



Feith Control Panel
Version 9.2
User Guide

Updated 2/8/2018

**Feith Control Panel
Version 9.2
User Guide**

© Copyright 2018 Feith Systems and Software, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the written permission of Feith Systems and Software, Inc.

All information in this work is subject to change and reflects software current at the time of publication.

FDD and the FDD logo are trademarks of Feith Systems and Software, Inc. All other trademarks, product names and company names may be trademarks or registered trademarks of their respective holders.

**Feith Systems and Software, Inc.
425 Maryland Drive
Fort Washington, PA 19034
Tel (215) 646-8000
Fax (215) 540-5495
www.feith.com**

Table of Contents

Introduction	7
Welcome.....	8
What's New?.....	9
Frequently Asked Questions.....	10
Tips and Tricks	11
Login.....	12
FCP Modules.....	13
Plan for FDD	15
Define File Cabinets	16
Security.....	17
Task Permissions	18
Resource Permissions.....	25
Document Permissions.....	26
Notes on Setting Permissions	27
Database Roles.....	28
Levels of Administrators	29
FCP Module Access.....	32
Audit Events	35
Bins	43
Bins.....	44
Add Bin	45
Modify Bin	47
Clone Bin	49
Delete Bin	49
Bin Reports.....	49
Classifications.....	50
Classifications.....	51
Add Classification	52
Manage Classifications.....	53
Export and Import Classifications	53
Database Statistics	54
Database Statistics	55
Document Permissions	56
Document Permission Templates	57
Add Document Permission Template	58
Manage Document Permission Templates	59
Document Permission Template Reports	60
FDD Check.....	61
FDD Check	62
File Cabinets.....	64

File Cabinets.....	65
Add File Cabinet	67
Modify File Cabinet	71
Set File Cabinet Field Options	76
Clone File Cabinet	81
Delete File Cabinet	81
File Cabinet Reports	82
Export and Import File Cabinet	83
Full Text	86
Full Text Administrator	87
Groups	90
Groups	91
Add Group	92
Modify Group	96
Clone Group	97
Delete Group	98
Export and Import Group	99
Get Group Member Information	100
Set Group Audit Events for FDD Auditing	101
Group Reports	102
Leaps	103
Leap Editor	104
Create Application Leap	105
Create File Cabinet Leap	107
Create Highlight Leap	108
Create SQL Leap	109
Create URL Leap	110
Manage Leaps	111
Licenses.....	112
License Manager	113
Locks	114
Lock Manager	115
Lookup Tables.....	119
Lookup Tables	120
Add Lookup Table.....	121
Modify Lookup Table	123
Sort Lookup Values	124
Clone Lookup Table.....	126
Delete Lookup Table.....	126
Export and Import Lookup Table.....	127
Lookup Table Reports	127
Messages.....	128

Message Editor	129
Redaction Reason Codes.....	130
Redaction Code Editor.....	131
Servers.....	132
Servers	133
Add Server Entry	134
Add EDStor Server Entry.....	134
Add Full Text Server Entry	135
Add Web Server Entry.....	138
Manage Server Entries	141
Server Reports.....	141
States and Reasons	142
States and Reasons	143
Add State.....	144
Manage States	145
Export and Import States	145
Supplemental Markings.....	146
Supplemental Markings	147
Add Supplemental Marking.....	148
Manage Supplemental Markings	148
Export and Import Supplemental Markings	149
Change Marking Assignments	150
System Preferences.....	151
System Preferences	152
User Access Restrictions.....	153
User Access Restrictions.....	154
Add User Access Restriction Rule.....	155
Add User Access Restriction with One Rule.....	155
Add User Access Restriction with Two Rules Joined by AND	158
Add User Access Restriction with Two Rules Joined by OR	162
Modify User Access Restriction Rule	167
Delete User Access Restriction Rule	169
Users	170
Users	171
Add User.....	173
User Authentication Types	173
Add Database Authenticated User	174
Add Externally Authenticated User on Oracle	179
Add Externally Authenticated User on MS SQL Server	182
Change User Authentication Type.....	185
Set User Audit Events for FDD Auditing	187
Set User Clearance for RMA iQ	188

Set User Other Properties for Access Restrictions	189
Set User Proxies	190
Modify User	192
Clone User.....	193
Delete User.....	194
Enable/Disable User Account.....	194
Import Users From File	195
Import Users From LDAP	196
Password Complexity and Expiration Rules	198
Administer Proxy Users	201
User Reports	203
View Builder	204
View Builder.....	205
Add View	206
Add Synonym	210
Manage Views and Synonyms	211
Export and Import Views and Synonyms	212
Virtual File Cabinets	213
Virtual File Cabinets Overview.....	214
Add Virtual File Cabinet.....	215
Modify Virtual File Cabinet.....	222
Appendix.....	223
Appendix A: Field Mask and Regular Expression Syntax	224
Appendix B: Auto-Populated Field Names.....	226
Appendix C: LDAP Server Format.....	228
Glossary.....	229
Index	233

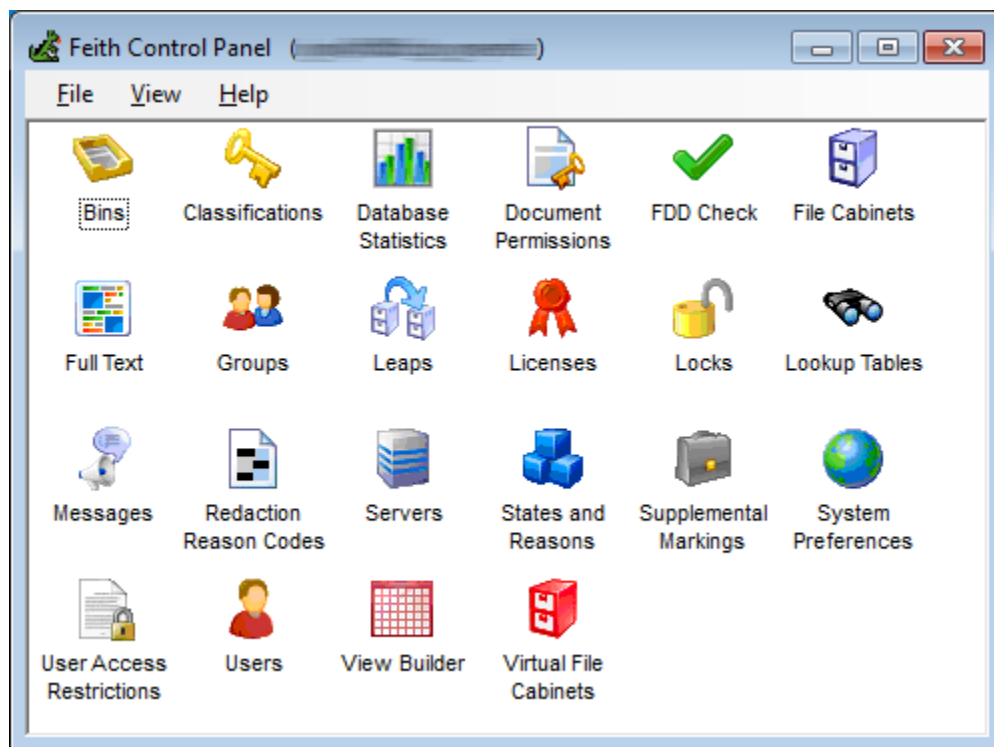
Introduction

Welcome

Administer your FDD system by creating and managing users, groups, file cabinets, permissions, and more. When starting out, you need to define the file cabinet structures that will store your documents and outline the security scheme your organization needs.

Get started:

- [License your FDD system](#)
- Create [file cabinets](#) and [virtual file cabinets](#) to store your documents
- [Define a security scheme](#)
- Create [users](#) and put them in [groups](#)
- ...and more in [all the FCP modules](#)



What's New?

The following are features which have been added or improved in Feith Control Panel:

- **Database Role Changes:** The [Database Role](#) settings - previously referred as the Database User Type - have been redesigned.
 - On Oracle, the Database Role options are **Feith Admin** and **Feith Connect**. Feith Admin grants the privileges needed to create users and tables in the database. This allows for an administrative user other than the fdd user who can create users and file cabinets.
 - On MS SQL Server, the Database Role options are **Feith Admin**, **Feith Connect with DB Owner**, and **Feith Connect**. Feith Admin grants the privileges needed to create users and tables in the database. This allows for an administrative user other than a DBA to create users.
- **View Builder:** Create database [views and synonyms](#) with this user-friendly tool. You may need a view to use as a lookup table on a file cabinet field, or a synonym of a non-fdd object for your dashboard in Dashboard iQ.
- **User Access Restrictions:** The [User Access Restrictions](#) module is used to create and maintain access restriction rules. These rules control document access based on user properties, typically through the comparison of user properties to RMA document properties.
- **Proxy Authentication and PKI:** Create [proxy users](#) which can be [assigned](#) to your FDD users for proxy authentication. Additionally, you can set your FDD users to be authorized through proxy using PKI. See [Add Database-Authenticated User](#) for more information on adding users.
- **Default Sort Order on File Cabinets:** Define a [default sort order](#) for users who search in that file cabinet. The default sort order may be on up to three columns.
- **Import Fields to Existing File Cabinets:** You can import just fields from a file cabinet export file and [append](#) them to an existing file cabinet.
- **Exclude Group Members from Export:** You can export groups with their settings while excluding the users that are members of that group. You may want to do this if the group members are completely different on your test and production systems. This applies when exporting [groups](#) or [file cabinets](#) (with groups).
- **Add Index ID to Virtual File Cabinet:** Easily add the internal Index ID of a document as a column in your [virtual file cabinets](#).
- **Classification Color:** Optionally set a Color to represent the [classification](#) throughout the FDD system in various applications.
- **Dash Allowed in Login Name:** On Oracle, more characters are allowed in the user's login name, including dash, underscore, period, and more.

Frequently Asked Questions

Why can't I deny task permissions in a group?

In a group, clearing a task permission (making it unset) would be the same as denying the task permission. Since the two are functionally the same, deny is not an option for groups.

The deny option is available when setting task permissions for users, because clearing or denying at the user level has different results depending on what task permissions are inherited from the user's groups.

See [Note on Setting Task, Resource and Document Permissions](#) for more information.

Can I make a mid-level administrator who can only administer some groups and file cabinets, but not all of them?

Yes. You would make a group and designate them as an **Administrator Group**. Then you would assign the group in the **Administered By** setting in the file cabinet properties, or the **Administered By** tab in the group properties. Users in this group would only have access to the file cabinets and groups to which they are assigned. See [Add File Cabinet](#) and [Add Group](#) for more information.

When the user is viewing a file cabinet in FDD Client, they do not see the field I just added?

The user may have set **Column Preferences** in FDD Client. If they reordered or hid any columns using this feature, any new fields are automatically added as hidden fields. See FDD User Guide for more information.

When the user does a search in a file cabinet, they are getting back case-sensitive results. Can I change the results to be case-insensitive?

Yes. Change the **Case Options** on the file cabinet field to be **Mixed Case (Case Insensitive Search)**. Note that this search may be less efficient. See [Set File Cabinet Field Options](#) for more information.

The user's search results do not come back in the Default Sort Order I defined on the file cabinet?

- If the user sorted the data themselves by clicking on the file cabinet field headers, this would override the admin-defined sort.
- If the user did a simple full text search in Elasticsearch with smart sorting, then the ranking from ES will be used and the admin-defined sort will be ignored.

Can I use another table or view as a Lookup on a file cabinet field, instead of the standard lookup tables?

Yes. You can use any view or table in your database as a **Lookup** on a file cabinet field. Instead of selecting a lookup table from the list, simply type in the view or table name and the column name(s) in the file cabinet field options. See [Set File Cabinet Field Options](#) for more information.

Can I change the name of the table or columns underlying the file cabinet?

No. You can change the friendly file cabinet name or file cabinet field name that display to end users, but the file cabinet's table and column names will remain unchanged.

Tips and Tricks

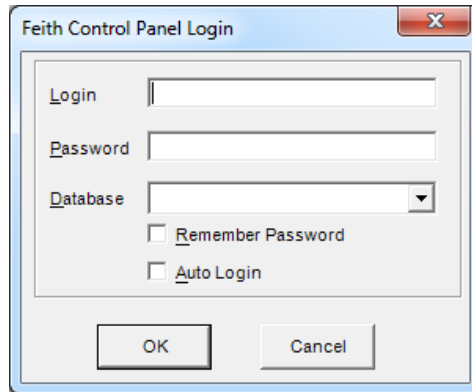
- Take advantage of virtual file cabinets when defining your security scheme. Instead of granting end users permission to the base file cabinet, create a virtual file cabinet for them and tailor it to their needs. For example, you could restrict the documents listed in the virtual file cabinet. You can also remove columns the users should not see, or even add columns from another table they need. See [Virtual File Cabinet Overview](#) for more information.
- It is recommended to set task permissions at the group level, instead of the user level, as well as grant groups resource permissions on file cabinets and documents, instead of individual users. If you manage permissions this way, you just need to change the group's task permissions in one place and then all the members' task permissions have been updated - no need to go into every user and change task permissions there. Also, if you want to stop a user accessing certain file cabinets, you just need to remove them from the group through which they got access - no need to go into every file cabinet and remove the user from each one.
- When viewing a list in a module, information is typically organized into a series of columns and you can click on a column header to sort the data.
- If you have a long list of users in the **Users** module, select **File>Find** to find the user you want to find. If the list is so long that you do not want it retrieved when the **Users** module loads, you can turn off **Full User List on Start** under the **File** menu. See [Users](#) for more information.
- To assign users to a group faster, you can double-click the user name to move it from one list to the other. See [Add Group](#) for more information.
- When setting resource permissions on a file cabinet, bin, or document permission template, you can select multiple groups/users in the list and change all their permissions at once.
- You can give a file cabinet field a special name in order for the field to be automatically populated with information from the file being imported. FDD and CheckIn automatically populate fields with certain names. See [Appendix B: Auto-Populated Field Names](#) for more information.
- Use any view or table in your database as a **Lookup** on a file cabinet field. Instead of selecting a lookup table from the list, simply type in the view or table name and the column name(s) in the file cabinet field options. See [Set File Cabinet Field Options](#) for more information.
- You can help out your users by setting up a default sort order on a file cabinet's search results. See [Modify File Cabinet](#) for more information.
- You can look up the database table and column names underlying a file cabinet by viewing a report: In the **File Cabinets** module, select the file cabinet and then select **Report>Selected File Cabinet - HTML**. See [File Cabinet Reports](#) for more information.
- When entering data in a lookup table, use **TAB** and **SHIFT+TAB** to navigate the columns and rows. You can also use the arrow keys to navigate the table. With a cell selected, hit **F2** to enter edit mode in that cell and start typing. See [Add Lookup Table](#) for more information.
- If you are switching to external authentication, such as Active Directory for Single Sign-On, you can change existing database-authenticated users to externally authenticated users. See [Change User Authentication Type](#) for more information.
- If you need to assign proxy users to a lot of FDD users, take advantage of the right-click options in the **Feith User Administrator** that let you assign proxy users en masse. See [Set User Proxies](#) for more information.
- When creating file cabinet leaps, if you map the same **From** field twice to two different **To** fields, FDD Client will take the value in the **From** field and search for it in both **To** fields using OR logic. The value can be in either field for a document to be returned.

If you map two different **From** fields to the same **To** field twice, FDD Client will take the values in the **From** fields and search for them both in the one **To** field using OR logic. Either value can be in the field for a document to be returned. See [Leaps](#) for more information.

Login

To login to the Feith Control Panel:

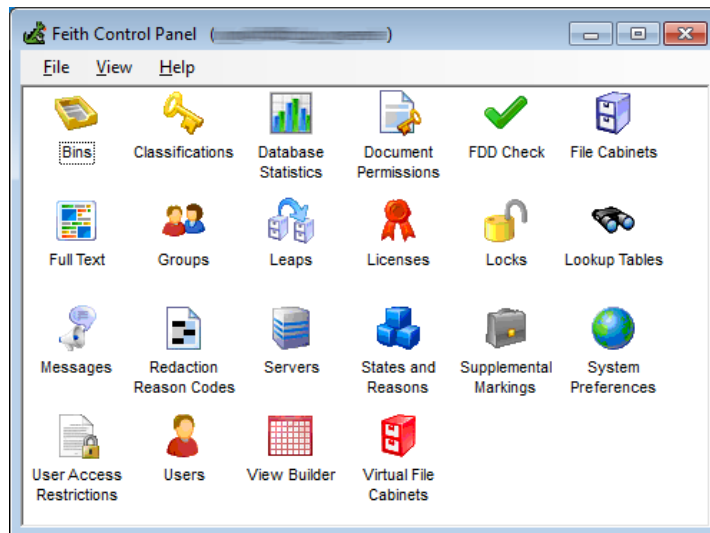
1. From the **Start** menu, select **Programs>Feith Systems>Feith Control Panel**. The **Feith Control Panel Login** dialog opens.



2. Enter your **Login**, **Password** and **Database** and click **OK**. Optionally check the **Remember Password** option; if checked, your login information will be remembered the next time you launch Feith Control Panel. Optionally check the **Auto Login** option to automatically login every time you start Feith Control Panel.

The **Feith Control Panel** window opens, listing the Feith Control Panel modules. See [Feith Control Panel Modules](#) for more information on each module.

To change the display style, select one of the following options from the **View** menu: **Small Icons**, **Medium Icons**, **Large Icons**, or **List**.








Reconnect

A **Reconnect** option is available under the **File** menu. This option opens the **Feith Control Panel Login** dialog so you can reconnect to the database. Reconnect only changes the user for future modules launched from Feith Control Panel. Current modules already launched stay connected with the current user.

FCP Modules

Feith Control Panel contains the following administrative modules. When [choosing a module](#), you must have permission to access and use the module. See [FCP Module Access](#) for more information.

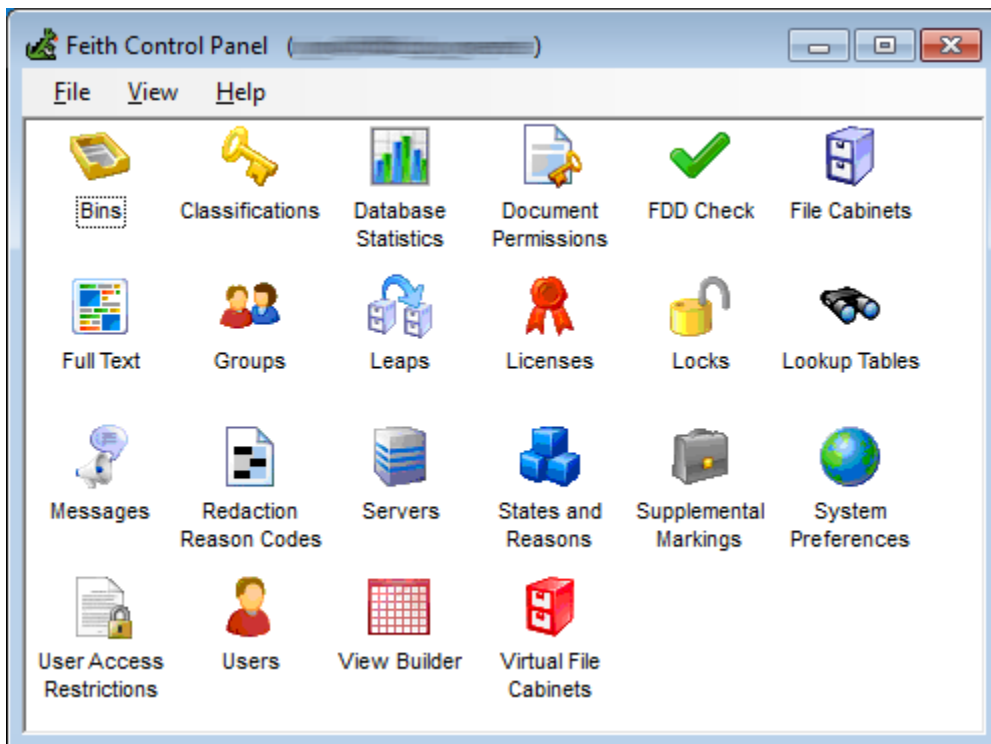
FEITH CONTROL PANEL MODULE	DESCRIPTION
 Bins	Create and maintain bins, which are temporary storage areas for documents.
 Classifications	Create and maintain document classifications, such as for RMA.
 Database Statistics	Displays information such as current count of pages, documents, users and groups.
 Document Permissions	Create and maintain document permission templates, which restrict access at the document level.
 FDD Check	Check the validity of pages, page notes, and document notes on Feith EDStor.
 File Cabinets	Create and maintain file cabinets, which are permanent storage areas for documents.
 Full Text	Manage your Autonomy IDOL full text database.
 Groups	Create and maintain user groups.
 Leaps	Create and maintain leaps, which are used to retrieve related documents or information.
 Licenses	License the FDD system.
 Locks	Unlock locked documents, workflows and work items.
 Lookup Tables	Create and maintain lookup tables, which are lists of suggested index values.
 Messages	Create and maintain FDD logon messages, which are messages that display to end users when they login to the FDD system.
 Redaction Reason Codes	Create and maintain redaction reason codes, which can be applied to redacted areas of FDD documents.
 Servers	Create and maintain FDD server entries, which Feith applications use to interact with one another.
 States and Reasons	Create and maintain document states, such as for RMA.
 Supplemental Markings	Create and maintain document supplemental markings, such as for RMA.

 System Preferences	Set the fiscal year start day and enable RMA features.
 User Access Restrictions	Create and maintain access restriction rules, which control document access based on user properties, such as for RMA.
 Users	Create and maintain FDD users.
 View Builder	Create and manage views and synonyms.
 Virtual File Cabinets	<p>Create and maintain virtual file cabinets, which are views of standard file cabinets.</p> <p>The Virtual File Cabinet Administrator is an optional module and can be used only if your FDD system is licensed for virtual file cabinets. For more information on licensing, please contact your Feith representative.</p>

Choose Module

To choose a module: After you login, select the desired module on the main **Feith Control Panel** screen.

While viewing a module, simply return to the **Feith Control Panel** screen by going to the window or selecting it in the task bar. The list of modules displays and you can choose another.



Plan for FDD

Define File Cabinets

Documents in Feith Document Database are stored in electronic file cabinets, similar to the way paper documents are stored in metal file cabinets. When a document is indexed, or permanently stored in a file cabinet, it is assigned a set of field values that allow users to search for and retrieve the document.

For example, an FDD file cabinet called Accounts Payable might store purchase orders, checks and invoices, just as a metal file cabinet would. Each document might be identified by fields such as Vendor, Amount, PO Number, Date and Document Type.

The system administrator designs the structure of each file cabinet, determining how many fields to include and the names of those fields.

The following questions may be useful in developing the file cabinet structure:

- What steps are currently involved in processing documents?
- What information (such as name, number, date or amount) is needed in order to look up documents?
- What functional or departmental groups are involved in document processing?
- How are people going to use information from the documents?
- How will document flow change with implementation of the FDD system?

Tip: The value for the first file cabinet field is used in many places to identify the document, such as when viewing or exporting. Keep this in mind when creating file cabinets; the first field should be the most important or most meaningful field.

Every file cabinet is independent of other file cabinets. Therefore, security and fields may be tailored for each individual file cabinet.

There is no limit to the number of file cabinets that may be created. However, it is best to minimize the number of file cabinets when possible. For example, use a Document Type field to further organize documents within a file cabinet.

Careful consideration and planning results in a more effective and easy-to-use system, and can eliminate the need for time-consuming changes later.

See [Add File Cabinet](#) for instructions on creating file cabinets in FDD.

Security

FDD provides several different levels of security that can be easily tailored to meet the security needs of your organization. Permissions determine what file cabinets, bins, and documents a group or user can access and what tasks they can perform.

By combining different levels of permissions, you can create a security system that is as simple or complex as you need. However, try to keep your security scheme as simple as possible in order to minimize the time spent maintaining permissions. You can modify security features at any time.

The following questions may be useful in developing the security scheme:

- What functional and departmental groups will be using the system?
- Who are the members of those groups?
- What tasks must these individuals and groups perform?

Use the following guidelines to keep the security scheme as simple as possible:

- Establish restrictions only when necessary.
- Minimize the number of groups and differences in permissions between groups.
- Avoid assigning user permissions that override inherited group permissions.
- Avoid restrictions that unnecessarily impede users' ability to work efficiently.

Security Features

There are five levels of FDD security:

FEATURE	WHAT DOES IT CONTROL?
Login Security	Each user is assigned an FDD login name. User login restricts unauthorized FDD access and helps to log user activity.
<u>Task Permissions</u>	Controls what FDD functions the user may perform.
<u>Resource Permissions</u>	Controls what bins and file cabinets the user may access.
<u>Document Permissions</u>	Controls who may access, add to, modify or delete a particular document.
<u>Database Role</u>	Controls what database privileges a user has.

Task Permissions

Task permissions define what FDD tasks, or actions, a user or group can perform.

Task permissions are divided into sets: [Basic](#), [Advanced](#), [Administrator](#), [Developer](#), [RMA iQ](#), [Reports iQ](#), and [Workflow iQ](#). See [Users](#) and [Groups](#) for instructions on assigning task permissions.

Tip: It is recommended to set task permissions at the group level, instead of the user level. Managing at the group level is easier than changing multiple users' permissions.

Basic Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
Scan/Import	Scan pages and import files into FDD.
Index	Create a new document by indexing pages into a file cabinet.
View	Display images in FDD.
Print	Print pages and documents from FDD.
Route	Move a batch from one bin to another bin.
Create Document Note	Add notes to a document.
Create Page Note	Add notes to a page.
Modify/Delete Notes	Modify or delete notes from a page or document.
Delete Pages	Remove a page from a batch or document.
Delete Batches	Delete batches from FDD.
Reorder Pages	Change the order of pages within a document.
Modify Indexing Values	Change a document's indexing information.
Delete Document	Delete documents from FDD.
Change Your Password	Change user password without system administrator interaction.
Add Page	Add a page to a batch or document.
Search File Cabinets	Search for documents in a file cabinet.
Export/Email Attachments	Export pages and documents from FDD; email pages and documents (as attachments) from FDD.
Email Document Link	Email page and document URL and FRL (FDD URL) links from FDD.
Save Rotation Settings	Save the rotation angle of an image.

Copy Images	Copy FDD pages to the clipboard.
Copy Selected Rows	Copy selected rows of index values (in the file cabinet grid) to the clipboard.
Fill Column	Fill a column with the specified value for multiple documents.

Advanced Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
Set Access Group	Assign a document permission template to a document.
View Access List	View document permission template descriptions in FDD.
View Audit Trail	View the audit trail. This is a list of actions showing time, date and user responsible for each action.
Check In/Check Out	Check in, check out or delete a document version.
Modify WebFDD Profile	Change your user profile in WebFDD.
Replace Page	Replace pages in FDD.
Maintain Folders	Create folders in FDD.
Edit Advanced Search	Edit the advanced search SQL query in FDD.
Edit Forms iQ SQL	Define Autofill from SQL Query or Option List from SQL Query in Feith Forms iQ Designer.
Create/Maintain Sections	Create and delete documents sections in FDD.
Auditor Login	Login to Auditor. Note that this permission only applies to Auditor version 8 or newer.
Edit Auditor SQL Wizard	Edit the SQL Wizard query in Auditor. Note that this permission only applies to Auditor version 8 or newer.
Manually UTR Index/Delete	Manually add/remove batches or documents from the full text database.

Administrator Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
Create Bins	Create bins.

Modify/Delete Bins	Modify and delete bins.
Create File Cabinets	Create file cabinets.
Modify/Delete File Cabinets	Modify and delete file cabinets.
Create Groups	Create groups.
Modify/Delete Groups	Modify and delete groups.
Create Users	Create users.
Modify/Delete Users	Modify and delete users.
Create Document Permission Templates	Create document permission templates.
Modify/Delete Document Permission Templates	Modify and delete document permission templates.
Maintain Servers	Create, modify and delete servers.
Commit Images to Optical	Move images to permanent optical storage (if the images are temporarily stored on magnetic media).
Selective Commit	Commit images based on selected criteria (e.g., a particular file cabinet).
Purge Audit Trail	Purge the audit trail in FDD Auditor.
Rebuild Full Text Database	Rebuild Autonomy IDOL.
Administer Autonomy IDOL	Manage the Autonomy IDOL full text database (e.g. create IDOL database, drop IDOL database).
Selective Delete	Delete records from a file cabinet based on selected criteria.
WebFDD Administration	WebFDD Administration permission.
Unlock/Delete Approval Notes	Unlock or delete approval notes.
Unlock Batches	Unlock a batch. (When a batch is being indexed, the database "locks" the batch to prevent other users from accessing it. If a user's PC shuts down during the indexing procedure, the batch may remain locked in the database.)
Unlock Documents	Unlock a locked document.
Create/Modify Leaps	Create, modify and delete leaps.
Create/Modify Lookup Tables	Create, modify and delete lookup tables.
Create/Modify Messages	Create, modify and delete logon messages.
Create/Modify QI Capture Patterns	Create, modify and delete QI capture patterns using the Quick Integrator Admin Capture Editor.

Create/Modify QI Tools	Create, modify and delete QI tools using the Quick Integrator Admin Tool Editor.
Create/Modify Dashboards	Create, modify and delete dashboards using the Dashboard iQ Designer.
Create/Modify Redaction Codes	Create, modify and delete redaction reason codes.
Setup Audit Trail	Setup the audit trail in Auditor.
Administer States and Reasons	Manage States and Reasons.
Administer Supplemental Markings	Manage Supplemental Markings.
Administer Classifications	Manage Classifications.
Administer RMA Properties and Templates	Manage RMA Properties and Templates.
Administer Access Restrictions	Create and maintain access restriction rules.
Create/Modify Feith Views	Create and modify views and synonyms in the Feith View Builder.
Access to WebFCP Bins Module	Access to WebFCP Bins Module
Access to WebFCP Registration Approvals Module	Access to WebFCP Registration Approvals Module
Access to WebFCP Registration Config Module	Access to WebFCP Registration Configurations Module
Access to WebFCP File Cabinets Module	Access to WebFCP File Cabinets Module
Access to WebFCP Groups Module	Access to WebFCP Groups Module
Access to WebFCP Locks Module	Access to WebFCP Locks Module
Access to WebFCP Lookup Tables Module	Access to WebFCP Lookup Tables Module
Access to WebFCP Markings Module	Access to WebFCP Supplemental Markings Module
Access to WebFCP Messages Module	Access to WebFCP Messages Module
Access to WebFCP Property Sets Module	Access to WebFCP Property Sets Module

Access to WebFCP RiQ Schedules Module	Access to WebFCP Reports iQ Schedules Module
Access to WebFCP RiQ Templates Module	Access to WebFCP Reports iQ Templates Module
Access to WebFCP Servers Module	Access to WebFCP Servers Module
Access to WebFCP System Info Module	Access to WebFCP System Info Module
Access to WebFCP Users Module	Access to WebFCP Users Module
Access to WebFCP View Builder Module	Access to WebFCP View Builder Module

Developer Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
Edit JavaScript	Edit JavaScript in Feith Developer.
Edit CSS	Edit CSS in Feith Developer.
Edit HTML	Edit HTML in Feith Developer.
Edit Text	Edit text in Feith Developer.
Edit XSL	Edit XSL in Feith Developer.
Edit XSD	Edit XSD in Feith Developer.
Edit XML	Edit XML in Feith Developer.
Edit Image	Edit images in Feith Developer.
Edit SQL	Edit SQL in Feith Developer.
Edit FreeMarker	Edit FreeMarker in Feith Developer.
Edit Fonts	Edit fonts in Feith Developer.

RMA iQ Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
Set Record State	Set the record state for a document.
Unset Record State	Unset the record state for a document.
Set/Unset Closed State	Set the closed state for a document.
Set/Unset Frozen State	Set the frozen state for a document.
Set/Unset Cutoff State	Set the cutoff state for a document.
Create/Modify Categories	Create, modify, and delete categories.
Assign/Remove Categories	Assign documents to and remove documents from a category.
Set User Clearance and Markings	Set user clearance and markings.
Edit Supplemental Marking Assignment	Edit supplemental marking assignments for a document.
Edit Classification Attributes	Edit classification attributes for a document.
View RMA Properties	View RMA properties for a document.
Modify RMA Properties	Modify RMA properties for a document.
Modify Document Country Assignment	Modify document country assignment for a document
Submit Ad Hoc Event	Submit an ad hoc event.

Reports iQ Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
Create Reports iQ Template	Create a Reports iQ template.
Create Reports iQ Schedule	Create a Reports iQ schedule.
Modify Reports iQ Template	Modify a Reports iQ template.
Modify Reports iQ Schedule	Modify a Reports iQ schedule.

Delete Reports iQ Template	Delete a Reports iQ template.
Delete Reports iQ Schedule	Delete a Reports iQ schedule.
Report Administrator	Administer Reports iQ reports.

Workflow iQ Task Permissions

PERMISSION NAME	GRANTS PERMISSION TO:
View Workflow	View workflow maps.
Workflow Administration	Create, publish, and delete a workflow.
Add To Workflow	Manually add document to a workflow.
Withdraw From Workflow	Manually remove document from a workflow.
Ad Hoc Route Document	Move a document from one workflow task to another workflow task on an ad hoc basis.
View Document History	View the document workflow history.
Send Back Document	Return a document to its previous workflow task.
Clear Error/Remove Hold/Change Priority/Change Deadline	Change a document's status (clear an error or remove a hold), priority or deadline.
Create/Modify Finishing Touches and Rule Tokens	Create, modify and delete workflow finishing touch rules and rule tokens.
Bulk Workflow Done	Mark multiple workflow documents as "Done".
View Workflow Document Properties	View workflow status information when viewing document properties in FDD.
Modify/Delete from Version History	Modify and delete versions from a workflow's version history.

Resource Permissions

Resource permissions determine which groups and users can access various FDD system resources. There are three main resources in FDD: bins, file cabinets and workflow tasks.

Tip: It is recommended to grant groups resource permissions on file cabinets, instead of individual users. Managing at the group level is easier than changing multiple users' permissions.

There are five types of resource permissions:

PERMISSION NAME	GRANTS PERMISSION TO:
Search	Controls the ability to retrieve batches, documents or folders.
View	Controls the ability to view batches, documents or folders.
Insert	Controls the ability to add new batches, documents or folders.
Update	Controls the ability to modify index values (for documents or folders).
Delete	Controls the ability to delete or move batches, documents or folders.

Resource permissions can be granted, denied or left unset.

See [Bins](#) and [File Cabinets](#) for instructions on assigning resource permissions for bins and file cabinets. See the Feith Workflow iQ Manager User's Guide for instructions on assigning resource permissions for workflow tasks.

Document Permissions

Permissions can be controlled at the document and folder level by assigning document permission templates to documents and folders. See [Document Permission Templates](#) for more information.

Tip: It is recommended to grant groups resource permissions on documents, instead of individual users. Managing at the group level is easier than changing multiple users' permissions.

There are five types of document permissions:

PERMISSION NAME	GRANTS PERMISSION TO:
Search	Controls the ability to retrieve a batch, document or folder.
View	Controls the ability to view a batch, document or folder.
Insert	Controls the ability to add new pages or documents to a batch, document or folder.
Update	Controls the ability to modify document or folder index values.
Delete	Controls the ability to delete, move or delete pages or documents from a batch, document or folder.

Public Access is the default document permission template assignment in FDD; this template gives all users permission to retrieve, view, add to, modify and delete the document or folder. Note the user must also have the resource and task permissions required to perform these actions. It is recommended that document and folder access be set to the default value of **Public Access**.

Note: The use of document level permissions is usually not necessary. In most situations, resource permissions can be used to adequately restrict access to documents and folders; see [Resource Permissions](#) for more information.

Notes on Setting Permissions

When setting task, resource and document permissions for a user or group, the following rules apply:

- Each permission is granted, denied or unset.
- User level permission assignment overrides group level permission assignment.
- If a user is a member of two groups - one that grants a permission and another that denies the same permission - grant overrides deny.
- If a permission is unset, the value of that permission defaults to denied. So, any permission that is not assigned to the user, either at the user level or at any group level, will be denied.

For example, assume a user only belongs to the **public** group. The following chart shows whether or not the user will be allowed to view images based on the combination of user task permission assignment and the **public** group task permission assignment.

USER	PUBLIC GROUP	CAN THE USER VIEW IMAGES?
view granted	irrelevant (view can be granted, denied or unset)	YES
view denied	irrelevant (view can be granted, denied or unset)	NO
view unset	view granted	YES
view unset	view denied	NO
view unset	view unset	NO

A user must have the appropriate combination of task, resource and document permission assignments in order to perform a task in FDD. For example, in order to be able to delete batches from a bin, a user must have both the delete batches task permission and the delete resource permission for the bin.

Tip: It is recommended to set task permissions at the group level, instead of the user level, as well as grant groups resource permissions on file cabinets and documents, instead of individual users. Managing at the group level is easier than changing multiple users' permissions.

Database Roles

The databases supported by FDD - Oracle and MS SQL Server - have different sets of rules governing access privileges. In Feith Control Panel, the user's database privileges are set as the **Database Role** on the [user properties](#) tab when adding or modifying a user.

The **Feith Admin** role grants the privileges needed to create users and tables in the database, allowing for an administrative user other than the **fdd** user who can create users and file cabinets.

See [FCP Module Access](#) for a chart showing the combination of permissions required to run each Feith Control Panel module.

Database Roles on Oracle and MS SQL Server

ROLE	HIERARCHY	GRANTS PERMISSION TO:
Feith Admin	Highest	<p>Create users and tables within the database.</p> <p>This permission is required to run the following Feith Control Panel modules:</p> <ul style="list-style-type: none"> • Document Permissions • File Cabinet Administrator • Group Administrator • Lookup Table Administrator • User Access Restrictions • User Administrator • Virtual File Cabinet Administrator
Feith Connect	Lowest	<p>Connect to the database.</p> <p>This is the default database user type for new users created in Feith Control Panel.</p>

Also:

- MS SQL Server has one more role called **Feith Connect with DB Owner** which can connect to the database outside of FDD applications; for example, when using a SQL management tool.
- Note that the **fdd** user has the **Feith Admin** (on Oracle) / **Database Admin** (on MS SQL Server) database role, as required to allow this user to create users and tables. This setting cannot be changed for the **fdd** user.

Consult your database documentation for more information on roles and privileges within your particular database.

Levels of Administrators

Feith Control Panel supports two levels of administrators: **Super Administrator** and **Mid-Level Administrator**.

CHARACTERISTICS	SUPER ADMINISTRATOR	MID-LEVEL ADMINISTRATOR
Authority	A super administrator has the highest administrative authority in the FDD system.	A mid-level administrator has less authority than a super administrator, but can perform limited administrative tasks.
Configuration	A user with the Super Administrator option turned on in the user's Properties tab.	A user who is <i>not</i> a super administrator but is a member of an administrator group. An administrator group has the Administrator Group option turned on in the group's Properties tab.
Objects	A super administrator can maintain <i>all</i> file cabinets and groups.	A mid-level administrator can maintain a <i>subset</i> of file cabinets and groups to which they have been assigned. The administrator group is assigned in the file cabinet's properties or group's Administered By tab.
Additional Privileges	A super administrator can do certain tasks that no one else can.	A mid-level administrator has no special privileges.

Notes:













- All administrators are still restricted by the [task permissions](#) they are granted at the [group](#) or [user](#) level. For example, even if a super administrator can always see all file cabinets in the list they still must have the **Modify/Delete File Cabinets** task permission in order to modify or delete file cabinets, otherwise those options will be disabled.
- Some actions are not permitted, even for a super administrator with all task permissions. For example, users cannot be removed from the public group, the public group cannot be deleted, and system file cabinets cannot be deleted.

Why Use Mid-Level Administrators?

This feature may be beneficial for sites running two or more separate applications, such as Accounts Payable and Human Resources. An administrator group can be created for each department, so that the administrators of a department will only be able to maintain the file cabinets and groups within that department. This allows the super administrator to delegate limited power to mid-level administrators who will maintain their own objects without calling on the super administrator.

Detailed Comparison of Super Administrators and Mid-Level Administrators

ACTION	SUPER ADMINISTRATOR	MID-LEVEL ADMINISTRATOR
 Assign resource permission to bin	A super administrator can assign bin resource permissions to any group or user.	A mid-level administrator can assign bin resource permissions to any group but not to any users.
 Assign resource permission to document permission template	A super administrator can assign document permission template resource permissions to any group or user.	A mid-level administrator can assign document permission template resource permissions to any group but not to any users.
 Use FDD Check	Only a super administrator can use the FDD Check module.	A mid-level administrator cannot perform this action.
 Modify or delete file cabinet	A super administrator can modify and delete any file cabinet.	A mid-level administrators can modify and delete only file cabinets they administer.
 Assign resource permissions to file cabinet	A super administrator can assign file cabinet resource permissions to any group or user.	A mid-level administrator can assign file cabinet resource permissions to any group but not to any users.
 Assign administrator group to file cabinet	A super administrator can assign any administrator group to a file cabinet.	A mid-level administrator can assign only administrator groups of which they are a member to a file cabinet.
 Perform high-level administrator functions on file cabinets	Only a super administrator can validate file cabinet options.	A mid-level administrator cannot perform this action.
 Modify or delete group	A super administrator can modify and delete any group.	A mid-level administrator can modify and delete only groups they administer.
 Add and remove users to and from a group	A super administrator can add and remove users to and from any group.	A mid-level administrator can add and remove users to and from only groups they administer.
 Grant task permissions to a group	A super administrator can grant any task permission to a group.	A mid-level administrator can grant task permissions only at the group level and can grant only task permissions that they possess.
 Assign administrator group to a group	A super administrator can assign any administrator group to a group.	A mid-level administrator can assign only administrator groups of which they are a member to a group.
 Add administrator group	Only a super administrator can add an administrator group.	A mid-level administrator cannot perform this action.






 Modify or delete leap	A super administrator can modify or delete any leap.	A mid-level administrator can modify or delete only leaps whose Access Group they administer.
 Modify or delete messages	A super administrator can modify or delete any message.	A mid-level administrator can modify or delete only messages whose Access Group they administer.
 Modify system preferences	Only a super administrator can modify system preferences.	A mid-level administrator cannot perform this action.
 Assign administrative database role to user	Only a super administrator can assign the Feith Admin (Oracle) and Database Admin (MS SQL Server) database roles to a user.	A mid-level administrator cannot perform this action.
 Add another super administrator	Only a super administrator can add another super administrator.	A mid-level administrator cannot perform this action.
 Add and remove users to and from a group	A super administrator can add and remove users to and from any group.	A mid-level administrator can add and remove users to and from only groups they administer.
 Grant task permissions to a user	Only a super administrator can grant task permissions at the user level.	A mid-level administrator cannot perform this action.
 Delete a user	A super administrator can delete any user.	A mid-level administrator can delete a user only if they administer <i>all</i> groups to which the user belongs.
 Perform high-level administrator functions on users	Only a super administrator can administer passwords, administer proxy users, delete users en masse, and convert users to external authentication en masse.	A mid-level administrator cannot perform these actions.
 Build virtual file cabinet on a file cabinet	A super administrator can build a virtual file cabinet on any file cabinet.	A mid-level administrator can build a virtual file cabinet only on file cabinets they administer.
 Modify or delete virtual file cabinet	A super administrator can modify and delete any virtual file cabinet.	A mid-level administrator can modify and delete only virtual file cabinets they administer.
 Assign resource permissions to virtual file cabinet	A super administrator can assign virtual file cabinet resource permissions to any group or user.	A mid-level administrator can assign virtual file cabinet resource permissions only to groups they administer.

FCP Module Access

You can set up administrators to use some modules but not others using a combination of the following settings:

- **Database Role:** A user is assigned a database role - for Oracle or MS SQL Server - which has a set of rules governing access privileges in the database. There is a hierarchy of database roles, with some roles having more powers than others. See [Database Roles](#) for more information.
- **Super Admin or Mid-Level Admin:** A user is either a super administrator with access to all objects and privileges, or a mid-level administrator with limited powers. See [Levels of Administrators](#) for more information.
- **Task Permissions:** Certain task permissions are required to access specific FCP modules. Task permissions are set at the [group](#) or [user](#) level.

The combinations of settings required to use each module are listed below. Change the settings to control which administrators can access which modules in FCP and what they can do.

FCP MODULE	MINIMUM DATABASE ROLE	REQUIRED ADMIN LEVEL	REQUIRED TASK PERMISSIONS
 Bins	Feith Connect	Super administrator or mid-level administrator. A mid-level administrator has limited powers .	Create Bins Modify/Delete Bins
 Classifications	Feith Connect	(none)	Administer Classifications
 Database Statistics	Feith Connect	(none)	(none)
 Document Permissions	Feith Admin (Oracle) or Database Admin (MS SQL Server)	Super administrator or mid-level administrator. A mid-level administrator has limited powers .	Create Document Permission Templates Modify/Delete Document Permission Templates
 FDD Check	Feith Connect	Super administrator only	(none)

 File Cabinets	Feith Admin (Oracle) or Database Admin (MS SQL Server)	Super administrator or mid-level administrator. A mid-level administrator has limited powers .	Create File Cabinets Modify/Delete File Cabinets
 Full Text	Feith Connect	(none)	Administer Autonomy IDOL Rebuild Full Text Database
 Groups	Feith Admin (Oracle) or Database Admin (MS SQL Server)	Super administrator or mid-level administrator. A mid-level administrator has limited powers .	Create Groups Modify/Delete Groups
 Leaps	Feith Connect	Any administrator. A mid-level administrator has limited powers .	Create/Modify Leaps
 Licenses	Feith Connect	(none)	(none)
 Locks	Feith Connect	(none)	Unlock Batches Unlock Documents
 Lookup Tables	Feith Admin (Oracle) or Database Admin (MS SQL Server)	(none)	Create/Modify Lookup Tables
 Messages	Feith Connect	Any administrator. A mid-level administrator has limited powers .	Create/Modify Messages
 Redaction Reason Code	Feith Connect	(none)	Create/Modify Redaction Codes
 Servers	Feith Connect	(none)	Maintain Servers

 States and Reasons	Feith Connect	(none)	Administer States and Reasons
 Supplemental Markings	Feith Connect	(none)	Administer Supplemental Markings
 System Info	Feith Connect	Super administrator only	(none)
 User Access Restrictions	Feith Admin (Oracle) or Database Admin (MS SQL Server)	(none)	Administer Access Restrictions
 Users	Feith Admin (Oracle) or Database Admin (MS SQL Server)	Any administrator. A mid-level administrator has limited powers .	Create Users Modify/Delete Users
 View Builder	Feith Admin (Oracle) or Database Admin (MS SQL Server)	(none)	Create/Modify Feith Views
 Virtual File Cabinets	Feith Admin (Oracle) or Database Admin (MS SQL Server)	Super administrator or mid-level administrator. A mid-level administrator has limited powers .	Create File Cabinets Modify/Delete File Cabinets

Audit Events

The following instructions apply only if your FDD system is licensed for FDD Auditor.

If your FDD system is licensed for **FDD Auditor**, you can configure which audit events to track for which FDD users and/or groups.

When an audit event is selected for a user, an entry is written to the **FDD Audit Trail** each time the user performs the action. For example, if the audit event **View Page** is selected for the **Jane Smith** user, then an audit entry is written each time Jane Smith views a page. The audit data includes the user's internal ID, the name of the action performed, and the date and time the action was performed. Audit reports and graphs are viewed in the **FDD Auditor iQ** application; see the **Auditor iQ** documentation for more information on viewing audit data.

Audit events can be turned on at both the user level and at the group level. For instructions on configuring audits at the user level, see [Set User Audit Events for FDD Auditing](#). For instructions on configuring audits at the group level, see [Set Group Audit Events for FDD Auditing](#).

The following tables list the audit events that can be tracked in the FDD system:

- [General User Audit Events](#)
- [Workflow User Audit Events](#)
- [RMA User Audit Events](#)
- [Feith Control Panel Audit Events](#)
- [Workflow iQ Manager Audit Events](#)
- [RMA iQ Administrator Audit Events](#)
- [Quick Integrator \(QI\) Audit Events](#)
- [Feith Developer Audit Events](#)
- [Reports iQ Audit Events](#)

General User Audit Events

AUDIT NAME	ACTION AUDITED
Check In Document	Check in a new version of a document.
Check Out Document	Check out a version of a document.
Create Document Note	Create a document note.
Create Page Note	Create a page note.

Create Redaction	Create a redaction note.
DDE Requests	Issue an FDD DDE request. Typically done when using the Quick Integrator application.
Delete Batch	Delete a batch.
Delete Document	Delete a document.
Delete Document Note	Delete a document note.
Delete Page	Delete a page.
Delete Page Note	Delete a page note.
Delete Redaction	Delete a redaction note.
Email Document	Email a document.
Email Page	Email a page.
Export Document	Export a document.
Export Page	Export a page.
Import Document	Import a document.
Import Page	Import a page.
Index Document	Index a document.
Index Page	Index a page.
Lock Batch	Lock a batch.
Logoff	Logoff. Log out of an FDD application.
Logon	Logon. Login to an FDD application.
Modify Document Note	Modify a document note.
Modify Index Values	Modify a document's indexing values (file cabinet field values).
Modify Page Note	Modify a page note.

Modify Redaction	Modify a redaction note.
Print Document	Print a document.
Print Document Note	Print a document note.
Print Page	Print a page.
Print Page Note	Print a page note.
Replace Page	Replace a page.
Route (Copy) Documents	Route a document to a batch, leaving the original document.
Route (Copy) Pages	Route a page to a batch, leaving the original page.
Route (Move) Document	Route a document to a batch, deleting the original document.
Route (Move) Page	Route a page to a batch, deleting the original page.
Scan Batch	Scan a document.
Scan Page	Scan a page.
Search for a Document	Search for a document.
Unlock Batch	Unlock a batch.
View Document	View a document.
View Document Note	View a document note.
View Page	View a page.
View Page Note	View a page note.

Workflow User Audit Events

AUDIT NAME	ACTION AUDITED
Finish Work in Workflow Task	Finish (“Done”) a document in a workflow task.
Route Work in Workflow Task	Route a document from one workflow task to another workflow task.

Skip Work in Workflow Task	Skip a document in a workflow task.
Withdraw Work from Workflow Task	Withdraw a document from a workflow task.

