Configuring Core Access

Release 9.1

Core Security SDI Corporation

1000 Holcomb Woods Parkway
Suite 401
Roswell, GA 30076
Phone: (678) 304-4500
Fax: (770) 573-3743

Trademarks

Contents

Chapter 1 - About Access Request Manager . . . 7

Access Keys . . . 8

Chapter 2 - About The Access Request Manager Workflows . . . 9

The Request and Approval WorkFlows . . . 10
Manage User Access . . . 12
Selecting Users . . . 12
Selecting Filters . . . 14
Categories . . . 14
Intelligent Modeling . . . 15
Tags . . . 15
Policy Violation Checking . . . 17
Approving a Request . . . 19
Viewing Request Details . . . 20

Chapter 3 - Configuring the Access Request Manager . . . 21

Configuring the Access Request Manager . . . 22
Getting Started with the Access Request Manager . . . 23
Authenticating in to the Access Assurance Portal . . . 23
Using Multi-Domain Authentication . . . 23
Overview of the Core Access Menu . . . 24
Access Menu . . . 25
Password Menu . . . 25
Admin Menu . . . 26
Configuration Menu . . . 26

Chapter 4 - Configuring Global Options . . . 27

Editing Global Options . . . 28
Editing Global Options with Config Type as Text . . . 28
Editing Global Options with Config Type as Complex . . . 28
Specifying Custom Macros in the Edit Complex Value Editor . . . 30
Adding Global Options to the GlobalConfigValues Table . . . 31
Grid Configuration . . . 31
Adding, Removing and Ordering of Fields in the Global Option . . . 32
Using Custom Macros in <column> Node . . . 32
Using the WordWrap Global Option . . . 32
Drop-Down Configuration . . . 33
Views Used in Global Options . . . 33
The vw_Role View . . . 33
The vw_Profile View . . . 34
The vw_Entitlement View . . . 37
The vw_Tag View . . . 38
The vw_Entitlement_Tag View . . . 38
The vw_Role_Tag View . . . 39
The vw_ManageAccessCatalog_Entitlement View . . . 39
The vw_ManagedUsersCurrentAccessDetails View . . . 40

Chapter 5 - Configuring Pick Lists . . . 43

Managing Pick lists . . . 44
Default Pick list Types and Values . . . 45
Adding a Pick List Value . . . 46

Chapter 6 - Configuring Access Items 47

Overview For Adding Access Items to the Access Catalog 48
Definitions of Access Terms 49
Adding a New Category 50
Adding a Grouping 51
Adding Information on the Definition Tab 51
Adding General Information About Grouping 51
Adding Definition and Access Approvers 52
Assigning Tags to Groupings 53
Adding Information on the Find Access Tab 54
Policy Violation Checking 55
Editing an Existing Grouping 57
Enabling or Disabling a Grouping 58
Adding Access Entitlements 59
Assigning Tags to Access Entitlements 62

Chapter 7 - Configuring the Manage Access Catalog 63

Configuring the Delete Button on Manage Access Catalog 64
Configuring Items on Groupings Tab 65
Configuring the Groupings Grid 65
Configuring the Search Tags Drop-down on Assign Tags Popup 66
Configuring Items on the Add/Modify Screen 66
Configuring the Advanced Search Grid To Search for Owners on Groupings Tab 66
Configuring the Owners or Approvers Drop-down on Groupings Tab 67
Configuring the Advanced Search Grid To Search for Approvers on Groupings Tab 67
Configuring the Search Tags Drop-down on Groupings Tab 67
Configuring the Tag Grid on Groupings Tab 68
Configuring the Search Users Drop-down on Find Access Tab 68
Configuring Advanced Search Grid for Intelligent Modeling on Find Access Tab 69
Configuring the Profile Grid for Intelligent Modeling 69
Configuring the Grouping Definition Grid 70
Configuring Items on Entitlements Tab 71
Configuring the Entitlements Grid 71

Chapter 8 - Configuring the Manage User Access Screen 73

Configuring Items for Selecting Recipients 74
Populating the Acting As Drop-Down List on Manage User Access 74
Configuring the Managed Users Drop-down on Users Tab 74
Configuring the Managed Users Grid With Recipient Information 74
Configuring the Grid for Grouping and Access Entitlement Details on Users Tab 75
Configuring the Advanced Search Grid on Users Tab 76
Configuring the Search Users Drop-down on Find Access Tab 76
Configuring the Profile Grid for Intelligent Modeling 77
Configuring the Advanced Search Grid on Find Access Tab 77
Configuring Access Items for Managing User Access 79
Configuring Items for Submitting the Request for Approval 80

Chapter 9 - Configuring the Approval Workflows 81

Adding Definition Approvers for Grouping Approval 82
Adding Access Approvers for Access Approval 83
Configuring the Approval Requests 84
Populating the Acting As Drop-Down List 84
Showing Pending Requests Based on Selection from Acting-As Drop-Down List 84
Enabling Delegatees to Approve Their Own Requests 84
Setting Up Fields for Pending Requests 85
Setting Up Fields for Request Details 85
Setting Up Fields To View Requester Details For All Request Types 85
Configuring Items for Grouping Definition 86
Setting Up Fields For the Grouping Characteristics Panel 86
Setting Up the Role Definition Grid 87
Configuring Items for Access Request 87
Setting Up Fields to View Recipient Details for Access Request 87

Enabling Editing of Access Entitlement Values for Access Request 88
Configuring the Access Grid 88
Configuring Items for Profile Request 89
Configuring the Approve and Deny Action Buttons 89
Approving New and Modified Groupings 90
Approving Requests 92

Chapter 10 - Using Macros 93

Adding a New Macro 94
Editing or Deleting an Existing Macro 96
Using Restriction Macros 97
Naming a Restriction Macro 97
Other Macros Used Within Restriction Macros 97
Restrictions Available On Manage Access Catalog 98
Restricting the Groupings Grid on Groupings Tab 98
Restricting the Access Entitlements Grid on Entitlements Tab 98
Restrictions on the Manage Access Catalog - Add/Modify 98
Restricting Profiles to Search for Grouping Owners on Groupings Tab 99
Restricting Profiles to Search for Approvers on Groupings Tab 99
Restricting Search for Tags on Groupings Tab 99
Restricting Search for Groupings on Find Access Tab 100
Restricting Search for Entitlements on Access Tab 100
Restricting Search for Profiles on Find Access Tab 100
Restricting Display of Groupings and Entitlements under Intelligent Modeling 101
Restrictions Available On Manage User Access 102
Restricting Search for Recipients on Users Tab 102
Restricting Display of Groupings and Entitlements on Users Tab 102
Restricting Search for Groupings on Access Tab 103
Restricting Search for Access Entitlements on Access Tab 103
Restricting Search for Profiles on Access Tab 104
Restricting Display of Groupings and Entitlements under Intelligent Modeling 104
Defining Filter Expressions in Restriction Macros 105
Using Custom Macros 110
Custom Macros for Manage Access Catalog 110
Show or Hide Groupings 110
Show or Hide Access Entitlements 110
Show or Hide Intelligent Modeling 110
Custom Macros for Manage User Access 111
Show or Hide Roles 111
Show or Hide Access Entitlements 111
Show or Hide Intelligent Modeling 111
Other Macros Used with Custom Macros 112
Retrieving the User ID of Logged in User 112
Retrieving the User ID of the Acting as User 112
Retrieving the User ID of the Delegator 112

Chapter 11 - Using Delegation 113

Delegating Your ARM Privileges 115
Delegating the Approvals 115
Withdrawing Delegation 116
Administrative Delegation of Approvals 117
Approving Delegated Requests 119
Checking for ARM Privileges Using Custom Macros 120
Custom Macros to check for ARM Privileges of a Delegator 120
Request Access 120
Manager Approval 120
Access Approval 121
Profile Approval 121
Using Restriction Macros for Delegation 122
Restriction on the Delegator Drop-Down Textbox for an Administrator 122
Restriction on the Delegator Advanced Search for an Administrator 122
Restriction on the Delegatee Drop-Down Textbox 122

Restriction on the Advanced Search Popup 122
Restriction on the History Tab 123
Using Global Options for Delegation 124
Hide or Show the Delegation - ARM Privileges Link 124
Specifying the Maximum Number of Days for Active Delegation 124
Customizing the Search Controls 124
Customizing the Drop-Down TextBoxes Using Global Options 124
Customizing the Advanced Search Using Global Options 125
Configuring the IsAccessDelegationDisabled Global Option 126

Chapter 12 - Disabling Access For Terminated Users 127

Configuring the Search Control Popup 127
Using the DisableUserSearchRestriction to Implement Restriction 128

Chapter 13 - Setting Up Email Notifications 129

Editing a Default Email Template 131

Chapter 14 - Customizing the Access Request Manager User Interface 133

Displayed Text in the Resource File 133
Customize Interface 135
Login 135
Navigation 136
Landing Page 137

Chapter 15 - Managing Access to the Access Request Manager Web Screens 139

Adding Communities and Entitlements 139
Communities and Entitlements in the Access Assurance Portal 140
Community 140
Entitlements 141
Securing Access to Web Screens in the Access Request Manager 145
Entitlement and Web Screen Pairs in the Access Request Manager 146
Adding Web Screens For a New Entitlement 146
Configuring Menu Items to the Access Assurance Portal Menu using Menu.XML File 148
Overview 148
Main Navigation 148
Customizing the Navigation using XML file 149
Adding a New Top Level Menu 150
Adding a New Child Menu 150
Adding a New Child to an existing Top Level Menu 150
Removing a Menu 151
Updating a Menu 151

Chapter 16 - Creating Profiles 153

Configuring Items to Add a New Profile 154
Providing a Label for the Profile Manager Link 154
Configuring DefaultApproverProfileUID Global Option 155
Approval Workflow for New Profiles 156
Access Request Approval Workflow for a New Profile 157

Appendix A - Obsolete Macros and Global Options 159

Obsolete Macros 159
Obsolete Global Options 160

Index 161

Chapter 1: About Access Request Manager

Core Access (formerly Access Request Manager) offers an intuitive Web-based interface that provides detailed information about requests that is easy for business managers and other approvers to use. The Core Access is a complete, highly functional request management system that enables:

- An individual, whether in IT or in a line of business, to request or remove access to resources, such as an online application system.
- Designated approvers to approve or reject requests.

This manual is intended for use by an IT administrator to configure the Access Request Manager. It describes how to use the Core Access administration menu available through the Access Assurance Portal to configure the request and approval workflows, and includes the following chapters:

- *“About The Access Request Manager Workflows” on page 9* describes the request and the approval workflows, and the screens associated with it.
- *“Configuring the Access Request Manager” on page 21* describes how to configure the Core Access, and introduces the administrative menu to configure the request and approval workflows.
- *“Configuring Global Options” on page 27* describes how to use the **CONFIGURE GLOBAL OPTIONS** to set up the global configurations.
- *“Configuring Pick Lists” on page 43* describes how to configure the pick list using the **PICK LIST ADMIN**.
- *“Configuring Access Items” on page 47* describes how to configure the roles and access entitlements, jointly referred to as access items.
- *“Configuring the Manage Access Catalog” on page 63* describes how to configure the UI items, including the grids and drop-down lists, on the **MANAGE ACCESS CATALOG**.
- *“Configuring the Manage User Access Screen” on page 73* describes how to configure the UI items on the **MANAGE USER ACCESS** screen.
- *“Configuring the Approval Workflows” on page 81* describes how to configure approvers and the **APPROVE REQUESTS** screen for the approval workflow.
- *“Using Macros” on page 93* describes how to configure a macro, and the macros required to configure the workflows for the Access Request Manager.
- *“Using Delegation” on page 113* describes how to delegate ARM privileges to other users.
- *“Disabling Access For Terminated Users” on page 127* describes how to disable access for a terminated user.
- *“Setting Up Email Notifications” on page 129* describes how to create and maintain email templates for notifications sent to requesters, recipients, and approvers.
- *“Customizing the Access Request Manager User Interface” on page 133* describes how to customize the text for buttons, tabs, and dialog boxes.

- *“Managing Access to the Access Request Manager Web Screens” on page 139* describes how to configure users to see only those web screens that they are entitled to in the Core Access.
- *“Creating Profiles” on page 153* describes how to create new profiles or modify

Access Keys

The Core Access solution requires a Core Access® access key obtained from Core Security.

Chapter 2: About The Access Request Manager Workflows

This chapter describes the Manage User Access and Approval workflows and the screens you need to configure to enable them. It includes the following sections:

- *“Manage User Access” on page 12*
- *“Approving a Request” on page 19*

The Request and Approval WorkFlows

The following workflows enable users to seamlessly request and approve access:

- **Managing User Access** - The actions a user (requester) takes to request access to resources in an enterprise. Requesters are users who request access for themselves or other users. A recipient includes any person in an enterprise who is given access to a resource.

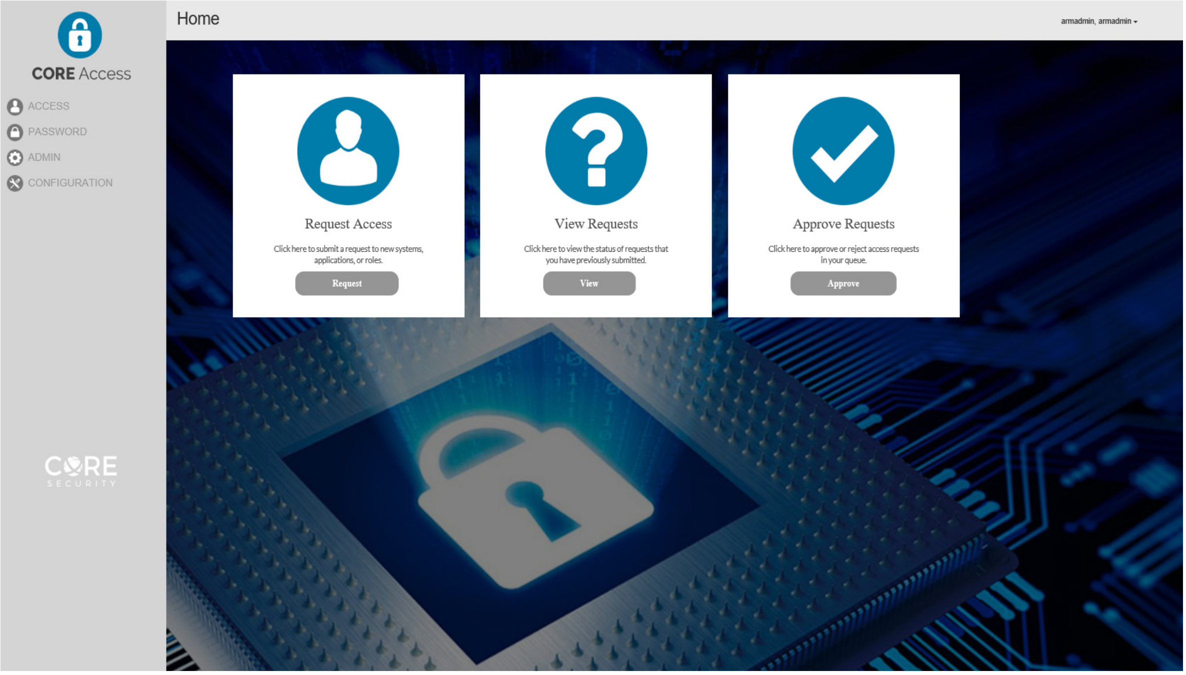
  This access request workflow includes creating a request by selecting recipients, adding or removing access items, and submitting the request for approval. For additional information about the access request workflow, refer to the section *“Manage User Access” on page 12*.

  Note: In this manual, the terms access request and request may be used as general statements to refer to the process of submitting a request to add or remove access for a user.

- **Approving Requests** - The actions an approver completes to approve pending requests. Approvers are users who approve requests.

To access the Access Request Manager (ARM), a requester authenticates through the Access Assurance Portal. Upon authentication, the Access Request Manager landing page is available as shown in *Figure 1*.

Figure 1: The Access Request Manager Landing Page



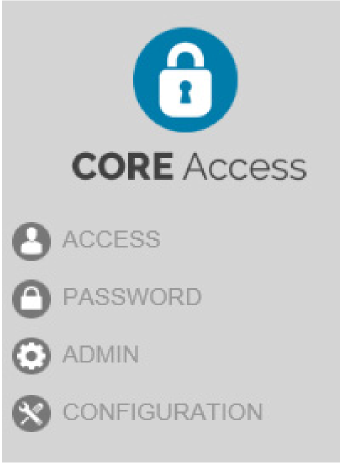
Click here to submit a request to new systems, applications, or roles.

Click here to view the status of requests that you have previously submitted.

Click here to approve or reject access requests in your queue.

A user with administrative privileges who belongs to the ARM Admins community has additional options as shown in *Figure 2*. The administrative items for the **Access Request Manager** under the **Admin** menu provides the administrator access to the related configuration screens. For more information about the menu items, refer to the chapter *“Configuring the Access Request Manager” on page 21*.

Figure 2: The Access Request Manager with the Admin Menu Item



For additional information about configuring the menu items, refer to the chapter *“Managing Access to the Access Request Manager Web Screens” on page 139*.

Manage User Access

From the Access Menu, select **Manage Access**. The **Users** and **Filters** tabs appear to enable you to add roles, entitlements, etc., then create a request to submit for approval.

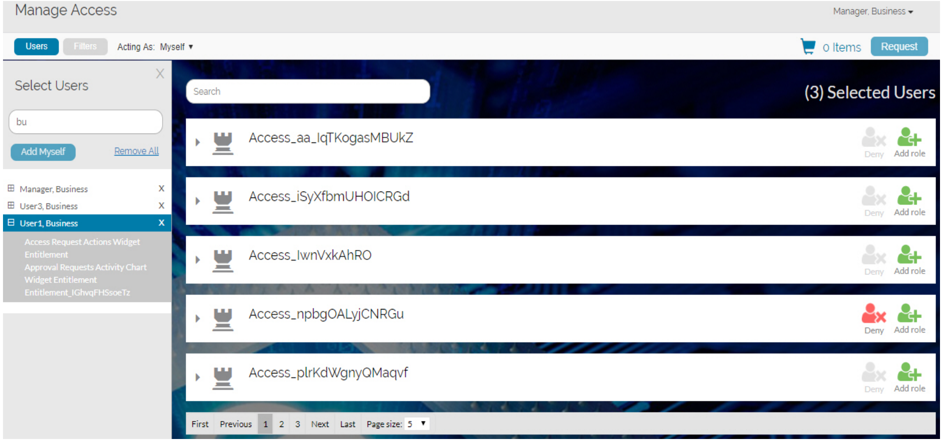
Note: In this section, the terms access request and request may be used as general statements to refer to the process of submitting a request to add or remove access for a user.

Selecting Users

The Manage Access menu options are used to select users, request access, and add/deny roles, entitlements, etc.

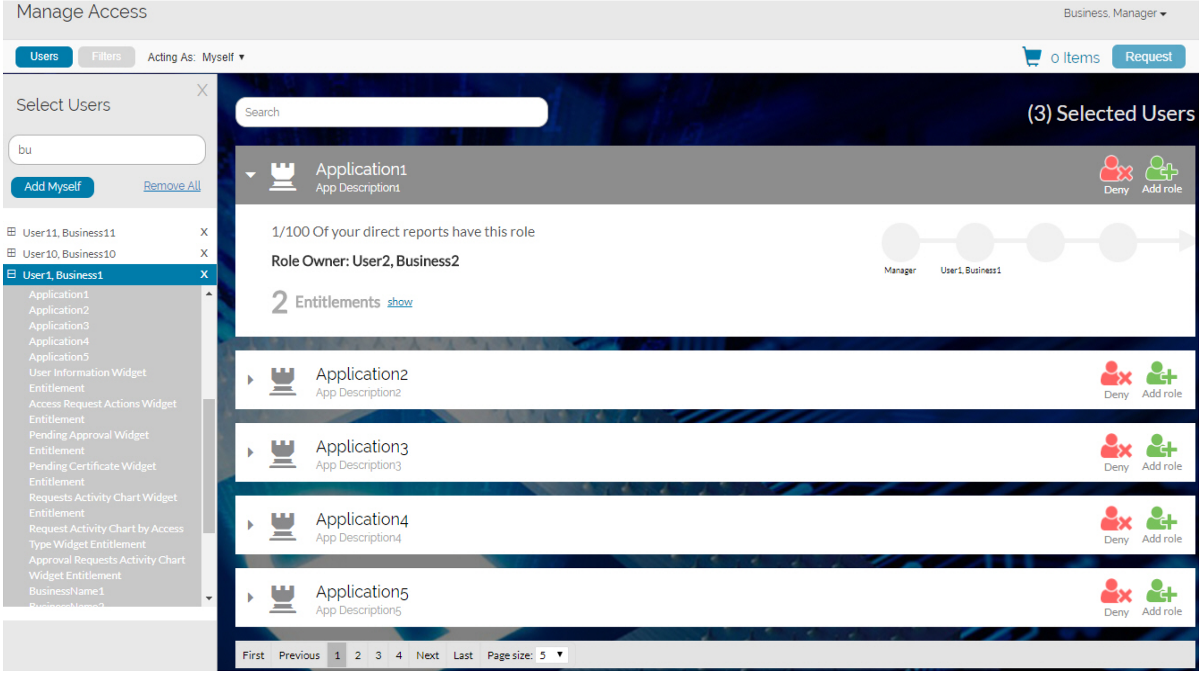
1. From the **Access** menu, go to **Manage Access** > **Users** tab, shown in *Figure 3*, enter one or more users in the **Select Users** field, and simultaneously manage their current access.

Figure 3: Manage Access — Users and Current Access



2. Click the user name(s) under the Select Users field to expand the access list assigned to that user. This access list(s) corresponds to the access in the Selected Users grid to the right, shown in *Figure 4*.

Figure 4: Selected Users Access Grid



User11, Business11 X
User10, Business10 X
User1, Business1 X

Application1
Application2
Application3
Application4
Application5
User Information Widget Entitlement
Access Request Actions Widget Entitlement
Pending Approval Widget Entitlement
Pending Certificate Widget Entitlement
Requests Activity Chart Widget Entitlement
Request Activity Chart by Access Type Widget Entitlement
Approval Requests Activity Chart Widget Entitlement
BusinessName1

Application1 App Description1

1/100 Of your direct reports have this role

Role Owner: User2, Business2

Application2 App Description2

Application3 App Description3

Application4 App Description4

Application5 App Description5

3. Click the pivot next to each access listed to display more details.
4. Click **Add Myself** to manage access for your own managerial needs as needed.

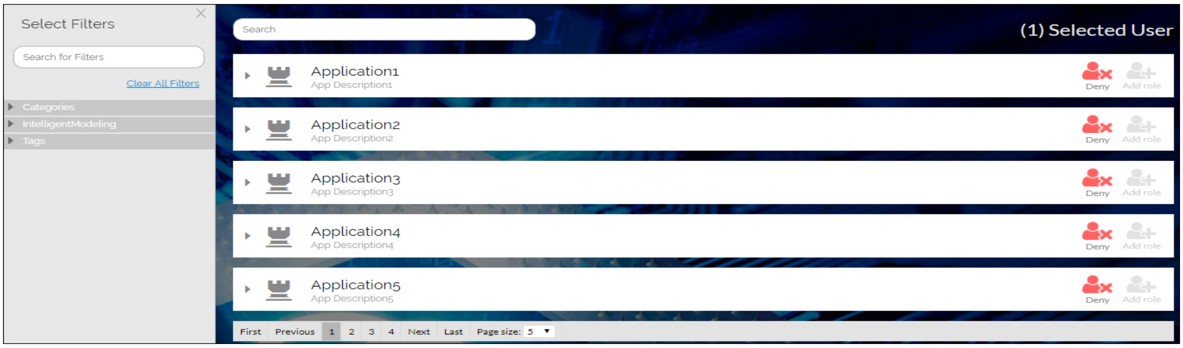
   NOTE: The Access Request Manager enables select users (owners of privileges) to delegate their privileges to other users (delegatees). A delegatee needs to first change his operating identity to the delegator's so that he can act as the delegator and request access. For more information about delegation, refer to the chapter *"Using Delegation" on page 113*.
5. Once users are selected, the Selected Users access grid on the right shows a summary of the access items that the currently managed users hold. The requester can manage access for all users in this grid by selecting access items in the grid, and then adding or denying the selected items. The **Add role** or **Deny** access change requests appear in the **VIEW REQUESTS** screen.

Selecting Filters

From the **ACCESS** menu, go to **MANAGE ACCESS** > **FILTERS** tab, shown in *Figure 5*, the requester can select items to filter by for the users being managed:

- Categories
- Intelligent Modeling
- Tags

Figure 5: Manage User Access — Filters



Filtered data is displayed in the grid with access items that may be added or denied. Click **Clear All Filters** to revert to the default display.

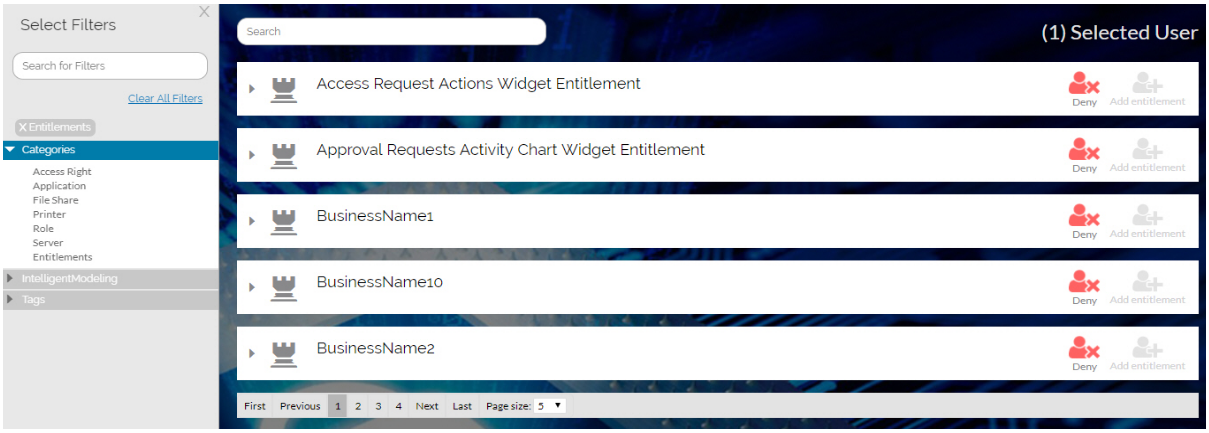
Categories

Categories include data access details.

To filter by Categories:

1. Click the Categories pivot to make a selection from the list.
2. Click **Add** or **Deny,** as applicable.
3. Click **Request** to send the request.
4. Click **Submit** in the Review Access Requests screen.
5. From the **ACCESS** menu, go to **VIEW REQUESTS** to view the request data entered.

