



Administration and Business Collaboration

User Manual

© Copyright 2007 by Eurekify Ltd., 8 Hasadna Street Raanana 43651, ISRAEL. All Rights Reserved.

This document maybe used in its complete form only and is solely for the use of Eurekify and Eurekify employees and authorized Eurekify channels or customers. The material herein is proprietary to Eurekify and any unauthorized reproduction, either by electronic or other means, use of or disclosure of any part thereof is strictly prohibited. Eurekify reserves the right to make changes to specifications at any time without prior notice. The information furnished in this document by Eurekify is presumed to be accurate and reliable at time of publication, but Eurekify takes no responsibility whatsoever for the consequences of its use.

Information in this manual is subject to change without notice. No part of this publication may be reproduced or distributed in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Eurekify, Ltd.

TRADEMARKS:

Eurekify and Sage are registered trademarks of Eurekify Ltd.

All other products or services referred to in this manual are the trademarks, service marks, or product names of their respective holders.

DISCLAIMER: The products and specifications, configurations, and other technical information regarding the products contained in this manual are subject to change without notice. All the statements, technical information, and recommendations contained in this manual are believed to be accurate and reliable but are presented without warranty of any kind, and users must take full responsibility for the application of any products specified in this manual.

IN NO EVENT SHALL EUREKIFY OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF EUREKIFY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Publication History:

Administration and Business Collaboration	September 2007	User Manual Version 3.2
--	-------------------	----------------------------

Sage Administration and Business Collaboration, Software Version 3.2

Contents

PREFACE	VII
About This Manual	vii
Who Should Use This Manual	vii
Document Conventions	vii
Contact Information	viii
1 – INTRODUCTION	1
2 ADMINISTRATION	3
2.1 Installing Administration and Business Collaboration Modules	3
2.2 Accessing the Administration Module	9
2.3 Managing Connections	11
2.3.1 <i>News and Events URL Pane</i>	12
2.4 Managing Eurekaify Portal Permissions	13
2.4.1 <i>Manage Individual Permissions</i>	14
2.4.1.1 Bootstrapping Sage Permissions	14
2.4.1.2 Setting Access Permissions	16
2.4.2 <i>Working with the Access Permissions Tree</i>	18
2.4.2.1 Using the Access Permissions Filter	19
2.4.2.2 Global Filters	20
2.4.3 <i>Manage Multiple User Permissions</i>	22
2.5 Manage Member Lists	23
2.5.1.1 Adding Users to the User List	24
2.6 Managing Campaigns	26
2.6.1 <i>Working with Campaigns</i>	26
2.6.1.1 Campaign Parameters	27
2.6.1.2 Adding a New Campaign	28
2.6.1.3 Changing Campaign Definitions	29
2.6.1.4 Remove Existing Campaigns	29
2.6.1.5 Start a Campaign	30
2.6.1.6 Stop a Campaign	31
2.6.1.7 Review Campaign Progress Status	32
2.6.1.8 Administrative Delegation	33
2.6.1.9 Send Campaign Emails	34
2.6.1.10 Manage Email Templates	35
2.7 Set Workform Defaults	37
2.8 Self Service Settings	39
2.9 Manage Mail Server	40
3 BUSINESS COLLABORATION	41
3.1 Accessing the Business Collaboration Module	41
3.2 Workform Structure	43
3.2.1 <i>Workform Settings Tab</i>	44
3.2.2 <i>Workform Main Tab</i>	45
3.2.2.1 Workform Operational Area	45
3.2.2.2 Drilling Down for Record Details	47
3.2.2.3 Approving Workform Changes	48
3.3 User Management	51
3.3.1 <i>Request a New User Definition</i>	51
3.3.2 <i>Request Changes to a User Definition</i>	53
3.3.3 <i>Request Removal of a User Definition</i>	54
3.3.4 <i>Request Role Privileges for My Team</i>	55
3.3.5 <i>Request Resource Privileges for My Team</i>	57
3.3.6 <i>Request Role Privileges for Myself</i>	58

- 3.3.7 *Request Resource Privileges for Myself*..... 60
- 3.3.8 *User Privileges Certification Workform*..... 62
- 3.3.8.1 *Operation Area Data*..... 64
- 3.4 *Role Management*..... 68
 - 3.4.1 *Request a New Role Definition*..... 68
 - 3.4.2 *Request Changes to a Role Definition*..... 70
 - 3.4.3 *Request Removal of a Role Definition*..... 71
 - 3.4.4 *Role Definitions Certification/Attestation* 72
- 3.5 *Resource Approval* 80
 - 3.5.1 *Request a New Resource Definition* 80
 - 3.5.2 *Request Changes to a Resource Definition* 82
 - 3.5.3 *Request Removal of a Resource Definition* 83
 - 3.5.4 *Resource Access Certification/Attestation*..... 85
- 3.6 *Privileges Navigation and Browsing* 90
 - 3.6.1 *Navigate a Hierarchy to Browse* 90
 - 3.6.2 *Browse User Privileges* 92
 - 3.6.3 *Browse Role Privileges* 92
 - 3.6.4 *Browse Resource Privileges* 93

List of Figures

FIGURE 1 SAGE PORTAL HOME PAGE	9
FIGURE 2 SAGE ADMINISTRATION WINDOW	10
FIGURE 3 SAGE CONNECTION ADMINISTRATION WINDOW	11
FIGURE 4 SAGE CONNECTION ADMINISTRATION WINDOW	12
FIGURE 5 MANAGE EUREKIFY PORTAL PERMISSIONS WINDOW.....	13
FIGURE 6 SAGE ERM PERMISSION ACCESS TREE.....	18
FIGURE 7 GLOBAL FILTERS ADMINISTRATION WINDOW	20
FIGURE 8 MANAGE MEMBER LISTS WINDOW.....	23
FIGURE 9 START CAMPAIGN WINDOW.....	30
FIGURE 10 SEND CAMPAIGN EMAILS WINDOW	31
FIGURE 11 STOP CAMPAIGNS WINDOW	31
FIGURE 12 REVIEW CAMPAIGN PROGRESS STATUS WINDOW	32
FIGURE 13 ADMINISTRATIVE DELEGATION WINDOW	33
FIGURE 14 SET WORKFORM DEFAULTS WINDOW	37
FIGURE 15 SAGE PORTAL HOME PAGE	41
FIGURE 16 BUSINESS COLLABORATION ICON	42
FIGURE 17 LIST OF WORKFORMS.....	42
FIGURE 18 USER CERTIFICATION SETTINGS TAB	43
FIGURE 19 WORKFORM SHOWING SELECTION AND OPERATIONAL AREAS	43
FIGURE 20 WORKFORM SETTINGS TAB	44
FIGURE 21 MAIN TAB	45
FIGURE 22 OPERATIONAL AREA	46
FIGURE 23 RECORD SHOWING FIRST LEVEL DRILL DOWN	47
FIGURE 24 WORKFORM DETAILS DISPLAYED IN TABULAR FORM.....	48
FIGURE 25 WORKFORM SHOWING SELECTIONS IN THE OPERATIONAL AREA.....	49
FIGURE 26 OPERATIONAL AREA SHOWING REMOVE CHECKBOXES	49
FIGURE 27 ROLE IDENTIFIED FOR REMOVAL	50
FIGURE 28 OPERATIONAL AREA SHOWING REASON FOR REMOVAL	50
FIGURE 29 USER PRIVILEGES CERTIFICATION WORKFORM-POPULATED	62
FIGURE 30 ROLE APPROVAL WORKFORM.....	73
FIGURE 31 RESOURCE APPROVAL WORKFORM	85

Preface

About This Manual

This manual describes operations and options that are unique to the Sage DNA Data Management module. This specifically treats the operations performed from within the Import, Export and Management menus. In the Management menu the unique options include the Enrich Users DB and Enrich Resources DB options. All other operations that can be performed from within the Sage DNA Data Management module are common to the Sage DNA module and are described in the Sage DNA manual.

Chapter 1 provides an overview of the Sage items treated in the manual.

Chapter 2 provides details of how you can set up and manage Sage Access Permissions for an organizations individual users and user groups.

Chapter 3 Covers details on how business and line managers use the collection of Workforms to review and certify change requests, privileges and policies assigned to members of their teams and organizational units.

Who Should Use This Manual

This manual is intended for Role Engineers who are responsible for the installation of Sage software, downloading and uploading of users and resources databases, role discovery and audit operations. Role Engineers are typically well-trained professionals who are familiar with the target organization. This manual assumes that the Role Engineer has had professional training on a Sage system and is familiar with the Sage documentation that accompanied the Sage installation package.

Familiarity with the Microsoft operating system and applications and relevant peripheral and remote equipment is also assumed.

Document Conventions

To facilitate working with this user manual, Eurekify has adapted the following symbols in the body of the manual to focus on issues of special importance. The user should pay careful attention to sections that contain the following conventions:



Important information. Read carefully.



Recommended activity.

Contact Information

Should there be any questions regarding Eurekify products, please either contact us directly or contact our local distributors.

Headquarters:

Eurekify, Ltd.

8 Hasadna Street

Raanana 43651, Israel

Telephone: +972-9-746-7346

Facsimile: +972-9-746-7347

Email: info@eurekify.com

Web: www.eurekify.com

1 – Introduction

This manual provides a review and instruction of how to use the Administration and Business Collaboration modules that are available from the Sage Portal.

The Sage Administration module provides you with an easy to use environment for setting up and managing Sage access permissions for an organizations individual users and user groups.

The Sage Business Collaboration module contains a collection of Workforms that business and line managers use to review and certify change requests, privileges and policies assigned to members of their teams and organizational units. The Business Collaboration module provides an easily accessible environment for managerial and IT personnel to share such information and to ensure they meet organization based and government driven compliance regulations.

2 Administration

The Sage Administration module provides you with an easy to use environment for setting up and managing Sage access permissions for an organizations individual users and user groups.

2.1 Installing Administration and Business Collaboration Modules

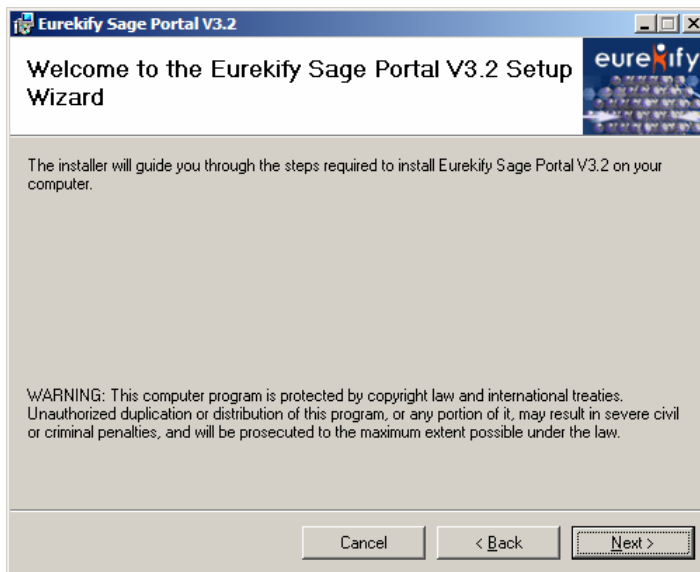
You install the Administration and Business Collaboration modules as part of the Sage Portal.

To install the Sage Portal:

1. From the Installation CD find and run *EurekifySageERM-PortalServer-V32.msi* to run the Sage Portal installation wizard.. The Splash Screen appears. Click *Next* to advance to the next step.



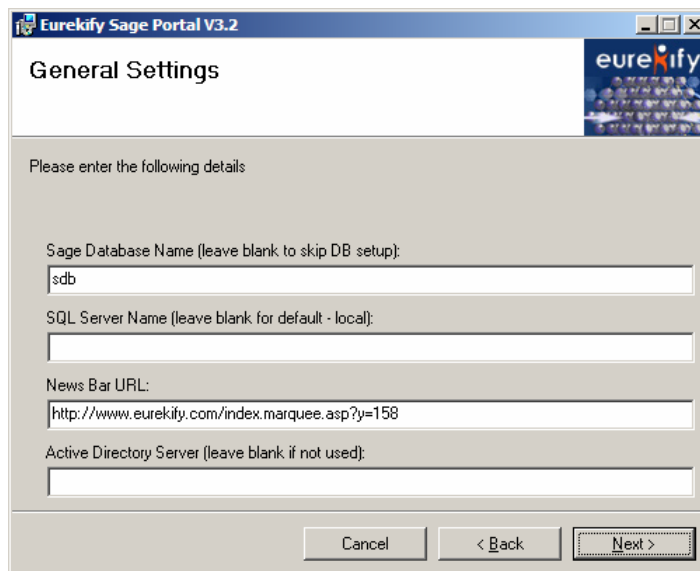
2. The Sage Portal *Welcome* screen appears. Click *Next* to advance to the next step.



- The *License Agreement* appears. Read the agreement carefully and the click *I Agree* to confirm you have read the agreement. Click *Next* to advance to the next step.



- The *General Settings* step appears.

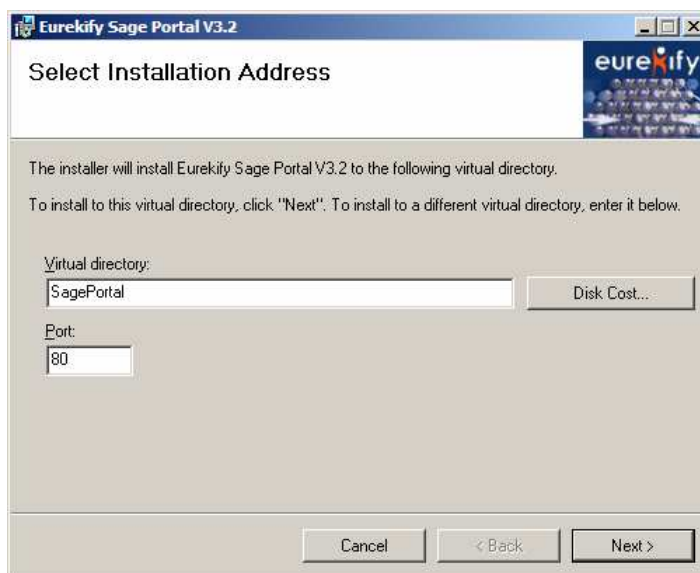


- If you are connecting to a specific SQL Server Machine then enter the address for the SQL Server in the SQL Server Name field. Otherwise leave the field empty.
- If you are connecting to an Active Directory Server then enter the name of the server in the Active Directory Server field. Otherwise leave the field empty.

7. Click *Next* to advance to the *Identification Method* step.

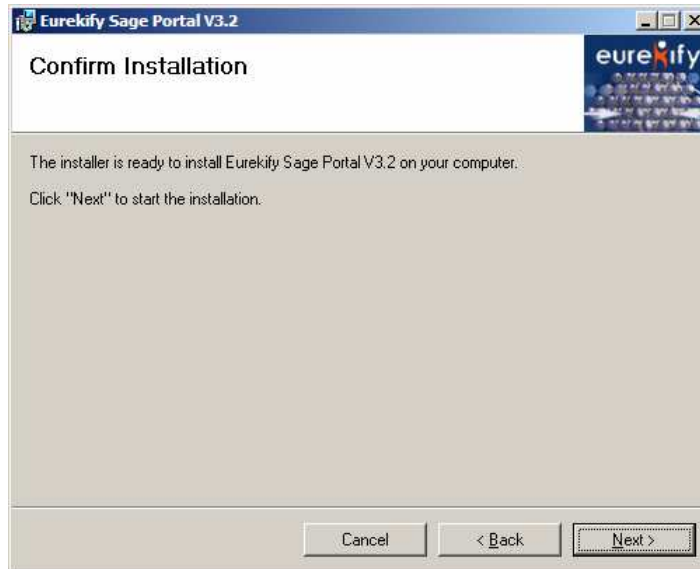


8. Choose *Use Impersonation* if you want SagePortal to use the logged in user when connecting to the *SQL Server, Reports Server and AD Server*.
9. Choose the *Use the ASPNET/Network Service Account* option if you want the IIS account (ASPNET or Network Service Account) to be used instead. In either case, the respective account should have the proper privileges on servers.
10. Click *Next* to advance to the *Select Installation Address* step.

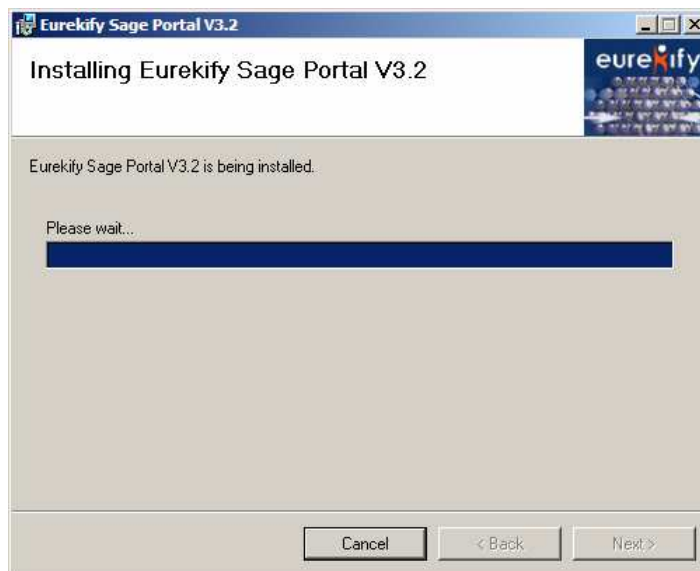


11. In the *Virtual directory* text field enter the name of the web site used for Sage Portal (e.g. `http://localhost/SagePortal`).

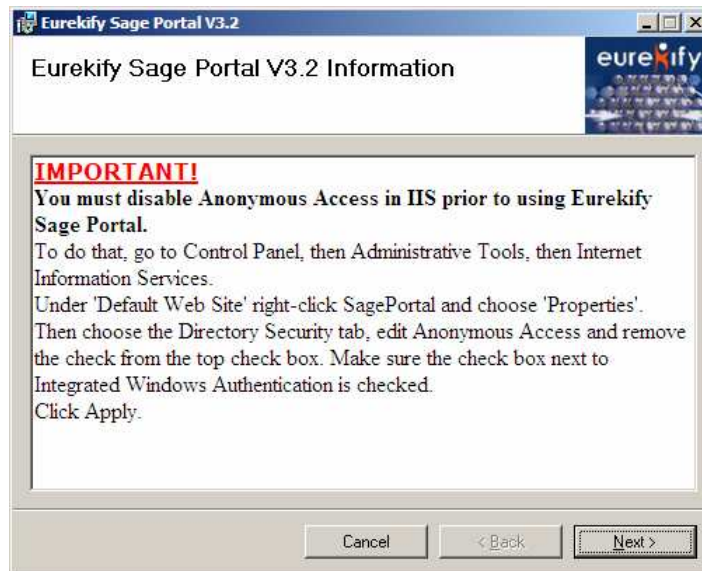
12. Click *Next* and the *Confirm Installation* step appears.



13. Click *Next* to install the Portal using the selected parameters. The progress bar appears while the installation is taking place.

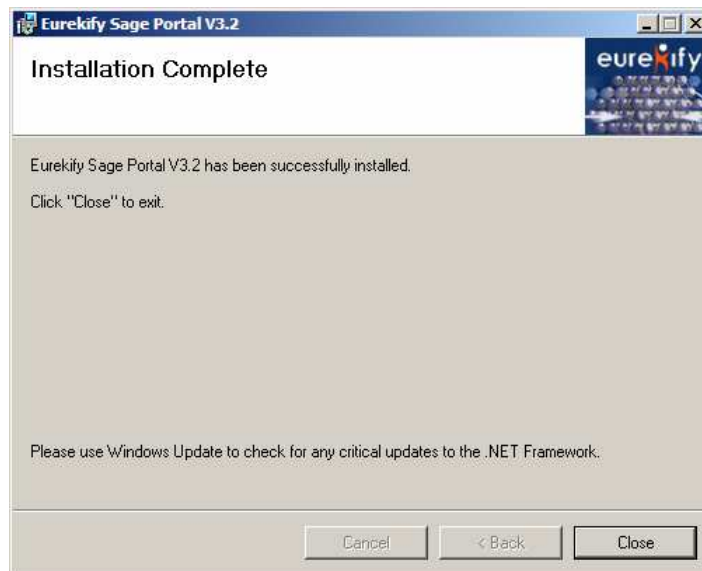


14. The *Sage Portal Information* step appears.



15. Read the notice and comply with any procedures as required.

16. Click *Next*, the *Installation Complete* step appears.



17. Click *Close*, to exit the installation wizard.

2.2 Accessing the Administration Module

You access the Administration module from the Sage Portal via your browser

To access the Administration module:

18. Run your browser.
19. In the *Address* text field type <http://localhost/sageportal> and type Enter on the keyboard. The Sage Portal Home Page opens. The page displays icons and menu bars for connecting to various work modules.