RMA User Audit Events

AUDIT NAME	ACTION AUDITED
Assign Category to Document	Assign a category to a document.
Assign Country to Document	Assign a country to a document.
Assign Marking to Document	Assign a supplemental marking to a document.
Assign State to Document	Assign a state to a document.
Classification Attribute Update	Update the classification attribute of a document (i.e., change the classification assigned to a document).
Document Property Modification	Modify the RMA document properties assigned to a document.
Remove Category from Document	Remove a category from a document.
Remove Country from Document	Remove a country from a document.
Remove Marking from Document	Remove a supplemental marking from a document.
Remove State from Document	Remove a state from a document.

Feith Control Panel Audit Events

AUDIT NAME	ACTION AUDITED
Add File Cabinet	Create a new file cabinet.
Add File Cabinet Field	Add a new file cabinet field.
Add Group	Create a new group.
Add User	Create a new user.
Add View via FCP Feith View	Add view in the View Builder.

Builder	
Add Virtual File Cabinet	Create a new virtual file cabinet.
Change a User's Assigned Clearance Level	Change a user's assigned clearance level.
Change a User's List of Assigned Supplemental Markings	Change a user's list of assigned supplemental markings.
Create a Classification	Create a new classification.
Create a New State/Reason	Create a new state/reason.
Create a Supplemental Marking	Create a new supplemental marking.
Delete a Classification	Delete a classification.
Delete a State	Delete a state.
Delete a Supplemental Marking	Delete a supplemental marking.
Delete File Cabinet	Delete a file cabinet.
Delete File Cabinet Field	Delete a file cabinet field.
Delete Group	Delete a group.
Delete User	Delete a user.
Delete View via FCP Feith View Builder	Delete view in the View Builder.
Disable User Account	Disable a user account.
Enable User Account	Enable a user account.
Modify a Classification	Modify a classification.
Modify a Supplemental Marking	Modify a supplemental marking.
Modify an Existing State/Reason	Modify an existing state/reason.
Modify File Cabinet	Modify a file cabinet.
Modify File Cabinet Field	Modify a file cabinet field.

Modify File Cabinet Permissions	Modify file cabinet permissions.
Modify Group	Modify a group.
Modify Group Membership	Modify group membership.
Modify User	Modify a user.
Modify User or Group Permissions	Modify user or group permissions.
Modify View via FCP Feith View Builder	Modify view in View Builder.
Update Fiscal Year Start Day via FCP System Preferences	Update the fiscal year start day in the System Preferences module.
Update RMA Mode via FCP System Preferences	Update the RMA Mode in the System Preferences module.
Add Bin	Add a bin.
Modify Bin	Modify a bin.
Modify Bin Perms	Modify bin permissions.
Delete Bin	Delete a bin.

Workflow iQ Manager Audit Events

AUDIT NAME	ACTION AUDITED
Add Workflow	Create a new workflow.
Delete Workflow	Delete a workflow.
Modify Workflow	Modify a workflow.
Modify Workflow Permissions	Modify workflow permissions.

RMA iQ Administrator Audit Events

AUDIT NAME	ACTION AUDITED
------------	----------------

Add a Category	Create a new category.
Create an Event	Create a new event.
Delete a Category	Delete a category.
Delete an Event	Delete an event.
Modify a Category	Modify a category.
Modify an Event	Modify an event.

Quick Integrator (QI) Administrator Audit Events

AUDIT NAME	ACTION AUDITED
Add QI Capture Pattern	Add a QI capture pattern.
Add QI Tool	Add a QI tool.
Delete QI Capture Pattern	Delete a QI capture pattern.
Delete QI Tool	Delete a QI tool.
Modify QI Capture Pattern	Modify a QI capture pattern.
Modify QI Tool	Modify a QI tool.
Run QI Tool	Run a QI tool.
Run Script in Tool Editor	Run script in the QI tool editor.

Feith Developer Audit Events

AUDIT NAME	ACTION AUDITED
Add Developer Object	Add a Feith Developer object.
Modify Developer Object	Modify a Feith Developer object.
Delete Developer Object	Delete a Feith Developer object.

View Developer Object	View a Feith Developer object.
------------------------------	--------------------------------

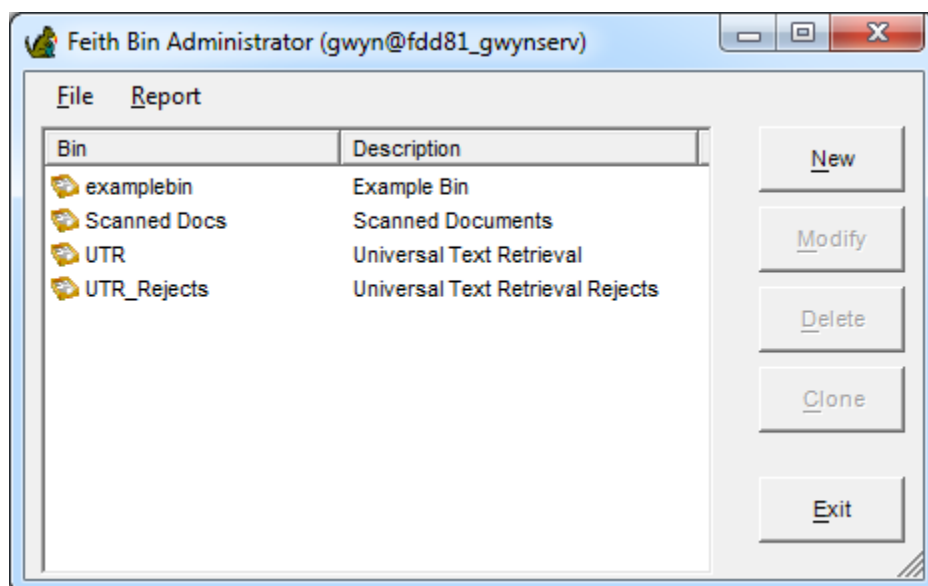
Reports iQ Audit Events

AUDIT NAME	ACTION AUDITED
Add Reports iQ Template	Add a Reports iQ template.
Add Reports iQ Schedule	Add a Reports iQ schedule.
Modify Reports iQ Template	Modify a Reports iQ template.
Modify Reports iQ Schedule	Modify a Reports iQ schedule.
Delete Reports iQ Template	Delete a Reports iQ template.
Delete Reports iQ Schedule	Delete a Reports iQ schedule.
Purge Reports iQ Template	Purge a Reports iQ template.
Purge Reports iQ Schedule	Purge a Reports iQ schedule.

Bins

Bins

A **bin** is a temporary storage area for batches waiting to be indexed; separate bins can be created to organize batches.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

System Bins

The **examplebin** bin is created during the FDD installation. These bins are created for use with FDD applications and cannot be deleted.

Add Bin

To add a bin:

1. Select **File>Bins**. The **Feith Bin Administrator** opens.
2. Click **New**. The **Add New Bin** screen opens.
3. On the **Properties** tab, enter the bin properties:

Name: Enter the bin name. A maximum of 16 characters is accepted.

Description: Enter the bin description. A maximum of 64 characters is accepted.

Storage Server: Choose an optical server from the list. All images acquired into the bin are stored on this server.

Volume: Optionally enter the optical volume.

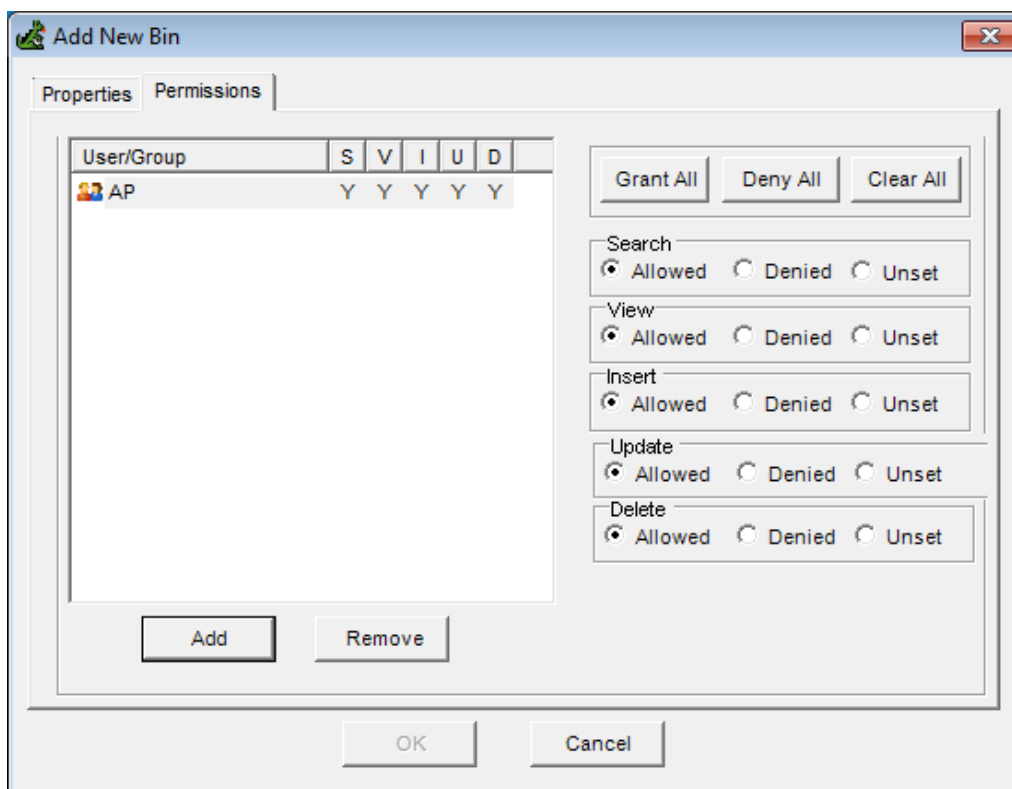
Full-Text Index: Optionally choose to automatically full text index all batches in this bin.

The screenshot shows a window titled "Add New Bin" with a close button in the top right corner. It has two tabs: "Properties" and "Permissions". The "Properties" tab is active. It contains the following fields:

- Name:** A text box containing "Invoices".
- Description:** A text box containing "Scanned Invoices".
- Storage Server:** A dropdown menu with a server icon on the left and a downward arrow on the right.
- Volume:** An empty text box.
- Full-Text Index:** A checkbox that is currently unchecked.

At the bottom of the window are two buttons: "OK" and "Cancel".

4. Select the **Permissions** tab and assign permissions as needed. Resource permissions are unset by default.



To grant permissions to a group or user:

- Click **Add**. The **Users/Groups** screen opens, listing all FDD groups and users to which you have administrative access.
- Select a group or user in the list and click **OK**. The selected group or user is granted permissions to the bin. By default, all five resource permissions - **Search**, **View**, **Insert**, **Update** and **Delete** - are granted to the group or user.
- Change the permissions as desired.

Tip: You can select multiple groups/users in the list and change all their permissions at once.

To modify the permissions assigned to a group or user:

- Select a group or user in the permissions list. Change the setting for a single permission by toggling between the **Allowed**, **Denied** and **Unset** options, or use the **Grant All**, **Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the group or user.

Tip: You can select multiple groups/users in the list and change all their permissions at once.

To revoke permissions from a group or user:

- Select a group or user in the permissions list and click **Remove**. All permissions to the bin are revoked from the group or user.

- Click **OK**. The bin is created and you are returned to the **Feith Bin Administrator**.

Modify Bin

To modify bin properties:

1. Select **File>Bin**. The **Feith Bin Administrator** opens.
2. Select a bin and click **Modify**. The **Modify Bin** screen opens.
3. Change properties as needed and click **OK**. The bin is modified and you are returned to the **Feith Bin Administrator**.

To modify bin permissions:

1. Select **Bins** from the **File** menu. The **Feith Bin Administrator** opens.
2. Select a bin and click **Modify**. The **Modify Bin** screen opens.
3. Select the **Permissions** tab.
4. Modify permissions as needed.

Note: A mid-level administrator is limited in who they can assign resource permission to a bin. See [Levels of Administrators](#) for more information.

- To grant permissions to a group or user:
 - a. Click **Add**. The **Users and Groups** screen opens, listing all FDD groups and users to which you have administrative access.
 - b. Select a group or user in the list and click **OK**. The selected group or user is granted permissions to the bin and is added to the permissions list. By default, all five resource permissions - **Search**, **View**, **Insert**, **Update** and **Delete** - are granted to group or user.
 - To modify the permissions assigned to a group or user:
 - Select a group or user in the permissions list. Change the setting for a single permission by toggling between the **Allowed**, **Denied** and **Unset** options, or use the **Grant All**, **Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the group or user.
 - To revoke permissions from a group or user:
 - Select a group or user in the permissions list and click **Remove**. All permissions to the bin are revoked from the group or user.
5. Click **OK**. You are returned to the **Modify Bin** screen.
 6. Click **Exit** to return to the **Feith Bin Administrator**.

To full text index all batches in a bin:

1. Select **Bins** from the **File** menu. The **Feith Bin Administrator** opens.
2. Right-click the desired bin and select **Full-Text Index Existing Batches**.
3. Click **Yes** to the prompt. All the batches currently in the bin will be full text indexed the next time Feith UTR runs.

Note that this action does not change the **Full-Text Index** setting in the bin's properties. To change the **Full-Text Index** setting:

1. Select a bin and click **Modify**. The **Modify Bin** screen opens.
2. Check the **Full-Text Index** checkbox.
3. Click **OK**. You will be prompted as to whether you want to full text index all the existing batches in the bin.
4. Answer the prompt and you are returned to the **Modify Bin** screen. Click **Exit** to return to the **Feith Bin Administrator**.

To remove existing full-text-indexed batches in a bin from full text search:

1. Select **Bins** from the **File** menu. The **Feith Bin Administrator** opens.
2. Right-click the desired bin and select **Remove Existing Batches from Full-Text Index**.
3. Click **Yes** to the prompt. All the batches currently in the bin will be removed from the full text search the next time Feith UTR runs.

Note that this action does not change the **Full-Text Index** setting in the bin's properties. To change the **Full-Text Index** setting:

1. Select a bin and click **Modify**. The **Modify Bin** screen opens.
2. Uncheck the **Full-Text Index** checkbox.
3. Click **OK**. You will be prompted as to whether you want to remove all the existing batches in the bin from full text search.
4. Answer the prompt and you are returned to the **Modify Bin** screen. Click **Exit** to return to the **Feith Bin Administrator**.

Clone Bin

To clone an existing bin:

1. Select **File>Bins**. The **Feith Bin Administrator** opens.
2. Select a bin and click **Clone**. The **Add New Bin** screen opens; the optical server selection and resource permissions are copied over from the original bin.

If you are logged in as an administrator group member, resource permissions are only copied over for the groups you administer.

3. On the **Properties** tab, enter the following properties for the new bin:
 - **Name:** Enter the bin name. A maximum of 16 characters is accepted.
 - **Description:** Enter the bin description. A maximum of 64 characters.
 - **Optical Server:** Choose an optical server from the list. All images acquired into this bin are stored on this server.
 - **Optical Volume:** Optionally enter the optical volume.
 - **Full-Text Index:** Optionally choose to automatically full text index all batches in this bin.
4. Optionally select the **Permissions** tab and modify the resource permissions.

Note: A mid-level administrator is limited in who they can assign resource permission to a bin. See [Levels of Administrators](#) for more information.

5. Click **OK**. The new bin is created and you are returned to the **Feith Bin Administrator**.

Delete Bin

You must delete all documents from a bin before you can delete the bin in FCP. If you attempt to delete a bin that contains documents, the delete will fail.

To delete a bin:

1. Select **File>Bin**. The **Create/Maintain Bins** screen opens.
2. Select a bin and click **Delete**.

Note: The FDD system bins cannot be deleted.

3. Answer **Yes** to the confirmation prompt. The bin is deleted.

Bin Reports

Two file cabinet reports are available: **Selected Bin** and **All Bins**.

The **Selected Bin** report lists the bin properties and resource permission assignments.

The **All Bins** report lists all bins by name and description.

To generate a bin report:

1. Select **File>Bins**. The **Feith Bin Administrator** opens.
2. Optionally select a bin.
3. Select the **Report** menu and choose either the **Selected Bin** or **All Bins** report option. The report opens in a browser window.

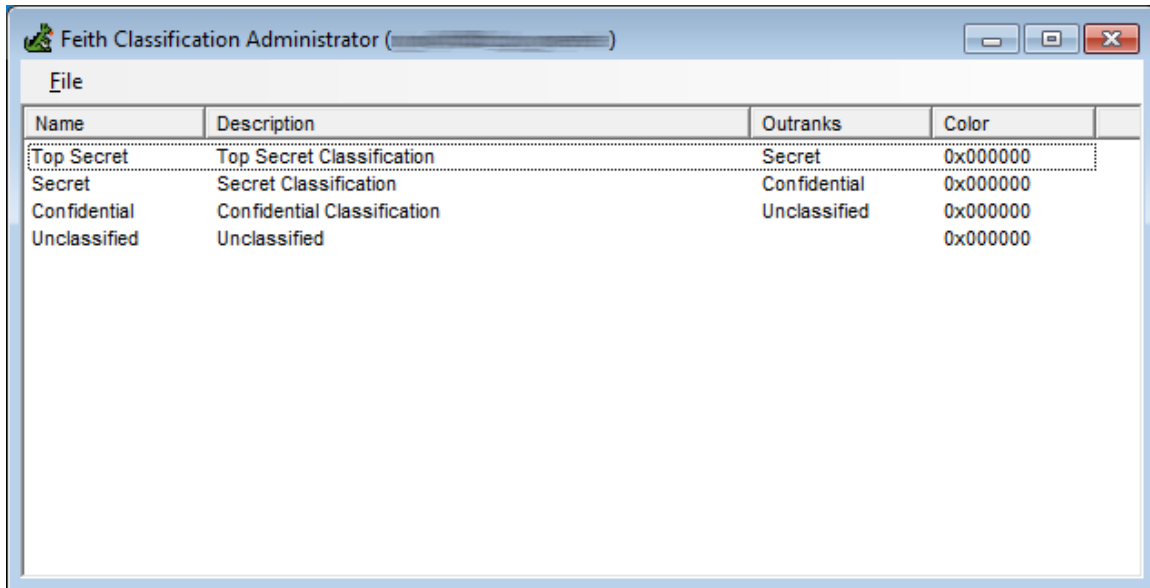
Classifications

Classifications

The following instructions apply only if your FDD system is licensed for RMA iQ.

Use **Classifications** to create and maintain record classification levels. The default classifications are **Confidential**, **Secret**, and **Top Secret**. Classifications are hierarchical: Top Secret outranks Secret which outranks Confidential.

To access a record that has a classification, a user must have a clearance level that is at or above the classification level assigned to the record. User clearances are set in the **Users** module under the [Clearances](#) tab.



The screenshot shows a window titled "Feith Classification Administrator". Inside, there is a table with the following data:

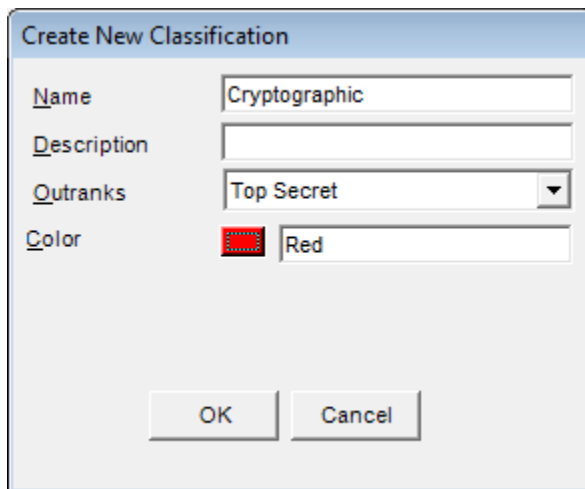
Name	Description	Outranks	Color
Top Secret	Top Secret Classification	Secret	0x000000
Secret	Secret Classification	Confidential	0x000000
Confidential	Confidential Classification	Unclassified	0x000000
Unclassified	Unclassified		0x000000

Add Classification

The following instructions apply only if your FDD system is licensed for RMA iQ.

To add a classification:

1. Select **File>Classifications**. The **Feith Classification Administrator** opens.
2. Click **File>New**. The **Create New Classification** dialog opens.
3. Enter a classification **Name**.
4. Optionally enter a **Description**.
5. Choose the classification that this new classification **Outranks**.
6. Optionally set a **Color** to represent the classification throughout the FDD system in various applications.



7. Click **OK**. The classification is created and you are returned to the **Feith Classification Administrator**.

Manage Classifications

The following instructions apply only if your FDD system is licensed for RMA iQ.

Modify Classification

To modify a classification:

1. Select **File>Classifications**. The **Feith Classification Administrator** opens.
2. Select a classification and click **File>Modify**. The **Modify Classification** dialog opens.
3. Make changes as desired, except to the **Outranks** setting which cannot be modified.
4. Click **OK** to save your changes.

Delete Classification

To delete a classification:

1. Select **File>Classifications**. The **Feith Classification Administrator** opens.
2. Select a classification and click **File>Delete**. You are prompted to confirm the deletion.
3. Click **Yes** to continue. The classification is deleted.

Note: Standard classifications that are included with Feith Control Panel cannot be deleted. Classifications that are assigned to documents also cannot be deleted.

Export and Import Classifications

The following instructions apply only if your FDD system is licensed for RMA iQ.

Export Classification

To export a classification:

1. Select **File>Classifications**. The **Feith Classification Administrator** opens.
2. Select a classification and click **File>Export**. The **File Save** dialog opens.

You can select multiple classifications using **SHIFT+click** or **CTRL+click**.
3. Browse to select a destination path and file name for the classification export file, then click **Save**. The classification is exported to a .csv file.

Import Classification

To import a classification:

1. Select **File>Classifications**. The **Feith Classification Administrator** opens.
2. Click **File>Import**. The **File Open** dialog opens.
3. Browse to select the classification file and click **Open**. The classification is imported and the **Import Complete** dialog displays the number of classifications that required updating.
4. Click **OK**. You are returned to the **Feith Classification Administrator**. The imported classification is included in the classification list.

Database Statistics

Database Statistics

The **database statistics** show the current counts of documents, pages, batches, folders, users, groups, file cabinets and bins.

To view database statistics:

1. Select **File>Database Statistics**. The **Database Statistics** screen opens.

Total Number Of			
Documents:	1066	Pages:	1149
Batches:	38	Folders	5
Users:	12	Groups:	10
Deleted Users	2	Deleted Groups	0
True FCs:	35	Bins:	5
Virtual FCs:	8	Workflows:	36
Tasks:	161	WF Users:	4

Number Of	
Documents and Folders:	File Cabinet or Task: Expense Approval 1
Batches:	Bin: Scanned Docs 6

Export Exit

The top portion of the window displays the total number of documents, pages, batches, folders, users, groups, deleted users, deleted groups, file cabinets and bins in the database.

2. In the bottom portion of the screen, select a file cabinet or bin from the drop-down lists to view the number of documents it holds.
3. Select **File>Refresh** to refresh the statistics if needed.

To export the statistics to file:

1. Select **File>Database Statistics**. The **Database Statistics** screen opens.
2. Either click the **Export** button or select **File>Export**. The **Save As** dialog opens.
3. Browse to select the destination path and file name and click **Save**. The statistics are exported to a .txt file. Note that it may take some time to generate the report.

Document Permissions

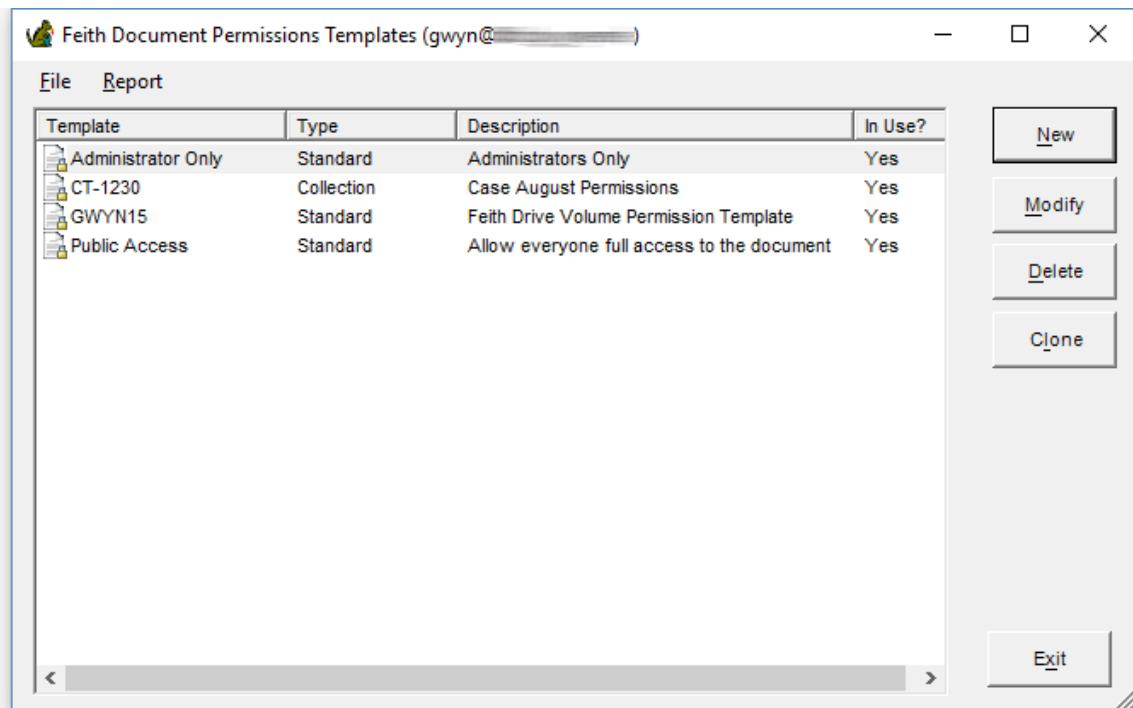
Document Permission Templates

Document permission templates control permissions at the document and folder level.

Public Access is the default document permission template assignment in FDD; this template gives all users permission to retrieve, view, add to, modify and delete the document or folder. Note the user must also have the resource and task permissions required to perform these actions.

Document permission templates are assigned to documents and folders in FDD during indexing. It is recommended that document and folder access be set to the default value of **Public Access**.

Note: The use of document level permissions is usually not necessary. In most situations, resource permissions can be used to adequately restrict access to documents and folders. See [Resource Permissions](#) for more information.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

Add Document Permission Template

To add a document permission template:

1. Select **File>Document Permissions**. The **Feith Document Permission Templates** screen opens.
2. Click **New**. The **Add New Document Permission Template** screen opens.
3. Enter a **Name** (maximum 64 characters).
4. Enter a **Description** (maximum 64 characters).
5. Assign permissions as needed. Permissions are unset by default.

Note: A mid-level administrator is limited in who they can assign resource permission to a document permission template. See [Levels of Administrators](#) for more information.

- To grant permissions to a group or user:
 - a. Click **Add**. The **Users and Groups** screen opens, listing all FDD groups and users to which you have administrative access.
 - b. Select a group or user in the list and click **OK**. The selected group or user is granted permissions to the document permission template. By default, all five resource permissions - **Search, View, Insert, Update** and **Delete** - are granted to the group or user.
 - c. Change permissions as desired.

Tip: You can select multiple groups/users in the list and change all their permissions at once.

- To modify the permissions assigned to a group or user:
 - Select a group or user in the permissions list. Change the setting for a single permission by toggling between the **Allowed, Denied** and **Unset** options, or use the **Grant All, Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the group or user.

Tip: You can select multiple groups/users in the list and change all their permissions at once.

- To revoke permissions from a group or user:
 - Select a group or user in the permissions list and click **Remove**. All permissions to the document permission template are revoked from the group or user.
3. Click **OK**. The document permission template is created and you are returned to the **Feith Document Permission Templates** screen.

Manage Document Permission Templates

Modify Document Permission Template

To modify a document permission template:

1. Select **File>Document Permissions**. The **Feith Document Permission Templates** screen opens.
2. Select a template and click **Modify**. The **Modify Permission Template** screen opens.
Note: The **Public Access** permission template cannot be modified.
3. Change any property and click **OK**. The template is modified and you are returned to the **Feith Document Permission Templates** screen.

Clone Document Permission Template

To clone a document permission template:

1. Select **File>Document Permissions**. The **Feith Document Permission Templates** screen opens.
2. Select a template and click **Clone**. The **Add New Document Permissions Template** screen opens; the **Permissions** assignments are copied from the original template.

If you are logged in as an administrator group member, resource permissions are only copied over for the groups you administer.
3. Enter a **Name**.
4. Enter a **Description**.
5. Optionally modify the resource permissions.

Note: A mid-level administrator is limited in who they can assign resource permission to a document permission template. See [Levels of Administrators](#) for more information.
6. Click **OK**. The template is created and you are returned to the **Feith Document Permission Templates** screen.

Delete Document Permission Template

To delete a document permission template:

1. Select **File>Document Permissions**. The **Feith Document Permission Templates** screen opens.
2. Select a template and click **Delete**. You are prompted to confirm the delete.

Note: The **Public Access** permission template cannot be deleted.
3. Click **Yes** to continue. The template is deleted.

If the template is currently assigned to any documents, you are asked to reassign the documents to another template. Choose a template from the list and click **OK**.

Document Permission Template Reports

To get a count of how many documents are assigned the template:

- Right-click a document permission template and select **Assignment Count**. The **Assignment Count** dialog displays with the number of documents assigned to the selected template.

To report on document permission templates:

1. Select **File>Document Permissions**. The **Feith Document Permission Templates** screen opens.
2. Optionally select a document permission template.
3. Select the **Report** menu and choose from the following:
 - **Selected Permission Template - HTML**: The template properties and permission assignments.
 - **All Permission Templates - CSV**: All templates by name and description in CSV format.
 - **All Permission Templates - HTML**: All templates by name and description in HTML format.

FDD Check

FDD Check

FDD Check is used to check the validity of pages, page notes, and document notes on Feith EDStor. For example, FDD Check can be run after a hardware failure to check if the objects on EDStor are intact or if some are missing or corrupted.

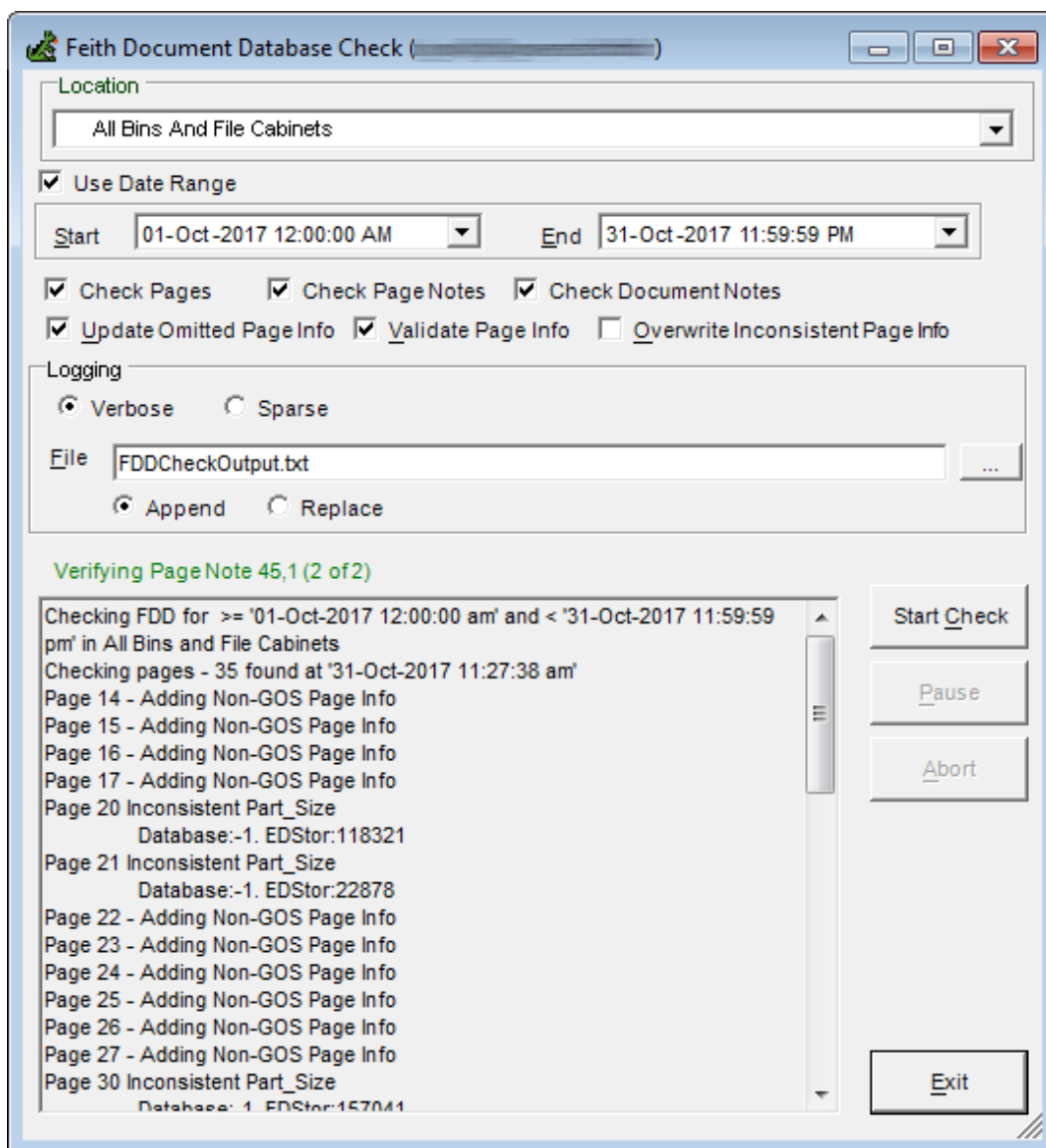
Note: When FDD Check is running it may slow down retrieval from EDStor. Therefore, it is recommended to not run FDD Check during business hours.

Run FDD Check

You must be a super administrator to use the FDD Check module.

To run FDD Check:

1. Select **File>FDD Check**. The **FDD Check** window is opened.
2. Choose the **Location**, a bin or file cabinet, where you want to check the pages and notes on EDStor. You can also check **All Bins And File Cabinets**.
3. Optionally check on **Use Date Range** and select the date and time range for which you want to run the check. FDD Check will look for pages and notes created during the selected date range.
4. Choose which objects you want to check: **Check Pages**, **Check Page Notes**, and/or **Check Document Notes**.
5. Optionally turn on additional features:
 - **Update Omitted Page Info:** Update missing page type and page information entries in the FDD database from the file information stored on EDStor.
 - **Validate Page Info:** Records in the log if there is a discrepancy discovered between the page type in the FDD database versus the page type in EDStor. For GOS pages, records in the log if there is a discrepancy between the page information entries in the FDD database versus the file information on EDStor.
 - **Overwrite Inconsistent Page Info:** For GOS pages, where there were any discrepancies found, updates page information entries in the FDD database with the file information on EDStor.
6. In the **Logging** section, choose from the following options:
 - Write a **Verbose** log, with more details. We recommend a .txt format.
 - Write a **Sparse** log, with a summary and fewer details. We recommend a .csv format.
 - Choose the desired **File** name, file extension, and location for the log.
 - Choose to **Append** to the existing log file or **Replace** the existing log file.
7. Click the **Start Check** button to begin the check. While FDD Check is running, you can **Pause** or **Abort** the check process.
8. Once the check is completed the results will display. Based on the details in FDD Check's log, you can proceed to troubleshoot any issues with the pages and notes stored on EDStor.

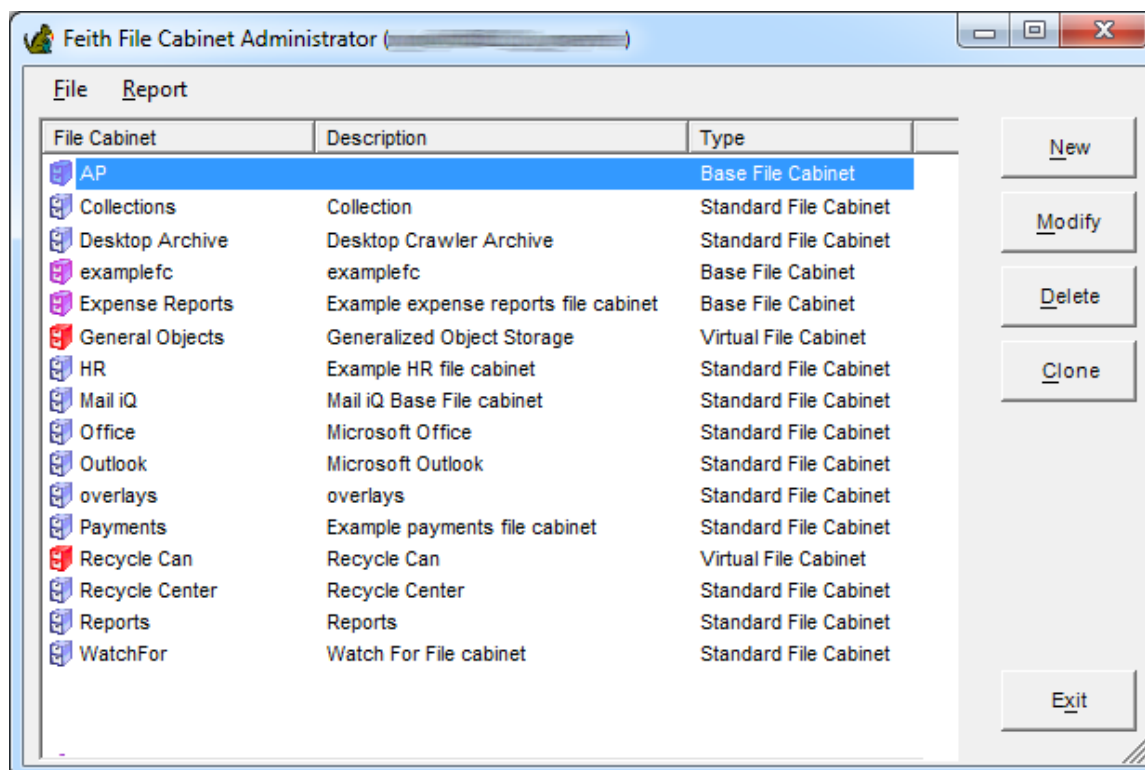


File Cabinets

File Cabinets

A **file cabinet** is a permanent storage area for indexed documents. Documents are indexed with a set of field values that identify the document, for example *Vendor*, *Amount*, *PO Number*, *Date*, and *Document Type*. Users can search for the document based on these field values.

Before creating your file cabinets, you should take some time to think about the file cabinet design to ensure it meets the needs of your organization and workers. See [Define File Cabinets](#) for more information.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

System File Cabinets

The following system file cabinets are created during the FDD installation. These file cabinets are created for use with FDD applications and cannot be deleted.

FILE CABINET	DESCRIPTION
AiQ Training Sets	Analyze iQ file cabinet
Collections	Collections file cabinet
Document Properties	RMA iQ Document Properties auxiliary file cabinet
examplefc	Sample file cabinet
FeithDrive	FeithDrive file cabinet

FeithDrive AIQ	FeithDrive file cabinet
FeithDrive Base	FeithDrive file cabinet
FeithDrive Revisions	FeithDrive file cabinet
General Objects	General Objects file cabinet
Group Properties	RMA iQ Group Properties auxiliary file cabinet
Mail iQ	Mail iQ file cabinet
My Reports	Reports iQ file cabinet
Office	Sample file cabinet for Office documents
Outlook	Sample file cabinet for Outlook documents
Overlays	Overlays file cabinet
Report Templates	Reports iQ file cabinet
Reports	Reports iQ file cabinet
Reports iQ Base	Reports iQ file cabinet
RMA iQ Change History	RMA iQ file cabinet
RMA iQ Compiled Rules	RMA iQ file cabinet
RMA iQ Event Formulas	RMA iQ file cabinet

Add File Cabinet

To add a file cabinet:

1. Select **File>File Cabinets**. The **Feith File Cabinet Administrator** opens.
2. Click **New**. The **Create New File Cabinet** wizard opens to **Step 1: Set Up File Cabinet Options**.
3. Enter the file cabinet properties:

- **Name:** The name of the file cabinet. Maximum 64 characters.
- **Description:** The description of the file cabinet. Maximum 64 characters.
- **Storage Server:** The storage server assigned to the file cabinet. Pages added directly to the file cabinet will be stored on this server.
- **Optical Volume:** The optical volume. This setting is optional.
- **Administered By:** Optionally select the administrator groups for the file cabinet.

Any assigned administrator group and all super administrators will be able to modify the file cabinet.

If you are logged in as a member of an administrator group, all administrator groups to which you belong are automatically assigned to the file cabinet.

Create New File Cabinet

Step 1: Setup File Cabinet Properties

Name

Description:

Storage Server

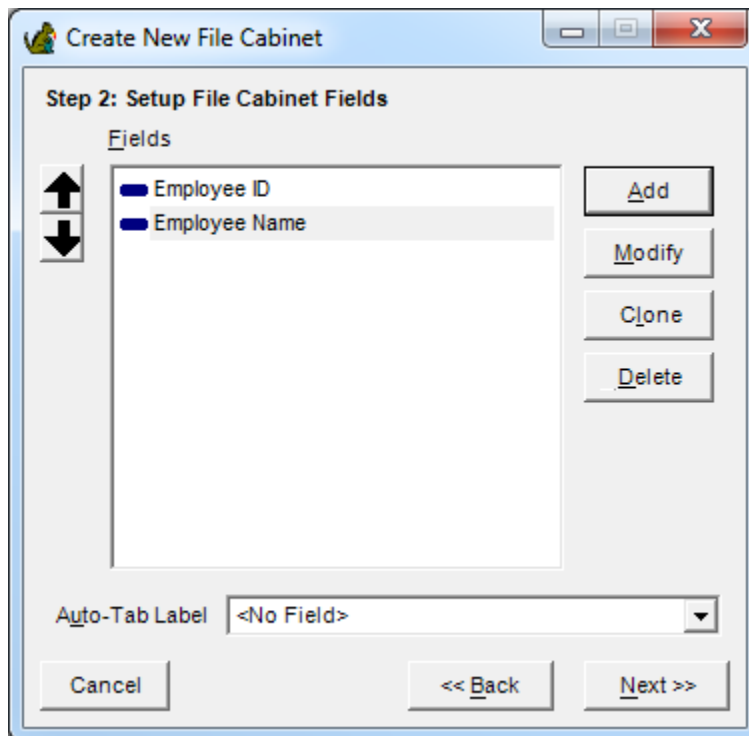
Volume

Administered By

Full-Text Index ☐

- To assign an administrator group to the file cabinet:
 - a. Click **Add Group**. The **Administrator Groups** list opens. If you are logged in as a super administrator, the list will show all administrator groups that are not currently assigned to the file cabinet. If you are logged in as an administrator group member, the list will show all administrator groups to which you belong that are not currently assigned to the file cabinet.
 - b. Select a group in the list and click **OK**. The selected group is granted administrative access to the file cabinet and is added to the **Administered By** list.
- To remove an administrator group from the file cabinet:

- Select a group in the **Administered By** list and click **Delete Group**. Administrative access is revoked from the group, and the group is removed from the **Administered By** list.
 - **Full-Text:** Optionally choose to automatically full text index all documents that are indexed into this file cabinet.
4. Click **Next**. **Step 2** of the wizard opens: **Set Up the File Cabinet Fields**.
 5. Click **Add**. The **Add New Field** screen opens. The field options are divided into three tabs: **General**, **Lookup** and **Advanced**.
- Tip:** The value for the first file cabinet field displays as the document title within FDD. Keep this in mind when creating file cabinets; the first field should be the most important or most meaningful field.
6. Enter the field options and click **OK** to add the field. See [Set File Cabinet Field Options](#) for instructions.
 7. Continue adding fields as needed. To add another field, click **Add** again. You can also clone the properties of a field you already added by selecting the desired field and clicking **Clone**. To delete a field, select the field and click **Delete**.



8. After you have finished adding fields, click **Next** to continue creating the file cabinet. The next step in file cabinet creation varies depending on what database you are running on.

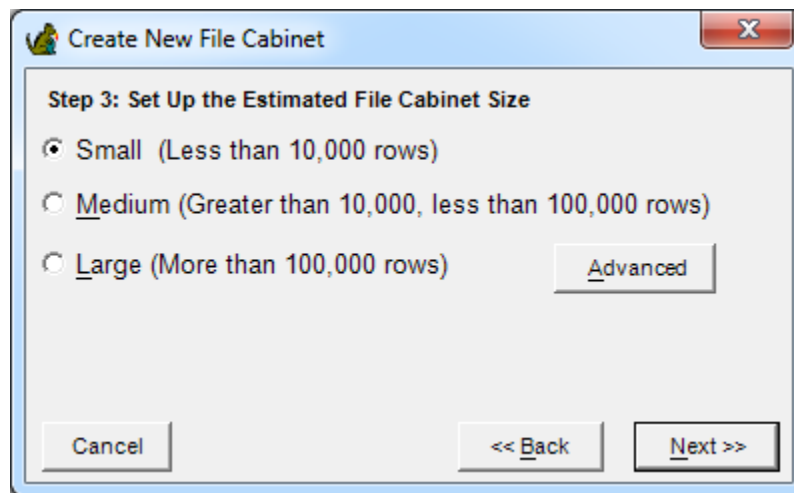
If you are running on Oracle, the next step in the wizard is setting the estimated file cabinet size.

If you are not running on Oracle, the next step in the wizard is setting permissions. Continue to next step in these instructions (setting file cabinet permissions).

To set the estimated file cabinet size (on Oracle only):

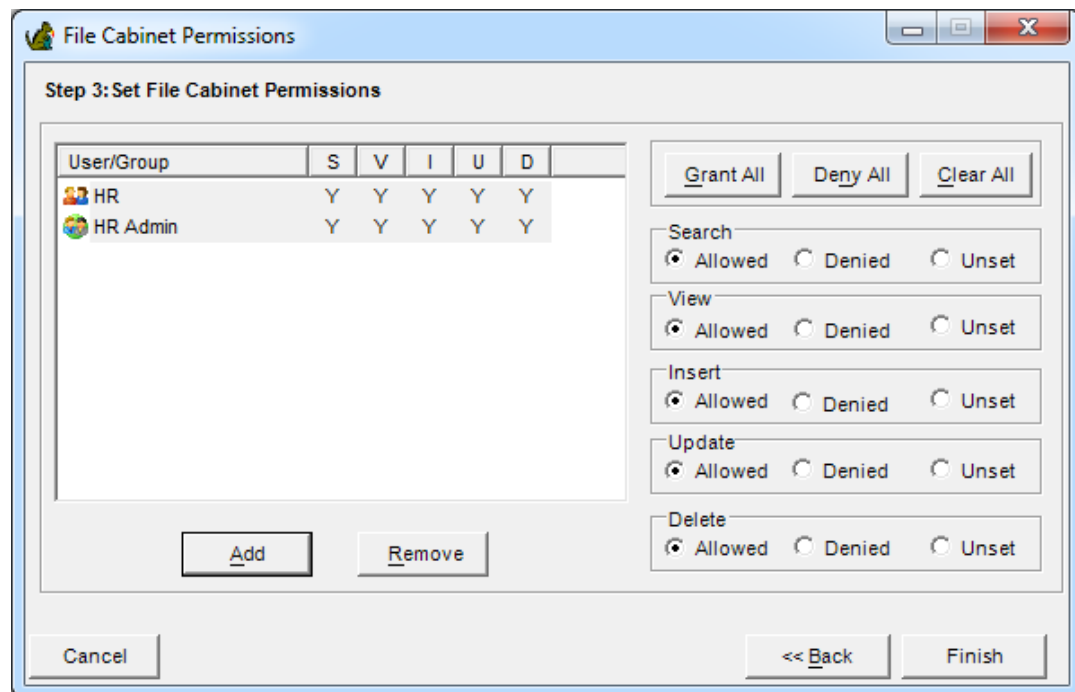
- a. In the **Set Up the Estimated File Cabinet Size** screen, either choose **Small**, **Medium** or **Large** (if one of these options is selected, Feith Control Panel estimates the amount of space required for the file cabinet table) or click **Advanced** to open the **Advanced Tablespace Settings** screen and manually set initial extent, next extent and percent growth.

- b. Click **Next** when done to continue creating the file cabinet.



9. The last step of the wizard is setting **File Cabinet Permissions**. Resource permissions are unset by default. Assign permissions as needed.

Note: A mid-level administrator is limited in who they can assign resource permission. See [Levels of Administrators](#) for more information.



- To grant permissions to a group or user:
 - a. Click **Add**. The **Users and Groups** screen opens, listing all FDD groups and users to which you have administrative access.
 - b. Select a group or user in the list and click **OK**. The selected group or user is granted permissions to the file cabinet. By default, all five resource permissions - **Search**, **View**, **Insert**, **Update** and **Delete** - are granted to the group or user.
 - c. Change the permissions as desired.

Tip: You can select multiple groups/users in the list and change all their permissions at once.

- To modify the permissions assigned to a group or user:
 - Select a group or user in the permissions list. Change the setting for a single permission by toggling between the **Allowed**, **Denied** and **Unset** options, or use the **Grant All**, **Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the group or user.

Tip: You can select multiple groups/users in the list and change all their permissions at once.

- To revoke permissions from a group or user:
 - Select a group or user in the permissions list and click **Remove**. All permissions to the file cabinet are revoked from the group or user.

10. Click **Finish**. The file cabinet is created and you are returned to the **Feith File Cabinet Administrator**.

Modify File Cabinet

To modify file cabinet properties:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. Change any property and click **OK**. You are returned to the **Modify File Cabinet** screen.
5. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To set an auto-tab label in file cabinet properties:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. On the **Main** tab, choose which field you want to use for the **Auto-Tab Label**.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To set a dynamic folder leap in file cabinet properties:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. On the **Advanced** tab, choose which leap you want to use for the **Dynamic Folder Leap**.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To set an auto SQL leap in file cabinet properties:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. On the **Advanced** tab, choose which leap you want to use for the **Auto SQL Leap**.
5. Optionally define an **Auto SQL Stylesheet** to apply to the information retrieved and displayed by the **Auto SQL Leap**. Stylesheets are created in FDD Client.
6. Click **OK**. You are returned to the **Modify File Cabinet** screen.
7. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To have the file cabinet open with an automatic blank search:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. On the **Advanced** tab, check on **Automatically Start With Blank Search**. A blank search (with no search criteria) will be performed automatically for end users who open the file cabinet.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To set a default sort order for the file cabinet's search results:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. On the **Advanced** tab, choose the **Default Sort Order** column(s) and direction (**Ascending** or **Descending**). You may sort on up to three columns. End users who search the file cabinet will receive the documents back in the default order; the user may choose their own sort order in the client applications.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To modify file cabinet permissions:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Permissions**. The **File Cabinet Permissions** screen opens.
4. Modify permissions as needed.