Figure 6: Manage User Access - Filter by Categories



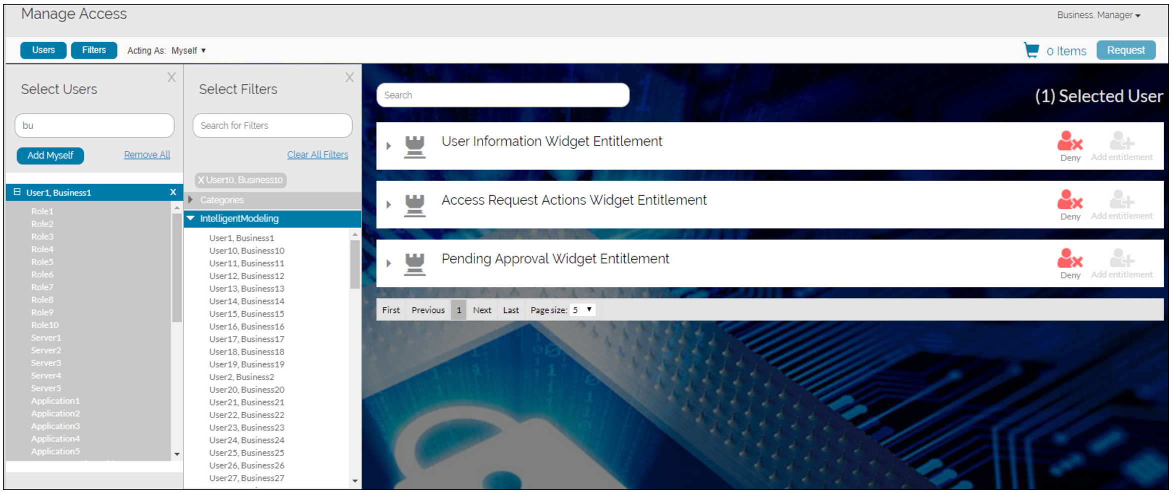
Intelligent Modeling

Intelligent Modeling is used to add or deny access that a selected user has (from the Selected users field) to a selected user in the Intelligent Modeling list.

To filter by Intelligent Modeling:

1. Confirm the **Selected User** from which you want to model access. This displays the options to add or deny.
2. Click the **Intelligent Modeling** pivot to select a user from the list.
3. Click **Add** or **Deny,** as applicable.
4. Click **Request** to send the request.
5. Click **Submit** in the Review Access Requests screen.
6. From the **ACCESS** menu, go to **VIEW REQUESTS** to view the request data entered.

Figure 7: Manage User Access - Filter by Intelligent Modeling



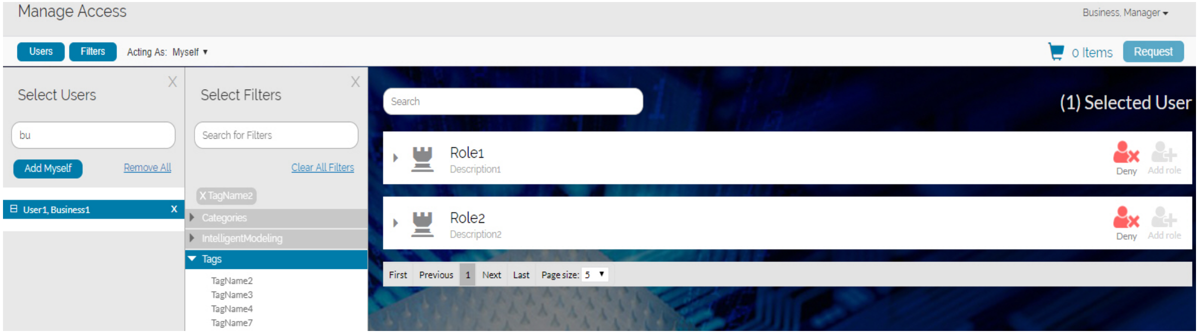
Tags

Tags are used to categorize a set of data based on your own customization.

To filter by Tags:

1. Click the **Tags** pivot to make a selection from the list.
2. Click **Add** or **Deny,** as applicable.
3. Click **Request** to send the request.
4. Click **Submit** in the Review Access Requests screen.
5. From the **ACCESS** menu, go to **VIEW REQUESTS** to view the request data entered.

Figure 8: Manage User Access - Filter by Tags



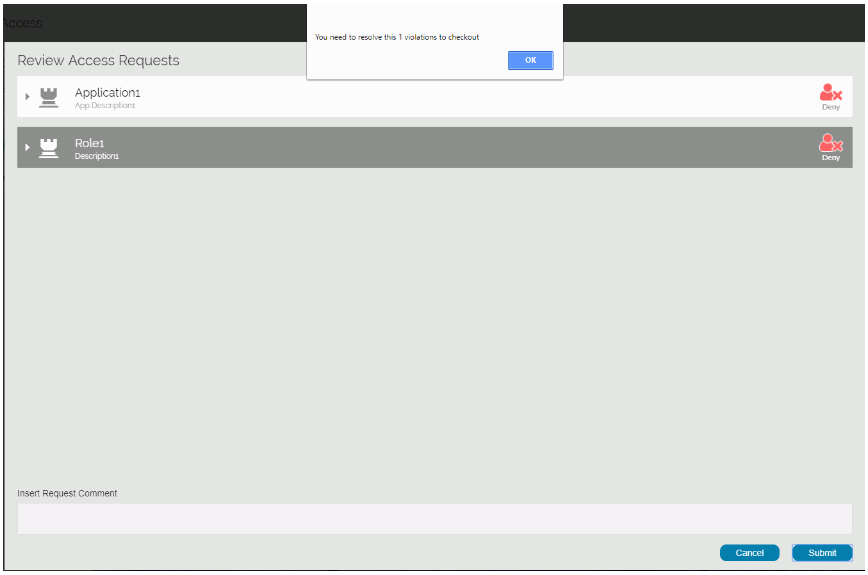
To configure the features described in this section, refer to the chapter *“Configuring the Manage User Access Screen” on page 73*.

Policy Violation Checking

Policy Violation Checking is automatic in Core Access. By default, the feature does not allow duplication of any access type related to:

- Segregation of Duties (SoD) Access Rights
- Segregation of Duties (SoD) Roles
- Segregation of Duties (SoD) Applications

Figure 9: Policy Violation for User Access Requests



Access

Review Access Requests

You need to resolve this 1 violations to checkout

Application1
App Description1

Role1
Description1

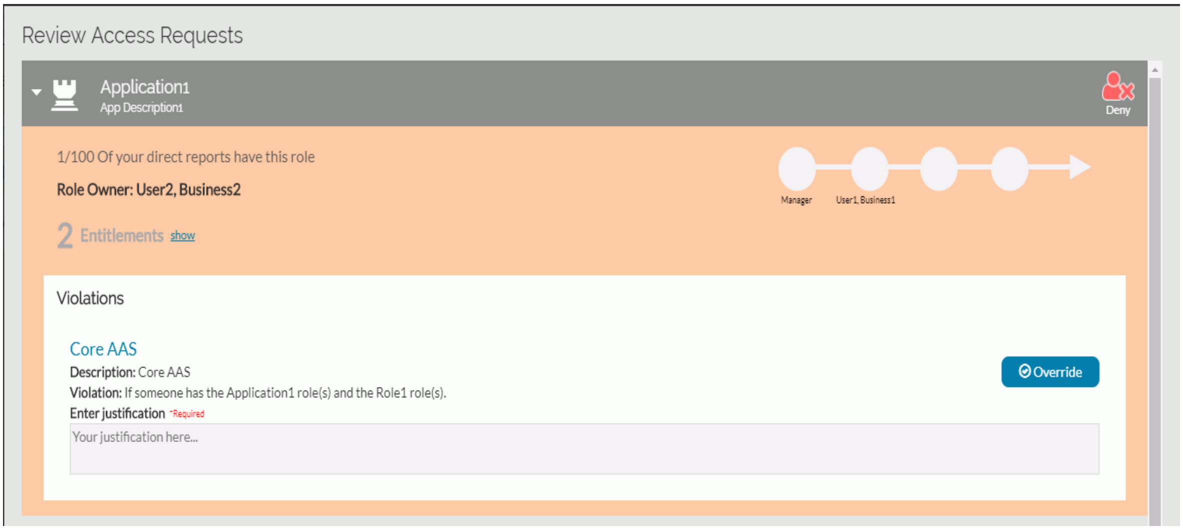
Insert Request Comment

The Policy Violation Checking feature displays a message to resolve violations, if any.

To resolve policy violations:

1. Click **OK** to display the Review Access Requests screen.

Figure 10: Policy Violation Details



Review Access Requests

Application1
App Description1

1/100 Of your direct reports have this role

Role Owner: User2, Business2

2 Entitlements show

Violations

Core AAS

Description: Core AAS

Violation: If someone has the Application1 role(s) and the Role1 role(s).

Enter justification *Required

Your justification here...

2. Click the pivot(s) associated with the request, then the **Core AAS** hyperlink.
3. Click **Deny** if the access is not applicable, or **Override** if the access is necessary.
4. Click **Submit** or **Cancel**.

An email notification is sent to the requester, recipient, and the approver about the request when the request is submitted. To configure the email notifications, refer to *“Setting Up Email Notifications” on page 129*.

Approving a Request

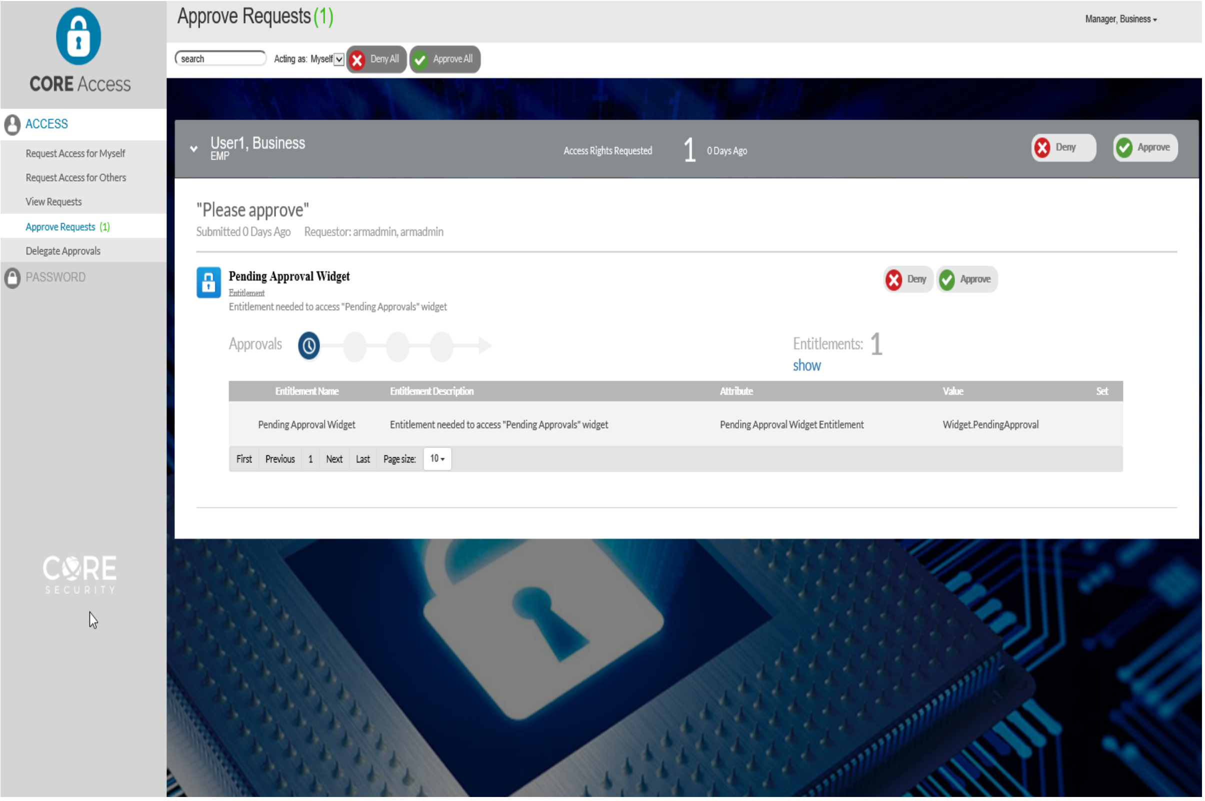
When approvers access the Access Request Manager, they can approve through the **Approve Requests** menu item.

On selecting **Approve Requests**, approvers see any outstanding requests they need to approve, as shown in *Figure 11* on the **Approve Requests** screen.

The Access Request Manager enables select users (delegators) to delegate their ability to approve requests to other users (delegatees). A delegatee needs to first change his operating identity to the delegator's so that he can act as the delegator and approve requests. The **Approve Requests** screen displays the selected delegator's outstanding requests to approve. For more information about delegation, refer to the chapter *"Using Delegation" on page 113*.

If a request was submitted as a bulk request (a request with more than one recipient), it is separated in to multiple requests with one request for each recipient. For example, a bulk request that includes three recipients with two access items splits into three separate requests on the **Approve Requests** screen. Each request includes one recipient and two access items. Splitting the bulk request enables the approver to act independently on each access item for each recipient.

Figure 11: Requests Pending Approval



User1, Business
EMP

Access Rights Requested 1 0 Days Ago

"Please approve"
Submitted 0 Days Ago Requestor: armadmin, armadmin

Pending Approval Widget
Entitlement
Entitlement needed to access "Pending Approvals" widget

Entitlement Name	Entitlement Description	Attribute	Value	Set
Pending Approval Widget	Entitlement needed to access "Pending Approvals" widget	Pending Approval Widget Entitlement	Widget.PendingApproval	

First Previous 1 Next Last Page size: 10

Items that you can configure on the **Approve Requests** screen include:

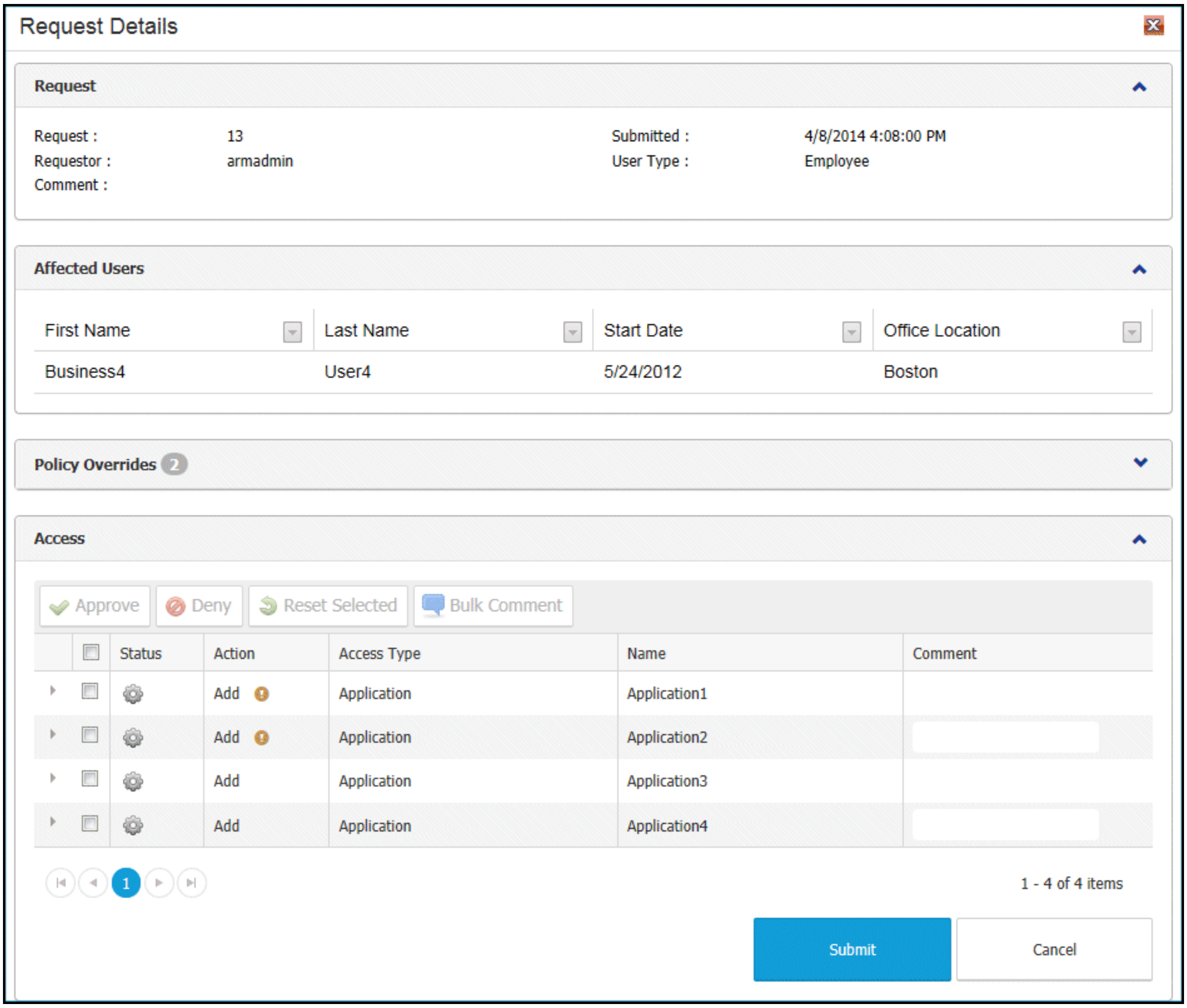
- The Approve Requests grid.
- The editing of access entitlements attributes.

Refer to *“Configuring the Approval Workflows” on page 81* for adding approvers and configuring the **APPROVE REQUESTS** screen.

Viewing Request Details

In order to evaluate a request, the approver can view the Request Details popup. It shows the affected user and a grid in which the approver can selectively approve the requested access items.

Figure 12: Request Details showing two Policy Violations



Request Details

Request

Request :	13	Submitted :	4/8/2014 4:08:00 PM
Requestor :	armadmin	User Type :	Employee
Comment :			

Affected Users

First Name	Last Name	Start Date	Office Location
Business4	User4	5/24/2012	Boston

Policy Overrides 2

Access

□	Status	Action	Access Type	Name	Comment
□		Add !	Application	Application1	
□		Add !	Application	Application2	
□		Add	Application	Application3	
□		Add	Application	Application4	

1 - 4 of 4 items

If you enabled Policy Violation Checking, access requests which have policy violation overrides are indicated to approvers in the **POLICY OVERRIDES** section of the Request Details popup. (They are also indicated by an exclamation mark symbol in the **ACCESS** section.) As designed, overrides are informational; they provide evidence for the approver to make an informed decision about the requested access. An override is specific to a single request; the override does not persist to apply to other requests.

Chapter 3: Configuring the Access Request Manager

This chapter describes how to configure Core Access. It also provides an overview of the Menu options available to configure the access request and approval workflows.

The chapter includes the following sections:

- *“Configuring the Access Request Manager” on page 22*
- *“Authenticating in to the Access Assurance Portal” on page 23*

Configuring the Access Request Manager

The Access Request Manager is installed with the Access Assurance Suite as described in the manual *Installing the Access Assurance Suite*.

After you install the Access Assurance Suite, do the following:

1. Populate the IdentityMap and Profile tables in the newly created **CORE** database as described in the *Using the Identity Mapping Solution* manual.
2. Configure an Active Directory domain with the Active Directory groups, including Managers, Owners, Approvers and ARM Admins.

   Note: Groups created for authentication and authorization need to be global.

   Note: A user with direct reports belongs to the Manager Active Directory group.
3. Configure a Microsoft-ADO-3.0 target named ARM. This target should point to the **CORE** database. You need the Active Directory target for the default authentication and authorization. See *Configuring Password Management Modules (PMMs), Connectors, and Agents* for information on how to create targets.

Getting Started with the Access Request Manager

The Access Request Manager is available through the Access Assurance Portal. This section explains how to log in to the Access Assurance Portal and then it lists the menu options which are visible to a user who is granted the ARM Admin entitlement.

Authenticating in to the Access Assurance Portal

To access the Portal on the server where it is installed, navigate to:

http://localhost/CoreARMS/Login/Login

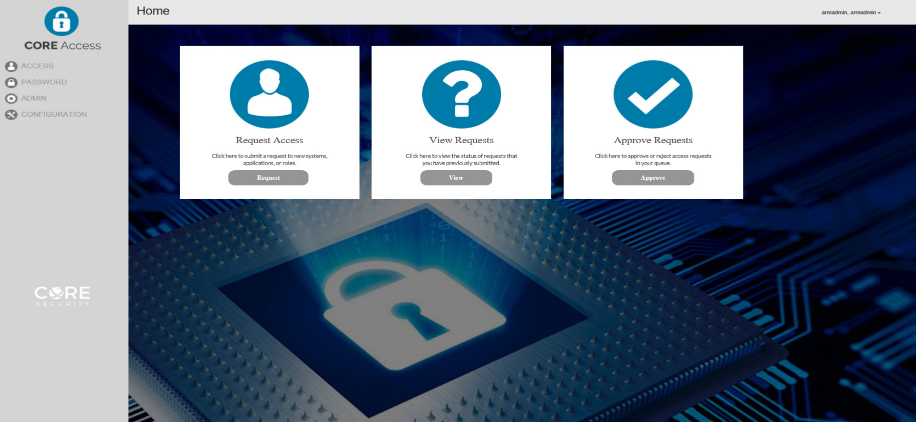
To access the Portal from another system, navigate to:

http://[machine-name or IP address]/CoreARMS/Login/Login

Note: You may need to add the machine name to the list of trusted sights on any system that accesses the Portal using the machine name or the IP address.

The screen in *Figure 13* appears after you authenticate into the Access Assurance Portal.

Figure 13: The Access Assurance Portal



Click here to submit a request to new systems, applications, or roles.

Click here to view the status of requests that you have previously submitted.

Click here to approve or reject access requests in your queue.

You need to be a member of the ARM Admins Active Directory group to authenticate in to the Portal, and access the **ADMIN** menu for administration.

Note: If the Integrated Authentication feature is configured, you are automatically authenticated in to the Access Assurance Portal.

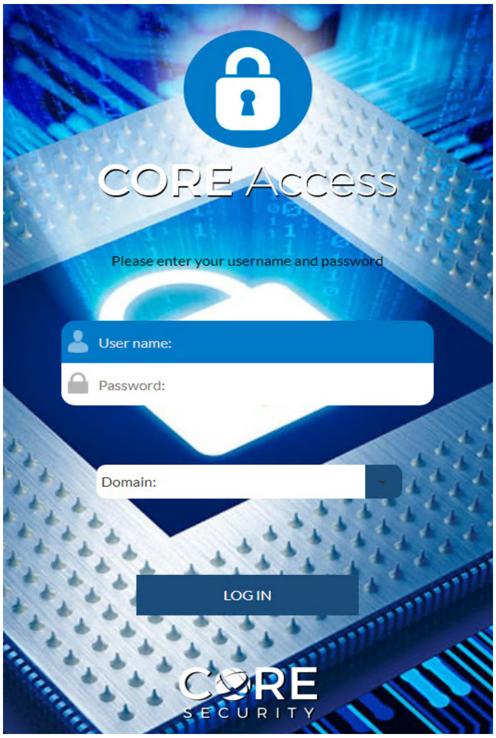
Upon authentication, the menu shows the available options based on the entitlements granted. For additional information about communities and entitlements, refer to the chapter *"Managing Access to the Access Request Manager Web Screens" on page 139*.

Using Multi-Domain Authentication

The multi-domain feature enables a user to authenticate in to the Access Assurance Portal by selecting a Microsoft® Active Directory® domain from a drop-down list.

If multi-domain authentication is enabled, the authentication screen displays the drop-down list with the available domains as shown in *Figure 14*.

Figure 14: Multi-Domain Authentication Enabled

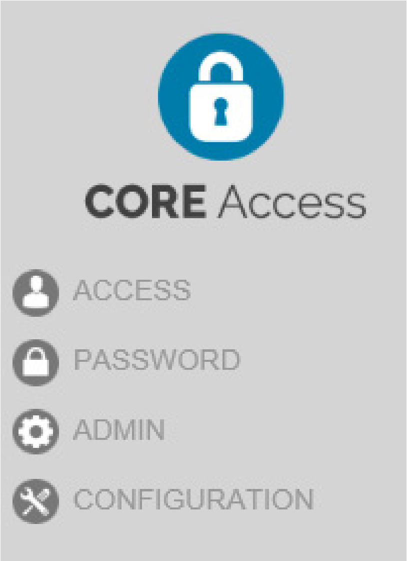


For additional information about multi-domain authentication, refer to the manual *Installing the Access Assurance Suite*.

Overview of the Core Access Menu

When you authenticate in to the Portal as a member of the ARM Admins community, you may see specific administrative menu items grouped under **ADMIN** of the Menu, as shown in *Figure 15*.

Figure 15: Core Access Menu Items



Access Menu

The Access options includes options such as Access Rights, Applications, File Shares, Printers, available in the menu include the following:

- **REQUEST ACCESS FOR MYSELF -** Requester is seeking access for themselves to new systems, applications, or roles.
- **REQUEST FOR OTHERS -** Requester is seeking access for others to new systems, applications, or roles.
- **VIEW REQUESTS -** View status of requests previously submitted.
- **APPROVE REQUESTS -** Approvers see outstanding requested they can approve or reject.
- **DELEGATE APPROVALS -** Delegate ARM privileges where appropriate.
- **PROFILE CREATION -** Enter User details related to profile.

Password Menu

The Password option is used to reset the password.

- **PASSWORD** — Users can perform a self-service reset to change password.

Admin Menu

The Admin options are used to manage access, user interface and provide documentation references.

- **MANAGE ACCESS CATALOG** — Select this option to create new roles, assign tags, and specify the definition and access approvers for roles. For more information, refer to the chapter *“Configuring Access Items” on page 47*.
- **MANAGE CATEGORIES** — Select this option to add, enable, disable, or delete the categories.
- **ADMIN MANAGER** — Select this option to access the Administration Manager for Core Provisioning, and Core Password functionality.
- **PRIORITY DISABLE —** Disable access for a terminated user. For more information, refer to the chapter *“Disabling Access For Terminated Users” on page 127*.
- **ACCESS REQUEST MANAGER > SECURITY ADMIN** — Select this option to configure the Active Directory Groups and the web screens to which they have access. For more information, refer to the chapter *“Managing Access to the Access Request Manager Web Screens” on page 139*.

Configuration Menu

The following Configuration Menu items are available for administration:

- **ACCESS REQUEST MANAGER > SECURITY ADMIN** — Select this option to configure the Active Directory Groups and the web screens to which they have access. For more information, refer to the chapter *“Managing Access to the Access Request Manager Web Screens” on page 139*.
- **GLOBAL CONFIGURATION MANAGER** —Select this option to configure the global configurations for the request and approval workflows. See *“Configuring Global Options” on page 27*.
- **EMAIL TEMPLATE CONFIGURATION** — Select the **EMAIL TEMPLATES MANAGER** to configure the email notifications sent to requesters, recipients, and approvers. Refer to the chapter *“Setting Up Email Notifications” on page 129* for additional information.
- **MACRO CONFIGURATION** — Select this option to configure custom and restriction macros. Refer to the chapter *“Using Macros” on page 93* for additional information.
- **MANAGE CONTENT** — Select this option to configure new content from Core Security such as data collectors for Identity Mapping. For more information, refer to *Using the Identity Mapping Solution*.
- **ACCESS REQUEST MANAGER > PICK LIST CONFIGURATION** — Select this option to create and manage picklists. See *“Configuring Pick Lists” on page 43* for more details on picklists.