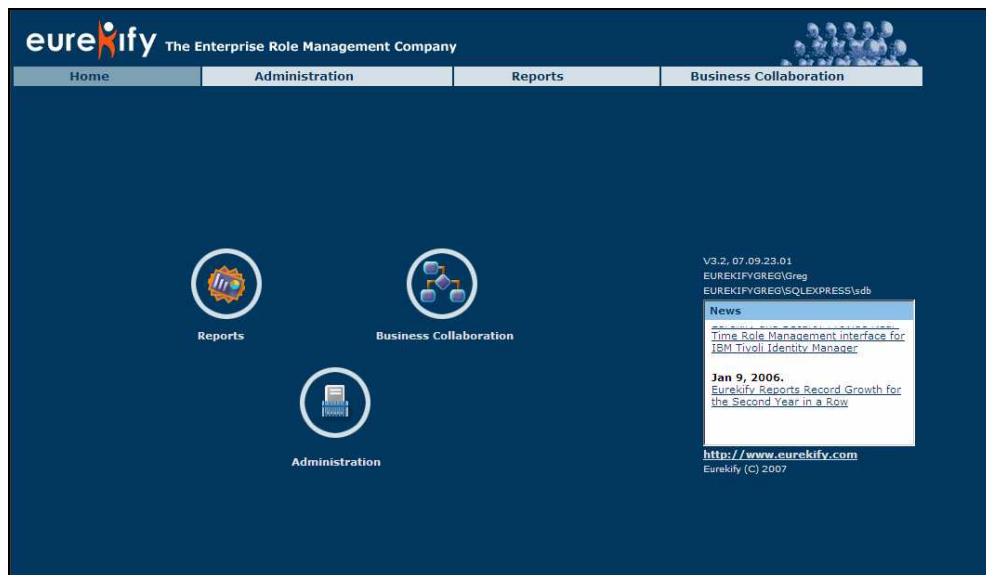


Figure 1 Sage Portal Home Page

Portal and database information is displayed directly above the News and Events area. The information includes:

- Sage Portal version number
- Current User connect to the portal
- The name of the database to which the portal is connected

20. Click the *Administration* icon. The Sage Administration module opens and displays links to each of the Administration subunits:

- Manage Connections
- Manage Eurekify Portal Permissions
- Manage Member Lists
- Managing Campaigns
- Set Workform Defaults
- Self Service Settings
- Manage Mail Server



Figure 2 Sage Administration Window

2.3 Managing Connections

After installing Sage ERM and its components on your system one of the first things you need to do is define the connection details between Sage ERM and the SQL Server and Database. You do this from the Manage Connections window.

To access the Manage Connections window:

1. From the *Sage Portal* home page click the *Administration* icon. The Administration module opens.
2. From the *Administration* module click the *Manage Connection* link. The *Manage Connections* window opens.

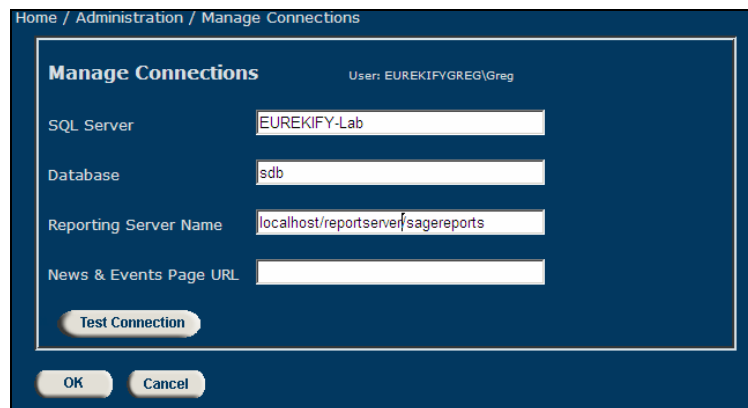


Figure 3 Sage Connection Administration Window

To set the Connection Parameters:

1. In the *SQL Server* text field type the name of the server machine that functions as the SQL Server.
2. In the *Database* text field type the name of the database that will house the Sage data that you generate and save.
3. In the *Reporting Serve Name* text field type the name of the server and path to the location of the Microsoft Reporting Services.
4. Click the *Test Connection* button to verify that a connection between the Sage ERM, SQL Server and Database is established. When a connection is established the Eurekify Sage Database number and Version release number are displayed.

If a connection was not established check:

- The accuracy of the details that you entered.
 - That the *Anonymous Access* parameter for IIS is disabled.
5. Click *OK* to save the connection details, exit the *Manage Connection* window and return to the Sage Administration module.

2.3.1 News and Events URL Pane

The Sage Portal home page contains a pane designed to display company news and announcements. By default the pane displays Eurekify announcements. The content is easily modified by setting the address for the URL that contains information that you want to display.

To customize the contents of the News and Events URL Pane:

1. From the *Administration* module click the *Manage Connection* link. The *Manage Connections* window opens.

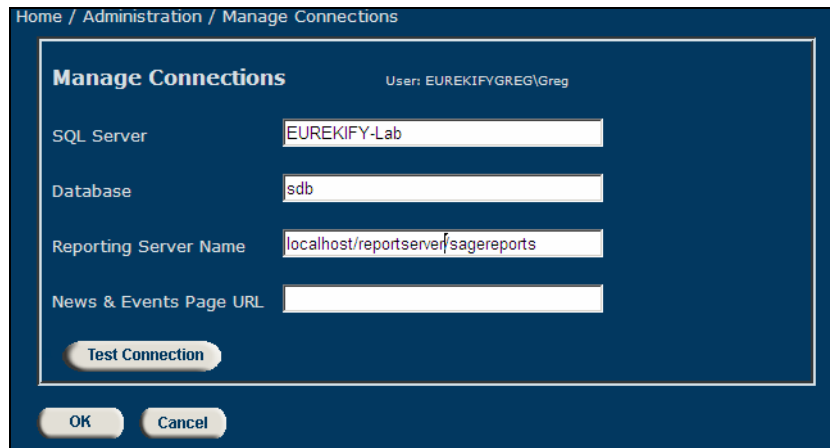


Figure 4 Sage Connection Administration Window

2. In the *News & Events Page URL* text field enter the URL address for the page containing your company's news and events ticker.
3. Click the *Test Connection* button to verify that you are connected.
4. Click the *OK* button to exit the window and return to the Sage Administration module.

2.4 Managing Eurekify Portal Permissions

Different members of your organization will be involved at different levels in the Role engineering and certification process. Their level of involvement in the process is reflected in their varying needs to view and manipulate data that is available from within the Sage ERM Portal. Sage ERM provides you with the capability to set and manage user access permissions for various data in the Sage ERM portal, based on individual users and members of specific divisions or workgroups in your organization. In this way you can set Sage Permissions to match the type of operations that any individual performs, and match the type of data that they require in order to perform such operations.

The *Manage Eurekify Portal Permissions* window provides you access to either:

- Manage Individual Permissions
- Manage Multiple- User Permissions
- Manage Business Managers Permissions.

All permissions pages are arranged in a similar manner. The upper section of the window contains fields for selecting the members of your organization to which the access permissions apply. This is called the Selection area. The fields that appear in the selection area vary according to whether the access permissions are being set for individuals, multiple-users, or business managers.

The lower section of the window contains fields for assigning the type of information to make available for viewing and for use by the members of your organization. This lower section of the window is called the Operation area.

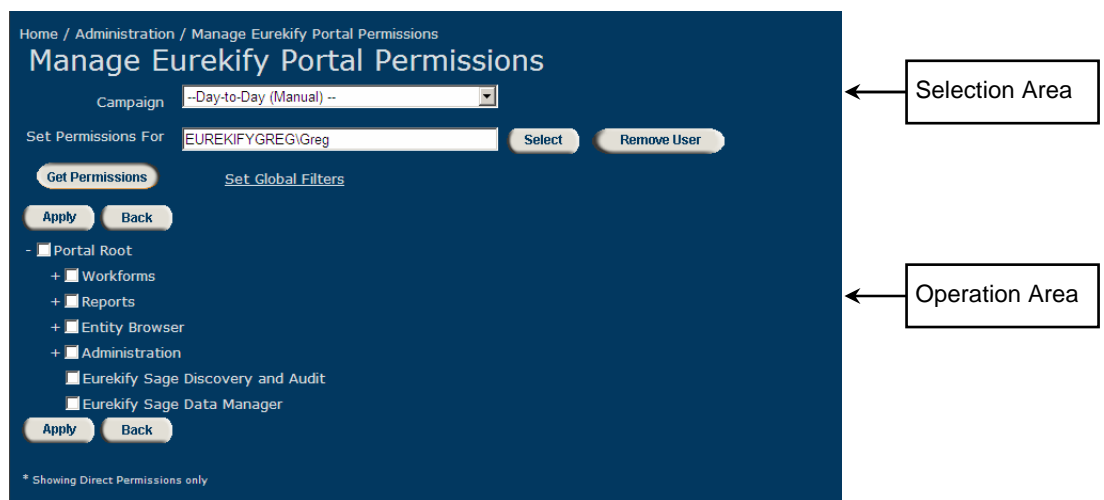


Figure 5 Manage Eurekify Portal Permissions Window

2.4.1 Manage Individual Permissions

You use the Sage permissions for individual users to allocate access permission to either individual members of your organization or a recognized group within your organization. When providing access to a group then each member of the group receives an identical set of permissions. Sometimes you may want to provide permissions to individuals who have already been treated as part of a group. In such cases the individual receives the set of all permissions granted as an individual in addition to those granted as part of the group.

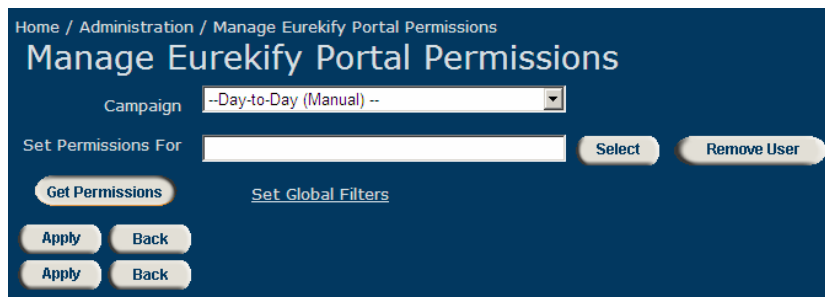
2.4.1.1 Bootstrapping Sage Permissions

Bootstrapping the system is performed by a system administrator on entering the *Manage Eurekify Portal Permissions* window for the very first time. This is a one-time only operation that is performed when selecting a User Name and setting Access Permissions for the first time. By bootstrapping the Eurekify Portal Permissions initial system access is generated for the administrator. The administrator can then add users and set permissions for those users.

To Bootstrap Sage Permissions:

1. From the *Administration* module click the *Manage Eurekify Portal Permissions* link. The *Manage Eurekify Portal Permissions* window opens and displays the Selection Area options.

The *Campaign* field is automatically populated with the *Day to Day (Manual)* option. The *Set Permissions For* field is blank.



Home / Administration / Manage Eurekify Portal Permissions

Manage Eurekify Portal Permissions

Campaign: --Day-to-Day (Manual) --

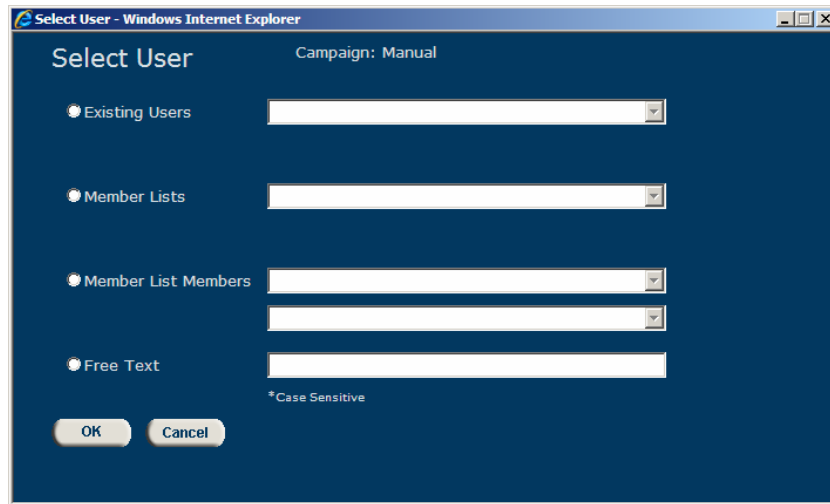
Set Permissions For: Select Remove User

Get Permissions [Set Global Filters](#)

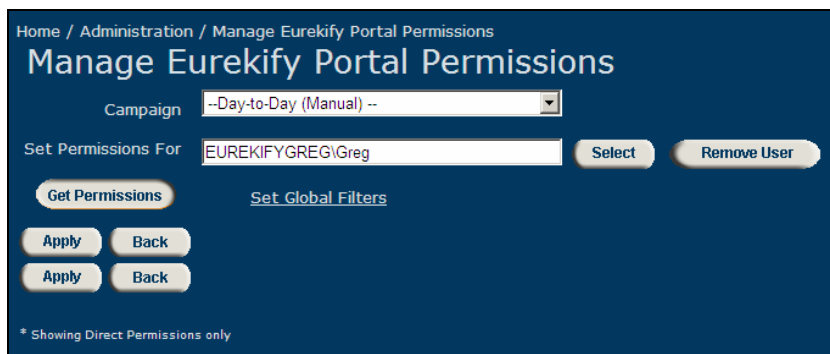
Apply Back

Apply Back

- Click the *Select User* button next to the *Set Permissions For* field. The *Select User* window opens.

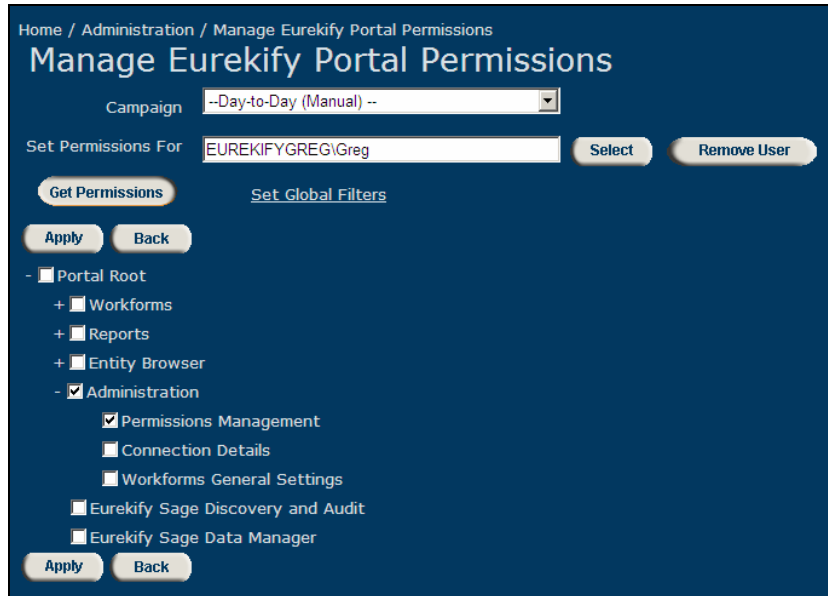


- Select the *Existing Users* option. The adjacent drop down list is automatically populated with your system login details. This takes the form of the *<Domain Name>\<User Name>*. For example *Eurekify-LAB\Admin*.
- Select the administrators' User name from the drop down list.
- Click OK. The *User Name* now appears in the *Set Permissions For* field.



- Click the *Get Permissions* button. A list of initial permissions is displayed in the Operation Area.

- Click the + symbol next to the permissions tree to expand the tree structure and reveal the *Administration* group. Select the *Permissions Management* check box if it is not already selected. This is the only Permission that is granted. All other access permission check boxes should be cleared.

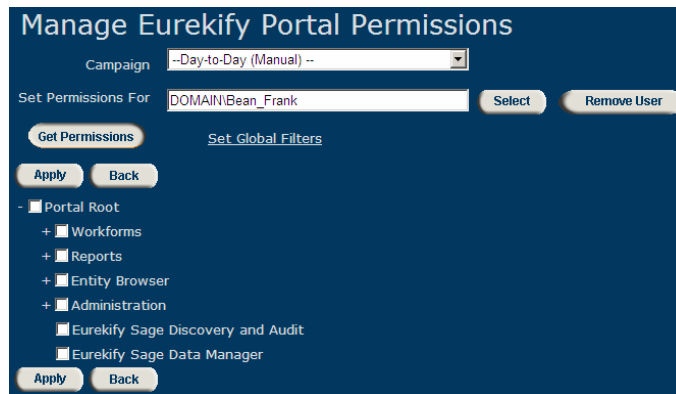


- Click the *Apply* button to add Permissions to the *User*.
- Click the *Back* button to return to the *Manage Eurekify Portal Permissions* window.

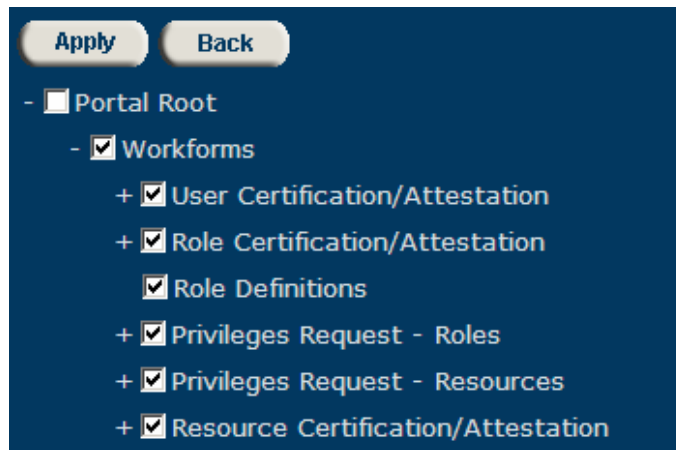
2.4.1.2 Setting Access Permissions

To Set Access Permissions for Individuals:

- From the *Administration* module click the *Manage Eurekify Portal Permissions* link. The *Manage Eurekify Portal Permissions* window opens.
- Click the *Select* button next to the *Set Permissions For* edit field. The *Select User* window opens.
- Select either the *Existing Users* or the *Member List Members* option.
- Select a member of your organization from the User drop down list and then click the OK button. You are returned to the *Manage Eurekify Portal Permissions* page.
- Click the *Get Permissions* button. The most recently saved set of permissions for the selected user are displayed in the Operation Area. For a new user the permissions check boxes are all cleared.



6. Click the + symbol next to the permissions tree items to expand the tree structure and reveal the Permissions Categories and items.
7. Select the check boxes next to the Sage entities for which the User should receive access permission.



8. Click the *Apply* button to save the selections in the database.

2.4.2 Working with the Access Permissions Tree

The Access Permissions tree appears in the operation area of the Manage Eurekify Portal Permissions window and is used to assign the set of Access Permissions available to the users selected in the Selection Area of the window. This section describes how to manipulate and work with the Access Permissions tree.

The Access Permissions tree is a hierarchically arranged tree that represents the Sage ERM entities and sub entities. Each entity throughout the tree is accompanied by a check box which is used to indicate whether permission to access that level of Sage ERM is granted or not. A selected check box indicates that permission to access that Sage ERM entity is granted. A cleared check box indicates that permission to access that Sage ERM entity is refused.