Note: A mid-level administrator is limited in who they can assign resource permission. See [Levels of Administrators](#) for more information.

- To grant permissions to a group or user:
 - a. Click **Add**. The **Users and Groups** screen opens, listing all FDD groups and users to which you have administrative access.
 - b. Select a group or user in the list and click **OK**. The selected group or user is granted permissions to the file cabinet and is added to the permissions list. By default, all five resource permissions - **Search**, **View**, **Insert**, **Update** and **Delete** - are granted to group or user.
 - To modify the permissions assigned to a group or user:
 - Select a group or user in the permissions list. Change the setting for a single permission by toggling between the **Allowed**, **Denied** and **Unset** options, or use the **Grant All**, **Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the group or user.
 - To revoke permissions from a group or user:
 - Select a group or user in the permissions list and click **Remove**. All permissions to the file cabinet are revoked from the group or user.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
 6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To add a new file cabinet field:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **New Field**. The **Add New Field** screen opens.

You can also clone an existing field by selecting the field you want to clone and clicking the **Clone Field** button.

4. Enter the field properties. See [Set File Cabinet Field Options](#) for instructions.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To modify a file cabinet field:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Select a field and click **Modify Field**. The **Modify Field Options** screen opens.
4. Change any option. See [Set File Cabinet Field Options](#) for instructions.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To set an associated leap for a file cabinet field:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Select a field and click **Modify Field**. The **Modify Field Options** screen opens.
4. In the **Associated Leap** field, choose the desired leap.
5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To delete a file cabinet field:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Select a field and click **Remove Field**.
4. Answer **Yes** to the conformation prompt. The field is deleted.
5. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To modify the file cabinet's administrator group settings:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. In the **Administered By** section, select the administrator groups for the file cabinet.

Any assigned administrator group and all super administrators will be able to modify the file cabinet.

- To assign an administrator group to the file cabinet:
 - a. Click **Add Group**. The **Administrator Groups** list opens. If you are logged in as a super administrator, the list will show all administrator groups that are not currently assigned to the file cabinet. If you are logged in as an administrator group member, the list will show all administrator groups to which you belong that are not currently assigned to the file cabinet.
 - b. Select a group in the list and click **OK**. The selected group is granted administrative access to the file cabinet and is added to the **Administered By** list.
- To remove an administrator group from the file cabinet:

- Select a group in the **Administered By** list and click **Delete Group**. Administrative access is revoked from the group, and the group is removed from the **Administered By** list.
- 5. Click **OK**. You are returned to the **Modify File Cabinet** screen.
- 6. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To full text index all documents in a file cabinet:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Right-click the desired file cabinet and select **Full-Text Index Existing Documents**.

Note that this action is disabled for virtual file cabinets.

3. Click **Yes** to the prompt. All the documents currently in the file cabinet will be full text indexed the next time Feith UTR runs.

Note that this action does not change the **Full-Text Index** setting in the file cabinet's properties. To change the **Full-Text Index** setting:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
2. Click **Properties**. The **File Cabinet Properties** screen opens.
3. Check the **Full-Text Index** checkbox.
4. Click **OK**. You will be prompted as to whether you want to full text index all the existing documents in the file cabinet.
5. Answer the prompt and you are returned to the **Modify File Cabinet** screen. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To remove existing full-text-indexed documents in a file cabinet from full text search:

1. Select **File Cabinets** from the **File** menu. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Right-click the desired file cabinet and select **Remove Existing Documents from Full-Text Index**.

Note that this action is disabled for virtual file cabinets.

3. Click **Yes** to the prompt. All the documents currently in the file cabinet will be hidden from the full text search the next time Feith UTR runs.

Note that this action does not change the **Full-Text Index** setting in the file cabinet's properties. To change the **Full-Text Index** setting:

1. Select a file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
2. Click **Properties**. The **File Cabinet Properties** screen opens.
3. Uncheck the **Full-Text Index** checkbox.
4. Click **OK**. You will be prompted as to whether you want to remove all the existing documents in the file cabinet from full text search.
5. Answer the prompt and you are returned to the **Modify File Cabinet** screen. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To allow or disallow full text search in a virtual file cabinet:

1. In **Feith Control Panel**, select the **File Cabinets** module. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a virtual file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Properties**. The **File Cabinet Properties** screen opens.
4. Select the **Advanced** tab. The advanced options display.

5. Turn on **Allow Full Text Search** to allow full text searching in the virtual file cabinet. Turn it off to disallow full text searching in the virtual file cabinet.
6. Click **OK**. You are returned to the **Modify File Cabinet** screen.
7. Click **Exit** to return to the **Feith File Cabinet Administrator**.

To validate file cabinet options:

Check the file cabinet for a couple of known problems, which may exist on some systems and cause issues, such as with Reports iQ.

To validate file cabinet options:

1. In the **File Cabinet Administrator**, select **Administrator>Validate File Cabinet Options**.
2. FCP checks the file cabinet options. If any problems are found, FCP prompts you to confirm you want them fixed.
 - File cabinets without an EDStor storage server. Every file cabinet should have an EDStor storage server.
 - Empty parameters for certain field options. These spurious entries can be removed.
3. Confirm the fixes you want FCP to make.

Set File Cabinet Field Options

File cabinet field options can be set when adding or modifying a file cabinet field.

To set file cabinet field options:

1. Open either the **Add New Field** screen or the **Modify File Cabinet Field Options** screen, depending on whether you are adding or modifying a file cabinet field.

To open the **Add New Field** screen when adding a new file cabinet, click the **Add** button on the **Setup File Cabinet Fields** screen of the **Create New File Cabinet** wizard.

To open the **Add New Field** screen when modifying a file cabinet, click the **New Field** button on the **Modify File Cabinet Fields** dialog.

To open the **Modify File Cabinet Field Options** screen, select the field and click the **Modify Field** button.

The **Add New Field** screen is divided into three tabs: **General**, **Lookup** and **Advanced**. The **Modify File Cabinet Field Options** screen displays all field options on a single screen.

2. Set or change the general file cabinet field options:

- **Name:** Enter the field name. Maximum 64 characters.

Tip: You can give a file cabinet field a special name in order for the field to be automatically populated with information from the file being imported. FDD and CheckIn automatically populate fields with certain names. See [Appendix B: Auto-Populated Field Names](#) for more information.

- **Description:** Enter the field description. Maximum 64 characters.
- **Field Type:** Choose the field type. Options include:
 - **String:** Any string of alphanumeric characters. Maximum 250 characters.
 - **Date:** Three integers with date separators (e.g., 08/02/2005).
 - **Datetime:** Date and time.
 - **Decimal:** Digits and one decimal holder (e.g., 432.344).
 - **Integer:** Any whole number between -2,147,483,647 and +2,147,483,647.
 - **Big Integer:** Any whole number between -9,223,372,036,854,775,807 and +9,223,372,036,854,775,807.
 - **Money:** A decimal in dollar format (e.g., 3223.32).
 - **Signature:** Stores a Forms iQ signature. No other field options can be set for this field type besides **Name**, **Description**, and **Field Type**.
 - **List of Strings:** Any string of alphanumeric characters. Multiple values can be entered. Maximum 250 characters.
 - **List of Numbers:** Digits and one decimal holder (e.g., 432.344). Multiple values can be entered.
 - **List of Dates:** Three integers with date separators (e.g., 08/02/2005). Multiple values can be entered.

Note: The field type cannot be changed when modifying an existing field, with the exception that date fields can be changed to datetime on Oracle.

- **Length:** Enter the length of the field. This setting only applies to string and decimal fields.

For **Decimal** fields and **Money** fields, the length applies to all characters in the field's value.

For **List of Strings** and **List of Numbers**, the length applies to the individual values. For example, in a **List of Strings** field with a length of "10" you could enter three 10-character

values. The total number of characters would be 30, but that's allowed since the field is a list-type field and each value is no more than 10 characters.

Field length cannot be decreased when modifying an existing field.

- **Scale:** Enter the scale (number of digits stored to the right of the decimal point) of the field. This setting only applies to decimal fields and list of numbers fields. For money fields, the scale is set to 2.
- **Case Options:** Choose the case of the value to be stored in the field; the default case is mixed case. Case options only apply to the String and List of Strings field types. Options include:
 - **Mixed Case (Case Insensitive Search):** Both upper and lower case characters are accepted and the field is optimized for case-insensitive searching.
 - **Mixed Case (Case Sensitive Search):** Both upper and lower case characters are accepted and the field is optimized for case-sensitive searching.
 - **Force Uppercase:** All field entries are forced to uppercase.
 - **Force Lowercase:** All field entries are forced to lowercase.
- **General Options:** The following settings are optional:
 -
 - **Read Only:** If checked, the field will be read-only. Users will not be able to enter data in the field.
 - **Mandatory:** If checked, the field will be mandatory. Users will be required to enter a value in the field when indexing or modifying documents.
 - **Strip Control Characters:** If checked, control characters (for example, line feed characters) will be removed from the value entered in the field. This option may be useful if users typically copy and paste text into the field from a source such as a word processing document.

The screenshot shows a dialog box titled "Add New File Cabinet Field" with three tabs: "General", "Lookup", and "Advanced". The "General" tab is active. It contains the following fields and options:

- Name:** A text box containing "Employee Name".
- Description:** An empty text box.
- Field Type:** A dropdown menu showing "String".
- Size:** A text box containing "64".
- Scale:** An empty text box.
- Case Option:** A dropdown menu showing "Mixed Case (Case Insensitive Search)".
- General Options:** A group box containing three unchecked checkboxes: "Read Only", "Mandatory", and "Strip Control Characters".

At the bottom of the dialog are "OK" and "Cancel" buttons.

3. Optionally assign a lookup table. Lookup tables provide the user with a list of values when indexing or searching the field.
 - To assign a lookup table to the field:
 - a. Select a **Table** from the list. Alternatively, you can type a table name in the **Table** textbox.

The **Table** list contains the FDD lookup tables, which are created and maintained in the **Lookup Table Editor**. See [Add Lookup Table](#) for more information.

 - b. Select the **Value** column. When the user selects a row from the lookup table during indexing or searching, the value from this column is inserted into the file cabinet field.
 - c. Optionally select a **Display** column. The display column is optional. Usually it is a column with values that describe the value column.
 - d. Optionally select an **Order** column. The order column specifies the sort order for the value column. The order can be set to any column in the lookup table or to <UNORDERED>. If an order column is not selected, order defaults to the display column if set, lookup column otherwise.
 - e. Optionally check the **Allow Override** option to allow users to index with a value not in the lookup table. By default, the **Allow Override** option is unchecked. When override is not allowed, users must select the index value from the lookup.
 - f. Optionally check **Hide Values**, to stop the user from selecting a value in the lookup table, while still using the other lookup table features. For example, you may want to stop the user from selecting an ID from a huge list of IDs in the lookup table, while still using the lookup table to validate the ID and cascade off of it.
 - To create a new lookup table while adding or modifying a file cabinet field, click the **New Table** button to open the **Create New Lookup Table** screen. See [Add Lookup Table](#) for instructions.

The screenshot shows the 'Add New File Cabinet Field' dialog box with the 'Lookup' tab selected. The 'Table' dropdown is set to 'students'. The 'Value' dropdown is set to 'student_id'. The 'Display' dropdown is set to 'student_name'. The 'Order' dropdown is set to 'student_name'. The 'Allow Override' and 'Hide Values' checkboxes are unchecked. The 'Cascade Lookups' checkbox is also unchecked. Below it, the 'File Cabinet Field' dropdown is empty. At the bottom are 'OK' and 'Cancel' buttons.

4. If you assigned a lookup table to the file cabinet field, optionally check the **Cascade Lookups** option to configure cascading lookup tables. Cascading lookup tables show a value list that is

filtered based on the lookup value entered in a related field in the same file cabinet. For example, cascading lookup assignment might be configured so that the value entered in a **Vendor Name** field is used to filter the lookup values for a **Vendor Location** field. This feature requires that the related file cabinet fields are assigned lookup columns from the same lookup table.

To configure cascading lookups:

- a. Check the **Cascade Lookups** option. This option is enabled if the lookup table assigned to the current field is also assigned to at least one other field in the file cabinet.
- b. Choose the related file cabinet field from the **File Cabinet Field** list. The lookup value entered in the related field will be used to filter the lookup list for the current field.

Note that you cannot choose a list-type field (**List of Strings**, **List of Numbers**, or **List of Dates**) in the **File Cabinet Field** list. List fields cannot be used to filter a lookup list.

The screenshot shows the 'Add New File Cabinet Field' dialog box with the 'Lookup' tab selected. The 'Table' dropdown is set to 'Locations'. The 'Value' dropdown is set to 'city'. The 'Display' dropdown is empty. The 'Order' dropdown is set to '<UNORDERED>'. The 'Cascade Lookups' checkbox is checked. The 'File Cabinet Field' dropdown is set to 'state'. There are 'OK' and 'Cancel' buttons at the bottom.

5. Optionally set the advanced field options:

- **Index:** Select whether or not an index is created on the field, and select whether to enable the distinct values list.
 - **Allow Duplicates:** If selected, an index is created for the field. Duplicate values are allowed.
 - **Unique:** If selected, a unique index is created for the field. Duplicate values are not allowed. Note that the **Index** option cannot be changed to **Unique** when modifying an existing field if the field contains duplicate values.
 - **None:** If selected, an index is not created for the field.

Note: The **Index** settings are not supported for list-type fields (**List of Strings**, **List of Numbers**, or **List of Dates**) on Oracle. The **Index** settings are supported - with the exception of the **Unique** index option - for list-type fields on MS SQL Server.

- **Enable Distinct Values List:** If selected, the distinct value list is enabled for the field in the FDD client applications. Users will be able to use the distinct values list when indexing and

searching; see the FDD User's Guide for instructions. This setting is off by default. Note that this option cannot be selected if the **Index** setting is **None**.

- **Default Value:** Enter a value to be used as the default during indexing. Note that date fields can default to either to the date indexed or to a specified date. Also note that when setting a default value for a list-type field (**List of Strings**, **List of Numbers**, or **List of Dates**), you can only set one value as a default. You cannot set multiple default values.
- **Illumitext:** If this option is selected, the field value is highlighted in context when viewing a document's UTR note. Note the ability to create UTR notes on documents requires **UTR**.
- **Mask:** A field mask automatically formats data entered into the field during indexing or modification.

To select a mask, click the **?** icon to open a list of masks. This list displays both the masks and their descriptions. Choose a mask from the list and click **OK**; the selected value is entered in the **Mask** field.

To enter a custom mask, type the mask in the **Mask** field. See [Appendix A: Field Mask and Regular Expression Syntax](#) for information on field mask syntax.

- **Regular Expression Validation:** A regular expression validation tests the field data against a regular expression pattern. When assigning a regular expression validation, you have to option whether to allow override. Regular expression validations can be used to prevent incomplete or poorly formatted data from entering the file cabinet fields during indexing or modification.

To select a regular expression validation, click the **?** icon to open a list of regular expressions. This list displays both the regular expressions and their descriptions. Choose a regular expression from the list and click **OK**; the selected value is entered in the **Regular Expression Validation** field. Check the **Allow Override** option if you want to allow users to enter index values that do not match the regular expression.

To enter a custom regular expression, type the regular expression in the **Regular Expression Validation** field. See [Appendix A: Field Mask and Regular Expression Syntax](#) for information on regular expression syntax.

6. Click **OK** to save the file cabinet field options. See [Add File Cabinet](#) and [Modify File Cabinet](#) for further instructions on adding and modifying file cabinets.

Clone File Cabinet

To clone an existing file cabinet:

1. Select **File>File Cabinets**. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Clone**. The **Clone File Cabinet** screen opens.
3. Select what fields to include in the **Included Fields** list. By default, all fields are selected.

You must include at least one field in the new file cabinet.

4. Enter the **New File Cabinet Name** (maximum 64 characters).
5. Enter the **New File Cabinet Description** (maximum 64 characters).
6. Optionally check the **Copy Permissions** option to copy the resource permission assignments from the original file cabinet. If **Copy Permissions** is unchecked, permissions will be unset for the new file cabinet.

If you are logged in as an administrator group member, resource permissions will be copied over only for the groups you administer.

7. Click **OK**. The file cabinet is created and you are returned to the **Feith File Cabinet Administrator**.

The storage server settings, administrator group settings, and full-text index setting are copied over from the original file cabinet.

To modify the cloned file cabinet's properties, permissions, fields or administrator group settings, select the file cabinet and click **Modify** to open the **Modify File Cabinet** screen. See [Modify File Cabinet](#) for instructions.

Delete File Cabinet

You must delete all documents from a file cabinet before you can delete the file cabinet in FCP. If you attempt to delete a file cabinet that contains documents, the delete will fail.

To delete a file cabinet:

1. Select **File>File Cabinets**. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select a file cabinet and click **Delete**.

Note: The FDD system file cabinets cannot be deleted.

3. Answer **Yes** to the confirmation prompt. The file cabinet is deleted.

File Cabinet Reports

Three file cabinet reports are available: **Selected File Cabinet**, **All File Cabinets**, and **Selected File Cabinet Fields**.

The **Selected File Cabinet** report lists the file cabinet properties, file cabinet field properties and resource permission assignments. This report is in HTML format.

The **All File Cabinets** report lists all file cabinets by name, description and type. This report is in HTML format.

The **Selected File Cabinet Fields** report lists all file cabinet fields with their properties. This report is in CSV format.

To generate a file cabinet report:

1. Select **File>File Cabinets**. The **Feith File Cabinet Administrator** opens.
2. Optionally select a file cabinet.
3. Select the **Report** menu and choose the desired report:
 - **Selected File Cabinet - HTML**
 - **All File Cabinets - HTML**
 - **Selected File Cabinet Fields – CSV**
4. If you chose an HTML-formatted report, the report opens in a browser window.

If you chose a CSV-formatted report, you are prompted to save the CSV file and the report opens.

Export and Import File Cabinet

The file cabinet [export](#) and [import](#) options can be used to copy a file cabinet design from one FDD database to another FDD database. For example, this feature can be used to export a file cabinet from a test system and import the file cabinet into a production system.

In addition to the file cabinet design itself, the file cabinet export typically includes any:

- Users or groups that were assigned resource permissions to the file cabinet.
- Administrator groups that were assigned to the file cabinet.
- FDD lookup tables that were assigned to the file cabinet.

Note: Exporting a file cabinet does NOT export the documents that reside in the cabinet; only the file cabinet design is exported.

[Importing a virtual file cabinet](#) is a slightly different process. Also, you can [import file cabinet fields](#) to an existing file cabinet

Export a File Cabinet or Virtual File Cabinet

The following instructions apply both when exporting a regular file cabinet and when exporting a virtual file cabinet.

To export a file cabinet:

1. Select **File>File Cabinets**. The **Feith File Cabinet Administrator** opens, listing all FDD file cabinets to which you have administrative access.
2. Select one or more file cabinets. You can select multiple file cabinets by using **SHIFT+click** or **CTRL+click**.
3. Select a file cabinet and select **File>Export** then choose either of the following options:
 - **With Assigned Groups with Members:** Include any users or groups that were assigned resource permissions to the file cabinet, including group members. Also include any administrator groups that were assigned to the file cabinet.
 - **With Assigned Groups without Members:** Include any users or groups that were assigned resource permissions to the file cabinet, but *excluding* group members. Also include any administrator groups that were assigned to the file cabinet.
 - **Without Assigned Groups:** Include file cabinet settings but *exclude* users or groups that were assigned resource permissions to the file cabinet or any administrator groups that were assigned to the file cabinet.
4. The **File Save** dialog opens. Browse to select a destination path and file name for the export file, then click OK. The file cabinet(s) is exported to an XML file.

Tip: You can select multiple file cabinets to export using **SHIFT+click** or **CTRL+click**.

Import a File Cabinet

To import a file cabinet:

1. Open the **Feith File Cabinet Administrator** and select **File>Import**. The **File Open** dialog opens.
2. Browse to select the file cabinet export file and click OK. You are prompted whether to import the file cabinet; answer **Yes** to import.
3. If the file cabinet export includes users that do not exist in the current database, you will be prompted to add each user. The user properties dialog is displayed for each user.

To add a user, enter the user password information and click **OK**.

To skip a user, click **Cancel**. If you cancel adding a user, you will be prompted whether to continue the import; answer **Yes** to continue the import.

4. The **Create New File Cabinet Wizard** opens, with the properties of the original file cabinet entered as defaults on each screen. See [Add File Cabinet](#) for details on setting file cabinet properties.
 - a. On the **Step 1: Set Up File Cabinet Properties** screen, enter the file cabinet properties including the name, description, storage server, administration group, and full-text index option. Click **Next** to continue the import.
 - b. On the **Step 2: Set Up the File Cabinet Fields** screen, configure the file cabinet fields. By default, the new file cabinet includes all fields from the original file cabinet. See [Set File Cabinet Field Options](#) for details on file cabinet field options. Click **Next** to continue the import.
 - c. If the file cabinet export includes a lookup table that does not exist in the current database, you will be prompted whether to add the lookup table.

To add the lookup table, answer **Yes**.

To skip the lookup table, answer **No**. If you answer **No**, you will be prompted to either change or clear the lookup table assignment.

To close the prompt and return to the **Step 2: Set Up the File Cabinet Fields** screen, click **Cancel**.

- d. If you are running on Oracle, set the estimated file cabinet size. Click **Next** to continue the import.
 - e. The last step of the wizard is setting **File Cabinet Permissions**. The permission assignments are copied from the original file cabinet, unless you opted to [exclude groups](#). The group's users are also migrated, unless you chose to [exclude members](#). Modify permissions as needed. Click **Next** to finish importing the file cabinet.
5. When the import process is complete, you are returned to the **Feith File Cabinet Administrator** and the imported file cabinet is included in the file cabinet list.

Note: If the file cabinet export includes one or more groups that do not exist in the current database, the groups will be automatically added during the file cabinet import. Note that this is not the case if you opted to export the file cabinet without assigned groups.

Import a Virtual File Cabinet

If the base file cabinet does not exist in the current database, create or import the base file cabinet first, then import the virtual file cabinet.

To import a virtual file cabinet:

1. Open the **Feith File Cabinet Administrator** and select **File>Import**. The **File Open** dialog opens.
2. Browse to select the virtual file cabinet export file and click OK. You are prompted whether to import the virtual file cabinet; answer **Yes** to import.
3. The **Create New File Cabinet Wizard** opens, with the properties of the original virtual file cabinet entered as defaults on each screen. See [Add Virtual File Cabinet](#) for details on setting virtual file cabinet properties.
 - a. On the **Step 1: Set Up File Cabinet Properties** screen, enter the virtual file cabinet properties including the name, description, administration group and base file cabinet. Click **Next** to continue the import.
 - b. On the **Create New Virtual File Cabinet - Customize** screen, modify the virtual file cabinet as needed. Click **Next** to continue the import.
 - c. The last step of the wizard is setting **File Cabinet Permissions**. By default, the permission assignments are copied from the original virtual file cabinet, unless you opted to export the file cabinet without assigned groups. Modify permissions as needed. Click **Next** to finish importing the virtual file cabinet.
4. When the import is complete, you are returned to the **Feith File Cabinet Administrator** and the imported virtual file cabinet is included in the file cabinet list.

Import File Cabinet Fields

To import fields from a file cabinet export file into an existing file cabinet:

1. Open the **Feith File Cabinet Administrator** and select the file cabinet to which you want to add fields.
2. Select the file cabinet to which you want to import fields.
3. Select **File>Import>Fields to Selected File Cabinet**. The **Import File Cabinet Fields** dialog opens and you are prompted to select a file cabinet export file.
4. Select the desired file cabinet export file and click **Open**. The **Append File Cabinet Fields** dialog opens and displays the **Exported File Cabinet** and the fields it has in the export file.
5. Check on the fields you want to append to the existing file cabinet. Uncheck the fields you do not want to append.
6. Click **OK**. The fields are imported and appended to the existing file cabinet. If the file cabinet export file contained multiple file cabinets, you will be prompted for each file cabinet separately to choose the fields you want.

Full Text

Full Text Administrator

The following instructions apply only if your FDD system is licensed for full text and if you are using Autonomy IDOL as the full text server.

The **Full Text Administrator** can be used to manage your **Autonomy IDOL** full text database.

To create new server entries:

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. Click the **New Server Entries** button. The **Add New Autonomy IDOL Server Entries** dialog opens.

You must have the **Maintain Servers** task permission in order to create new server entries.

3. Enter the following properties:
 - **Address:** IDOL server address.
 - **Database:** IDOL database name.
 - **Indexing Port:** Port number of the IDOL indexing service.
 - **Querying Port:** Port number of the IDOL querying service.
 - **Create IDOL Database:** Optionally create an IDOL database with the name specified in the **Database** field. Note that in order to create an IDOL database, you must have the **Administer Autonomy IDOL** task permission.

If the IDOL database already exists and you just want to create a new server entry pointing to that IDOL database, uncheck the **Create IDOL Database** checkbox.

4. Click **OK**. The new server entries are added.

To create an IDOL database:

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. In the **Indexing Server** field, select the IDOL server entry that includes the name of the database you want to create.

You must have the **Administer Autonomy IDOL** task permission in order to create an IDOL database.

3. Click the **Create IDOL Database** button.
4. Answer **Yes** to the prompt. The IDOL database is created.

To drop an IDOL database:

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. In the **Indexing Server** field, select the IDOL server entry that includes the name of the database you want to drop.

You must have the **Administer Autonomy IDOL** task permission in order to drop an IDOL database.

3. Click the **Drop IDOL Database** button.
4. Answer **Yes** to the prompt. The IDOL database is dropped.

To delete all records from an IDOL database:

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. In the **Indexing Server** field, select the IDOL server entry that includes the name of the database from which you want to delete all records.

You must have the **Administer Autonomy IDOL** task permission in order to delete records from an IDOL database.

3. Click the **Delete All Records From IDOL Database** button.
4. Answer **Yes** to the prompt. All records are deleted from the IDOL database.

To compact Autonomy IDOL:

Note: This action applies to all IDOL databases in Autonomy IDOL. Compacting may take a while and will impair Autonomy IDOL's performance, therefore compacting should be done when Autonomy IDOL is not otherwise needed.

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. Click the **Compact Autonomy IDOL (All Databases)** button.

You must have the **Administer Autonomy IDOL** task permission in order to compact Autonomy IDOL.

3. Answer **Yes** to the prompt. Compacting of Autonomy IDOL begins.

To check how many documents are in an IDOL database:

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. Click the **Database Status** button. The **Full Text Administrator Request** dialog opens.

You must have the **Administer Autonomy IDOL** task permission in order to check the status of an IDOL database.

3. In the **Query Server** field, enter the address of the server you want to query.
4. In the **Database** field, enter the name of the IDOL database you want to query.
5. The number of documents in the IDOL database is displayed in the **Result** field. To refresh the result, click the **Check Status** button.

Tip: For troubleshooting purposes, you can view the source of the result by clicking the **Show Source** button.

To check the status of an Autonomy IDOL request:

1. Select **File>Full Text**. The **Full Text Administrator** opens.
2. Click the **Check Status of Request ID** button. The **Full Text Administrator Request** dialog opens.

You must have the **Administer Autonomy IDOL** task permission in order to check the status of an Autonomy IDOL request.

3. In the **Query Server** field, enter the address of the server you want to query.
4. In the **Request ID** field, enter the request ID of the request you want to check.
5. The status of the request is displayed in the **Result** field. To refresh the result, click the **Check Status** button.

Tip: For troubleshooting purposes, you can view the source of the result by clicking the **Show Source** button.

To rebuild Autonomy IDOL:

1. Select **File>Full Text** to open the **Full Text Administrator**.
2. Take one of the following two steps to clear the existing data from the IDOL database (recommended):
 - a. Delete all existing records from the IDOL database. To do this, use the **Delete All Records From IDOL Database** option described above.

Or:

 - b. Drop the existing IDOL database and add a new, blank IDOL database. To do this, use the **Drop IDOL Database** and **Create IDOL Database** options described above.
3. Select the **Rebuild** tab in the **Full Text Administrator**.
4. Click the **Request Full Text Database Rebuild** button.

You must have the **Rebuild Full Text Database** task permission in order to rebuild Autonomy IDOL.

5. Click **Yes** to the prompt. Rebuilding of the Autonomy IDOL begins.

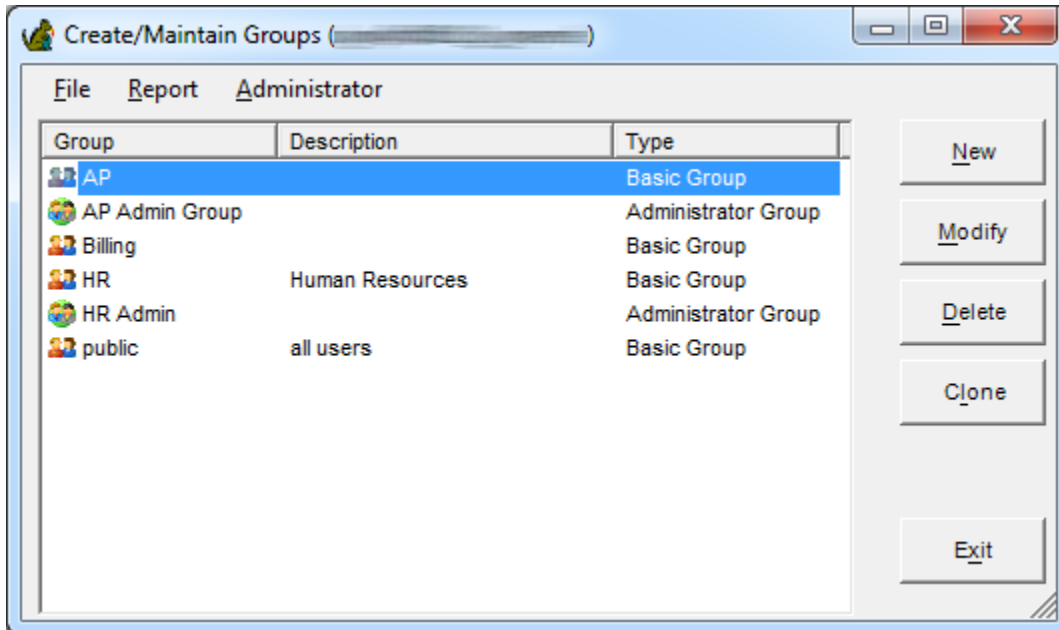
Note: It may take some time for the Feith UTR Engine to complete the rebuild. Canceling the rebuild process will result in a partially-rebuilt IDOL database.

Groups

Groups

Groups are sets of users with similar responsibilities who perform similar tasks. Users can be assigned to more than one group.

All users assigned to a group inherit the group's permissions. The simpler the group structure, the easier it is to maintain.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

System Groups

The following system groups are created during the FDD installation. These groups are created for use with FDD applications and cannot be deleted.

Note that all FDD users belong to the **public** group. Users cannot be removed from the **public** group.

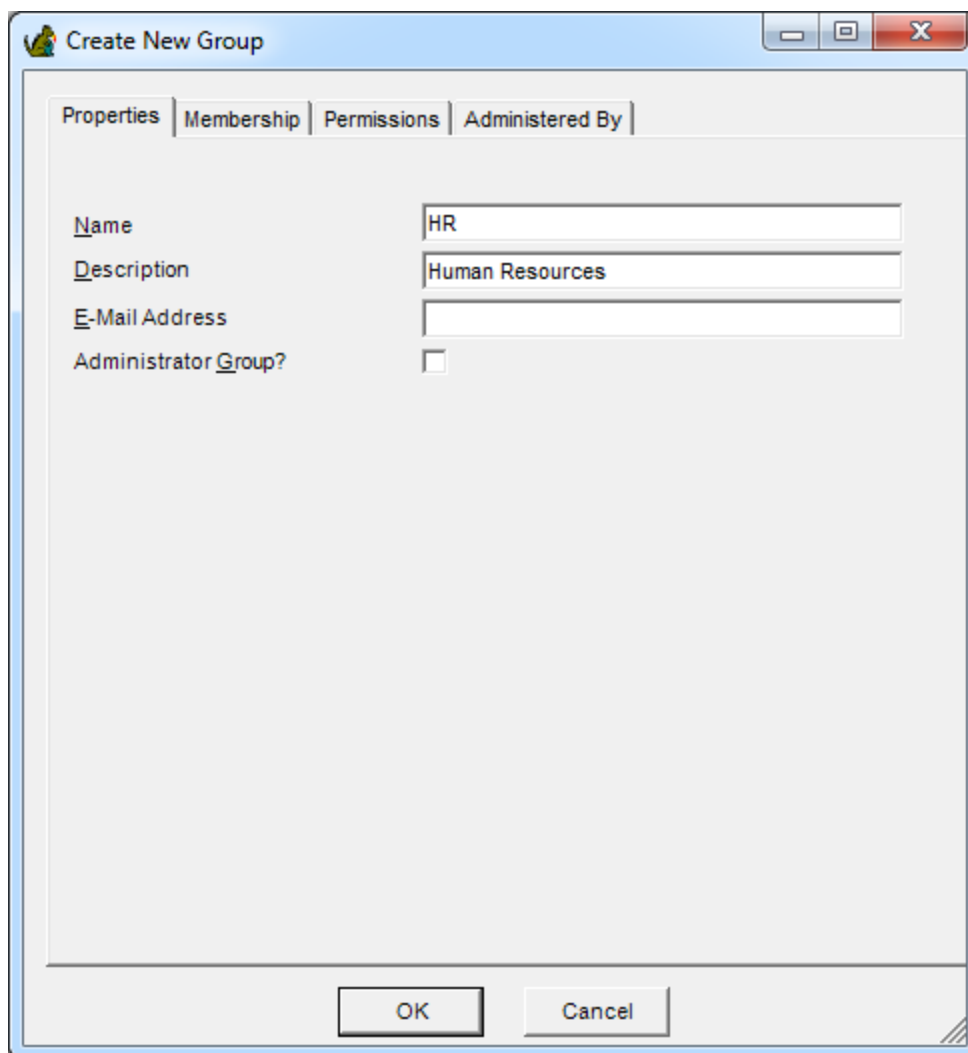
GROUP	DESCRIPTION
FeithDrive	FeithDrive User Group
public	All Users
UTR	Universal Text Retrieval Group

Add Group

To add a group:

1. Select **File>Groups**. The **Feith Group Administrator** opens.
2. Click **New**. The **Create New Group** screen opens.
3. On the **Properties** tab, enter the following group properties:
 - **Name**: Enter the group name. A maximum of 64 characters is accepted.
 - **Description**: Enter the group description. A maximum of 64 characters is accepted.
 - **Email Address**: Optionally enter the group's email address. A maximum of 64 characters is accepted.
 - **Administrator Group?**: Check this option if you want to make the group an administrator group. An administrator group can be assigned administrative access to specific file cabinets and groups. See [Levels of Administrators](#) for more information.

Note: This property can be set only by a super administrator.



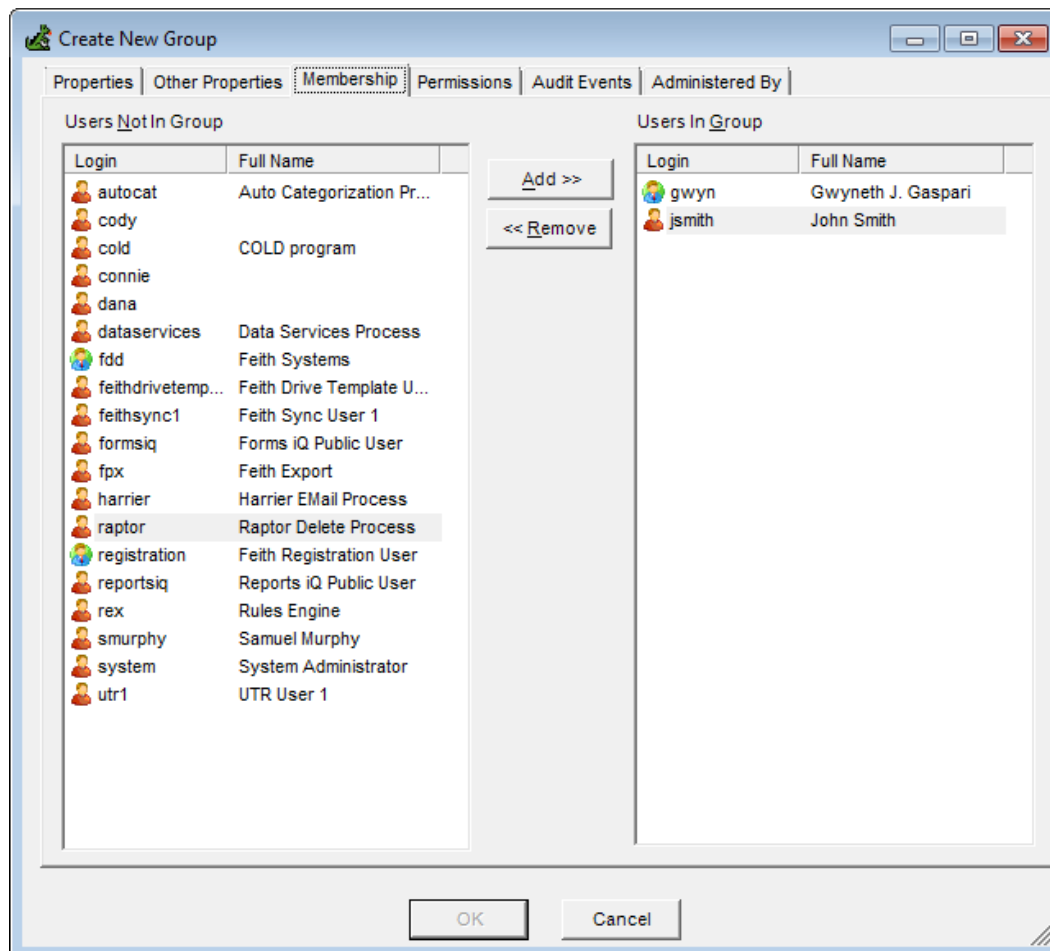
The screenshot shows a window titled "Create New Group" with a standard Windows-style title bar (minimize, maximize, close buttons). Inside the window, there are four tabs: "Properties", "Membership", "Permissions", and "Administered By". The "Properties" tab is currently selected. Below the tabs, there are four labeled input fields:

- Name**: A text box containing the value "HR".
- Description**: A text box containing the value "Human Resources".
- E-Mail Address**: An empty text box.
- Administrator Group?**: A checkbox that is currently unchecked.

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

4. Select the **Membership** tab and set the group membership. To assign users faster, you can select multiple users using **CTRL+click** or **SHIFT+click**. You can also double-click the user name to move it from one list to the other.

Group membership can also be set for an individual user in the user properties. See [Add Database Authenticated User](#) or [Modify User](#) for instructions.



- To add a user to the group:
 - Select the user in the **Users Not in Group** list and click **Add**. The user is added to the group and now appears in the **Users in Group** list.

Tip: You can also double-click the user to move them from one list to the other.

When selecting users to add, you can select users by right-clicking in the **Users Not In Group** list and choosing one of the options:

Select Users in Groups: Select users based on one or more other groups they are in.

Select Users Not in Groups: Select users based on one or more other groups they are *not* in.

- To remove a user from the group:
 - Select the user in the **Users in Group** list and click **Remove**. The user is removed from the group and now appears in the **Users Not in Group** list.

Tip: You can also double-click the user to move them from one list to the other.

When selecting users to remove, you can select users by right-clicking in the **Users In Group** list and choosing one of the options:

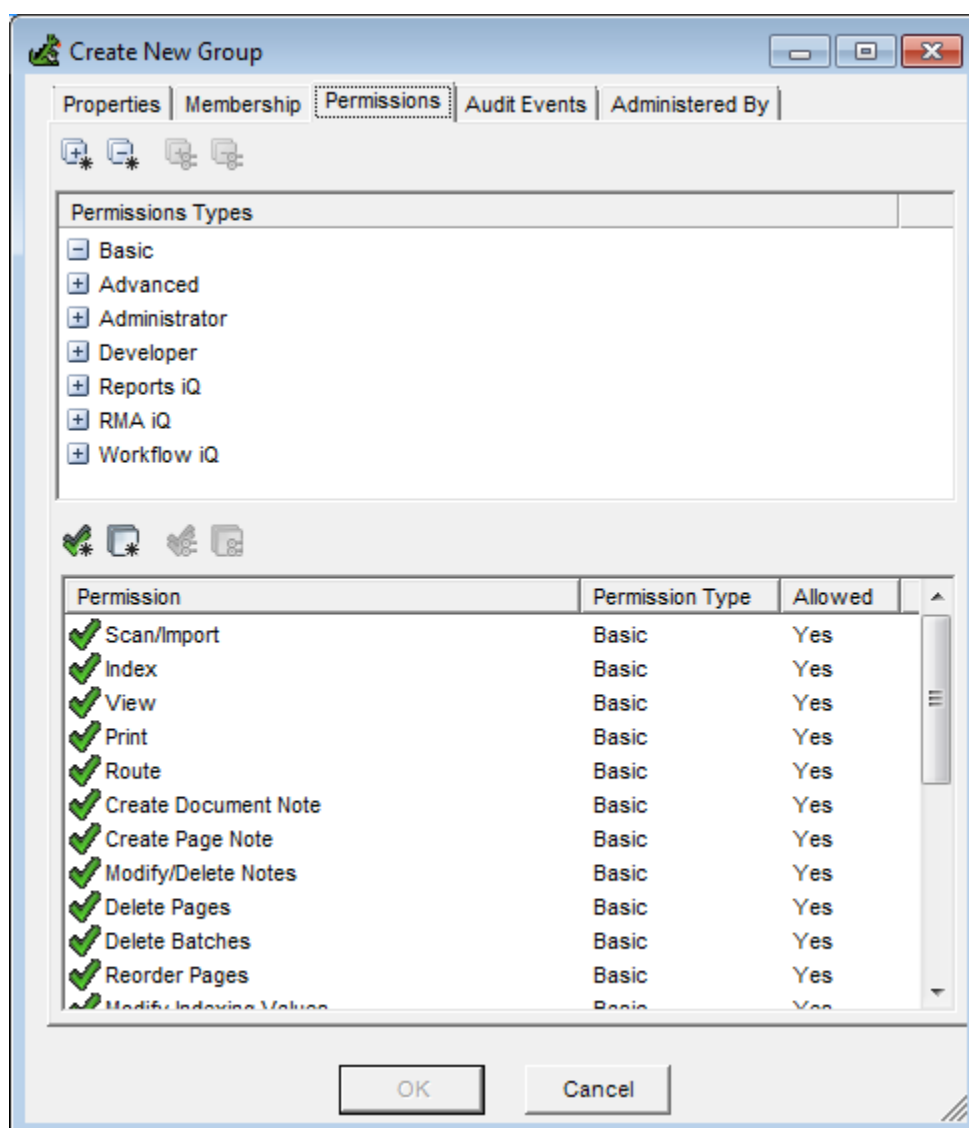
Select Users in Groups: Select users based on one or more other groups they are in.

Select Users Not in Groups: Select users based on one or more other groups they are *not* in.

5. Select the **Permissions** tab and set the group's task permissions, which control what actions the users in the group are allowed to take in various Feith applications.

Permissions are broken down into types and you can choose which permission types are listed by expanding or collapsing the **Permission Types** in the top list.

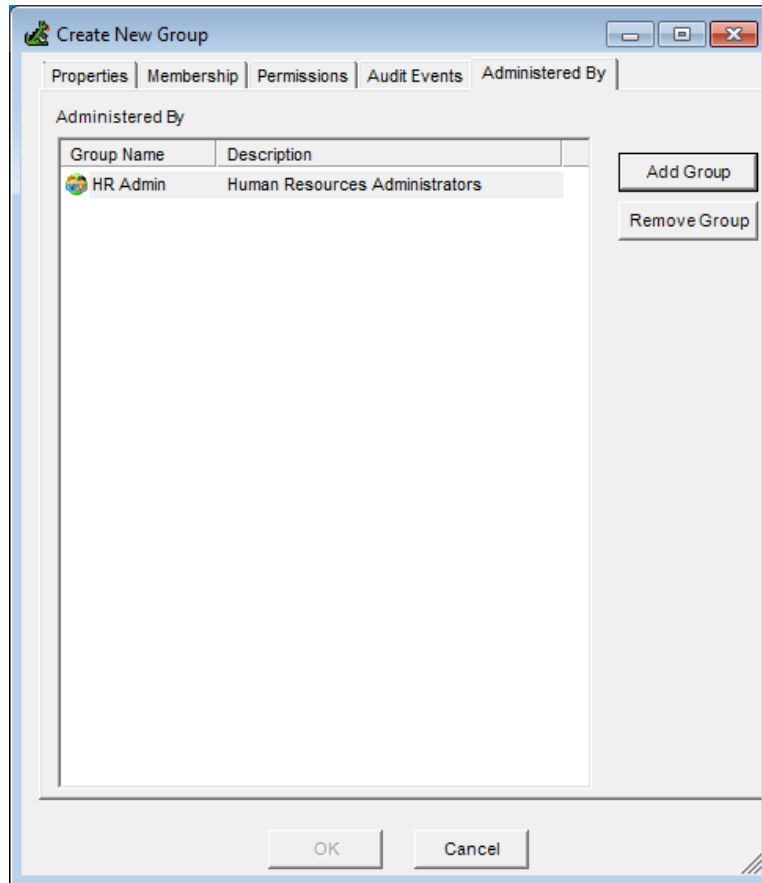
When you have found the desired permissions, you can double-click an individual permission to either grant or clear it. You can also use the toolbar buttons to change all listed permissions or multiple, selected permissions (select multiple using **CTRL+click** or **SHIFT+click**).



6. Optionally select the **Administered By** tab and assign administrator groups to the new group.

Any assigned administrator group and all super administrators will be able to modify the group.

If you are logged in as a member of an administrator group, all administrator groups to which you belong are automatically assigned to the group.



- To assign an administrator group to the group:
 - a. Click **Add Group**. The **Administrator Groups** list opens. If you are logged in as a super administrator, the list will show all administrator groups that are not currently assigned to the group. If you are logged in as an administrator group member, the list will show all administrator groups to which you belong that are not currently assigned to the group.
 - b. Select a group in the list and click **OK**. The selected group is granted administrative access to the group and is added to the **Administered By** list.
 - To remove an administrator group from the group:
 - Select a group in the **Administered By** list and click **Delete Group**. Administrative access is revoked from the group, and the group is removed from the **Administered By** list.
7. If your FDD system is licensed for auditing, the **Audit Events** tab will appear in the **Group Properties** dialog. Refer to [Set Group Audit Events for FDD Auditing](#) for instructions on configuring audit events for the group.
8. Click **OK**. The group is created and you are returned to the **Feith Group Administrator**.

Modify Group

To modify group properties:

1. Select **File>Groups**. The **Feith Group Administrator** opens, listing all FDD groups to which you have administrative access.
2. Select a group and click **Modify**. The **Modify Group** screen opens.
3. Change any property and click **OK**. The group properties are modified and you are returned to the **Feith Group Administrator**.

Note: Users cannot be removed from the **public** group.

Clone Group

To clone an existing group:

1. Select **File>Groups**. The **Feith Group Administrator** opens, listing all FDD groups to which you have administrative access.
2. Select a group and click **Clone**. The **Create New Group** screen opens. The group membership, task permissions and administrator group settings are copied over from the original group.
3. On the **Properties** tab, enter the following properties for the new group:
 - **Name:** Enter the group name. A maximum of 16 characters is accepted.
 - **Description:** Enter the group description. A maximum of 64 characters is accepted.
 - **Group Email:** Optionally enter the group's email address. A maximum of 64 characters is accepted.
 - **Administrator Group?:** Check this option if you want to make the group an administrator group. An administrator group can be assigned administrative access to specific file cabinets and groups.

Note: This property can only be set by a super administrator.

4. Optionally select the **Membership** tab and modify the group membership.

Group membership can also be set for an individual user in the user properties. See [Add Database Authenticated User](#) or [Modify User](#) for instructions.

- To add a user to the group:
 - Select the user in the **Users Not in Group** list and click **Add**. The user is added to the group and now appears in the **Users in Group** list.
 - To remove a user from the group:
 - Select the user in the **Users in Group** list and click **Remove**. The user is removed from the group and now appears in the **Users Not in Group** list.
5. Optionally select the **Permissions** tab and modify the group's task permissions.

Assign permissions individually or use the **Grant All**, **Deny All** and **Clear All** buttons.

6. Optionally select the **Administration** tab and modify the administrator group settings for the group.

Any assigned administrator group and all super administrators will be able to modify the group.

- To assign an administrator group to the group:
 - a. Click **Add Group**. The **Administrator Groups** list opens. If you are logged in as a super administrator, the list will show all administrator groups that are not currently assigned to the group. If you are logged in as an administrator group member, the list will show all administrator groups to which you belong that are not currently assigned to the group.
 - b. Select a group in the list and click **OK**. The selected group is granted administrative access to the group and is added to the **Administered By** list.
 - To remove an administrator group from the group:
 - Select a group in the **Administered By** list and click **Delete Group**. Administrative access is revoked from the group, and the group is removed from the **Administered By** list.
7. Click **OK**. The group is created and you are returned to the **Feith Group Administrator**.

Delete Group

To delete a group:

1. Select **File>Groups**. The **Feith Group Administrator** opens, listing all FDD groups to which you have administrative access.
2. Select a group and click **Delete**.

Note: The **public** group cannot be deleted.

