RunAs command so simply run the client as the test account. In Windows XP or Windows Server 2003, right-click on the Microsoft Dynamics AX 2009 shortcut and choose "Run As…" This will then prompt which user to run the application under. In Vista or Server 2008 the right-click option is not the same and cannot be used. Instead a command prompt can be used with the following command:

Runas /user:domain\testAccount "C:\path\to\client\bin\ax32.exe"
"C:\path\to\config\myConfig.axc"

With this command substitute the correct user credentials, path to the Microsoft Dynamics AX 2009 client executable, and the path to a valid client configuration file.

Once the client has been launched with the test accounts credentials, the permissions can be tested to ensure that all desired functionality is working and that users do not have unexpected access.

Transferring Security

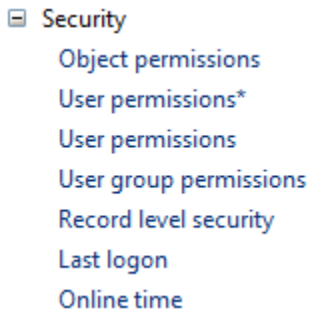
There are a few options available if you need to move security between different environments:
You could use the Export/Import functionality on the user group permissions form to export a group as an .asg file, and then import the permissions into the new environment. This is good when moving only small sets of permissions.
However, the export will only import permissions for one user group/domain combination at a time. So if you had 5 domains, it would mean each group could have 5 export files. Each would then have to be imported. With a large number of groups and a few domains, this becomes a very time consuming and tedious process.
Alternatively, you could use the standard export/import functionality of Microsoft Dynamics AX 2009 to export the security tables from you system and then import them into another. Depending on what has already been setup in the environments, you may import all or some of the following tables:

- AccessRightsList* – security permissions for user groups
- UserGroupInfo* – User groups
- UserGroupList – user group membership
- UserInfo – AX users
- SysUserInfo – User settings
- SysLastValue – Usage data (user)
- DataArea - companies
- DomainInfo* – domains
- CompanyDomainList – companies belonging to domain

Note that when doing this, the export/import needs to be done from the DAT company, as all security information is stored in DAT. Also, note that the tables denoted with a * above should always be transferred.
A third option available for transferring security would be to move the same tables, but to do so directly in SQL. This approach may be a little quicker, but there may also be some risks with RECIDs and other values that are usually automatically generated and tracked by Microsoft Dynamics AX 2009. This approach is not recommended for production environments.

Auditing Security Setup

Microsoft Dynamics AX 2009 offers a number of reports that can be used to review the current security setup. Also, changes to security can be monitored by using other Microsoft Dynamics AX 2009 features.
In Microsoft Dynamics AX 2009, there are a number of reports available under **Administration** > **Reports** > **Security**, which is pictured in the following image:



These reports offer a few different views of the existing security setup, allowing administrators to review the permissions currently granted for an object, user, or user group.
NOTE: The * on report above denotes it is an SSRS report. The online time report requires that the UserLog configuration key is enabled. Similar reports can be obtained for Microsoft Dynamics® AX 2009, Microsoft Dynamics® AX 4.0 and Microsoft Dynamics® Axapta 3.0.
While these reports provide options to review the current setup, it may also be desired to actively monitor when security changes occur. There are two features Microsoft Dynamics AX 2009 offers that could be used to do this:

1) Database Logging – Under **Administration** > **Setup** > **Database** log an administrator can configure tables to monitor for changes, and which types of changes to monitor. To monitor security, track changes to the same tables mentioned in the Transferring Security section. Keep in mind that all security settings are stored in DAT, so the Database Log results (**Administration** > **Inquiries** > **Database Log**) must be view from the DAT company to see security changes
2) The second option is to use Change based alerts on the same security tables. The alerts would notify the administrator when security is changed, unlike database logging where the admin would have to view the results to see if changes had been made. The pitfall to alerts is that the only historical data will be the alerts in the admins inbox.

For historical data on security changes Database Logging is an available option, and for notification of changes administrators can use Change Based Alerts.