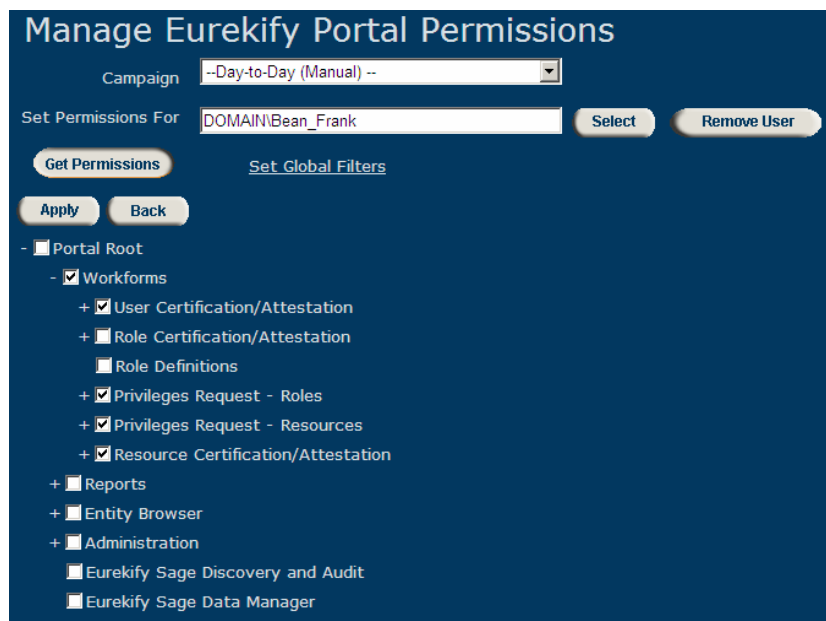


Figure 6 Sage ERM Permission Access Tree

Figure 6 illustrates this showing that permission to access all workforms is granted except for the Role Certification/Attestation and Role Definitions workforms.

Selecting a specific level in the Access Permissions tree that contains subordinate levels automatically selects all subordinate levels. So as in Figure 6, permission to access the User Certification/Attestation Work form and all its subordinate entities is granted.

2.4.2.1 Using the Access Permissions Filter

You can filter the access permissions so that within a given entity only specific data that matches the filter settings is available for use by the selected users.

To use an Access Permission Filter

1. Successively navigate to deeper levels within the Access Permissions tree until you reach a level that displays a check box for a filter.
2. Set the filter by entering the name of the Category and the Value for the category to which you want to provide access. For example *UserName* and *Alex Patrick* respectively.
3. Click the Add button to submit and save the filter details in the database. The filter parameters are saved in the system but they are not displayed until the Permissions Tree is updated.

Enter the Category and Value to be used by the filter

4. Click *Get Permissions* to update the screen and navigate to the level that for which you set the filter. The filter Category and Value are now listed as an *Extra* filter in the *Permissions Tree*.

2.4.2.2 Global Filters

Global filters are a means of providing access to data for any entity that matches the filter settings throughout the entire access permissions tree. This reduces the need to repetitively set the same filter for multiple entities throughout the access permissions tree.

Category	Value	
UserName	*	<input type="checkbox"/>
Country	US	<input type="checkbox"/>
OrganizationType	Corporate	<input type="checkbox"/>

Figure 7 Global Filters Administration Window

The window into left and right regions: the left region contains the selection fields for defining the filter; the right region lists the global filters.

To Set Global Filters:

1. From the *Administration* module click the *Manage Eurekify Portal Permissions* link. The *Manage Eurekify Portal Permissions* window opens.
2. Select a Campaign from the Campaign drop down list.
3. Click the *Select* button next to the *Set Permissions For* edit field. The *Select User* window opens.
4. Select a User and click OK. You have set the campaign and selected the user to assign global filters to.
5. Click the *Set Global Filters* link that is next to the *Get Permissions* button. The *Global Filters Administration* window opens. Figure 7 shows how the Global Filters Administration window appears after several Global Filters are added to the Filter List. Table 1 Global Filter Parameters and Descriptions.
6. Select the Entity Filter type from the Filter Entity options.
7. Select the Configuration from the Configuration drop down list.
8. Select the Category and Value parameters from their respective drop down lists.
9. Click the Add Filter button to move the filter components to the Global Filter list.

Table 1 Global Filter Parameters and Descriptions

Parameter	Description
Filter Entity	Sets the Entity type, User, Role, or Resource, on which the selected filters operate.
Configuration	Select the Configuration for which you want to set global filters.
Category	Select a Category to include it in the filter. Choose the <i>All Values (*)</i> item from the drop down list to provide access to all the categories in the configuration.
Value	Select a Value from the Value drop down list to include the value in the filter. If All Values (*) is selected from the Category list box, then All Values(*) is automatically selected for the Value list box.
Add Filter	Click the Add Filter button to list the selected Category/Value filter pair to the Filter list.
New Value	New Values represent items that do not currently appear in the configuration but that you want to be used as filters as soon as they are added to the configuration. Enter the Name of an item that you want to include as a part of a filter.
Add to Categories	Adds the New Value as an entry in the Category drop down list.
Add to Values	Adds the New Value as an entry in the Value drop down list.
Enforce Global Filters	Imposes the listed Global filters on the workforms wherever they are relevant and at the same time override all existing Extra filters.
Done	Imposes the listed Global filters on the workforms wherever they are relevant without affecting the status of any Extra filters that exist.

2.4.3 Manage Multiple User Permissions

You can assign Access Permissions to a group of users that do not necessarily belong to a recognized division or group within your organization. This may reflect itself by selecting members of your organization that have similar positions but that are located in disjointed business divisions.

You will need to create a permissions file that lists the user name for each member of the organization that you will include in the multiple user group and then use the file to create a Members List.

To assign access permissions to multiple-users

1. From the *Administration* module click the *Manage Eurekify Portal Permissions* link. The *Manage Eurekify Portal Permissions* window opens.
2. Click *Select* next to the *Set Permissions For* edit field. The *Select User* window opens.
3. Select the *Member Lists* option and then select a member list from the Member List drop down list. Click *OK* and you return to the *Manage Eurekify Portal Permissions* window. The Member List name now appears in the *Set Permissions For* edit field.
4. Click the *Get Permissions* button to open the Access Permissions tree.
5. Set permissions and save the permissions as described working with access permissions. See section 2.4.2, Working with the Access Permissions Tree.

2.5 Manage Member Lists

You use the Manage Member Lists window to:

- Create member lists
- Add members to a list
- Map attributes to list fields.

Member lists contain lists of Users and user associated attributes. You can use Member lists as the input for Campaigns and for setting Portal Permission. You create member lists by importing Member Files that are formatted as CSV text files and that contain user attributes. The attributes commonly included in the member files include: Login, Name, Email, Category and Category Value. When opening a Member File Sage ERM refers to the first row as a header row and identifies the values in the first row as parameters for list mapping.

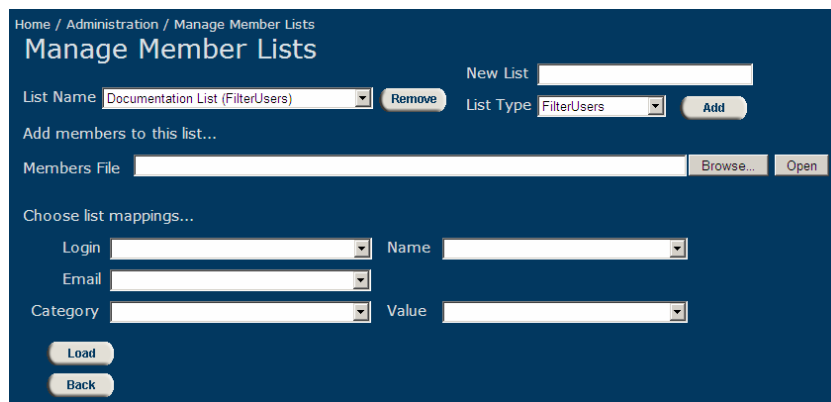


Figure 8 Manage Member Lists window

To create and map member lists:

1. From the *Administration* module click *Manage Member Lists*. The *Manage Member Lists* window opens.
2. Enter the name of the List in the New List text field.
3. Select a Filter option from the List Type drop down list.
4. Click the Add button next to the List Type drop down list. The name is displayed in the List Name text field.

To add Users to a Members List and select the List Mapping

1. Select a List from the *List Name* drop down list.

2. Click the *Browse* button next to the *Members File* text field to locate and select the CSV formatted file that contains the Member list data.
3. Click the *Open* button next to the *Members File* text field. The Member File's path and file now appear in the *Members File* text field and the *List Mapping* fields display the first value taken from the Members File.
4. Each List Mapping drop down list contains the Header names for each column in the Member File. For each *List Mapping* field select the column that contains the data that you want to associate with the *Login*, *Name*, *Email*, *Category* and *Value* attributes.
5. Click the *Load* button and Sage ERM reads and records the mapped data from the Members File. When Sage finishes loading the mapped data, the number of rows that were successfully read and those that failed to be read is listed next to the Load button.
6. Click the *Back* button to return to the *Administration* window.

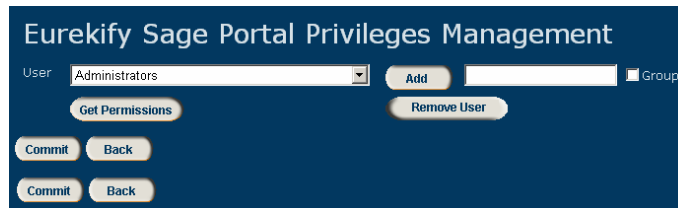
2.5.1.1 Adding Users to the User List

You can add either an individual user or a group of users to the User list. The format for entering the User and Group names is as follows.

Entry Type	Format
User	<Domain Name>\<User Name>
Group	<Domain Name>\<Active Directory Group Name>

To Add Users or Groups to the User List

1. From the *Administration* module click the *Manage Sage Permissions* link. The *Sage Permissions* window opens.
2. Click the *Manage Individual Permissions* link. The *Manage Individual Permissions* window opens and displays the Selection Area options.



Eurekify Sage Portal Privileges Management

User: Administrators Add Group

Get Permissions Remove User

Commit Back

Commit Back

3. Type the *User* or *Group Name* in the *Add* text field. When entering a *Group Name* select the *Group* check box.
4. Click the *Add* button. The *User Name* is added to the *User* drop down list.

2.6 Managing Campaigns

Campaigns allow you to include a group of the organization's users in the business collaboration process that provides department managers and business line managers with the capability to certify and approve the access privileges for their employees.

This includes:

- Defining the participating users
- Defining the participant's access rights to specific business collaboration processes from within the Sage Portal.
- Notifying the participating users via email
- Allowing participants to individually request changes and approve the access rights of the employees functioning in their business units.
- Allowing individuals to request changes to access rights.
- Tracking the progress of participating users in their respective Business Collaboration process.
- Sending automated reminders to managers and individuals participating in their respective Business Collaboration process.
- Retrieve user requests that were made and implement such requests.

2.6.1 Working with Campaigns

To access and set campaign parameters:

1. From the *Administration* module click the *Manage Campaigns* link. The *Manage Campaigns* window opens and displays a series of links to perform specific campaign operations. These include:
 - Adding a New Campaign
 - Changing Campaign Definitions
 - Remove Existing Campaigns
 - Start Campaigns
 - Stop Campaigns
 - Review Campaign Progress Status
 - Send Campaign Emails
 - Administrative Delegation
 - Manage Email Templates

2. Select a link that matches the operation that you want to perform. The appropriate Campaign page opens.
3. Make selections in the Selection Area to define the Campaign and select the appropriate Permissions file.
4. Click the + symbol next to the permissions tree items to expand the tree structure and reveal the Permissions Categories and items.
5. Select the check boxes next to the Sage entities for which the Users should receive access permission.
6. Click the OK button to save the selections in the database.
7. Click the *Back* button to return to the *Sage Permissions* window.

2.6.1.1 Campaign Parameters

When you create or modify campaigns you must set or alter parameters that define the campaign. Table 2 lists the parameters used to define a campaign and provides a description of each parameter.

Table 2 Campaign Parameters

Parameter	Description
Campaign	The campaign name.
Status	A campaign can have one of 3 statuses that each indicates the activity level of the campaign. These are: <i>New</i> Recently created and not yet started. <i>Active</i> The campaign is started and in process. A campaign is active when it is started manually or reaches the pre-set start date. <i>Stopped</i> The campaign was either manually stopped or exceeded the pre-set expiration date. The campaign is not active.
Owner	The name of the user that created the campaign.
Create Date	The date on which the campaign was created.
Start Date	The date from which users with access rights to the campaign can participate in or interact with the campaign.
Expiration Date	The date on which users with access rights to the campaign can no longer participate in or interact with the campaign.
Type	Indicates the type of workform that the campaign is based on.
Member List	A CSV list that includes the group of users that have rights to participate in the campaign.
Configuration	The name of the configuration containing the Sage ERM entities on which the campaign is performed.
AuditCard	The name of the Sage ERM AuditCard used in the campaign. Use an AuditCard in a campaign to restrict the access rights to those that are identified by the AuditCard as being problematic.
Category	Indicates that category in the configuration that forms that subject of the campaign.

2.6.1.2 Adding a New Campaign

To add a new campaign:

1. From the *Administration* module click the *Manage Campaigns* link. The *Manage Campaigns* window opens.
2. In the *Campaign* edit field enter the name of the new campaign.
3. The parameter for the *Status* drop down list is automatically set to *New*.
4. The current user is listed as the campaign *Owner* and the *Create Date* and *Time* are listed below the *Status* edit field.
5. Enter the date for the campaign to begin in the *Start Date* edit field. By default the Creation date is listed as the Start Date. To change the Start Date, click the *Set* link next to the edit field to open a calendar and select a new start date.
6. Enter the date on which you want to end the campaign in the *Expiration* date edit field. By default the expiration date is automatically set to seven days later than the campaign creation date. To change the Expiration date, click the *Set* link next to the edit field to open a calendar and select a new date.
7. From the *Type* drop down list select the work form type for the campaign.
8. From the *Member List* drop down list select the *Member List* to be included in the campaign. You can set parameters to define the contents of an Auto-Generated member list. To do so click the *Settings for Auto Generated Lists* located under the *Member List* drop down list.
9. Select a *Configuration* for the campaign from the *Configuration* drop down list.
10. Select an *AuditCard* for the campaign from the *AuditCard* drop down list. To disregard the use of AuditCards in the campaign, choose the *None* item from the list. If you choose an AuditCard then the *Filter by AuditCard* check box is displayed.
11. Select the *Filter by AuditCard* check box to limit the review to only those access rights identified as problematic in the selected AuditCard.
12. From the *Category* drop down list select the configuration category to be the subject of the campaign.
13. Click the *OK* button. If a campaign parameter is missing a warning is displayed next to the field that needs to be treated. Supply the missing information and then click *OK*. On successfully adding a campaign a notice is displayed and you have the option of allowing campaign members to view requests from previous campaigns.
14. Click the *OK* button to complete the process and return to the Campaigns window.

2.6.1.3 Changing Campaign Definitions

Prior to activating and starting a campaign you can change a number of parameters. These include;

- Campaign Status
- Description
- Start Date
- Stop Date

This gives some flexibility when scheduling and implementing the campaign.

To change Campaign Definitions:

1. From the *Administration* module click the *Manage Campaigns* link.
2. In the *Campaigns* window click the *Change Campaign Definitions* link. The Change Campaign Definitions window opens.
3. Modify the Status, Description, Start date and Stop date parameters as required.
4. Click *OK*. The changes are saved and you can cancel out of the window to return to the Campaigns window.

2.6.1.4 Remove Existing Campaigns

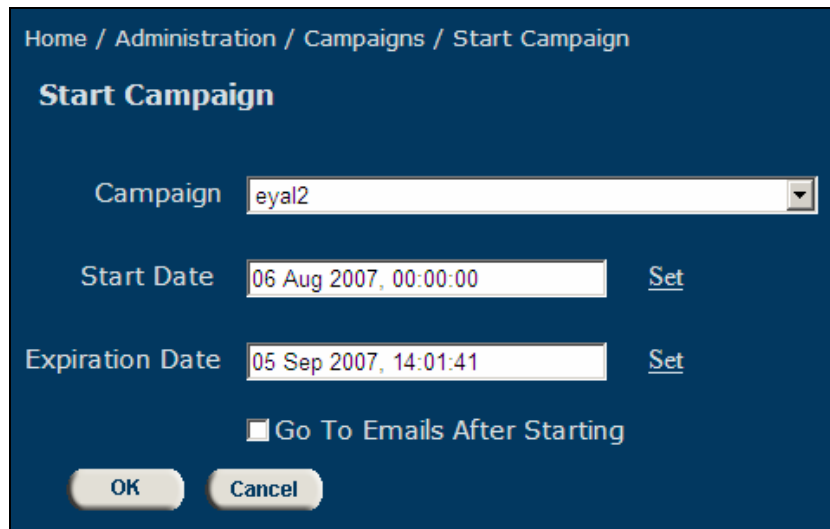
When a campaign is either over or is of no further use you can remove it from the database.

To remove and existing campaign:

1. From the *Administration* module click the *Manage Campaigns* link.
2. In the *Campaigns* window click the *Remove Existing Campaign* link. The Remove Existing Campaign window opens.
3. From the *Campaign* drop down list select the campaign to remove.
4. Select the *Remove Associated Member List* check box to remove the campaign's member list along with the campaign. Clear the check box to maintain the member list for later use.
5. Select the *Remove Associated Certification Requests* check box to remove the campaign's certification requests along with the campaign. Clear the check box to maintain the certification requests for later use.
6. Click *OK* to confirm the changes. A confirmation message is displayed to verify that you intend to remove the campaign. Click *Yes* to remove the campaign or *No* to discard your changes.

2.6.1.5 Start a Campaign

You can use the *Start Campaign* link either to redefine a campaign's Start and Expiration dates to better suit your work schedule, or to restart a campaign after it was manually stopped. You start a campaign by resetting the *Start Date* in the *Start Campaign* window.



The screenshot shows a window titled "Start Campaign" with a breadcrumb path "Home / Administration / Campaigns / Start Campaign". The window contains the following elements:

- A "Campaign" dropdown menu with "eyal2" selected.
- A "Start Date" text box containing "06 Aug 2007, 00:00:00" and a "Set" link to its right.
- An "Expiration Date" text box containing "05 Sep 2007, 14:01:41" and a "Set" link to its right.
- A checkbox labeled "Go To Emails After Starting" which is currently unchecked.
- "OK" and "Cancel" buttons at the bottom.

Figure 9 Start Campaign Window

To Start a Campaign:

1. From the *Administration* module click the *Manage Campaigns* link.
2. In the *Campaigns* window click the *Start Campaign* link. The *Start Campaign* window opens.
3. Select the campaign you want to start from the *Campaign* drop down list.
4. The Start Date is automatically set to the current date and time. Click the *Set link* next to the Start Date field to select a new start date for the campaign.
5. Click the *Set link* next to the Expiration Date field to select a new expiration date for the campaign.
6. Select the *Go To Emails After Starting* check box to display the *Send Campaign Emails* window immediately after starting the campaign. Otherwise leave the check box cleared.
7. Click *OK* to confirm the changes. If the *Go To Emails After Starting* check box is selected then the *Send Campaign Emails* window is displayed as in Figure 10.

Home / Administration / Campaigns / Send Campaign Emails

Send Campaign Emails

Campaign From

Message Template Sending message to all (8) campaign members.

Subject

Body

Dear %%NAME%%:

Our company IT security and compliance policies require that you certify periodically the privileges of the people that report to you.

According to our records, in the "%%CAMPAIGN%%" campaign, you are responsible for %%CATEGORY%% = %%VALUE%%.

If this email was sent to you by mistake, or you are not %%NAME%% (%%ACCOUNT%%), please reply and notify the Sage Administrator at SageAdmin@company.com.

Figure 10 Send Campaign Emails window

2.6.1.6 Stop a Campaign

You can use the Stop Campaign link to immediately stop a campaign or to redefine a campaign's Expiration dates to better suit your work schedule. You stop a campaign by resetting the Expiration Date in the Stop Campaign window.

Home / Administration / Campaigns / Stop Campaign

Stop Campaign

Campaign

Expiration Date [Set](#)

Go To Emails After Stopping

Figure 11 Stop Campaigns window

To stop a campaign:

1. From the *Administration* module click the *Manage Campaigns* link.
2. In the *Campaigns* window click the *Stop Campaign* link. The *Stop Campaign* window opens.
3. Select the campaign you want to stop from the *Campaign* drop down list.
4. The Expiration Date is automatically set to the current date and time. Click the *Set* link to open a calendar and select a different expiration date if needed.
5. Select the *Go To Emails After Stopping* check box to display the *Send Campaign Emails* window immediately after stopping the campaign. Otherwise leave the check box cleared.
6. Click *OK* to confirm the changes. If the *Go To Emails After Starting* check box is selected then the *Send Campaign Emails* window is displayed as in Figure 10.

2.6.1.7 Review Campaign Progress Status

At any point during a campaign you can view the campaign status and the progress of participating members in the campaign. This information can be viewed in the *Review Campaign Progress Status* window.