3. Answer **Yes** to the confirmation prompt. The group is deleted.

Export and Import Group

The group export and import options can be used to copy a group from one FDD database to another FDD database. For example, this feature can be used to export a group from a test system and import the group into a production system.

The group export includes any users that are members of the group.

To export a group:

1. Select **File>Groups**. The **Feith Group Administrator** opens, listing all FDD groups to which you have administrative access.
2. Select one or more groups. You can select multiple groups by using **SHIFT+click** or **CTRL+click**.
3. Select **File>Export** then choose either of the following options:
 - **With Members:** Include all the group settings and members.
 - **Without Members:** Include the group settings but exclude the users assigned as members in the group.
4. The **File Save** dialog opens. Browse to select a destination path and file name for the export file, then click OK. The group(s) is exported to an XML file.

To import a group:

1. Open the **Feith Group Administrator** and select **File>Import**. The **File Open** dialog opens.
2. Browse to select the group export file and click OK. You are prompted whether to import the group; answer **Yes** to import.
3. If the group export [includes members](#) and these users do not exist in the current database, you will be prompted to add each user. The user properties dialog is displayed for each user.

To add a user, enter the user password information and click **OK**.

To skip a user, click **Cancel**. If you cancel adding a user, you will be prompted whether to continue adding users. To continue adding users, answer **Yes**. To skip all users (but continue the group import), answer **No**.

4. When the import is complete, you are returned to the **Feith Group Administrator** and the imported group is included in the group list.

Note: A file cabinet export includes the groups and users that are assigned to the file cabinet. See [Export and Import File Cabinet](#) for instructions on adding groups and users to the FDD system during a file cabinet import.

Get Group Member Information

There are two options that let you get group information: **Copy Members** and **Copy E-Mail Addresses**.

Copy Members

To copy members:

1. Select **File>Groups**. The **Feith Group Administrator** opens, listing all FDD groups to which you have administrative access.
2. Select a group and click **Modify**. The **Modify Group** screen opens.
3. Select the **Membership** tab.
4. Right-click in the **Users In Group** list and select **Copy Members**. The membership information is copied to the clipboard in a tab-delimited format.
5. The membership information can be pasted into the desired application (e.g. Excel).

The information includes the members' user names, full names, and email addresses.

Copy E-Mail Addresses

To copy email addresses:

1. Select **File>Groups**. The **Feith Group Administrator** opens, listing all FDD groups to which you have administrative access.
2. Select a group and click **Modify**. The **Modify Group** screen opens.
3. Select the **Membership** tab.
4. Right-click in the **Users In Group** list and select **Copy E-Mail Addresses**. The members' email addresses are copied to the clipboard in a comma-delimited format.
5. The members' email addresses can be pasted into the desired application.

Set Group Audit Events for FDD Auditing

The following instructions apply only if your FDD system is licensed for FDD Auditor.

If your FDD system is licensed for **FDD Auditor**, the audit events for a group are set on the **Audit Events** tab of the group properties dialog.

When an audit event is selected for a group, an entry is written to the **FDD Audit Trail** each time a member of the group performs the action. For example, if the audit event **View Page** is selected for the **HR** group, then an audit entry is written each time a member of the group views a page. The audit data includes the user's internal ID, the name of the action performed, and the date and time the action was performed. Audit reports and graphs are viewed in the **FDD Auditor** application.

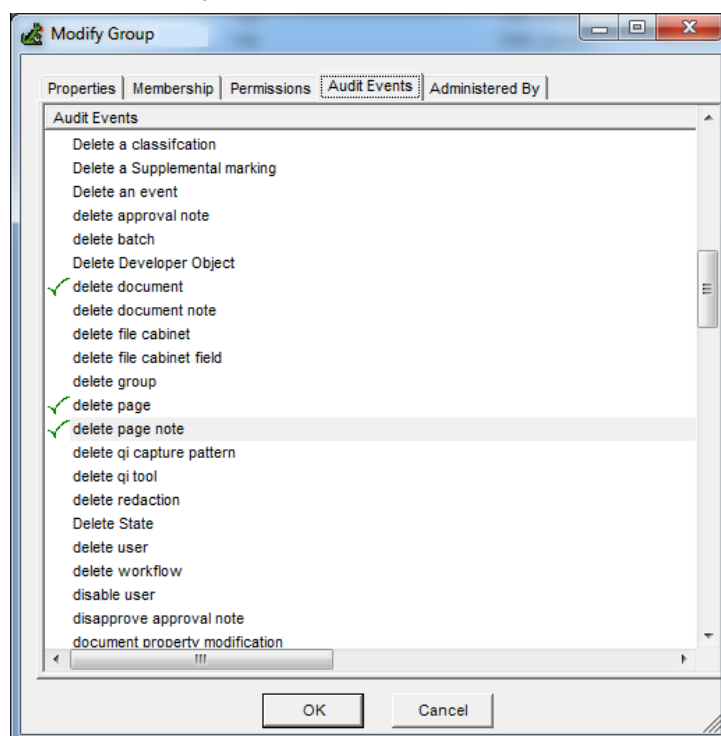
Note: Audit events can be turned on at both the [user level](#) and at the group level. See [Audit Events](#) for the list of audit events that can be tracked in the FDD system.

To set group audit events:

1. Select **File>Groups** to open the **Feith Group Administrator**.
2. Open either the **Create New Group** screen or the **Modify Group** screen, depending on whether you are adding or modifying a group.

To open the **Create New Group** screen, click the **New** button. To open the **Modify Group** screen, select a group and click **Modify**.

3. Select the **Audit Events** tab and set the group's audit events. Double-click an event to select it for auditing. A check mark ✓ is shown in front of selected audit events. To deselect an audit event, double-click the event again; the check mark should be cleared.



Note: The **Audit Events** tab appears only if your FDD system is licensed for FDD Auditor.

4. Finish setting the group properties as needed on the other tabs, then click **OK** to save the properties. You are returned to the **Feith Group Administrator**.

Group Reports

Two group reports are available: **Selected Group** and **All Groups**.

The **Selected Group(s)** report lists the group properties, group membership and task permission assignments. This report is in HTML format.

The **All Groups** report lists all groups by name, description and type. This report is in HTML format.

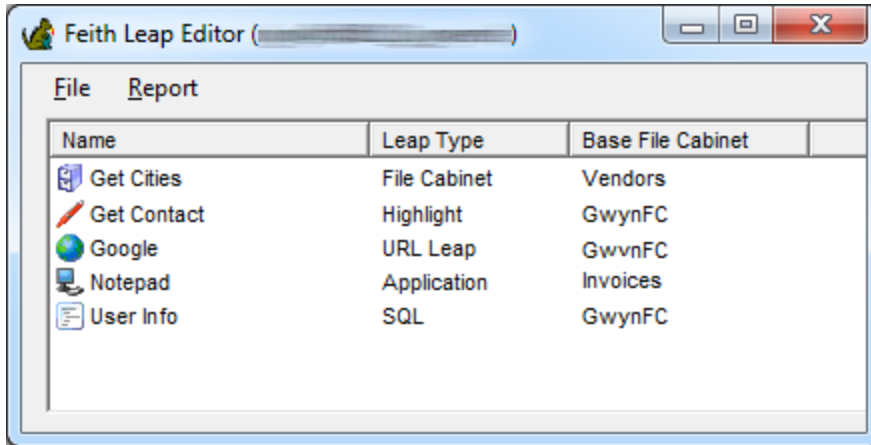
To generate a group report:

1. Select **File>Groups**. The **Feith Group Administrator** opens.
2. Optionally select a group.
3. Select the **Report** menu and choose the desired report:
 - **Selected Group(s) - HTML**
 - **All Groups - HTML**
4. The report opens in a browser window.

Leaps

Leap Editor

Leaps retrieve related documents or information.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

Leap Types

There are five types of leaps:

LEAP TYPE	DESCRIPTION	SUPPORTED IN FDD CLIENT?	SUPPORTED IN WEBFDD?	SUPPORTED IN QUICK INTEGRATOR?
Application Leap	Sends keystrokes to an external application.	✓		✓
File Cabinet Leap	Searches a file cabinet for related documents.	✓	✓	
Highlight Leap	Searches a file cabinet on a word or phrase that has been highlighted and copied to your clipboard.	✓		
SQL Leap	Performs a SQL query. The query can include file cabinet field values.	✓	✓	
URL Leap	Opens a browser window and goes to a URL. The URL can include file cabinet field values.	✓	✓	✓

Create Application Leap

An **application leap** sends keystrokes to an external application.

To create an application leap:

1. Choose **File>Leaps**. The **Leap Editor** opens.
2. Choose **File>New>Application Leap**. The **New Application Leap** screen opens.
3. Enter a **Leap Name**.
4. Choose a **Base File Cabinet** from the drop-down list.
5. Enter the **Terminal Program** name.
6. Choose an **Access Group** from the drop-down list.
7. Add the leap commands. Commands can be combined to create a series of actions.
 - To send keystrokes:
 - a. Click **Keystrokes**. The **Send Keystrokes** screen opens.
 - b. Enter the keystrokes in the text field. To insert commonly used keystrokes or file cabinet field values: choose the value from the **Insert Keystroke For** or **Insert Field Value** drop-down list and click **Insert**.
 - c. Click **OK**. You are returned to the **Application Leap** screen.
 - To wait for a window to appear:
 - a. Click **Wait for Window**. The **Wait for Window** screen opens.
 - b. Enter the **Window Name**.
 - c. Click **OK**. You are returned to the **Application Leap** screen.
 - To add a pause:
 - a. Click **Pause**. The **Pause** screen opens.
 - b. Enter the length of time (in seconds) to pause. (The pause must be between 1 - 9 seconds.)
 - c. Click **OK**. You are returned to the **Application Leap** screen.
 - To edit a command, highlight the command and click **Modify**.
 - To delete a command, highlight the command and click **Delete**.
 - Use the up and down arrows to reorder commands.

New Application Leap

Leap Name:

Base File Cabinet:

Terminal Program:

Access Group:

Pause for 3 Second(s)
Send Keystrokes: "<FC_VALUE:Employee_ID>"
Send Keystrokes: "~"
Send Keystrokes: "<FC_VALUE:First_Name>"
Send Keystrokes: "~"
Send Keystrokes: "<FC_VALUE>Last_Name>"

- Click **OK** to save the leap and return to the **Leap Editor**.

Create File Cabinet Leap

A **file cabinet leap** searches a file cabinet for related documents.

To create a file cabinet leap:

1. Choose **File>Leaps**. The **Leap Editor** opens.
2. Choose **File>New>File Cabinet Leap**. The **New File Cabinet Leap** screen opens.
3. Enter a **Leap Name**.
4. Choose a **Base File Cabinet** from the drop-down list.
5. Choose a **Leap To File Cabinet** from the drop-down list.
6. Choose an **Access Group** from the drop-down list.
7. Set the leap mapping:
 - To add mapping fields:
 - a. Click **Add**. The **Leap Mapping** screen opens.
 - b. Choose the **Map Field** from the drop-down list.
 - c. Choose the **To Field** from the drop-down list.
 - d. Click **OK**. You are returned to the **File Cabinet Leap** screen.
 - To add another mapping, click the **Add** button to open the **Leap Mapping** dialog again.
 - To delete a mapping, highlight the mapping in the list and click **Delete**.
 - **Tip:** If you map the same **From** field twice to two different **To** fields, FDD Client will take the value in the **From** field and search for it in both **To** fields using OR logic. The value can be in either field for a document to be returned.

If you map two different **From** fields to the same **To** field twice, FDD Client will take the values in the **From** fields and search for them both in the one **To** field using OR logic. Either value can be in the field for a document to be returned.

From Field	To Field
Invoice_ID	Invoices

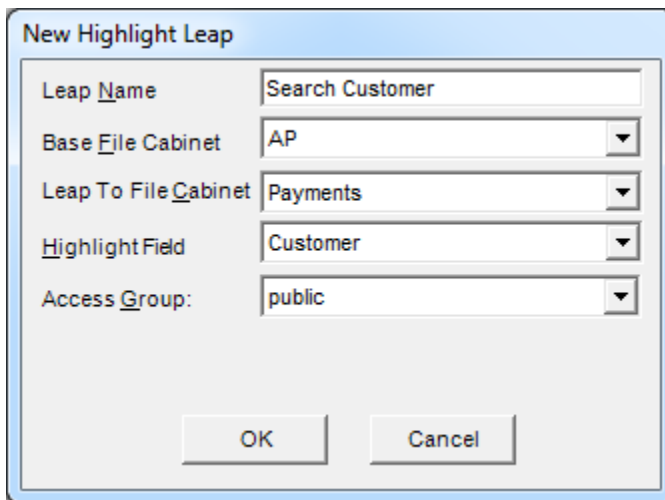
8. Click **OK** to save the leap and return to the **Leap Editor** screen.

Create Highlight Leap

A **highlight leap** searches a file cabinet on a word or phrase that has been highlighted and copied to your clipboard.

To create a highlight leap:

1. Choose **File>Leaps**. The **Leap Editor** opens.
2. Choose **File>New>Highlight Leap**. The **New Highlight Leap** screen opens.
3. Enter a **Leap Name**.
4. Choose a **Base File Cabinet** from the drop-down list.
5. Choose a **Leap To File Cabinet** from the drop-down list.
6. Choose a **Highlight Field** from the drop-down list. The copied value is pasted into this field as search criteria.
7. Choose an **Access Group** from the drop-down list.



The screenshot shows a dialog box titled "New Highlight Leap". It contains the following fields and values:

Field	Value
Leap Name	Search Customer
Base File Cabinet	AP
Leap To File Cabinet	Payments
Highlight Field	Customer
Access Group	public

At the bottom of the dialog are two buttons: "OK" and "Cancel".

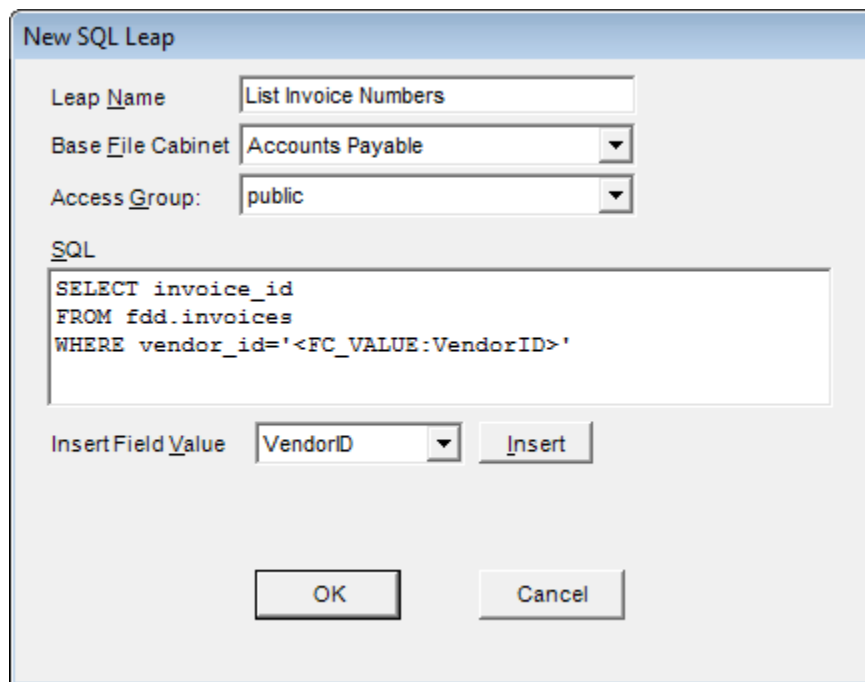
8. Click **OK** to save the leap and return to the **Leap Editor** screen.

Create SQL Leap

A **SQL leap** performs a SQL query and displays the results in a grid. The SQL query can include file cabinet field values.

To create a SQL leap:

1. Choose **File>Leaps**. The **Leap Editor** opens.
2. Choose **File>New>SQL Leap**. The **New SQL Leap** screen opens.
3. Enter a **Leap Name**.
4. Choose a **Base File Cabinet** from the drop-down list.
5. Choose an **Access Group** from the drop-down list.
6. Enter the SQL query in the text field. To insert a file cabinet field value: choose the value from the **Insert Field Value** drop-down list and click **Insert**.



New SQL Leap

Leap Name: List Invoice Numbers

Base File Cabinet: Accounts Payable

Access Group: public

SQL

```
SELECT invoice_id
FROM fdd.invoices
WHERE vendor_id='<FC_VALUE:VendorID>'
```

Insert Field Value: VendorID Insert

OK Cancel

7. Click **OK** to save the leap and return to the **Leap Editor** screen.

Create URL Leap

A **URL leap** opens a browser window and goes to a URL. The URL can include file cabinet field values.

To create a URL leap:

1. Choose **File>Leaps**. The **Leap Editor** opens.
2. Choose **File>New>URL Leap**. The **New URL Leap** screen opens.
3. Enter a **Leap Name**.
4. Choose a **Base File Cabinet** from the drop-down list.
5. Choose an **Access Group** from the drop-down list.
6. Enter the URL in the text field. To insert a file cabinet field value: choose the value from the **Insert Field Value** drop-down list and click **Insert**.

New URL Leap

Leap Name: Show Invoices

Base File Cabinet: AP

Access Group: public

URL

http://localhost:80/webfdd/url.do?a=2&fn=AP&VendorName=<FC_VALUE:VendorName>

Insert Field Value: Field VendorName

Insert

OK **Cancel**

7. Click **OK** to save the leap and return to the **Leap Editor** screen.

Manage Leaps

Modify Leap

To modify a leap:

1. Choose **File>Leaps**. The **Leap Editor** opens, listing leaps by name, type and base file cabinet.
Note: A mid-level administrator is limited in what leaps they can modify.
2. In the **Leap Editor**, right-click a leap and select **Modify**. The **Modify Leap** screen opens.
3. Make any change and click **OK**. You are returned to the **Leap Editor**.
4. Choose **File>Exit** to return to the Feith Control Panel main screen.

Delete Leap

To delete a leap:

1. Choose **File>Leaps**. The **Leap Editor** opens, listing leaps by name, type and base file cabinet.
Note: A mid-level administrator is limited in what leaps they can delete.
2. In the **Leap Editor**, right-click a leap and select **Delete**.
3. Answer **Yes** to the confirmation prompt. The leap is deleted.
4. Choose **File>Exit** to return to the Feith Control Panel main screen.

Licenses

License Manager

License Your FDD System

You must license your FDD system in order to create users, groups, bins, file cabinets, pages, documents, folders, workflows, workflow users, workflow tasks and virtual file cabinets.

Your license file is based on your **FDD System ID** and must be obtained from the Feith Systems and Software, Inc.

To find your FDD system ID:

- Select **File>Licenses**. The **Feith License Manager** opens; the **System ID** is listed at the top of the screen.

To import your license file and license your FDD system:

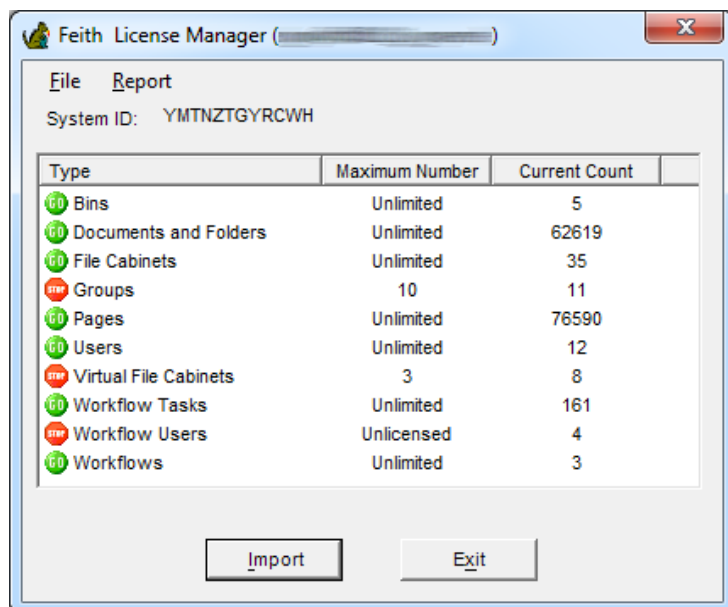
1. Select **File>Licenses**. The **Feith License Manager** opens.
2. Select **File>Import**. The **File Open** dialog opens.
3. Browse for and import your license file (.dat file).

After you have licensed your system, the **Feith License Manager** displays the current count and maximum number of FDD system objects.


Check Your License Count

Select **File>Licenses**. The **Feith License Manager** opens, displaying the current count and maximum number of FDD system objects.

If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.



In the example shown, **10** of the available **10** virtual file cabinet licenses have been used, and **5** of the available **50** workflow user licenses have been used. All other FDD system objects shown have an unlimited number of licenses.

The red STOP icon  indicates that all licenses for an object type have been used.

Locks

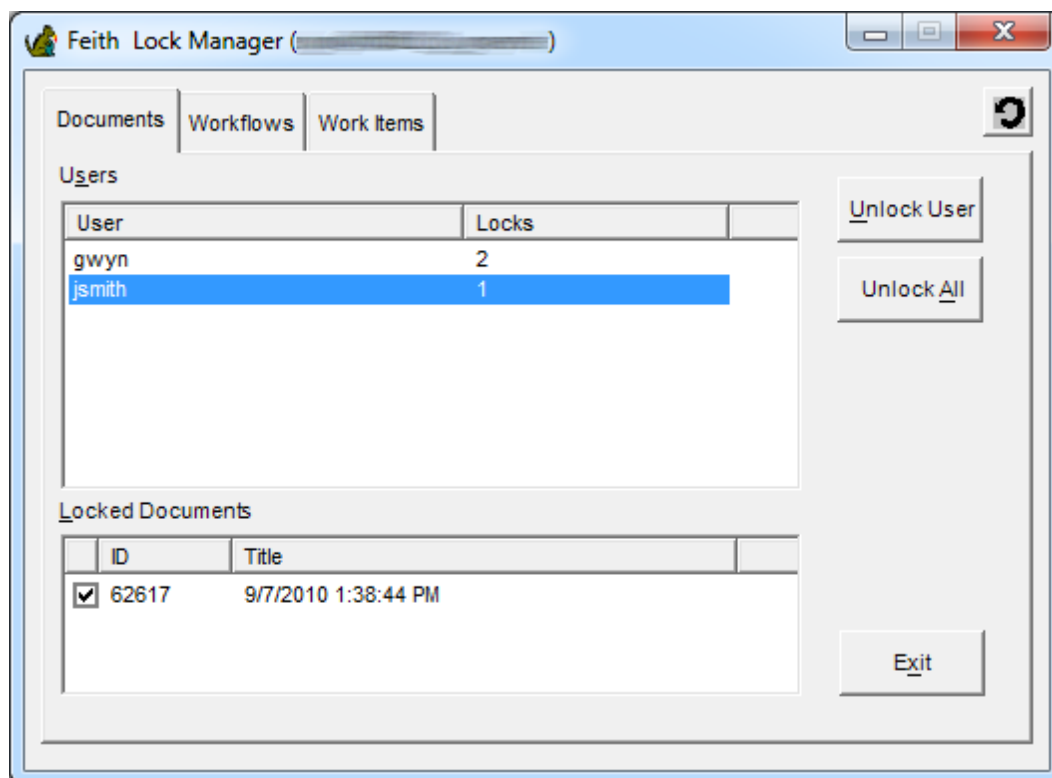
Lock Manager

Use the **Lock Manager** to unlock locked documents, workflows and work items.

Note the term "locked document" refers to both locked documents (indexed pages in file cabinets) and locked batches (non-indexed pages in bins).

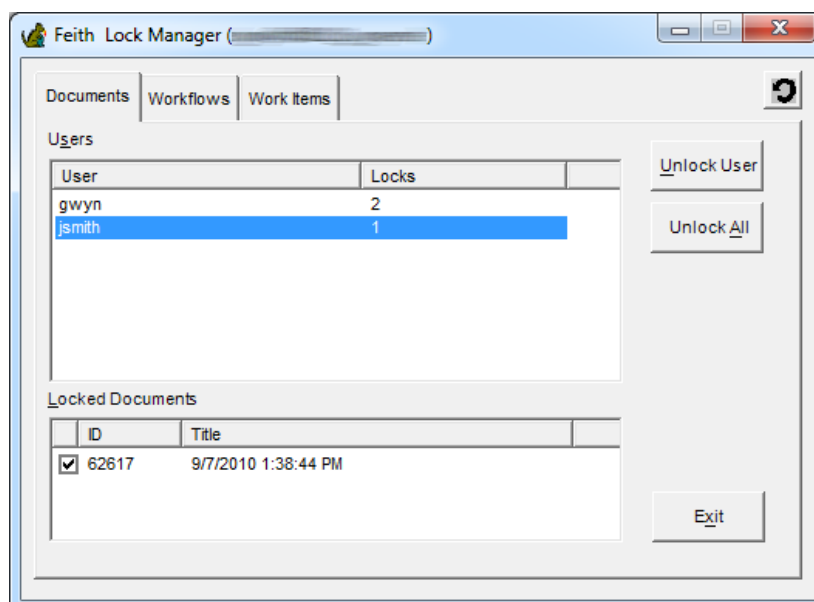
To unlock a locked document:

1. Select **File>Locks**. The **Lock Manager** opens.
2. Select the **Documents** tab.
3. Select a user from the **Users** list. The user's locked documents display in the **Locked Documents** list.
4. Uncheck the box next to the document's ID and title. The document is unlocked.



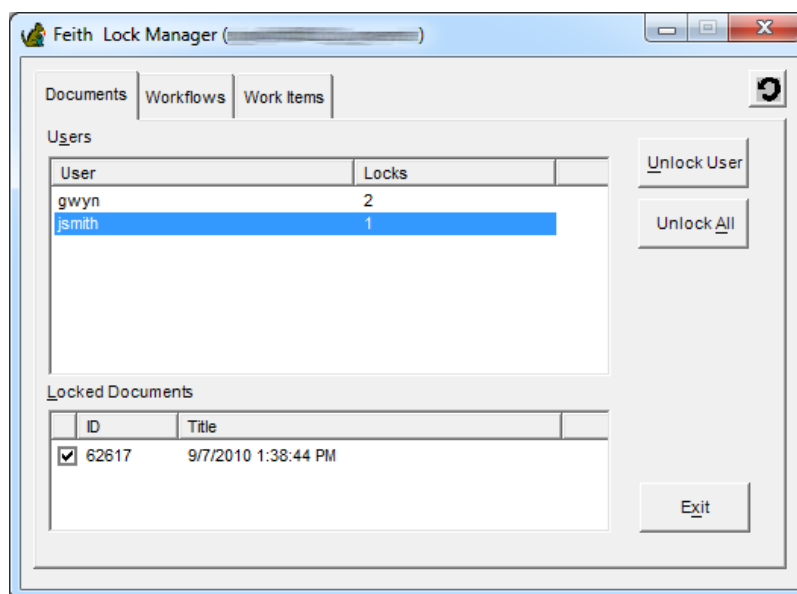
To unlock a user's locked documents:

1. Select **File>Locks**. The **Lock Manager** opens.
2. Select the **Documents** tab.
3. Select the user from the **Users** list. The user's locked documents display in the **Locked Documents** list.
4. Click the **Unlock User** button. All documents locked by this user are unlocked.



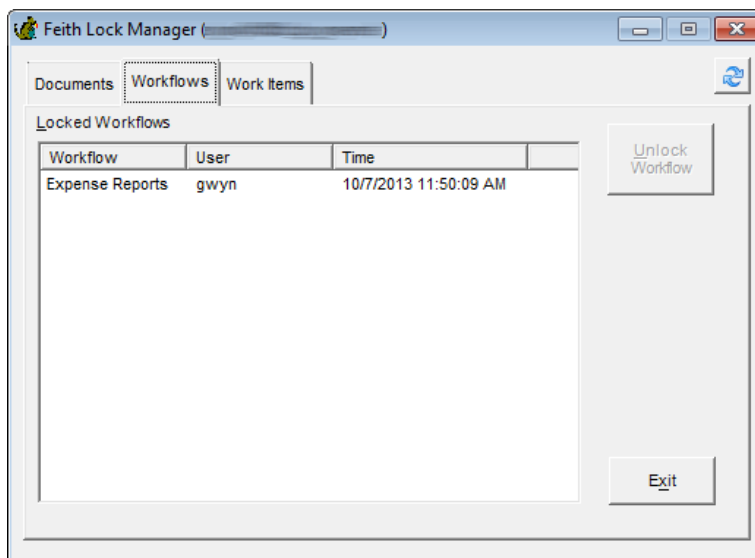
To unlock all locked documents:

1. Select **File>Locks**. The **Lock Manager** opens.
2. Select the **Documents** tab.
3. Click the **Unlock All** button. All locked documents are unlocked.



To unlock a locked workflow:

1. Select **File>Locks**. The **Lock Manager** opens.
2. Select the **Workflows** tab.
3. Select a workflow from the **Locked Workflows** list.
4. Click **Unlock Workflow**.

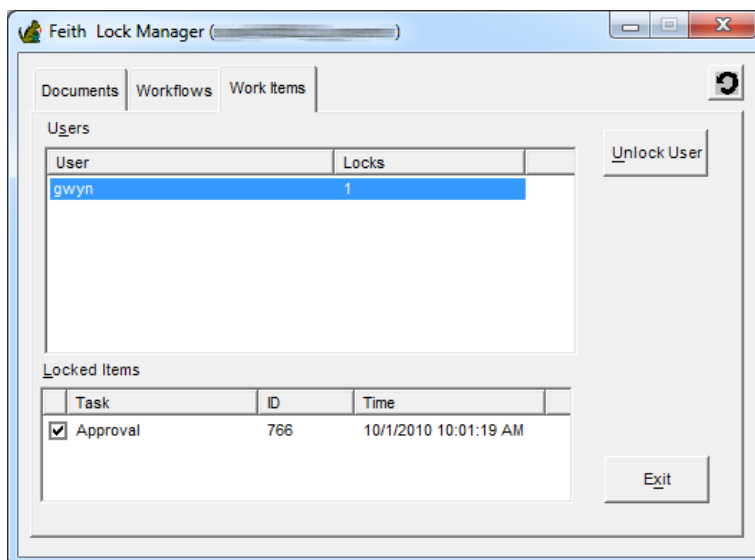


5. Answer **Yes** to the confirmation prompt. The workflow is unlocked.

The **Workflows** tab only appears to users with the **Workflow** Administration permission.

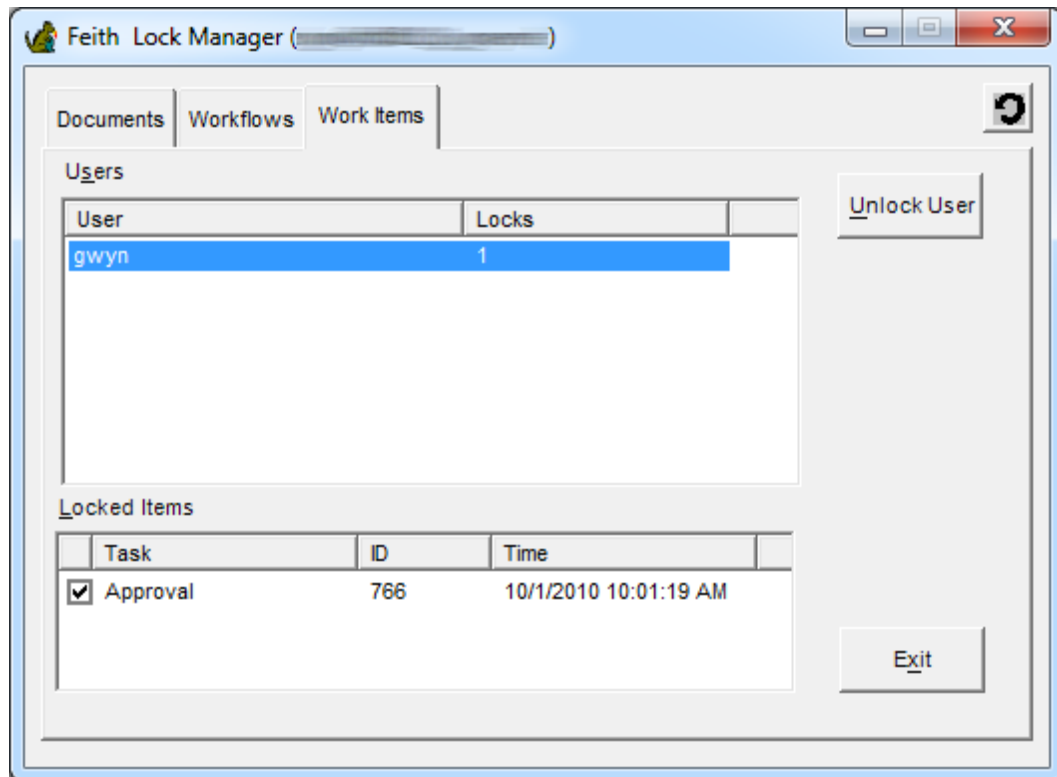
To unlock a locked work item:

1. Select **File>Locks**. The **Lock Manager** opens.
2. Select the **Work Items** tab.
3. Select a user from the **Users** list. The user's locked work items display in the **Locked Items** list.
4. Uncheck the box next to the item's ID and task name. The item is unlocked.



To unlock a user's locked work items:

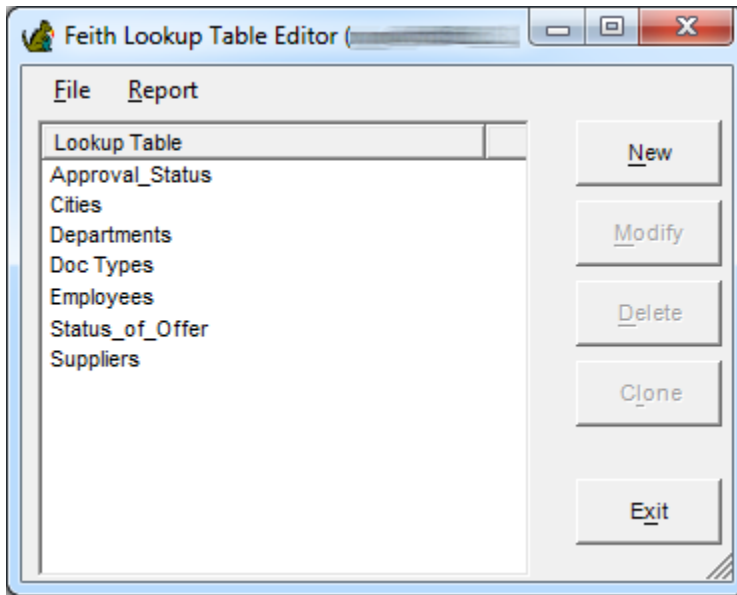
1. Select **File>Locks**. The **Lock Manager** opens.
2. Select the **Work Items** tab.
3. Select the user from the **Users** list. The user's locked work items display in the **Locked Items** list.
4. Click the **Unlock User** button. All work items locked by this user are unlocked.



Lookup Tables

Lookup Tables

A **lookup table** provides a list of suggested values for use when indexing or searching for documents. A lookup table can be assigned to a file cabinet field when adding a field or when modifying the properties of an existing field. See [Set File Cabinet Field Options](#) for instructions on assigning a lookup table to a file cabinet field.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

System Lookup Tables

The following system file cabinets are created during the FDD installation. These file cabinets are created for use with FDD applications.

FILE CABINET	DESCRIPTION
doc_types	Sample lookup table
report_printers	Report Printers lookup table used by Feith Reports iQ
rma_disposition_locations	RMA Disposition Locations lookup table used by Feith RMA iQ File Plan Administrator

Add Lookup Table

To add a lookup table:

1. Select **File>Lookup Tables**. The **Lookup Table Editor** opens, listing all FDD lookup tables.
2. Click **New** to open the **Create New Lookup Table** screen.
3. Enter the lookup table name in the **Name** field. A maximum of 16 characters is accepted for the lookup table name.
4. Click **Add** to open the **Lookup Column** screen. Enter the **Name**, **Type**, and **Length** of the lookup column and click **OK**. The column is added to the lookup table.

A maximum of 16 characters is accepted for the lookup column name.

5. Optionally add another column. To delete a column, select the column and click **Delete**.

Create New Lookup Table

Name:

Columns:

Name	Type	Length	Scale
Abbreviation	String	2	
Name	String	64	

Buttons: **Add**, **Modify**, **Delete**

Buttons: **OK**, **Cancel**

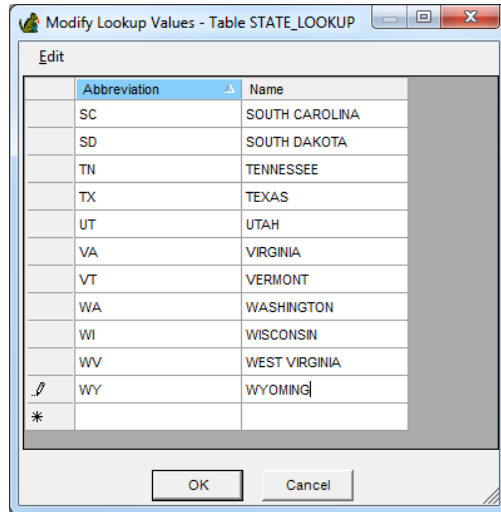
6. Click **OK** to create the table. The **Modify Lookups Values** screen opens so values can be entered for the new table.
7. Enter the lookup values in the grid.

Use the **TAB** key to navigate between columns left-to-right. When you are in the last column, hitting **TAB** takes you to the first column in the next row. Use **SHIFT+TAB** to move in the reverse direction, right-to-left. Alternatively, you can use the arrow keys to navigate the grid.

With a cell selected, use **F2** to enter edit mode in that cell.

To copy one or more existing rows and paste as new rows: Select the rows in the grid, then right-click and choose **Copy Rows**. The selected rows are copied and pasted as new rows in the table. This option may be useful if you need to copy and edit values when modifying an existing lookup table.

To fill cells with a selected value: Select the cell containing the value you want to copy, then drag the cursor and select the cells you want to fill, and then right-click and choose **Fill Cells**. The cells are filled with the value.



The lookup values can be sorted by clicking on one of the column headers. See [Sort Lookup Values](#) for more information.

You can automatically adjust the width of the columns by right-clicking in the grid and selecting **Auto-Fit**. The available fit options are:

- **To Data:** Columns adjusted to width of data.
- **To Header:** Columns adjusted to width of column header labels.
- **Best Fit:** Columns adjusted to width of data or column header labels, whichever is longer.

The following options are available under the **Edit** menu:

- **Find:** Opens the **Find** dialog so you can find text within the lookup values. Find options include: **Find Whole Word**, **Match Case**, **Direction**, **Current Column Only** and **Find Next**.
 - **Find Next:** Finds the next occurrence of the text entered in the **Find** dialog.
 - **Modify Columns:** Opens the **Modify Lookup Table** dialog so you can add a new column to the lookup table, modify the properties of an existing column, or delete a column from the table. When modifying existing columns, the following changes are supported: length can be increased for string columns, and length and scale can be increased for decimal columns.
 - **Clear All Values:** Clears all lookup values in the grid.
 - **Import Values:** Imports lookup values from a pipe-delimited .txt file.
 - **Export Values:** Exports lookup values to a pipe-delimited .txt file.
 - **With Column Headers:** Exports lookup values with the column headers. **Note:** If you use this file to import values to a lookup table, the column headers will be imported as values.
 - **Without Column Headers:** Exports lookup values without the column headers.
8. Click **OK** when you are done adding lookup values. The values are saved and you are returned to the **Lookup Table Editor**.
 9. Exit the **Lookup Table Editor** to return to the main **FDD Control Panel** screen.

See [Set File Cabinet Field Options](#) for instructions on assigning a lookup table to a file cabinet field. For convenience, lookup tables can also be created when adding or modifying file cabinet fields.

Modify Lookup Table

To modify a lookup table:

1. Select **File>Lookup Tables**. The **Lookup Table Editor** opens, listing all **FDD** lookup tables.
2. Select a table and click **Modify** to open the **Modify Lookup Values** screen.

The lookup values can be sorted by clicking on one of the column headers. See [Sort Lookup Values](#) for more information.

You can automatically adjust the width of the columns by right-clicking in the grid and selecting **Auto-Fit**. The available fit options are:

- **To Data:** Columns adjusted to width of data.
 - **To Header:** Columns adjusted to width of column header labels.
 - **Best Fit:** Columns adjusted to width of data or column header labels, whichever is longer.
3. Modify the lookup values as needed.

Use the **TAB** key to navigate between columns left-to-right. When you are in the last column, hitting **TAB** takes you to the first column in the next row. Use **SHIFT+TAB** to move in the reverse direction, right-to-left. Alternatively, you can use the arrow keys to navigate the grid.

With a cell selected, use **F2** to enter edit mode in that cell.

To copy one or more existing rows and paste as new rows: Select the rows in the grid, then right-click and choose **Copy Rows**. The selected rows are copied and pasted as new rows in the table. This option may be useful if you need to copy and edit values when modifying an existing lookup table.

To fill cells with a selected value: Select the cell containing the value you want to copy, then drag the cursor and select the cells you want to fill, and then right-click and choose **Fill Cells**. The cells are filled with the value.

The following options are available under the **Edit** menu:

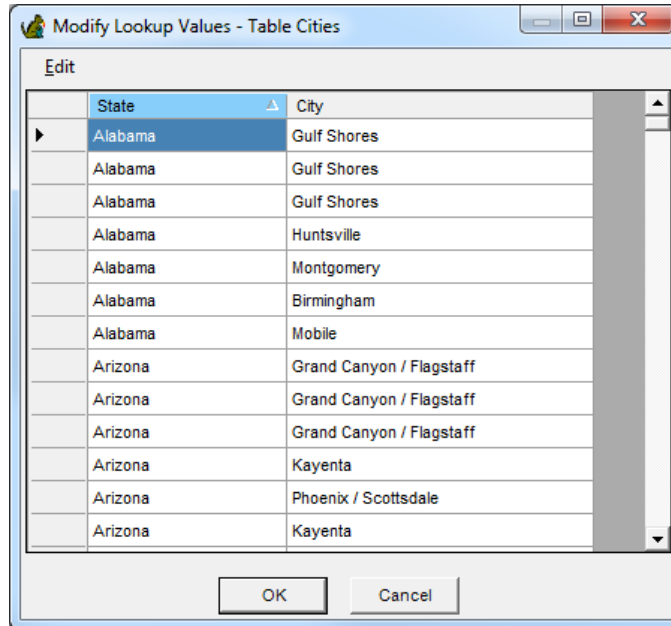
- **Find:** Opens the **Find** dialog so you can find text within the lookup values. Find options include: **Find Whole Word**, **Match Case**, **Direction**, **Current Column Only** and **Find Next**.
 - **Find Next:** Finds the next occurrence of the text entered in the **Find** dialog.
 - **Modify Columns:** Opens the **Modify Lookup Table** dialog so you can add a new column to the lookup table, modify the properties of an existing column, or delete a column from the table. When modifying existing columns, the following changes are supported: length can be increased for string columns, and length and scale can be increased for decimal columns.
 - **Clear All Values:** Clears all lookup values in the grid.
 - **Export Values:** Exports lookup values to a pipe-delimited .txt file.
 - **With Column Headers:** Exports lookup values with the column headers. **Note:** If you use this file to import values to a lookup table, the column headers will be imported as values.
 - **Without Column Headers:** Exports lookup values without the column headers.
 - **Import Values:** Imports lookup values from a pipe-delimited .txt file.
4. Click **OK** when you are done modifying the lookup values. The changes are saved and you are returned to the **Lookup Table Editor**.

Sort Lookup Values

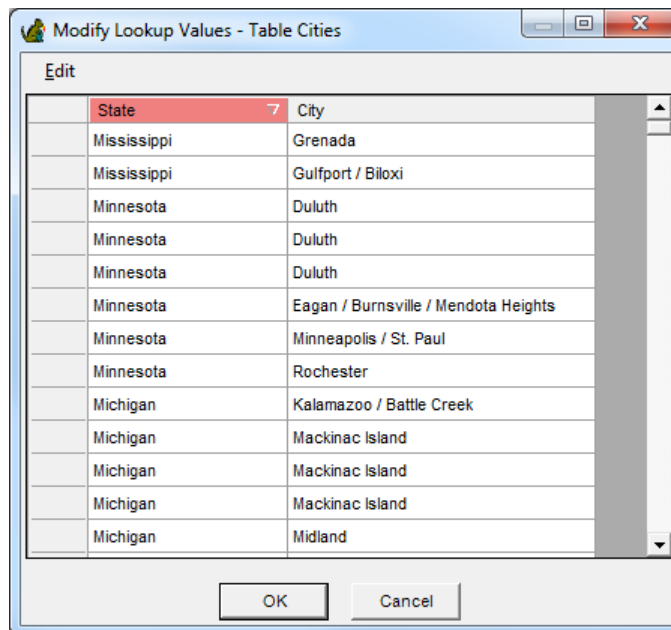
The values in a lookup table can be sorted by any column or by multiple columns. By default, the lookup table is sorted by the first column in ascending order.

To sort values by a column:

1. Click on the column header. The column header turns blue to indicate the values are sorted in ascending order.



2. Click the column header a second time to reverse the sort order. The column header turns red to indicate the values are sorted in descending order.

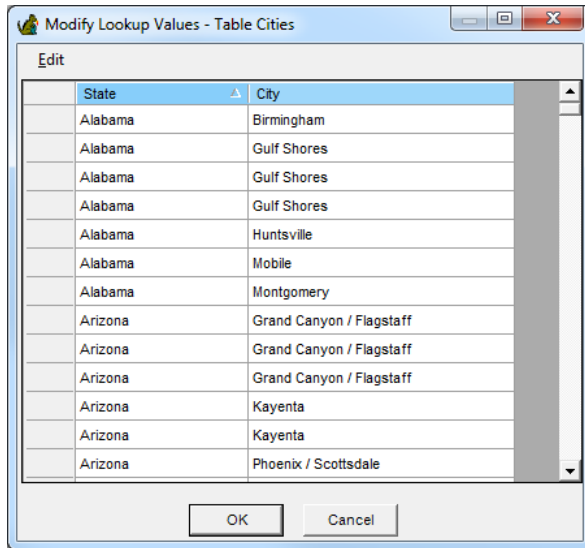


To sort values by multiple columns:

1. Click on a column header as necessary to get the desired sort order. The column header changes color to indicate the sort order as ascending (blue) or descending (red).
2. Click another column header as necessary to get the desired sort order.

The last column clicked is the primary sort. For example, if you click the "City" column header then the "State" column header, the primary sort will be on "State" and the secondary sort will be on "City".

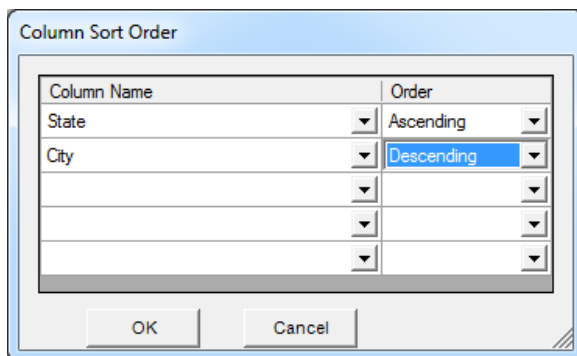
The headers of the columns used for secondary and lesser sorts are indicated with lighter shades of blue (ascending) or red (descending).



3. Continue to click column headers as desired to get a multi-column sort. Multi-column sort is supported up to five columns.

To sort values using the Column Sort Order interface:

1. Right-click in the lookup grid and select **Sort Order**. The **Column Sort Order** dialog opens.



2. In the first row, select the **Column Name** of the column you want to use for the primary sort, then choose the desired sort **Order** on that column.
3. If desired, select more columns to sort by. You can sort by up to five columns.
4. Click **OK**. You are returned to the lookup grid and the values are sorted.

Clone Lookup Table

Cloning a lookup table will copy both the lookup table structure and the lookup table values.

To clone an existing lookup table:

1. Select **File>Lookup Tables**. The **Lookup Table Editor** opens, listing all FDD lookup tables.
2. Select a lookup table and click **Clone**. The **Clone Lookup Table** screen opens.
3. Enter the **New Lookup Table Name** and click **OK**. The **Copy Values** window opens, displaying the values from the original lookup table.
4. Modify the lookup table columns and values as needed, then click **OK**. The lookup table is added and you are returned to the **Lookup Table Editor**.

Note: To clone the lookup table structure without copying the values, click **Cancel** on the **Copy Values** screen. The new table will be added with 0 rows.

Delete Lookup Table

To delete a lookup table:

1. Select **File>Lookup Tables**. The **Lookup Table Editor** opens, listing all FDD lookup tables.
2. Select a table and click **Delete**.
3. Answer **Yes** to the confirmation prompt.
4. If the lookup table is assigned to any file cabinet fields, you are asked whether or not to delete the assignments. Answer **Yes** to remove the assignments; answer **No** to retain the assignments.

If the assignments are not removed, users may receive an error trying to open a deleted lookup table when indexing or searching in FDD or WebFDD. To remove the lookup table assignment from a specific file cabinet field, modify the file cabinet field options and clear the lookup table selection.

Export and Import Lookup Table

The lookup table export and import options can be used to copy a lookup table from one FDD database to another FDD database. For example, this feature can be used to export a lookup table from a test system and import the lookup table into a production system.

The export and import process copies over both the lookup table structure and the lookup table values.

To export a lookup table:

1. Select **File>Lookup Tables**. The **Feith Lookup Table Editor** opens, listing all FDD lookup tables.
2. Select a lookup table and select **File>Export**. The **File Save** dialog opens.

You can select multiple lookup tables using **SHIFT+click** or **CTRL+click**.

3. Browse to select a destination path and file name for the lookup table export file, then click OK. The lookup table design is exported to an XML file.

To import a lookup:

1. Open the **Feith Lookup Table Editor** and select **File>Import**. The **File Open** dialog opens.
2. Browse to select the lookup table export file and click **OK**. You are prompted whether to import the lookup table; answer **Yes** to import.
3. When the import is complete, a success message is shown and you are returned to the **Feith Lookup Table Editor**; the imported lookup table is included in the lookup table list.

Note: A file cabinet export includes the lookup tables that are assigned to the file cabinet. See [Export and Import File Cabinet](#) for instructions on adding lookup tables to the FDD system during a file cabinet import.