Chapter 4: Configuring Global Options

This chapter describes the types of global options and how to edit them thorough the **CONFIGURE GLOBAL OPTIONS** screen, or add new global options to the GlobalConfigValues table. It includes the following sections:

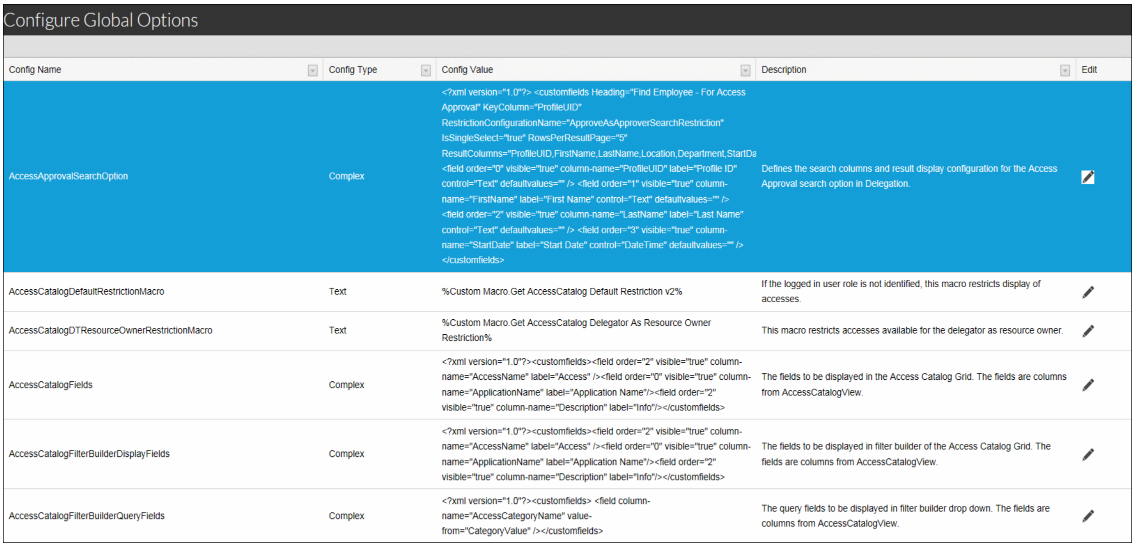
- *"Editing Global Options" on page 28*
- *"Adding Global Options to the GlobalConfigValues Table" on page 31*

From the **Configuration** menu, select **GLOBAL OPTIONS** to modify the values. In general, global options enable the user to configure grids, apply restrictions, or configure the search fields for a grid.

Editing Global Options

From the Configuration menu, click on **Global Options**. The **Configure Global Options** screen appears as shown in *Figure 16*, and shows the current global options.

Figure 16: Configure Global Options



Configure Global Options

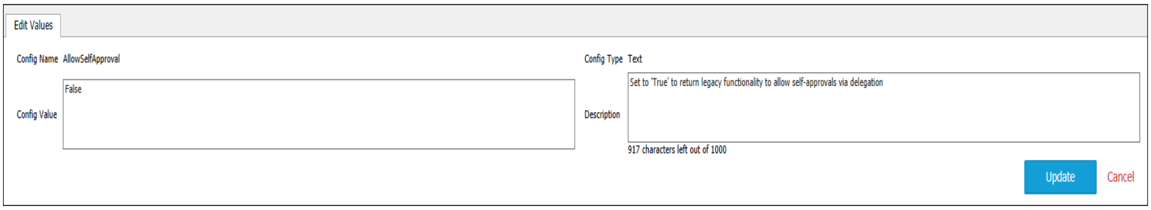
Config Name	Config Type	Config Value	Description	Edit
AccessApprovalSearchOption	Complex	<?xml version="1.0"?> <customfields Heading="Find Employee - For Access Approval" KeyColumn="ProfileUID" RestrictionConfigurationName="ApproveAsApproverSearchRestriction" IsSingleSelect="true" RowsPerResultPage="5" ResultColumns="ProfileUID,FirstName,LastName,Location,Department,StartDa <field order="0" visible="true" column-name="ProfileUID" label="Profile ID" control="Text" defaultvalues="" /> <field order="1" visible="true" column-name="FirstName" label="First Name" control="Text" defaultvalues="" /> <field order="2" visible="true" column-name="LastName" label="Last Name" control="Text" defaultvalues="" /> <field order="3" visible="true" column-name="StartDate" label="Start Date" control="DateTime" defaultvalues="" /> </customfields>	Defines the search columns and result display configuration for the Access Approval search option in Delegation.	✎
AccessCatalogDefaultRestrictionMacro	Text	%Custom Macro.Get AccessCatalog Default Restriction v2%	If the logged in user role is not identified, this macro restricts display of accesses.	✎
AccessCatalogDTResourceOwnerRestrictionMacro	Text	%Custom Macro.Get AccessCatalog Delegator As Resource Owner Restriction%	This macro restricts accesses available for the delegator as resource owner.	✎
AccessCatalogFields	Complex	<?xml version="1.0"?><customfields><field order="2" visible="true" column-name="AccessName" label="Access" /><field order="0" visible="true" column-name="ApplicationName" label="Application Name"/><field order="2" visible="true" column-name="Description" label="Info"/></customfields>	The fields to be displayed in the Access Catalog Grid. The fields are columns from AccessCatalogView.	✎
AccessCatalogFilterBuilderDisplayFields	Complex	<?xml version="1.0"?><customfields><field order="2" visible="true" column-name="AccessName" label="Access" /><field order="0" visible="true" column-name="ApplicationName" label="Application Name"/><field order="2" visible="true" column-name="Description" label="Info"/></customfields>	The fields to be displayed in filter builder of the Access Catalog Grid. The fields are columns from AccessCatalogView.	✎
AccessCatalogFilterBuilderQueryFields	Complex	<?xml version="1.0"?><customfields> <field column-name="AccessCategoryName" value-from="CategoryValue" /></customfields>	The query fields to be displayed in filter builder drop down. The fields are columns from AccessCatalogView.	✎

The global options are of two types: text and complex. To edit global options of type text, refer to the section *"Editing Global Options with Config Type as Text" on page 28*. To edit global options of type complex, refer to the section *"Editing Global Options with Config Type as Complex" on page 28*.

Editing Global Options with Config Type as Text

To edit a global option with **Config Type** as **Text**, select **Edit** for that global option. The **Edit Values** screen appears, as shown in *Figure 17*.

Figure 17: Global Options with Config Type as Text



Edit Values

Config Name AllowSelfApproval

Config Value: False

Config Type Text

Description: Set to 'True' to return legacy functionality to allow self-approvals via delegation

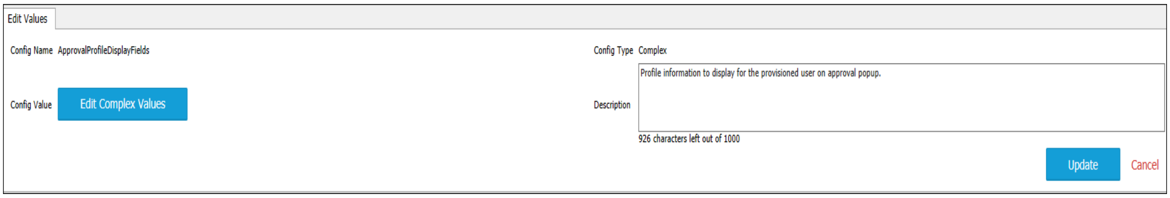
917 characters left out of 1000

Edit the **Config Value** and **Description**. Click **Update** when done.

Editing Global Options with Config Type as Complex

To edit a global option with **Config Type** as **Complex**, select **Edit.** For example, select **Edit** for the **ApprovalProfileDisplayFields** global option. The **Edit Values** screen appears, as shown in *Figure 18*.

Figure 18: ApprovalProfileDisplayFields Global Option



Config Name ApprovalProfileDisplayFields

Config Value

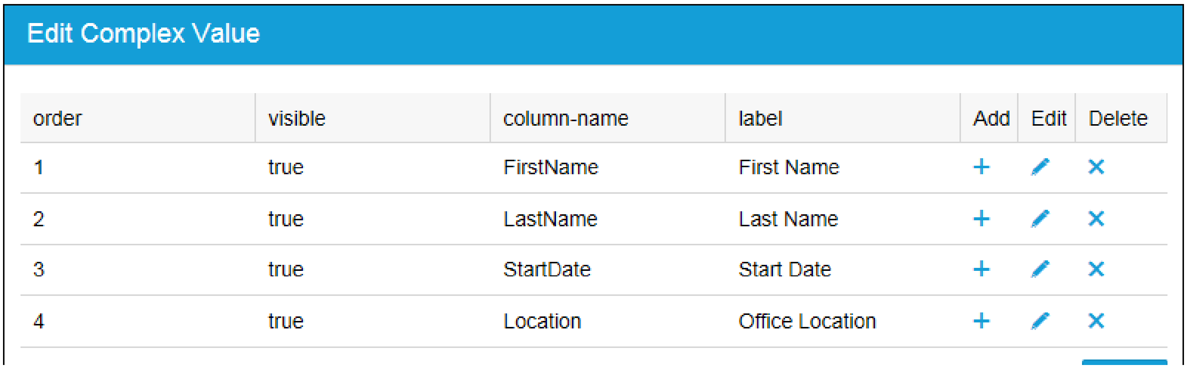
Config Type Complex

Description: Profile information to display for the provisioned user on approval popup.

926 characters left out of 1000

Select **Edit Complex Values**. An **Edit Complex Value** editor appears as shown in *Figure 19*.

Figure 19: Edit Complex Value Editor



order	visible	column-name	label	Add	Edit	Delete
1	true	FirstName	First Name	+	✎	×
2	true	LastName	Last Name	+	✎	×
3	true	StartDate	Start Date	+	✎	×
4	true	Location	Office Location	+	✎	×

The editor allows you to **Edit** values for one or more of the fields, **Delete** an entire row, or add a **New** row to the global option.

Make the changes you want, and select **Update**. Select **OK** to exit from the editor. Modify the text in the **Description** field, and select **Update** on the **Edit Value** screen to save the changes.

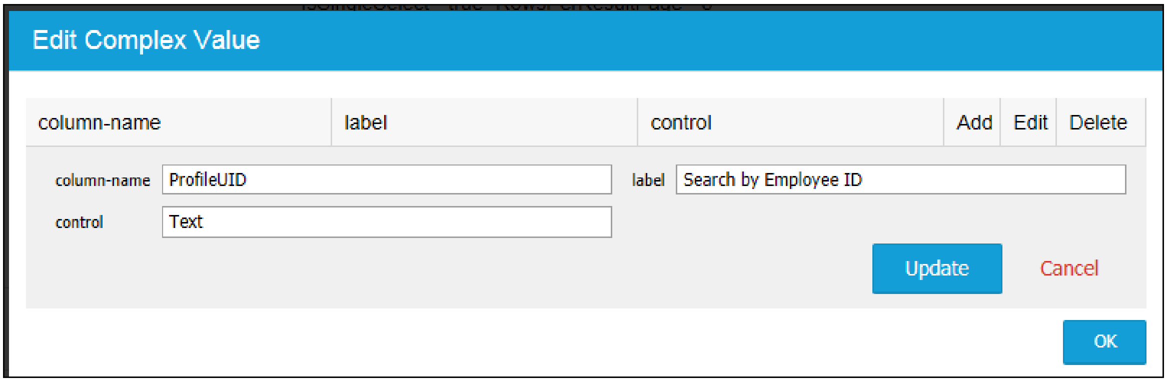
The **Edit Complex Value** editor may display one or more of the following fields for global options with **Config Type** as **Complex**:

- **Order**: Accepts an integer. The fields are displayed in the order specified.
- **Visible**: Accepts a Boolean value of true or false. True shows a field and false hides it.
- **Column-name**: Accepts a string. It identifies a field from a table.
- **Label/Alias**: Accepts a string. Enter a user-friendly alias for a field. This alias appears as the field name on the user screens.
- **Control**: Accepts a string. The data types supported are text, Boolean, list and date time. Text displays a textbox, Boolean displays a checkbox, list displays a drop-down list, date time displays date time control.
- **Clause**: Accepts a custom macro name.
- **Defaultvalues**: Accepts a string. Specify the information you want to appear as default. For example, if the control data type is a list, the user is shown a drop-down list with default values. The values you specify populate the drop-down list.
- **Required**: Accepts a Boolean value of true or false. If it is true, user input is required; if it is false, no input is required.
- **Require-comment**: Accepts a Boolean value of true or false. If true, the user is required to enter a comment when some action is performed.
- **ImageURL**: Accepts a path for an image.

Specifying Custom Macros in the Edit Complex Value Editor

The global option fields are enabled to also accept custom macros. For example, the **column-name** column for the **SingleUserSearchKey** global option contains a field name from the Profile table by default, as shown in *Figure 20*.

Figure 20: SingleUserSearchKey without a Custom Macro



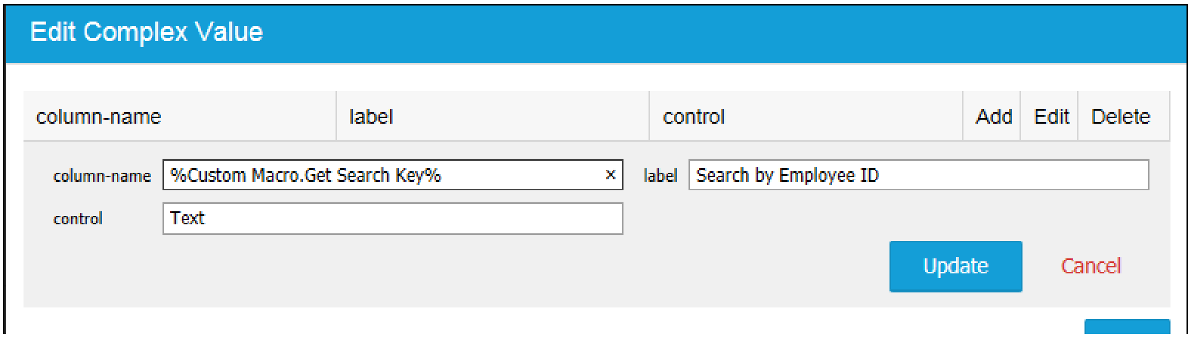
Edit Complex Value

column-name	label	control	Add	Edit	Delete

column-name: ProfileUID
label: Search by Employee ID
control: Text

Edit the **column-name** for the **SingleUserSearchKey** global option to reference a custom macro, as shown in *Figure 21*,

Figure 21: SingleUserSearchKey with the Custom Macro



Edit Complex Value

column-name	label	control	Add	Edit	Delete

column-name: %Custom Macro.Get Search Key%
label: Search by Employee ID
control: Text

The following fields in the **Edit Complex Value** editor are enabled to accept custom macros and support a return value from the custom macro of the type described for each:

- **Order** - Integer
- **Visible** - Boolean (True or False)
- **Column-name** - String
- **Label** - String
- **Control** - String for data types text, Boolean, list and date time.
- **Required** - Boolean (True or False)
- **Require-comment** - Boolean (True or False)
- **Defaultvalues** - String (For control = list, the string should be with comma-separated values).

The custom macros enable you to make the fields configurable and conditional.

Adding Global Options to the GlobalConfigValues Table

Some global options are unavailable to edit through the **CONFIGURE GLOBAL OPTIONS** screen, and you may need to add them to the GlobalConfigValues table. This section describes how to add the global options for grids and drop-downs.

Note: Regardless of the type of global option, the ConfigType is always text when you insert the values described in this section.

Grid Configuration

To add a global option for a grid to the GlobalConfigValues table:

1. Navigate to the location where your Core database resides.
2. Add the global option to the GlobalConfigValues table. For example, to insert Admin.Catalog.SharedGroupingsGridColumns, add this T-SQL statement:

```
INSERT INTO GlobalConfigValues (ConfigName, ConfigType,
ConfigValue)
VALUES ('Admin.Catalog.SharedGroupingsGridColumns', 'Text',
'<grid-columns>
  <column model-name="RoleId" label="Id" />
  <column model-name="Name" label="Name" />
  <column model-name="Description" label="Description" />
  <column model-name="IsAssignable" label="Enabled">
    <attribute name="class" value="k-capitalize" />
  </column>
  <column model-name="OwnerName" label="Owner" />
  <column model-name="Assignments" label="Assignments"
filterable="false" sortable=”false”/>
</grid-columns>')
```

The XML schema for the <column> node supports these attributes:

- Name — This is the object ID used by the system to reference the column name. Do not change the defaults.
- Label — Enter the text you want to display in the grid for the column name.
- Filterable — Accepts true and false. If true, the column is filterable; if false, the column is non-filterable.

  Note: Datetime fields are not filterable.
- Sortable — Accepts true and false. If true, the column is sortable; if false, the column is non-sortable.

Note: By default, a column is sortable and filterable if these attributes are not specified in the column node.

Adding, Removing and Ordering of Fields in the Global Option

To add a column, add a column node. For example, to add a new column:

```
<column model-name="Location" label="Location" />
```

To delete a column, include hidden=”true” as shown in this example:

```
<column model-name=”description” hidden=”true” />
```

To specify a certain display order for a column, follow this example:

```
<column model-name="RoleId" label="Id" />
<column model-name="Name" label="Name" />
<column model-name="Description" label="Description" />
```

The above example demonstrates that *Id* appears first, *Name* in the second place, and *Description* in the third place within a grid. To reorder, change the order of the fields within the XML.

Using Custom Macros in <column> Node

The model-name and label attributes of the <column> node can resolve custom macros. To resolve a custom macro in the <column> node, follow this example:

```
<column model-name=”%Custom Macro.MyMacro%” />
```

You need to first create a custom macro before you use it in the <column> node. To create the custom macro, refer to the chapter *“Using Macros” on page 93*.

Using the WordWrap Global Option

The global option, WordWrap, controls how characters break at the end of a line in a grid. When the value is 'False', the word-break:break-all CSS style imposes a break within the word and shows remaining characters on the next line. No characters are lost. This is the default behavior.

If you want to break long words and wrap them on the next line in a grid, you need to change the value to 'True' (using Global Options from the Configuration menu). Depending on the length of the word/ string, some characters may be lost due to size limitations.

This global option applies to the following screens:

- Priority Disable
- Manage User Access
- Manage My Access
- Manage Access Catalog
- Delegate ARM Privileges
- Approve Requests - (Request Details)

Drop-Down Configuration

To add a global option for a drop-down to the GlobalConfigValues table:

```
INSERT INTO GlobalConfigValues (ConfigName, ConfigType,
ConfigValue)

VALUES ('Access.ManageUsersAccess.UserMgProfileSearch',
'Text',

'<dropdown-properties minimum-query="2" maximum-
results="20" />')
```

The XML schema for the drop-down global option supports the following attributes:

- Minimum-query — The minimum number of characters required to initiate a query to populate a drop-down list.
- Maximum-results — The maximum number of items to present in a drop-down list.

Views Used in Global Options

This section provides all the views with fields that may be referenced by the global options and restriction macros described in the manual. The fields are case sensitive, and should be used as indicated in this section.

Notes: All fields are configurable, unless indicated otherwise. Datetime fields do not support filtering.

The vw_Role View

Table 1 lists all the fields in the vw_Role view.

Table 1: vw_Role

Fields	Data Type
RoleId	string
Version	integer
Name	string
Description	string
IsTemplate	string
Type	integer
Creator	string
CreatorName	string
Owner	string
OwnerName	string

Table 1: vw_Role

Fields	Data Type
IsApproved	string
IsAssignable	string
IsInheritable	string
CustomAccessTypeId	string
CustomAccessTypeName	string
Assignments	integer
ChangedOn	datetime
ChangedBy	string
HasEditableEntitlements	Boolean

The vw_Profile View

Table 2 lists all the fields in the vw_Profile view.

Table 2: vw_Profile

Fields	Data Type
ProfileUID	string
ManagerID	string
RoleID	integer
LocationID	integer
FirstName	string
MiddleName	string
LastName	string
EmployeeType	string
EmployeeNo	string
EmployeeStatus	string
JobCode	string
Company	string
Department	string
DepartmentDescription	string
Division	string
BusinessUnit	string
Location	string

Table 2: vw_Profile

Fields	Data Type
Phone	string
JobTitle	string
StartDate	datetime
LOAReturnDate	datetime
TermDate	datetime
Email	string
Status	integer
UserType	integer
DeleteHold	Boolean
Active	Boolean
SelfQuestion01	string
SelfQuestion02	string
SelfQuestion03	string
SelfQuestion04	string
SelfQuestion05	string
SelfAnswer01	string
SelfAnswer02	string
SelfAnswer03	string
SelfAnswer04	string
SelfAnswer05	string
SupportQuestion01	string
SupportQuestion02	string
SupportQuestion03	string
SupportQuestion04	string
SupportQuestion05	string
SupportAnswer01	string
SupportAnswer02	string
SupportAnswer03	string
SupportAnswer04	string
SupportAnswer05	string
TOAQuestion01	string
TOAQuestion02	string

Table 2: vw_Profile

Fields	Data Type
TOAQuestion03	string
TOAQuestion04	string
TOAQuestion05	string
TOAAnswer01	string
TOAAnswer02	string
TOAAnswer03	string
TOAAnswer04	string
TOAAnswer05	string
ProfileRegistrationDate	datetime
EmployeeID	string
ContractorEndDate	datetime
CustomAttrStr1	string
CustomAttrStr2	string
CustomAttrStr3	string
CustomAttrStr4	string
CustomAttrStr5	string
CustomAttrStr6	string
CustomAttrStr7	string
CustomAttrStr8	string
CustomAttrStr9	string
CustomAttrStr10	string
CustomAttrDecimal1	decimal
CustomAttrDecimal2	decimal
CustomAttrDecimal3	decimal
CustomAttrDecimal4	decimal
CustomAttrDecimal5	decimal
CustomAttrDateTime1	datetime
CustomAttrDateTime2	datetime
CustomAttrDateTime3	datetime
CustomAttrDateTime4	datetime
CustomAttrDateTime5	datetime
CustomAttrBit1	Boolean

Table 2: vw_Profile

Fields	Data Type
CustomAttrBit2	Boolean
CustomAttrBit3	Boolean
CustomAttrBit4	Boolean
CustomAttrBit5	Boolean

The vw_Entitlement View

Table 3 lists all the fields in the vw_Entitlement view.

Table 3: vw_Entitlement

Column	Data Type
EntitlementId	string
EntitlementConfiguration_key	bigint
TargetID	string
BusinessName	string
Name	string
Value	string
Description	string
IsUserCreated	Boolean
IsEditable	Boolean
SingleValueAttribute	Boolean
Automated	Boolean
CustomControl	Boolean
ControlLabel	string
ControlType	string
ControlValues	string
Required	Boolean
HelpText	string
Provisioner	string
ProvisionerEmail	string
ClosedLoop	Boolean
UserVisible	Boolean
ChangedOn	datetime

Table 3: vw_Entitlement

Column	Data Type
ChangedBy	string

The vw_Tag View

Table 4 lists all the fields in the vw_Tag view.

Table 4: vw_Tag

Column	Data Type
TagId	string
Name	string
Description	string
Owner	string
State	Boolean
ChangedOn	datetime
ChangedBy	string

The vw_Entitlement_Tag View

Table 5 lists all the fields in the vw_Entitlement_Tag view.

Table 5: vw_Entitlement_Tag

Column	Data Type
Target_ID	string
Name	string **Note**: If you use this in a macro, use BusinessName as this column is derived from the Entitlement table.
Value	string
IsEditable	Boolean
EntitlementId	string
Description	string

The vw_Role_Tag View

Table 6 lists all the fields in the vw_Role_Tag view.

Table 6: vw_Role_Tag

Column	Data Type
RoleID	string
Name	string
Description	string
Owner	string
IsActive	string
IsApproved	string
Tag_Id	string
TagName	string
OwnerName	string

The vw_ManageAccessCatalog_Entitlement View

Table 7 lists all the fields in the vw_ManageAccessCatalog_Entitlement view.

Table 7: vw_ManageAccessCatalog_Entitlement

Columns	Data Type
EntitlementId	string
TargetID	string
Name	string
Value	string
EntitlementConfiguration_key	bigint
BusinessName	string
Description	string
IsEditable	Boolean
SingleValueAttribute	Boolean
Automated	Boolean
CustomControl	Boolean
IsUserCreated	Boolean
ControlLabel	string
ControlType	string

Table 7: vw_ManageAccessCatalog_Entitlement

Columns	Data Type
ControlValues	string
Required	Boolean
HelpText	string
Provisioner	string
ProvisionerEmail	string
ClosedLoop	Boolean
UserVisible	Boolean
ChangedOn	datetime
ChangedBy	string

The vw_ManagedUsersCurrentAccessDetails View

Table 8 lists all the fields in the vw_ManagedUsersCurrentAccessDetails view.

Table 8: vw_ManagedUsersCurrentAccessDetails

Columns	Data Type
EntitlementId	string
TargetID	string
Value	string
EntitlementConfiguration_key	bigint
BusinessName	string
Description	string
IsEditable	Boolean
SingleValueAttribute	Boolean
Automated	Boolean
CustomControl	Boolean
ControlLabel	string
ControlType	string
ControlValues	string
Required	Boolean
HelpText	string
Provisioner	string
ProvisionerEmail	string

Table 8: vw_ManagedUsersCurrentAccessDetails

Columns	Data Type
ClosedLoop	Boolean
UserVisible	Boolean
EntitlementName	string
RoleModifiedDate	datetime
RoleId	string
Owner	string
OwnerName	string
RoleName	string

Chapter 5: Configuring Pick Lists

This chapter describes how to configure pick lists, and it includes the following sections:

- *“Managing Pick lists” on page 44*

Managing Pick lists

You can create and manage pick lists through the **CONFIGURE PICK LIST** screen that appears under the **CONFIGURE** category. A pick list enables you to create a list of pre-defined values. The pre-configured set of pick list values is available to you later from which you can select your preferred value in the user interface.

This section lists the default pick list types available to you, and describes the general procedure to add a list of values to them.

Default Pick list Types and Values

Table 9: The Default Pick List Types

Default Pick List Types	Pick List Values Supported	Where is the Pick List Value Used	Description
ApprovalType	Manager, Secondary, and ProfileApproval	System Use	If the Business Manager approves a request, then the approval type is Manager. If a second-level approver approves the request, the approval type is secondary.
Severity	High, Medium, and Low.	Populates the **SEVERITY** drop-down list for access levels on the **APPLICATION/ ACCESS MANAGER.**	
Status	Pending - the request is submitted and awaiting approval. Approved - the request is approved. Denied - the request is denied. On Hold - the request is on hold if there are multiple levels of approvals. Processing - the request is in processing until AccountCourier or manual action is taken on the request. Ready - the request is ready to be provisioned. Complete - the request is complete if AccountCourier or manual action is taken on the request.	Displayed on the View Request and Admin - View All Requests screens.	Defines the different states of a request.

Table 9: The Default Pick List Types

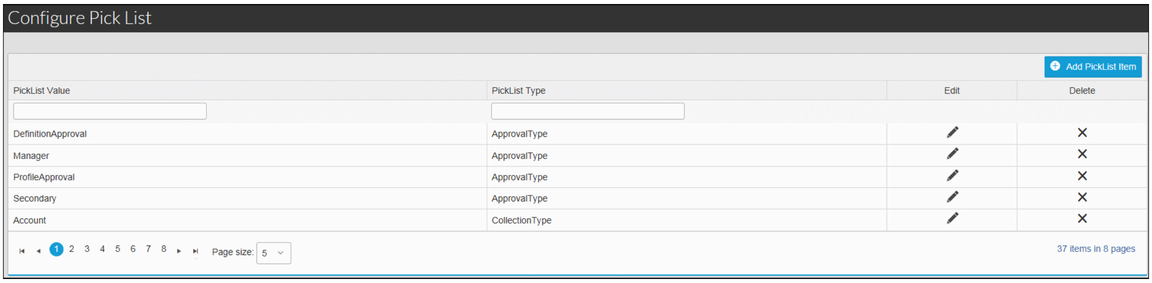
Default Pick List Types	Pick List Values Supported	Where is the Pick List Value Used	Description
UserStatus	Active and Inactive	Used to indicate the status in the Active column of the Profile table. If the Active column is true, the User Status is Active; if the Active column is false, the User Status is Inactive.	Defines the state of a profile request. The User Status is Active if the request was approved. The User Status is Inactive if the profile request is waiting to be approved.