All	Name	Target	Category	Value	Last Request	Deadline	Worked on	Out of	Completed	Of Which Approved	% Completed
<input checked="" type="checkbox"/>	Cooper Amos	UserCert	ManagerID	54672910		05/09/2007	0	19	0	0	0%
<input checked="" type="checkbox"/>	Goodman Bruce	UserCert	ManagerID	88311130		05/09/2007	0	3	0	0	0%
<input checked="" type="checkbox"/>	Herman Barbara	UserCert	ManagerID	64646410		05/09/2007	0	18	0	0	0%
<input checked="" type="checkbox"/>	Katz Nancy	UserCert	ManagerID	97373330		05/09/2007	0	4	0	0	0%
<input checked="" type="checkbox"/>	Levi Jay	UserCert	ManagerID	82922230		05/09/2007	0	7	0	0	0%
<input checked="" type="checkbox"/>	Purple Mary	UserCert	ManagerID	67762440		05/09/2007	0	10	0	0	0%
<input checked="" type="checkbox"/>	Schwartz Barry	UserCert	ManagerID	67565330		05/09/2007	0	5	0	0	0%
<input checked="" type="checkbox"/>	Allen Sherman	UserCert	ManagerID	99883135		05/09/2007	0	2	0	0	0%

Figure 12 Review Campaign Progress Status window

To review a campaigns progress:

1. From the *Administration* module click the *Manage Campaigns* link.
2. In the *Campaigns* window click the *Review Campaign Progress Status* link. The *Review Campaign Progress Status* window opens.
3. Select a campaign from the *Campaign* drop down list. The status of the selected campaign is displayed to the right of the drop down list. The *Members Status* table is updated to reflect the members list that belongs to the selected campaign and indicates the degree to which each member of the campaign has completed their work.

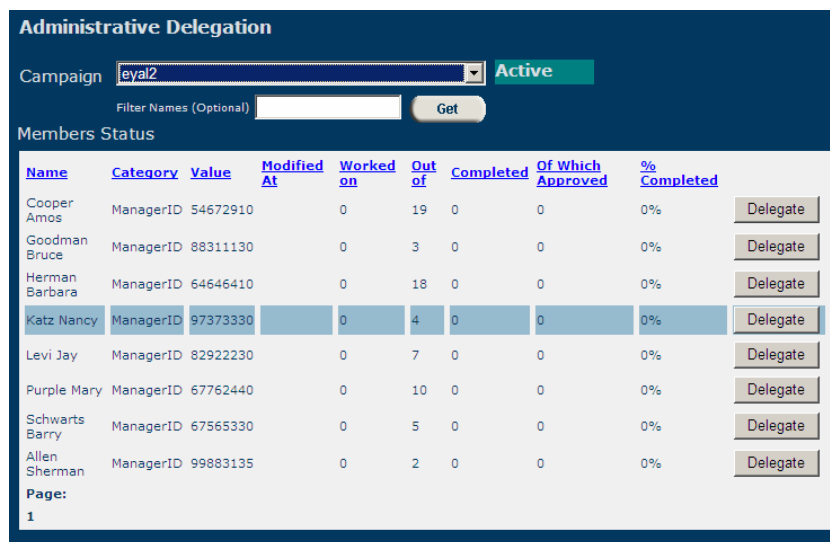
4. Enter a numeric value in the *Mark members who completed less than* edit field and click Apply. The check box in the *All* column is selected for any member that meets the set criteria.
5. Click the *Send* button to send email notifications to each of the selected campaign members.
6. Click *OK* to exit and return to the Campaigns window.

2.6.1.8 Administrative Delegation

You can delegate administrative responsibility from one member of a campaign to any member in the campaign member list.

To delegate administrative responsibility:

1. From the *Administration* module click the *Manage Campaigns* link.
2. In the *Campaigns* window click the *Administrative Delegation* link. The *Administrative Delegation* window opens.
3. From the *Campaign* drop down list select a campaign. The *Member Status* table for the selected campaign appears.



The screenshot shows the 'Administrative Delegation' window. At the top, there is a 'Campaign' dropdown menu set to 'leval2' and an 'Active' status indicator. Below this is a 'Filter Names (Optional)' input field and a 'Get' button. The main area contains a table titled 'Members Status' with the following columns: Name, Category, Value, Modified At, Worked on, Out of, Completed, Of Which Approved, and % Completed. Each row also has a 'Delegate' button. The table lists several members, with 'Katz Nancy' highlighted in blue.

Name	Category	Value	Modified At	Worked on	Out of	Completed	Of Which Approved	% Completed	
Cooper Amos	ManagerID	54672910		0	19	0	0	0%	Delegate
Goodman Bruce	ManagerID	88311130		0	3	0	0	0%	Delegate
Herman Barbara	ManagerID	64646410		0	18	0	0	0%	Delegate
Katz Nancy	ManagerID	97373330		0	4	0	0	0%	Delegate
Levi Jay	ManagerID	82922230		0	7	0	0	0%	Delegate
Purple Mary	ManagerID	67762440		0	10	0	0	0%	Delegate
Schwartzs Barry	ManagerID	67565330		0	5	0	0	0%	Delegate
Allen Sherman	ManagerID	99883135		0	2	0	0	0%	Delegate

Page:
1

Figure 13 Administrative Delegation window

4. In Members Status list navigate to the row containing the member that administrative responsibility is being removed from and click the Delegate button. The *Member to Delegate* window opens.
5. From the *Choose Target for Delegation* drop down list select a configuration entity and click the *Get* button. A list of Users appears. Navigate to the user that is to receive administrative delegation rights and click the *Select* button at the end of the row. A confirmation message appears below the list indicating that administrative delegation has been transferred.

Member to delegate:

Campaign: eyal2

Login: DOMAIN\Katz_Nancy

Target: ManagerID - 97373330

Choose target for delegation:

UserName

PersonID	Name	Login	Email	
45489940	Steiven Pat	DOMAIN\Steiven_Pat	Steiven_Pat@company.com	<input type="button" value="Select"/>
47868650	Moris Bill	DOMAIN\Moris_Bill	Moris_Bill@company.com	<input type="button" value="Select"/>
52656727	Rodman Adam	DOMAIN\Rodman_Adam	Rodman_Adam@company.com	<input type="button" value="Select"/>
54672910	Cooper Amos	DOMAIN\Cooper_Amos	Cooper_Amos@company.com	<input type="button" value="Select"/>
56765465	Greg Heiman			<input type="button" value="Select"/>

1 2 3 4 5 6 7 8 9 10 ...

Delegate To: Steiven Pat DOMAIN\Steiven_Pat
Steiven_Pat@company.com

6. Click the *OK* button to confirm the changes in the system.

2.6.1.9 Send Campaign Emails

At various times throughout the course of a campaign you may need to send emails to campaign members as reminders, or to inform them of changes in status of the campaign. Sage ERM provides you with a number of default email templates that you can use to send such emails. These include:

Email Template Type	Description
New Campaign	Informs company members that there is a new campaign and that they are participants in the campaign. Campaign data such as tasks and targets are detailed in the mail. The email contains a link to the campaign.
Campaign Reminder	Reminds campaign participants of their tasks and target due dates. The email contains a link to the campaign.
Campaign Stopped	Informs campaign participants that the campaign was stopped.
Delegation Message	Informs a participant in a campaign that they are no longer responsible for their tasks and that the tasks were delegated to another user.
Delegation Target Message	Informs users that they were added to a campaign and that they were delegated certain campaign activities. The email contains a link to the campaign.

To send campaign emails:

1. From the *Administration* window select *Manage Campaigns>Send Campaign Emails*. The *Send Campaign Emails* window appears.

2. Select a Message Template from the *Message Template* drop down list. The content of the Subject and Body fields is updated to reflect the template.
3. Click the *Send* button, a confirmation message appears to verify that really wan to send mail.
4. Click *Yes* to send the email, or click *No* to discard the changes and refrain from sending any email.

2.6.1.10 Manage Email Templates

Use the Manage Email Templates feature to modify the content of default supplied Email templates, create new templates or translate the templates into additional languages. You can modify the content of the Subject and Body text however you can only use the existing parameters. These include:

<i>Email Template Parameter</i>	<i>Description</i>
Name	The user name of each participant in the campaign member list.
Campaign	The Campaign name as selected from the Campaign drop down list.
Category	The category assigned to the list member when the member list was created.
Value	The specific value for the category's that is associated with the list member when the member list was created.
Expiration	The campaign expiration date.
Account	The domain\User for each member in the selected campaign's member list
Link	Directs the targeted user to their assignment in the selected campaign.

For Sage ERM to correctly refer to the Parameters they must be bounded by a double set of % symbols. For example: %%Name%%.

To edit email templates:

1. From the *Administration* window select *Manage Campaigns > Manage Email Templates*. The *Manage Email Templates* window appears.

Home / Administration / Campaigns / Manage Email Templates

Manage Email Templates

Add New Template

Template Name

New Campaign [Remove] [Add]

Subject Campaign Alert: New Campaign

Body

Dear %%NAME%%:

Our company IT security and compliance policies require that you certify periodically the privileges of the people that report to you.

According to our records, in the "%%CAMPAIGN%%" campaign, you are responsible for %%CATEGORY%% = %%VALUE%%.

If this email was sent to you by mistake, or you are not %%NAME%% (%%ACCOUNT%%), please reply and notify the Sage Administrator at SageAdmin@company.com.

[OK] [Cancel] [Apply]

2. From the *Template Name* drop down list select the template that you want to modify.
3. Select the text in *Subject* or *Body* fields and edit the text.
4. Click *Apply* to save your changes without closing the window.
5. Click *OK* to save your changes and return to the *Campaigns* window.

To add a new template:

1. From the *Administration* window select *Manage Campaigns > Manage Email Templates*. The *Manage Email Templates* window appears.
2. Enter a name for the new template in the *Add New Template* edit field and click the *Add* button located below the edit field. The new name is added to the *Template Name* drop down list and the contents of the *Subject* and *Body* fields are deleted.
3. Enter content for the new message in the *Subject* and *Body* fields.
4. Click *Apply* to save your changes without closing the window.
5. Click *OK* to save your changes and return to the *Campaigns* window.

2.7 Set Workform Defaults

For each workform type you must assign separate workform default settings. These are assigned in the *Set Workform Defaults* window and are reflected in the settings pane of the associated workforms. For example default settings assigned to the *User Certification/Attestation* workform type determine the campaigns that are available for use in Settings pane of the *User Privileges Certification/Attestation* workform.

Home / Administration / Set Workform Defaults

Set Workform Defaults

Workform: FilterUsers

Default Campaign Allow User Setting

Allow Alternate Settings:

Configuration Allow User Setting

AuditCard Allow User Setting

Category Allow User Setting

OK Cancel Apply

Figure 14 Set Workform Defaults window

To set workform defaults:

1. From the *Administration* window select *Set Workform Defaults*. The *Set Workform Defaults* window appears.
2. From the Workform drop down list select a workform type. The workform default setting fields are populated with previously assigned settings if they exist. If this is the first time that the workform settings are being assigned then the setting fields remain empty.
3. Select the Default Campaign check box to allow the use of a default campaign.
4. From the Default Campaign drop down list select a campaign to function as the default campaign. Select the adjacent Allow User Setting check box if you want to allow Users access to any campaign other than the default campaign.
5. Select the Allow Alternate Settings check box if you want workform users to be able to assess workform content based on the use of Configurations, AuditCards and Categories irrespective of whether a default campaign has been assigned. Otherwise to prevent the use of alternate settings leave the check box cleared.

6. Select a Configuration from the Configuration drop down list. Select the adjacent check box to allow workform users to choose other configurations than that assigned.
7. Select an AuditCard from the AuditCard drop down list. Select the adjacent check box to allow workform users to choose other AuditCards than that assigned.
8. Select a Category from the Category drop down list. Select the adjacent check box to allow workform users to choose other Categories than that assigned.
9. Click Apply to save your settings and click OK to save your settings and exit the window.

2.8 Self Service Settings

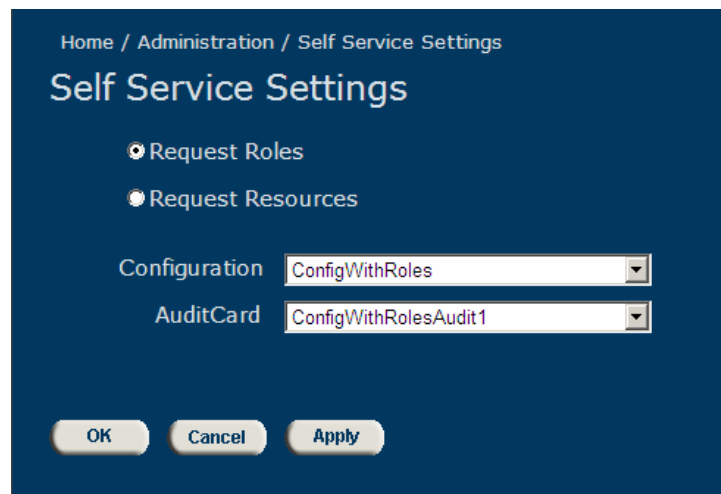
Use the parameters in the Self Service Settings to set the Configuration and AuditCards that are used when requesting roles and resources. This affects the following Self Service workforms:

- Request Role Privileges for Myself
- Request Role Privileges for My Team
- Request Resource Privileges for Myself
- Request Resource Privileges for My Team

An error message is displayed if you attempt to open any of the Self Service workforms without setting the Self Service Settings.

To set the Self Service Settings

1. From the *Administration* window select *Self Service Settings*. The *Self Service Settings* window appears.



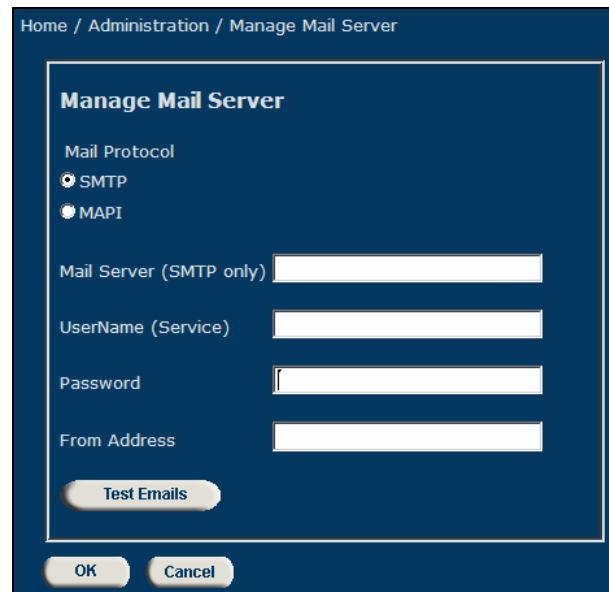
2. Select the *Request Roles* option.
3. From the *Configuration* drop down list select the configuration to be used in the *Request Role Privileges for Myself* and the *Request Role Privileges for My Team* workforms.
4. Click *Apply* to confirm and save your selections.
5. From the *AuditCard* drop down list select the *AuditCard* to be used in the *Request Role Privileges for Myself* and the *Request Role Privileges for My Team* workforms.
6. Select the *Request Resources* option and now select the *Configuration* and *AuditCard* to be used in the *Request Resource Privileges for Myself* and the *Request Resource Privileges for My Team* workforms.
7. Click the *OK* button to save your selections and return to the *Administration* window.

2.9 Manage Mail Server

The Manage Mail Server window is used to assign the Server address and credentials for the server from which you distribute campaign emails.

To assign mail server address and credentials:

1. From the *Administration* window select *Manage Mail Server*. The *Manage Mail Server* window appears.
2. Select the Mail Protocol option that your mail server uses.
3. In the *Mail Server (SMTP only)* field enter the address for server machine from which campaign mail is distributed.
4. In the *UserName* and *Password* fields enter the respective credentials if they are required in order to access the server machine. If the *UserName* and *Password* are not required, then leave the fields blank.
5. In the *From Address* field enter the address that should appear in the *From* field on each mail item sent for a campaign.
6. Click the Test Emails button to verify that the settings are correct.



Home / Administration / Manage Mail Server

Manage Mail Server

Mail Protocol

SMTP

MAPI

Mail Server (SMTP only)

UserName (Service)

Password

From Address

Test Emails

OK Cancel

7. Click OK to save the settings and exit the window.

3 Business Collaboration

The Sage Business Collaboration module contains a collection of Workforms that business and line managers use to review and certify change requests, privileges and policies assigned to members of their teams and organizational units. The Business Collaboration module provides an easily accessible environment for managerial and IT personnel to share such information and to ensure they meet organization based and government driven compliance regulations.

3.1 Accessing the Business Collaboration Module

The Business Collaboration module is accessed via a browser using the Sage Portal.

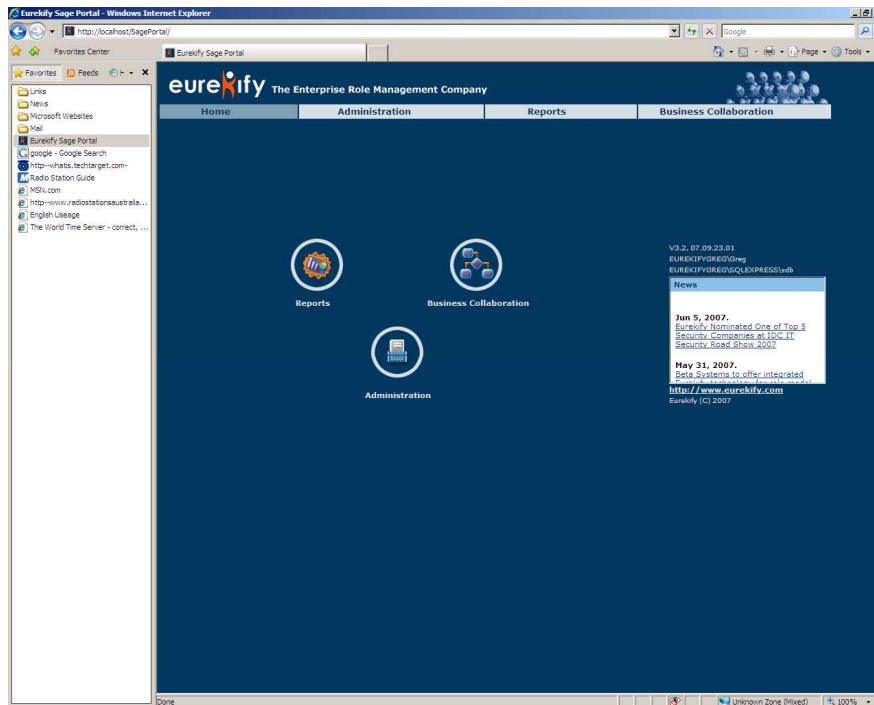


Figure 15 Sage Portal Home Page

To view business collaboration work forms via the Sage Portal:

1. Open the Microsoft Explorer browser.
2. Enter the URL <http://localhost/sageportal>. The Sage Portal opens to the home page.

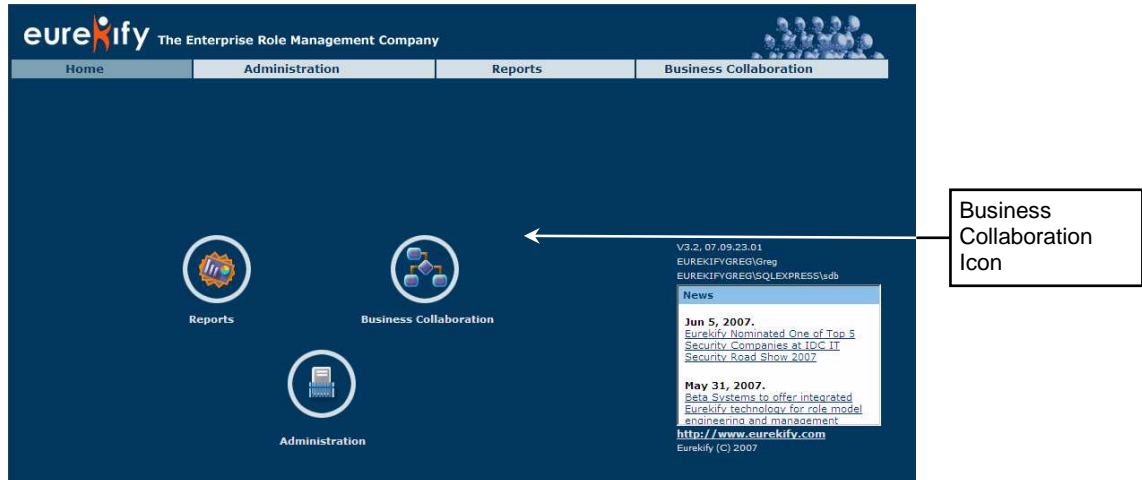


Figure 16 Business Collaboration Icon

3. Either click the *Business Collaboration icon* in the body of the page, or the *Business Collaboration button* from the menu bar at the top of the page, the Business Collaboration page opens. Workform categories are displayed in the left pane of the window. The remainder of the window serves to display this list of work-forms available for a given category.
4. Click a category folder to display the list of Workforms.