Lookup Table Reports

Two lookup table reports are available: **Selected Lookup Tables** and **All Lookup Tables**.

The **Selected Lookup Tables** report lists the lookup table properties, lookup table column properties, and file cabinets and tasks that use the lookup table. This report is in HTML format.

The **All Lookup Tables** report lists all lookup tables by name. This report is in HTML format.

To generate a lookup table report:

1. Select **File>Lookup Tables**. The **Feith Lookup Table Editor** opens.
2. Optionally select a lookup table.
3. Select the **Report** menu and choose the desired report:
 - **Selected Lookup Tables - HTML**
 - **All Lookup Tables - HTML**
4. The report opens in a browser window.

Messages

Message Editor

A **logon message** displays on logon to FDD and WebFDD. The user will need to click **OK** to the message in order to launch the application. An effective date range and access group can be set for each message.

To add a logon message:

1. Select **Messages** from the **File** menu. The **Feith Message Editor** opens, listing all the messages.

If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.
2. Click **New**. The **Logon Message** window opens.
3. Enter the following properties:
 - **Subject:** Enter the logon message subject. A maximum of 32 characters is accepted. The subject value will display on the title bar of the login message.
 - **Message:** Enter the logon message text.
 - **Show To:** Choose the access group of the logon message. The message will only display to users in the selected group.
 - **Buttons:** Choose what buttons should be shown when the message displays. Choices are **OK and Cancel** or **OK Only**. FDD and WebFDD users will need to click **OK** to the message to launch the application; if the user cancels the message, the application will not be launched.
 - **Effective:** Choose the initial date that the message should display. Choices are **Immediately** or a specified date. To display the calendar control when selecting a date, click the down arrow in the date field.
 - **Expires:** Choose the last date that the message should display. Choices are **Never** or a specified date. To display the calendar control when selecting a date, click the down arrow in the date field.
4. Click **OK**. The message is added and you are returned to the **Feith Message Editor**.

To modify a logon message:

1. Select **Messages** from the **File** menu. The **Feith Message Editor** opens, listing messages by subject and access group.

Note: A mid-level administrator is limited in which messages they can modify. See [Levels of Administrators](#) for more information.
2. Select a message and click **Modify**. The **Logon Message** dialog opens.
3. Change any property and click **OK**. The properties are modified and you are returned to the **Feith Message Editor**.

To delete a logon message:

1. Select **Messages** from the **File** menu. The **Feith Message Editor** opens.

Note: A mid-level administrator is limited in which messages they can delete. See [Levels of Administrators](#) for more information.
2. Select a message and click **Delete**, then answer **Yes** to the confirmation prompt. The message is deleted.

Redaction Reason Codes

Redaction Code Editor

Redaction reason codes are a centrally maintained list of codes that can be applied to redacted areas of FDD documents. Redaction notes can be applied to documents in either the FDD Windows client or WebFDD.

To add a redaction reason code:

1. From the **File** menu, select **Redaction Reason Codes**. The **Feith Redaction Code Administrator** opens, listing all the codes.

If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

2. Click **New**. The **Add New Reason Code** dialog opens.
3. Enter the following properties:
 - **Code Name**: Enter the code name. A maximum of 32 characters is accepted. This value will display over the redacted area.
 - **Description**: Enter the code description. This value will be listed next to the code when selecting the code in the clients.
4. Click **OK**. You are returned to the **Feith Redaction Code Administrator** and the new code is added to the reason code list.

To modify a redaction reason code:

1. From the **File** menu, select **Redaction Reason Codes**. The **Feith Redaction Code Administrator** opens.
2. Select a reason code and click **Modify**. The **Modify Reason Code** dialog opens.
3. Change any property and click **OK**. The properties are modified and you are returned to the **Feith Redaction Code Administrator**.

To delete a redaction reason code:

1. From the **File** menu, select **Redaction Reason Codes**. The **Feith Redaction Code Administrator** opens.
2. Select a reason code and click **Delete**.
3. Answer **Yes** to the confirmation prompt.
4. You are asked to reassign existing redactions with this reason code to another code. Choose a code from the list and click **OK**.

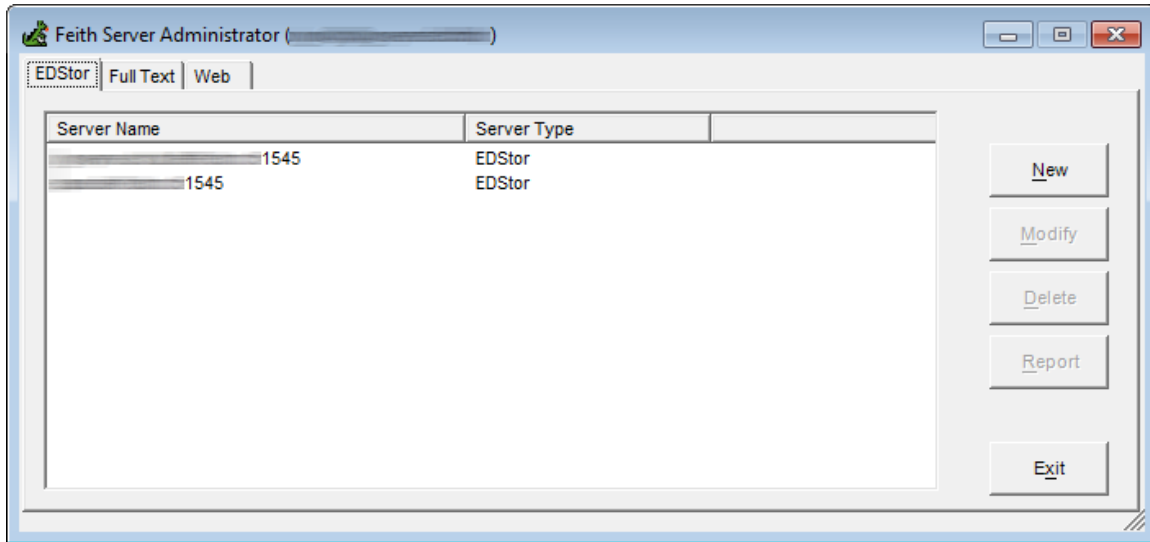
To generate a redaction code report:

1. Select **File>Redaction Reason Codes**. The **Feith Redaction Code Administrator** opens.
2. Select the **Report** menu and choose the **All Redaction Codes** option. The report opens in a browser window.

Servers

Servers

Create and manage server entries, which are used by Feith applications to call server applications. For example, the server entry for Forms iQ allows the clients to call Forms iQ Server when displaying submitted forms in file cabinets.



If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

Server Types

SERVER TYPE	DESCRIPTION
EDStor	Stores the pages for your documents and a few other objects.
Full Text	Stores the text from FDD documents, making them full text searchable. We support the Elasticsearch and Autonomy IDOL full text servers.
Web	A web server is an application installed on a server that you can access from workstations in a browser. E.g. WebFDD, Forms iQ, Dashboard iQ, and more.

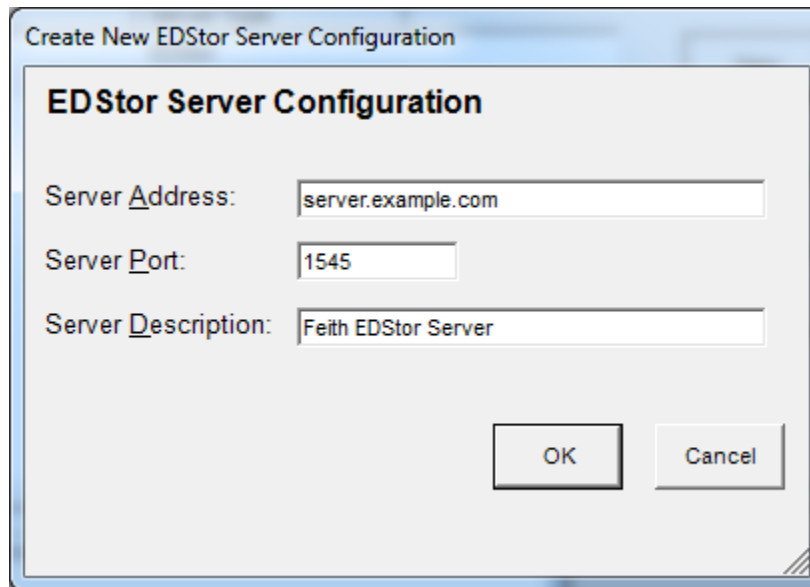
Add Server Entry

Add EDStor Server Entry

An **EDStor Server** is a storage server controlled by **Feith EDStor** software.

To add an **EDStor Server** entry:

1. Select **File>Servers**. The **Server Administrator** screen opens.
2. Select the **EDStor** tab.
3. Click **New**. The **EDStor Server Configuration** screen opens.
4. Enter the **Server Address** and **Server Port**. Optionally enter a **Server Description**.



Create New EDStor Server Configuration

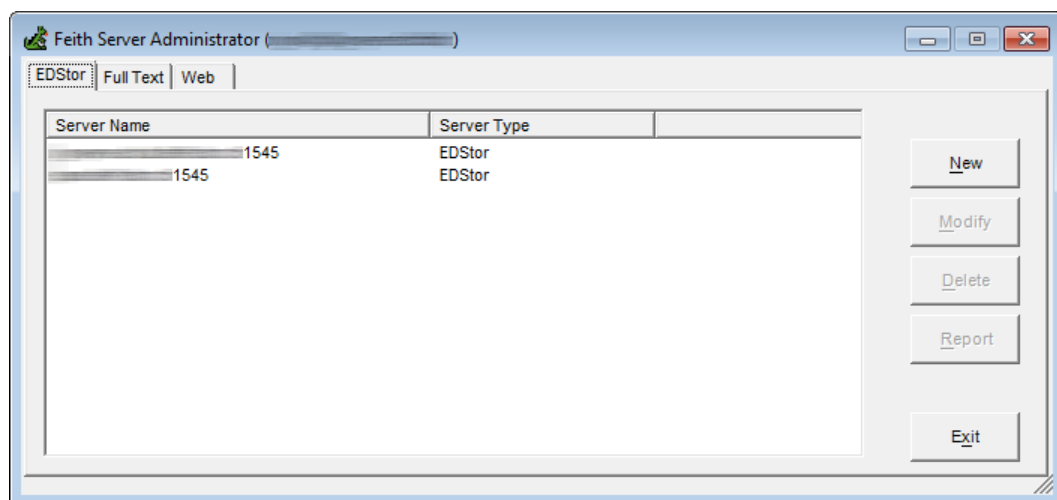
EDStor Server Configuration

Server Address:

Server Port:

Server Description:

5. Click **OK**. The server entry is added and you are returned to the **Server Administrator** screen.



Feith Server Administrator

EDStor | Full Text | Web

Server Name	Server Type
1545	EDStor
1545	EDStor

Add Full Text Server Entry

A **Full Text Server** is a text retrieval server controlled by **Elasticsearch** or **Autonomy IDOL** software.

To add a **Full Text Server** entry:

1. Select **File>Servers**. The **Server Administrator** screen opens.
2. Select the **Full Text** tab.
3. Click **New**. The **Full Text Server Configuration** screen opens.
4. Select the **Server Type**. Choices are **Elasticsearch**, **Autonomy IDOL Indexing**, or **Autonomy IDOL Querying**.

If you are using **Autonomy IDOL**, you need two server entries: One for the indexing server - **Autonomy IDOL Indexing** - and one for the querying server - **Autonomy IDOL Querying**.

5. Enter the **Server Address** and **Server Port**.
6. Enter the **Database Name**.

Note: The **Database Name** should be set as follows:

- If you are using **Elasticsearch**, the **Database Name** should be the name of the **Index** on the **Elasticsearch Server**.
- If you are using **Autonomy IDOL**, the **Database Name** should be the name of the **IDOL Database**.

7. Optionally enter a **Server Description**.

Example Configuration: Elasticsearch server entry.

The screenshot shows a Windows-style dialog box titled "Create New Full Text Server Configuration". Inside the dialog, the title "Full Text Server Configuration" is displayed. Below the title, there are five labeled input fields arranged vertically: "Server Type" (a dropdown menu showing "Elasticsearch"), "Server Address:" (a text box containing "server.example.com"), "Server Port:" (a text box containing "9200"), "Database Name:" (a text box containing "fdd"), and "Server Description:" (a text box containing "Elasticsearch Server"). At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

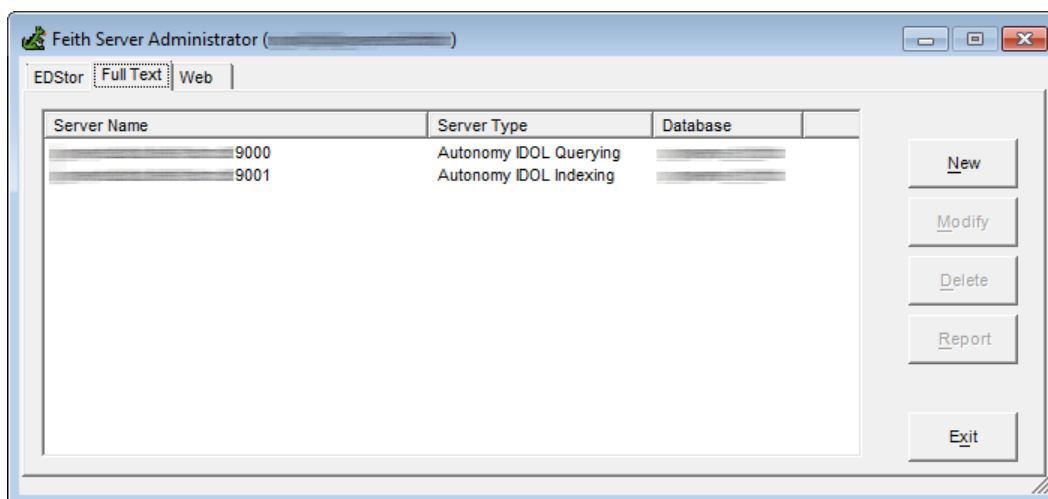
Example Configuration: Autonomy IDOL Indexing server entry.

The screenshot shows a Windows-style dialog box titled "Create New Full Text Server Configuration". Inside, there is a section titled "Full Text Server Configuration". It contains five input fields: "Server Type" is a dropdown menu with "Autonomy IDOL Indexing" selected; "Server Address:" is a text box with "server.example.com"; "Server Port:" is a text box with "9001"; "Database Name:" is a text box with "fdd"; and "Server Description:" is a text box with "Autonomy IDOL Indexing". At the bottom right, there are "OK" and "Cancel" buttons.

Example Configuration: Autonomy IDOL Querying server entry.

The screenshot shows a similar Windows-style dialog box titled "Create New Full Text Server Configuration". Inside, there is a section titled "Full Text Server Configuration". It contains five input fields: "Server Type" is a dropdown menu with "Autonomy IDOL Querying" selected; "Server Address:" is a text box with "server.example.com"; "Server Port:" is a text box with "9000"; "Database Name:" is a text box with "fdd"; and "Server Description:" is a text box with "Autonomy IDOL Querying". At the bottom right, there are "OK" and "Cancel" buttons.

8. Click **OK**. The server entry is added and you are returned to the **Server Administrator** screen.



Add Web Server Entry

Web server entries should be added for each Feith web application installed in your FDD system. Web server entries are also required for specific external web servers called by Feith applications; for example, you must add a Geomap Server entry if you are building geomap dashpods in Dashboard iQ Designer.

For example, to add a WebFDD web server entry:

1. Select **File>Servers**. The **Server Administrator** screen opens.
2. Select the **Web** tab.
3. Click **New**. The **Web Server Configuration** screen opens.
4. Select **WebFDD** the **Server Type**. See [below](#) for all server type choices.
5. In the **Server Address** field, enter the URL to the WebFDD application. See [below](#) for example URLs for all server types.
6. Optionally enter a **Server Description**.
7. Enter the **Database**. This is required for server entries added for Feith web applications.

The Database value must match the FDD database name entered during installation of the web application (the name of the connection in its configuration file). If they do not match, problems could occur later on.

8. Click **OK**. The WebFDD server entry is added and you are returned to the **Server Administrator** screen.

Server Name	Server Type	Database
http://.../dashboardiq	Dashboard iQ	
http://.../docview/vie...	Document Viewer	
http://.../feithdrive	FeithDrive	
http://.../formsiq	Forms iQ	
http://.../rma/workpla...	RMA iQ Properties	
http://.../webfdd	WebFDD	

We recommend you use the same database connection name in all your web servers' configuration files and therefore the same FDD Database Name for all your web server entries. Inconsistent database connection names could cause problems later on.

WEB SERVER TYPE	EXAMPLE WEB APPLICATION URL
Auditor iQ View dashboards and reports on audited activity and more in your FDD system.	http://yourserver/auditoriq
AutoCat Manager Configure rules for AutoCat Server to auto-categorize documents.	http://yourserver/autocat
CRE (Central Rendering Engine) Renders pages in various formats for Document Viewer and other applications.	http://yourserver/cre
Dashboard iQ (Server) View and track your organizations key performance indicators in dashboards you built in Dashboard iQ Designer.	http://yourserver/dashboardiq/home
Developer (Server) Serves up objects you coded in the Developer client.	http://yourserver/dataservices/rest/v1/api/developer
Document Viewer View documents, make notes, download pages, and more.	http://yourserver/docview/viewer
External Reference an external, 3rd-party application, such as MS SharePoint.	http://yoursharepoint/
FAST View and manage your documents in the FDD system using a web application.	http://yourserver/fast
FeithDrive Upload files into a private cloud to share and collaborate with coworkers.	http://yourserver/feithdrive
Forms iQ (Server) Upload files into a private cloud to share and collaborate with coworkers.	http://yourserver/formsiq

Geomap Reference and external, third-party geographical mapping server for Geomap pods in Dashboard iQ.	http://amappingservice
RMA iQ Properties View and update a record's RMA document properties, category, supplemental markings, and more.	http://yourserver/rmaiQ
WebFCP Administer your FDD system by creating and managing users, groups, file cabinets, permissions, and more, all in a web application.	http://yourserver/fcp
WebFDD View and manage your documents in the FDD system using a web application.	http://yourserver/webfdd

Manage Server Entries

Modify Server Entry

To modify a server entry:

1. Select **File>Servers**. The **Server Administrator** screen opens.
2. Select the **EDStor**, **Full Text**, **Database**, or **Web** tab.
3. Select a server entry and click **Modify**. (You can also double-click the server entry to open it for modification.) The **Modify Server Configuration** screen opens.
4. Change the server properties as needed and click **OK**. The server entry is modified and you are returned to the **Server Administrator** screen.

Delete Server Entry

To delete a server entry:

1. Select **File>Servers**. The **Server Administrator** screen opens.
2. Select the **EDStor**, **Full Text**, **Database**, or **Web** tab.
3. Select a server entry and click **Delete**.
4. Answer **Yes** to the confirmation prompt. The server entry is deleted.

Note: If objects in the FDD system are associated with the server, you will be prevented from deleting the server entry. For example, if pages are stored on an EDStor server, you will not be able to delete the EDStor server entry.

Server Reports

The server report lists the server properties.

To generate a server report:

1. Select **File>Servers**. The **Server Administrator** screen opens.
2. Select a server and click **Report**. The report opens in a browser window.

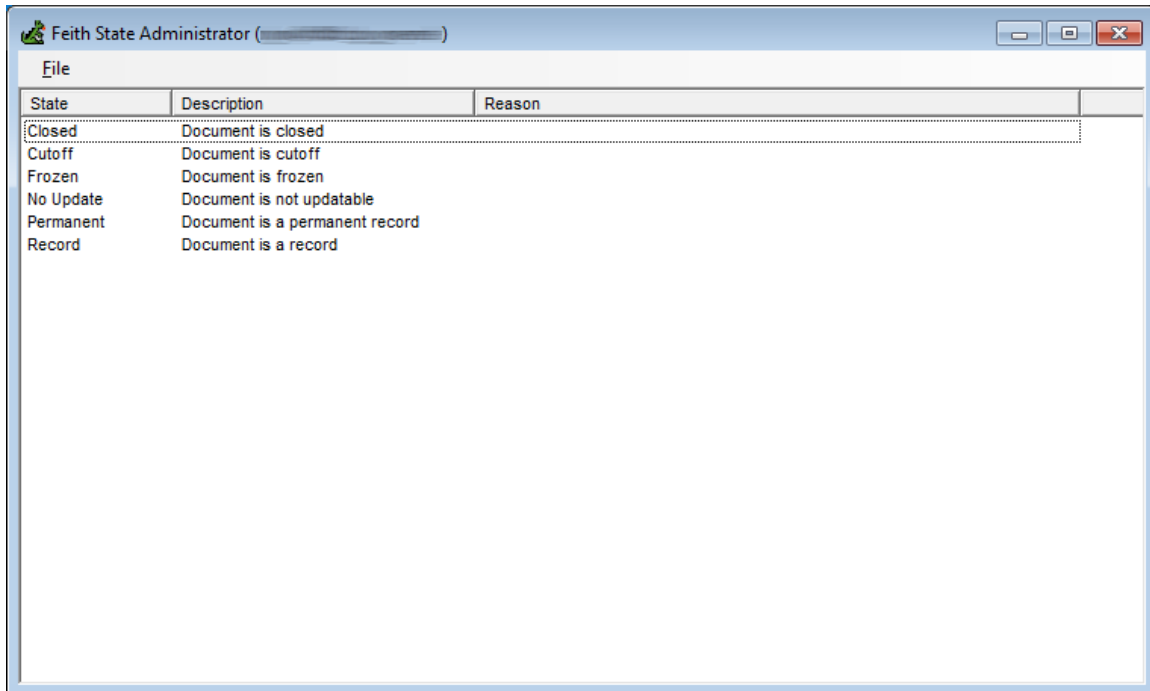
States and Reasons

States and Reasons

The following instructions apply only if your FDD system is licensed for RMA iQ.

Use **States and Reasons** to create new frozen states, to edit frozen state reasons, and to delete frozen states.

A **frozen record** cannot be deleted or destroyed, even if eligible for scheduled disposition, until the frozen state is removed from the record. Frozen states might be created to correspond to specific legal holds; in this implementation, the frozen state reason would likely reflect the name of the legal hold.

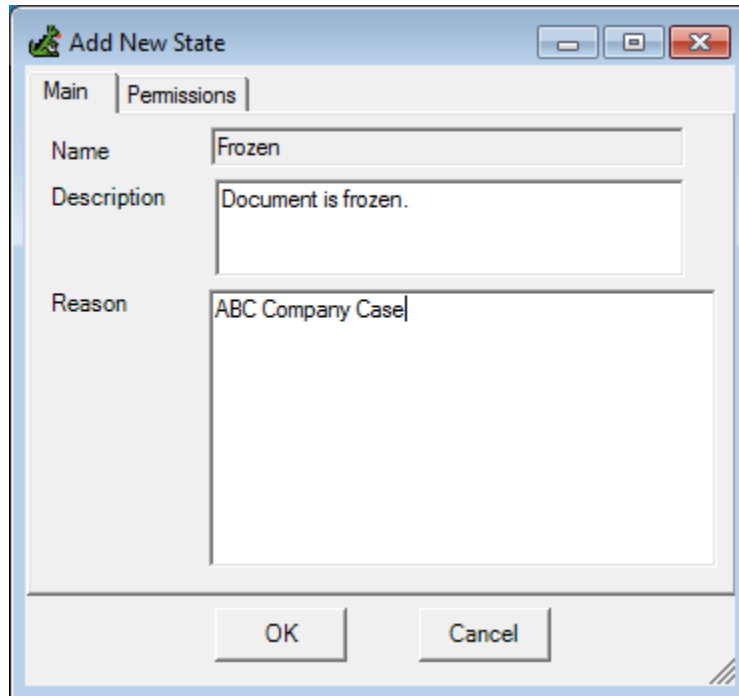


Add State

The following instructions apply only if your FDD system is licensed for RMA iQ.

To add a state:

1. Select **File>States and Reasons**. The **Feith State Administrator** opens.
2. Click **File>New**. The **Add New State** dialog opens.
3. Enter a **Description** and **Reason**.



The screenshot shows a Windows-style dialog box titled "Add New State". It has a standard title bar with minimize, maximize, and close buttons. Below the title bar are two tabs: "Main" and "Permissions". The "Main" tab is selected. Inside the dialog, there are three labeled text input fields: "Name" containing the text "Frozen", "Description" containing "Document is frozen.", and "Reason" containing "ABC Company Case". At the bottom of the dialog are two buttons: "OK" and "Cancel".

4. Click **OK**. The state is created and you are returned to the **Feith State Administrator**.

Manage States

The following instructions apply only if your FDD system is licensed for RMA iQ.

Modify State

To modify a state:

1. Select **File>States and Reasons**. The **Feith State Administrator** opens.
2. Click **File>Modify**. The **Add New State** dialog opens.
3. Make the desired changes to the **Description** or **Reason**. You can also view the state's **Permissions**.
4. Click **OK** to save your changes.

Delete State

To delete a state:

1. Select **File>States and Reasons**. The **Feith State Administrator** opens.
2. Click **File>Delete**. You are prompted to confirm the deletion.
3. Click **Yes** to continue. The state is deleted.

Note: States can only be deleted if they are not assigned to any documents.

Export and Import States

The following instructions apply only if your FDD system is licensed for RMA iQ.

Export State

To export a state:

1. Select **File>States and Reasons**. The **Feith State Administrator** opens.
2. Select a state and click **File>Export**. The **File Save** dialog opens.

You can select multiple states using **SHIFT+click** or **CTRL+click**.

3. Browse to select a destination path and file name for the state export file, then click **Save**. The state is exported to a .csv file.

Import State

To import a state:

1. Select **File>States and Reasons**. The **Feith State Administrator** opens.
2. Click **File>Import**. The **File Open** dialog opens.
3. Browse to select the state file and click **Open**. The state is imported and the **Import Complete** dialog displays the number of imported states that required updating.
4. Click **OK**. You are returned to the **Feith State Administrator**. The imported state is included in the state list.

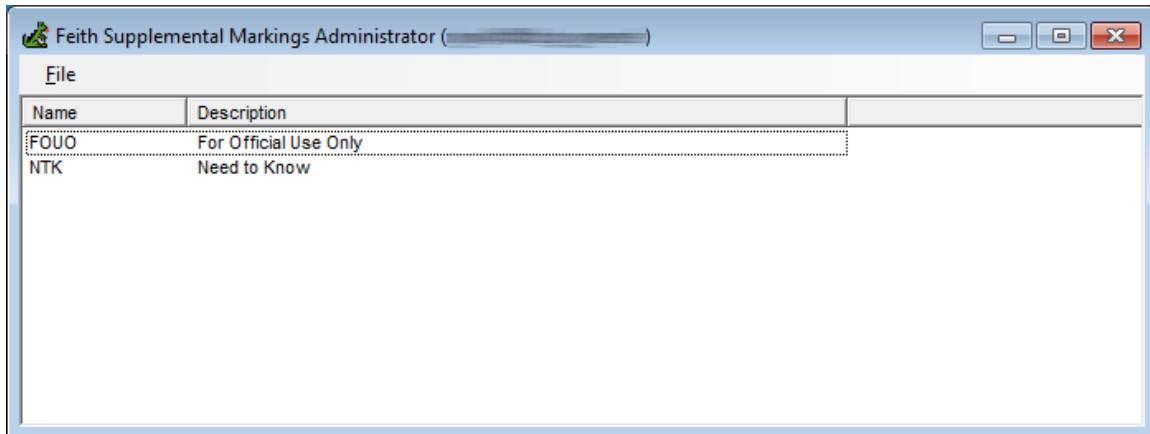
Supplemental Markings

Supplemental Markings

The following instructions apply only if your FDD system is licensed for RMA iQ.

Use **Supplemental Markings** to create and maintain supplemental markings.

Supplemental markings are applied in addition to a record's classification to further restrict access to the record. To access a record that has supplemental markings, a user must be assigned all markings applied to the record. Supplemental markings are assigned to users in the **Users** module under the [Clearances](#) tab.

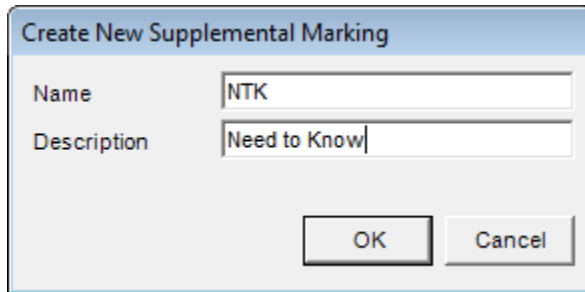


Add Supplemental Marking

The following instructions apply only if your FDD system is licensed for RMA iQ.

To add a supplemental marking:

1. Select **File>Supplemental Markings**. The **Feith Supplemental Markings Administrator** opens.
2. Click **File>New**. The **Create New Supplemental Marking** dialog opens.
3. Enter a **Name** and **Description**.



4. Click **OK**. The supplemental marking is created and you are returned to the **Feith Supplemental Markings Administrator**.

Manage Supplemental Markings

The following instructions apply only if your FDD system is licensed for RMA iQ.

Modify Supplemental Marking

To modify a supplemental marking:

1. Select **File>Supplemental Markings**. The **Feith Supplemental Markings Administrator** opens.
2. Click **File>Modify**. The **Modify Supplemental Marking** dialog opens.
3. Make the desired changes.
4. Click **OK**. The supplemental marking is modified.

Delete Supplemental Marking

To delete a supplemental marking:

1. Select **File>Supplemental Markings**. The **Feith Supplemental Markings Administrator** opens.
2. Select a supplemental marking and click **File>Delete**. You are prompted to confirm the deletion.
3. Click **Yes** to continue. The supplemental marking is deleted.

Note: A supplemental marking can only be deleted if it is not assigned to any documents.

Export and Import Supplemental Markings

The following instructions apply only if your FDD system is licensed for RMA iQ.

Export Supplemental Marking

To export a supplemental marking:

1. Select **File>Supplemental Markings**. The **Feith Supplemental Markings Administrator** opens.
2. Select a supplemental marking and click **File>Export**. The **File Save** dialog opens.

You can select multiple supplemental markings using **SHIFT+click** or **CTRL+click**.

3. Browse to select a destination path and file name for the supplemental marking export file, then click **Save**. The supplemental marking is exported to a .csv file.

Import Supplemental Marking

To import a supplemental marking:

1. Select **File>Supplemental Markings**. The **Feith Supplemental Markings Administrator** opens.
2. Click **File>Import**. The **File Open** dialog opens.
3. Browse to select the supplemental marking file and click **Open**. The supplemental marking is imported and the **Import Complete** dialog displays the number of imported supplemental markings that required updating.
4. Click **OK**. You are returned to the **Feith Supplemental Markings Administrator**. The imported supplemental marking is included in the supplemental marking list.

Change Marking Assignments

Take the documents assigned to a marking and assign another marking to those documents. [Copy](#), [move](#), or [remove](#) marking assignments on documents. You may need to do this if a specific marking is being phased out and needs to be replaced with another marking.

Copy Assignments

Take the documents that are assigned to a marking and also assign them another marking, while keeping the existing marking assignments.

To copy assignments:

1. In the **Supplemental Markings Administrator**, select the desired marking that is assigned to documents.
2. Select **File>Copy Assignments**. The **Copy Supplemental Markings Assignment** dialog opens.
3. Select the marking(s) that you want to assign to the documents.
4. Click **OK**. All the documents that were assigned the original marking now also have the additional, selected marking(s).

Move Assignments

Take the documents that are assigned to a marking and replace it with another marking.

To move assignments:

1. In the **Supplemental Markings Administrator**, select the desired marking that is assigned to documents.
2. Select **File>Move Assignments**. The **Move Supplemental Markings Assignment** dialog opens.
3. Select the marking(s) that you want to assign to the documents.
4. Click **OK**. All the documents that were assigned the original marking are now assigned the selected marking(s). The original marking was removed from the documents.

Remove Assignments

Remove a marking from the documents it's assigned to.

To remove assignments:

1. In the **Supplemental Markings Administrator**, select the desired marking that is assigned to documents.
2. Select **File>Remove Assignments**. You are prompted to confirm the removal.
3. Click **Yes** to continue. The marking is removed from the documents where it had been assigned.

System Preferences

System Preferences

In **System Preferences** set the fiscal year start day and enable RMA features.

Note: Only a super administrator can set system preferences.

To set the system preferences:

1. In the **Feith Control Panel**, select the **System Preferences** module. The **Feith System Preferences** opens.
2. Change system preferences as needed:
 - **Fiscal Year Start Day:** Used to set the start day of the fiscal year for the FDD system.
 - **Site ID:** A system-wide ID used for generating unique IDs for database objects (e.g. when the CXE transfers records).
 - **Optional Features:** Enable or disable features in the FDD system by checking them on and off. These settings are typically used for RMA.
 - **Minimum Workflow Comment Length:** The minimum number of characters a person must enter for the comment when they publish a workflow. The comments are very important to understanding how and when the workflow design changed and may be referenced in future when troubleshooting. If you do not want to require a comment on publish, set the length to **0**.

Feith System Preferences (gwyn@...)

Fiscal Year Start Day: Apr 01

Site ID: abcco132

Optional Features:

- Category: ☐
- Classification: ☐
- Country: ☒
- State: ☐
- Supplemental Markings: ☐

Minimum Workflow Comment Length: 1

Apply OK Cancel

4. Click **OK**. Changes to the system preferences are saved.

User Access Restrictions

User Access Restrictions

The following instructions apply only if your FDD system is licensed for RMA iQ.

User access restriction rules control document access based on user properties, typically through the comparison of user properties to RMA document properties.

An example implementation might compare a user property field called "Organization" to an RMA document property field of the same name. The user's "Organization" value would have to match the "Organization" assigned to a document in order for the user to access the document.

Note on Implementing User Access Restrictions

The topics in this section provide instructions for [adding](#), [modifying](#), and [deleting](#) user access restriction rules in Feith Control Panel. To fully implement user access restrictions in an FDD system, the following steps are required:

- Add fields to the **Document Properties** and **Group Properties** auxiliary file cabinets. To add fields to the **Document Properties** or **Group Properties** file cabinet, follow the standard instructions for [adding fields](#) to a file cabinet.
- Assign **Group Properties** field values to users on the **Other Properties** tab of the user properties dialog. See [Set User Other Properties for Access Restrictions](#) for instructions.
- Add **User Access Restrictions Rules**. See [Add User Access Restriction with One Rule](#), [Add User Access Restriction with Two Rules Joined by AND](#), or [Add User Access Restriction with Two Rules Joined by OR](#) for instructions.
- Add the **Document Properties** fields to one or more **Document Property Templates** using **RMA iQ Workplace Admin**. See the RMA iQ Workplace documentation for more information.
- Assign document properties to FDD documents using **RMA iQ Workplace**. See the RMA iQ Workplace documentation for more information.

Add User Access Restriction Rule

Add User Access Restriction with One Rule

The following instructions apply only if your FDD system is licensed for RMA iQ.

A user access restriction with one rule compares a single **Document Property** field to a single **User Property** field. When the user's properties match the document's properties, the user has access to the document.

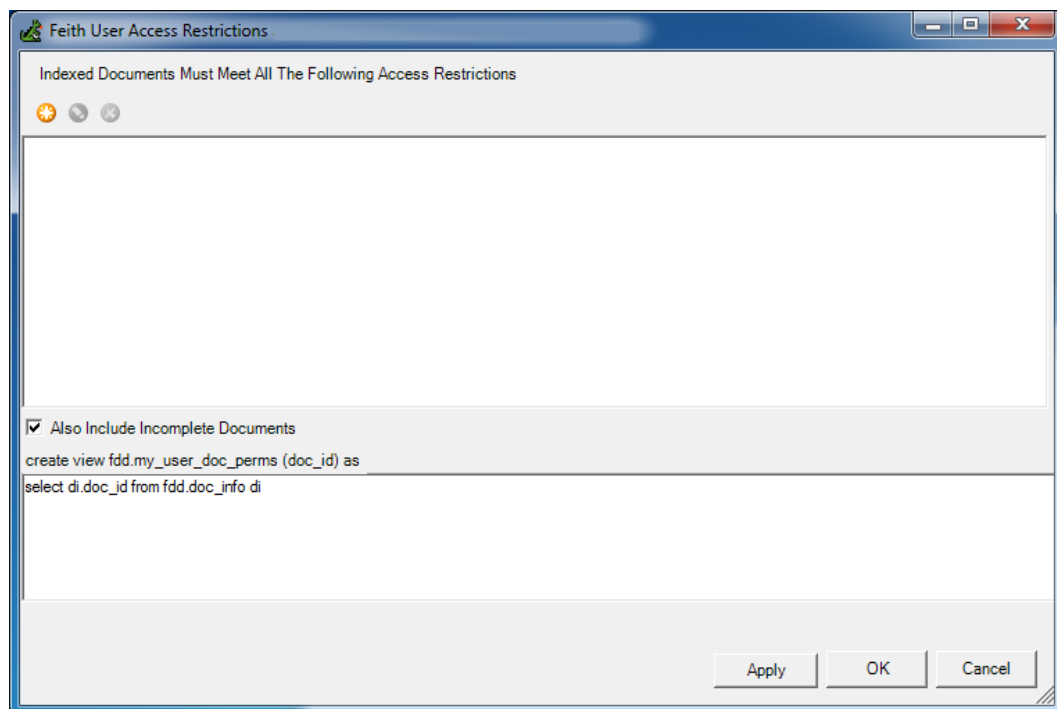
In the example shown below, the access restriction rule is:


- Document Property *Originating Organization* = User Property *Organization*

In this scenario, to access a document, the user must be assigned the organization value associated with the document.

To add a user access restriction with a single rule:

1. Select **File>User Access Restrictions** to open the **User Access Restrictions** dialog.



2. Click the **Create** icon  to open the **Add Access Restriction** dialog so you can add a new rule.
3. Enter a **Description** for the rule.
4. Select the **Leaf** option (this is the default).
5. Construct the rule by selecting a **Document Property**, an **Operator**, and a **User Property**. For example, a rule could be defined as **Document Property Originating Organization = User Property Organization**.

The fields shown in the **Document Properties** list are the fields from the **Document Properties** auxiliary file cabinet. Likewise, the fields shown in the **User Properties** list are the fields from the **Group Properties** auxiliary file cabinet. To add fields to the **Document Properties** or **Group Properties** file cabinet, follow the standard instructions for [adding fields](#) to a file cabinet.

Tip: You can use the **Clone Field** option on the **Add Access Restriction** dialog to easily copy a field from the **Document Properties** file cabinet to the **Group Properties** file cabinet, or vice versa.

By default, the **Document Properties** list is shown on the left and the **User Properties** list is shown on the right. The lists can be reversed if needed; to do so, change the selection in the drop-down box. Also, the right-hand side drop-down box contains a **Constant** option; this allows a **Document Properties** or **User Properties** field selected on the left-hand side to be compared to a constant value.

6. Choose whether to include documents with nulls values in the **Document Properties** or **User Properties** field selected on the left-hand side. To include these documents, check the **Include Null** option (this is the default). To exclude these documents, uncheck the **Include Null** option.

Example: Access restriction rule where **Document Property *Originating Organization* = User Property *Organization***.

Add Access Restriction

Description: Originating Organization = Organization

☐ Parent ☒ Leaf

Document Properties: [Originating Organization]

User Properties: [Organization]

Operator: =

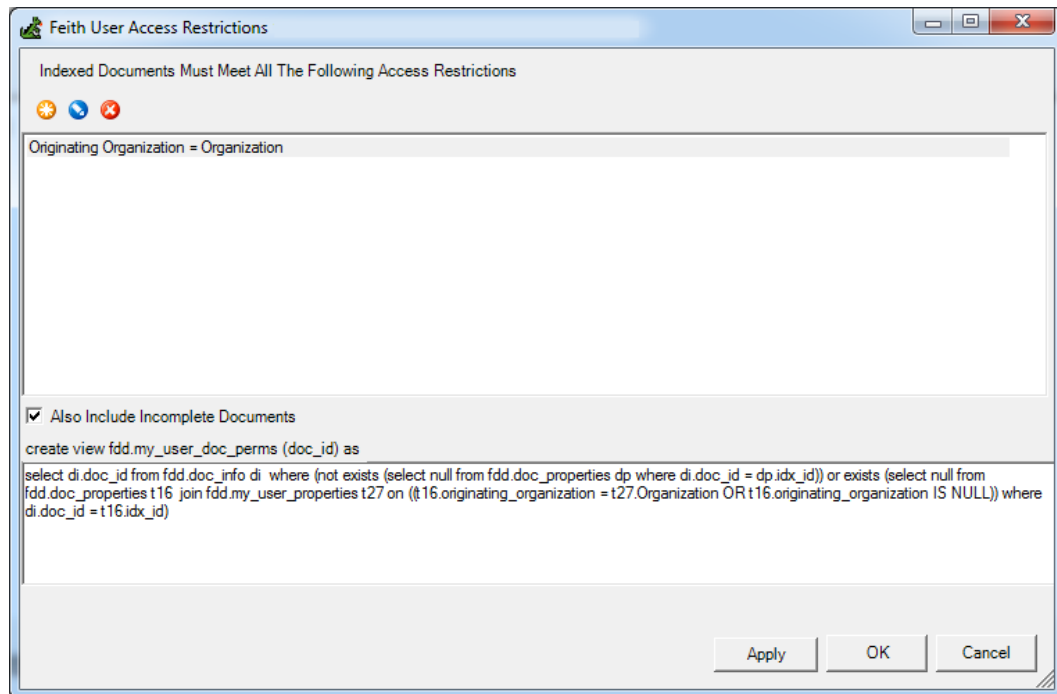
☒ Include Null

Clone Field >>

t16.originating_organization = t27.Organization OR t16.originating_organization IS NULL

OK Cancel

7. Click **OK**. The new rule is created and you are returned to the **User Access Restrictions** dialog.



8. Choose whether to include documents that do not have any document properties set. To include these documents, check the **Also Include Incomplete Documents** option (this is the default setting). To exclude these documents - for example, if documents should not be accessible by any users until document properties have been assigned - uncheck the **Also Include Incomplete Documents** option.

Access restriction rules apply only to those documents with document property field values. When the **Also Include Incomplete Documents** option is checked, "incomplete documents" - i.e., documents that do not have any document properties set - are accessible by the end user, in addition to those documents with document property values that match the user's other properties settings.

Add User Access Restriction with Two Rules Joined by AND

The following instructions apply only if your FDD system is licensed for RMA iQ.

If a user access restriction consists of two or more rules joined by **AND**, then **ALL** of the rules must be met in order for a user to access a document.

In the example shown below, the two rules joined by AND are:

- Document Property *Department* = User Property *Department*

AND

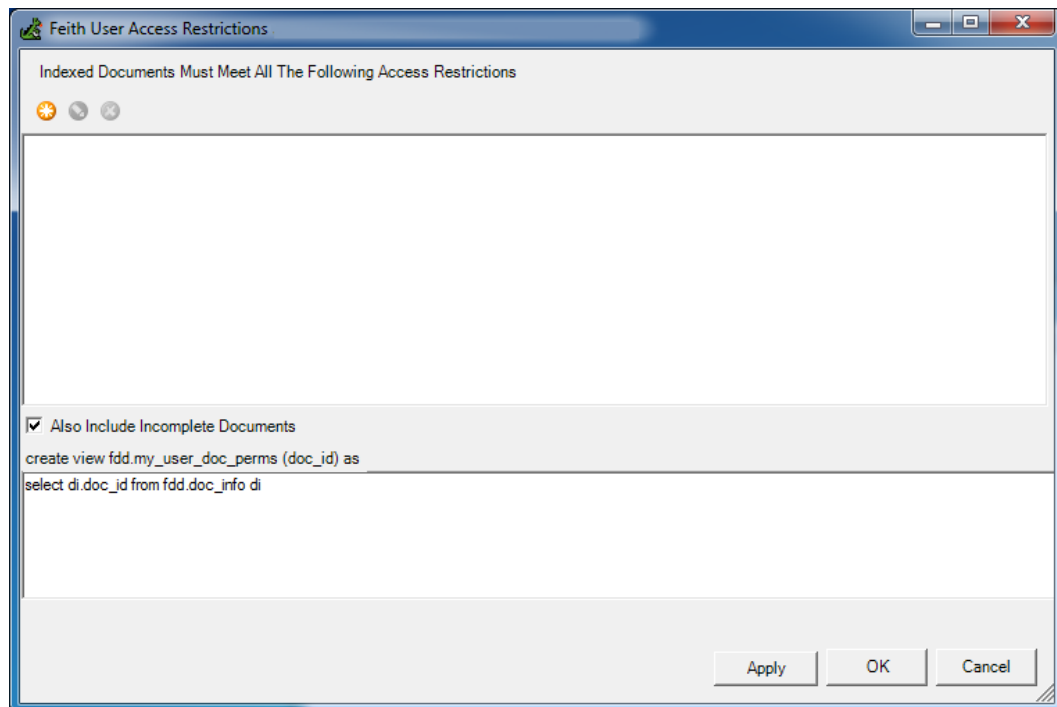
- Document Property *Project Name* Is Included In User Property *Assigned Projects*.


In this scenario, to access a document, the user must be assigned both the department value and the project value associated with the document.

Note: Multiple rules listed on the **User Access Restrictions** dialog will be joined by AND. To add rules joined by OR, you need to create a parent rule with two or more leaf rules. See [Add User Access Restriction with Two Rules Joined by OR](#) for more information.

To add a user access restriction with two rules joined by AND:

1. Select **File>User Access Restrictions** to open the **User Access Restrictions** dialog.



2. Click the **Create** icon  to open the **Add Access Restriction** dialog.
3. Add the first rule:
 - a. Enter a **Description** for the rule.
 - b. Construct the rule by selecting a **Document Property**, an **Operator**, and a **User Property**. For example, a rule could be defined as **Document Property Originating Organization = User Property Organization**.

The fields shown in the **Document Properties** list are the fields from the **Document**

Properties auxiliary file cabinet. Likewise, the fields shown in the **User Properties** list are the fields from the **Group Properties** auxiliary file cabinet. To add fields to the **Document Properties** or **Group Properties** file cabinet, follow the standard instructions for [adding fields](#) to a file cabinet.

Tip: You can use the **Clone Field** option on the **Add Access Restriction** dialog to easily copy a field from the **Document Properties** file cabinet to the **Group Properties** file cabinet, or vice versa.

By default, the **Document Properties** list is shown on the left and the **User Properties** list is shown on the right. The lists can be reversed if needed; to do so, change the selection in the drop-down box. Also, the right-hand side drop-down box contains a **Constant** option; this allows a **Document Properties** or **User Properties** field selected on the left-hand side to be compared to a constant value.

- c. Choose whether to include documents with nulls values in the **Document Properties** or **User Properties** field selected on the left-hand side. To include these documents, check the **Include Null** option (this is the default). To exclude these documents, uncheck the **Include Null** option.

Example: Access restriction rule where **Document Property Department = User Property Department**

Add Access Restriction

Description: Department = Department

☐ Parent ☒ Leaf

Document Properties: [Dropdown]

User Properties: [Dropdown]

Name	Type
Downgrade Instruct...	String
Reviewed On	Date
Reviewed By	String
Downgraded On	Date
Downgraded By	String
Declassified On	Date
Declassified By	String
Upgraded On	Date
Reason(s) for Upgr...	List of Strings
Upgraded By	String
Department	String

Operator: =


☒ Include Null

Clone Field >>

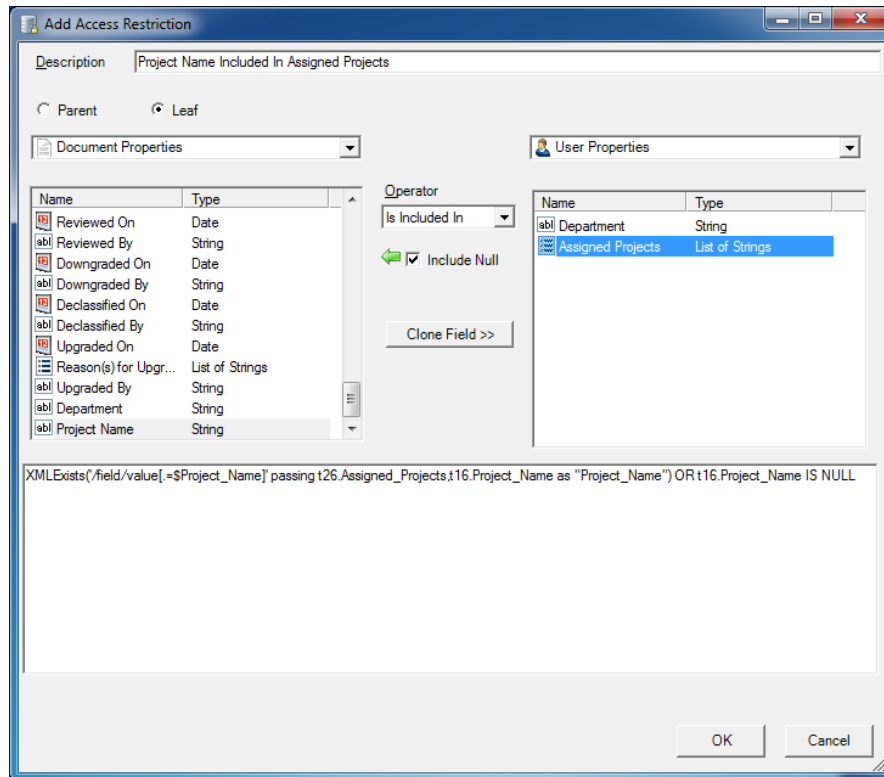
Name	Type
Department	String
Assigned Projects	List of Strings

t16.Department = t26.Department OR t16.Department IS NULL

OK Cancel

4. Click the **Create** icon  to open the **Add Access Restriction** dialog again.
5. Add the second rule, following the same instructions used to add the first rule.

Example: Access restriction rule where **Document Property Project Name Is Included In User Property Assigned Projects**.