Adding a Pick List Value

To add a pick list value to a default pick list type, follow these steps:

1. From the main menu, under **CONFIGURATION**, select **PICK LIST**. The **CONFIGURE PICK LIST** screen appears, as shown in *Figure 22*.

Figure 22: Configure Pick List



Configure Pick List

PickList Value	PickList Type	Edit	Delete
DefinitionApproval	ApprovalType	✎	✕
Manager	ApprovalType	✎	✕
ProfileApproval	ApprovalType	✎	✕
Secondary	ApprovalType	✎	✕
Account	CollectionType	✎	✕

37 items in 8 pages

2. Select **ADD PICKLIST ITEM**, as shown in *Figure 2*.
3. Enter a value for the pick list value and the default pick list type. The default pick list types are listed in the table Table 9 .
4. Click **INSERT** to confirm and save your changes.

Click the Edit icon ✎ to edit, or the Delete icon ✕ to delete a pick list value.

Chapter 6: Configuring Access Items

This chapter describes the steps to add an access item to the Access Catalog. The access items created are used in the access request workflow.

This chapter includes the following sections:

- *“Overview For Adding Access Items to the Access Catalog” on page 48*
- *“Definitions of Access Terms” on page 49*
- *“Adding a New Category” on page 50*
- *“Adding a Grouping” on page 51*
- *“Editing an Existing Grouping” on page 57*
- *“Enabling or Disabling a Grouping” on page 58*
- *“Enabling or Disabling a Grouping” on page 58*
- *“Adding Access Entitlements” on page 59*
- *“Assigning Tags to Access Entitlements” on page 62*

Overview For Adding Access Items to the Access Catalog

This section is an overview of how the administrator uses the Manage Categories and the Manage Access Catalog screens to create an access item in the Access Catalog.

The steps in this section are described in detail later in this chapter. To configure an access item, the administrator follows these steps:

1. Create categories using the **MANAGE CATEGORIES** screen. Categories that the administrator creates are referred to as user-defined categories. There are system-defined categories that are available by default with the Access Request Manager. For detailed steps refer to the section, *“Adding a New Category” on page 50*.
2. Use the **MANAGE ACCESS CATALOG** to:
   - Create groupings and categorize them with a system-defined or user-defined category.
   - Select the grouping owner.
   - Select the definition and the Add and Remove access approvers.
   - Apply optional tags to the grouping.
   - Add groupings to the grouping definition.
   - Find access entitlements that already exist or create new access entitlements. Add these access entitlements to complete the grouping definition and submit it for approval.

   The approved grouping definition creates a new access item, and the grouping and the access entitlement are added to the Access Catalog as an access item. For additional information, refer to the section *“Adding a Grouping” on page 51*.

Definitions of Access Terms

The table in this section defines the terms that are used in the context of the grouping definition, the Manage User Access (access request) and approval workflows.

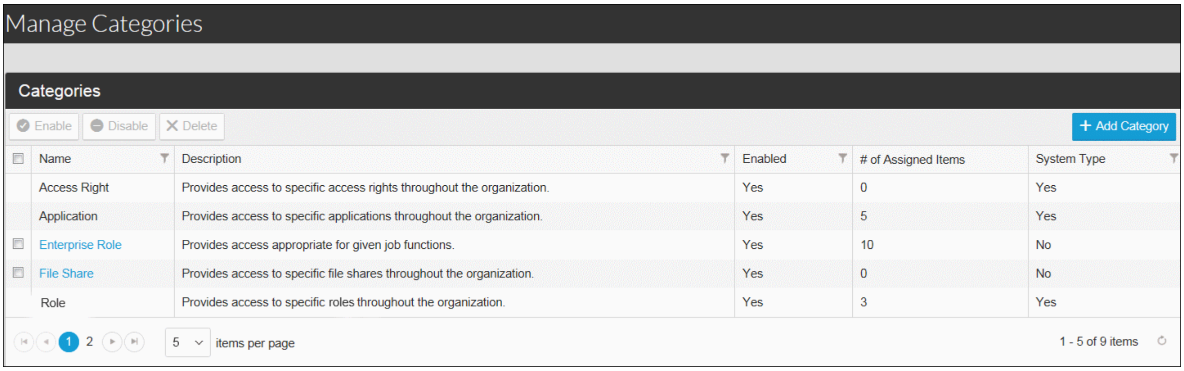
Table 10:

Term	Description	Example
Grouping	A grouping is a manageable access item comprised of a collection of access items that may include access entitlements and other groupings, which together represent something meaningful to a business. For example, application access required for a job function like a Finance Analyst.	ApplicationX, ApplicationY
Category	An administratively defined categorization that is assigned to a grouping to denote that the grouping is of a certain type. For example, a grouping may be classified into the Application or Job Title category to facilitate organization and simplify searches for access request.	Application, Job Title
Entitlement	The combination of an attribute name, an attribute value, and a target name. <Target Name> is the target where the attribute value you are claiming exists. For example, Server 1. <Attribute Value> is the resource name. For example, the Team Foundation Server. <Attribute Name> is the name the user provides, such as TFS.	Microsoft Outlook, Team Foundation Server
Access Item	Term used to refer to groupings or access entitlements.	ApplicationX with Team Foundation Server
Access Catalog	Comprised of both the Entitlement Catalog and the Grouping Catalog.	

Adding a New Category

To add a new category, go to the main menu and select **Manage Categories** under **Admin**. The **Manage Categories** screen appears.

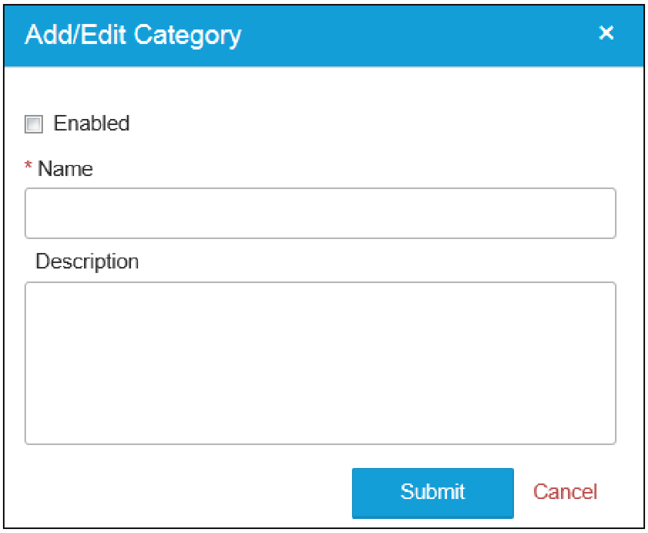
Figure 23: Manage Categories



□	Name	Description	Enabled	# of Assigned Items	System Type
	Access Right	Provides access to specific access rights throughout the organization.	Yes	0	Yes
	Application	Provides access to specific applications throughout the organization.	Yes	5	Yes
□	Enterprise Role	Provides access appropriate for given job functions.	Yes	10	No
□	File Share	Provides access to specific file shares throughout the organization.	Yes	0	No
	Role	Provides access to specific roles throughout the organization.	Yes	3	Yes

Click on the **Add New Category** button to add a new category. The **Manage Access Catalog - Add/ Edit Category** popup appears.

Figure 24: Add New Category



Enter a valid name and description for the category in the respective fields. Select the **Enabled** button to make the newly created category available in the grouping definition. Leaving it unselected hides the category on the **Manage Access Catalog** screen for adding new groupings. Click the **Submit** button to save the category or click the **Cancel** button to exit without saving the entry. The newly created categories are the user-defined categories. You can enable or disable as these categories as needed.

Note: The system-defined categories are available by default and cannot be edited or disabled. The categories are always available when a grouping is created or access is requested.

The **MaxAccessTypesAllowed** global option controls the number of default categories that a user can add. The default value is 20.

Adding a Grouping

To add a new grouping, go to the main menu and select **Manage Access Catalog** under **Admin**. The **Manage Access Catalog** screen appears with the **Groupings** and **Entitlements** tabs.

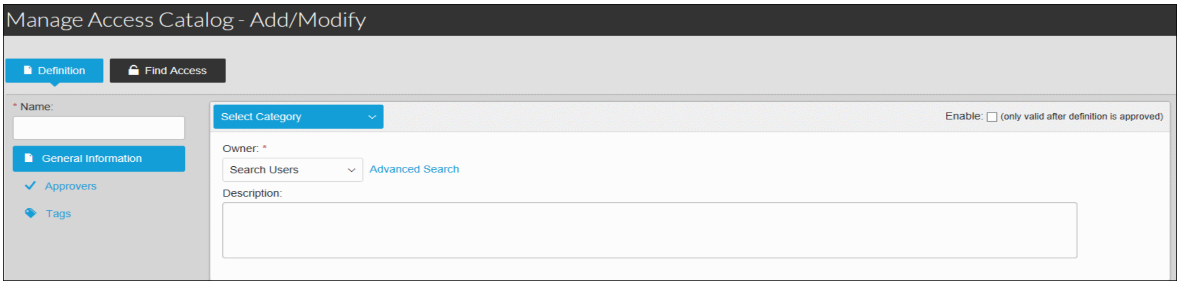
Click on the **Add New** button to add a new grouping. The **Manage Access Catalog - Add/Modify** screen appears with the **Definition** and **Find Access** tabs.

Adding Information on the Definition Tab

The **Definition** tab (see *Figure 25*) enables you to:

- Add general information about a grouping.
- Assign approvers for grouping definition or utilization (access request approval).
- Tagging the grouping to facilitate search for this grouping later.

Figure 25: Add New Grouping



Adding General Information About Grouping

In the **General Information** section (see figure), complete the following details:

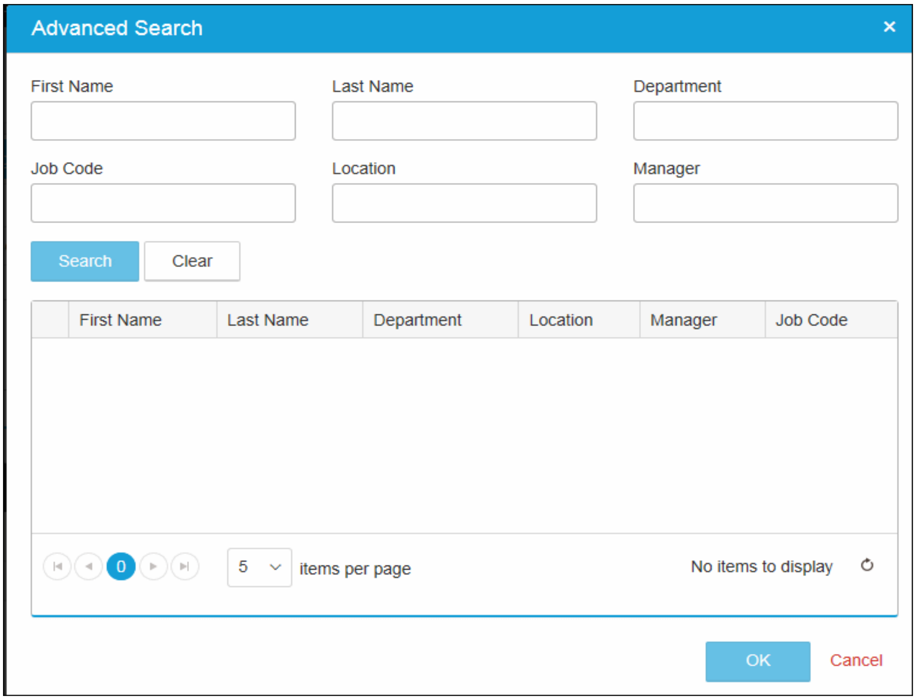
- **Select Category —** Select a category to assign the new grouping that is being created.
- **Name** — Enter a descriptive name for the grouping.
- **Owner** — Select an owner for the grouping by typing a search criteria in the textbox. You can also click on the **Advanced Search** button to search for more profiles, and an **Advanced Search** popup appears similar to *Figure 26*
- **Description** — Enter a user-friendly description to provide more information about the grouping.

The checkbox determines whether a grouping definition is enabled (checked) or disabled (unchecked) after it is approved. By default, the checkbox is unchecked. Grouping definitions that are disabled cannot be used in other definitions or assigned to users even if they have been approved.

Adding Definition and Access Approvers

In the **Approvers** section, select one or more approvers for the grouping definition and access request approvals. Enter your search text in the Search Users textbox, and select an approver. The selected profile is automatically added to the Approver grid. Use the **Advanced Search** popup to add more than one approver.

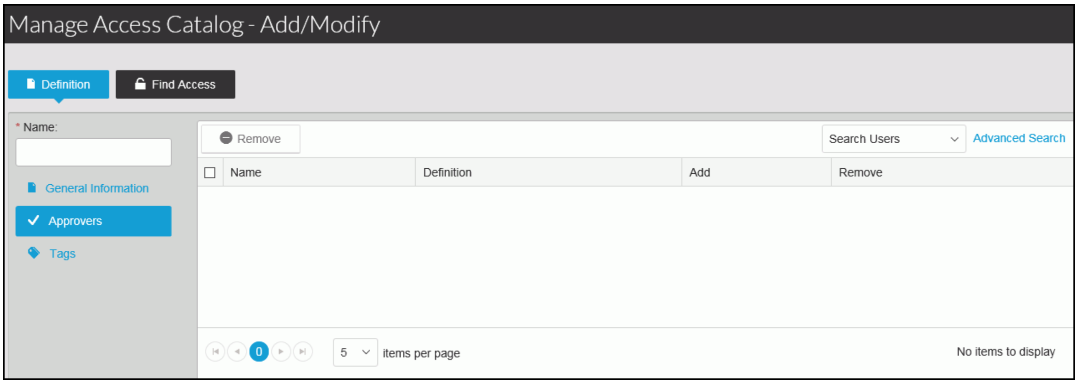
Figure 26: Advanced Search



Select one or more approvers, and click **Add Selected** on the **Advanced Search** popup. Exit the popup, and the selected profiles are automatically added to the Approver grid.

After selecting the approvers, you can check the Definition and Access checkboxes for an individual approver.

Figure 27: Approvers



Check the Definition checkbox for one or more users, if you want them to be Definition approvers. All the users for whom the Definition checkbox is checked constitute the group of Definition approvers. At least one person from this group needs to approve a grouping definition for the grouping to be approved. Hence, the first approver from this group to take action determines whether the grouping definition is approved or denied for the entire Definition approvers' group.

Check the Add checkbox for one or more users, if you want them to be Add approvers. All the users for whom the Add checkbox is checked constitute the group of Add Request approvers. At least one person from this group needs to approve the add request for the grouping.

Check the Remove checkbox for one or more users, if you want them to be Remove approvers. All the users for whom the Remove checkbox is checked constitute the group of Remove Request approvers. At least one person from this group needs to approve the remove request for the grouping.

A user for whom the Definition, Add or Remove checkbox is unchecked, that user is removed from the Definition approvers' group or Add approvers' or Remove approvers' group, respectively, when the grouping is submitted for approval.

Note: The absence of at least one user with a checked box for Definition or Add or Remove in the approvers grid eliminates the need for a Definition or Add or Remove Approvers group, respectively, for a grouping.

For additional information about the approval process, refer to *"Editing an Existing Grouping" on page 57*.

Assigning Tags to Groupings

In the **TAGS** section, you can create new tags, and associate new or existing tags to a grouping. Tag groupings to facilitate future searches for a grouping. To associate tags to a grouping, create new tags. The newly created tags are added to the **TAGS** grid. Once the grouping is approved, all the tags added to the **TAGS** grid are associated with the grouping.

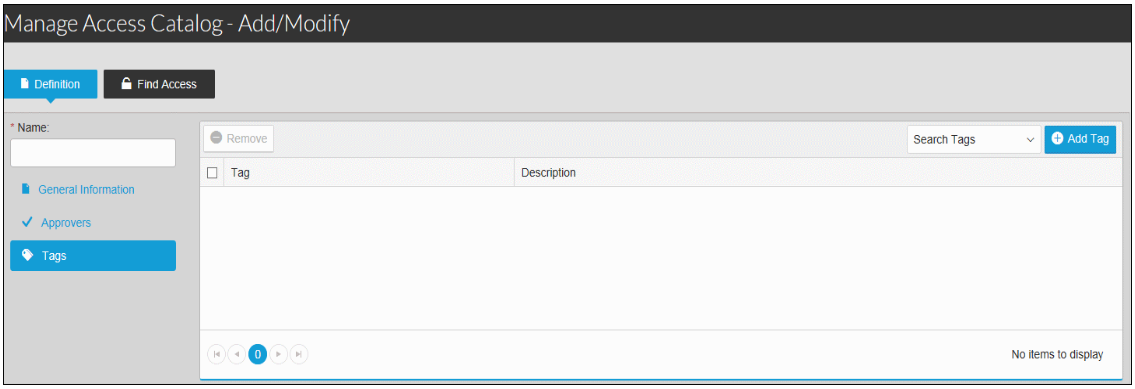
To associate existing tags to a grouping, enter the search text in the Search Tags textbox, and select a tag from the drop-down list. The tag you select is added to the **TAGS** grid.

To create new tags and associate them to a grouping, click **ADD TAG**. In the **ADD TAG** popup, enter a name and description for the tag. Click **ADD**, and the tag is added to the **TAGS** grid.

Note: The new tags are added to the Tag catalog, and you can use these later to tag other groupings.

To remove tags associated with a grouping, select an individual tag or check the Select All checkbox, and click **REMOVE**. The tags are removed from the **TAGS** grid and disassociated from the grouping.

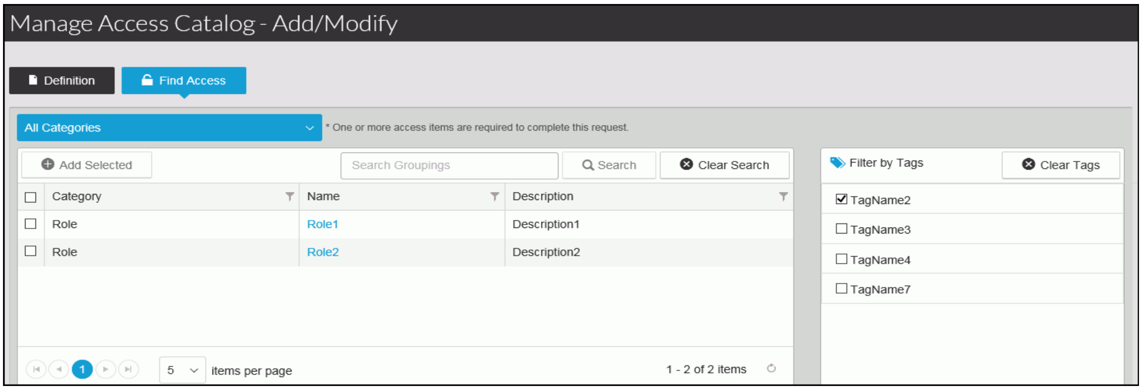
Figure 28: Tags



Adding Information on the Find Access Tab

After you add the general information for the grouping definition with the optional approvers and tags, add the access entitlements and groupings — only the approved and enabled groupings are visible — to complete the grouping definition on the **Find Access** tab as shown.

Figure 29: Find Access



□	Category	Name	Description
□	Role	Role1	Description1
□	Role	Role2	Description2

All the Grouping Catalogs are displayed in the grid, by default. Use the **All Categories** drop-down list to filter access by **Categories**, **Entitlement** or **Intelligent Modeling**.

Filtering the category, such as Application or Entitlement enables you to search for access from the Grouping or Entitlement catalog, respectively. Enter the search text in the search textbox and click **Search** to search the catalogs. The search results show the name and description of groupings that are associated with the selected category. To narrow the search results further, select and filter by tags. Select the groupings or access entitlements from the grid, and click **Add Selected**. The selected groupings or access entitlements appear in the Access grid.

To search for access based on the current access of one or more existing profiles, you can use Intelligent Modeling. If you select this option, a secondary **Search Users** drop-down list appears.

Select a profile from the drop-down list, and the search results show the selected user profile with all the access related to that profile. Filter additional profiles as needed. The profile appears in the left grid with the access in the right grid. The access may be a grouping or an access entitlement, depending on the icon shown against it. The Entitlement icon ▣ represents an access entitlement type and a Grouping icon ☰ represents the grouping that is associated with a specific category.

As you select more profiles, the percentages in the gridl vary depending on how many profiles contain a specific access. For example, assume you select the User1 and User2 profiles. If User1 and User2 share Business1, the percentage shows 100%; if Business1 only belongs to User 1, the percentage shows 50%. To find out the distribution of access across profiles, expand an access by clicking on the arrow in the grid.

Select one or more access from the grid, or select all using the Select All checkbox. Click **ADD SELECTED** to add the access to the grid.

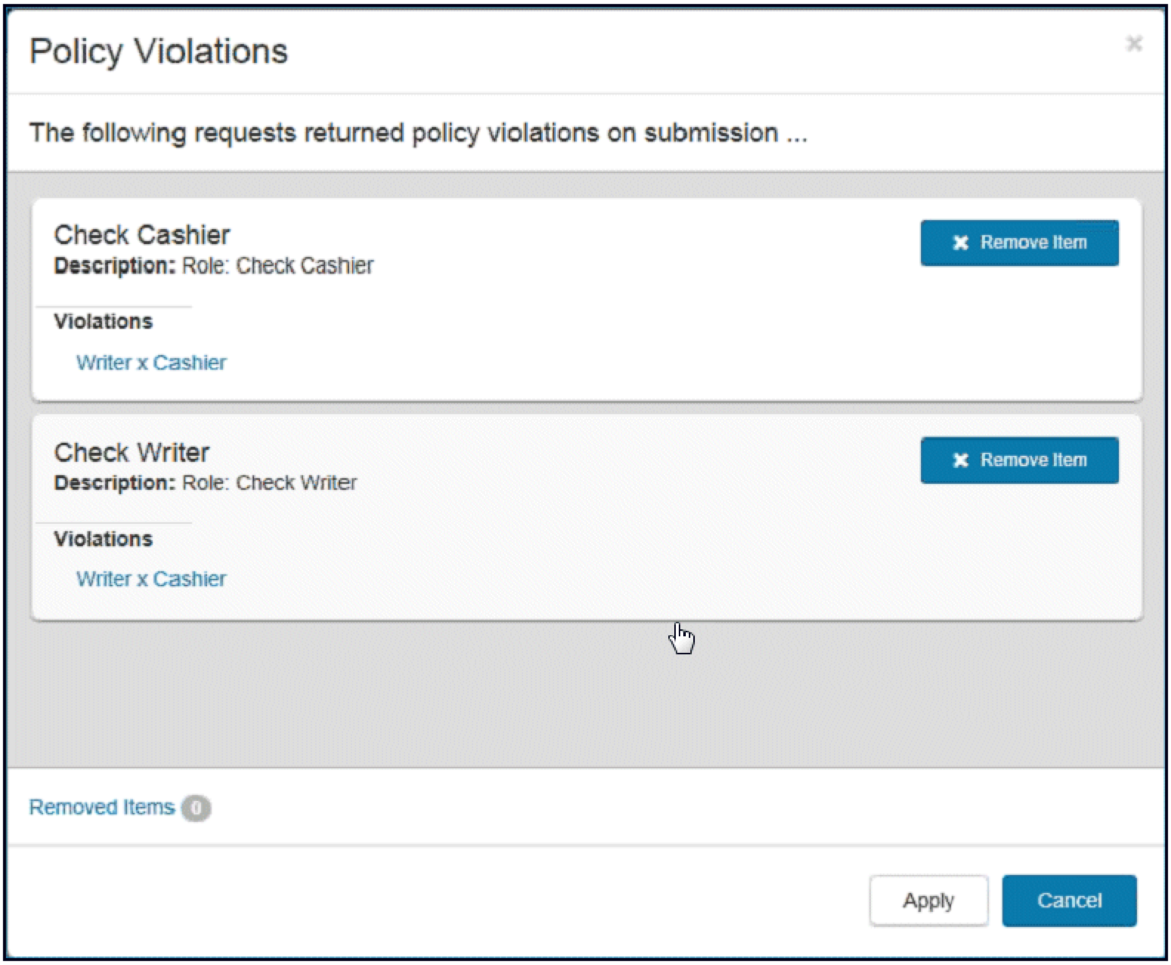
Click on **SUBMIT** to send the grouping definition to the approvers for approval. Click **CANCEL** to exit without saving the grouping definition. For additional information about approving grouping definitions, refer to *“Editing an Existing Grouping” on page 57*.

Policy Violation Checking

Policy Violation Checking extends the Grouping Definition Request feature of the Access Request Manager to respond to policy violations reported by the Access Insight(AI). By default, the feature only pertains to policies created in Access Insight (AI) using the following policy types:

Upon submission of a grouping definition request, AI runs policies, given the context of the grouping and the new set of access requested. If policy violations occur, the Policy Violations popup lists each access item and the associated violation. In the following figure, Check Cashier and Check Writer are two access items which cannot be provisioned together because of an SoD Roles policy in AI.

Figure 30: Policy Violations upon Submission of Grouping Definition Request



Policy Violations

The following requests returned policy violations on submission ...

Check Cashier
Description: Role: Check Cashier

Violations

Writer x Cashier

Check Writer
Description: Role: Check Writer

Violations

Writer x Cashier

Click **Remove Item** to remove a requested item that violates the policy. You may have to remove more than one item to resolve all violations. (You cannot request an override of the policy.) When all violations are resolved, click **Apply** to continue with the grouping definition.

The Policy Violation Checking feature requires a complete installation and configuration of AAS and either AI or AIE. For information about enabling the Policy Violation Checking feature, refer to the *Installing the Access Assurance Suite* manual.

Editing an Existing Grouping

To edit an existing grouping, go to the main menu and select **Manage Access Catalog** under **Admin.** On the **Groupings** tab, click on the **Edit** button next to the grouping you want to modify. The **Manage Access Catalog - Add/Modify** screen appears. Make the modifications and submit the modified grouping definition for approval.

Once the modified grouping definition is submitted for approval, the grouping is shown as read-only on the **Manage Access Catalog** screen. Click the **View** button next to the grouping in the **Details** column to view the original grouping definition.

Note: The original grouping definition remains available for use within another grouping definition or access request.

Click **Enable** to enable a grouping definition, and **Disable** to disable it on the **Manage Access Catalog.** Enabled groupings are always available for use within another grouping definition or access request.

To view the modified grouping, go to the main menu and under **Access**, select **View Requests**. After the screen refreshes, click **View** next to your request to modify the grouping definition.