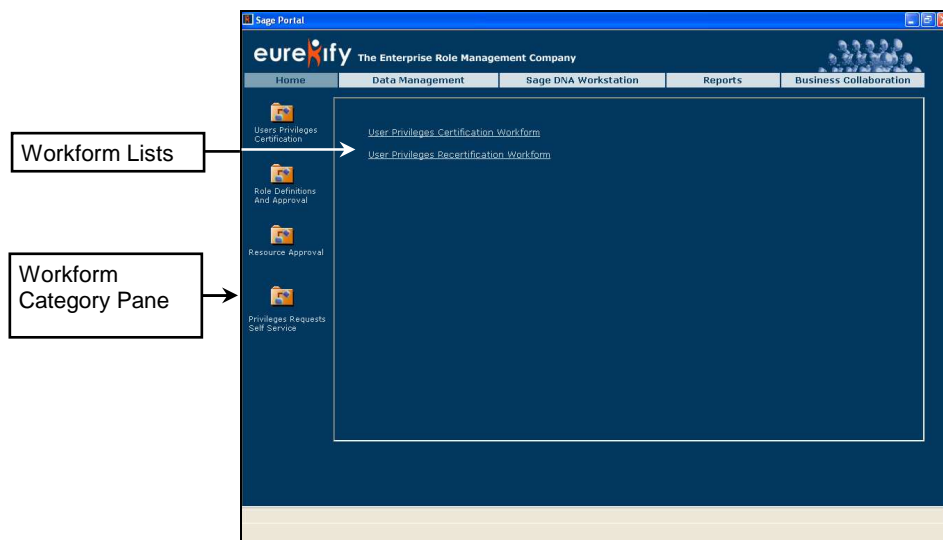


Figure 17 List of Workforms

5. Click a Workform from the list to open the Workform in the display area.

3.2 Workform Structure

Most Workforms are arranged in a similar manner where the workform has two tabs: a *Settings* tab and a *Main* tab. Each of the tabs can be divided into an upper and lower region. You use the options on the Settings tab to select the parameters and attributes which are used to extract information to be displayed on the Main tab. In Figure 18 the Configuration, AuditCard and Category parameters are assigned for use in displaying User Certification data.

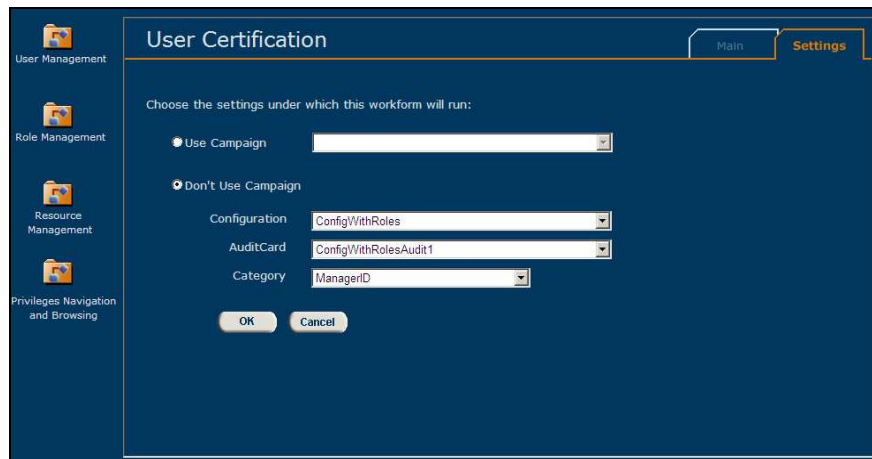


Figure 18 User Certification Settings Tab

Figure 19 shows how the Main tab of the User Certification workform is divided. In the upper region of the Workform you select a specific instance for which you want to extract information. In this case you select a Manager and then User Certification data for the manager’s employees is displayed in the lower region of the Workform, the Operational Area. The lower region displays the extracted information as defined in the upper region. It is in the lower region that you perform operations to review and certify user privileges, and to authorize role and resource definitions.

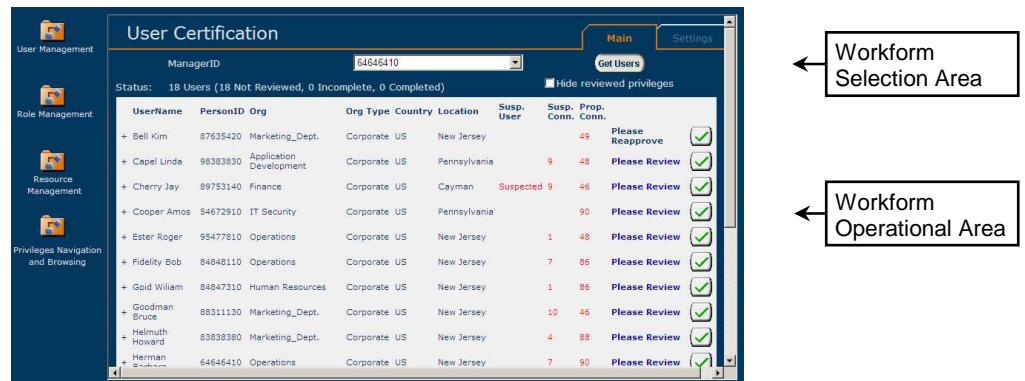


Figure 19 Workform Showing Selection and Operational Areas



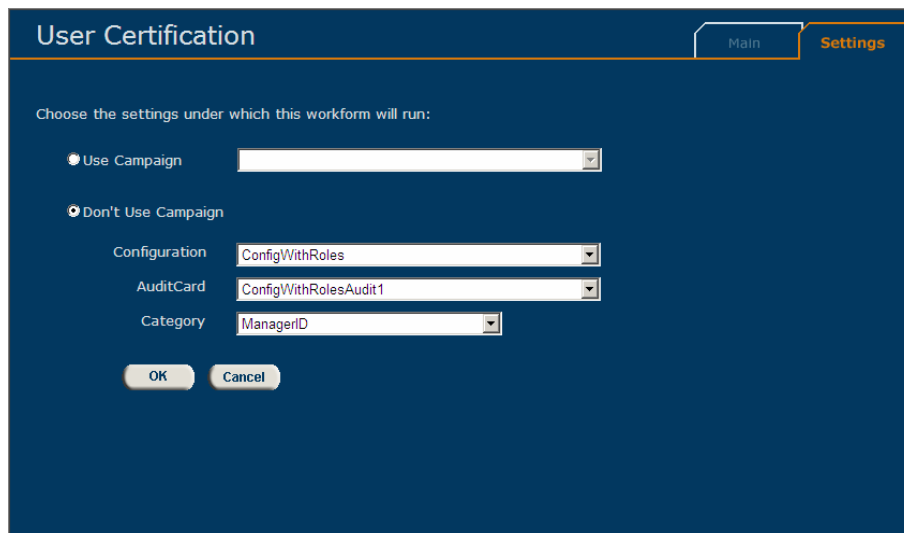
Note: Some workforms such as those used for *Role Approval* and *Role Requests* are organized differently to what is described in this section. The arrangement and use of those workforms is described separately for each individual workform.

3.2.1 Workform Settings Tab

Use the Workform's *Setting tab* to select the type, and refine the amount of information that is displayed in the *Workform Main tab*. Choose Category and Value attributes to focus on sub groups of the database entities. The fields that appear in the *Setting* tab are dynamic, and vary according to the Workform being used.

Figure 20 illustrates the options available for the *User Privileges Certification* Workform. These include:

- Campaign
- Configuration
- AuditCard
- Category



The screenshot shows a dialog box titled "User Certification" with two tabs: "Main" and "Settings". The "Settings" tab is active. The dialog contains the following elements:

- A heading: "Choose the settings under which this workform will run:"
- Two radio buttons: "Use Campaign" (selected) and "Don't Use Campaign".
- Three dropdown menus:
 - Configuration: ConfigWithRoles
 - AuditCard: ConfigWithRolesAudit1
 - Category: ManagerID
- Two buttons at the bottom: "OK" and "Cancel".

Figure 20 Workform Settings Tab

After selecting the settings click the OK button to view the Main tab.

3.2.2 Workform Main Tab

The Workform Main Tab contains the upper selection area from which you select a set of information based on the settings that were selected on the Settings tab. The lower area called the Operational area displays the data extracted from the database. This is the section of the workform that you use to perform operations such as accepting or rejecting requests, and performing periodic reviews.

UserName	PersonID	Org	Org Type	Country	Location	Susp. User	Susp. Conn.	Prop. Conn.	
+ Atek Rogers	87623490	Fifth Ave Branch	Branches	US	New York			16	Please Review
+ Deer Alex	91238730	Fifth Ave Branch	Branches	US	New York			16	Please Review
+ Eagle Richard	76329130	Fifth Ave Branch	Branches	US	New York	3	25	25	Please Review
+ German Tom	94738470	Fifth Ave Branch	Branches	US	New York	7	15	15	Please Review
+ Hill Gary	82653450	Fifth Ave Branch	Branches	US	New York	2	25	25	Please Review
+ Hill Silver	89213478	Fifth Ave Branch	Branches	US	New York			16	Please Review
+ Mills Robert	84774660	Fifth Ave Branch	Branches	US	New York			28	Please Review
+ Purple Mary	67762440	Fifth Ave Branch	Branches	US	New York	4	37	37	Please Review
+ Saven Werner	87473220	Fifth Ave Branch	Branches	US	New York			16	Please Review
+ Sharon Johnson	89123470	Fifth Ave Branch	Branches	US	New York			16	Please Review

Figure 21 Main Tab

3.2.2.1 Workform Operational Area

The Workform Operational area is divided into columns, where each column displays a different type of information taken from the database. Each row represents a single entry record in the database. This is illustrated in Figure 22.

The business manager's job is to review each entry in the workform and to approve the content, or to request changes. Using Sage tools, Role Engineers identify exceptions as to the use of resources and distribution of privileges amongst employees. These exceptions are indicated as Suspected and Proposed AuditCard Alerts and are colored Red in the workform. The AuditCard Alerts are suggestions for action which must be confirmed or rejected by the Business Managers that have a day to day understanding of the access privileges required by their employees to perform their jobs.

UserName	PersonID	Org	Org Type	Country	Location	Susp. User	Susp. Conn.	Prop. Conn.	
Atek Rogers	87623490	Fifth Ave Branch	Branches	US	New York	16	Please Review	✓	AuditCard Alerts
+ Deer Alex	91238730	Fifth Ave Branch	Branches	US	New York	16	Please Review	✓	
+ Eagle Richard	76329130	Fifth Ave Branch	Branches	US	New York	3	25	Please Review	✓
+ German Tom	94738470	Fifth Ave Branch	Branches	US	New York	7	15	Please Review	✓
+ Hill Gary	82653450	Fifth Ave Branch	Branches	US	New York	2	25	Please Review	✓
+ Hill Silver	89213478	Fifth Ave Branch	Branches	US	New York	16	Please Review	✓	Review Status
+ Mills Robert	84774660	Fifth Ave Branch	Branches	US	New York	28	Please Review	✓	Review Confirmation
+ Purple Mary	67762440	Fifth Ave Branch	Branches	US	New York	4	37	Please Review	✓
+ Saven Werner	87473220	Fifth Ave Branch	Branches	US	New York	16	Please Review	✓	

Figure 22 Operational Area

Information Type	Description
Configuration Data columns	<p>Configuration data appears in black. Each column displays information extracted from the database. The exact content type is indicated at the top of each column by a Header.</p> <p>In Figure 22, running from left to right these columns include data on UserName, PersonID, Org, Org Type, Country and Location.</p> <p>Each row in the table represents information taken from a separate record in the database. Depending on the Workform and Configuration being referenced, these refer to Users, Roles, or Resources.</p>
AuditCard Alerts columns	<p>AuditCard alerts appear in Red. These represent suggestions for action to be taken on the data.</p> <p><i>Suspected User Alerts</i> indicate that the user is a collector.</p> <p><i>Suspected Connection Alerts</i> indicate that the access privilege for the entity may need to be removed.</p> <p><i>Proposed Connection Alerts</i> indicate that the access privilege for the entity may need to be added.</p>
Review Status column	<p>The review status column has three states and indicates whether the row entry is waiting for review or has been approved.</p> <p><i>Please Review</i> Entry is waiting to be reviewed.</p> <p><i>Approved</i> Entry was reviewed and confirmed without changes.</p> <p><i>Changes Requested</i> Entry reviewed and confirmed with requested changes</p>
Review Confirmation column	<p>This is the column that is located on the far right of the table and contains a Green colored check mark. Clicking the check mark records the status of each item within the record and confirms that the record underwent review. Each time the check mark is clicked the status of each item is written to the database. Each instance is preserved in the database, however only the last instance is presented in the user interface.</p>

3.2.2.2 Drilling Down for Record Details

Each record in the Workform can be expanded to reveal greater levels of detail of data extracted from the database. Again the type of information that is presented depends on the type of information that is treated by the Workform. That is, whether the Workform focus is on Users, Roles, or Resources.

A plus sign (+) appears to the left of the first column in each record. In Figure 22, in section 3.2.2, the record for *Hill Gary* is highlighted and the plus sign is visible. The Plus sign indicates that the record contains internal levels of information and that you can drill down into the record to view the information. Figure 23 shows the first level drill down for the same record. This reveals a list of roles linked to *Hill Gary*, some of which have audit card alerts associated with them. Figure 23 also shows that the record contains *Resources*, *Related Roles* and *Related Resources*, which can each be expanded to reveal a second internal level of information.

The screenshot shows a user record for Hill Gary with the following details:

- ID: 82653450
- Branch: Fifth Ave Branch
- Country: US
- Location: New York
- Alerts: 7 Incomplete (5), 15 Please Review

The record is expanded to show a table of roles:

Name	Description	Link Type	Audit Card Status	History	Remove All	Approve All	Comment
BASIC ROLE	New Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
Organization - Fifth Ave Branch	Characteristic Role (80%)	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
Title - Branch Officer/Clerk	Characteristic Role (50%)	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
UGTELSAVE	Automation & document management	Direct	*Suspect User-Role Connection By Privilege (Score:28 Status: Suspected);	Suspected Violation 7/10/2007 6:06:52 PM	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
TS17611	Sage Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
B5AVEJ1	Sage Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	

Below the roles table, there are expandable sections for Resources (6), Related Roles (14), Related Resources (11), and User Alerts (0).

Callout boxes in the image provide the following information:

- A box on the left points to the plus sign next to the Hill Gary record, stating: "+ Sign indicates that the record contains internal levels of information".
- A box on the right points to the red text in the UGTELSAVE row, stating: "AuditCard Alerts for Roles linked to the selected user".

Figure 23 Record showing first level drill down

Within a Workform you can:

- Expand/Collapse Workform entries
- Display Workform entry details in tabular form

To expand/collapse Workform entries:

1. Open a Workform and make selections in the selection area to display the Workform operational area.
2. From within the Workform operational area place the mouse pointer on the + sign and click. The entry expands to display internal levels of information.
3. Click the + sign again to collapse the level and hide the information.

To display Workform entity details in a table:

1. Open a Workform and make selections in the selection area to display data in the Workform operational area.
2. From inside the Operational area, place the mouse pointer over an item in the first column of the Workform. The mouse pointer changes shape to a hand.
3. Click the mouse. A new window opens displaying information related to the selected entity.

User details for German Tom

Person ID	94738470
Name	German Tom
Organization	Fifth Ave Branch
Organization Type	Branches
Country	US
Location	New York
Title	Branch Officer/Clerk
Cost Center	22321
Field5	
Field6	

Roles

Name	Description	Organization	Owner	Type	Create Date	Reviewer	Approve Code	Approve Date	Filter	Org2	Org3	Link Type
BASIC ROLE	New Role	Enterprise	Levi Jay	Org Role	1/16/2006 9:31:00 AM	Levi Jay	Approved	4/16/2006 12:37:00 PM			Coorporate	Direct
Organization - Fifth Ave Branch	Characteristic Role (80%)	Fifth Ave Branch	Eagle Richard	Org Role	1/16/2006 9:31:00 AM	Levi Jay	Approved	4/16/2006 12:37:00 PM			Coorporate	Direct
Title - Branch Officer/Clerk	Characteristic Role (50%)	Title - Branch Officer/Clerk	Hill Gary	Org Role	1/16/2006 9:31:00 AM		Pre Approved	4/16/2006 12:39:00 PM			Coorporate	Direct
UGSAVESYS	Automation & document management	Production	Garr Jim	Org Role	1/16/2006 9:31:00 AM		Approved	4/16/2006 12:39:00 PM			Coorporate	Direct
BRLIMSYS	Automation & document management	Production	Garr Jim	Org Role	1/16/2006 9:31:00 AM		Pre Approved	4/16/2006 12:39:00 PM			Coorporate	Direct
BSAVEPRIV	Sage Role	IT	SageBank	Org Role	1/16/2006 9:31:00 AM		Pre Approved	4/16/2006 12:39:00 PM			Coorporate	Direct
BSAVEJ1	Sage Role	IT	SageBank	Org Role	1/16/2006 9:31:00 AM		Pre Approved	4/16/2006 12:39:00 PM			Coorporate	Direct

Figure 24 Workform details displayed in tabular form

3.2.2.3 Approving Workform Changes

Workforms are either opened by business line managers or sent to business line managers as part of an organization's review or periodic campaign. In either case the goal is for the manager to review each entry and assess whether the entity is correctly allocated.

An entry in a Workform may appear with or without an associated AuditCard alert. The AuditCard alerts show that the Role Engineer identified that the entry differs from other entities of the same type in such a way as to raise suspicion. The manager's job is to assess whether the alert is correct. When reviewing each entry, the business line manager can add to, or remove users, roles, or resources from the configuration, by accepting or rejecting the AuditCard alerts. Where a record does not contain any proposed changes the business line manager is still required to review and approve the content.

In the case of a suspected alert the manger can remove the entity by clicking the checkbox, or disregard the alert by leaving the check box unselected. In the case of a Proposed alert the manager can add the entity by clicking the checkbox, or disregard the alert by the leaving the checkbox unselected.

Once reviewed and approved, the information is available to be treated by role engineers, and the reviewed data may be loaded to the production machine.

To approve Workform changes:

1. Open a Workform and make selections to display data in the Main tab operational area.

UserName	PersonID	Org	Org Type	Country	Location	Susp. User	Susp. Conn.	Prop. Conn.	
+ Atek Rogers	87623490	Fifth Ave Branch	Branches	US	New York			16	Please Review <input checked="" type="checkbox"/>
+ Deer Alex	91238730	Fifth Ave Branch	Branches	US	New York			16	Please Review <input checked="" type="checkbox"/>
+ Eagle Richard	76329130	Fifth Ave Branch	Branches	US	New York	3	25		Please Review <input checked="" type="checkbox"/>
+ German Tom	94738470	Fifth Ave Branch	Branches	US	New York	7	15		Please Review <input checked="" type="checkbox"/>
+ Hill Gary	82653450	Fifth Ave Branch	Branches	US	New York	2	25		Please Review <input checked="" type="checkbox"/>
+ Hill Silver	89213478	Fifth Ave Branch	Branches	US	New York			16	Please Review <input checked="" type="checkbox"/>
+ Mills Robert	84774660	Fifth Ave Branch	Branches	US	New York			28	Please Review <input checked="" type="checkbox"/>
+ Purple Mary	67762440	Fifth Ave Branch	Branches	US	New York	4	37		Please Review <input checked="" type="checkbox"/>
+ Saven Werner	87473220	Fifth Ave Branch	Branches	US	New York			16	Please Review <input checked="" type="checkbox"/>

Figure 25 Workform showing selections in the Operational Area

2. Select an entry. The entry may or may not display AuditCard alerts. If the entry contains alerts they can be Proposed connections or Suspect Connection. Either way they appear as red text.
3. Click the + sign to expand the record until you reach the first level that contains a column of check boxes for removing or approving changes.