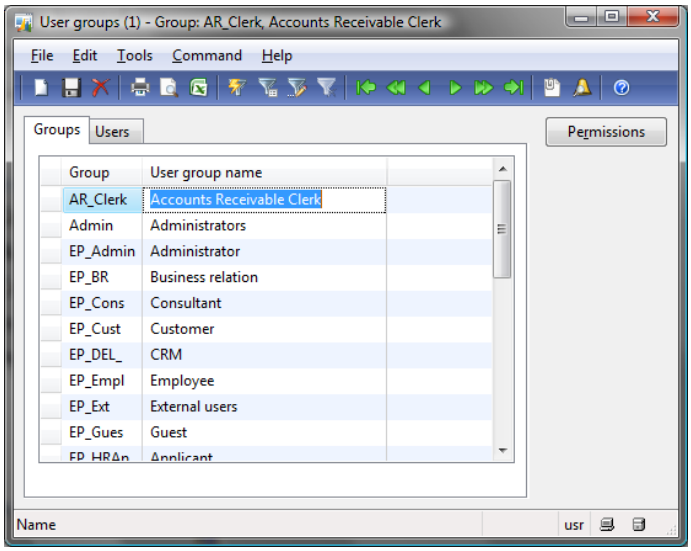
Defining User Group Permissions

In this exercise you'll create a new user group and grant access to objects. For the purpose of this exercise you'll be defining a group based on the company role of an Account Receivable clerk with rights to the following:

- View Customers
- Create Sales orders
- Create Sales Journal
- Edit Payment journal
- Run Sales order Report

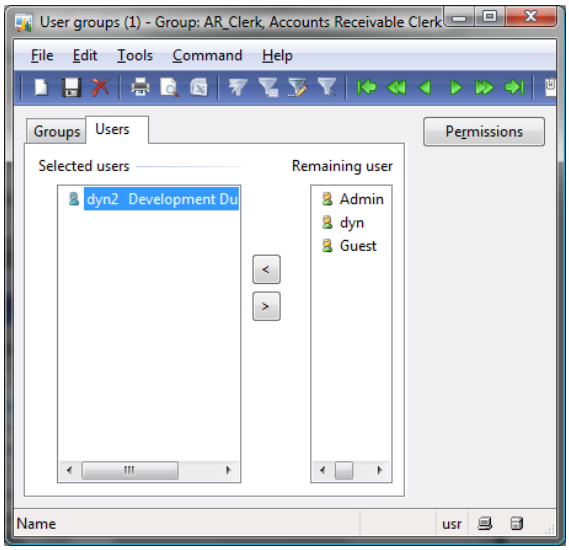
Create a New User Group

1. Open the client.
2. Navigate to **Administration** > **Setup** > **User Groups**.
3. Create a new record.
4. In the Group field type: AR_Clerk.
5. In the Name field type: Accounts Receivable Clerk.
6. Save the record and leave the form open.