Add Access Restriction

Description: Project Name Included In Assigned Projects

☐ Parent ☒ Leaf

Document Properties: [v]
User Properties: [v]

Name	Type
Reviewed On	Date
Reviewed By	String
Downgraded On	Date
Downgraded By	String
Declassified On	Date
Declassified By	String
Upgraded On	Date
Reason(s) for Upgr...	List of Strings
Upgraded By	String
Department	String
Project Name	String

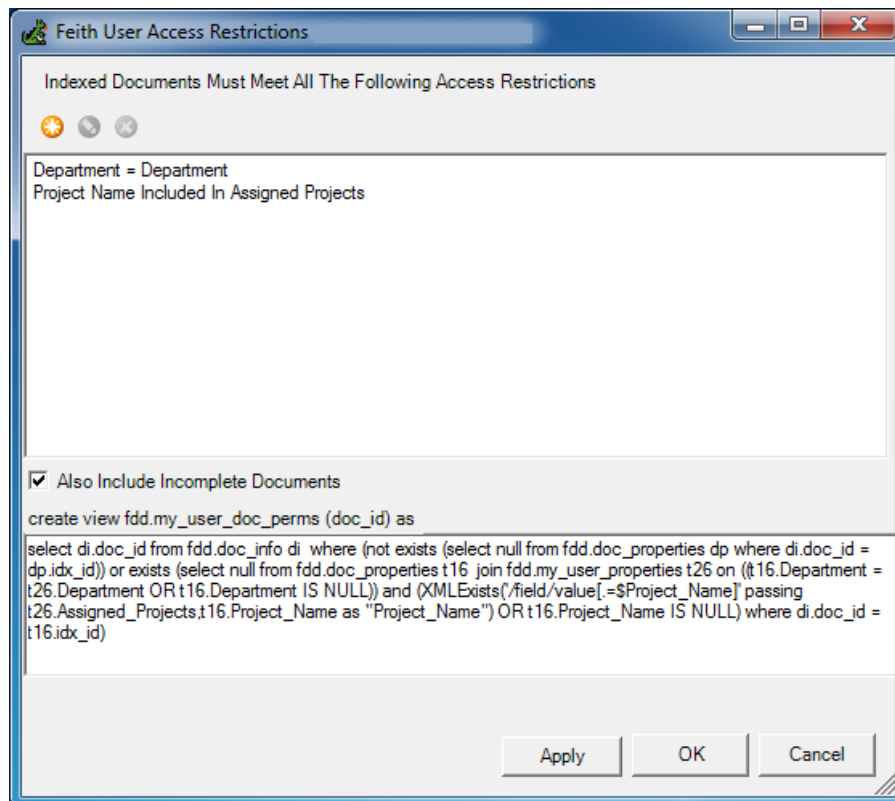
Operator: Is Included In [v]
☒ Include Null
 Clone Field >>

Name	Type
Department	String
Assigned Projects	List of Strings

XMLExists('/field/value[=\$Project_Name]' passing t26.Assigned_Projects.t16.Project_Name as "Project_Name") OR t16.Project_Name IS NULL

OK Cancel

6. Click **OK**. You are returned to the **User Access Restrictions** dialog, and both rules are displayed. Optionally add more rules, if needed.



Feith User Access Restrictions

Indexed Documents Must Meet All The Following Access Restrictions

☒ ☐ ☐

Department = Department
 Project Name Included In Assigned Projects

☒ Also Include Incomplete Documents

create view fdd.my_user_doc_perms (doc_id) as
 select di.doc_id from fdd.doc_info di where (not exists (select null from fdd.doc_properties dp where di.doc_id = dp.idx_id)) or exists (select null from fdd.doc_properties t16 join fdd.my_user_properties t26 on ((t16.Department = t26.Department OR t16.Department IS NULL)) and (XMLExists('/field/value[=\$Project_Name]' passing t26.Assigned_Projects.t16.Project_Name as "Project_Name") OR t16.Project_Name IS NULL) where di.doc_id = t16.idx_id)

Apply OK Cancel

7. Choose whether to include documents that do not have any document properties set. To include these documents, check the **Also Include Incomplete Documents** option (this is the default setting). To exclude these documents - for example, if documents should not be accessible by any users until document properties have been assigned - uncheck the **Also Include Incomplete Documents** option.

Access restriction rules apply only to those documents with document property field values. When the **Also Include Incomplete Documents** option is checked, "incomplete documents" - i.e., documents that do not have any document properties set - are accessible by the end user, in addition to those documents with document property values that match the user's other properties settings.

Add User Access Restriction with Two Rules Joined by OR

The following instructions apply only if your FDD system is licensed for RMA iQ.

If a user access restriction consists of two or more rules joined by **OR**, then **AT LEAST ONE** of the rules must be met in order for a user to access a document.

In the example shown below, the two rules joined by OR are:

- Document Property *Project Name* Is Included In User Property *Assigned Projects*

OR

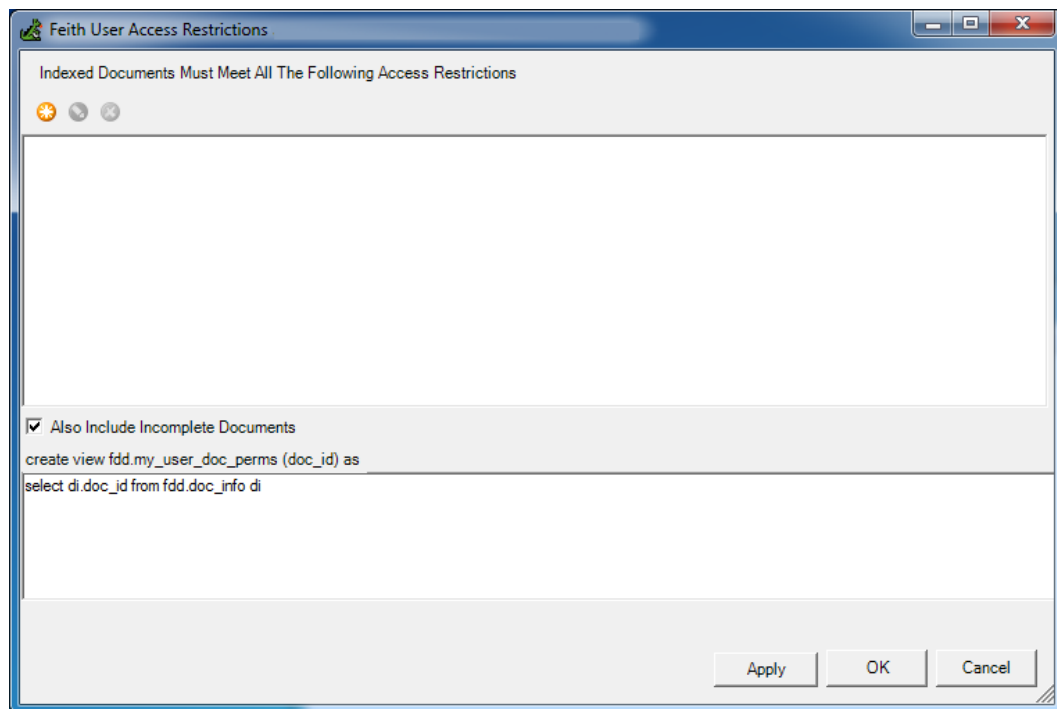
- User Property *Employee Position* = Constant *VP*


In this scenario, to access a document, the user must either be assigned to the project associated with the document or have an employee position of VP.

Note: When adding rules joined by OR, this creates a **parent rule** with two or more **leaf rules**, as shown below.

To add a user access restriction with two rules joined by OR:

1. Select **File>User Access Restrictions** to open the **User Access Restrictions** dialog.



2. Click the **Create** icon  to open the **Add Access Restriction** dialog.
3. Add the first rule:
 - a. Enter a **Description** for the rule.
 - b. Construct the rule by selecting a **Document Property**, an **Operator**, and a **User Property**. For example, a rule could be defined as **Document Property Originating Organization = User Property Organization**.

The fields shown in the **Document Properties** list are the fields from the **Document Properties** auxiliary file cabinet. Likewise, the fields shown in the **User Properties** list are the fields from the **Group Properties** auxiliary file cabinet. To add fields to the **Document**

Properties or **Group Properties** file cabinet, follow the standard instructions for [adding fields](#) to a file cabinet.

Tip: You can use the **Clone Field** option on the **Add Access Restriction** dialog to easily copy a field from the **Document Properties** file cabinet to the **Group Properties** file cabinet, or vice versa.

By default, the **Document Properties** list is shown on the left and the **User Properties** list is shown on the right. The lists can be reversed if needed; to do so, change the selection in the drop-down box. Also, the right-hand side drop-down box contains a **Constant** option; this allows a **Document Properties** or **User Properties** field selected on the left-hand side to be compared to a constant value.

- c. Choose whether to include documents with nulls values in the **Document Properties** or **User Properties** field selected on the left-hand side. To include these documents, check the **Include Null** option (this is the default). To exclude these documents, uncheck the **Include Null** option.

Example: Access restriction rule where **Document Property Project Name** Is Included In **User Property Assigned Projects**.

Add Access Restriction

Description: Project Name Included In Assigned Projects OR Employee = VP

☐ Parent ☒ Leaf

Document Properties: [Dropdown]

User Properties: [Dropdown]

Name	Type
Downgrade Instruct...	String
Reviewed On	Date
Reviewed By	String
Downgraded On	Date
Downgraded By	String
Declassified On	Date
Declassified By	String
Upgraded On	Date
Reason(s) for Upgr...	List of Strings
Upgraded By	String
Project Name	String

Operator: Is Included In

☒ Include Null

Clone Field >>

Name	Type
Employee Position	String
Assigned Projects	List of Strings

SQL Query: t27.Assigned_Projects.exist('/field/value[=sql:column('t16.Project_Name')]') = 1 OR t16.Project_Name IS NULL

OK Cancel

4. Change the **Parent** / **Leaf** selection from **Leaf** to **Parent**.

☒ Parent ☐ Leaf

5. Change the operator from **AND** to **OR**.

☒ AND ☐ OR

6. Click the **Create** icon to open a second **Add Access Restriction** dialog.

7. Add the second rule, following the same instructions used to add the first rule.

Example: Access restriction rule where **User Property *Employee Position* = Constant *VP***.

Add Access Restriction

Description: Employee = VP

Parent ☐ Leaf ☒

User Properties π Constant

Name	Type
Employee Position	String
Assigned Projects	List of Strings

Operator: = VP

☐ Include Null

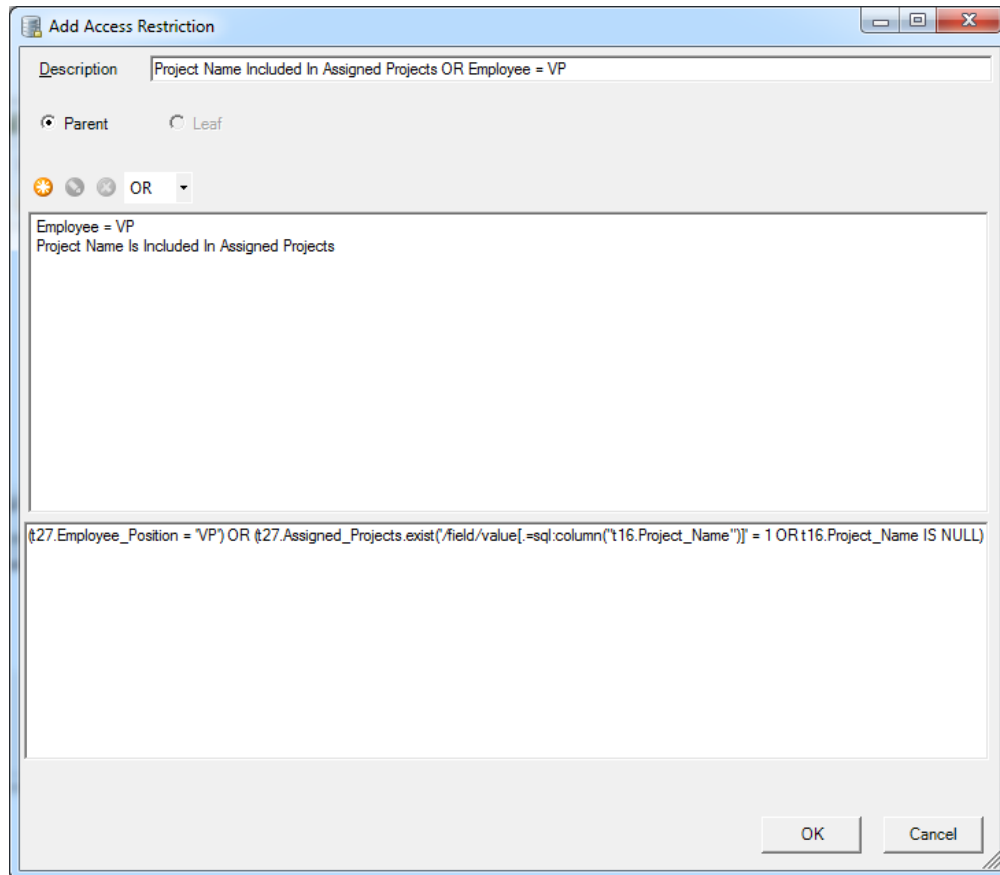
Clone Field >>

SQL: t27.Employee_Position = 'VP'

OK Cancel

8. Click **OK**. You are returned to the first **Add Access Restriction** dialog, and both rules are displayed. Optionally add more rules, if needed.

Note: The individual rules can be modified or deleted, if needed, on this dialog. To do so, select the rule, then click the **Modify**  or **Delete** icon .



Add Access Restriction

Description: Project Name Included In Assigned Projects OR Employee = VP

☒ Parent ☐ Leaf

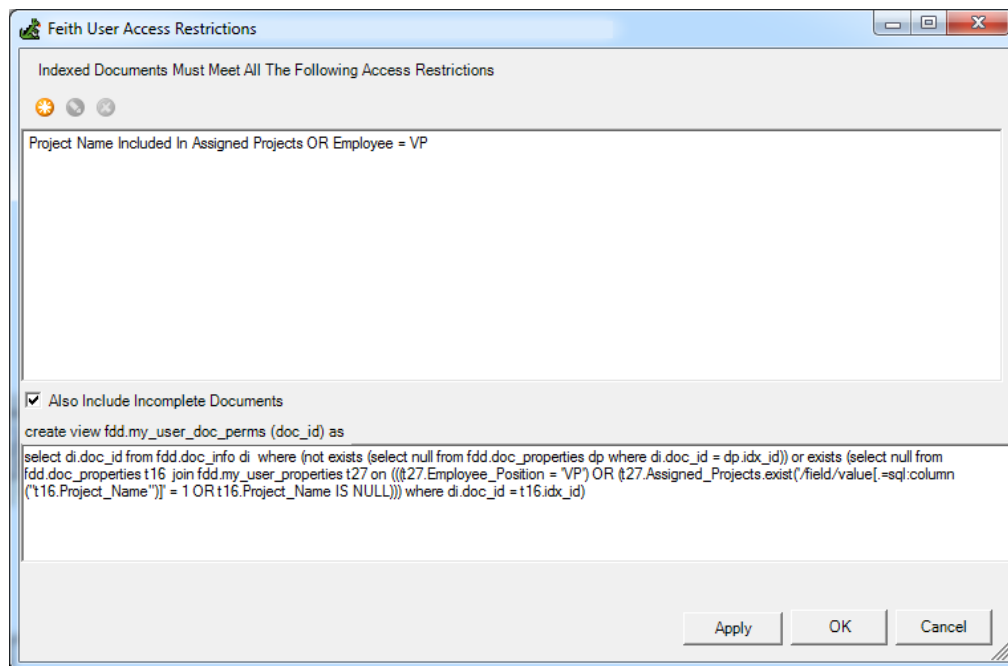
OR

Employee = VP
Project Name Is Included In Assigned Projects

`{27.Employee_Position = 'VP'} OR {27.Assigned_Projects.exist('/field/value[.=sql:column('t16.Project_Name')]') = 1 OR t16.Project_Name IS NULL}`

OK Cancel

9. Click **OK**. You are returned to the **User Access Restrictions** dialog. The parent rule is displayed as a single rule on this dialog.



Feith User Access Restrictions

Indexed Documents Must Meet All The Following Access Restrictions

Project Name Included In Assigned Projects OR Employee = VP

☒ Also Include Incomplete Documents

create view fdd.my_user_doc_perms (doc_id) as

`select di.doc_id from fdd.doc_info di where (not exists (select null from fdd.doc_properties dp where di.doc_id = dp.idx_id)) or exists (select null from fdd.doc_properties t16 join fdd.my_user_properties t27 on (({27.Employee_Position = 'VP'} OR {27.Assigned_Projects.exist('/field/value[.=sql:column('t16.Project_Name')]') = 1 OR t16.Project_Name IS NULL))) where di.doc_id = t16.idx_id)`

Apply OK Cancel


10. Choose whether to include documents that do not have any document properties set. To include these documents, check the **Also Include Incomplete Documents** option (this is the default setting). To exclude these documents - for example, if documents should not be accessible by any users until document properties have been assigned - uncheck the **Also Include Incomplete Documents** option.

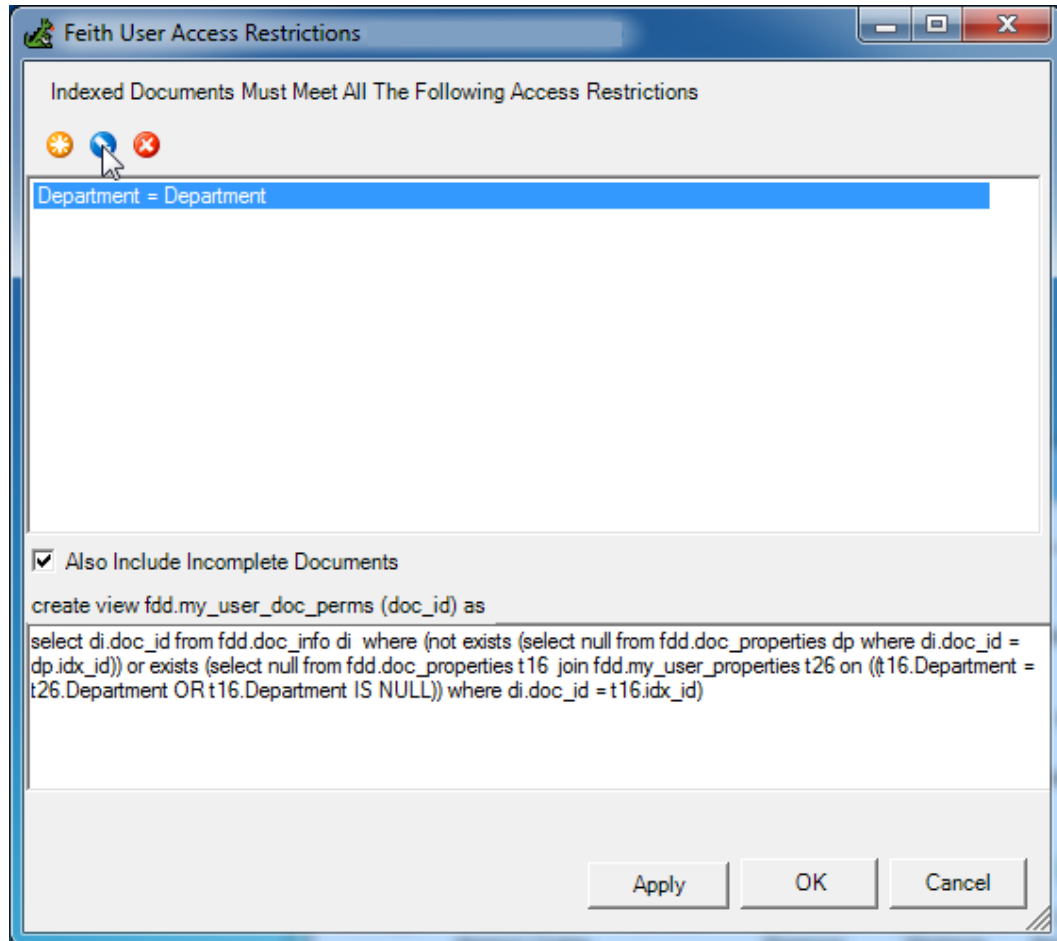
Access restriction rules apply only to those documents with document property field values. When the **Also Include Incomplete Documents** option is checked, "incomplete documents" - i.e., documents that do not have any document properties set - are accessible by the end user, in addition to those documents with document property values that match the user's other properties settings.

Modify User Access Restriction Rule

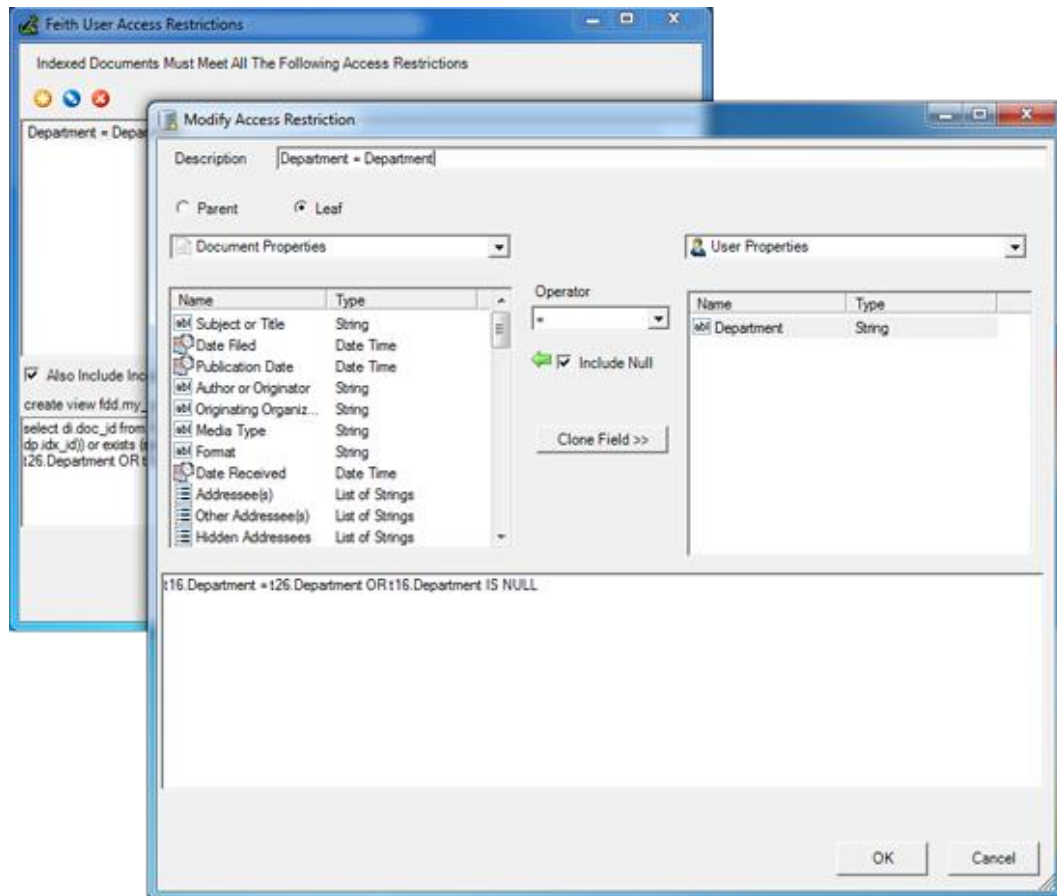
The following instructions apply only if your FDD system is licensed for RMA iQ.

To modify a user access restriction rule:

1. Select **File>User Access Restrictions** to open the **User Access Restrictions** dialog.
2. Select the rule you wish to modify, then click the **Modify** icon  to open the **Modify Access Restriction** dialog.



- On the **Modify Access Restriction** dialog, edit the rule properties as needed.




- Click **OK**. The changes are saved and you are returned to the **User Access Restrictions** dialog.

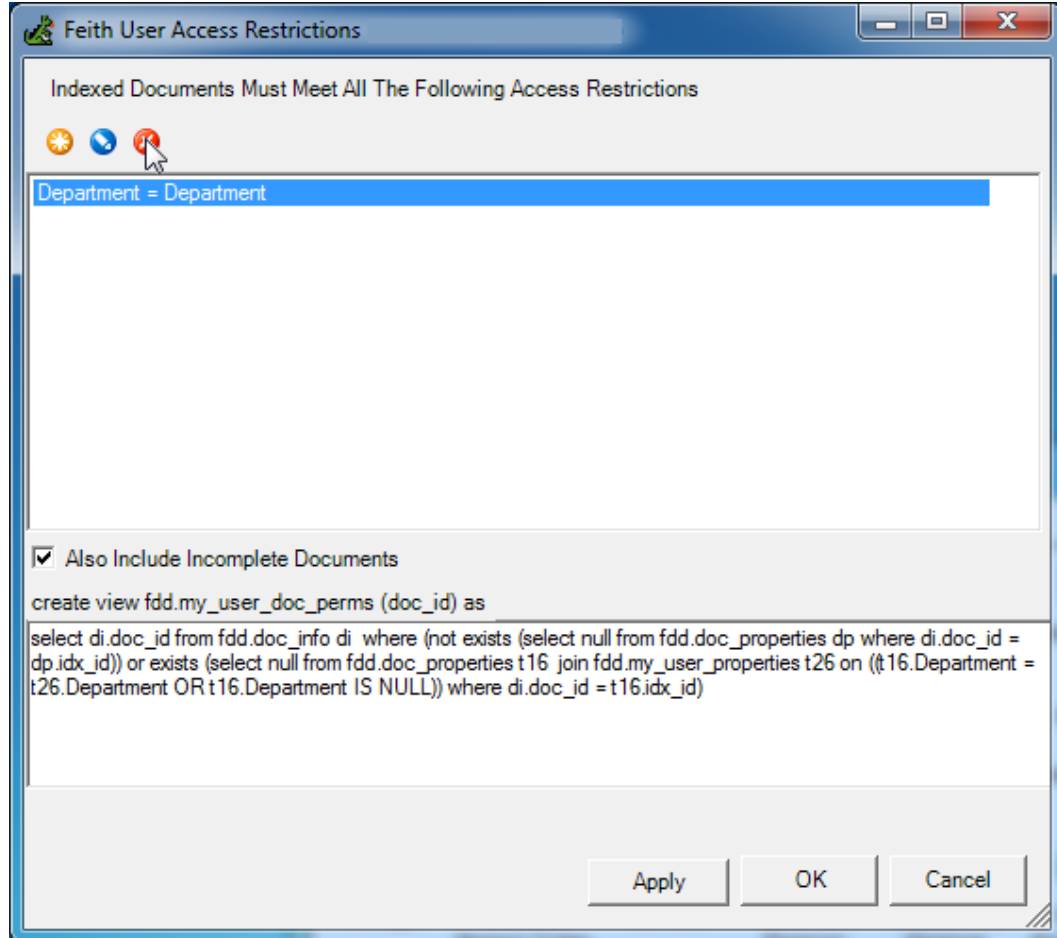
Note: If you have a **parent rule** with two or more **leaf rules**, the individual leaf rules can be modified on the [parent rule dialog](#).

Delete User Access Restriction Rule

The following instructions apply only if your FDD system is licensed for RMA iQ.

To delete a user access restriction rule:

1. Select **File>User Access Restrictions** to open the **User Access Restrictions** dialog.
2. Select the rule you wish to delete, then click the **Delete** icon . The rule is deleted.



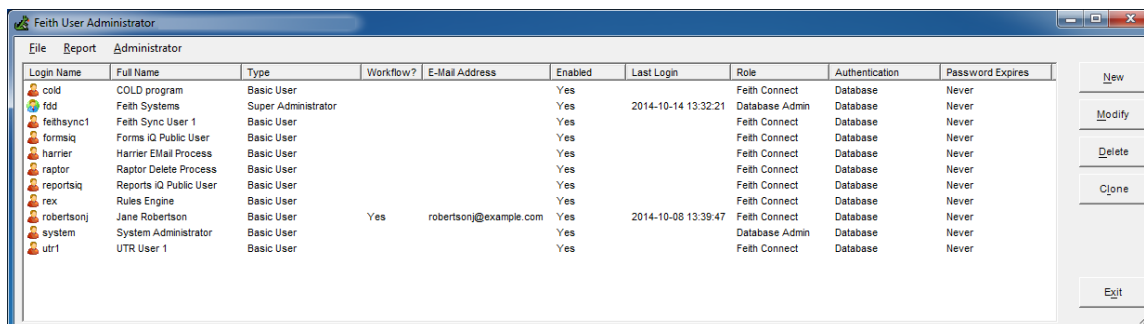
Note: If you have a **parent rule** with two or more **leaf rules**, the individual leaf rules can be deleted on the [parent rule dialog](#).

Users

Users

Create and maintain FDD users in the **Feith User Administrator**. Create users for your people to login to the FDD system. Add users to groups, set permissions, and more.

Tip: If you have a lot of users to manage, you may want to use some [search tools](#) available in the User Administrator.



To do a find within the user list, select **File>Find** or press **CTRL+F** to open the find dialog. Next, enter the text you would like to search in the text box labeled **Find What**. Find options include: **Find Whole Word**, **Match Case**, **Direction**, **Column** and **Find Next**.

If there are many users in your system and you do not want the full user list retrieved when the **Feith User Administrator** opens, select **File>Full User List on Start** to turn the option on or off. When this option is turned off, the **Feith User Administrator** will open up empty, at which point you can use **File>Retrieve User List** to bring up a search dialog in which you would enter search criteria to retrieve a portion of the user list (to retrieve the entire user list, you would enter no search criteria).

If you want to export the list to a CSV, right-click in the grid and select **Save to CSV**.

System Users

The following system users are created during the FDD installation. These users are created for use with FDD applications and cannot be deleted.

USER	DESCRIPTION
autocat	Auto Categorization Process
cold	COLD user
dataservices	Data Services Process
fdd	Feith Systems Administrative user
feithsync1	Feith Sync user
formsiq	Forms iQ user
harrier	Harrier user
raptor	Raptor user
reportsiq	Reports iQ user

rex	Rules Engine user
system	System Administrator
utr1	Universal Text Retrieval user

Add User

User Authentication Types

FDD users are added as either **database authenticated** users or **externally authenticated** users.

- **Database authenticated.** Unless your FDD system is configured for external authentication, users must be added as database authenticated users. When adding a database authenticated user, a password must be set for the user. The password must be entered every time the user logs in to FDD.
- **Externally authenticated.** Externally authenticated users can be added when your FDD system is configured for external authentication; for example, if FDD is integrated with Microsoft Active Directory.

SSO. Integrating with Active Directory using Kerberos authentication provides Single Sign-On (SSO) in addition to external authentication. With SSO, when a user logs into their computer they can login to FDD without typing in their FDD user name and password, because FDD takes the credentials from the operating system and verifies them against Active Directory directly. Note that SSO does *not* apply when running on an Oracle database that is configured to use RADIUS authentication.

For instructions on adding users, see [Add Database Authenticated User](#), [Add Externally Authenticated User on Oracle](#), or [Add Externally Authenticated User on MS SQL Server](#).

For instructions on importing multiple users into FDD, see [Import Users from File](#) and [Import Users from LDAP](#).

Add Database Authenticated User

To add a database authenticated user:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Click **New**. The **Create New User** screen opens.

The screenshot shows the 'Create New User' dialog box with the following fields and options:

- Properties** (selected tab) | Other Properties | Membership | Permissions | Clearances | Proxies | Audit Events
- ☒ **Database Authenticated** | ☐ Externally Authenticated
- Login Name**: [Text Field] **Find** button
- Full Name**: [Text Field]
- Email Address**: [Text Field]
- Database Role**: [Feith Connect] (dropdown)
- User Type**: [Standard] (dropdown)
- Super Administrator**: ☐
- Optional Description**: [Text Area]
- Password**: [Text Field]
- Confirm Password**: [Text Field]
- Password Expires**: ☒ Never | ☐ [05-Feb-2018] (dropdown)
- Connect Through Proxy Only**: ☐
- Use PKI**: ☐ [Text Field]
- OK** | **Cancel** buttons at the bottom.

3. On the **Properties** tab, select the **Database Authenticated** option.

4. Enter the following user properties. [See the figure below for example user property settings.](#)

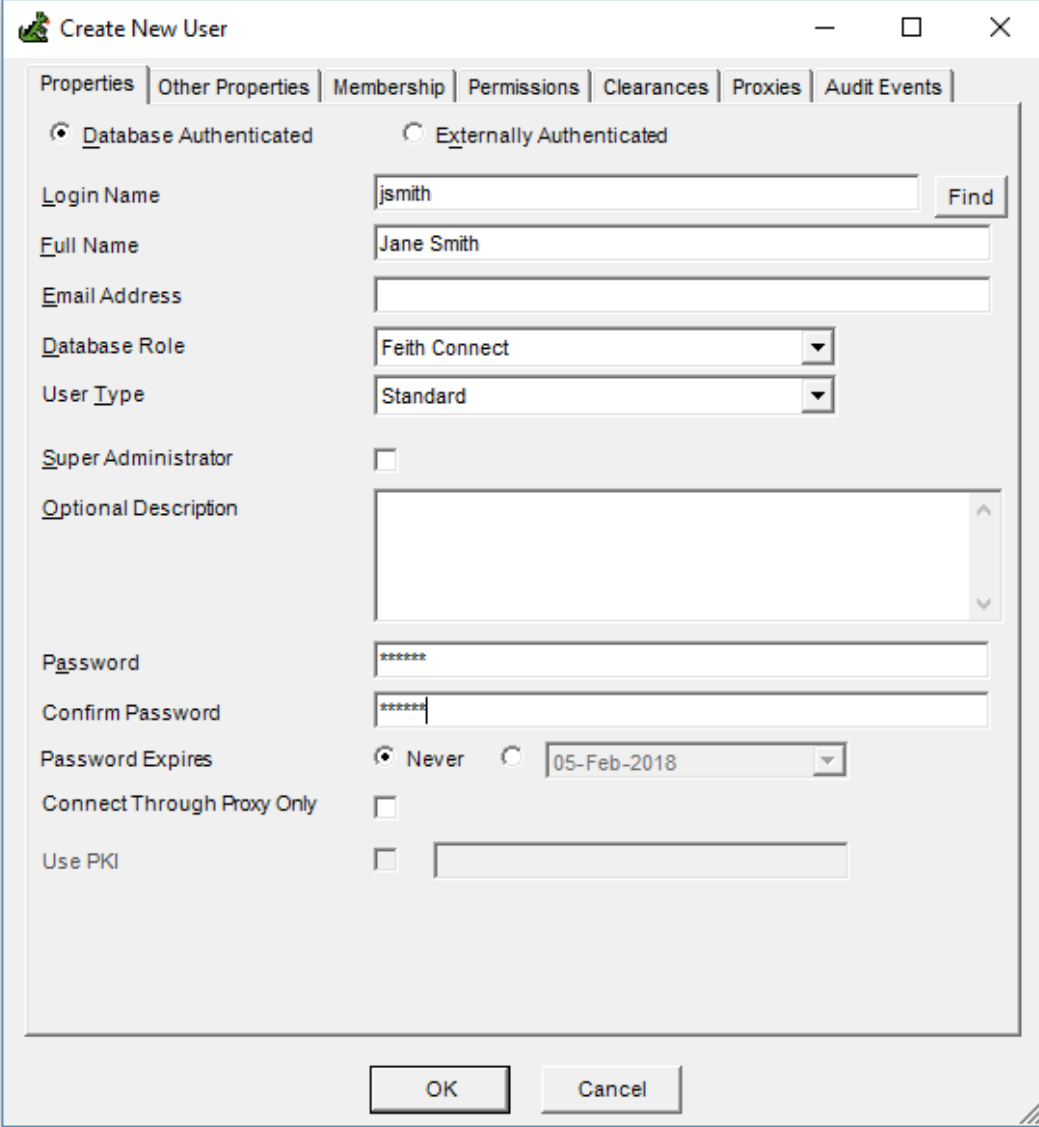
- **Login Name:** Enter the user's login name. The maximum number of characters accepted varies per database.
- **Full Name:** Enter the user's full name. A maximum of 64 characters is accepted.
- **Email Address:** Optionally enter the user's email address. A maximum of 64 characters is accepted.
- **Database Role:** Select the database role. The default setting is **Feith Connect**. The privileges of each database role differ between databases; see [Database Roles](#) and/or refer to your database vendor's documentation for more information.

Note: Only super administrators can set the **Feith Admin** and **Database Admin** database roles.

- **User Type:** Select the user type. Options are:
 - **Standard:** Standard user with no specific designation.
 - **Guest:** For unauthenticated users to access specific functions and objects within Feith Applications. This type of account is typically used by Feith Developer.
 - **Service:** Account for service application, such as REX, Harrier, and Raptor.
 - **Workflow:** A workflow user who has access to workflow features in the clients (e.g. FDD Client). Your system must be licensed for workflow and you must have available workflow user licenses (see [License Manager](#) for more information).
- **Super Administrator:** Check this option if you want to make this user a super administrator. See [Levels of Administrators](#) for more information on super administrators.

Note: This property can be set only by a super administrator.

- **Optional Description:** Optionally enter a user description. This description displays when viewing user properties in Feith Control Panel and on the user report generated from Feith Control Panel.
- **Password:** Enter the user's password. The maximum number of characters accepted varies per database.
- **Confirm Password:** Re-enter the password for verification.
- **Password Expires:** Choose when the user's password should expire. Options include:
 - **Never:** The user's password never expires.
 - **Date:** The user's password will expire on the selected date. See [Password Complexity and Expiration Rules](#) for more information on password expiration.
- **Connect Through Proxy Only:** Have this user only connect through a proxy. See [Set User Proxies](#) for more information.
 - If you want this proxy user to be authorized using PKI, check on **Use PKI** and enter their distinguished name.



The "Create New User" dialog box features a title bar with a standard icon, a minus button, a maximize button, and a close button. Below the title bar is a tabbed interface with the following tabs: Properties, Other Properties, Membership, Permissions, Clearances, Proxies, and Audit Events. The "Properties" tab is currently selected. At the top of the Properties tab, there are two radio buttons: "Database Authenticated" (which is selected) and "Externally Authenticated". Below these are several input fields and checkboxes. The "Login Name" field contains "jsmith" and has a "Find" button to its right. The "Full Name" field contains "Jane Smith". The "Email Address" field is empty. The "Database Role" field is a dropdown menu showing "Feith Connect". The "User Type" field is a dropdown menu showing "Standard". There is a checkbox for "Super Administrator" which is unchecked. The "Optional Description" field is a large text area, currently empty. Below this are two password fields, both containing "*****". The "Password Expires" field has two radio buttons: "Never" (selected) and a date "05-Feb-2018" (which is also selected). There is a checkbox for "Connect Through Proxy Only" which is unchecked. The "Use PKI" checkbox is also unchecked, followed by an empty text field. At the bottom of the dialog are "OK" and "Cancel" buttons.

Create New User

Properties | Other Properties | Membership | Permissions | Clearances | Proxies | Audit Events

☒ Database Authenticated ☐ Externally Authenticated

Login Name: jsmith Find

Full Name: Jane Smith

Email Address:

Database Role: Feith Connect

User Type: Standard

Super Administrator: ☐

Optional Description:

Password: *****

Confirm Password: *****

Password Expires: ☒ Never ☐ 05-Feb-2018

Connect Through Proxy Only: ☐

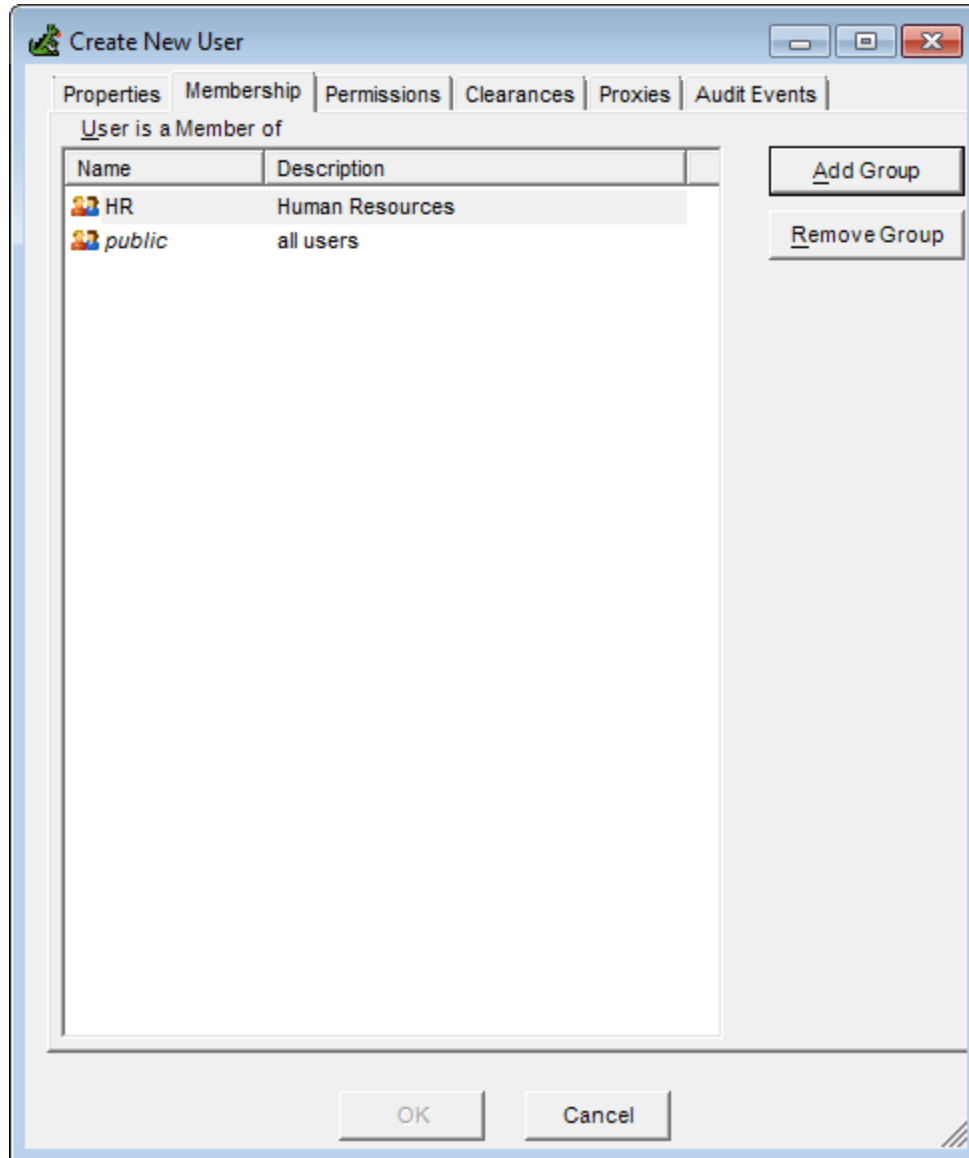
Use PKI: ☐

OK Cancel

5. Select the **Membership** tab and set the user's group membership.

All users belong to the **public** group. Users cannot be removed from the [public group](#).

Group membership can also be set when adding or modifying a group. See [Add Group](#) or [Modify Group](#) for instructions.



To add the user to a group:

- a. Click **Add Group**. The **Groups** dialog opens, listing all groups to which you have administrative access.
- b. Select a group in the list and click **OK**. The user is added to the group and the group name appears in the **User is a Member of** group list.

To remove the user from a group:

- Select a group in the **User is a Member of** group list and click **Remove Group**. The user is removed from the group.

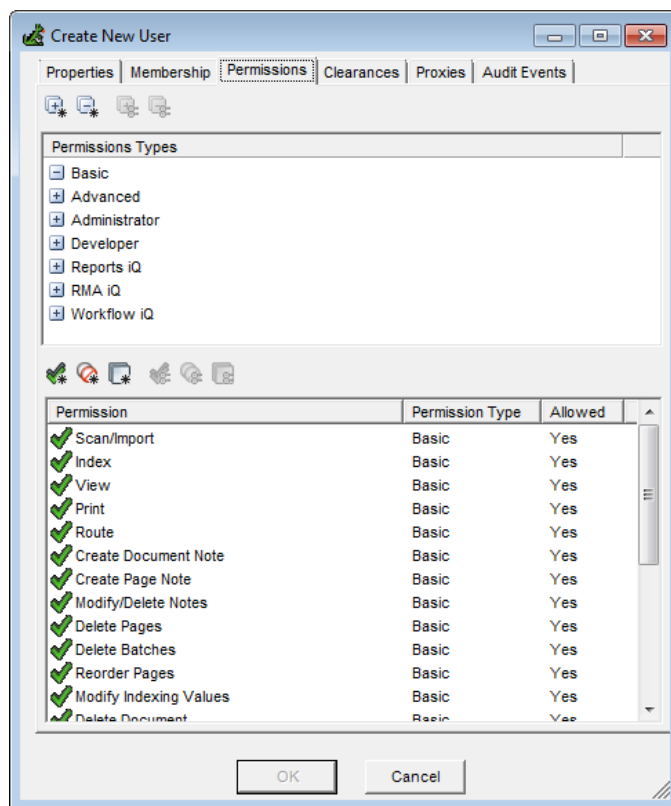
6. Select the **Permissions** tab and set the user's task permissions, which control what actions a user is allowed to take in various Feith applications.

Permissions are broken down into types and you can choose which permission types are listed by expanding or collapsing the **Permission Types** in the top list.

When you have found the desired permissions, you can double-click an individual permission to either grant, deny, or clear it. You can also use the toolbar buttons to change all listed permissions or multiple, selected permissions (select multiple using **CTRL+click** or **SHIFT+click**).

Tip: You may want to consider setting task permissions at the [group level](#) instead. If you manage permissions this way, you just need to change the group's task permissions in one place and then all the members' task permissions have been updated - no need to go into every user and change task permissions there.

Note: Only super administrators can set permissions at the user level.



7. You may see additional tabs for the user, depending on your FDD system licensing and configuration. Refer to the following topics for instructions on setting the additional user properties:
 - [Set User Audit Events for FDD Auditing](#)
 - [Set User Clearance for RMA iQ](#)
 - [Set User Other Properties for Access Restrictions](#)
 - [Set User Proxies](#)
8. Click **OK**. The new user is added.

Add Externally Authenticated User on Oracle

The following instructions apply only if your FDD system is configured for external authentication.

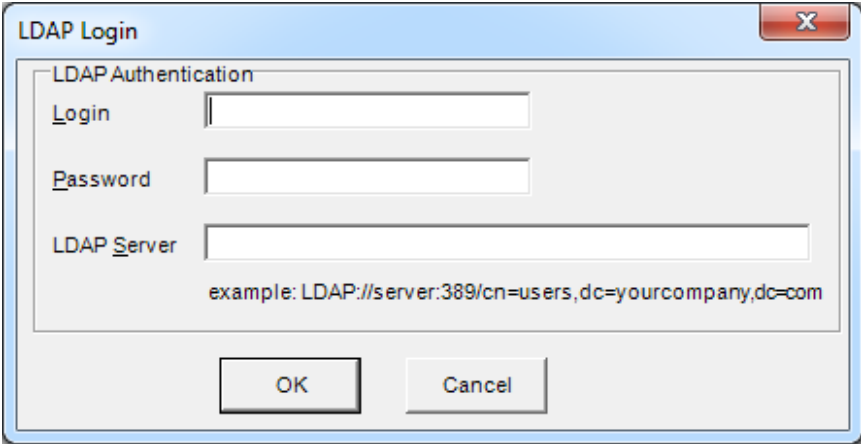
If your FDD system is not configured for external authentication, users must be added as [database authenticated users](#).

To add an externally authenticated user on Oracle:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Click **New**. The **Create New User** screen opens.
3. On the **Properties** tab, select the **Externally Authenticated** option.
4. If you have an LDAP server that contains a list of users that corresponds to your external authentication system (for example, if you are using Microsoft Active Directory), click the **Find** button to the right of **External Name** to search for the user in your LDAP server. This option populates the **External Name** and **Login Name** fields with the appropriate values from the user's LDAP account.
 - a. Click the **Find** button next to the **External Name** field.
 - b. If prompted, login to your LDAP server.

If you are automatically logged into an LDAP server and want to change your connection, a **Reconnect to LDAP** option is available under the **File** menu on the **LDAP User Search** screen.

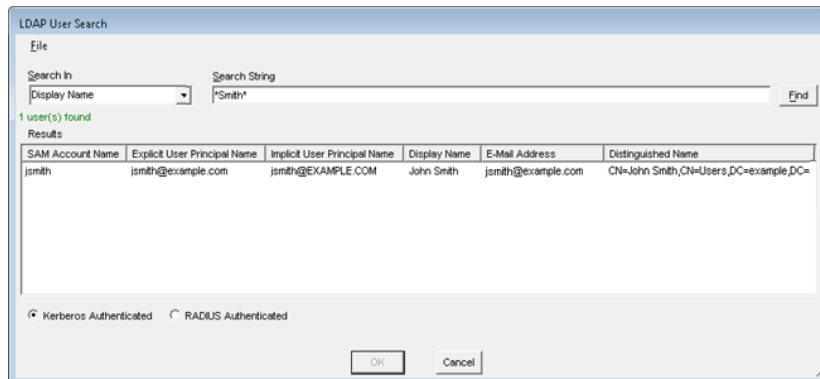
See [Appendix C: LDAP Server Format](#) for more information on how to construct the server address.



The image shows a dialog box titled "LDAP Login". It contains three text input fields: "Login", "Password", and "LDAP Server". Below the "LDAP Server" field, there is an example text string: "example: LDAP://server:389/cn=users,dc=yourcompany,dc=com". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

- c. After logging in, enter the search criteria on the **LDAP User Search** screen and click **Find**.

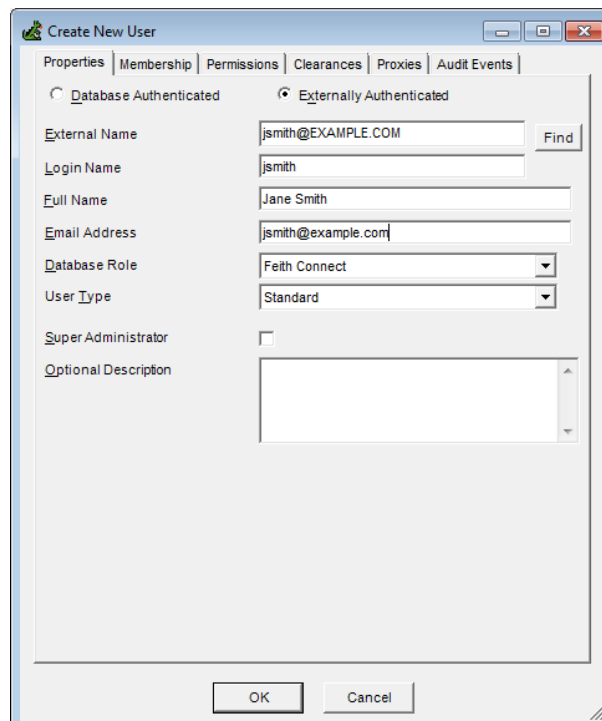
Tip: The asterisk character (*) can be used as a wildcard to replace any number of characters in the search string.