The screenshot shows the Eureka Enterprise Role Management interface. The main content area displays a list of roles for a selected user (Hill Gary). The roles table includes columns for Name, Description, Link Type, Audit Card Status, History, Remove All, Approve All, and Comment. A callout box with an arrow points to the 'Remove All' and 'Approve All' columns, labeled 'Remove / Approve check box'. The interface also shows a sidebar with navigation options like User Management, Role Management, Resource Management, and Privileges Navigation and Browsing.

Figure 26 Operational Area showing Remove Checkboxes

- To accept the proposed change, place a check mark in the check box. Once a check box is selected, an edit field appears adjacent to the check box.



Figure 27 Role identified for removal

- Enter a comment in the edit field to indicate the reason for your action. This information is used by the role engineer.



Figure 28 Operational area showing reason for removal

- To reject a proposed change leave the check box blank.
- Repeat this process for each proposed alert for the entity. Drill down to deeper levels within the record where required.
- Once you have reviewed each proposed change, click the Review Confirmation button for that workflow record.

3.3 User Management

The User Management folder contains workforms that give you the capability to:

- Review roles and resources assigned to users
- Focus on exceptions as identified by audit card alerts
- Approve or reject user access to roles and resources
- Propose changes

The Users Privileges Certification folder contains the following workforms:

- Request a New User Definition
- Request Changes to a User Definition
- Request Removal of a User Definition
- Request Role Privileges for My Team
- Request Resource Privileges for My Team
- Request Role Privileges for Myself
- Request Resource Privileges for Myself
- User Privileges Certification/Attestation

3.3.1 Request a New User Definition

Use the *Request a New User Definition* to supply the details of a new user to be added to a configuration. Details for a new user definition include

- User values for the configuration attributes
- Roles to assign the user
- Resources to assign the user

To request a new user definition:

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request a New User Definition* link.
2. Click the *Settings* tab to bring it forward.
3. From the *Configuration* drop down list select the configuration that you want to request a new user definition for, and then click *OK*. The *Main* tab opens displaying a text field for each attribute in the selected configuration.

Attribute	Input Field
ConfigWithRoles	
Person ID*	
User Name	
Organization	
Organization Type	
Country	
Location	
Title	
Cost Center	
ManagerID	
email	
LoginID	
Field8	

4. Enter the appropriate values for the new user definition in each of the text fields. Fields marked with an asterisk are mandatory. If you do not know the correct value for a given field click the *Find* button to open a window displaying the range of values available for the selected attribute. Select the value and click *OK* to enter the value in the attribute text field.
5. Click the *OK* button, the *Request Modification to Existing User Definition* window opens. Review the details for the new user definition request.

Attribute	Value
User ID	
Person ID	66554443
User Name	John Satler
Organization	
Organization Type	
Country	
Location	
Title	
Cost Center	
ManagerID	
email	
LoginID	
Field8	
Field9	
Field10	
Field11	
Field12	

Actual Roles - none

6. Click *Edit* to open the *Edit User Definition* window and modify the user definition details. Click the *OK* button to save changes and return to the *Request Modification to Existing User Definition* window.
7. Now add Roles to the User Definition. Click the *Select to Add* button next to the Actual Roles section just below the user details table. The *Find Roles* window opens.
8. Enter role details in the filter text fields and click select. A table of roles matching the search details is displayed.
9. Mark the check box next to the role that you want to add to the User Definition and then click *OK*. The selected role is added to the list of Requested Roles for the User Definition.

Find Roles

ConfigWithRoles

Where Contains and

Where Contains and

Where Contains

Existing Roles

<input type="checkbox"/> All <input checked="" type="checkbox"/> None	Role Name	Description	Organization	Owner	Approval
<input checked="" type="checkbox"/>	BASIC ROLE	New Role	Enterprise	82922230	Approved
<input type="checkbox"/>	Organization - Database Administrators	http://localhost/temp/role_database_administrators.html	Database Administrators	99883135	Approved

Requested Roles

10. Now add Resources to the User Definition. Click the *Select to Add* button next to the Actual Resources section just below the user details table. The *Find Resources* window opens.
11. Enter resource details in the filter text fields and click *Select*. A table of resources matching the search details is displayed.
12. Mark the check box next to the resource that you want to add to the User Definition and then click *OK*. The selected resource is added to the list of Requested Resources for the User Definition.
13. The request for a new user definition should now include User details, a list of Roles and a list of Resources. Click *OK*. The window is closed and the request for a new user definition is stored for review and approval.

3.3.2 Request Changes to a User Definition

Use the Request Changes to a User Definition workflow to modify the details of an existing user.

To request changes to a User Definition:

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request Changes to a User Definition* link.

2. Click the *Settings* tab to bring it forward.
3. From the *Configuration* drop down list select the configuration that User Definition belongs to and then click *OK*. The *Main* tab opens.

4. Enter the *Person ID* in the text field for the User Definition that you want to change.
5. If you do not know the Person ID click *Select to Edit* to search for the Person ID. The Find User window opens.
6. Enter search strings in the *Find User* fields and click *Select*. A list of Users matching the search string is displayed.
7. Select the check box next to the User for which you want to change the definition and click *OK*. The Person ID for the selected User is loaded into the *Person ID* text field.
8. Click *OK*. The *Request Modification to Existing User Definition* window opens and displays the details for the selected user.
9. Modify the User details in the *Request Modification to Existing User Definition* window by clicking *Edit*, changing the details in the Edit User Definitions window. Click *OK* to save your changes and return to the *Request Modification to Existing User Definition* window.
10. To add a role/resource to the Requested Roles/Resource list click the *Select to Add* button adjacent to the *Actual Roles* or the *Actual Resource* list. Use the *Find Roles/Resource* window to identify roles or resources that match a search string and click select to display matching roles or resources.
11. Select a role/resource from the list and click *OK*. The selected role/resource is added to the Requested Roles/Resource list.
12. To remove a role or resource from the User Definition, select the check box in the role's or resources' Remove column and click the *OK* button. The request is saved and the window is closed.

3.3.3 Request Removal of a User Definition

Where a user is no longer required to be a member of a configuration you can submit a request to remove the user definition from the configuration.

To request removal of a User Definition:

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request Removal of a User Definition* link. The *Request User Removal* window opens.
2. Click the *Settings* tab to bring it forward.

- From the *Configuration* drop down list select the configuration that User Definition belongs to and then click *OK*. The *Main* tab opens.

- In the Person ID text field, enter the Person ID for the User Definition that you want to remove from the configuration.
- If you do not know the Person ID, click Get Users. The Find Users window opens.
- Enter search strings in the *Find User* fields and click *Select*. A list of Users matching the search string is displayed.
- Select the check box next to the User that you want to remove and click *OK*. The Person ID for the selected User is loaded into the *Person ID* text field.
- You can add a comment in the Comment field if required.
- Click *OK*. The request to remove the user definition is saved.

3.3.4 Request Role Privileges for My Team

Use the Request Roles for My Team workform to add access rights to roles to members of your team.

This form is a Self Service form and requires you to set the *Configuration* and *AuditCard* parameters in the *Self Service Settings* page before using the workform. If you open the workform without assigning the parameters an error message is displayed.



See section 2.8 *Self Service Settings* for details.

To request roles for you team:

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request Role Privileges for My Team* link. The *Request Roles for My Team* window opens.

Request Roles For My Team

Please select your team:

Category: Value:

Users

All	Person ID	User ID	User Name	Org	Org Type
<input checked="" type="checkbox"/>	88261730	36	Green Richard	Human Resources	Corporate
<input checked="" type="checkbox"/>	99883134	66	Ron Mark	Human Resources	Corporate
<input checked="" type="checkbox"/>	99883135	73	Allen Sherman	Sales	Corporate
<input checked="" type="checkbox"/>	12345678	75	Greg Meyers	Human Resources	Branches

2. Select a Category from the Category list. This should be the Category that identifies you as the Manager of a team.
3. Select the Value from the Value drop down list that matches your ID as manager or team leader.
4. Click the Get Users button. The Users list is displayed and loaded with the members of your team.
5. Select the Users from the list that you are requesting roles for.
6. Click the Get Roles button. The list of roles is displayed.
7. Select the check box in the *Link* column for each role that you want to request for you team.

Currently Enrolled Roles

Role Name	Role Description	Org	Role Owner	Use In Selection	Link
BASIC ROLE	New Role	Enterprise	82922230	1/4 25%	<input checked="" type="checkbox"/> <input type="text"/>
Sales	Role By 2 Users	Sales	99883135	1/4 25%	<input checked="" type="checkbox"/> <input type="text"/>

Almost Matching Roles

Role Name	Description	Org	Role Owner	Use In Selection	Link
BASIC ROLE	New Role	Enterprise	82922230	1/4 25%	<input checked="" type="checkbox"/> <input type="text"/>
ADMGNRL	Sage Role	IT	67565330	0/4 0%	<input type="checkbox"/> <input type="text"/>

Proposed Roles

8. Click *OK*. The requests are saved and window closes.

3.3.5 Request Resource Privileges for My Team

Use the Request Resources for My Team workflow to add access rights to resources to members of your team.

This form is a Self Service form and requires you to set the *Configuration* and *AuditCard* parameters in the *Self Service Settings* page before using the workflow. If you open the workflow without assigning the parameters an error message is displayed.



See section 2.8 *Self Service Settings* for details.

To request resources for your team:

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request Resource Privileges for My Team* link. The *Request Resources for My Team* window opens.



2. Select a Category from the Category list. This should be the Category that identifies you as the Manager of a team.
3. Select the Value from the Value drop down list that matches your ID as manager or team leader.
4. Click the Get Users button. The Users list is displayed and loaded with the members of your team.
5. Select the Users from the list that you are requesting resources for.
6. Click the Get Resources button. The list of resources is displayed.
7. Select the check box in the *Link* column for each resource that you want to request for you team.

Currently Enrolled Resources				
ResName1	ResName2	ResName3	Use In Selection	Link
UGADGEN1.Administration.[ROOT]	NOVELADM	Novell4	1/4 25%	<input checked="" type="checkbox"/> <input type="text"/>
UGMPBR	RACFPDOD	RACF22	1/4 25%	<input checked="" type="checkbox"/> <input type="text"/>
e-mail	outlook	WinNT	2/4 50%	<input checked="" type="checkbox"/> <input type="text"/>
office2003	2003	WinNT	2/4 50%	<input checked="" type="checkbox"/> <input type="text"/>

Proposed Resources				

Other Resources				
ResName1	ResName2	ResName3	Link	
BRLIMSYS	RACFPDOD	RACF22	<input checked="" type="checkbox"/>	<input type="text"/>

- Click *OK*. The requests are saved and window closes.

3.3.6 Request Role Privileges for Myself

Use the *Request Roles for Myself* workform to request access rights to roles that you require.

This form is a Self Service form and requires you to set the *Configuration* and *AuditCard* parameters in the *Self Service Settings* page before using the workform. If you open the workform without assigning the parameters an error message is displayed.

Eurekify Sage Portal Info:
V3.2, 07.09.23.02
EYALLAP\Eyal

Error

This self service was not defined yet. Please refer to a Eurekify administrator

See section 2.8 *Self Service Settings* for details.

To request role privileges for your own use:

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request Role Privileges for Myself* link. The *Request Roles for Myself* window opens.

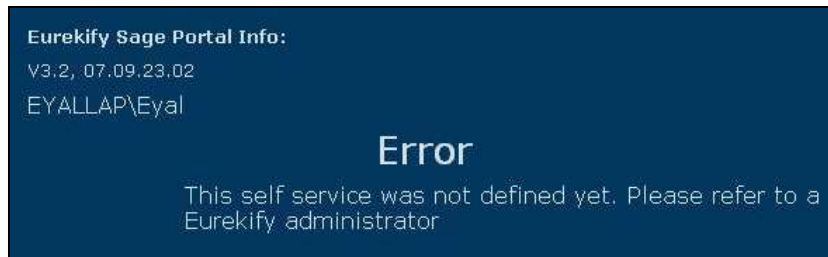
All	Person ID	User ID	User Name	Org	Org Type
<input checked="" type="checkbox"/>	54672910	3	Cooper Amos	IT Security	Corporate

2. Select your Person ID from the *Value* drop down list.
3. Click *Get Users*, your user details are displayed in the Users list.
4. Click *Get Roles*, the list of roles is displayed.
5. Select the check box in the Link column for any role that you want to request for yourself.
6. Click *OK*. A confirmation message is displayed indicating that the requests were submitted. Click *OK*, the message closes.

3.3.7 Request Resource Privileges for Myself

Use the *Request Resources for Myself* workform to request access rights to resources that you require.

This form is a Self Service form and requires you to set the *Configuration* and *AuditCard* parameters in the *Self Service Settings* page before using the workform. If you open the workform without assigning the parameters, an error message is displayed.



See section 2.8 *Self Service Settings* for details.

To request resource privileges for your own use:

1. From the *Business Collaboration* module select the *User Management* Folder, and then click the *Request Resource Privileges for Myself* link. The *Request Roles for Myself* window opens.

Request Resources For Myself

Please select your Person ID:

PersonID Value: 87635420

Users

All	Person ID	User ID	User Name	Org	Org Type
<input checked="" type="checkbox"/>	87635420	35	Bell Kim	Marketing_Dept.	Corporate

2. Select your Person ID from the *Value* drop down list.
3. Click *Get Users*, your user details are displayed in the Users list and the list of available resources is displayed.

Request Resources For Myself

Configuration: Audit Card:
PersonID: Value:

Users

All	Person ID	User ID	User Name	Org	Org Type
<input checked="" type="checkbox"/>	57644540	4	Alex Patrick	Application Development	Corporate

Currently Enrolled Resources

ResName1	ResName2	ResName3	Use In Selection	Link
DEVELOP	RACFPDOD	RACF22	1/1 100%	<input checked="" type="checkbox"/> <input type="text"/>
DEVELOP	RACFTEST	RACF22	1/1 100%	<input checked="" type="checkbox"/> <input type="text"/>
TESTDEV	RACFPDOD	RACF22	1/1 100%	<input checked="" type="checkbox"/> <input type="text"/>
TESTDEV	RACFTEST	RACF22	1/1 100%	<input checked="" type="checkbox"/> <input type="text"/>

- Expand the resource trees to view the available resources.
- Select the check box in the *Link* column for any resource that you want to request for yourself.
- Click *OK*. A confirmation message is displayed indicating that the requests were submitted. Click *OK*, the message closes.

3.3.8 User Privileges Certification Workform

The User Privileges Certification Workform provides business managers with the ability to certify the addition or removal of user access to roles and resources. Proposed and Suspected roles and resources are based on generated AuditCard alerts.

To certify the user access to roles and resources:

1. From the *Business Collaboration* module select the *User Management* Folder, and then click the *User Privileges Certification/Attestation* link. The *User Certification* window opens.
2. Click the *Settings* tab to bring it forward.
3. Choose the settings to match your requirements. Either select a *Campaign* or select a combination of *Audit Card*, *Category* and *Value* options from their respective drop down lists.
4. Click *OK* to return to the Main tab.
5. Select a Manager ID from the *Manager ID* drop down list and click Get Users. A list of users that match the selected parameters is displayed. The list indicates the number of proposed and suspected proposed and suspected connections for each user.

UserName	PersonID	Org	Org Type	Country	Location	Auditcard Status	
+ Atek Rogers	87623490	Fifth Ave Branch	Branches	US	New York	Proposed Connections: 1	Approved <input checked="" type="checkbox"/>
+ Deer Alex	91238730	Fifth Ave Branch	Branches	US	New York	Proposed Connections: 1	Please Review <input checked="" type="checkbox"/>
+ Eagle Richard	76329130	Fifth Ave Branch	Branches	US	New York	Suspected Connections: 4; Proposed Connections: 2	Changes Requested(3) <input checked="" type="checkbox"/>
+ German Tom	94738470	Fifth Ave Branch	Branches	US	New York	Suspected Connections: 8; Proposed Connections: 2	Changes Requested(1) <input checked="" type="checkbox"/>
+ Hill Gary	82653450	Fifth Ave Branch	Branches	US	New York	Suspected Connections: 2; Proposed Connections: 1	Please Review <input checked="" type="checkbox"/>
+ Hill Silver	89213478	Fifth Ave Branch	Branches	US	New York	Proposed Connections: 1	Please Review <input checked="" type="checkbox"/>
+ Mills Robert	84774660	Fifth Ave Branch	Branches	US	New York	Proposed Connections: 1	Please Review <input checked="" type="checkbox"/>
+ Purple Mary	67762440	Fifth Ave Branch	Branches	US	New York	Suspected Connections: 5; Proposed Connections: 1	Approved <input checked="" type="checkbox"/>
+ Saven Werner	87473220	Fifth Ave Branch	Branches	US	New York	Proposed Connections: 1	Please Review <input checked="" type="checkbox"/>

Figure 29 User Privileges Certification Workform-Populated

The table at the end of this section lists the types of information, their values and provides a description for the information included in the User Privileges Certification list.

- Click the +symbol next to a *UserName* to expand the Users privileges tree and view the privileges to review. The user tree now shows the user privileges divided according to their type. These are Role, Resources, Related Roles, Related Resources and User Alerts.

+ Deer Alex	91238730	Fifth Ave Branch	Branches US	New York	16	Please Review	<input checked="" type="checkbox"/>
- Eagle Richard	76329130	Fifth Ave Branch	Branches US	New York	3	25 Please Review	<input checked="" type="checkbox"/>
Title:Branch Officer/Clerk Cost Center:22321 Version:0							
+ Roles - 7 (1) + Resources - 7 (2) + Related Roles - 15 + Related Resources - 10 + User Alerts - 0							
+ German Tom	94738470	Fifth Ave Branch	Branches US	New York	7	15 Incomplete(5)	<input checked="" type="checkbox"/>

- Click the +symbol next to the Roles node to expand the node and view the roles on the privileges tree. Roles with either Suspected or Proposed Connections are indicated by Red text that appears in the Audit Card Status column. Use the Audit Card status information as additional tool in deciding whether to Remove or Approve the User’s access rights to the role.

Roles - 7 (1)							
Name	Description	Link Type	Audit Card Status	History	Remove All	Approve All	Comment
BASIC ROLE	New Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
Organization - Fifth Ave Branch	Characteristic Role (80%)	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
Title - Branch Officer/Clerk	Characteristic Role (50%)	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
UGTEL5AVE	Automation & document management	Direct	*Suspect User-Role Connection By Privileges (Score:30 Status: Suspected);	Suspected Violation 7/10/2007 6:06:52 PM	<input type="checkbox"/>	<input type="checkbox"/>	
TS176J1	Sage Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
B5AVEMGR	Sage Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
B5AVEJ1	Sage Role	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
+ Resources - 7 (2) + Related Roles - 15 + Related Resources - 10 - User Alerts - 0 (None)							

- To remove a role, mark the check box in the *Remove* column. To approve a role, mark the check box in the *Approve* column. After you mark a check box a text field appears in the comment column for you to enter comments. You must indicate whether you want to approve or Remove each and every role.
- Click the +symbol next to the *Resources* node to expand the node and view the user’s resources. Mark either the Approve or Remove check box for each and every resource. Again you can use the Audit Card Status alert as to help make a decision.
- Similarly, expand the *Related Roles* and the *Related Resources* nodes. These nodes list potential roles and resources that can be provided to the User. The content of the lists is extracted from the results based on the Audits performed on the configuration. To provide access rights to the related roles or related resources mark the check box in the Add column.
- Collapse all the nodes and click the *Review Confirmation* check mark at the end of the row to submit your changes.

3.3.8.1 Operation Area Data

The operational area displays data for each user that is divided into the following categories:

- User Information
- Roles
- Resources
- Related Roles
- Related Resources

The table lists the data types that are displayed for each category and provides a brief description on each data type.

Information Type	Value	Description
User Information	UserName	The name of the User
	PersonID	A unique employee ID as taken from the configuration file.
	Org	Lists the name of the Organization to which the User belongs, as taken from the configuration file
	Org Type	Lists the Organization Type with which the user is associated, as taken from the configuration file.
	Country	Lists the Country in which the user is located, as taken from the configuration file.
	Location	Lists the area in which the user is located, as taken from the configuration file.
	AuditCard Status	List the number and type of AuditCard exceptions associated with the User. These are divided between 3 columns: Suspected Users, Suspected Connections and Proposed Connections.
Roles	Name	The name of the Role
	Description	The Role description
	Link Type	Lists the way in which the User is connected to the specific role. For example Role-Based
	AuditCard Status	Audit codes that explain the reason that the system has designated the record as suspicious.