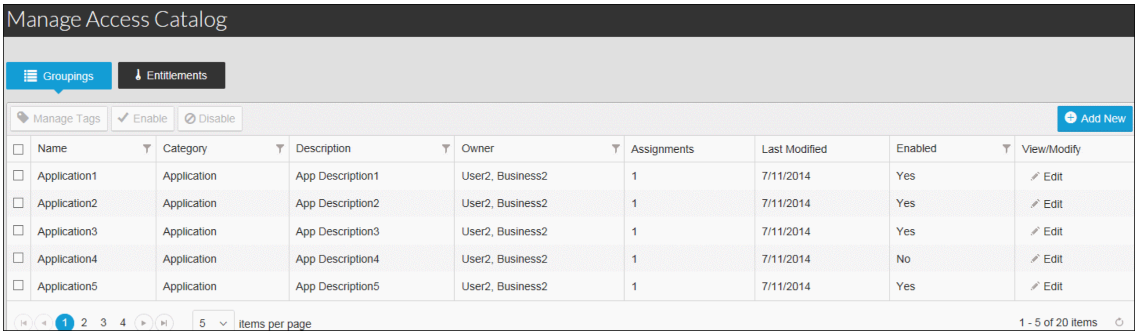
The modified grouping definition is immediately available for use in another grouping definition or access request if it is approved. If the modified grouping definition is denied, the modifications are lost and the original definition becomes editable and available for use in another grouping definition or access request.

For additional information about the grouping definition approval, refer to the section *“Enabling or Disabling a Grouping” on page 58*.

Enabling or Disabling a Grouping

Individual groupings can be enabled or disabled through the **MANAGE ACCESS CATALOG - ADD/MODIFY** screen while creating or modifying a grouping. In addition, you can simultaneously enable or disable multiple groupings through the **MANAGE ACCESS CATALOG** screen after the groupings have been created and approved. To enable one or more groupings, select the groupings and click **ENABLE**. To disable one or more groupings, select the groupings and click **DISABLE**. The **ENABLED** column shows a Yes or No depending on whether or not the groupings is enabled.

Figure 31: Enable or Disable Groupings



□	Name	Category	Description	Owner	Assignments	Last Modified	Enabled	View/Modify
□	Application1	Application	App Description1	User2, Business2	1	7/11/2014	Yes	Edit
□	Application2	Application	App Description2	User2, Business2	1	7/11/2014	Yes	Edit
□	Application3	Application	App Description3	User2, Business2	1	7/11/2014	Yes	Edit
□	Application4	Application	App Description4	User2, Business2	1	7/11/2014	No	Edit
□	Application5	Application	App Description5	User2, Business2	1	7/11/2014	Yes	Edit

Only approved and enabled groupings can be used in other grouping definitions or access requests.

Note: A grouping that is approved, but disabled is not available for future groupings definitions or access requests.

The **ASSIGNMENTS** column in *Figure 31* shows the number of users who have been assigned a grouping. As you assign an enabled grouping to more users, the number increases. When an enabled grouping is disabled, the **ASSIGNMENTS** column shows the number of assignments before its status was changed to disabled.

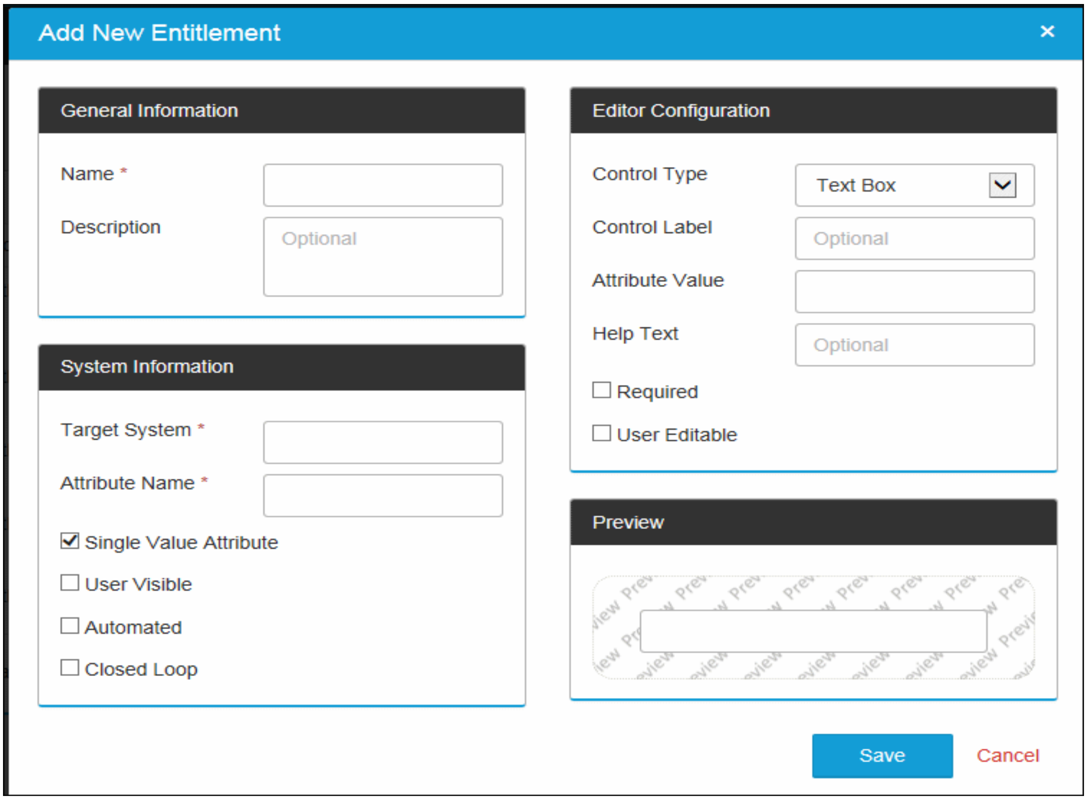
Adding Access Entitlements

To add access entitlements, go to the main menu and select **Manage Access Catalog** under **Admin** After the screen refreshes, click on the **Entitlements** tab.

Note: You can also add a new entitlement or configure an existing entitlement when creating or editing a grouping. An entitlement is created whether or not the request for the grouping is approved. If you are editing an existing entitlement, however, the changes to the entitlement take effect only if the grouping request is approved.

Click on the **Add New Entitlement** button to add a new access entitlement. The **Add New Entitlement** popup appears as shown in *Figure 32*.

Figure 32: Add New Entitlement



Add New Entitlement ×

General Information

Name *

Description: Optional

System Information

Target System *

Attribute Name *

☑ Single Value Attribute

□ User Visible

□ Automated

□ Closed Loop

Editor Configuration

Control Type: Text Box

Control Label: Optional

Attribute Value

Help Text: Optional

□ Required

□ User Editable

Preview

Configure the following fields on the popup under **General Information**:

- **Name** — Enter a business-friendly name to identify an access entitlement. This name appears on both the **Manage Access Catalog** and **Manage User Access** screens when you search for access entitlements.
- **Description** — Enter a user-friendly description to provide more information about the entitlement.
- **Target System** — Enter a target name (TargetID). If the target already exists, then the access entitlement is mapped to the TargetID. If the target does not exist, an entry for the target is created and then mapped to the access entitlement.
- **Attribute Name** and **Value** — Enter a name and value for the attribute. The value you enter becomes editable on the **Manage User Access** screen, if **User Editable** is checked.

- **USER VISIBLE** — If checked the access entitlement is visible on the **MANAGE USER ACCESS** screen.
- **SINGLE VALUE ATTRIBUTE** — This may be used for provisioning beyond the scope of the Access Request Manager.

Configure the following fields on the popup under **EDITOR CONFIGURATION**:

- **CONTROL TYPE —** Select a control type from the drop-down list. Depending on your selection, the options change for some fields. The control types include Text Box, Text Area, True/False (Checkbox), Drop Down, and Radio Buttons.

  Note: Selecting a different control type permanently deletes all the existing values for the entitlement while creating or editing it.
- **CONTROL LABEL —** Enter text that appears as the control label for the entitlement.
- **ATTRIBUTE VALUE —** Enter or select a value depending on the control type selected. For the Drop Down and Radio Button control types, blank entries (when you hit the enter key without any text) are displayed as valid entries.

  Note: Remove any blank entries that you do not want to display.
- **DEFAULT VALUE —** Appears if you have selected either the drop-down list or the radio button. The value you enter is shown as the default selection on the **MANAGE USER ACCESS** screen.
- **HELP TEXT —** Enter text that describes what the control type does.
- **REQUIRED** — Check this option to require input from the user.
- **USER EDITABLE** — Check this option to enable the requester to edit the attribute value on the **MANAGE USER ACCESS** screen.

Depending on the control type selected, the **PREVIEW** section suggests how the control looks on the **MANAGE USER ACCESS** screen when creating an access request.

Table 11 indicates the behavior of access entitlements when an access request is created and approved.

Table 11: Entitlement Behavior

Required Checked	User Visible Checked	User Editable Checked	Suggestions on Default Value
Y	N	Y	Not supported
N	N	Y	Not supported
Y	N	N	Requires a default value
Y	Y	N	Requires a default value
N	N	N	Requires a default value
N	Y	N	Requires a default value

Table 11: Entitlement Behavior

Required Checked	User Visible Checked	User Editable Checked	Suggestions on Default Value
N	Y	Y	Does not require a default value
Y	Y	Y	Does not require a default value

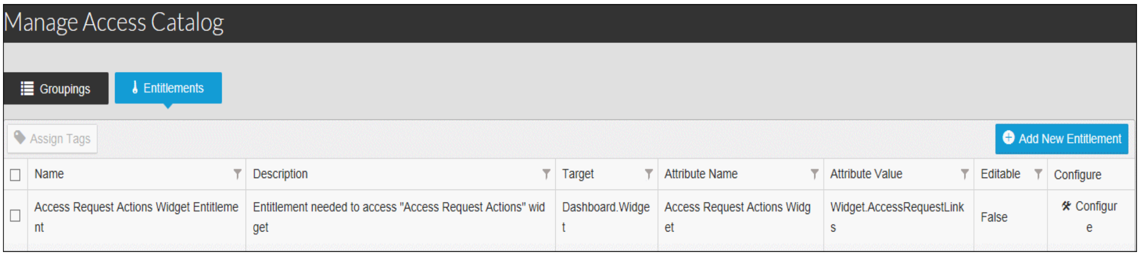
Once an entitlement is created it is available to all the new groupings that may get created in the future. Any modifications made to an existing entitlement do not apply retroactively to groupings created in the past. The modification is only available to new groupings.

Assigning Tags to Access Entitlements

Select the access entitlements to which you want to assign tags, and click **Assign Tags**.

You can assign a tag to one or more access entitlements. An access entitlement may be associated with one or more tags.

Figure 33: Access Entitlements



□	Name	Description	Target	Attribute Name	Attribute Value	Editable	Configure
□	Access Request Actions Widget Entitlement	Entitlement needed to access "Access Request Actions" widget	Dashboard.Widget	Access Request Actions Widget	Widget.AccessRequestLinks	False	Configure

You can later use these tags as a filter to search for the tagged access entitlements.

Chapter 7: Configuring the Manage Access Catalog

This chapter describes how to configure items such as grids, buttons, textboxes on the **MANAGE CATEGORIES** and **MANAGE ACCESS CATALOG** screens using the global options, and includes the following sections:

- *"Configuring Items on Groupings Tab" on page 65*
- *"Configuring Items on Entitlements Tab" on page 71*

Before you configure the grids and drop-downs, review *"Configuring Global Options" on page 27* that describes the global options in general and how to add or edit them.

Note: The global options described in this chapter for the grids and drop-downs are not visible in the **CONFIGURE GLOBAL OPTION** by default. To add them to the GlobalConfigValues table, follow the steps described in the section *"Adding Global Options to the GlobalConfigValues Table" on page 31*.

To configure the restriction macros for the **MANAGE ACCESS CATALOG**, see the chapter *"Using Macros" on page 93*.

Configuring the Delete Button on Manage Access Catalog

The Delete button on the **MANAGE ACCESS CATALOG** screen enables the deletion of groupings. By default, this button is hidden from view as the value in DeleteRole global option is false. To show the button, change the value in the DeleteRole global option to true.

Note: If a grouping is assigned or used in other grouping definitions, any related assignments are deleted. It is recommended that you do not delete groupings. If you have to delete groupings, review and confirm before you delete them.

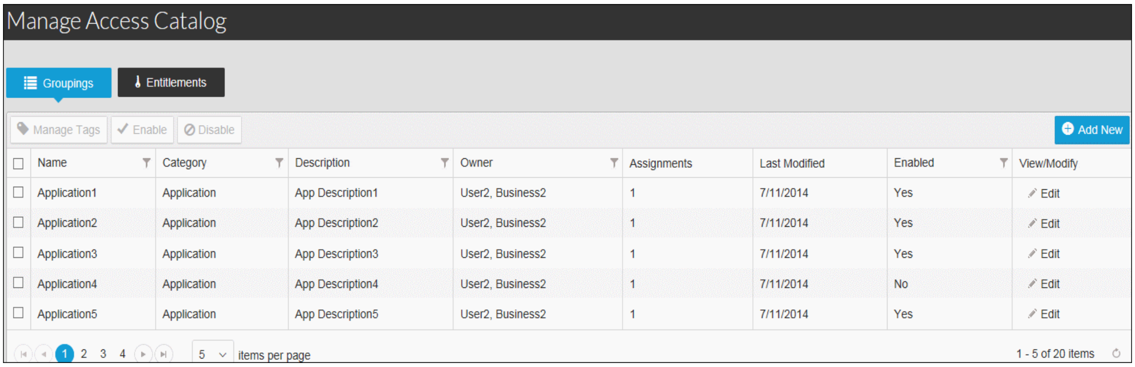
Configuring Items on Groupings Tab

This section describes the global options that are applicable to the grids and drop-downs on the **GROUPINGS** tab, and the **ADD/MODIFY** screen for groupings.

Configuring the Groupings Grid

The Groupings grid (see *Figure 34*) shows all the groupings that were created with details including the grouping owner and whether or not a grouping is enabled. You can configure this grid using the **ADMIN.CATALOG.SHAREDGROUPINGSGRIDCOLUMNS** global option. The fields are from the vw_Role view.

Figure 34: Groupings Grid



□	Name	Category	Description	Owner	Assignments	Last Modified	Enabled	View/Modify
□	Application1	Application	App Description1	User2, Business2	1	7/11/2014	Yes	Edit
□	Application2	Application	App Description2	User2, Business2	1	7/11/2014	Yes	Edit
□	Application3	Application	App Description3	User2, Business2	1	7/11/2014	Yes	Edit
□	Application4	Application	App Description4	User2, Business2	1	7/11/2014	No	Edit
□	Application5	Application	App Description5	User2, Business2	1	7/11/2014	Yes	Edit

The default XML is as follows:

```
<grid-columns>

  <column model-name="Name" label="Name" />

  <column model-name="Description" label="Description" />

  <column model-name="OwnerName" label="Owner" />

  <column model-name="Assignments" label="Assignments"
filterable="false" />

  <column model-name="DisplayChangedOnDate" label="Last
Modified" filterable="false"/>

  <column model-name="IsAssignable" label="Enabled">

    <attribute name="class" value="k-capitalize" />

  </column>

</grid-columns>
```

For additional information, refer to the section *"Adding Global Options to the GlobalConfigValues Table" on page 31*.

Configuring the Search Tags Drop-down on Assign Tags Popup

Configure the Search Tags drop-down list to search for tags with the **ADMIN.CATALOG.SHAREDTAGSEARCHPROPERTIES** global option on the **ASSIGN TAGS** popup. This configuration allows you to set the minimum number of characters required to initiate a query and the maximum number of items to present in a drop-down list.

The default XML is as follows:

```
<dropdown-properties minimum-query="2" maximum-
results="20" />
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring Items on the Add/Modify Screen

This section describes all the configurable items on the **ADD/MODIFY** screen for groupings.

Configuring the Advanced Search Grid To Search for Owners on Groupings Tab

You can use the **ADVANCED SEARCH** (see *Figure*) to search for a grouping owner. The Search Result grid that appears on the **ACCESS SEARCH** shows results based on your search criteria. Use the **ADMIN.CATALOGMODIFY.GROUPINGOWNERPROFILESEARCH** global option to configure the fields. The global option uses the vw_Profile view. To view the fields from the vw_Profile view, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

The default XML is as follows:

```
<grid-columns>

  <column model-name="FirstName" label="First Name" />

  <column model-name="LastName" label="Last Name" />

  <column model-name="Department" label="Department" />

  <column model-name="Location" label="Location" />

  <column model-name="ManagerID" label="Manager" />

  <column model-name="JobCode" label="Job Code" />

</grid-columns>
```

Configuring the Owners or Approvers Drop-down on Groupings Tab

Configure the Search Users drop-down list to search for a grouping owner or an approver (see *Figure*) with the **ADMIN.CATALOGMODIFY.SHAREDPROFILESEARCHPROP** global option. This configuration allows you to set the minimum number of characters required to initiate a query and the maximum number of items to present in a drop-down list.

The default XML is as follows:

```
<dropdown-properties minimum-query="2" maximum-
results="20" />
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Advanced Search Grid To Search for Approvers on Groupings Tab

You can use the **ADVANCED SEARCH** (see *Figure*) to search for a access and definition approvers. The Search Result grid that appears on the **ACCESS SEARCH** shows results based on your search criteria. Use the **ADMIN.CATALOGMODIFY.GROUPINGAPPROVERPROFILESEARCH** configuration to configure the fields. The global option uses the vw_Profile view. To view the fields from the vw_Profile view, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

The default XML is as follows:

```
<grid-columns>

  <column model-name="FirstName" label="First Name" />

  <column model-name="LastName" label="Last Name" />

  <column model-name="Department" label="Department" />

  <column model-name="Location" label="Location" />

  <column model-name="ManagerID" label="Manager" />

  <column model-name="JobCode" label="Job Code" />

</grid-columns>
```

Configuring the Search Tags Drop-down on Groupings Tab

Configure the Search Users drop-down list (see *Figure 35*) on the **ASSIGN TAGS** popup to search for tags with the **ADMIN.CATALOGMODIFY.SHAREDTAGSEARCHPROPERTIES** global option. This configuration allows you to set the minimum number of characters required to initiate a query and the maximum number of items to present in a drop-down list.

The default XML is as follows:

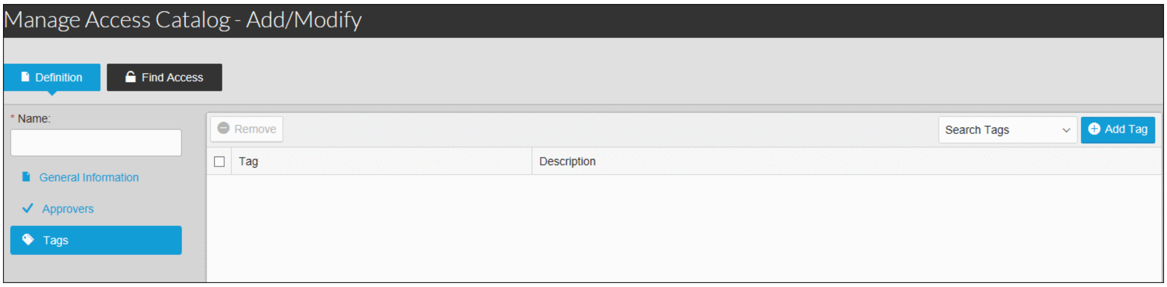
```
<dropdown-properties minimum-query="2" maximum-
results="20" />
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Tag Grid on Groupings Tab

The **TAG** grid (see *Figure 35*) in the **TAGS** section shows the tags that you can select using the Search Tags filter or the new tags you can create using the **ADD TAG** button. Use the **ADMIN.CATALOGMODIFY.SHAREDTAGSEARCHCOLUMNS** global option to configure the grid. The fields are from the vw_Tag view.

Figure 35: Tag Grid



The default XML is as follows:

```
<grid-columns>

  <column model-name="Name" label="Tag"
filterable="false" />

  <column model-name="Description" label="Description"
filterable="false" />

</grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Search Users Drop-down on Find Access Tab

Configure the Search Users drop-down list (see *Figure*) for Intelligent Modeling with the **ADMIN.CATALOGMODIFY.SHAREDPROFILESEARCHPROP** global option. This configuration allows you to set the minimum number of characters required to initiate a query and the maximum number of items to present in a drop-down list.

The default XML is as follows:

```
<dropdown-properties minimum-query="2" maximum-
results="20" />
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring Advanced Search Grid for Intelligent Modeling on Find Access Tab

You can use **Advanced Search** (see *Figure*) to search for users for intelligent modeling. The Search Result grid that appears on the **Access Search** shows results based on your search criteria. Use the **Admin.CatalogModify.AccessCatalogProfileSearch** configuration to configure the fields. The global option uses the vw_Profile view. To configure the grid from the vw_Profile view, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

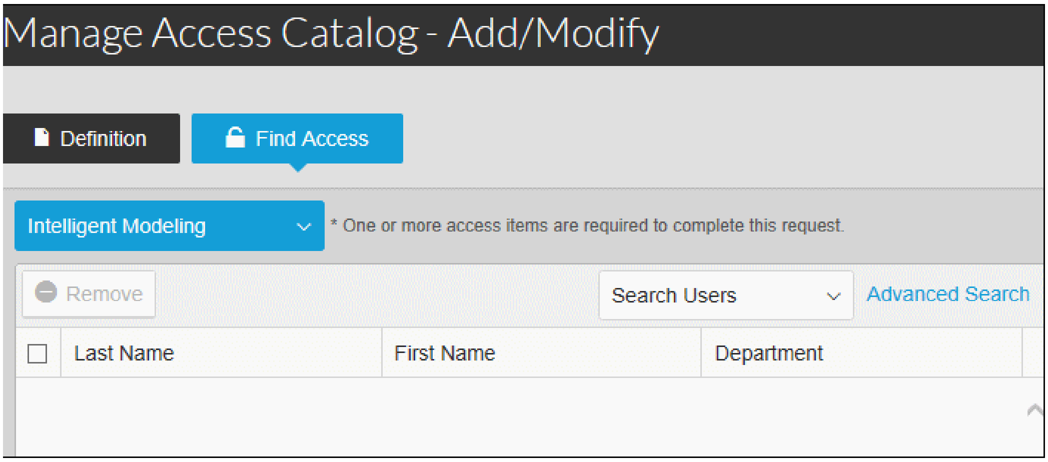
The default XML is as follows:

```
<grid-columns>
  <column model-name="FirstName" label="First Name" />
  <column model-name="LastName" label="Last Name" />
  <column model-name="Department" label="Department" />
  <column model-name="Location" label="Location" />
  <column model-name="ManagerID" label="Manager" />
  <column model-name="JobCode" label="Job Code" />
</grid-columns>
```

Configuring the Profile Grid for Intelligent Modeling

The Profile grid (see *Figure 36*) for Intelligent Modeling on the **Find Access** tab uses the **Admin.CatalogModify.SharedProfileGridColumns** global option. This grid shows the users selected for Intelligent Modeling, and the fields are from the vw_Profile view.

Figure 36: Profile Grid for Intelligent Modeling



* One or more access items are required to complete this request.

□	Last Name	First Name	Department

The default XML is as follows:

```
<grid-columns>
  <column model-name="LastName" label="Last Name" />
```

```
           <column model-name="FirstName" label="First Name" />

           <column model-name="Department" label="Department" />

         </grid-columns>
```

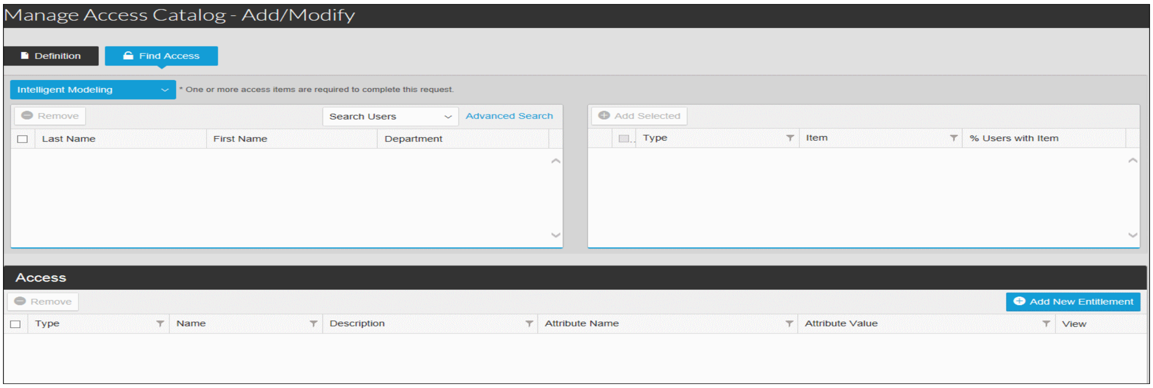
For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Grouping Definition Grid

The **Access** grid appears (see *Figure 37*) at the bottom of both the **Grouping** and **Find Access** tabs when you add or modify a grouping through the **Manage Access Catalog - Add/Modify** screen. The grid is populated when you select access items (groupings and access entitlements) from the **Find Access** tab during grouping definition of a new grouping or while editing an existing grouping.

This virtual grid contains configurable fields that include Name, Description, and OwnerName. These fields are configurable using the **Admin.CatalogModify.GroupingDefAccessGrid** global option. The Type column is non-configurable.

Figure 37: Grouping Definition



* One or more access items are required to complete this request.

The default XML is as follows:

```
         <grid-columns>

           <column model-name="BusinessName" label="Name"
         filterable="true" />

           <column model-name="Description" label="Description"
         filterable="true" />

           <column model-name="Name" label="Attribute Name"
         filterable="true" />

           <column model-name="Value" label="Attribute Value"
         filterable="true" />

          </grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

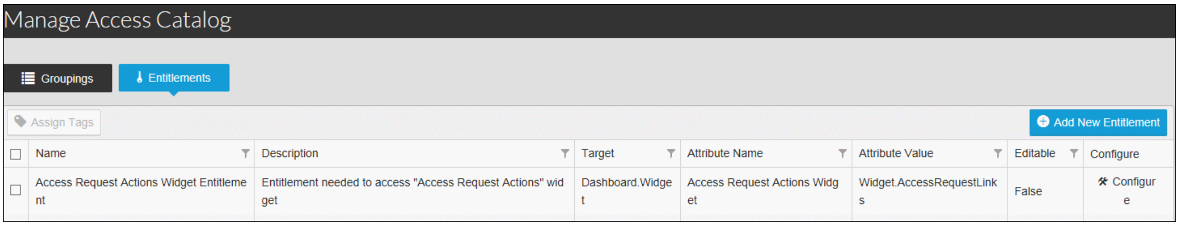
Configuring Items on Entitlements Tab

This section describes the configurations available on the **ENTITLEMENTS** tab.

Configuring the Entitlements Grid

The Entitlements grid (see *Figure 38*) shows the access entitlements from the Entitlement catalog. The grid is configurable using the **ADMIN.CATALOG.SHAREDENTITLEMENTSGRIDCOLUMNS** global option. the fields are from the vw_ManageAccessCatalog_Entitlement view.