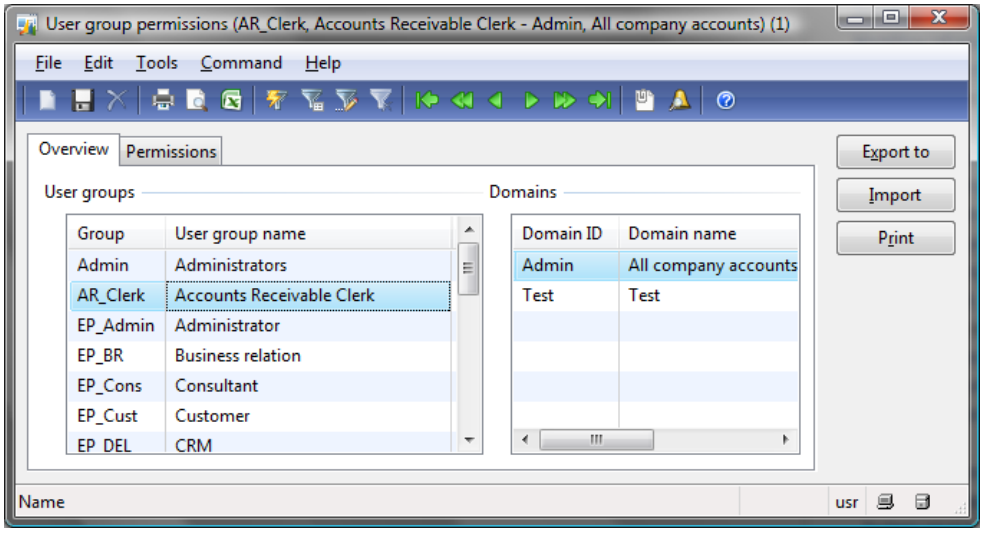
Assign Users to the Group

1. On the user groups form, select the Users tab.
2. Select a test user from the Remaining Users (not members of the group).
3. Click on the '**<**' button in the center of the form.
4. The user is added to the Selected Users (members of the group).
5. If the user belongs to any other groups, remove the user from them.
6. Close the User groups form.

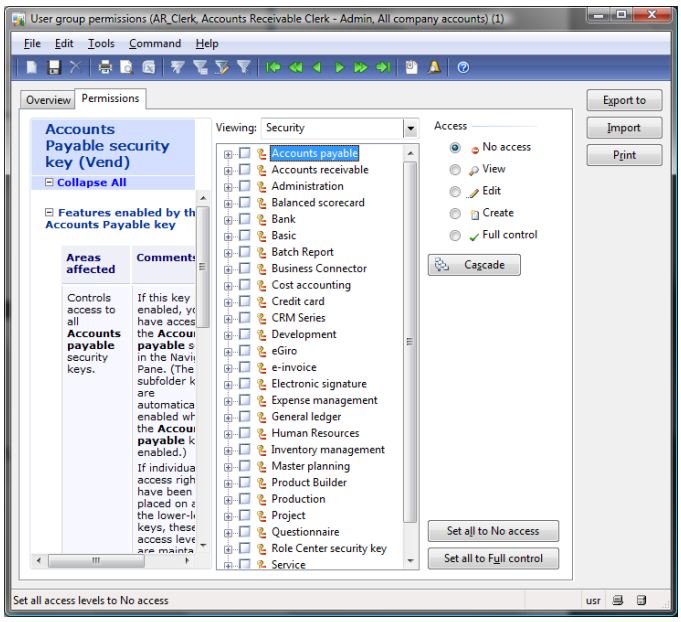


Assign Group Permissions

1. User Group Permissions to assign group permissions. Navigate to **Administration** > **Setup** > **Security** > **User group permissions.** The User group permissions form opens
2. Select the AR_Clerk group in the right hand column.
3. Select the Admin domain in the left hand column.



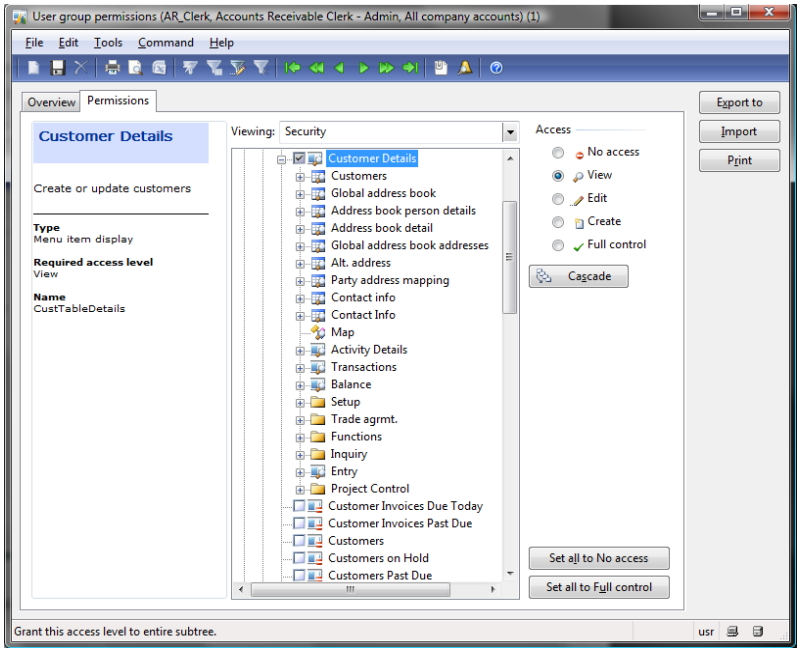
4. Click on the Permission tab and verify that no permissions are granted. Click Set all to No access if there are any.