Information Type	Value	Description
	History	Indicates the date and time of the previous request for the role.
	Remove	Select the Remove check box to indicate whether you want the link to the Suspected role removed from the user. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate whether you want the link to the Proposed role provided for the user. After selecting the Approve check box an edit field appears to the right of the check box for entering comments.
Resources	Name1 Name2 Name3	Name1, Name2, Name3 should correspond to the format of other resources in the Resources Database. Res Name 1, Res Name 2 and Res Name 3 become key fields.
	Manager ID-Owner	Lists the name of the entity to which the resource belongs.
	Link Type	Lists the way in which the User is connected to the specific resource. For example Role-Based
	AuditCard Status	Audit codes that explain the reason that the system has designated the record as suspicious.
	History	Indicates the date and time of the previous request for the role.
	Remove	Select the Remove check box to indicate whether you want the link to the Suspected resource removed from the user. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate whether you want the link to the Proposed resource removed from the user. After selecting the Approve check box an edit field appears to the right of the check box for entering comments.

<i>Information Type</i>	<i>Value</i>	<i>Description</i>
Related Roles	Name	The Name column lists the name of the role that is being proposed as a potential connection for the selected user, based on the results of the Audit.
	Status	The Status column indicates the stage in the Audit workflow that the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected. The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.
	Score	Represents the relative degree to which the role is suitable for the User based on a comparison between the role identified by this alert, and other roles identified by all other alerts of the same type. A role with a score of 50 is more suited than a role with a score of 10.
	Type	The Type column lists the name of the Audit Code that indicates the reason for identifying the role as a potential role for the selected user.
	Alert Description	Displays the text entered in the Description column in the Audit Card from which the Alert was generated.
	Add	Select the Add check box to indicate whether you want the link to the Suspected role added for the selected User. After selecting the Add check box an edit field appears to the right of the check box for entering comments.
Related Resources	Name1 Name2 Name3	The name of a resource that is being proposed as a potential resource for the selected user.

<i>Information Type</i>	<i>Value</i>	<i>Description</i>
	Status	<p>The Status column indicates the stage in the Audit workflow that the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected.</p> <p>The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.</p>
	Score	<p>Represents the relative degree to which the resource is suitable for the User based on a comparison between the resource identified by this alert, and other resources identified by all other alerts of the same type.</p> <p>A role with a score of 50 is more suited than a role with a score of 10.</p>
	Type	<p>Lists the name of the Audit Code for the alert which indicates the reason for identifying the role for potential use by the selected user.</p>
	Alert Description	<p>Displays the text as entered in the Description column in the Audit Card from which the Alert was generated.</p>
	Add	<p>Select the Add check box to indicate whether you want the link to the Suspected role added for the selected User.</p> <p>After selecting the Add check box an edit field appears to the right of the check box for entering comments.</p>

3.4 Role Management

The Role Definitions and Approval folder contains workforms that give you the capability to:

- View a configuration's roles filtered according to Role Categories as they appear in the Role Panel in the selected configuration file.
- Focus on exceptions as identified by audit card alerts.
- Approve or reject links to roles by users, resources, parent roles, Sub-roles, Subsumed roles, and related entities.
- Propose changes

The Role Definitions and Approval folder contains the following workforms:

- Role Approval

3.4.1 Request a New Role Definition

Use the Request a New Role Definition to supply the details of a new role to be added to a configuration. Details for a new role definition include

- User values for the configuration attributes
- Roles to assign the user
- Resources to assign the user

To request a new role definition:

1. From the Business Collaboration module select the Role Management Folder, and then click the Request a New Role Definition link.
2. Click the Settings tab to bring it forward.
3. From the Configuration drop down list select the configuration that you want to request a new role definition for, and then click OK. The Main tab opens displaying a text field for each role attribute in the selected configuration.

4. Enter the appropriate values for the new role definition in each of the text fields. Fields marked with an asterisk are mandatory. If you do not know the correct value for a given field click the *Find* button to open a window displaying the range of values available for the selected attribute. Select the value and click *OK* to enter the value in the attribute text field.
5. Click the *OK* button, the Request Modification to Existing Role Definition window opens. Review the details for the new role definition request.

6. Click *Edit* to open the Edit Role Definition window and modify the role definition details. Click the *OK* button to save changes and return to the Request Modification to Existing Role Definition window.
7. Now add Users to the Role Definition. Click the *Select to Add* button next to the Actual Users section just below the user details table. The Find Users window opens.
8. Enter user details in the filter text fields and click *Select*. A table of users matching the search details is displayed.
9. Mark the check box next to the user that you want to add to the Role Definition and then click *OK*. The selected user is added to the list of Requested Users for the Role Definition.

Role details for MPHR (on request) Edit

Role Name	MPHR
Description	
Organization	
Owner	
Type	
Create Date	
Reviewer	
Approve Code	
Approve Date	
Filter	
Organization2	
Organization3	
Expiration Date	

Actual Users - none Select To Add

Person ID	User Name	Type	Description	Remove
99883134	Ron Mark	Add	Add user to role	<input type="checkbox"/>

Actual Resources - none Select To Add

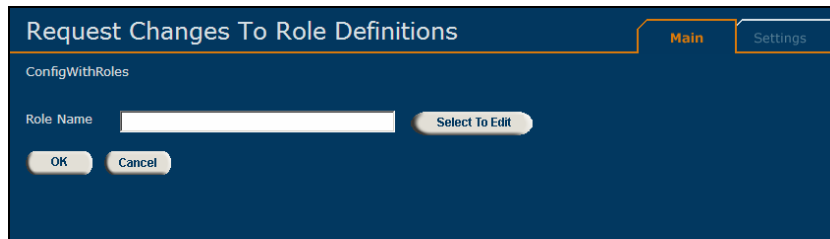
10. Now add Resources to the Role Definition. Click the *Select to Add* button next to the *Actual Resources* section just below the user details table. The *Find Resources* window opens.
11. Enter resource details in the filter text fields and click *Select*. A table of resources matching the search details is displayed.
12. Mark the check box next to the resource that you want to add to the Role Definition and then click *OK*. The selected resource is added to the list of *Requested Resources* for the Role Definition.
13. In a similar fashion add Parent Roles and Sub Roles to the Role definition as required.
14. The request for a new role definition should now include Role details, a list of Users and a list of Resources, a list of Parent Roles and Sub Roles. Click *OK*. The window is closed and the request for a new role definition is stored for review and approval.

3.4.2 Request Changes to a Role Definition

Use the Request Changes to a Role Definition workflow to modify the details of an existing role.

To request changes to a Role Definition:

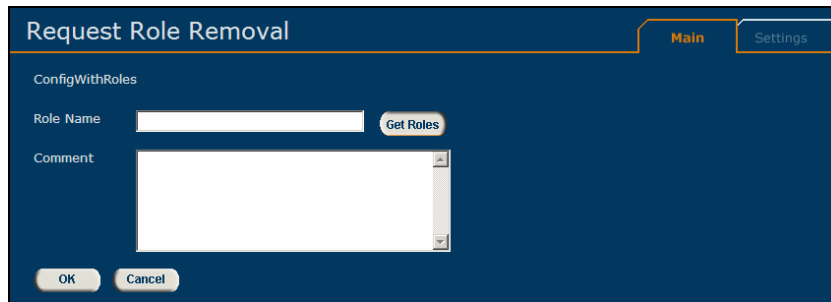
1. From the *Business Collaboration* module select the *User Management* Folder, and then click the *Request Changes to a Role Definition* link.
2. Click the *Settings* tab to bring it forward.
3. From the *Configuration* drop down list select the configuration that the Role Definition belongs to and then click *OK*. The Main tab opens.



4. Enter the *Role Name* in the text field for the Role that you want to change.
5. If you do not know the *Role Name* click *Select to Edit* to search for the Role Name. The *Find Role* window opens.
6. Enter search strings in the *Find Role* fields and click *Select*. A list of Roles matching the search string is displayed.
7. Select the check box next to the Role for which you want to change the definition and click *OK*. The name for the selected Role is loaded into the Role Name text field.
8. Click *OK*. The *Request Modification to Existing Role Definition* window opens and displays the details for the selected role.
9. Modify the Role details in the *Request Modification to Existing Role Definition* window by clicking *Edit*, changing the details in the *Edit Role Definitions* window. Click *OK* to save your changes and return to the *Request Modification to Existing Role Definition* window.
10. To add a user/resource to the *Requested User/Resource* list click the *Select to Add* button adjacent to the *Actual Users* or the *Actual Resource* list. Use the *Find User/Resource* window to identify users or resources that match a search string and click select to display matching users or resources. Similarly perform the same actions to add a Parent Role or Sub-Role.
11. Select a user/resource from the list and click *OK*. The selected user/resource is added to the Requested User/Resource list.
12. To remove a user or resource from the Role Definition, select the check box in the user's or resources' *Remove* column and click the *OK* button. The request is saved and the window is closed.

3.4.3 Request Removal of a Role Definition

1. From the *Business Collaboration* module select the *User Management Folder*, and then click the *Request Removal of a Role Definition* link. The *Request Role Removal* window opens.
2. Click the *Settings* tab to bring it forward.
3. From the *Configuration* drop down list select the configuration that User Definition belongs to and then click *OK*. The *Main* tab opens.



4. In the *Role Name* text field, enter the Role Name for the Role Definition that you want to remove from the configuration.
5. If you do not know the Role Name, click *Get Roles*. The *Find Roles* window opens.
6. Enter search strings in the *Find Roles* fields and click *Select*. A list of Roles matching the search string is displayed.
7. Select the check box next to the Role that you want to remove and click *OK*. The role name for the selected Role is loaded into the *Role Name* text field.
8. You can add a comment in the Comment field if required.
9. Click *OK*. The request to remove the Role Definition is saved.

3.4.4 Role Definitions Certification/Attestation

The Role Definitions Certification/Attestation workflow provides business managers with the ability to certify the addition or removal of user and resource connections to roles. Proposed and Suspected roles and resources are based on generated AuditCard alerts.

To certify the user access to roles and resources:

1. From the *Business Collaboration* module select the *Role Management* Folder, and then click the *Role Definitions Certification/Attestation* link. The *Role Approval* window opens.
2. Click the *Settings* tab to bring it forward.
3. Choose the settings to match your requirements. Either select a Campaign or select a combination of Audit Card, Category and Value options from their respective drop down lists.
4. Click *OK* to return to the Main tab.
5. Select an item from the *Role Category* drop down list and click *Get Role*. A list of Roles that match the selected parameters is displayed. The list indicates if the role is suspected and the number of proposed and suspected connections for each role.

RoleName	Description	Organization	Owner	Type	Susp. Role	Susp. Conn.	Prop. Conn.	
+ Development	Automation & document management	Production	77371120	Org Role		2	44	Please Review <input checked="" type="checkbox"/>
+ Organization - Application Development	Characteristic Role (80%)	Application Development	57644540		Suspected	9	45	Please Review <input checked="" type="checkbox"/>
+ Organization - Purchasing	Characteristic Role (80%)	Purchasing	82922230			3	2	Please Review <input checked="" type="checkbox"/>
+ Organization - Silicon Valley Branch	Characteristic Role (80%)	Silicon Valley Branch	93872110			4	19	Please Review <input checked="" type="checkbox"/>
+ Organization - Stamford Branch	Characteristic Role (80%)	Stamford Branch	82922230			4	18	Please Review <input checked="" type="checkbox"/>
+ Organization - System Management	Characteristic Role (80%)	System Management	45489940		Suspected	8	43	Please Review <input checked="" type="checkbox"/>
+ Title - Accountant	Characteristic Role (50%)	Title - Accountant	91724340			4	48	Please Review <input checked="" type="checkbox"/>
+ Title - Branch Manager	Characteristic Role (50%)	Title - Branch Manager	67762440			5	23	Please Review <input checked="" type="checkbox"/>
+ Title - Branch Officer/Clerk	Characteristic Role (50%)	Title - Branch Officer/Clerk	67762440		Suspected	3	14	Please Review <input checked="" type="checkbox"/>

Figure 30 Role Approval Workflow

The table at the end of this section lists the types of information, their values and provides a description of the information included in the *Role Approval* list.

- Click the +symbol next to a RoleName to expand the Role privileges tree and view the connections to review. The Role tree now shows the role connections divided according to their type. These are Current Resources, Current Parent Roles, Current Sub-Roles, Related Users, Related Resources, Related Parent Roles, Related Sub-Roles, Subsumed Roles, and Role Alerts.

RoleName	Description	Organization	Owner	Type	Susp. Role	Susp. Conn.	Prop. Conn.				
- Development	Automation & document management	Production	77371120	Org Role		2	44	Please Review <input checked="" type="checkbox"/>			
- Current Users (4)											
Name	Person ID	Organization	Org Type	Country	Location	Link Type	AuditCard Status	History	Remove All	Approve All	Comment
Alex Patrick	57644540	Application Development	Corporate	US	Pennsylvania	Direct		Request to approve 9/11/2007 11:17:46 AM	<input type="checkbox"/>	<input type="checkbox"/>	
Keren Cindy	77292450	Application Development	Corporate	US	Pennsylvania	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
poster Jillian	94362210	Application Development	Corporate	US	Pennsylvania	Direct		Show History	<input type="checkbox"/>	<input type="checkbox"/>	
Capel Linda	98383830	Application Development	Corporate	US	Pennsylvania	Direct	*Suspect User-Role Connection By Privileges (Score:22 Status:Suspected);	Suspected Violation 9/11/2007 1:08:54 PM	<input type="checkbox"/>	<input type="checkbox"/>	
+ Current Resources (7)											
+ Current Parent Roles (0)											
+ Current Sub-Roles (0)											
+ Related Users (44)											
+ Related Resources (0)											
+ Related Parent Roles (0)											

- Click the +symbol next to a Role node to expand the node and view the roles on the roles tree. Roles with either Suspected or Proposed Connections are indicated by Red text that appears in the Audit Card Status column. Use the Audit Card status information as additional tool in deciding whether to Remove or Approve the User's access rights to the role.

8. To remove a user or role-connection, mark the check box in the Remove column. To approve a user or role-connection, mark the check box in the Approve column. After you mark a check box a text field appears in the comment column for you to enter comments. You must indicate whether you want to Approve or Remove each and every entry. Repeat this process for each entry in each node in the tree.
9. Click the +symbol next to the Resources node to expand the node and view the user's resources. Mark either the Approve or Remove check box for each and every resource. Again you can use the Audit Card Status alert as to help make a decision.
10. Similarly, expand the Related Users, Related Resources and remaining Related nodes. These nodes list potential users and resources that can be connected to the role. The content of the lists is extracted from the results of Audits performed on the configuration. To provide access rights to the related users or related resources mark the check box in the Add column.
11. Collapse all the nodes and click the Review Confirmation check mark at the end of the row to submit your changes.

The table list the information presented in the Operation Area of the main tab and provides a brief description for each type.

Information Type	Value	Description
Role	RoleName	The name of the Role
	Description	A unique employee ID as taken from the configuration file.
	Org	Lists the name of the Organization to which the Role belongs, as taken from the configuration file.
	Owner	Lists the name of the role owner, as taken from the configuration file.
	Type	Lists the Role Type as taken from Type column in the configuration file.
	AuditCard Status	List the number and type of AuditCard exceptions associated with the Role. This is divided into 3 columns as follows; Suspected Role, Suspected Connections, Proposed Connections.
	Review	Click the check mark to indicate that the Role has been reviewed and the amendments can be viewed by the role engineer.
Current Users	Name	The name of the User that is linked to the role
	Person ID	A unique employee ID as taken from the configuration file.
	Organization	Lists the name of the Organization to which the User belongs, as taken from the configuration file

Information Type	Value	Description
	Org Type	Lists the Organization Type with which the user is associated, as taken from the configuration file.
	Location	Indicates the office or region to which the user is assigned.
	Link Type	The way in which the User and is linked to the Role. Direct, Indirect or Dual.
	Audit Card Status	List the number and type of AuditCard exceptions identified between the User and the Role.
	History	Indicates when the most recent request was made with respect to the role.
	Remove	Select the Remove check box to indicate whether you want the link to the current user removed. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate whether you want to create a link to the current user. After selecting the Approve check box an edit field appears to the right of the check box for entering comments.
Current Resources	Name1 Name2 Name3	Name1, Name2, Name3 corresponds to the format of other resources in the Resources Database. Res Name 1, Res Name 2 and Res Name 3 become key fields.
	Link Type	Lists the way in which the Resource is connected to the specific role. For example Direct or Indirect
	AuditCard Status	Audit codes that explain the reason that the system has designated the record as suspicious.
	History	Indicates when the most recent request was made with respect to the role.
	Remove	Select the Remove check box to indicate whether you want the link to the current resource. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.

Information Type	Value	Description
	Approve	Select the Approve check box to indicate whether you want to create a link to the current resource. After selecting the Approve check box an edit field appears to the right of the check box for entering comments.
Current Parent Roles	Name	The name of the Role
	Description	The Role description
	Link Type	Lists the way in which the Parent Role is connected to the specific role. For example Direct or Indirect
	AuditCard Status	Audit codes that explain the reason that the system has designated the record as suspicious.
	Remove	Select the Remove check box to indicate whether you want the link to the Suspected role. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate whether you want to create a link to the proposed role. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
Current Sub Roles	Name	The name of the Role
	Description	The Role description
	Link Type	Lists the way in which the Sub Role is connected to the specific role. For example Direct or Indirect
	Audit Card Status	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.

Information Type	Value	Description
	Remove	Select the Remove check box to indicate whether you want the link to the Suspected role removed. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate whether you want to create a link to the proposed role. After selecting the Remove check box an edit field appears to the right of the check box for entering comments
Related Users	UserName	The name of the User
	Status	The Status column indicates the stage in the Audit workflow that the Alert is currently located.
	Score	The value in the Score field provides a relative indication as to the severity of the audit card alert, compared to all other audit card alerts. A score of a very high value would warrant a higher priority than a score with a very low value.
	Type	Displays the Audit Code listed in the Audit Card for the Role.
	Audit Card Status	Lists the Audit codes that explain the reason that the system has designated the record as suspicious
	Add	Select the check box to indicate you want to create a link to the proposed used.
Related Resources	Name1 Name2 Name3	Name1, Name2, Name3 corresponds to the format of other resources in the Resources Database. Res Name 1, Res Name 2 and Res Name 3 become key fields.

<i>Information Type</i>	<i>Value</i>	<i>Description</i>
	Status	The Status column indicates the stage in the Audit workflow that the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected. The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.
	Score	The value in the Score field provides a relative indication as to the severity of the audit card alert, compared to all other audit card alerts. A score of a very high value would warrant a higher priority than a score with a very low value.
	Type	Displays the Audit Code listed in the Audit Card for the Role.
	AuditCard Status	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.
	Add	Select the Add check box to indicate whether you want the link to the Suspected resource to be added to the selected Role. After selecting the Add check box an edit field appears to the right of the check box for entering comments.
Related Parent Roles	Name	The name of the Role
	Description	The Role description
	AuditCard Status	Indicates the stage in the Audit workflow in which the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected. The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.
	Link Type	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.

Information Type	Value	Description
	Add	Select the Add check box to indicate whether you want the link to the Suspected resource to be added to the selected Role. After selecting the Add check box an edit field appears to the right of the check box for entering comments.
Related Sub Roles	Name	The name of the Role
	Description	The Role description as taken from the configuration file.
	AuditCard Status	Indicates the stage in the Audit workflow in which the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected. The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.
	Link Type	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.
	Add	Select the Add check box to indicate whether you want the link to the Suspected resource to be added to the selected Role. After selecting the Add check box an edit field appears to the right of the check box for entering comments.
Subsumed Roles	Role Name	The name of the Role
	Description	The Role description as taken from the configuration file.
	AuditCard Status	Indicates the stage in the Audit workflow in which the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected. The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.

3.5 Resource Approval

The Resource Approval folder contains workforms that give you the capability to:

- View a configuration's resources filtered according to Resource Categories as they appear in the Resource Panel in the selected configuration file.
- Focus on exceptions as identified by audit card alerts.
- Approve or reject links to resources by users, roles, and related entities.
- Propose changes

The Resource Approval folder contains the following workforms:

- Resource Approval

3.5.1 Request a New Resource Definition

Use the Request a New Resource Definition to supply the details of a new resource to be added to a configuration. Details for a new resource definition include:

- User values for the configuration attributes
- Resource Names
- Manager ID-Owner
- Organization
- Location

To request a new role definition:

1. From the *Business Collaboration* module select the *Resource Management* folder, and then click the *Request a New Resource Definition* link.
2. Click the *Settings* tab to bring it forward.
3. From the *Configuration* drop down list select the configuration that you want to request a new resource definition for, and then click *OK*. The *Main* tab opens displaying a text field for each role attribute in the selected configuration.