- d. Select a user name from the search results. The information on this screen, such as SAM Account Name, are Active Directory terms for user attributes. Refer to Microsoft Active Directory documentation for more information on user attributes in Active Directory.
- e. Select whether your Oracle database is configured for **Kerberos Authentication** or **RADIUS Authentication**. The default FDD **External Name** value will differ slightly depending on the type of authentication selected.
- f. Click **OK** to add the selected user to FDD. The **External Name**, **Login Name**, **Full Name**, and **Email Address** fields will be populated with values from the user's LDAP account properties.

For example, if you are using Microsoft Active Directory the user properties are copied as follows:

- **External Name** = Implicit UPN
- **Login Name** (alias) = sAMAccountName
- **Full Name** = DisplayName
- **Email Address** = Email Address



5. If you cannot use the **Find in LDAP** option to search for the user, then enter the user properties by hand as follows:

- **External Name.** The external name must match the user name in the external authentication system (e.g., Microsoft Active Directory).

Notes:

- The **External Name** is case sensitive.
 - If using Active Directory, the FDD user's **External Name** must match the user's Implicit UPN in Active Directory.
 - **Login Name.** The login name is the alias for the external name; this is the name that will display as the user name in FDD applications. A maximum of 30 characters is accepted.
5. Set the remaining user properties - **Database Role**, **User Type**, **Super Administrator** and **Optional Description**. See the [user properties step in Add Database Authenticated User](#) for details.

The password options - **Password**, **Confirm Password** and **Password Expires** - do not apply and are not shown when adding an externally authenticated user.
 6. Select the **Membership** tab and set the user's group membership. See the [group membership step in Add Database Authenticated User](#) for details.
 7. Select the **Permissions** tab and set the user's task permissions. See the [permissions step in Add Database Authenticated User](#) for details.
 8. You may see additional tabs for the user, depending on your FDD system licensing and configuration. Refer to the following topics for instructions on setting the additional user properties:
 - [Set User Audit Events for FDD Auditing](#)
 - [Set User Clearance for RMA iQ](#)
 - [Set User Other Properties for Access Restrictions](#)
 - [Set User Proxies](#)
 9. Click **OK**. The new user is created and you are returned to the **Feith User Administrator**.

Add Externally Authenticated User on MS SQL Server

The following instructions apply only if your FDD system is configured for external authentication.

If your FDD system is not configured for external authentication, users must be added as [database authenticated users](#).

To add an externally authenticated user on MS SQL Server:

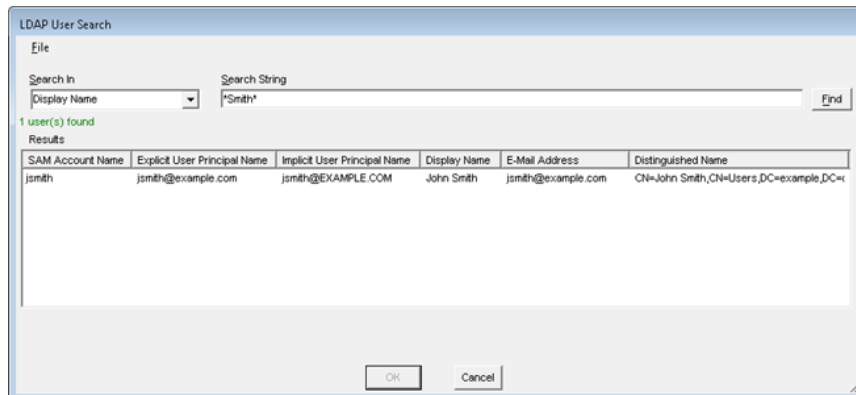
1. Select **File>Users** to open the **Feith User Administrator**.
2. Click **New**. The **Create New User** screen opens.
3. On the **Properties** tab, select the **Externally Authenticated** option.
4. If you have an LDAP server that contains a list of users that corresponds to your external authentication system (for example, if you are using Microsoft Active Directory), click the **Find** button to the right of **Domain** to search for the user in your LDAP server. This option populates the **Domain** and **Login Name** fields with the appropriate values from the user's LDAP account.
 - a. Click the **Find** button next to the **Domain** field.
 - b. If prompted, login to your LDAP server.

If you are automatically logged into an LDAP server and want to change your connection, a **Reconnect to LDAP** option is available under the **File** menu on the **LDAP User Search** screen.

See [Appendix C: LDAP Server Format](#) for more information on how to construct the server address.

- c. After logging in, enter the search criteria on the **LDAP User Search** screen and click **Find**.

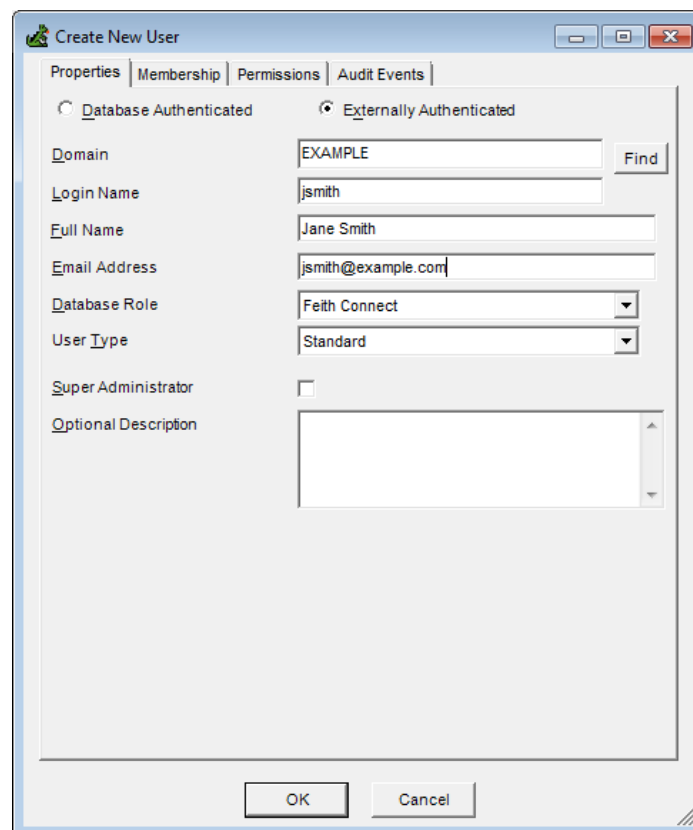
Tip: The asterisk character (*) can be used as a wildcard to replace any number of characters in the search string.



- d. Select a user name from the search results. The information on this screen, such as SAM Account Name, are Active Directory terms for user attributes. Refer to Microsoft Active Directory documentation for more information on user attributes in Active Directory.
- e. Click **OK** to add the user to FDD. The **Domain**, **Login Name**, **Full Name**, and **Email Address** fields will be populated with values from the user's LDAP account properties.

For example, if you are using Microsoft Active Directory the user properties are copied as follows:

- **Domain** = Domain name (the first part if multi-part)
- **Login Name** = sAMAccountName
- **Full Name** = DisplayName
- **Email Address** = Email Address



5. If you cannot use the **Find in LDAP** option to search for the user, then enter the user properties by hand as follows:
 - **Domain.** Enter your domain name.
 - **Login Name.** The login name must match the user name in the external authentication system (e.g., Microsoft Active Directory).
5. Set the remaining user properties - **Database Role**, **User Type**, **Super Administrator** and **Optional Description**. See the [user properties step in Add Database Authenticated User](#) for details.

The password options - **Password**, **Confirm Password** and **Password Expires** - do not apply and are not shown when adding an externally authenticated user.
6. Select the **Membership** tab and set the user's group membership. See the [group membership step in Add Database Authenticated User](#) for details.
7. Select the **Permissions** tab and set the user's task permissions. See the [permissions step in Add Database Authenticated User](#) for details.
8. You may see additional tabs for the user, depending on your FDD system licensing and configuration. Refer to the following topics for instructions on setting the additional user properties:
 - [Set User Audit Events for FDD Auditing](#)
 - [Set User Clearance for RMA iQ](#)
 - [Set User Other Properties for Access Restrictions](#)
 - [Set User Proxies](#)
9. Click **OK**. The new user is created and you are returned to the **Feith User Administrator**.

Change User Authentication Type

Caution

The following instructions include steps that result in the FDD user's database login being deleted and re-added.

The following instructions apply only if your FDD system is configured for external authentication.

If your FDD system is not configured for external authentication, users must be added as [database authenticated users](#).


If you are configuring an existing FDD system for external authentication, you may want to convert existing database authenticated users to externally authenticated users. This process involves changing both the user authentication type and the user name.

If you already have external authentication accounts set up with identical names for the users, you can [convert many users at once](#).


Convert Single User

To convert a database authenticated user to an externally authenticated user:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select a user and click **Modify**. The **Modify User** screen opens.
3. On the **Properties** tab, change the authentication type from **Database Authenticated** to **Externally Authenticated**.

 **Use with caution:** On MS SQL Server, changing the user's authentication type results in a change to the login name, which results in the database login being deleted and re-added.

4. Change the FDD user name to match the user's name in your external authentication system.

 **Use with caution:** On both Oracle and MS SQL Server, changing the user name for an FDD user will delete and re-add the user's database login.

- a. If you have an LDAP server that contains a list of users that corresponds to your external authentication system (for example, if you are using Microsoft Active Directory), use the **Find** option to search for the user in your LDAP server. This option populates the **External Name** and **Login Name** fields (on Oracle) or **Domain** and **Login Name** fields (on MS SQL Server) with the appropriate values from the user's LDAP account.
 - i. To do this on Oracle, see the [Find step in Externally Authenticated User on Oracle](#) for details.
 - ii. To do this on MS SQL Server, see the [Find step in Externally Authenticated User on MS SQL Server](#) for details.
- b. If you cannot use the **Find in LDAP** option to search for the user, then enter the user properties by hand as follows:
 - i. On Oracle:

External Name. The external name must match the user name in the external authentication system. The External Name is case sensitive. If using Active Directory, the FDD user's External Name must match the user's Implicit UPN in Active Directory.

Login Name. The login name is the alias for the external name; this is

the name that will display as the user name in FDD applications. A maximum of 30 characters is accepted.


- ii. On MS SQL Server:

Domain. Enter your domain name.

Login Name. The login name must match the user name in the external authentication system.

5. Click **OK** to save changes. The user properties are modified and you are returned to the **Feith User Administrator**.

Convert Many Users

 **Use with caution:** This option is intended for use only when the users exist in the external authentication system (e.g., Microsoft Active Directory) with names identical to their current FDD user names.

To convert many database authenticated users to externally authenticated users:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select multiple users that you want to convert. Use **CTRL+click** and **SHIFT+click** to select multiple users.
3. Select **Administrator>Convert Selected Users to External Authentication**. The **Convert to External Authentication** dialog opens.
4. Enter **Suffix** (Oracle) or **Domain** (MS SQL Server), depending on your database.
5. Click **OK**. A confirmation prompt opens, informing you:
 - The users must exist in the external authentication system (e.g., Microsoft Active Directory) with names identical to their current FDD user names.
 - The old database users will be deleted from the FDD system and replaced with the new externally authenticated users.
6. Click **Yes** to proceed. The users are converted from database authenticated to externally authenticated users.

Set User Audit Events for FDD Auditing

The following instructions apply only if your FDD system is licensed for FDD Auditor.

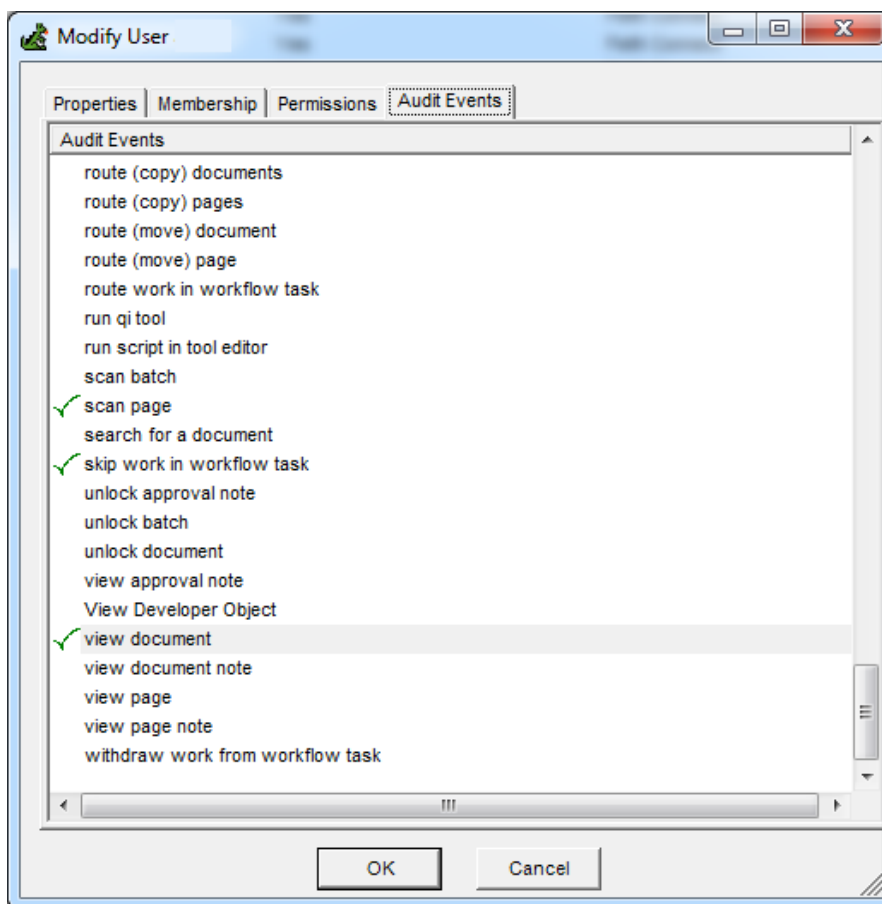
If your FDD system is licensed for **FDD Auditor**, the audit events for a user are set on the **Audit Events** tab of the user properties dialog.

When an audit event is selected for a user, an entry is written to the **FDD Audit Trail** each time the user performs the action. For example, if the audit event **View Page** is selected for the **Jane Smith** user, then an audit entry is written each time Jane Smith views a page. The audit data includes the user's internal ID, the name of the action performed, and the date and time the action was performed. Audit reports and graphs are viewed in the **FDD Auditor** application.

Note: Audit events can be turned on at both the user level and at the [group level](#). See [Audit Events](#) for the list of audit events that can be tracked in the FDD system.

To set user audit events:

1. When creating or modifying a user, select the **Audit Events** tab. The available audits are listed.
2. Double-click an event to select it for auditing. A check mark ✓ is shown in front of selected audit events. To deselect an audit event, double-click the event again; the check mark should be cleared



Note: The **Audit Events** tab appears only if your FDD system is licensed for FDD Auditor.

4. Finish setting the user properties as needed on the other tabs, then click **OK** to save the properties.

Set User Clearance for RMA iQ

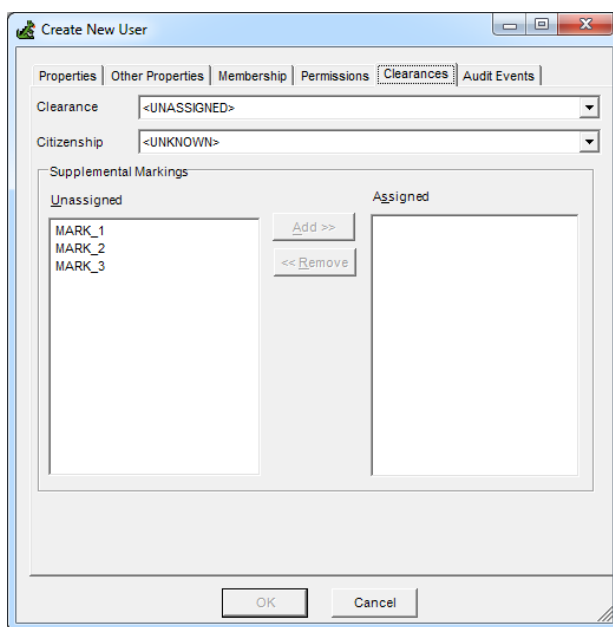
The following instructions apply only if your FDD system is licensed for RMA iQ.

If you are using **Feith RMA iQ**, the clearances for a user are set on the **Clearances** tab of the user properties dialog.

To set user clearances:

1. When creating or modifying a user, select the **Clearances** tab. The clearance options display.
2. Set the user's clearances:
 - Choose the user's **Clearance** level. Users granted a certain level of clearance (e.g. Secret) will have access to documents with that level of classification or lower (e.g., Secret, Confidential).
 - Choose the **Citizenship** of the user. A document with an assigned country code can only be accessed by users with the corresponding citizenship.
 - Assign **Supplemental Markings** to the user. Documents with supplemental markings can only be viewed by users who have been assigned all supplemental markings on the document.

To assign or remove supplemental markings, select the marking and use the **Add** or **Remove** button to move it to the appropriate list (**Assigned** or **Unassigned**). You can multi-select supplemental markings using **SHIFT+click** or **CTRL+click**.



Note: The **Clearances** tab appears only if one or more of its features are enabled in [System Preferences](#), and if you have the **Set User Clearances and Markings** task permission.

3. Finish setting the user properties as needed on the other tabs, then click **OK** to save the properties.

Set User Other Properties for Access Restrictions

The following instructions apply only if your FDD system is licensed for RMA iQ.

If your FDD system is configured to use **User Access Restrictions**, the access restriction properties for a user are set on the **Other Properties** tab of the user properties dialog.

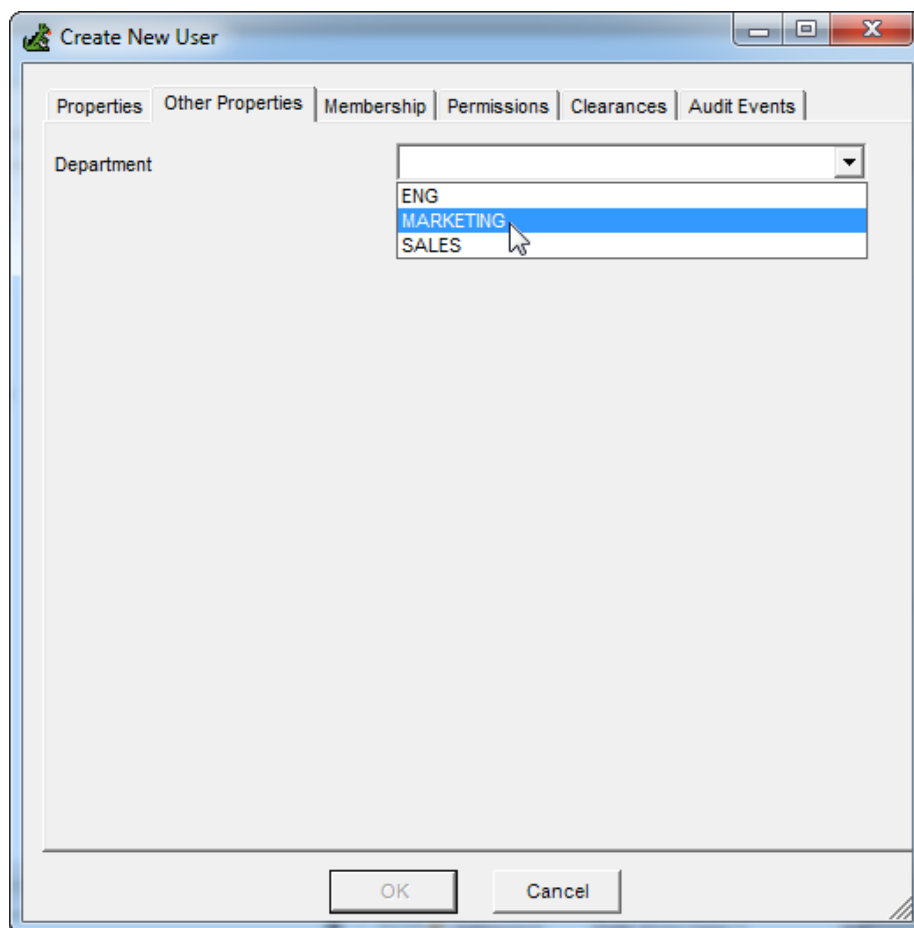
User access restriction rules control document access based on user properties. See [User Access Restrictions](#) for more information.

To set the access restriction properties for a user:

1. When creating or modifying a user, select the **Other Properties** tab. Any other properties display.

Note: The **Other Properties** tab appears only if fields have been added to the **Group Properties** auxiliary file cabinet. If the file cabinet contains 0 fields, then this tab does not appear.

2. Assign properties as needed.



3. Finish setting the user properties as needed on the other tabs, then click **OK** to save the properties.

Tip: A user's **Other Properties** are displayed on both the **Other Properties** tab and on the user's individual user report. To generate an individual user report, select the user in the user list and select **Report>Selected User**.

Set User Proxies

The following instructions apply only if your FDD system is running on Oracle and is configured for Proxy Authentication.

If your FDD system is configured for user authentication by proxy, the user's proxies are assigned in the **Proxies** tab of the user properties dialog. You can also assign proxies to [multiple users at once](#).

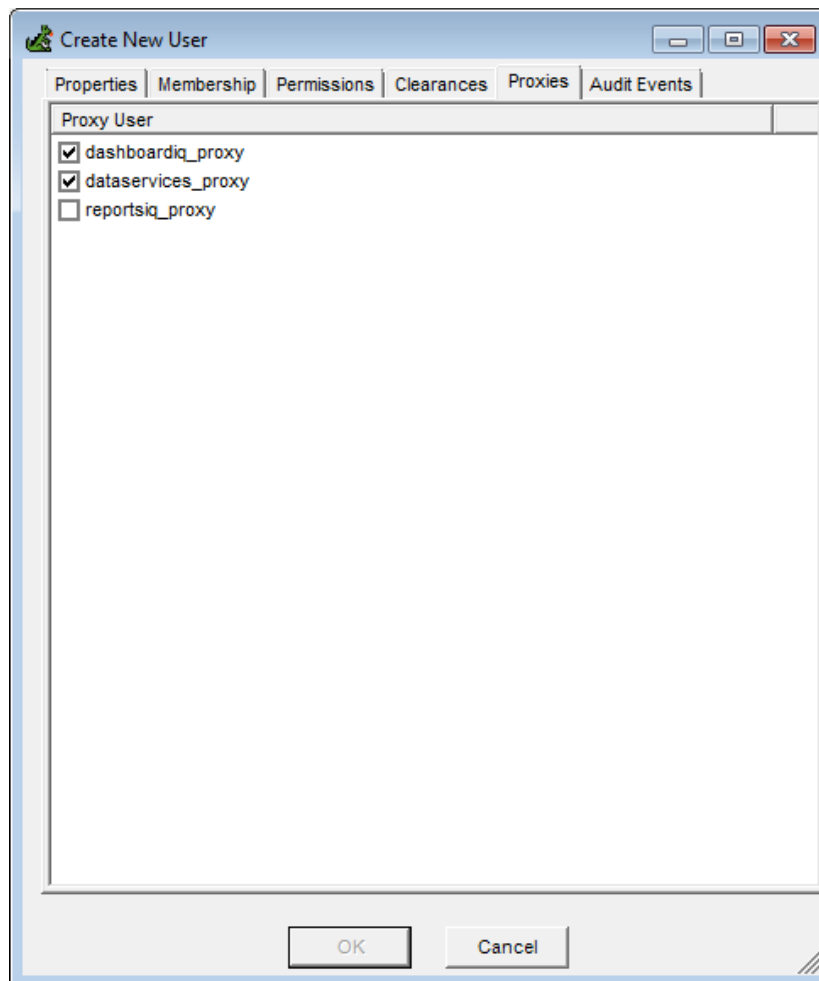
Assign Proxies to Single User

To set user proxies:

1. When creating or modifying a user, select the **Proxies** tab. Any proxy users in the system are listed.

Proxy users are added in the **Feith Proxy User Administrator**. See [Administer Proxy Users](#) for more information.

2. Check on the proxy users you want to assign to this user.



3. Finish setting the user properties as needed on the other tabs, then click **OK** to save the properties. You are returned to the **Feith User Administrator**.

Assign Proxies to Multiple Users

To assign proxies to multiple users:

1. In the **Feith User Administrator**, select multiple users using **CTRL+click** or **SHIFT+click**.
2. Right-click a selected user and select **Update Proxies>Assign Proxy Users to Selected Users**. The **Select Proxy Users** dialog opens.
3. Check on the proxy users you want to assign to the selected users.
4. Click **OK**. The proxy users are assigned to the selected users.

To remove proxies assignments from multiple users:

1. In the **Feith User Administrator**, select multiple users using **CTRL+click** or **SHIFT+click**.
2. Right-click a selected user and select **Update Proxies>Remove Proxy Users from Selected Users**. The **Select Proxy Users** dialog opens.
3. Check on the proxy users you want to remove from the selected users.
4. Click **OK**. The proxy users are removed from the selected users.

Modify User

To modify the properties of an existing user:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select a user and click **Modify**. The **Modify User** screen opens.
3. On the **Properties** tab, change the [user properties](#) as needed.

Caution

All user properties are editable, including the [authentication type](#) and the user name. Changing the authentication type and/or user name for an FDD user will delete and re-add the user's database login.

The ability to change the authentication type and user name for an FDD user is provided so that, if your FDD system is configured for external authentication, existing FDD users can be converted to externally authenticated users. See [Change User Authentication Type](#) for instructions on converting existing users to externally authenticated users.

4. Select the **Membership** tab and change the user's [group membership](#) as needed.
5. Select the **Permissions** tab and change the user's [task permissions](#) as needed.

You can assign permissions individually, or you can use the **Grant All**, **Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the user.

Note: Only super administrators can set permissions at the user level.

7. You may see additional tabs for the user, depending on your FDD system licensing and configuration. Refer to the following topics for instructions on setting the additional user properties:

- [Set User Audit Events for FDD Auditing](#)
- [Set User Clearance for RMA iQ](#)
- [Set User Other Properties for Access Restrictions](#)
- [Set User Proxies](#)

6. Click **OK** to save changes. The user is modified.

Clone User

To clone an existing user:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select a user and click **Clone**. The **Create New User** screen opens.

The extent to which properties are copied over from the original user to the new user depends on your administrative privileges:

- If you are logged in as a super administrator, group membership and task permissions are copied over from the original user to the new user.
- If you are logged in as a mid-level administrator, group membership for the groups you administer is copied over from the original user to the new user. Task permissions will be left unset for the new user.

3. On the **Properties** tab, enter the [properties](#) for the new user.
4. Optionally select the **Membership** tab and modify the user's [group membership](#).

Note: Mid-level administrators are limited in which groups they can assign a user. See [Levels of Administrators](#) for more information.

5. Optionally select the **Permissions** tab and modify the user's [task permissions](#).

Note: Only super administrators can set permissions at the user level.

6. You may see additional tabs for the user, depending on your FDD system licensing and configuration. Refer to the following topics for instructions on setting the additional user properties:
 - [Set User Audit Events for FDD Auditing](#)
 - [Set User Clearance for RMA iQ](#)
 - [Set User Other Properties for Access Restrictions](#)
 - [Set User Proxies](#)
6. Click **OK**. The new user is created.

Delete User

Delete Single User

To delete a user from the FDD system:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select a user and click **Delete**.

Note: A mid-level admin is limited in who they can delete. See [Levels of Administrators](#) for more information.

3. Answer **Yes** to the delete confirmation prompt. The user is deleted.

Mass Delete Selected Users

The **Mass Delete Selected Users** option will delete multiple users at one time. When using this option, note that only one confirmation prompt is shown before all selected users are deleted.

Note: Only super administrators can access this option.

To delete multiple users at one time:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select the users you wish to delete.
3. Select the **Mass Delete Selected Users** option from the **Administrator** menu. This option does not appear if you are not logged in as a super administrator.
4. A single confirmation prompt is shown, asking you whether you want to delete all of the selected users. Answer **Yes** to the confirmation prompt if you are certain you want to delete all of the selected users.

A status dialog is shown while the users are being deleted. If a large number of users were selected for deletion, the delete process may take a significant amount of time.

5. A success message is returned when the delete is complete; the message states the number of users deleted.

Enable/Disable User Account

Disabling a user account prevents that user from logging in through FDD.

To enable or disable a user account:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select a user and right-click on the user's login name.
3. In the right-click menu, click to **Enable Users** or **Disable Users**.
4. The value in the **Enabled** column will change to **Yes** or **No** depending on whether the selected user is enabled or disabled. If a user is disabled, he or she will not be able to login through FDD.

Import Users From File

To import users from file:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select the **File>Import Users>From File** menu option. The **Import Users** window opens.
3. Optionally choose a **Template User**. If a template user is selected, the following properties will be copied from the template user to the new users:
 - **Database Role**
 - **Workflow User Setting**
 - **Group Membership**
 - **Task Permissions**
4. Click **Open File** and select the text file to be used for import.

The file must be a pipe-delimited text file containing the login, full name, password and optional email address for the users; for example:

```
jsmith|Joe Smith|smith1234
```

After opening a file, the grid is populated with the user property information from the file.

User Name	Full Name	Password	E-Mail Address
jsmith	John Smith	jsmith1234	
cmorgan	Caroline Morgan	cmorgan1234	
jdoe	Jane Doe	jdoe1234	

5. Click the **Create Users** button to add the users. A status message is returned, indicating the number of users added.
6. Click **Exit Import** to return to the **Feith User Administrator**.

Import Users From LDAP

The following instructions apply only if your FDD system is configured for external authentication, and if your LDAP server contains a list of users that corresponds to your external authentication system (for example, if you are using Microsoft Active Directory).

Users imported from LDAP are added to FDD as [externally authenticated users](#).

To import users from LDAP:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select the **File>Import Users>From LDAP** menu option.
3. If prompted, login to your LDAP server. After logging into the LDAP server, the **Import Users** window opens.

Note: If you are automatically logged into an LDAP server and want to change your connection, a **Reconnect to LDAP** option is available under the **File** menu on the **LDAP User Search** screen. To open the **LDAP User Search** screen from the **Import Users** window, click the **Find Users** button.
4. On the **Import Users** window, optionally choose a **Template User**. If a template user is selected, the following properties will be copied from the template user to the new users:
 - **Database Role**
 - **Workflow User Setting**
 - **Group Membership**
 - **Task Permissions**
5. Search for LDAP users to import:
 - a. Click the **Find Users** button to open the **LDAP User Search** window.
 - b. Enter the search criteria in the **User Name** field on the **LDAP User Search** screen and click **Find**. The asterisk character (*) can be used as a wildcard to replace any number of characters in the search string.

To find all users, enter the asterisk character (*) as your search criteria.
 - c. If you are running on Oracle, select whether your database is configured for **Kerberos Authentication** or **RADIUS Authentication**. The FDD user **External Name** value will differ slightly depending on the type of authentication selected.
 - d. To select users from the search results, select one or more user names and click **OK**. The selected users will be listed on the **Import Users** dialog by **External Name**, **Login Name**, and **Distinguished Name**.

Import Users

Template User: <None>

LDAP Users

External Name	Login Name	Distinguished Name
jsmith@EXAMPLE.COM	jsmith	CN=John Smith,CN=...
sfields@EXAMPLE.COM	sfields	CN=Sarah Fields,CN=...

Find Users

Import Selected Users

Exit Import

- Click the **Import Selected Users** button to add the users to FDD. A status message is returned, indicating the number of users added.

For each imported user, the **External Name** (if on Oracle), **Domain** (if on MS SQL Server), **Login Name**, **Full Name**, and **Email Address** properties are set to values from the user's LDAP account properties.

- Click **Exit Import** to return to the **Feith User Administrator**.

Password Complexity and Expiration Rules

Only a super administrator can set password complexity and expiration rules.

FDD password complexity and expiration rules apply only to [database authenticated users](#).

Password complexity and expiration rules are set in the **User Password Admin** dialog. This dialog is accessed by selecting the **Administer Passwords** option from the **Administrator** menu in the **Feith User Administrator**.

Password Complexity

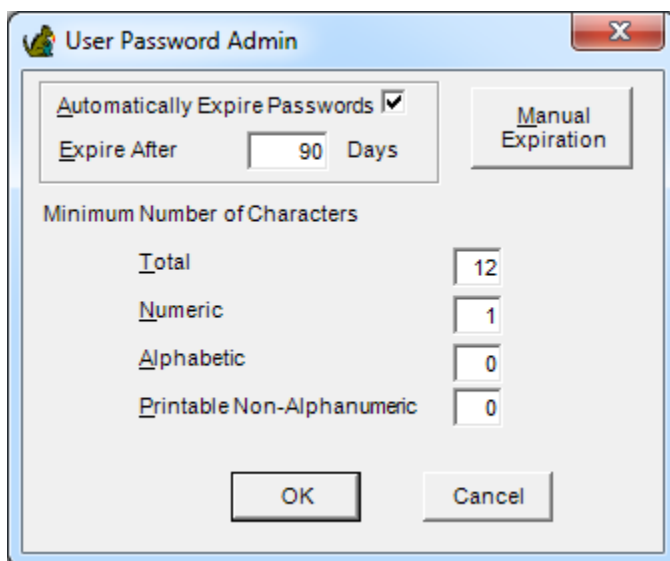
There are four password rules that can be set to govern the choice of passwords:

- The minimum length of a password.
- The minimum number of numeric characters (0-9).
- The minimum number of alpha characters (a-z and A-Z).
- The minimum number of printable non-alphanumeric characters (i.e., punctuation characters).

Password rules are system wide.

To set password complexity rules:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select **Administrator>Administer Passwords**. The **User Password Admin** dialog opens.
3. Set the following in the **Minimum Number of Characters** section:
 - **Total**: Enter the minimum length to be required of a password.
 - **Numeric**: Enter the minimum number of numeric characters (0-9) to be required in a password.
 - **Alphabetic**: Enter the minimum number of alpha characters (a-z and A-Z) to be required in a password.
 - **Printable Non-Alphanumeric**: Enter the minimum number of printable non-alphanumeric characters (punctuation characters) to be required in a password.



4. Click **OK** to save the settings.

Password Expiration

Passwords can be expired either automatically at a specified interval or manually for a specific group.

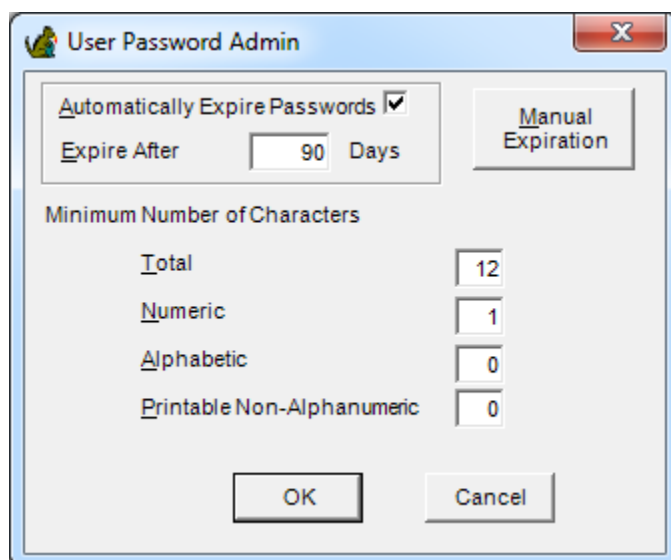
During login to FDD or WebFDD, the user's password will be checked for expiration. If the user's password has expired, the user will be prompted to change their password. The user will be unable to login to FDD or WebFDD until the password is changed.

A **Password Never Expires** option can be set per user, in the user's properties.

To set automatic password expiration:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select **Administrator>Administer Passwords**. The **User Password Admin** dialog opens.
3. Check the **Automatically Expire Passwords** option.
4. Enter the interval, in days, at which passwords should expire.

Note this setting does not apply to users whose passwords do not expire.

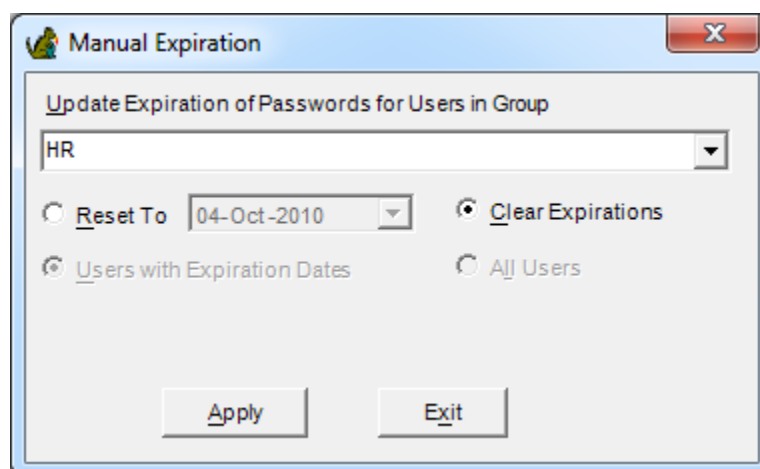


5. Click **OK** to save the settings.

To manually expire passwords for a group:

1. Select **File>Users** to open the **Feith User Administrator**.
2. Select **Administrator>Administer Passwords**. The **User Password Admin** dialog opens.
3. Click **Manual Expiration**. The **Manual Expiration** dialog opens.
4. Choose a group from the drop-down list.
5. Select whether to reset expirations or clear expirations.
 - To reset expirations:
 - a. Select the **Reset Expirations** option and choose the new expiration date from the calendar.
 - b. Select whether to apply the reset expirations to **Users with Expiration Dates** or **All Users**.
 - To clear expirations:

- Select the **Clear Expirations** option.



6. Click **Apply**.
7. Click **OK** to the confirmation prompt and exit the **Manual Expirations** dialog to return to the **User Password Admin** dialog.

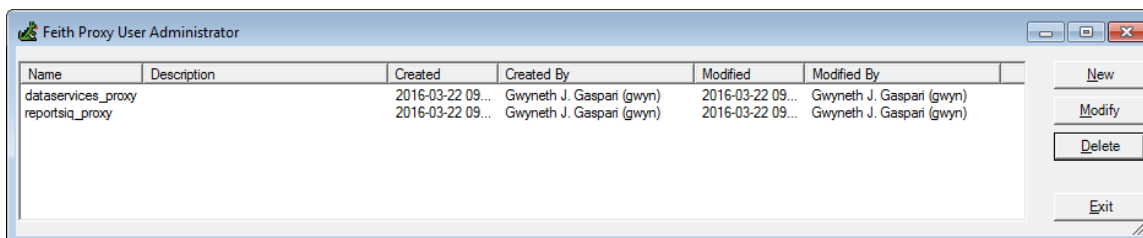
When viewing the properties for a user, the password expiration date shown is the date the user's password will next expire. If a password expiration interval is set for the FDD system, the user's password will repeatedly expire at the specified interval.

Administer Proxy Users

The following instructions apply only if your FDD system is running on Oracle and is configured for Proxy Authentication.

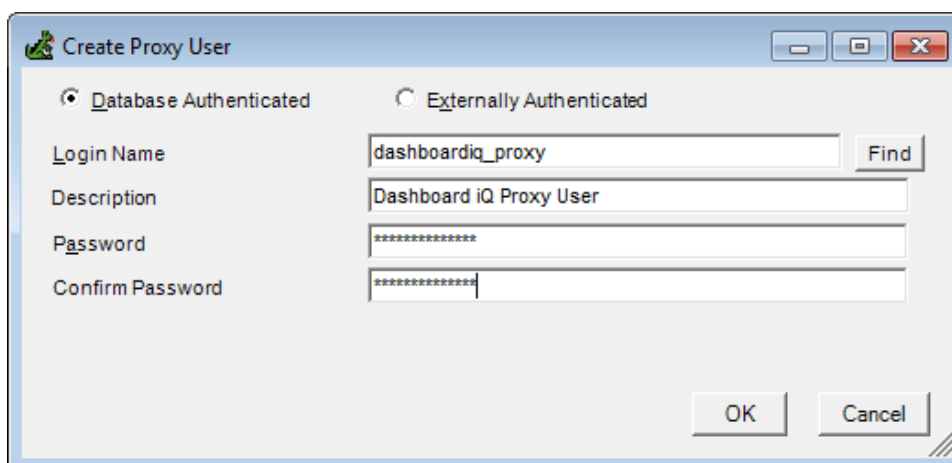
Create and maintain proxy users which can be used for authentication of your FDD users. See [Set User Proxies](#) for more information on assigning a proxy user to an FDD user.

Note: Only super administrators can access this option.



To create a Database Authenticated proxy user:

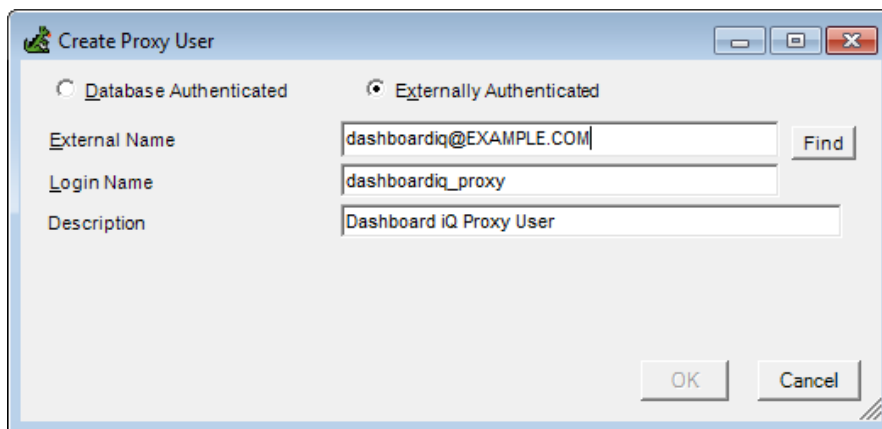
1. In the **Feith User Administrator**, select **Administrator>Administer Proxy Users**. The **Feith Proxy User Administrator** opens.
2. Click **New**. The **Create Proxy User** dialog opens.
3. Select the **Database Authenticated** option. See [User Authentication Types](#) for more information.
4. Enter the following user properties.
 - **Login Name:** Enter the user's login name. The maximum number of characters accepted varies per database.
 - **Description:** Optionally enter a user description. This description displays when viewing user properties in Feith Control Panel and on the user report generated from Feith Control Panel.
 - **Password:** Enter the user's password. The maximum number of characters accepted varies per database.
 - **Confirm Password:** Re-enter the password for verification.



5. Click **OK**. The proxy user is created and available to assign in a user's **Proxies** tab. See [Set User Proxies](#) for more information.

To create an Externally Authenticated proxy user:

1. In the **Feith User Administrator**, select **Administrator>Administer Proxy Users**. The **Feith Proxy User Administrator** opens.
2. Click **New**. The **Create Proxy User** dialog opens.
3. Select the **Externally Authenticated** option. See [User Authentication Types](#) for more information.
4. If you have an LDAP server that contains a list of users that corresponds to your external authentication system (for example, if you are using Microsoft Active Directory), click the **Find** button to the right of **External Name** to search for the user in your LDAP server. This option populates fields in the Create Proxy User dialog with the appropriate values from the user's LDAP account.
 - To do this on Oracle, see the [Find step in Externally Authenticated User on Oracle](#) for details.
 - To do this on MS SQL Server, see the [Find step in Externally Authenticated User on MS SQL Server](#) for details.
5. Optionally enter a user **Description**.



6. Click **OK**. The proxy user is created and available to assign in a user's **Proxies** tab. See [Set User Proxies](#) for more information.

To modify a proxy user:

1. In the **Feith User Administrator**, select **Administrator>Administer Proxy Users**. The **Feith Proxy User Administrator** opens.
2. Modify the **Description**, **Password**, and **Confirm Password** as needed. The authentication type and **Login Name** cannot be modified.
3. Click **OK**. The proxy user is modified.

To delete a proxy user:

1. In the **Feith User Administrator**, select **Administrator>Administer Proxy Users**. The **Feith Proxy User Administrator** opens.
2. Select a user and click **Delete**. You are prompted to confirm the delete.
3. Click **Yes** to continue. The proxy user is deleted.

User Reports

Two user reports are available: **Selected User** and **All Users**.

The **Selected User(s)** report lists the user properties, group membership and task permission assignments. This report is in HTML format.

The **All Users** report lists all users by login name, full name, type, workflow user designation, email address and password expiration. This report is in HTML format.

To generate a user report:

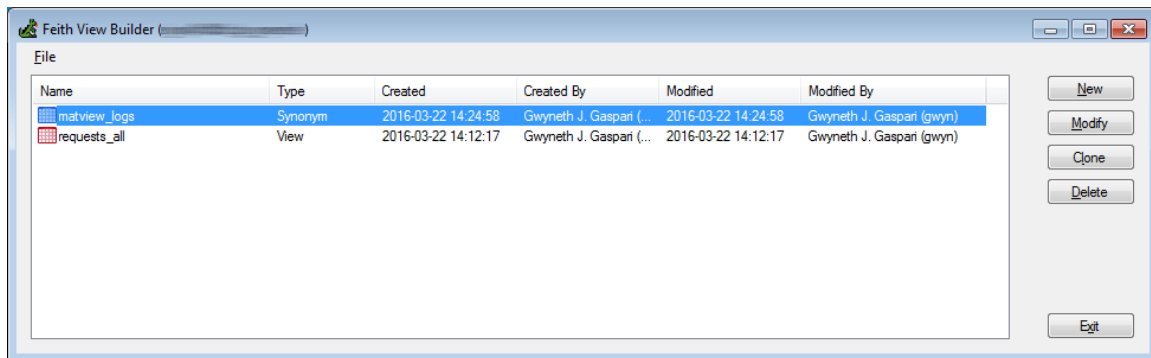
1. Select **File>Users** to open the **Feith User Administrator**.
2. Optionally select a user.
3. Select the **Report** menu and choose the desired report:
 - **Selected User(s) - HTML**
 - **All Users - HTML**
4. The report opens in a browser window.

View Builder

View Builder

Create database views and synonyms with this user-friendly tool. You may need a view to use as a lookup table on a file cabinet field, or a synonym of a non-fdd object for your dashboard in Dashboard iQ.

Note: Only views and synonyms created in the View Builder are available in this tool. Other views and synonyms in the FDD database, created outside the View Builder, are not listed.






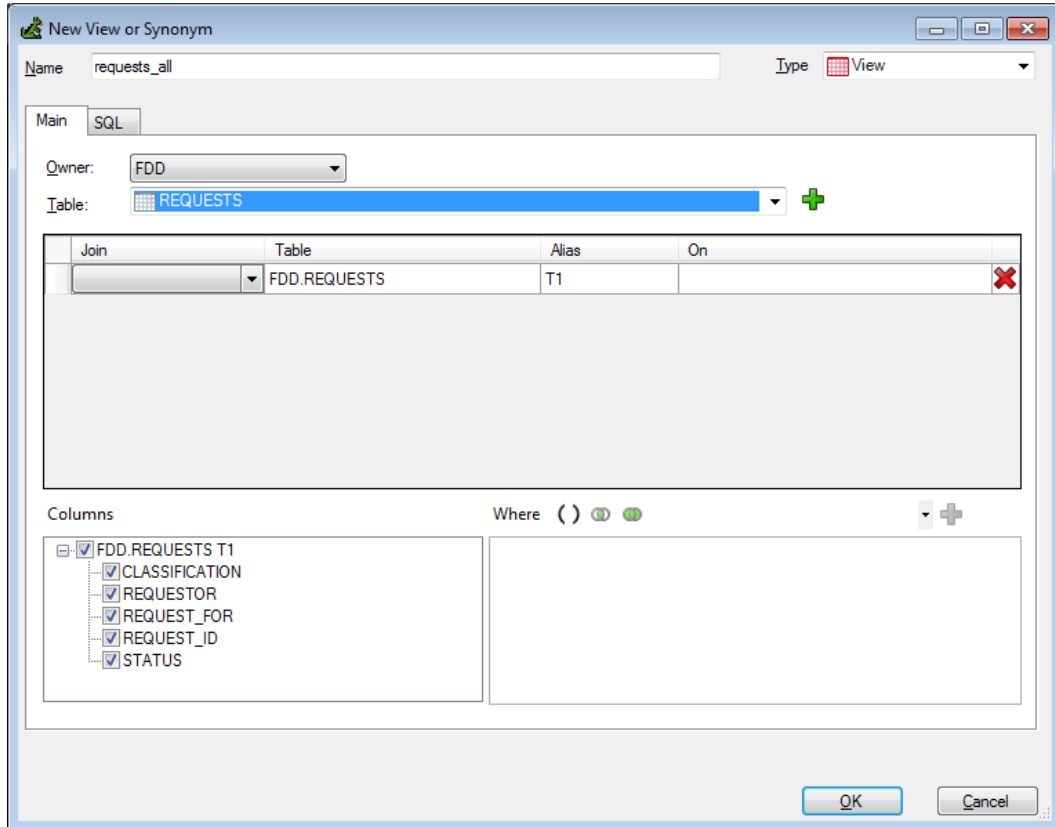
Add View

Add a database view with the user-friendly View Builder.

Note: Only views created in the View Builder are available in this tool. Other views in the FDD database, created outside the View Builder, are not listed.

To add a view:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Click **New**. The **New View or Synonym** dialog opens.
3. Enter a **Name** for the view.
4. Confirm the **Type** is set to **View**.
5. On the **Main** tab, select the **Owner** of the table or view on which you want to build this new view. Tables and views owned by the selected Owner are listed in the **Table** field. Tables are gray , views are red , and synonyms are blue .
6. Select the **Table** you want to include in the view and click **Add Table**. The table is added to the table list and its **Columns** are listed in the bottom left.