Grant Customer Permissions

1. Expand the Accounts Receivable category.
2. Expand the Daily sub-category.
3. Find and select the Customer Details' object.
4. With Customer Details selected, click on the View radio button.
5. Expand Customer Details and notice that some related objects were not granted permissions.
6. With Customer details still selected click on the Cascade button.

   Notice that now the View permissions have been cascaded down. Collapse the Customer Details object and notice that some other objects now show View access as these were part of the requirement for customer details.



Grant Sales Order permissions

1. Select the Sales Order Details object.
2. Click the Create radio button to allow users to create sales orders.
3. Expand Sales Order Details.
4. Again click on the Cascade button to cascade changes to other required objects.
5. The user should also be able to delete Sales lines since they created the order:
    a. Select 'Order lines and grant Full Control to this table.
    b. Select the Create lines object.
    c. Click on the Full Control radio button.
    d. Expand Create lines and click the Cascade button.
    e. Select the Items object (beneath Create lines) and set this to View – users should be able to view the items for sale, but probably should not make changes to them.
    f. Collapse the Create Lines section.
6. Collapse (-)Sales Order Details and collapse Daily.

Grant Journal Permissions

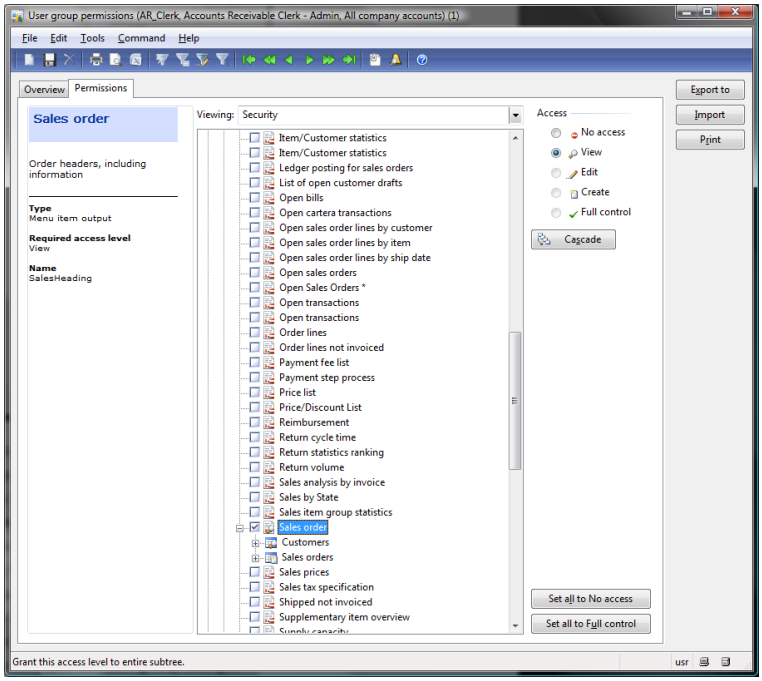
1. Expand the Journals section and select the Sales Journal object.
2. Click on the Create radio button.
3. Expand Sales Journal.
4. Notice that table permissions have already been set, because Sales Order Details uses the same tables. Do *not* click on the Cascade button. This would set some tables, such as sales lines back to only Create rather than Full Control (delete).

5. Collapse the Sales Journal and Select the Payment Journal object.
6. Click the Edit radio button.
7. Expand Payment Journal and click Cascade if necessary.
8. Expand the first Lines object (form), notice the cascade did not affect the tables required for lines. With Lines selected click on cascade one more time.
9. Collapse Payment journal.
10. Collapse Journals.

Notice that when cascading permissions to required objects for each object, it has not been limited to just accounts receivable. There are also a number of objects which have been affected in other areas including Accounts Payable, Basic, General Ledger, and many more.