4. Enter the appropriate values for the new resource definition in each of the text fields. Fields marked with an asterisk are mandatory. If you do not know the correct value for a given field click the *Find* button to open a window displaying the range of values available for the selected attribute. Select the value and click *OK* to enter the value in the attribute text field.
5. Click the *OK* button, the *Request Changes to Resource Definition* window opens. Review the details for the new resource definition request.

Res Name1	qqqq
Res Name2	www
Res Name3	eeee
Field1	
Field2	
Field3	
Field4	
Field5	
Field6	

6. Click *Edit* to open the *Edit Resource Definition* window and modify the resource definition details. Click the *OK* button to save changes and return to the *Request Changes to Resource Definition* window.
7. Now add Users to the Resource Definition. Click the *Select to Add* button next to the *Actual Users* section just below the user details table. The *Find Users* window opens.
8. Enter user details in the filter text fields and click *Select*. A table of users matching the search details is displayed.
9. Mark the check box next to the user that you want to add to the Resource Definition and then click *OK*. The selected user is added to the list of Requested Users for the Role Definition.

Request Changes To Resource Definition

Resource details for qqqq-www-eeee (on request) Edit

Res Name1	qqqq
Res Name2	www
Res Name3	eeee
Field1	
Field2	
Field3	
Field4	
Field5	
Field6	

Actual Users - none Select To Add

Requested Users

PersonID	User Name	Type	Description	Remove
98662230	Tortia Dan	Add	Add user to res	<input type="checkbox"/>

Actual Roles - none Select To Add

OK Cancel

10. Now add Roles to the Resource Definition. Click the *Select to Add* button next to the *Actual Resources* section just below the user details table. The *Find Roles* window opens.
11. Enter role details in the filter text fields and click *Select*. A table of roles matching the search details is displayed.
12. Mark the check box next to the role that you want to add to the Resource Definition and then click *OK*. The selected resource is added to the list of Requested Roles for the Resource Definition.
13. The request for a new resource definition should now include Resource details, a list of Users and a list of Roles. Click *OK*. The window is closed and the request for a new resource definition is stored for review and approval.

3.5.2 Request Changes to a Resource Definition

Use the Request Changes to a Resource Definition workflow to modify the details of an existing resource.

To request changes to a Resource Definition:

1. From the *Business Collaboration* module select the *Resource Management* folder, and then click the *Request Changes to a Resource Definition* link.
2. Click the *Settings* tab to bring it forward.
3. From the *Configuration* drop down list select the configuration that the Resource Definition belongs to and then click *OK*. The *Main* tab opens.

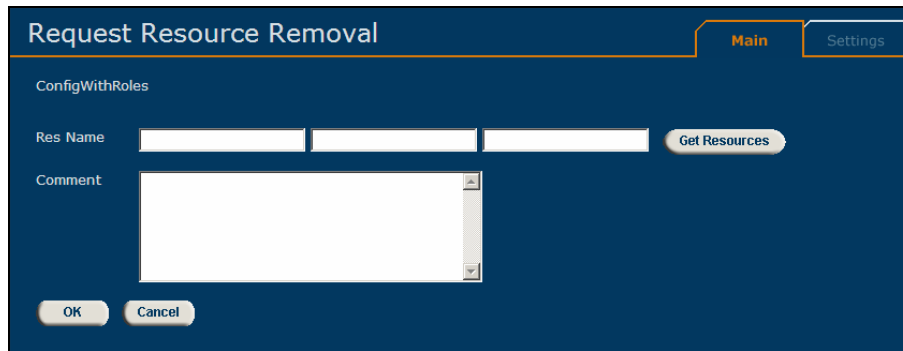
4. Enter the *Resource Name* in the text field for the resource that you want to change.
5. If you do not know the Resource Name click *Select to Edit* to search for the Resource Name. The *Find Resource* window opens.
6. Enter search strings in the *Find Resource* fields and click *Select*. A list of resources matching the search string is displayed.
7. Select the check box next to the resource for which you want to change the definition and click *OK*. The name for the selected resource is loaded into the *Resource Name* text field.
8. Click *OK*. The *Request Changes to Resource Definition* window opens and displays the details for the selected resource.
9. Modify the Resource details in the *Request Changes to Existing Resource Definition* window by clicking *Edit* and changing the details in the *Edit Resource Definitions* window. Click *OK* to save your changes and return to the *Request Changes to Resource Definition* window.
10. To add a user/role to the Requested User/Role list click the *Select to Add* button adjacent to the *Actual Users* or the *Actual Roles* list. Use the *Find User/Role* window to identify users or roles that match a search string, and then click *Select* to display matching users or roles.
11. Select a user/role from the list and click *OK*. The selected user/role is added to the *Requested User/Role* list.
12. To remove a user or role from the Resource Definition, select the check box in the user's or roles' *Remove* column and click the *OK* button. The request is saved and the window is closed.

3.5.3 Request Removal of a Resource Definition

To request the removal of a resource definition:

1. From the *Business Collaboration* module select the *Resource Management* folder, and then click the *Request Removal of a Resource Definition* link. The *Request Resource Removal* window opens.
2. Click the *Settings* tab to bring it forward.

3. From the *Configuration* drop down list select the configuration that Resource Definition belongs to and then click *OK*. The Main tab opens.



The screenshot shows a dialog box titled "Request Resource Removal" with a dark blue background. At the top right, there are two tabs: "Main" (which is highlighted in orange) and "Settings". Below the tabs, the text "ConfigWithRoles" is visible. The main area contains three text input fields for "Res Name", a "Get Resources" button, and a larger text area for "Comment". At the bottom, there are "OK" and "Cancel" buttons.

4. In the *Resource Name* text field, enter the Name for the Resource Definition that you want to remove from the configuration.
5. If you do not know the resource name, click *Get Resources*. The *Find Resources* window opens.
6. Enter search strings in the *Find Resources* fields and click *Select*. A list of roles matching the search string is displayed.
7. Select the check box next to the resource that you want to remove and click *OK*. The name of the selected Resource is loaded into the *Resource Name* text field.
8. You can add a comment in the Comment field if required.
9. Click *OK*. The request to remove the Resource Definition is saved.

3.5.4 Resource Access Certification/Attestation

The Resource Approval workflow provides business managers with the ability to certify the addition or removal of user and role connections to resources. Proposed and Suspected connections to users and roles are based on generated AuditCard alerts.

To certify the user access to resources:

1. From the *Business Collaboration* module select the *Resource Management* folder, and then click the *Resource Access Certification/Attestation* link. The *Resource Approval* window opens.
2. Click the *Settings* tab to bring it forward.
3. Choose the settings to match your requirements. Either select a *Campaign* or select a combination of *Configuration*, *Audit Card*, and *Category* options from their respective drop down lists.
4. Click *OK* to return to the *Main* tab.
5. Select an item from the *Resource Category* drop down list and click *Get Resources*. A list of Resources that match the selected parameter is displayed. The list indicates if the resource is suspected and the number of proposed and suspected connections for each resource.

Name1	Name2	Name3	ManagerID-Owner	Organization	Susp. Res.	Susp. Conn.	Prop. Conn.	
+ appldev	UNXMARKT	Solaris26	89123140	Marketing Sun Server			21	Please Review <input checked="" type="checkbox"/>
+ public	UNXMARKT	Solaris26	89123140	Marketing Sun Server	15	20		Please Review <input checked="" type="checkbox"/>
+ purchase	UNXMARKT	Solaris26	89123140	Marketing Sun Server				Please Review <input checked="" type="checkbox"/>
+ root	UNXMARKT	Solaris26	89123140	Marketing Sun Server				Please Review <input checked="" type="checkbox"/>
+ secmgr	UNXMARKT	Solaris26	89123140	Marketing Sun Server			24	Please Review <input checked="" type="checkbox"/>
+ ucisdev	UNXMARKT	Solaris26	89123140	Marketing Sun Server				Please Review <input checked="" type="checkbox"/>
+ ucismgr	UNXMARKT	Solaris26	89123140	Marketing Sun Server				Please Review <input checked="" type="checkbox"/>
+ ucisusr	UNXMARKT	Solaris26	89123140	Marketing Sun Server	3	23		Please Review <input checked="" type="checkbox"/>
+ ugrkdba	UNXMARKT	Solaris26	89123140	Marketing Sun Server	4	21		Please Review <input checked="" type="checkbox"/>

Figure 31 Resource Approval Workform

The table at the end of this section lists the types of information, their values and provides a description of the information included in the Resource Approval list.

6. Click the +symbol next to a ResourceName to expand the Resource privileges tree and view the connections to review. The Resource tree now shows the resource connections divided according to their type. These are Location, Users, Roles, Related Users, Related Roles, and Resource Alerts.

7. Click the +symbol next to a Users node to expand the node and view the connections on the resource tree. Resources with either Suspected or Proposed Connections are indicated by Red text that appears in the Audit Card Status columns. Use the Audit Card status information as an additional tool in deciding whether to Remove or Approve access rights to the resource.
8. To remove a user or role-connection, mark the check box in the Remove column. To approve a user or role-connection, mark the check box in the Approve column. After you mark a check box a text field appears in the comment column for you to enter comments. You must indicate whether you want to Approve or Remove each and every entry. Repeat this process for each entry in each node in the tree.
9. Click the +symbol next to the Roles node to expand the node and view the resource's roles. Mark either the Approve or Remove check box for each and every resource. Again you can use the Audit Card Status alert as to help make a decision.
10. Similarly, expand the Related Users and Related Roles nodes. These nodes list potential users and roles that can be connected to the resource. The content of the lists is extracted from the results of Audits performed on the configuration. To provide access rights to the related users or related roles mark the check box in the Add column.
11. Collapse all the nodes and click the Review Confirmation check mark at the end of the row to submit your changes.

The table lists the types of information presented in the Operation Area of the Main tab and provides a brief description for each type.

Information Type	Value	Description
Resources	Name1 Name2 Name3	Name1, Name2, Name3 corresponds to the format of other resources in the Resources Database. Res Name 1, Res Name 2 and Res Name 3 become key fields.
	Owner	Displays the name of the resource owner as taken from the roles panel in the configuration file.
	Organization	The name of the organization to which the resource is associated.
	AuditCard Status	Indicates the type and number of audit card alerts identified with the resource. This is divided into 3 columns: Suspected Resources, Suspected Connections and Proposed Connections.
Users	Person ID	A unique employee ID as taken from the configuration file.
	Name	The name of the User that is linked to the resource.

<i>Information Type</i>	<i>Value</i>	<i>Description</i>
	Org	Lists the name of the Organization to which the Resource belongs, as taken from the configuration file
	Org Type	Lists the Organization Type with which the resource is associated, as taken from the configuration file.
	Link Type	The way in which the user is linked to the Resource. Role-Based, Direct, Indirect or Dual.
	Audit Card Status	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.
	History	Indicates when the most recent request was made with respect to the resource.
	Remove	Select the Remove check box to indicate whether you want the link to the Suspected resource removed from the user. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate that you want the link to the Proposed connection approved for the user. After selecting the Approve check box an edit field appears to the right of the check box for entering comments.
Roles	Name	The name of the role
	Description	The Role description
	Link Type	The way in which the role is linked to the Resource. Role-Based, Direct, Indirect or Dual.
	Auditcard Status	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.
	History	Indicates when the most recent request was made with respect to the resource.

Information Type	Value	Description
	Remove	Select the Remove check box to indicate whether you want the link to the Suspected resource removed from the role. After selecting the Remove check box an edit field appears to the right of the check box for entering comments.
	Approve	Select the Approve check box to indicate that you want the link to the Proposed connection approved for the user. After selecting the Approve check box an edit field appears to the right of the check box for entering comments.
Related Users	UserName	The name of the User
	PersonID	A unique employee ID as taken from the configuration file.
	Status	The Status column indicates the stage in the Audit workflow that the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected. The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.
	Score	The value in the Score field provides a relative indication as to the severity of the audit card alert, compared to all other audit card alerts. A score of a very high value would warrant a higher priority than a score with a very low value.
	Type	Displays the Audit Code listed in the Audit Card for the Resource.
	Audit Card Status	Lists the Audit codes that explain the reason that the system has designated the record as suspicious.
	Add	Select the Add check box to indicate whether you want the link to the Suspected user to be added to the selected resource. After selecting the Add check box an edit field appears to the right of the check box for entering comments.

<i>Information Type</i>	<i>Value</i>	<i>Description</i>
Related Roles	Name	The name of the Role
	Status	<p>The Status column indicates the stage in the Audit workflow that the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected.</p> <p>The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.</p>
	Score	<p>The value in the Score field provides a relative indication as to the severity of the audit card alert, compared to all other audit card alerts.</p> <p>A score of a very high value would warrant a higher priority than a score with a very low value.</p>
	Type	Displays the Audit Code listed in the Audit Card for the Role.
	AuditCard Status	<p>Indicates the stage in the Audit workflow in which the Alert is currently located. When an audit card is first generated, all alerts are set by default as Suspected.</p> <p>The remaining Statuses are OK, Addressed and In Progress. These are set manually by the Role Engineer.</p>
	Add	<p>Select the Add check box to indicate whether you want the link to the Suspected resource to be added to the selected Role.</p> <p>After selecting the Add check box an edit field appears to the right of the check box for entering comments.</p>

3.6 Privileges Navigation and Browsing

The Privileges Navigation and Browsing folder contains workforms that give you the capability to view the details of Users, Roles and Resources:

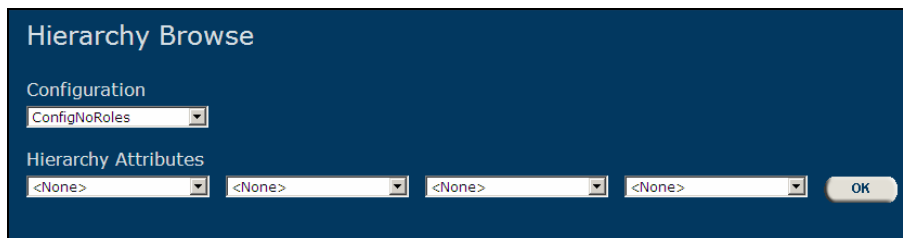
The Privileges Navigation and Browsing folder contains the following workforms:

- Navigate a Hierarchy to Browse.
- Browse User Privileges.
- Browse Role Privileges.
- Browse Resource Privileges.

3.6.1 Navigate a Hierarchy to Browse

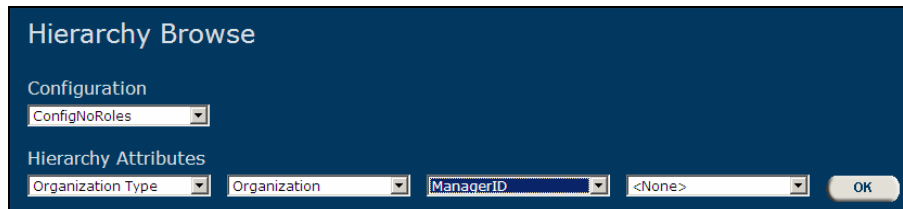
To navigate a hierarchy to browse:

1. From the *Business Collaboration* module select the *Privileges Navigation and Browsing* folder, and then click the *Navigate a Hierarchy to Browse* link. The *Hierarchy to Browse* window opens.



The screenshot shows the 'Hierarchy Browse' window. It has a dark blue header with the title 'Hierarchy Browse'. Below the header, there are two sections: 'Configuration' and 'Hierarchy Attributes'. The 'Configuration' section has a dropdown menu currently set to 'ConfigNoRoles'. The 'Hierarchy Attributes' section has four dropdown menus, all currently set to '<None>', followed by an 'OK' button.

2. Select a *Configuration* from the *Configuration* drop down list box.
3. From the *Hierarchy Attributes* drop down lists, moving from left to right, select a series of attributes that describes the hierarchy that you want to browse. For example Organization Type, Organization, ManagerID.



The screenshot shows the 'Hierarchy Browse' window after selection. The 'Configuration' dropdown remains 'ConfigNoRoles'. In the 'Hierarchy Attributes' section, the first three dropdown menus are now selected: 'Organization Type', 'Organization', and 'ManagerID'. The fourth dropdown menu remains '<None>', and the 'OK' button is still present.

- Click *OK*. A Hierarchy tree appears and is structured according to your Hierarchy Attribute selection.

The screenshot shows a window titled "Hierarchy Browse" with a configuration section and a data table. The configuration includes "ConfigWithRoles" and "Hierarchy Attributes" with dropdowns for "Organization Type", "Organization", "ManagerID", and "<None>". The table below shows a hierarchy of organizations with columns for Organization Type, Organization, ManagerID, Users, Roles, and Resources.

Organization Type	Organization	ManagerID	Users	Roles	Resources
+ Organization Type			71	92	62
- Branches			22	27	19
- Fifth Ave Branch			10	11	9
		67762440	10	11	9
- Human Resources			1	0	0
		12345678	1	0	0
- Silicon Valley Branch			4	11	10
		97373330	4	11	10
+ Stamford Branch			7	13	12

- Click on an entity in the Hierarchy tree and window opens displaying a list of users that belong to the selected Hierarchy element.

The screenshot shows a web browser window with the URL "http://localhost/SagePortal/WorkformsWeb/Priv...". It displays a "Show Users per Page" control set to 15 and a "Refresh" button. Below this, it shows "Users 1-10 of 10" with navigation arrows. The main content is a table listing users with columns for Person ID and User Name.

Person ID	User Name
87623490	Atek Rogers
91238730	Deer Alex
76329130	Eagle Richard
94738470	German Tom
82653450	Hill Gary
89213478	Hill Silver
84774660	Mills Robert
67762440	Purple Mary
87473220	Saven Werner
89123470	Sharon Johnson

- Click on a User in the list and open the User Details window for that user.

3.6.2 Browse User Privileges

Use the Browse User Privileges workflow to view the user details for a specific User.

To browse for user privileges:

1. From the *Business Collaboration* module select the *Privileges Navigation and Browsing* folder, and then click the *Browse User Privileges* link. The *Find Users* window opens.
2. On the Settings tab select a configuration from the Configuration drop down list and click OK. The Main tab displays browsing fields for the selected configuration.
3. Select attributes for the configuration and enter search strings in adjacent the text fields.
4. Click Select and a list of Users matching the search strings are displayed.

The screenshot shows the 'Find Users' window with the 'Main' tab selected. The search criteria are as follows:

- Where: Contains and
- Where: Contains and
- Where: Contains

The results table is as follows:

Person ID	Name	Org	Org Type	Country	Location	Title	Cost Center
75675330	Davis Brett	Database Administrators	Corporate	US	Pennsylvania	DB Admin Manager	2,933,311,234
88311130	Goodman Bruce	Marketing_Dept.	Corporate	US	New Jersey	Marketing Manager	2,533,111,234
98732770	Brazil Bill	Application Development	Corporate	US	Pennsylvania	Developer	30111

5. Click the Person ID for any user on the list and the User details for that user is displayed.

3.6.3 Browse Role Privileges

Use the Browse Role Privileges workflow to view the details of a specific role.

To browse for role privileges:

1. From the *Business Collaboration* module select the *Privileges Navigation and Browsing* folder, and then click the *Browse Role Privileges* link. The *Find Roles* window opens.
2. On the Settings tab select a configuration from the Configuration drop down list and click OK. The Main tab displays browsing fields for the selected configuration.
3. Select attributes for the configuration and enter search strings in adjacent the text fields.
4. Click Select and a list of Roles matching the search strings are displayed.

5. Click a role name from within the list and the Role Details window opens.

3.6.4 Browse Resource Privileges

Use the Browse Resource Privileges workform to view the details of a specific resource.

To browse for role privileges:

1. From the Business Collaboration module select the Privileges Navigation and Browsing folder, and then click the Browse Resource Privileges link. The Find Resource window opens.
2. On the Settings tab select a configuration from the Configuration drop down list and click OK. The Main tab displays browsing fields for the selected configuration.
3. Select attributes for the configuration and enter search strings in adjacent the text fields.
4. Click Select and a list of Resources matching the search strings are displayed.
5. Click a resource name from within the list, and the Resource Details window opens.