New View or Synonym

Name: requests_all Type: View

Main SQL

Owner: FDD

Table: REQUESTS


Join	Table	Alias	On
	FDD.REQUESTS	T1	

Columns

- ☒ FDD.REQUESTS T1
 - ☒ CLASSIFICATION
 - ☒ REQUESTOR
 - ☒ REQUEST_FOR
 - ☒ REQUEST_ID
 - ☒ STATUS

Where ()

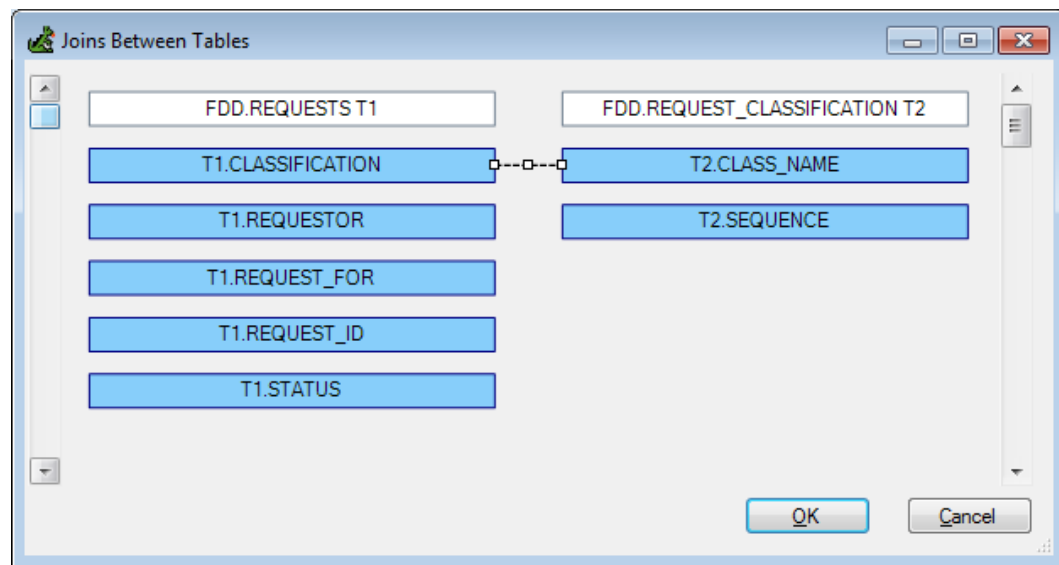
OK Cancel

7. Optionally uncheck **Columns** that you do not want to be in the view.
8. You may want to add another table to your view. To do so, select the desired **Owner** and **Table** and click **Add Table** . The **Joins Between Tables** dialog opens with the columns from the first table on the left and the columns from the second table on the right.
9. Set up the needed joins between the two tables. If the two tables have any column names in common, it is assumed those columns contain the same data and they are automatically suggested as a join.

Click-and-drag from a column on one side to the column on the other side. A line is drawn between the two columns, indicating a join. Create as many joins as needed.

Tip: You can select a join's line and click-and-drag the end points to change the column mapping.


To delete a join, select the line then right-click the line and select **Delete Join** (or just hit the **DELETE** key).



10. Once the join's columns are mapped click **OK**. The second table is added to the table list and its **Columns** are listed in the bottom left.
11. In the list of tables, optionally change the type of **Join**.

If you want to go back and change your join's column mappings, click the join's "link" in the **On** column which will return you to the **Joins Between Tables** dialog.

12. Optionally uncheck **Columns** from the second table that you do not want to be in the view.
13. Continue to add tables, make joins, and hide/show columns as needed until the view contains all the information you want.

To delete a table from the view, go to the table list and click **Delete Row** .

14. Optionally enter a **Where** clause to limit the data that comes back in the view. Use these tools to help you write your where clause:

- **Place Selected Text in Parentheses**
- **Insert AND operator**
- **Insert OR operator**
- Select an operator or column from the drop-down list and click **Insert Selected Value**

New View or Synonym

Name: requests_all Type: View

Main SQL

Owner: FDD Table: REVIEW_STATUS

Join	Table	Alias	On
	FDD.REQUESTS	T1	
INNER JOIN	FDD.REQUEST_CLASSIFICATION	T2	T1.CLASSIFICATION = T2.CLASS_NAME
INNER JOIN	FDD.REVIEW_STATUS	T3	T1.STATUS = T3.STATUS_NAME

Columns

- FDD.REQUESTS T1
 - CLASSIFICATION
 - REQUESTOR
 - REQUEST_FOR
 - REQUEST_ID
 - STATUS
- FDD.REQUEST_CLASSIFICATION T2
 - CLASS_NAME
 - SEQUENCE
- FDD.REVIEW_STATUS T3
 - SEQUENCE
 - STATUS_NAME

Where () = T1.STATUS = 'Pending'

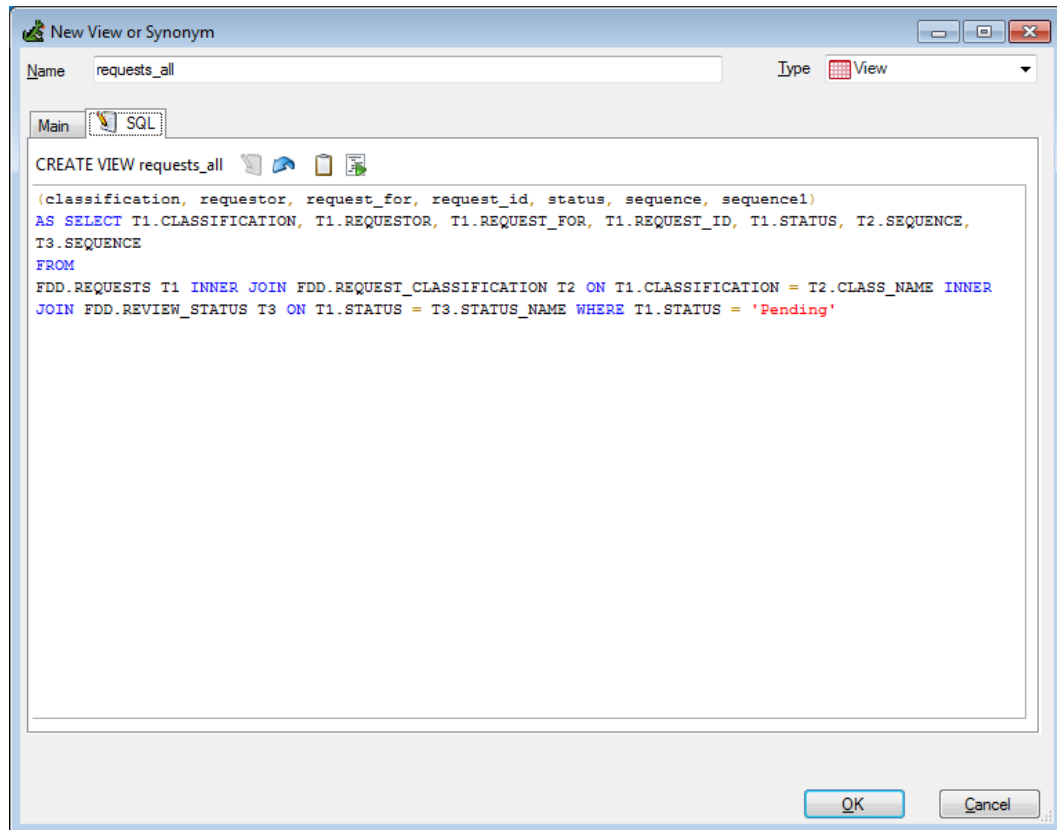
OK Cancel

15. As you choose options, the View Builder writes SQL (Structured Query Language) in the **SQL** tab for you and then you can use your SQL knowledge to customize the query. You may want to customize the query in order to put a function on a column, concatenate columns values, and more.

To customize your query, go to the **SQL** tab and click **Edit SQL** . Edit the SQL as needed, and you can use the **Test Query** or **Copy to Clipboard** buttons to help you.

If you dislike the changes you made, simply click **Revert SQL** to go back to the SQL generated by your selections in the **Main** tab.

Note: Once you edit the SQL, you can no longer modify the view using the friendly tools provided in the **Main** tab. To use the builder tools again you have to revert the SQL.






16. Click **OK**. The view is added.

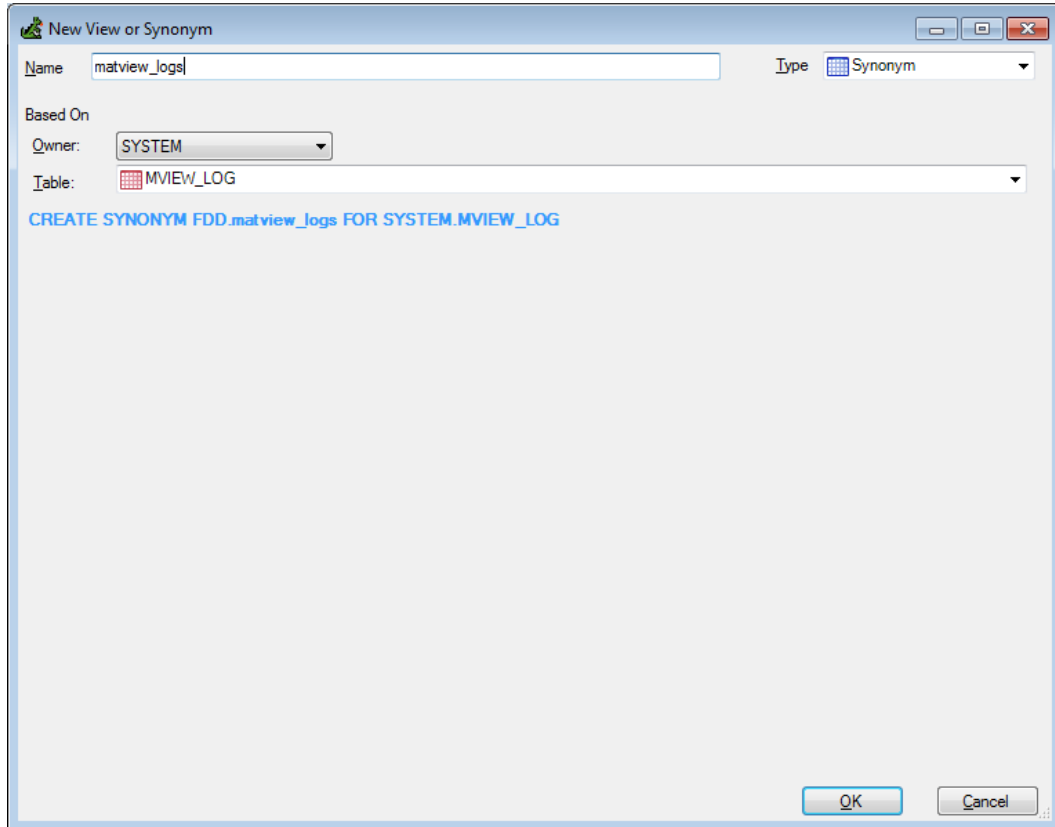
Add Synonym

Add a database synonym with the user-friendly View Builder.


Note: Only synonyms created in the View Builder are available in this tool. Other synonyms in the FDD database, created outside the View Builder, are not listed.

To add a synonym:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Click **New**. The **New View or Synonym** dialog opens.
3. Enter a **Name** for the synonym.
4. Change the **Type** to **Synonym**.
5. Select the **Owner** of the table or view you want to make a synonym for. Tables and views owned by the selected Owner are listed in the **Table** field. Tables are gray , views are red , and synonyms are blue .
6. Select the **Table** you want to make a synonym for. The SQL (Structured Query Language) to make the synonym is displayed below.



New View or Synonym

Name: Type:  Synonym

Based On



Owner:  SYSTEM

Table:  MVIEW_LOG

CREATE SYNONYM FDD.matview_logs FOR SYSTEM.MVIEW_LOG

7. Click **OK**. The synonym is added.

Manage Views and Synonyms

Manage your views and synonyms.

Modify View or Synonym

To modify a view or synonym:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Select the desired view or synonym and click **Modify**. The **Modify** dialog opens.
3. Make changes as needed. See the following for details:
 - [Add View](#)
 - [Add Synonym](#)
4. Click **OK**. The view or synonym is modified.

Clone View or Synonym

To clone a view or synonym:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Select the desired view or synonym and click **Clone**. The **Clone** dialog opens with settings identical to the original view or synonym but with a number appended to the **Name**.
3. Optionally change the **Name** and other settings.
4. Click **OK**. The view or synonym is created.

Delete View or Synonym

To delete a view or synonym:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Select the desired view or synonym and click **Delete**. You are prompted to confirm the delete.
3. Click **Yes** to proceed. The view or synonym is deleted.

Export and Import Views and Synonyms

Migrate View Builder views and synonyms from one FDD system to another, such as from test to production.

Export View or Synonym

To export a view or synonym:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Select the desired view or synonym and then select **File>Export View or Synonym**. The **Export View or Synonym** dialog opens.
3. Browse to a location on your computer and click **Save**. The export .XML file is saved.

Import View or Synonym

To import a view or synonym:

1. In the **Feith Control Panel**, select the **View Builder** module. The **Feith View Builder** opens.
2. Select **File>Import View or Synonym**. The **Import** dialog opens with settings from the export file.

If the **Name** in the export file is identical to an existing view's or synonym's name, a number is appended on the end.
3. Optionally change the **Name** and other settings.
4. Click **OK**. The view or synonym is imported.

Virtual File Cabinets

Virtual File Cabinets Overview

The following instructions apply only if your FDD system is licensed for virtual file cabinets.

A **virtual file cabinet** is based on a database view of a regular file cabinet.

When adding a virtual file cabinet, you select which file cabinet fields to include and can optionally specify a condition to restrict which documents are returned. A virtual file cabinet can be a join of the base file cabinet and another table.

Examples:

- A virtual file cabinet could return a subset of the documents contained within the base file cabinet. For example, a virtual file cabinet might return only documents where a **Document Type** file cabinet field value equals **Invoice**.
- A virtual file cabinet could join the base file cabinet against a database table used by another application. For example, a virtual file cabinet might join against a table in an ERP or accounting system to display additional metadata for FDD documents.

Virtual file cabinets do not actually contain any documents. The documents reside in the virtual file cabinet's base file cabinet.

Add Virtual File Cabinet

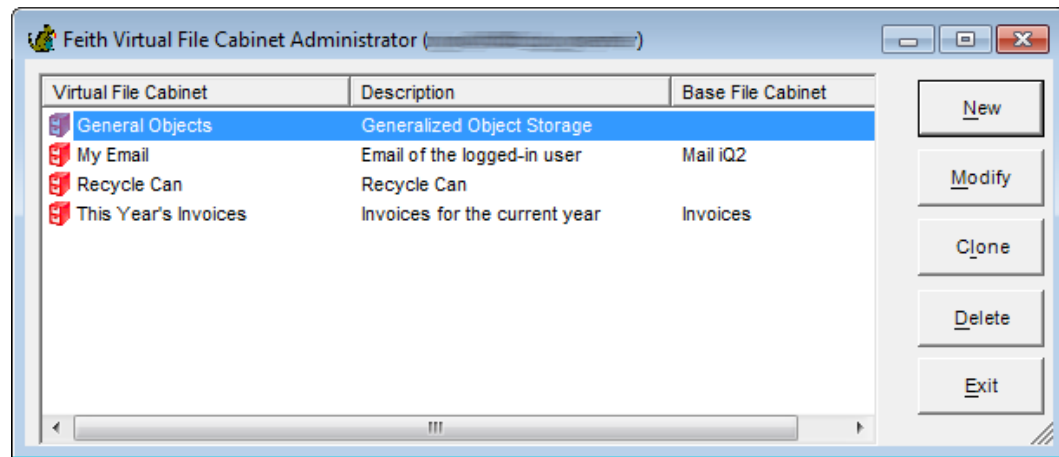
The following instructions apply only if your FDD system is licensed for virtual file cabinets.

To add a virtual file cabinet:

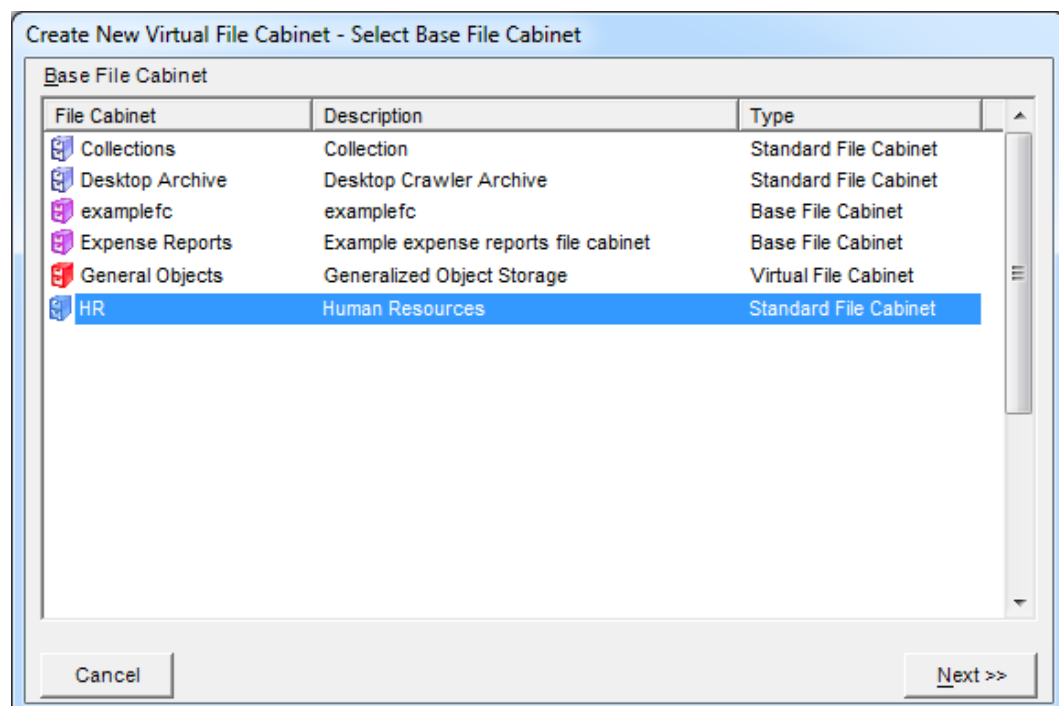
1. Select the **Virtual File Cabinets** option from the **File** menu. The **Virtual File Cabinet Administrator** opens. All virtual file cabinets to which you have administrative access are listed.

Note the following system virtual file cabinets are created during the FDD installation: **FeithDrive**, **FeithDrive AIQ**, **General Objects** and **My Reports**.

See [File Cabinet Overview](#) for more information on system file cabinets.



2. Click **New**. The **Create New Virtual File Cabinet** wizard opens to the **Select Base File Cabinet** window. All file cabinets to which you have administrative access are listed.
3. Select the file cabinet on which to base the virtual file cabinet.



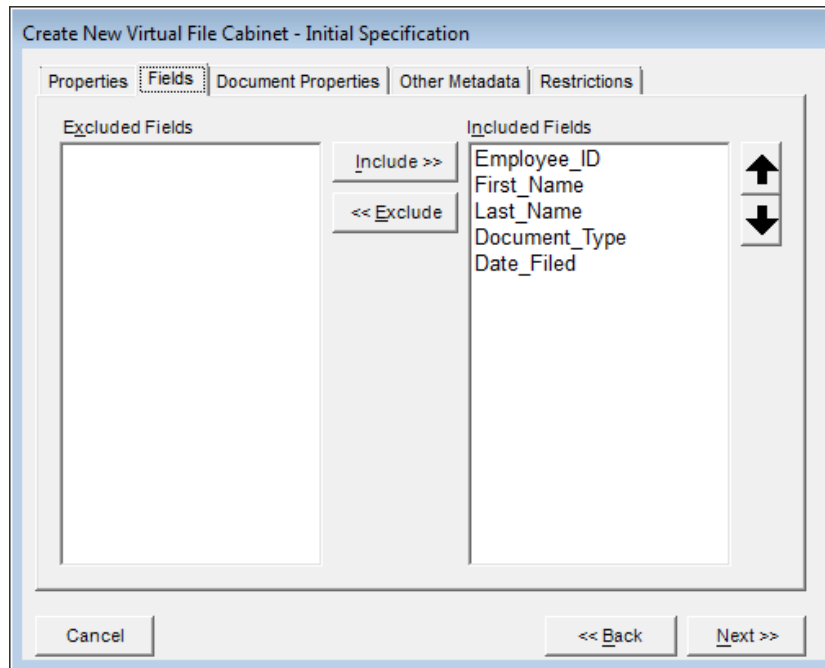
4. Click **Next**. The **Create New Virtual File Cabinet - Initial Specification** window opens. The **Initial Specifications** window has three tabs - **Properties**, **Fields** and **Restrictions**. The **Properties** tab is selected by default.
5. On the **Properties** tab of the **Initial Specification** window, enter the following properties for the virtual file cabinet:
 - **Name:** Enter the virtual file cabinet name. The maximum length is 64 characters.
 - **Description:** Enter the virtual file cabinet description. The maximum length is 132 characters.
 - **Allow Full Text Search:** Turn on to allow full text searching in the virtual file cabinet. Turn off to disallow full text searching on the virtual file cabinet (say, for a sensitive value).

The screenshot shows a dialog box titled "Create New Virtual File Cabinet - Initial Specification". It has five tabs: "Properties", "Fields", "Document Properties", "Other Metadata", and "Restrictions". The "Properties" tab is active. Inside the tab, there are three input fields: "Name" with the text "Resumes", "Description" with the text "Resumes in HR file cabinet", and a checkbox labeled "Allow Full Text Search" which is checked. At the bottom of the dialog, there are three buttons: "Cancel", "<< Back", and "Next >>".

6. On the **Fields** tab, select which fields from the base file cabinet to include in the virtual file cabinet. All fields are included by default.

Included fields are shown in the **Included Fields** list; excluded fields are shown in the **Excluded Fields** list. Use the **Include** and **Exclude** buttons to move a selected field from one list to the other list. Double-clicking a field will also move the field from one list to the other list.

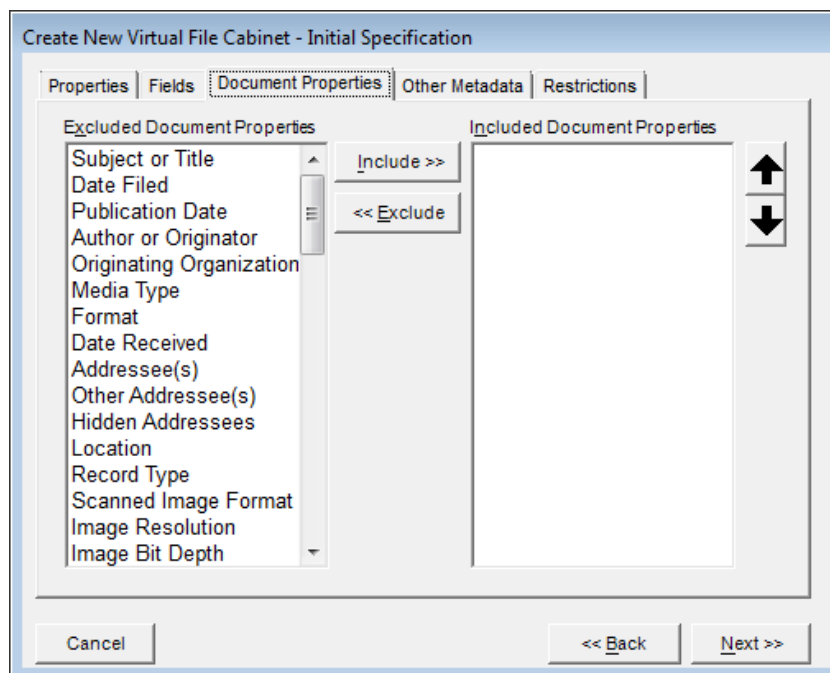
To reorder the fields in the **Included Fields** list, select a field and use either the **Up** or **Down** arrow to move the field.



7. On the **Document Properties** tab, optionally select which document properties to include in the virtual file cabinet. All properties are excluded by default.

Excluded properties are shown in the **Excluded Document Properties** list; included properties are shown in the **Included Document Properties** list. Use the **Include** and **Exclude** buttons to move a selected property from one list to the other list. Double-clicking a property will also move the property from one list to the other list.

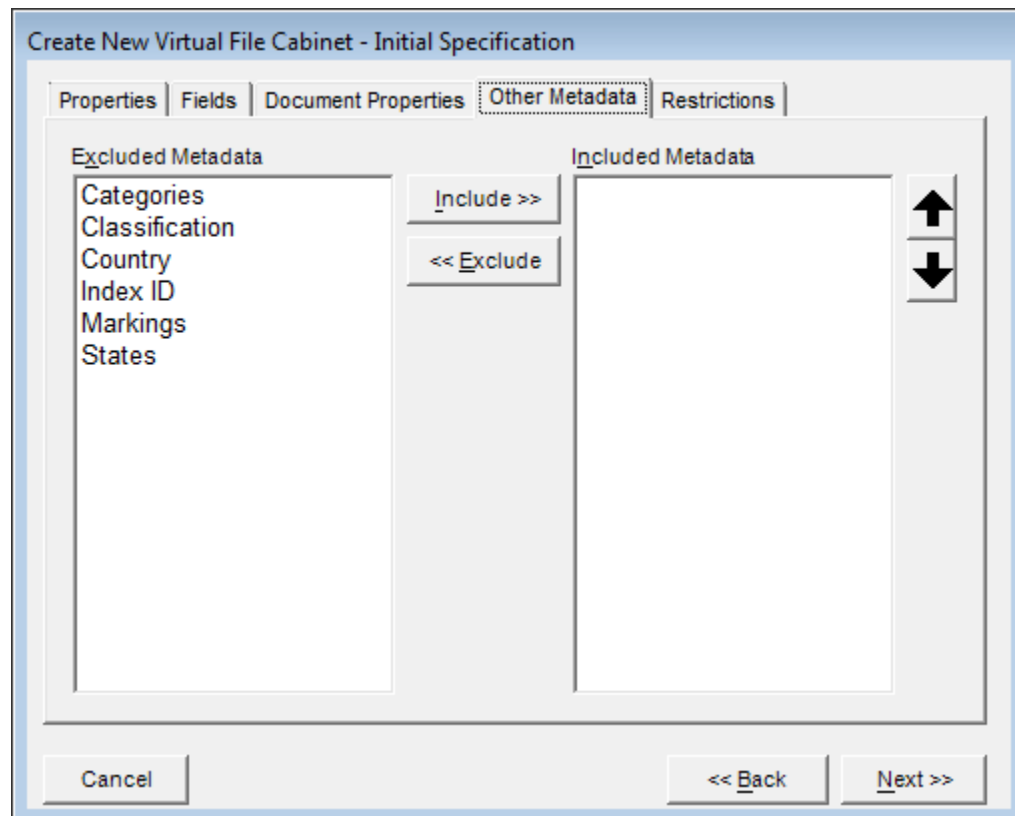
To reorder the properties in the **Included Document Properties** list, select a property and use either the **Up** or **Down** arrow to move the property.



8. On the **Other Metadata** tab, optionally select which other metadata fields to include in the virtual file cabinet, including the internal Index ID of the document and RMA information. All fields are excluded by default.

Excluded fields are shown in the **Excluded RMA Fields** list; included fields are shown in the **Included RMA Fields** list. Use the **Include** and **Exclude** buttons to move a selected field from one list to the other list. Double-clicking a field will also move the field from one list to the other list.

To reorder the fields in the **Included Fields** list, select a field and use either the **Up** or **Down** arrow to move the field.



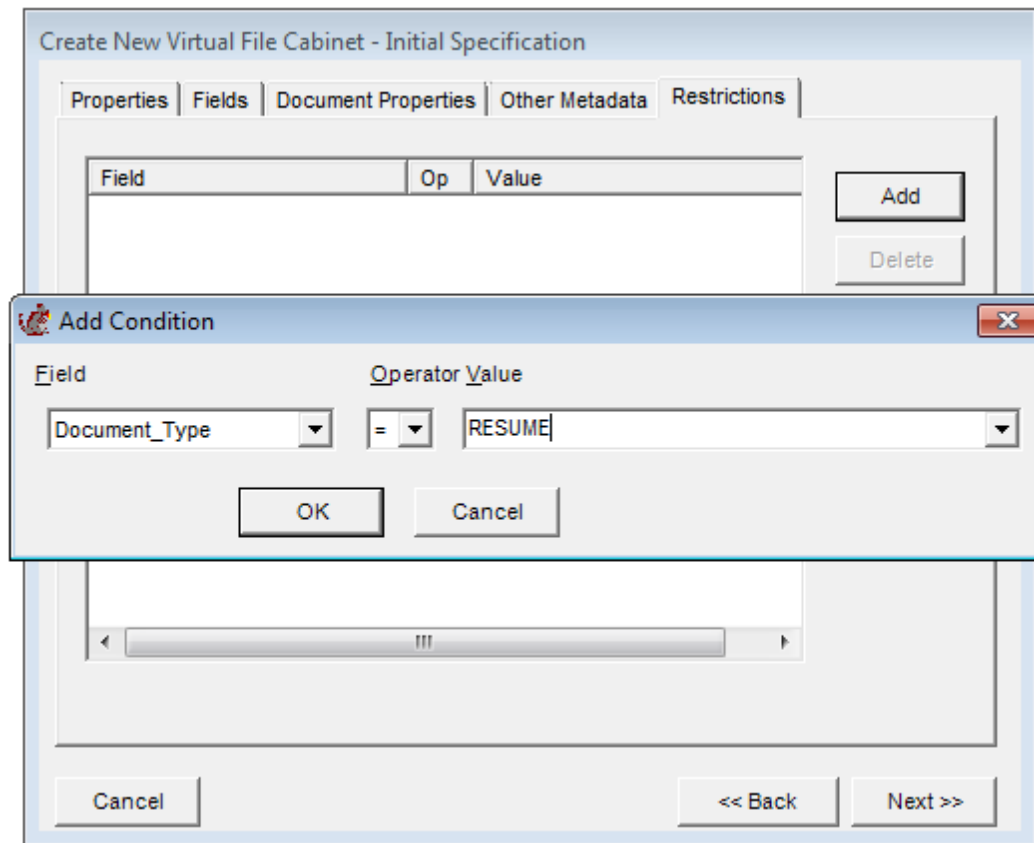
9. Optionally specify a file cabinet field based restriction on the **Restrictions** tab.

If a restriction is specified, the virtual file cabinet will return only the documents in the base file cabinet that meet the condition.

To add a restriction: Click **Add** to open the **Add Condition** dialog. Select the file cabinet field, the operator, and the value from the **Field**, **Operator** and **Value** lists. If the selected file cabinet field has a lookup table, the lookup values are shown in the **Value** list. Click **OK** to add the condition.

To delete a restriction, select the restriction and click **Delete**.

Multiple restrictions can be specified. By default, the restrictions are joined by **AND**. To join the restrictions by **OR**, change the **Join With** radio button selection from **AND** to **OR**.



10. Click **Next**. The **Create New Virtual File Cabinet - Customize** window opens. At this stage, you can customize the virtual file cabinet. Customization is optional; if your virtual file cabinet is complete, click **Next** to finish the process.

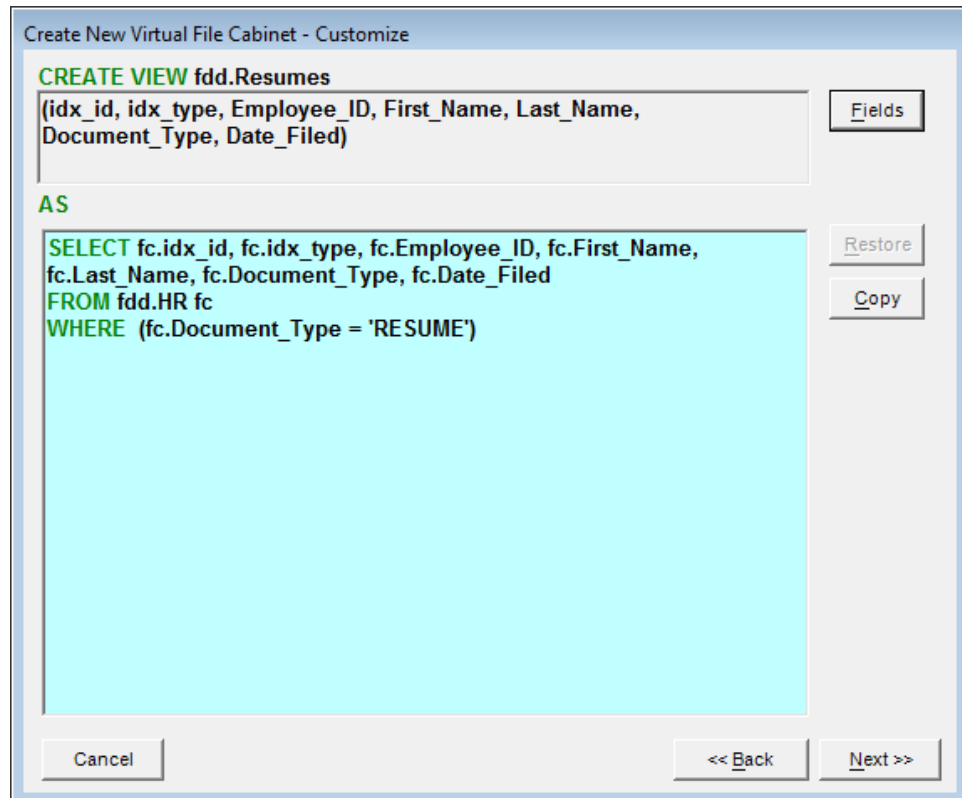
Note that if you add or remove a field to or from the virtual file cabinet (under the **Fields** interface), the select clause of the view must be manually edited to reflect the change.

When editing the virtual file cabinet SQL, you can click the **Restore** button to restore the original SQL (as defined by the selections in the preceding step on the **Initial Specifications** dialog).

Selected text can be copied to the clipboard by clicking **Copy**.

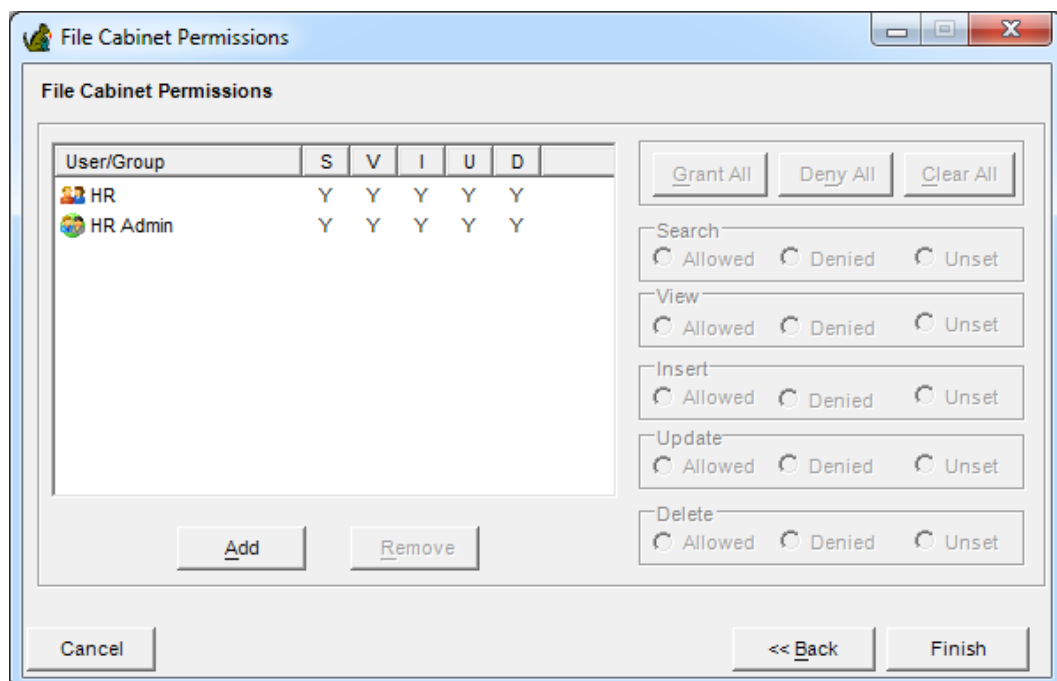
Notes:

- If you join to another table or view in your customized virtual file cabinet SQL, it is recommended you deny **Update (U)** resource permission on the virtual file cabinet. Updates will not work as expected and therefore should be prohibited.
- An ORDER BY clause in your customized virtual file cabinet will not work as intended due to the client applications' permission-checking. Instead, set a **Default Sort Order** in the virtual file cabinet's properties. See [Modify File Cabinet](#) for more information.



11. When you are finished customizing the virtual file cabinet, click **Next**. The **File Cabinet Permissions** window opens. The base file cabinet permission assignments are copied over as the default. Modify permissions as needed.

Note: Because a virtual file cabinet is based on a database view, some permission settings may not work as expected. Test the results when granting permissions other than "View".



- To grant permissions to a group or user:
 - a. Click **Add**. The **Users and Groups** screen opens, listing all FDD groups and users to which you have administrative access.
 - b. Select a group or user in the list and click **OK**. The selected group or user is granted permissions to the file cabinet. By default, all five resource permissions - **Search, View, Insert, Update** and **Delete** - are granted to the group or user.
 - To modify the permissions assigned to a group or user:
 - Select a group or user in the permissions list. Change the setting for a single permission by toggling between the **Allowed, Denied** and **Unset** options, or use the **Grant All, Deny All** and **Clear All** buttons to grant, deny or clear all permissions for the group or user.
 - To revoke permissions from a group or user:
 - Select a group or user in the permissions list and click **Remove**. All permissions to the file cabinet are revoked from the group or user.
12. Click **Finish**. The virtual file cabinet is created and you are returned to the **Virtual File Cabinet Administrator**.

Modify Virtual File Cabinet

The following instructions apply only if your FDD system is licensed for virtual file cabinets.

It is not recommend to modify a virtual file cabinet here in power FCP that was originally created in WebFCP. Modifying the virtual file cabinet in power FCP may cause errors and prevent the use of more advanced features that WebFCP supports.

To modify the permissions for a virtual file cabinet:

1. Select **File>File Cabinets** to open the **File Cabinet Administrator**.
2. Select the virtual file cabinet and click **Modify**. The **Modify File Cabinet** screen opens.
3. Click **Permissions**. The **File Cabinet Permissions** screen opens.
4. Modify permissions as needed. See [Add Virtual File Cabinet](#) for instructions on assigning permissions.

Note: Because a virtual file cabinet is based on a database view, some permission settings may not work as expected. Test the results when granting permissions other than "View".

5. Click **OK** to save the changes, then click **Exit** to return to the **Feith File Cabinet Administrator**.

To modify an existing virtual file cabinet:

1. Select **File>Virtual File Cabinets** to open the **Virtual File Cabinet Administrator**.
2. Select the virtual file cabinet and click **Modify**. The **Modify Virtual File Cabinet** screen opens.
3. Modify the virtual file cabinet as needed.

To modify fields in the virtual file cabinet, click the **Fields** button and make changes as needed.

When editing the virtual file cabinet SQL, you can click the **Restore** button to restore the original SQL.

4. Click **OK** to save the changes; you are returned to the **Feith Virtual File Cabinet Administrator**.

Appendix

Appendix A: Field Mask and Regular Expression Syntax

Field Masks

A field mask is created by setting up a sequence of placeholder characters. The characters are listed below.

#	The digit place holder. 0-9
A	Alphanumeric place holder. 0-9 and a-Z
?	Alpha place holder.
\	The escape character.
.	The decimal place holder.

For example, **###-###-#### Ext ###** will provide an input mask for **area code**, **phone number** and **extension**.

Regular Expression Validations

Regular expressions provide a way to define a string pattern. Since file cabinet indexing values frequently follow a pattern or format, a regular expression can be created to test input data for proper format.

[^\$. ?*()]	These are the special characters of regular expressions. When these characters exist in the pattern, then they can be escaped with a '\' character.
^	The caret specifies the beginning of a pattern.
\$	The dollar sign specifies the end of a pattern.
[]	This specifies a set of characters. For example, [abc] specifies 'a' or 'b' or 'c'. [a-zA-Z] specifies the alphabet.
[^]	Specifies anything but the listed set of characters. For example, [^0-9] specifies anything but the digits 0 through 9.
\d	Specifies a digit.
\w	A word character. The same as [a-zA-Z0-9]
	The pipe character performs an OR. For example, abc xyz specifies "abc" or "xyz".
{n}	Specifies a sequence of characters. For example, z{2} specifies "zz". \d{3} specifies 3 digits.
{n,m}	Specifies a sequence of characters of at least n and less than equal to m. For example, \d{2,3} specifies 2 or 3 digits.
?	Specifies that the previous item optional. For example, Bills? Specifies "Bill" or "Bills"
*	Specifies that the previous item will be repeat zero or more times. The period specifies any single character.

+	Specifies that the preceding character(s) will repeat 1 or more times.
()	The parenthesis supports precedence.

For example, `^\d{3}-\d{2}-\d{4}$` will test for a **Social Security number**:

^	The beginning of the pattern.
\d{3}	The first 3 digits.
-	The first hyphen.
\d{2}	The middle 2 digits.
-	The second hyphen.
\d{4}	The last 4 digits.
\$	The end of the pattern.

Appendix B: Auto-Populated Field Names

You can give a file cabinet field a special name in order for the field to be automatically populated with information from the file being imported. FDD and CheckIn automatically populate fields with certain names.

Results will vary based on the file type, operating system, and method of submitting the document through CheckIn. The below table is based on files saved to FDD through CheckIn from within Microsoft Office applications.

In order for this feature to work, the file cabinet fields must be given specific names when creating them in Feith Control Panel.

FIELD NAME	APPLICATION	SUGGESTED FIELD TYPE	WORD, EXCEL, POWERPOINT	OUTLOOK
Addressee	CheckIn	String	No	Yes
Application Name	CheckIn	String	Yes	No
Author	CheckIn	String	Yes	No
CC	CheckIn	String	No	Yes
Comments	CheckIn	String	Yes	No
Creation Date	CheckIn	Date	Yes	Yes
Date Received	CheckIn	Date	No	Yes
Extension	FDD and CheckIn	String	Yes	Yes
Filename	FDD and CheckIn	String	Yes	Yes
Filesize	FDD and CheckIn	Integer	Yes	Yes
Recipient	CheckIn	String	No	Yes
Sender	CheckIn	String	No	Yes
Sent On	CheckIn	Date	No	Yes
Start Date	CheckIn	Date	No	Yes
Subject	CheckIn	String	Yes	Yes
Title	CheckIn	String	Yes	No
Type	CheckIn	String	No	Yes

Notes:

- **Filesize** contains the size of the file measured in bytes.
- FDD and CheckIn will recognize the field name whether it is typed in uppercase, lowercase, or mixed case.
- The presence or absence of spaces in two-word field names *does* matter. Enter the field name exactly as shown in the above list

Appendix C: LDAP Server Format

When you use the **Find** feature to login to LDAP and add externally-authenticated users to your FDD database, whether on [Oracle](#) or [MS SQL Server](#), enter the **LDAP Server** in the following format:

LDAP://yourserver:389/cn=users,dc=yourcompany,dc=com

LDAP	Connect using the LDAP protocol (Lightweight Directory Access Protocol).
yourserver	Name of your LDAP server. Typically this is the name of the Microsoft Active Directory server.
389	Port on which to connect to the LDAP server. Typically this is 389.
cn=users	Common name of the "users" container in LDAP from which you want to get information to create the FDD user.
dc=yourcompany	Domain component, such as your company name (e.g. the "acmec" in "acmec.com").
dc=com	Domain component, such as your domain extension (e.g. the "com" in "acmec.com").

Note: The portion of the LDAP Server example **cn=users,dc=yourcompany,dc=com** is the typical format used by Microsoft Active Directory. Other LDAP implementations may use a different format.

Glossary

A

Administrator Group: A group that has administrative access to specific FDD file cabinets and groups. When administrator group members login to Feith Control Panel, they will only see those file cabinets and groups to which they have been assigned.

Audit Trail: A record of actions taken by users in the FDD system. The audit data includes the user's internal ID, the name of the action performed, and the date and time the action was performed. An FDD administrator configures which actions to track for which users and groups.

B

Base File Cabinet: A file cabinet which has another object built upon it. Objects that can be built on file cabinets include virtual file cabinets, workflows, and Forms iQ forms.

Batch: A temporary grouping of one or more pages. Batches reside in bins. A batch of pages is usually acquired into FDD as a group.

Bin: A temporary storage area for batches waiting to be indexed.

C

Classification: Restricts access to a document according to the level assigned to the document and level assigned to the user. Classifications are hierarchical and a user must have a clearance level that is at or above the classification level assigned to the document.

D

Dashboard iQ Server: A web server running the Feith Dashboard iQ Server application.

Developer Server: A web server running the Feith Developer application.

Document: A permanent grouping of related pages. Documents reside in file cabinets. The pages in a document were indexed with the same indexing values.

Document Permission: A permission set at the document and folder level by assigning a document permission template to a document or folder.

Document Permission Template: A template assigned to a document or folder, which will restrict access and operations on the document/folder based on the template's settings.

Document Viewer Server: A web server running the Feith Document Viewer application.

E

EDStor Server: A storage server controlled by Feith EDStor software.

F

File Cabinet: A permanent storage area for indexed documents. Each file cabinet is defined by the index fields (e.g., name, date, amount) it uses to organize stored images. Each entry in the file cabinet consists of a group of index field values (e.g., Joe Smith, 12/19/14, \$1410.43) and the images associated with those values.

Forms iQ Server: A web server running the Feith Forms iQ Server application.

Full Text: The text content of a document's pages made searchable in the clients.

Full Text Server: A text retrieval server.

G

Group: Groups of users who can be assigned specific tasks and functions.

L

Leap: A feature that lets users "jump" from one location to another, retrieving related documents and information. There are five types of leaps: Application leap, file cabinet leap, highlight leap, SQL leap, and URL leap.

Logon Message: Also known as "Message of the Day". A configurable message that displays to a user or group when they login to the FDD Client or WebFDD.

Lookup Table: A list of suggested index values for use when indexing or searching. A lookup can be assigned to a file cabinet field.

P

Page: A single image or file that is stored in FDD. A page belongs to either a batch or a document.

R

Reason: The purpose for which a state is applied. For example, the legal case for which a document is assigned the "frozen" state.

Redaction Reason Code: A code applied to a redacted area of an FDD document. For example "Limited Access".

Resource Permission: A permission that determines which groups and users can access various FDD system resources. The three main resources in FDD are bins, file cabinets, and workflow tasks.

RMA iQ Properties Server: A web server running the Feith RMA iQ Workplace application.

S

Single Sign-On: When a user logs into their computer and then can login to FDD without typing in their FDD user name and password. This can be done with "externally authenticated" users in a system setup that integrates Active Directory with Kerberos/LDAP authentication.

State: Restricts what actions can be taken on a document. For example, a "frozen" document is on legal hold and cannot be deleted or destroyed.

Super Administrator: A user that has administrative access to all file cabinets and groups, as well as additional privileges that other users cannot do (e.g. setting permissions at the user level).

Supplemental Marking: Restricts access to document according to the markings the document has and the markings the user has. A user must have all markings applied to the document in order to access it.

T

Task Permission: A permission that allows or prohibits groups and users to perform specific tasks (e.g. scan, print, delete a document, change password).

U

User Access Restrictions: Rules that control document access based on user properties, typically through the comparison of user properties to RMA document properties.

V

Virtual File Cabinet: A "virtual" or "view" file cabinet that shows the contents of a standard file cabinet. The virtual file cabinet does not actually contain any of the documents. This feature provides a way to store documents centrally in one file cabinet, while making subsets of those documents available to specific groups and users.

W

WebFDD Server: A web server running the Feith WebFDD application.

Work Item: A document or folder that is being processed through a workflow.

Workflow: A network of tasks that moves an FDD document through a set of defined rules.

Workflow Task: A node in a workflow (e.g., user task, end task).

Index

A

[Administrator Group](#) 29
 Application Leap 105
 Audit Events 35
 Auto-Populated Field Names 226

B

Bins 44

C

Classifications 51

D

[Dashboard iQ Server Entry](#) 138
[Database Authenticated User](#) 174
[Database Roles](#) 28
 Database Statistics 55
[Developer Server Entry](#) 138
 Document Permission Templates 57
[Document Viewer Server Entry](#) 138

E

[EDStor Server Entry](#) 134
 Enable/Disable User Account 194
 Export and Import File Cabinet 83
 Export and Import Group 99
 Export and Import Lookup Table 127
[Externally Authenticated User, MS SQL Server](#) 182
[Externally Authenticated User, Oracle](#) 179

F

FDD Check 62
 Feith Control Panel Login 12
 Field Masks 224
 File Cabinet 65
 File Cabinet Field Options 76
 File Cabinet Leap 107
 Fiscal Year Start Day 152
[Forms iQ Server Entry](#) 138
 Full Text Administrator 87
[Full Text Server Entry](#) 135

G

[Geomap Server Entry](#) 138
 Group Audit Options 101
 Groups 91

H

Highlight Leap 108

I

Import Users From File 195
 Import Users From LDAP 196

L

Leaps 104
 Licensing 113
 Lock Manager 115
 Logon Messages 129
 Lookup Tables 120

M

[Mid-Level Administration](#) 29

P

Password Complexity and Expiration Rules 198
[Permissions, Database](#) 28
[Permissions, Document](#) 26
[Permissions, Resource](#) 25
[Permissions, Task](#) 18
[Proxy Authentication](#) 190, 201

R

Redaction Reason Codes 131
 Regular Expression 224
[Resource Permissions](#) 25
[RMA iQ Properties Server Entry](#) 138

S

Security 17
 Server Entries 133
 SQL Leap 109
 States and Reasons 143
[Super Administrator](#) 29
 Supplemental Markings 147

T

[Task Permissions](#) 18

U

URL Leap 110
 User Access Restrictions 154, 189
[User Audit Options](#) 187
[User Authentication Types](#) 173
[User Clearances](#) 188
 Users 171

V

View Builder 205

Virtual File Cabinets 214

W

[WebFDD Server Entry](#) 138