Grant Report Permissions

1. Expand the Reports section within Accounts receivable.
2. Locate and select the Sales Orders report object.
3. Click on the View Radio button – note that Edit, Create, and Full Control are not available as View access is the highest available level for reports.
4. Expand the Sales Order's report, but do NOT click Cascade.
5. Notice that the required tables already have permissions granted. There is already View access to the Customer table, and Create access to the 'ales order table. Clicking cascade here would set them both to view, which would then prevent users from creating sales orders, since they need Create level access on this table in order to do so.
6. Leave the table permissions as they are and save the user group changes.
7. After saving your changes, close the User group permissions form.



Test the Security Group Settings

1. Launch a second client for testing using “RunAs” .(See section on Testing security).
2. Test each piece of desired functionality, note any errors.
3. View Customers – Make sure you cannot create records, if you select the ‘Payment’ tab, an error will occur as the group does not have access to the CustBankAccount table. Click on a different tab, and then close the infolog window.
4. Create Sales Orders – verify you can create an order, and also delete a sales line on orders.
5. Create a Sales Journal – verify you can create the journal. Also, try deleting a line.
6. Edit a payment journal – try to edit a payment journal record.
7. Run the Sales Order report.

Results

- You were able to view customers, but could not create them. You were not able to view the Payment tab. To resolve this you would have to grant access to the CustBankAccount table.
- You could create a Sales Order and Sales Lines, however you could not delete a line. This is because the menu item (Sales Order Details) is set only to create; therefore the most the form will allow is create, even though you have full access to SalesLines. To resolve this set the MenuItem to full control, leave the Sales Line pieces as full control, and limit the Sales order table to Create.
- Sales journals will behave the same as the Sales table, as the same permissions have been set. The resolution is the same if you wish for users to delete sales journal lines.

- You can modify the payment journal, but the forms design only allows a few fields to be changed. You don't have access to the journal lines. To resolve this you will have to find the key needed for the 'Lines' button of this form.
- The report should have worked. If you see an error stating simply 'Insufficient rights' run the report again and check the printer. The user you run this report with needs to be a local user with a default printer. If this isn't setup errors may occur.

Identify Missing Security Objects

1. Go back to the client that is running as an administrator to resolve the errors.
2. Open the AOT.
3. Expand **Data Dictionary** > **Tables**.
4. Find the CustBankAccount table.
   Note the label and security key of the table.

Apply Security for Missing Sales Order Objects

1. Open **Administration** > **Setup** > **Security** > **User group permissions.**
2. Select the AR_Clerk group, the Admin domain, and click the 'Permissions' tab.
3. Expand **Accounts Receivable** > **Tables**. (CustTables security key)
   a. Locate the Customer bank accounts table (the label of CustBankAccount).
   b. Select the table and set permissions to View.
   c. Collapse the Tables section.
      Expand Daily and locate the Sales Order Details form.
   d. Set Sales Order Details to Full Control.
   e. Expand Sales Order details.
   f. Select the Sales orders table (first in list).
   g. Make sure this table is still set to create, if not set it to Create.
   h. These changes will allow the user to delete lines, but will restrict them from deleting. entire orders.
   i. Collapse Sales Order details and Daily.

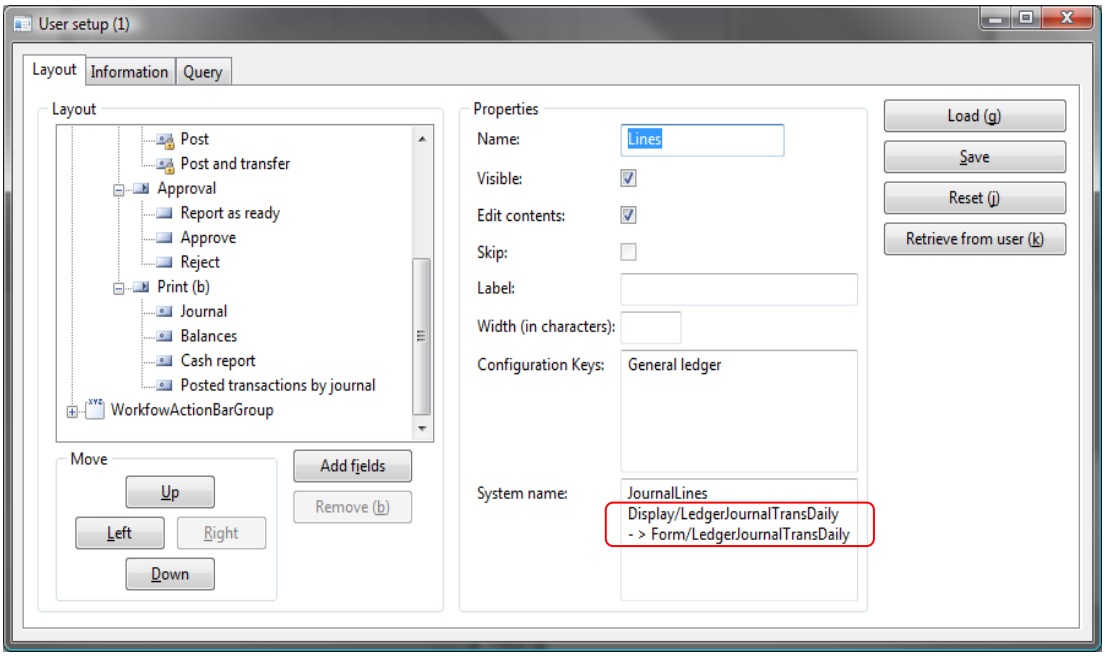
Apply Security for Missing Journal Objects

1. Expand the Journals section and locate the Sales journal.
   a. Set Sales journal to Full Control.
   b. Expand Sales journal.
   c. Select the Sales orders table (first in list and make sure this table is still set to Create. These changes will allow the user to delete lines, but will restrict them from deleting entire orders.
   d. Collapse Sales journal.

2. Expand Payment Journal and review the different Lines options. It appears that permissions have been granted, but yet the Lines button did not appear on the payment journal form.
3. Minimize the User group permissions window and return to the client.

Locate Payment Journal information

1. Navigate to **Accounts Receivable** > **Journals** > **Payments** > **Payment journal** in the client.
2. On the Payment journal form, right click on the Lines button and click on the Setup option. The following User setup form should appear:



NOTE: The System name field is showing information about the Lines button, including the menu item it calls (Display/LedgerJournalTransDaily), and the form it will open (Form/LedgerJouranlTransDaily)

3. Select the Information tab and make a note of the form name and Caller.
4. Close the User setup and payment journal windows.
5. Open the AOT (find the Display/LedgerJouranlTransDaily menu item).
   e. Expand Menu Items.
   f. Expand Display (note that the menu item type was given by the setup form).
   g. Find the LedgerJournalTransDaily item.
6. Note the label and security key and then close the AOT window.

Apply Payment Journal security

1. Go back to the User group permissions window that was minimized.
2. Collapse the Payment Journal, Journals, and Accounts Receivable.
3. Expand **General Ledger** > **Miscellaneous** (SecurityKey).

4. Locate the Lines option.
    a. Notice that there are many Lines, *formName* entries.
    b. You will need the Lines, LedgerJournalTransDaily – note that you already have this because it was one of the items listed beneath Payment Journal in Accounts Receivable.
    c. The caller for this form was LedgerJournalTable_CustPaym, so this is going to be customer payment journal.
    d. Scroll down from the Lines entries until you find a couple of "Payment Journal" entries, notice there is one for CustPaym and one for VendorPaym.
    e. You'll need the Payment journal, LedgerJouranlTransCustPaym, and may also want to give access to the VendPaym option as well. These keys are not ones typically easy to track down aside from a lot of hunting and testing.
    f. After giving this access collapse Miscellaneous and General Ledger.

Complete Security Setup

1. At this point all of the issues found in previous testing have been resolved. To save time, there is one last issue that would appear when tested again. The Payment Journal Lines would throw an error stating you have insufficient rights to the Bank Accounts Table if tested again with the current setup.
    a. Expand **Bank** > **Tables.**
    b. Locate the Bank accounts table.
    c. Grant View access.
2. Save changes and close the User Group Permissions form.
3. Test functionality again, and the user should be able to perform each task successfully.

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship and supply chain processes in a way that helps you drive business success.

U.S. and Canada Toll Free 1-888-477-7989
Worldwide +1-701-281-6500
www.microsoft.com/dynamics