Figure 38: Entitlements Grid



□	Name	Description	Target	Attribute Name	Attribute Value	Editable	Configure
□	Access Request Actions Widget Entitlement	Entitlement needed to access "Access Request Actions" widget	Dashboard.Widget	Access Request Actions Widget	Widget.AccessRequestLinks	False	Configure

The default XML is as follows:

```
<grid-columns>

  <column model-name="Description" label="Description" />

  <column model-name="TargetID" label="Target" />

  <column model-name="Name" label="Attribute Name" />

  <column model-name="Value" label="Attribute Value" />

  <column model-name="IsEditable" label="Editable" />

</grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Chapter 8: Configuring the Manage User Access Screen

Using the **MANAGE USER ACCESS** screen you can create the access request workflow, which includes creating a request by selecting recipients, adding or removing access items, and submitting the request for approval.

This chapter describes how to configure the **MANAGE USER ACCESS** screen for the access request workflow, and it includes the following sections:

- *“Configuring Items for Selecting Recipients” on page 74* - Describes how to configure the **GROUPINGS** and **FIND ACCESS** tabs to enable a requester to select recipients.
- *“Configuring Access Items for Managing User Access” on page 79* - Describes how to add groupings and access entitlements.
- *“Configuring Items for Submitting the Request for Approval” on page 80*

Before you configure the grids and drop-downs, review *“Configuring Global Options” on page 27* that describes the global options in general and how to add or edit them.

Note: The global options described in this chapter for the grids and drop-downs are not visible in the **CONFIGURE GLOBAL OPTIONS** screen by default. To add them to the GlobalConfigValues table, follow the steps described in the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

To configure the restriction macros for the **MANAGE USER ACCESS**, see the chapter *“Using Macros” on page 93*.

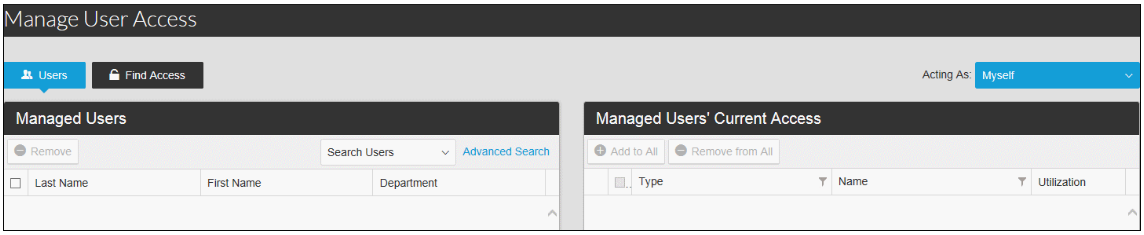
Configuring Items for Selecting Recipients

This section describes the configurations available on the **Users and Access** tabs to enable a requester to search for recipients consistent with the policies specific to your enterprise. The requesters can select themselves as the recipients or select direct reports if the requester is a manager.

Populating the Acting As Drop-Down List on Manage User Access

When a user logs in, he can select who he can act as based on the selection from the **Acting As** drop-down list, as shown in *Figure 39*. The user acts as himself, as by default the **Myself** option is selected. If the user is delegated with the Request Access ARM privilege, the drop-down list shows the name of the owner of the delegated privilege.

Figure 39: Managed Users



Acting As: Myself

The Get Request Delegators custom macro populates the drop-down list with the names of the delegators who have delegated their privileges. For more information about delegation, refer to *"Using Delegation" on page 113*.

Configuring the Managed Users Drop-down on Users Tab

Configure the Search Users drop-down list (see *Figure 39*) with the **Access.ManageUsersAccess.SharedProfileSearchProp** global option. This configuration allows you to set the minimum number of characters required to initiate a query and the maximum number of items to present in a drop-down list.

The default XML is as follows:

```
<dropdown-properties minimum-query="2" maximum-
results="20" />
```

For additional information, refer to the section *"Adding Global Options to the GlobalConfigValues Table" on page 31*.

Configuring the Managed Users Grid With Recipient Information

The **Managed Users** grid (see *Figure 39*) shows the recipients you select for the access request. This grid is configurable using the **Access.ManageUsersAccess.SharedProfileGridColumns** global option**.** The fields are from vw_Profile view.

The default XML is as follows:

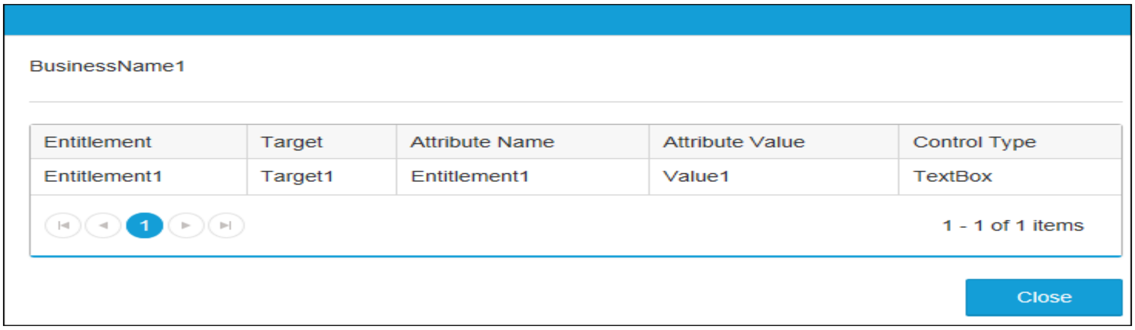
```
<grid-columns>

  <column model-name="LastName" label="Last Name" />

  <column model-name="FirstName" label="First Name" />

  <column model-name="Department" label="Department" />

</grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Grid for Grouping and Access Entitlement Details on Users Tab

The Current Access grid shows all the groupings and access entitlements that the recipients currently own. You can view additional details for an access item by clicking on it. The details are shown in a popup, as in *Figure 40*. The entitlement grid in the popup is configurable using the **ACCESS.MANAGEUSERSACCESS.CURRENTUSERSDETAILSENTITLEMENTSCOLUMNS** global option. This global option uses the vw_ManageAccessCatalog_Entitlement and vw_ManagedUsersCurrentAccessDetails views for the configuration. For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Figure 40: Details of Selected Access Entitlement or Grouping



BusinessName1

Entitlement	Target	Attribute Name	Attribute Value	Control Type
Entitlement1	Target1	Entitlement1	Value1	TextBox

The default XML is as follows:

```
<grid-columns>

  <column model-name="EntitlementName"
label="Entitlement" />

  <column model-name="Target" label="Target" />

  <column model-name="AttributeName" label="Attribute
Name" />

  <column model-name="AttributeValue" label="Attribute
Value "/>

</grid-columns>
```

Configuring the Advanced Search Grid on Users Tab

A requester uses **Advanced Search** to search for one or more recipients on the **Users** tab. The Search Result grid that appears on the **Access Search** shows results based on the requester's search criteria. Use the **Access.ManageUsersAccess.UserMgProfileSearch** global option to configure the fields. The global option uses the vw_Profile view, described in the section *"Adding Global Options to the GlobalConfigValues Table" on page 31*.

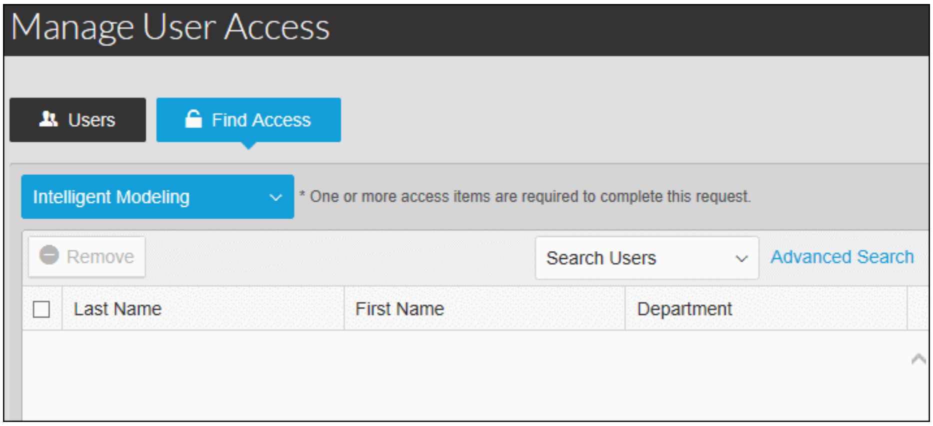
The default XML is as follows:

```
<grid-columns>

  <column model-name="FirstName" label="First Name" />

  <column model-name="LastName" label="Last Name" />

  <column model-name="Department" label="Department" />

  <column model-name="Location" label="Location" />

  <column model-name="ManagerID" label="Manager" />

  <column model-name="JobCode" label="Job Code" />

</grid-columns>
```

Configuring the Search Users Drop-down on Find Access Tab

Configure the Search Users drop-down list (see *Figure 41*) for Intelligent Modeling with the **Access.ManageUsersAccess.SharedProfileSearchProp** global option. This configuration allows you to set the minimum number of characters required to initiate a query and the maximum number of items to present in a drop-down list.

Figure 41: Search Users Drop-Down for Intelligent Modeling With Profile Grid



* One or more access items are required to complete this request.

The default XML is as follows:

```
<dropdown-properties minimum-query="2" maximum-
results="20" />
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Profile Grid for Intelligent Modeling

The Profile grid (see *Figure 41*) shows the users you select through Intelligent Modeling. This grid is configurable using the **ACCESS.MANAGEUSERSACCESS.SHAREDPROFILEGRIDCOLUMNS** global option**.** The fields are from vw_Profile view.

The default XML is as follows:

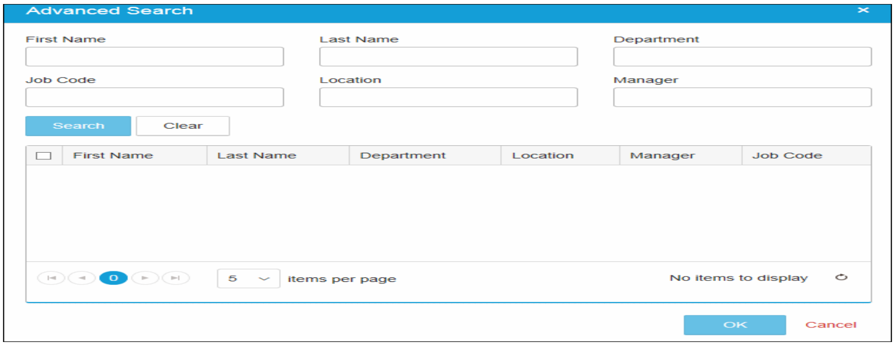
```
        <grid-columns>

          <column model-name="LastName" label="Last Name" />

          <column model-name="FirstName" label="First Name" />

          <column model-name="Department" label="Department" />

</grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring the Advanced Search Grid on Find Access Tab

The **ADVANCED SEARCH** grid enables you to select users for Intelligent Modeling, as shown in *Figure 42*). The grid at the bottom shows the search results based on the requester’s search criteria. Use the **ACCESS.MANAGEUSERSACCESS.USERACCESSPROFILESEARCH** global option to configure the fields in this grid. The global option uses the vw_Profile view. To view the fields in this view, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Figure 42: Search Results



The default XML is as follows:

```
        <grid-columns>

          <column model-name="FirstName" label="First Name" />
```

```
  <column model-name="LastName" label="Last Name" />

  <column model-name="Department" label="Department" />

  <column model-name="Location" label="Location" />

  <column model-name="ManagerID" label="Manager" />

  <column model-name="JobCode" label="Job Code" />

</grid-columns>
```

Configuring Access Items for Managing User Access

Once the requester selects recipients for whom the access is being requested, the requester can manage their current access or select new access items (groupings and entitlements).

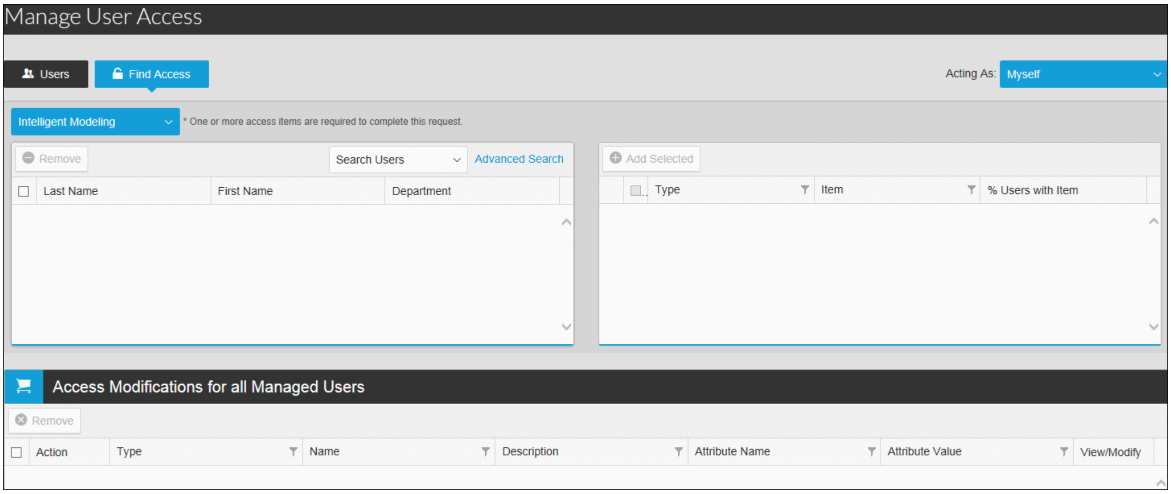
You need to first add groupings and entitlements to the Grouping and Entitlement Catalogs, respectively, before the requester can start managing user access. For additional information about adding access items, refer to the chapter *“Configuring Access Items” on page 47*.

Configuring Items for Submitting the Request for Approval

Requesters can review groupings and access entitlements selected for modifications, removal or additions in the Access Modifications grid before they submit the request for approval.

The Access Modifications grid appears at the bottom of the **USERS** and **FIND ACCESS** tab. This virtual grid shows the groupings and access entitlements selected for modification or removal on the **USERS** tab, and new groupings and access entitlements selected on the **ACCESS** tab. This grid shows several fields, including some that are configurable using the **ACCESS.MANAGEUSERSACCESS.SHAREDACCESSMODIFICATIONGRIDCOLUMNS** global option. The configurable fields include Description, Attribute Name, and AttributeValue. The non-configurable fields include Action, ActionType (Type), and BusinessName (Name). By default, the non-configurable fields precede the configurable fields.

Figure 43: Access Modifications Grid



Acting As: Myself

* One or more access items are required to complete this request.

The default XML is as follows:

```
<grid-columns>

  <column model-name="Description" label="Description" />

  <column model-name="Name" label="Attribute Name" />

  <column model-name="AttributeValue" label="Attribute
Value" />

</grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Chapter 9: Configuring the Approval Workflows

This chapter describes how to configure the approval workflows for both the groupings and user access approvals, and includes the following sections:

- *“Adding Definition Approvers for Grouping Approval” on page 82*
- *“Adding Access Approvers for Access Approval” on page 83*
- *“Configuring the Approval Requests”*
- *“Approving New and Modified Groupings”*
- *“Approving Requests” on page 92*

Before you configure the grids and drop-downs, review *“Configuring Global Options” on page 27* that describes the global options in general and how to add or edit them.

Note: Some global options may not be visible in the **CONFIGURE GLOBAL OPTION** by default. To add them to the GlobalConfigValues table, follow the steps described in the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Adding Definition Approvers for Grouping Approval

During a grouping definition, the grouping creator may select definition approvers who approve groupings if the **DEFINITION** approval is checked for them.

You can configure the definition approvers through the **MANAGE ACCESS CATALOG**. For additional information on adding approvers, refer to the section *“Adding Definition and Access Approvers” on page 52*.

For additional information about the grouping approval workflow, refer to the section *“Approving New and Modified Groupings” on page 90*.

Adding Access Approvers for Access Approval

Requests submitted by requesters in the access request workflow are sent to approvers for approval. Managers of the recipients are by default the first-level approvers. The access approvers, who are the second-level approvers are then notified about the request for their approval.

Note: Access approvers receive a notification only if the **ACCESS** approval is checked for them during grouping definition.

You can configure the access approvers through the **MANAGE ACCESS CATALOG**. For additional information on adding approvers, refer to the section *“Adding Definition and Access Approvers” on page 52*.

For additional information about the access request workflow, refer to the section *“Approving Requests” on page 92*.

Configuring the Approval Requests

Approvers can view all the pending approval requests on the **APPROVE REQUESTS** screen. The items that you can configure on the **APPROVE REQUESTS** screen include:

- The delegator list
- The Pending Requests grid
- The grids on the Request Details screen based on the request type
- The editing of access entitlement values

Populating the Acting As Drop-Down List

If the logged in approver is delegated with Manager Approval or Access Approval privileges, the Acting As drop-down list displays names of delegators. The approver selects the name of the delegator he is acting as to approve any outstanding requests pending for that delegator. To know more about delegation, refer to the chapter *"Using Delegation" on page 113*.

This drop-down list is populated by the Get Approval Delegators custom macro, which you can modify.

Showing Pending Requests Based on Selection from Acting-As Drop-Down List

If the approver selects Myself from the **ACTING AS** drop-down list, the approver sees pending requests requiring his approval.

If the approver selects a delegator, the pending requests shown are based on the ARM privilege of the delegator. For example, if the delegator is a Manager, pending requests for only Manager Approval are shown.

The Get Delegatee ApprovalTypes custom macro determines which pending requests are shown, based on the selection from the **ACTING AS** drop-down list.

For more information about delegation, refer to the chapter *"Using Delegation" on page 113*.

Enabling Delegatees to Approve Their Own Requests

By default, delegatees who are delegated with Manager Approval and Access Approval cannot approve requests that were made by them. If you need to enable delegatees to approve their own requests, set the **ALLOWSELFAPPROVAL** to true.

For more information about delegation, refer to the chapter *"Using Delegation" on page 113*.

Setting Up Fields for Pending Requests

The approver can see the pending requests in the Pending Requests grid. Specify the fields for this grid by configuring the **APPROVALQUEUEDISPLAYCOLUMNS** global option. The fields are from the RequestItem table.

Table 12 shows the default values for ApprovalQueueDisplayColumns.

Table 12: ApprovalQueueDisplayColumns Default Values

Column-name	Order	Visible	Label
RequestItem_Id	0	True	Request
Provisioner	1	True	Requestor
Provisionee	2	True	Request For
RequestDate	3	True	Submitted
RequestType	4	True	Request Type
FirstName	5	False	First Name
LastName	6	False	Last name
ManagerID	7	False	Manager ID
Status	8	True	Details

Setting Up Fields for Request Details

The approver can see additional information about a particular request on the **REQUEST DETAILS** screen. The **REQUEST DETAILS** screen changes based on the request type. The request types include Grouping Definition, access Request, and Profile.

The approver can approve or deny the request. You can configure the fields that appear within the respective grids on this screen.

Setting Up Fields To View Requester Details For All Request Types

The approver can see details about the requester in the **REQUEST** grid. This grid is common for all the request types. The information is from the RequestItem table. To specify the fields from the RequestItem table, use the **EDIT COMPLEX VALUES** button for the **APPROVALREQUESTDETAILFIELDS** global option.

Table 13 shows the default values for ApprovalRequestDetailFields.

Table 13: ApprovalRequestDetailFields Default Values

Column-name	Order	Visible	Label
RequestItemId	1	True	Request

Table 13: ApprovalRequestDetailFields Default Values

Column-name	Order	Visible	Label
RequestDate	2	True	Submitted
Provisioner	3	True	Requestor
UserType	4	True	User Type
Comments	5	True	Comment

Configuring Items for Grouping Definition

This section describes the grids specific to the grouping definition.

Setting Up Fields For the Grouping Characteristics Panel

The Grouping Definition request includes a **ROLE CHARACTERISTICS** panel with information about the role owner, and the definition and access approvers.

To configure this panel to show the role details, such as the role owner and role name, use the **APPROVALROLECHARACTERISTICSDISPLAYFIELD** global option. The fields are from the Role table.

Table 14 shows the default values for **APPROVALROLECHARACTERISTICDISPLAYFIELD.**

Table 14: Role Characteristics with Role Details

Column-name	Order	Visible	Label
Name	1	True	Name
AccessType Name	2	True	Access Type
Owner	3	True	Owner
Description	4	True	Description
isAssignable	5	True	Enabled

Table 15 shows the default values for **APPROVALROLECHARACTERISTICSAPPROVERSDISPLAYFIELDS** to show information about the definition and access approvers.

Table 15: Role Characteristics with Definition and Role Approvers

Column-name	Order	Visible	Label
Profile.LastName	1	True	Last Name
Profile.FirstName	2	True	First Name
IsDefinitionapprover	3	True	Definition
IsAddApprover	4	True	Add
IsRemoveApprover	5	True	Remove

The fields for this grid are from the RoleApprover table.

Setting Up the Role Definition Grid

The **ROLE DEFINITION** grid shows details about the role definition, such as the access entitlements used to construct the role. To configure this grid, use the **APPROVALROLEDEFINITIONDISPLAYFIELDS** global option. The columns are from this Entitlement table.

Table 16 shows the default values for **APPROVALROLEDEFINITIONDISPLAYFIELDS** to show information about the role definition.

Table 16: Role Definition

Column-name	Order	Visible	Label
BusinessName	1	True	Business Name
Description	2	True	Description
Name	3	True	Attribute Name
Value	4	True	Attribute Value

Configuring Items for Access Request

This section describes the grids specific for access request.

Setting Up Fields to View Recipient Details for Access Request

The approver can see the recipient information in the **EMPLOYEE** grid for the access and profile request type. The information is from the Profile table. To specify the fields from the Profile table, use the **EDIT COMPLEX VALUES** button for the **APPROVALPROFILEDISPLAYFIELDS** global option.

Table 17 shows the default values for **APPROVALPROFILEDISPLAYFIELDS**.

Table 17: ApprovalProfileDisplayFields Default Values

Column-name	Order	Visible	Label
FirstName	1	True	First Name
LastName	2	True	LastName
StartDate	3	True	Start Date
Location	4	True	Office Location

Enabling Editing of Access Entitlement Values for Access Request

The approver can edit an access entitlement value for an access entitlement before approving a request.

To enable the approver to change the access entitlement value, configure the **ALLOWATTRIBUTEVALUEEDITINGONAPPROVAL** global option by changing the **CONFIG VALUE** to **TRUE**. The default **CONFIG VALUE** is **FALSE**, which makes the access entitlement value read only.

Note: An access entitlement value is editable only if the **USER VISIBLE** is set to true, and **EDITABLE** is checked when you create an access entitlement. For additional information about making the access entitlement value user visible and editable, refer to the *“Adding Access Entitlements” on page 59* section.

Configuring the Access Grid

The **ACCESS** grid shows the access items requested for the recipient. You can configure this grid using the **SHAREDACCESSGRIDCOLUMNS** global option.

The default XML for the global option:

```
<grid-columns>

<column model-name="ActionStatus" label="Status"/>

  <column model-name="ApprovalAction" label="Action"/>

  <column model-name="AccessType" label="Type"/>

  <column model-name="Name" label="Name"/>

  <column model-name="Comment" label="Comment"/>

</grid-columns>
```

For additional information, refer to the section *“Adding Global Options to the GlobalConfigValues Table” on page 31*.

Configuring Items for Profile Request

To configure the **EMPLOYEE** grid, refer to *“Setting Up Fields to View Recipient Details for Access Request” on page 87*.

Configuring the Approve and Deny Action Buttons

The approver can approve or deny a request by clicking the action buttons.

To set up the **APPROVE** button, configure the **APPROVALACTIONAPPROVE** global option. Table 18 shows the default values for **APPROVALACTIONAPPROVE.**

Table 18: ApprovalActionApprove Default Values

Column-name	Label	Require-comment	ImageURL
Approve	Approve	False	Accepts a path for an image.

To set up the **DENY** button, configure the **APPROVALACTIONDENY** global option. Table 19 shows the default values for **APPROVALACTIONDENY.**

Table 19: ApprovalActionDeny Default Values

Column-name	Label	Require-comment	ImageURL
Deny	Deny	True	Accepts a path for an image.

If the require-comment field is set to true, the approver is required to provide a comment. If the field is set to false, the comment is optional.

Note: The **COLUMN-NAME** in **APPROVALACTIONAPPROVE** and **APPROVALACTIONDENY** identifies an action.

Approving New and Modified Groupings

If you create a new grouping, the grouping needs to be first approved and enabled before it can be used in a grouping definition of another grouping or in an access request. Follow the steps in *“Adding a Grouping” on page 51* to create and submit a new grouping for approval.

Similarly, if a grouping is modified it needs to be approved before it can be used in another grouping definition or access request. For information about editing groupings, refer to *“Editing an Existing Grouping” on page 57*.

When a grouping definition is sent for approval, the approver can either approve or deny the entire request.

The approval workflow for new and modified groupings involves a sequential process as follows:

1. In the first step of grouping approval, the grouping owner (GO) always takes the first action to approve or deny the grouping.
2. In the second step of approval, any grouping definition approver (GDA) can approve or deny the grouping. Since the grouping definition may include several grouping definition approvers, the first RDA to take the action determines if the grouping is approved or denied.

The approval workflow fails if either the grouping owner or any grouping definition approver denies a grouping definition.

The approval workflow for new and modified grouping depends on the grouping definition indicated in Table 20 .

Table 20: Grouping Approval

Who Created or Modified the Grouping	First Step of Grouping Approval	Second Step of Grouping Approval	Grouping Approval Status
User	Grouping Owner (GO) approves	A Grouping Definition Approver (GDA) approves	Grouping is approved
User	GO approves	GDA denies	Grouping is denied
User	GO approves	No second step approval if no GDAs are specified	Grouping is approved
User	GO denies	No second-step approval	Grouping is denied
Grouping Owner	First step is automatically approved since the user is also the GO	GDA approves	Grouping is approved
Grouping Owner	First step is automatically approved	GDA denies	Grouping is denied

Table 20: Grouping Approval

Who Created or Modified the Grouping	First Step of Grouping Approval	Second Step of Grouping Approval	Grouping Approval Status
Grouping Owner	First step is automatically approved	No second step approval if no GDAs are specified	Grouping is automatically approved

Note: Only enabled groupings can be assigned to users after they are approved. A grouping that is approved, but disabled cannot be assigned to users or used to create other groupings.

Approving Requests

Any bulk request that the requester submits is split and shown as individual requests for each recipient. For example, if a Manager selects three recipients for an access item in a request, the approver receives three individual requests.

The approval workflow varies depending on who requested access. The workflow works as described in the following table.

Table 21: Approval Workflow for Access Requests

Who Requested Access	First Step of Access Request Approval	Second Step of Request Approval	Request Status
User himself	Manager approves	No access approver defined	Request is approved
User himself	Manager approves	Access approver approves (if defined)	Request is approved
User himself	Manager approves	Manager is defined as the access approver. Second step is auto approved.	Request is approved
User himself	Manager denies	No second-step approval	Request is denied
User himself	Manager approves	Access approver denies (if defined)	Request is denied
Manager	First step is auto approved	No access approver defined	Request is approved
Manager	First step is auto approved	Access approver approves	Request is approved
Manager	First step is auto approved	Access approver denies	Request is denied.
Manager	First step is auto approved	Manager is defined as the access approver. Second step is auto approved	Request is approved

Note: Once the Manager approves a request, the request is then sent in parallel to all access approvers. If there are multiple access approvers, the first one to act approves or denies the request.

Chapter 10:Using Macros

This chapter describes how to add, edit or delete macros through the **MANAGE MACROS** screen. It also describes the custom and restriction macros used on the **MANAGE ACCESS CATALOG** and **MANAGE USER ACCESS SCREENS**.

This chapter includes the following sections:

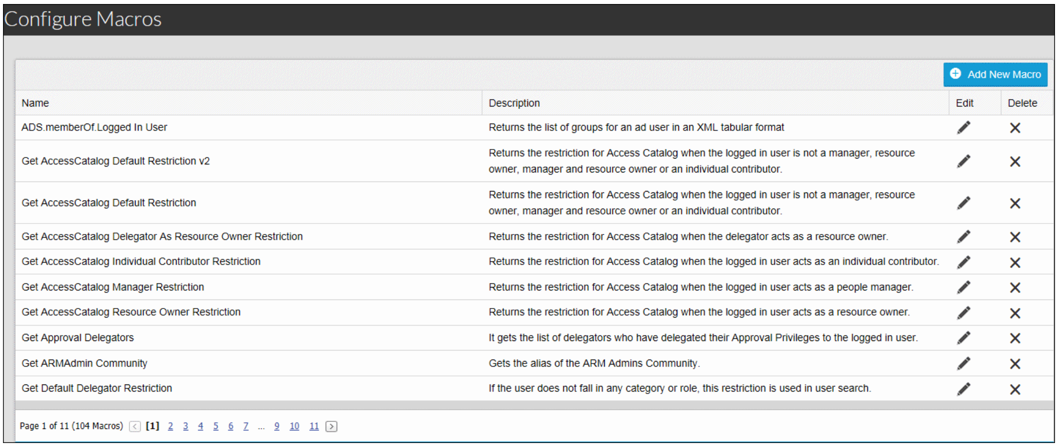
- *“Adding a New Macro” on page 94*
- *“Editing or Deleting an Existing Macro” on page 96*
- *“Using Restriction Macros” on page 97*
- *“Using Custom Macros” on page 110*

Adding a New Macro

To add new macros or edit existing macros, go to the main menu. Click on **Macros** that is available under **Configuration**. The **Configure Macros** screen appears, as shown in *Figure 44*.

Note: You need a Core Provisioning® or a Core Compliance™ license to access the **Manage Macros** screen.

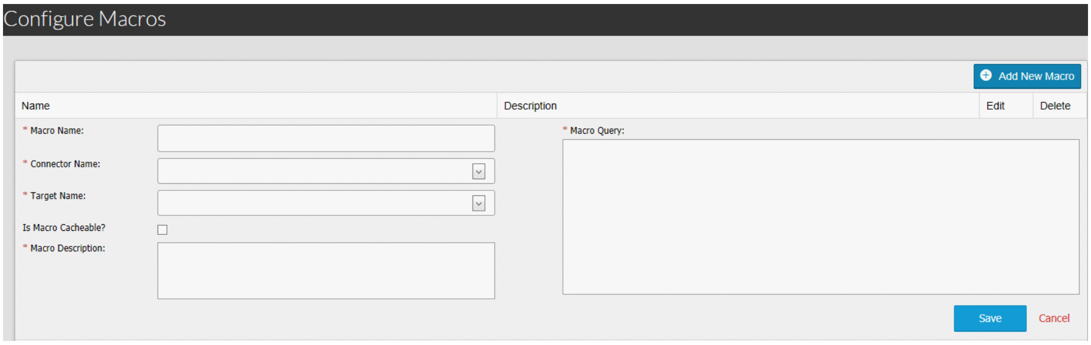
Figure 44: Manage Macros



Name	Description	Edit	Delete
ADS.memberOf.Logged In User	Returns the list of groups for an ad user in an XML tabular format	✎	✕
Get AccessCatalog Default Restriction v2	Returns the restriction for Access Catalog when the logged in user is not a manager, resource owner, manager and resource owner or an individual contributor.	✎	✕
Get AccessCatalog Default Restriction	Returns the restriction for Access Catalog when the logged in user is not a manager, resource owner, manager and resource owner or an individual contributor.	✎	✕
Get AccessCatalog Delegator As Resource Owner Restriction	Returns the restriction for Access Catalog when the delegator acts as a resource owner.	✎	✕
Get AccessCatalog Individual Contributor Restriction	Returns the restriction for Access Catalog when the logged in user acts as an individual contributor.	✎	✕
Get AccessCatalog Manager Restriction	Returns the restriction for Access Catalog when the logged in user acts as a people manager.	✎	✕
Get AccessCatalog Resource Owner Restriction	Returns the restriction for Access Catalog when the logged in user acts as a resource owner.	✎	✕
Get Approval Delegators	It gets the list of delegators who have delegated their Approval Privileges to the logged in user.	✎	✕
Get ARMAdmin Community	Gets the alias of the ARM Admins Community.	✎	✕
Get Default Delegator Restriction	If the user does not fall in any category or role, this restriction is used in user search.	✎	✕

Click **Add New Macro**. The **Manage Macros** screen expands to display the fields required to add a new macro as shown in *Figure 45*.

Figure 45: Add a New Macro



Configure the following fields:

Macro Name: Enter a name for the new custom macro you want to create

Macro Description: Brief description about what the custom macro does.

Connector Name: The name of the connector against which the custom macro is resolved. For example, AD Connector.

Target Name: The name of the configured target for the specified connector. For example, Active Directory.

Is Macro Cacheable: Accepts a boolean value of true or false. Check the checkbox to enable caching. Uncheck the checkbox to disable caching.

Macro Query: A query that runs against the target system. For example, if the target is Active Directory, the query is against this target.

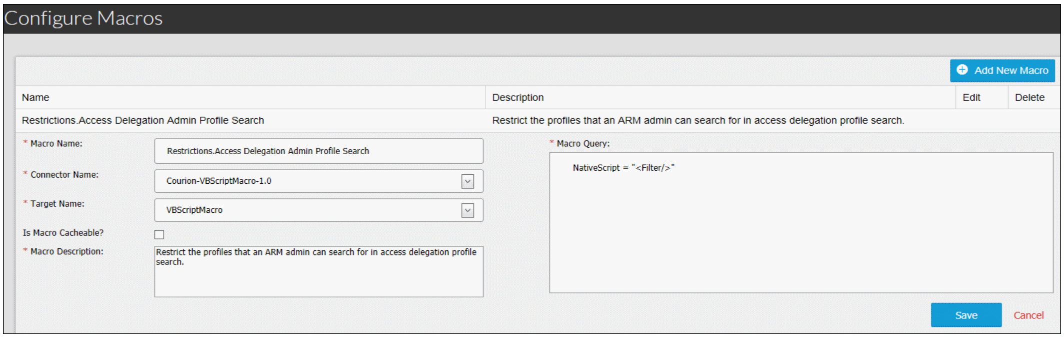
Click **SAVE** to create a new macro. The newly created macro appears in the **MANAGE MACROS** screen.

Click **CANCEL** if you prefer to close the panel without creating a new macro.

Editing or Deleting an Existing Macro

To edit an existing macro, select the Edit icon ✎ . The screen expands to show the configured fields as shown in *Figure 46*.

Figure 46: Edit a Macro



Configure Macros

Name	Description	Edit	Delete
Restrictions.Access Delegation Admin Profile Search	Restrict the profiles that an ARM admin can search for in access delegation profile search.		

* Macro Name: Restrictions.Access Delegation Admin Profile Search

* Connector Name: Courion-VBScriptMacro-1.0

* Target Name: VBScriptMacro

Is Macro Cacheable? □

* Macro Description: Restrict the profiles that an ARM admin can search for in access delegation profile search.

* Macro Query:

```
NativeScript = "<Filter/>"
```

Edit the fields you want, and click **SAVE**.

To delete a custom macro, click the Delete icon ✕ .

Using Restriction Macros

Restriction macros restrict information in the UI elements, including drop-down lists and search filters. Use restriction macros to restrict what a user can or cannot access.

The restriction macros are used on both the **MANAGE ACCESS CATALOG** and **MANAGE USER ACCESS** screens.

Naming a Restriction Macro

A restriction macro needs to conform to the following naming convention:

Restrictions.<restriction macro name>

Other Macros Used Within Restriction Macros

The following macros are automatically available for use within restriction macros:

- %Restrictions-IsArmAdmin% — A boolean value that is represented as a string in lowercase. It indicates whether the logged-in user is an ARM administrator. The value is either set to true or false.
- %Restrictions-LoggedInUser% — The ProfileUID of the logged in user.
- %Restrictions-DelegatedUser% — If the user (delegatee) is acting as the delegator, then the ProfileUID is of the delegator. Otherwise, the value is null.
- %Restrictions-EffectiveUser% — If the user is acting as a delegatee for another user (delegator), the value is the ProfileUID of the delegatee. Otherwise, the value is the ProfileUID of the logged-in user. This value is never empty.

By default, the restriction macros are VBScript macros.

Restrictions Available On Manage Access Catalog

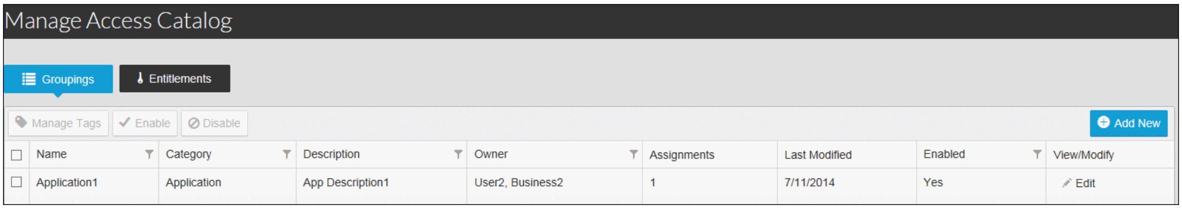
This section describes the restriction macros available for the **MANAGE ACCESS CATALOG** screen.

Restricting the Groupings Grid on Groupings Tab

By default, the groupings grid on the **GROUPINGS** tab shows all the groupings that were created and approved. To restrict the groupings that appear, use the **RESTRICTIONS.MANAGE ACCESS CATALOG ROLES** macro. This restriction macro applies to the vw_Role view.

By default, the ARM administrator can see all the groupings, while grouping owners only see the groupings they own.

Figure 47: Groupings Grid



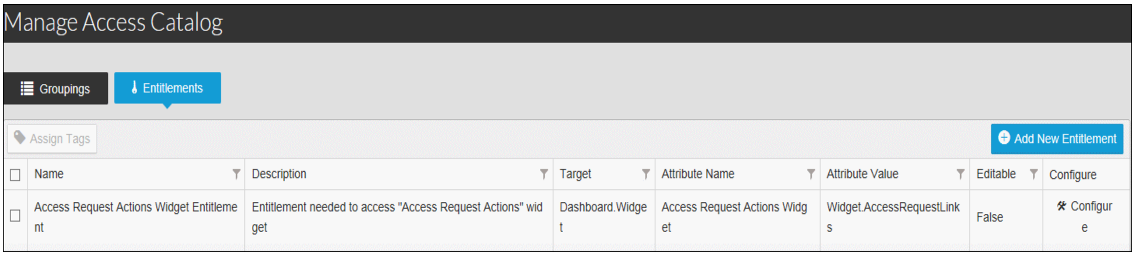
☐	Name	Category	Description	Owner	Assignments	Last Modified	Enabled	View/Modify
☐	Application1	Application	App Description1	User2, Business2	1	7/11/2014	Yes	Edit

Restricting the Access Entitlements Grid on Entitlements Tab

The access entitlements grid on the **ENTITLEMENTS** tab shows all the entitlements to a logged in user. By default there is no restriction applied to this grid. To apply a restriction, you need to create a macro with the name **RESTRICTIONS.MANAGE ACCESS CATALOG ENTITLEMENTS**. This restriction macro applies to the vw_Entitlement view.

To create the macro, refer to the section *“Adding a New Macro” on page 94*.

Figure 48: Access Entitlements Grid



☐	Name	Description	Target	Attribute Name	Attribute Value	Editable	Configure
☐	Access Request Actions Widget Entitlement	Entitlement needed to access "Access Request Actions" widget	Dashboard.Widget	Access Request Actions Widget	Widget.AccessRequestLinks	False	Configure

Restrictions on the Manage Access Catalog - Add/Modify

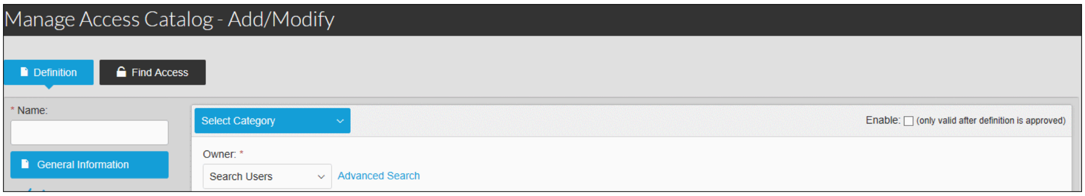
The **MANAGE ACCESS CATALOG - ADD/MODIFY** screen contains the Groupings and Access tabs. Use the restriction macros described in this section, to restrict the grids on these tabs.

Restricting Profiles to Search for Grouping Owners on Groupings Tab

The Search Users drop-down list in **General Information** shows profiles from which you can select a grouping owner. The **Restrictions.Manage Access Catalog Search Owner** macro restricts the profiles shown in this drop-down list. This restriction macro applies to the vw_Profile view.

By default, the list shows all the active profiles.

Figure 49: Owner Drop-Down List

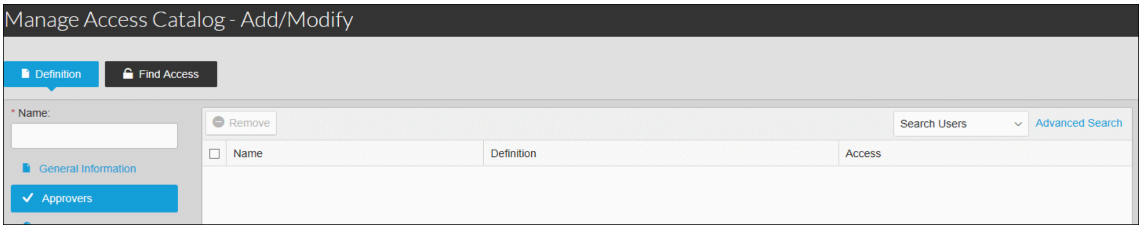


Restricting Profiles to Search for Approvers on Groupings Tab

The Search User drop-down list in the **Approvers** section shows profiles from which you can select one or more approvers. Use the **Restrictions.Manage Access Catalog Search Approvers** macro to restrict the profiles shown in this drop-down list. This restriction macro applies to the vw_Profile view.

By default, the list shows all the active profiles, except the logged in user creating the grouping.

Figure 50: Approver Drop-Down List

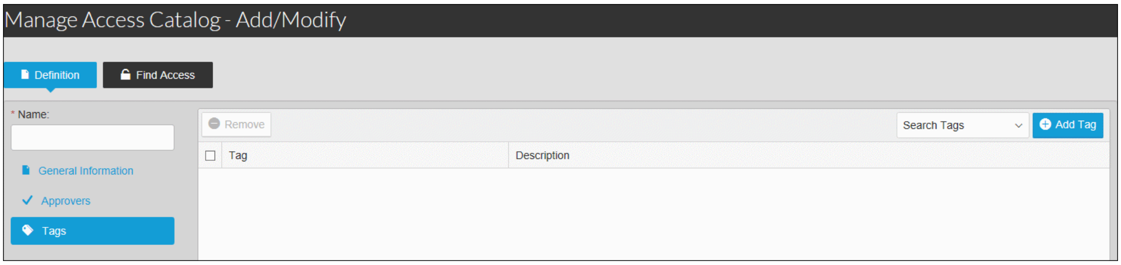


Restricting Search for Tags on Groupings Tab

By default there is no restriction applied to the Search Tags filter in the Tags section. To apply a restriction, you need to create a macro with the name **Restrictions.Manage Role Search Tags**. This restriction macro applies to the vw_Tag view.

To create the macro, refer to the section *"Adding a New Macro" on page 94*.

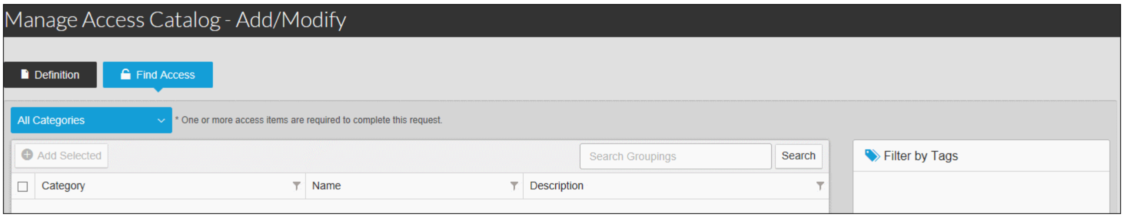
Figure 51: Search Tags Filter



Restricting Search for Groupings on Find Access Tab

A user can search for existing groupings using the **All Categories** drop-down list when they submit a request to create a new grouping. By default, **Restrictions.Manage Access Catalog Search Roles** shows the ARM administrator all the groupings, while grouping owners only see the groupings they own. Modify the restriction macro to change the default restriction. This restriction macro applies to the vw_Role_Tag view.

Figure 52: Find Access By Groupings



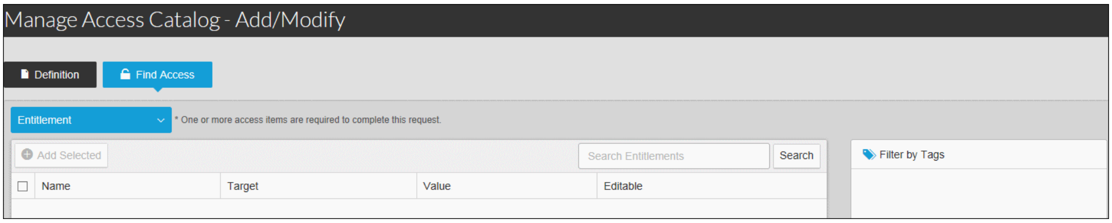
* One or more access items are required to complete this request.

Restricting Search for Entitlements on Access Tab

A user can search for access entitlements using the **All Categories** drop-down list to create a new grouping. By default, there are no restrictions. To apply a restriction, create a macro with the name **Restrictions.Manage Access Catalog Search Entitlements**. This restriction macro applies to the vw_Entitlement_Tag view.

To create the macro, refer to the section *"Adding a New Macro" on page 94*.

Figure 53: Find Access By Entitlements



* One or more access items are required to complete this request.

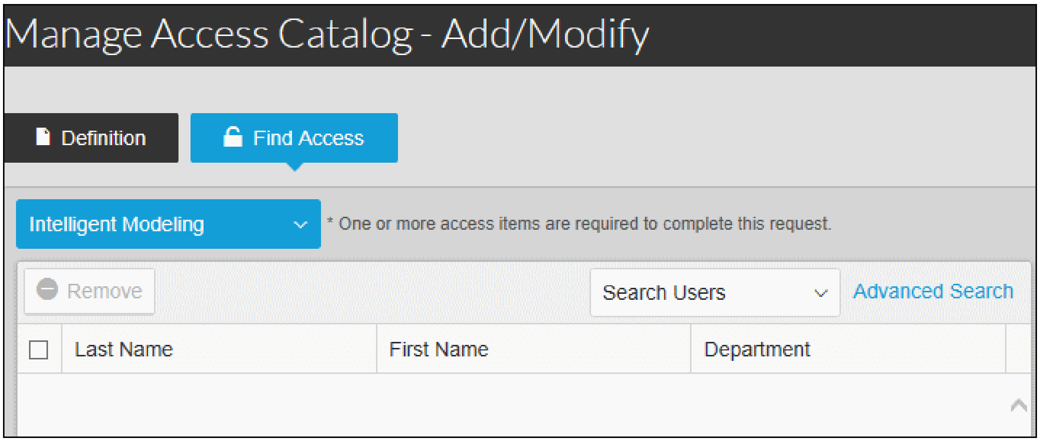
Restricting Search for Profiles on Find Access Tab

To create a grouping, a user (generally, the Manager) can search for profiles using the **All Categories** drop-down list, and selecting **Intelligent Modeling**. The Search Users textbox enables the Manager to search for profiles.

By default, **Restrictions.Manage Access Catalog Search Users** only shows active profiles of the Manager's direct reports.

This restriction macro applies to the vw_Profile view.

Figure 54: Find Access By Intelligent Modeling

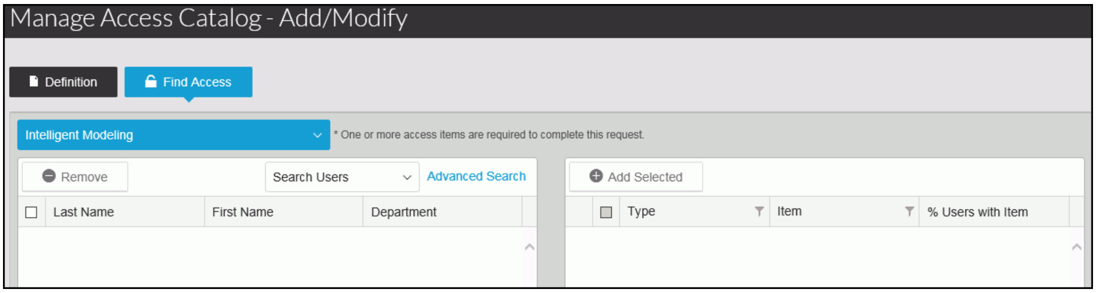


Restricting Display of Groupings and Entitlements under Intelligent Modeling

To create a grouping, a user (generally, the Manager) can search for profiles using the **ALL CATEGORIES** drop-down list, and select **INTELLIGENT MODELING**. The Search Users text box enables the Manager to search for profiles. The user can select grouping and entitlements from the Current Access grid and click the Add Selected button to add them to the grouping.

By default, **RESTRICTIONS.MANAGE CATALOG.INTELLIGENT MODELING.GROUPING** and **RESTRICTIONS.MANAGE CATALOG.INTELLIGENT MODELING.ENTITLEMENT** only show the grouping and entitlements that the user has privileges to view.

Figure 55: Add Groupings and Entitlements by Intelligent Modelling



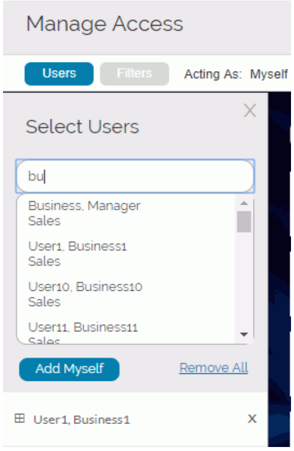
Restrictions Available On Manage User Access

This section describes the restriction macros available for the **MANAGE USER ACCESS** screen.

Restricting Search for Recipients on Users Tab

A logged in user can search for profiles using the Search Users filter to add or modify access for self or other users. The **RESTRICTIONS.MANAGE ACCESS FIND RECIPIENTS** macro restricts the profiles that appear. The ARM administrator sees all users, while a Manager only sees his direct reports. The direct reports may be active or inactive. This restriction macro applies to the vw_Profile view.

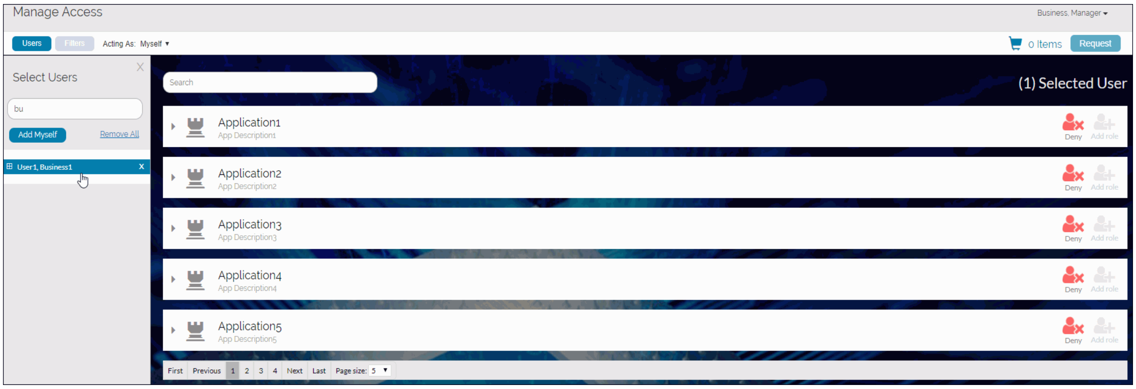
Figure 56: Search Profile



Restricting Display of Groupings and Entitlements on Users Tab

A logged in user can view the current access for self or other users. By default, **RESTRICTIONS.MANAGE USER.USER ACCESS.GROUPING** and **RESTRICTIONS.MANAGE USER.USER ACCESS.ENTITLEMENT** only show the grouping and entitlements in the Managed Users' Current Access grid that the user has privileges to view.

Figure 57: Managed User's Current Access

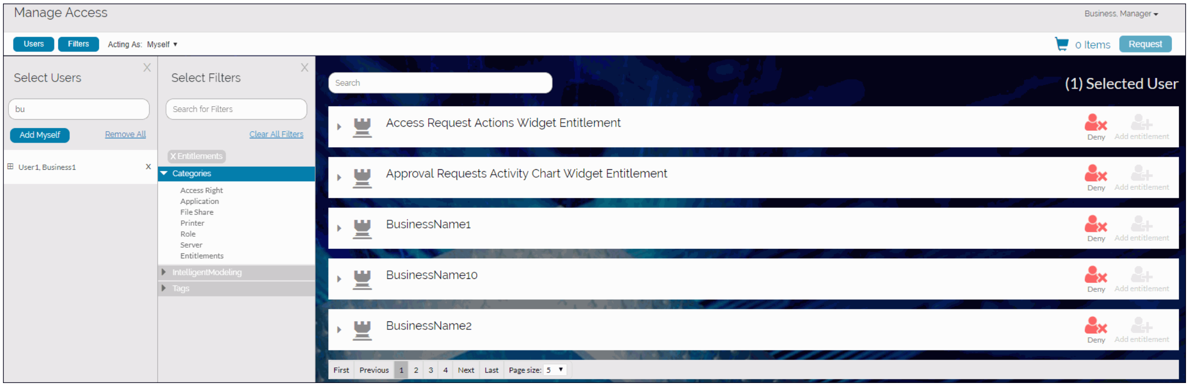


Restricting Search for Groupings on Access Tab

A logged in user searches for groupings using the **ALL CATEGORIES** drop-down list to assign for self or others. By default, the search shows all the groupings. To apply a restriction, create a macro with the name **RESTRICTIONS.MANAGE ACCESS SEARCH ROLES** to restrict the groupings that appear. This restriction macro applies to the vw_Role_Tag view.

To create the macro, refer to the section *"Adding a New Macro" on page 94*.

Figure 58: Find Access By Groupings

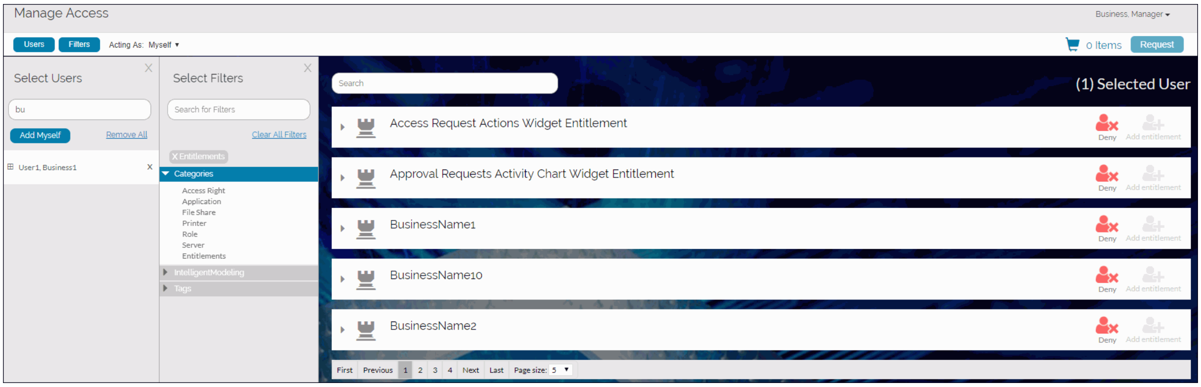


Restricting Search for Access Entitlements on Access Tab

A user can search for access entitlements using the **ALL CATEGORIES** drop-down list to assign to self or others. By default, there are no restrictions and the search shows all the access entitlements. To apply a restriction, create a macro with the name **RESTRICTIONS.MANAGE ACCESS SEARCH ENTITLEMENTS** to restrict the access entitlements that appear.

To create the macro, refer to the section *"Adding a New Macro" on page 94*.

Figure 59: Find Access By Entitlements

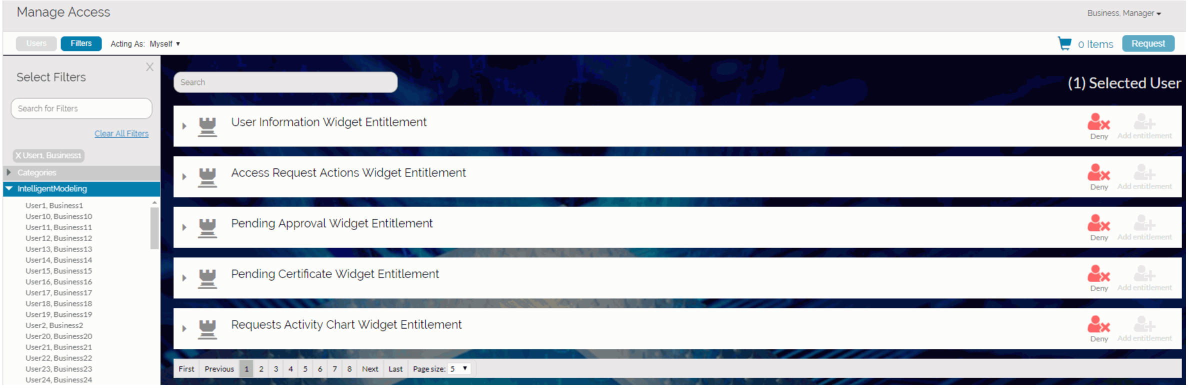


Restricting Search for Profiles on Access Tab

To assign access modeled on another profile, a logged in user searches for profiles using the **ALL CATEGORIES** drop-down list, and selecting **INTELLIGENT MODELING**. The Search Users filter appears with the profiles the user can select. By default, **RESTRICTIONS.MANAGE ACCESS SEARCH USERS** shows only direct reports to a Manager. The profiles need to be active.

This restriction macro applies to the vw_Profile view.

Figure 60: Find Access By Intelligent Modeling

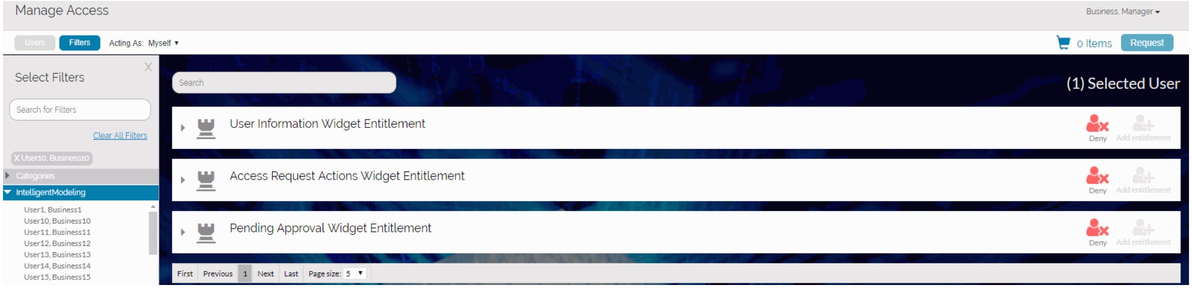


Restricting Display of Groupings and Entitlements under Intelligent Modeling

To assign access modeled on another profile, a logged in user (generally, the Manager) can search for profiles using the **ALL CATEGORIES** drop-down list, and select **INTELLIGENT MODELING**. The Search Users filter appears with the profiles the user can select. The user can select grouping and entitlements and click the Add Selected button to add them to the grouping.

By default, **RESTRICTIONS.MANAGE USER.INTELLIGENT MODELING.GROUPING** and **RESTRICTIONS.MANAGE USER.INTELLIGENT MODELING.ENTITLEMENT** only show the grouping and entitlements that the user has privileges to view.

Figure 61: Add Groupings and Entitlements by Intelligent Modeling



Defining Filter Expressions in Restriction Macros

The restriction macros use a Filter element to filter data. The filter expression you create needs to adhere to the syntax described in this section.

The filter declaration needs to start with the Filter element, and it is case-sensitive. For example:

```
<Filter>
    <!--Filter expression-->
</Filter>
```

Note: The restriction macros can be of any type, such as Javascript, but they must return a valid XML document with a root node called Filter. The minimum allowable return document is <Filter/>.

See Table 22 for the comparison predicates that you can use within a filter expression. A comparison predicate contains one or more conditions, and the condition may be true or false.

Note: The comparison predicates are case-sensitive.

Table 22: Comparison Predicates

Comparison Predicate	Description	Format	Example

Not	Contains a condition which needs to be false.	`<Not>`
		`<!--a single filtering predicate>`
		`</Not>`
			`<Filter>`
			`<Not>`
			`<EqualTo>`
			`<ColumnName>Role_Id</ColumnName>`
			`<Value>Fred’s Role</Value>`
			`</EqualTo>`
			`</Not>`
			`</Filter>`

Table 22: Comparison Predicates

Comparison Predicate	Description	Format	Example
And	Contains a set of conditions, all of which need to be true. The number of contained conditions may be arbitrary.	<And> <!-- a list of filtering predicates --> </And>	<Filter> <And> <EqualTo> <ColumnName>role_id</ColumnName> <Value>32</Value> </EqualTo> <Not> <EqualTo> <ColumnName>Owner</ColumnName> <Value>buser1</Value> </EqualTo> </Not> </And> </Filter>
Or	Contains a set of conditions, of which at least one needs to be true. The number of contained conditions may be arbitrary.	<Or> <!-- a list of filtering predicates --> </Or>	
EqualTo	A single condition in which a comparison between the first and second operands results in equality. The comparison may be between two column names, values or between a column name and a value. The values you compare may be a macro that needs to be resolved.	Comparison between a column name and value: <EqualTo> <ColumnName/> <Value/> </EqualTo> Comparison using a macro: <EqualTo> <ColumnName>Owner</ColumnName> <Value>%Restriction-LoggedInUser%</Value> </EqualTo>	<Filter> <EqualTo> <ColumnName>Role_Id</ColumnName> <Value>Fred’s Role</Value> </EqualTo> </Filter>

Table 22: Comparison Predicates

Comparison Predicate	Description	Format	Example

Contains	A single condition in which the first string contains within it a second string.
	This predicate contains two operands. The first may be a column name or value, and the second is a value.
		`<Contains>`
		`<ColumnName/>`
		`<Value/>`
		`</Contains>`	

StartsWith	A single condition in which the first string starts with the second string.
	This predicate contains two operands. The first may be a column name or value, and the second is a value.
		`<StartsWith>`
		`<ColumnName/>`
		`<Value/>`
		`</StartsWith>`	

EndsWith	A single condition in which the first string ends with the second string.
	This predicate contains two operands. The first may be a column name or value, and the second is a value.
		`<EndsWith>`
		`<ColumnName/>`
		`<Value/>`
		`</EndsWith>`	

Table 22: Comparison Predicates

Comparison Predicate	Description	Format	Example

In	A single condition in which the first operand contains an element from the list represented by remaining operands. The number of list items may be arbitrary.
	The first operand may contain a column name or value. At least one list item needs to contain a string.
	An In condition with exactly one ListItem functions similar to EqualTo.
		`<In>`
		`<ColumnName/>`
		`<ListItem/>`
		`<ListItem/>`
		`</In>`
			`<Filter>`
			`<In>`
			`<ColumnName>tag_id</ColumnName>`
			`<ListItem>4</ListItem>`
			`<ListItem>5</ListItem>`
			`</In>`
			`</Filter>`

IsNull	A condition which tests where a column name or value is null.
	The operand of an IsNull may contain a column name or value.
		`<IsNull>`
		`<ColumnName/>`
		`</IsNull>`
			`<Filter>`
			`<IsNull>`
			`<ColumnName>role_id</ColumnName>`
			`</IsNull>`
			`</Filter>`
			If the operand contains a value with a true return:
			`<Value xsi:nil = “true”/>`

Table 22: Comparison Predicates

Comparison Predicate	Description	Format	Example

GreaterThan	A condition which tests whether a column name or value is greater than another column name or value.
	Either operand may contain a column name or value. The values to be compared may be a macro that needs to be resolved.
	GreaterThan in a Not condition, is equivalent to LessThan or EqualTo.
		`<GreaterThan>`
		`<ColumnName/>`
		`<Value/>`
		`</GreaterThan>`
			`<Filter>`
			`<GreaterThan>`
			`<ColumnName>Assignments</ColumnName>`
			`<Value>12</Value>`
			`</GreaterThan>`
			`</Filter>`

LessThan	A condition which tests whether a column name or value is less than another column name or value.
	Either operand may contain a column name or value. The values to be compared may be a macro that needs to be resolved.
	LessThan in a Not condition, is equivalent to GreaterThan or EqualTo.
		`<LessThan>`
		`<ColumnName/>`
		`<Value/>`
		`</LessThan>`
			`<Filter>`
			`<LessThan> <ColumnName>Assignments</ColumnName>`
			`<Value>1</Value>`
			`</LessThan>`
			`</Filter>`

Using Custom Macros

Custom macros retrieve data from a connector resource based on a specific search criteria. These macros, for example, determine what is shown or hidden on a screen from a user.

Custom Macros for Manage Access Catalog

The custom macros described here are available on the **MANAGE ACCESS CATALOG** to determine whether or not groupings, access entitlements or intelligent modeling are available to a logged in user.

To show or hide a value on this screen, follow these steps:

1. Go to **CONFIGURATION > MACRO**.
2. Navigate to the specific macro for which you need to change the value. For example, to hide groupings from showing on the Manage Access Catalog screen, look for the Has Catalog Find Access by Roles custom macro and click on the Edit icon. Follow the steps in the *“Editing or Deleting an Existing Macro” on page 96*.
3. Change the Macro Query value to true if it is false, and click **SAVE**. The groupings now show on the **MANAGE ACCESS CATALOG** screen for the logged in user.

Show or Hide Groupings

The **HAS CATALOG FIND ACCESS BY ROLES** custom macro determines whether or not the logged in user has access to Groupings on the **FIND ACCESS BY** drop-down list on the **ACCESS** tab. To show Groupings, change the value in the macro query to true. A value of false hides the Groupings from the logged in user.

Show or Hide Access Entitlements

The **HAS CATALOG FIND ACCESS BY ENTITLEMENTS** custom macro determines whether or not the logged in user has access to Entitlements on the **FIND ACCESS BY** drop-down list on the **ACCESS** tab. To show Entitlements, change the value in the macro query to true. A value of false hides the Entitlements from the logged in user.

Show or Hide Intelligent Modeling

The **HAS CATALOG FIND ACCESS BY INTELLIGENT MODELING** custom macro determines whether or not the logged in user has access to Intelligent Modeling on the **FIND ACCESS BY** drop-down list on the **ACCESS** tab. To show Intelligent Modeling, change the value in the macro query to true. A value of false hides the Intelligent Modeling from the logged in user.

Custom Macros for Manage User Access

The custom macros described here are available on the **MANAGE USER ACCESS** to determine whether or not groupings, entitlements or intelligent modeling are available to a logged in user.

To show or hide a value on this screen, follow these steps:

1. Go to **MACRO CONFIGURATION**.
2. Navigate to the specific macro for which you need to change the value. For example, to hide groupings from showing on the Manage Access Catalog screen, look for the Has Catalog Find Access by Roles custom macro and click on the Edit icon. Follow the steps in the *“Editing or Deleting an Existing Macro” on page 96*.
3. Change the Macro Query value to true if it is false, and click **SAVE**. The groupings will now show on the **MANAGE ACCESS CATALOG** screen for the logged in user.

Show or Hide Roles

The Has Access Find Access By Roles custom macro determines whether or not the logged in user has access to Roles on the **FIND ACCESS BY** drop-down list on the **ACCESS** tab. To show Roles, change the value in the macro query to true. A value of false hides the Roles from the logged in user.

Show or Hide Access Entitlements

The Has Access Find Access By Entitlements custom macro determines whether or not the logged in user has access to Entitlements on the **FIND ACCESS BY** drop-down list on the **ACCESS** tab. To show Entitlements, change the value in the macro query to true. A value of false hides the Entitlements from the logged in user.

Show or Hide Intelligent Modeling

The Has Access Find Access By Intelligent Modeling custom macro determines whether or not the logged in user has access to Intelligent Modeling on the **FIND ACCESS BY** drop-down list on the **ACCESS** tab. To show Intelligent Modeling, change the value in the macro query to true. A value of false hides the Intelligent Modeling from the logged in user.

Other Macros Used with Custom Macros

This section describes the macros that you can use with custom macros described in the section *“Using Custom Macros” on page 110* to retrieve user information. To use the macros, use the % sign to enclose them. For example:

```
IF '%EffectiveUserId%' = 'buser2'

Select 'true' as Value

ELSE

Select 'false' as Value
```

Retrieving the User ID of Logged in User

Use the LoggedInUserID macro to retrieve the ProfileUID of the logged-in user.

Retrieving the User ID of the Acting as User

Use the EffectiveUserID macro to retrieve the ProfileUId of the acting as user. For example, a user authenticates in to the Portal with his username. If the user is delegated with other privileges, he may act as the delegator or as himself to request access. This macro identifies who is the acting as user in this scenario.

Retrieving the User ID of the Delegator

Use the DelegatingUserID macro to retrieve the ProfileUID of the delegator.

Chapter 11:Using Delegation

This chapter describes how users can delegate their ARM privileges to others using the **DELEGATE ARM PRIVILEGES** screen. It also describes the global options and restrictions available to configure the search controls.

Before you configure the search controls, review the chapter *“Configuring Global Options” on page 27* that describes in general how to edit global options.

This chapter includes the following sections:

- *“Approving Delegated Requests” on page 119*
- *“Delegating Your ARM Privileges” on page 115*
- *“Approving Delegated Requests” on page 119*
- *“Checking for ARM Privileges Using Custom Macros” on page 120*
- *“Using Restriction Macros for Delegation” on page 122*
- *“Using Global Options for Delegation” on page 124*

The delegation feature enables authorized users to delegate their ARM privileges to others for the access request and approval workflows.

Users who delegate their owned privileges to others are called delegators. Users who receive delegated privileges are called delegatees.

If an administrator delegates privileges of another user, the administrator becomes the delegator. The user, whose privileges were delegated by the administrator, is the owner of the ARM privileges.

Delegation can happen in two ways:

- Delegators delegate their ARM privileges directly to the delegatees. When a user delegates his own privileges, the user is both the delegator and the owner.
- An administrator, on behalf of the owner of the ARM privileges, delegates the owner’s ARM privileges to a delegatee.

When ARM privileges are delegated or withdrawn, notifications are sent to the following users:

- To the delegator (when owner delegates his own privileges) and the delegatee.
- To the administrator (the delegator), the owner, and the delegatee. The notification is also sent to a former delegatee if the delegatee was changed.

At these point in times:

- When delegation is created.
- When delegation starts at least a day after which it was created.
- When delegation is withdrawn or terminated.

The email notification templates for delegation are described in the chapter *“Setting Up Email Notifications”* , which you can customize using the email template editor.

The ARM Privileges that can be delegated include:

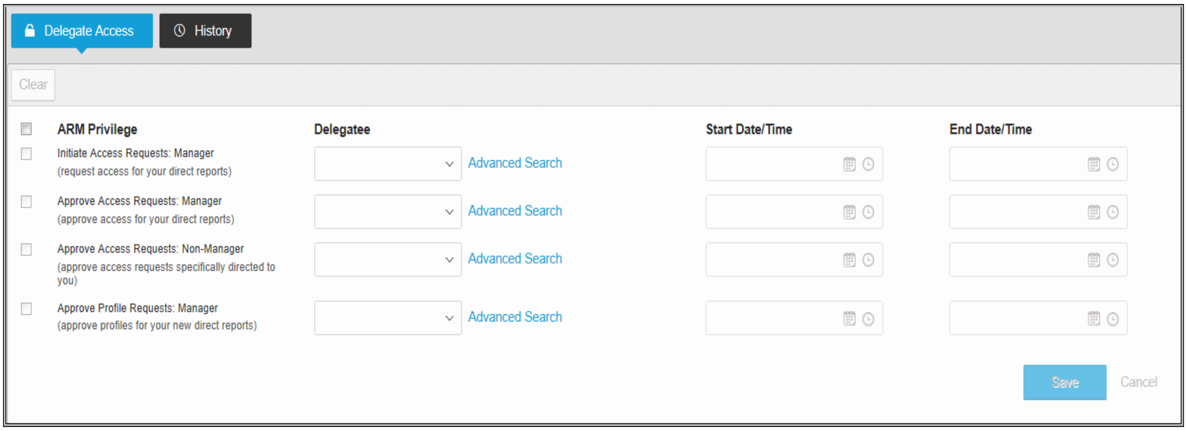
- **Request Access** (Initiate Access Requests: Manager) — This privilege allows business managers to request access for their direct reports.
- **Manager Approval** (Approve Access Requests: Manager) — This privilege allows business managers to approve access for their direct reports when the access is requested by another user. The user who is requesting access may be another user or manager (not a direct manager).
- **Access Approval** (Approve Access Requests: Non-Manager) — This privilege allows users to approve access requests directed to them.
- **Profile Approval** (Approve Profile Requests: Manager) — This privilege allows business managers to approve profile requests for new direct reports.

Delegating Your ARM Privileges

If you are the owner of ARM privileges, then you can delegate them to any active user in the database.

To delegate your privileges, go to the main menu and under **ACCESS** select **DELEGATE APPROVALS**. The **DELEGATE APPROVALS** screen appears as shown. This screen contains the **DELEGATE ACCESS** and **HISTORY** tabs.

Figure 62: Delegate ARM Privileges



□	ARM Privilege	Delegatee		Start Date/Time	End Date/Time
□	Initiate Access Requests: Manager (request access for your direct reports)		Advanced Search		
□	Approve Access Requests: Manager (approve access for your direct reports)		Advanced Search		
□	Approve Access Requests: Non-Manager (approve access requests specifically directed to you)		Advanced Search		
□	Approve Profile Requests: Manager (approve profiles for your new direct reports)		Advanced Search		

The **HISTORY** tab shows the history of actions taken for delegation.

The grid automatically shows your privileges on the **DELEGATE ACCESS** tab. Follow the steps described in the section *"Delegating the Approvals" on page 115* to select a delegatee for delegation.

Similarly, follow the steps in the section *"Withdrawing Delegation" on page 116* to clear a delegatee and withdraw the privileges delegated to them.

For more information about approveals and how to customize the options, refer to the section *"Checking for ARM Privileges Using Custom Macros" on page 120*.

Note: All the privileges in the **DELEGATE APPROVALS** screen are disabled and you cannot delegate privileges if the **ISACCESSDELEGATIONDISABLED** global option is configured to not allow delegation. For more information on this global option, refer to the section,*"Configuring the IsAccessDelegationDisabled Global Option" on page 126*.

Delegating the Approvals

You can delegate each approval individually to a distinct user for a specific period of time. Follow these steps to select a delegatee and the duration of the delegation:

1. Use the **DELEGATEE** textbox. This textbox is enabled with a type-ahead feature that displays the usernames that match as you type. Select the user and hit enter. Alternatively, use the Advanced Search to narrow down your search by using filters. The Delegatee textbox restricts the logged-in user from selecting oneself as the delegatee. Also, the search results only show the active users that are in the database.

2. Specify a start and end date and time during which period the delegation remains active. After the specified end date and time, the delegation is withdrawn automatically from the delegatee. The active period is restricted to start date + 7 days by default. The time period is configurable. Refer to the section *"Using Global Options for Delegation" on page 124*.
3. Click **Save** to confirm your selection.

Withdrawing Delegation

To remove delegatees and withdraw delegation:

1. Select the delegations you prefer to withdraw by selecting the individual checkboxes or the Select All checkbox. If you click the Select All option, only those rows are selected that have a delegatee.
2. Click on the **CLEAR** button to withdraw the selected delegations and remove the selected delegatees.

Administrative Delegation of Approvals

If you are an administrator, you can delegate the privileges owned by another user to a delegatee. For example, if Tom Baker is traveling, then an administrator can delegate his privileges to another user by following these steps:

1. Search for Tom Baker (the owner of the ARM privileges) using your administrator privileges through the **Delegate Approvals** screen.
2. Assign the ARM privileges of Tom Baker to another user (the delegatee).

Note: Only users who belong to the Admin community can delegate on behalf of the owner.

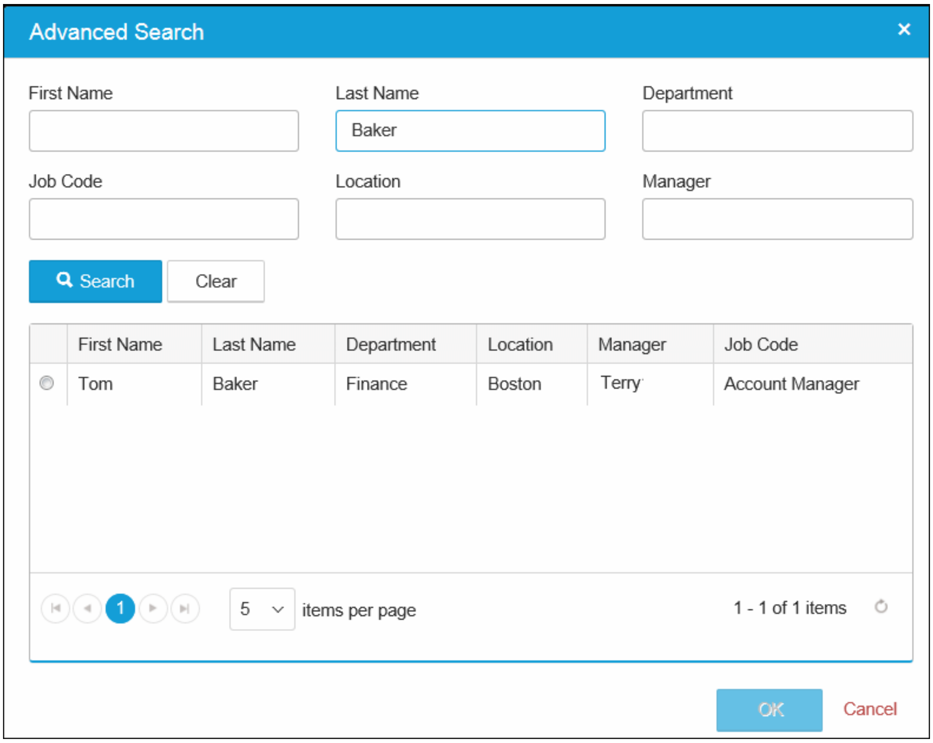
To start delegating, go to the main menu and under **Access**, select **Delegate Approvals**. The **Delegate Approvals** screen contains the **Delegate Access** and **History** tabs.

To select the person whose privileges are delegated (that is, the owner), enter the search string in the drop-down textbox and hit enter. The type-ahead feature shows the closest match.

The drop-down textbox on the **Delegate Approvals** screen is only visible to users who belong to the Admin community. The Get ARMAdmin Community custom macro checks if the user belongs to the Admin Community before the drop-down appears to search for owners. If you want to check for another community, customize this custom macro.

Alternatively, you can use the **Advanced Search** to search for an owner using more filters as shown.

Figure 63: Advanced Search



Advanced Search ×

First Name:

Last Name: Baker

Department:

Job Code:

Location:

Manager:

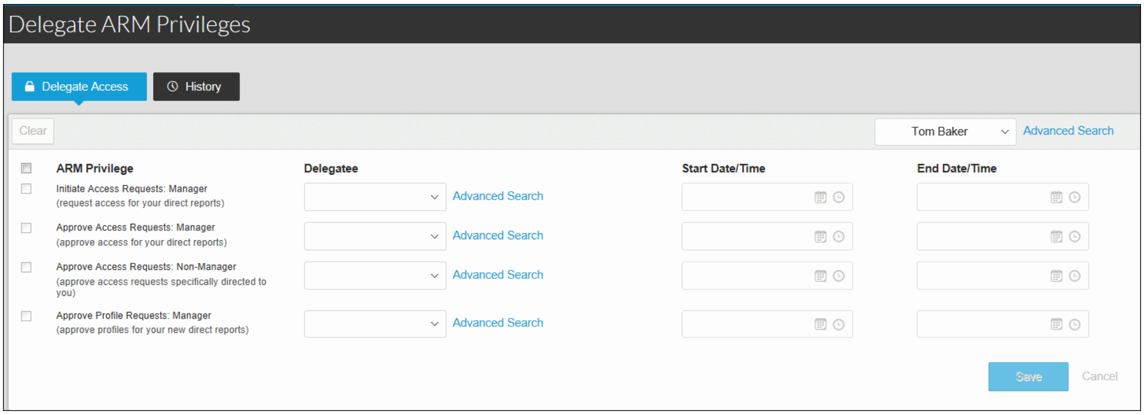
Search | Clear

	First Name	Last Name	Department	Location	Manager	Job Code
○	Tom	Baker	Finance	Boston	Terry	Account Manager

The search results appear at the bottom of the popup. Select the owner and click **OK** to continue. Selecting **Cancel** closes the screen without making any selection.

The selected owner appears in the drop-down textbox of the **DELEGATE APPROVALS** screen. All the privileges that the selected owner holds appear on the **DELEGATE ACCESS** tab as shown.

Figure 64: Administrative Delegation



☐ ARM Privilege	Delegatee	Start Date/Time	End Date/Time
☐ Initiate Access Requests: Manager (request access for your direct reports)	Advanced Search		
☐ Approve Access Requests: Manager (approve access for your direct reports)	Advanced Search		
☐ Approve Access Requests: Non-Manager (approve access requests specifically directed to you)	Advanced Search		
☐ Approve Profile Requests: Manager (approve profiles for your new direct reports)	Advanced Search		

Follow the steps described in the section *“Delegating the Approvals” on page 115* to select a delegatee for delegation.

Similarly, follow the steps in the section *“Withdrawing Delegation” on page 116* to clear a delegatee and withdraw the privileges delegated to them.

For more information about privileges and how to customize the options, refer to the section *“Checking for ARM Privileges Using Custom Macros” on page 120*.

Approving Delegated Requests

When an owner of ARM privileges or an administrator delegates the ARM privileges to another user (delegatee), the delegatee sees approval requests that were delegated when acting as the delegator.

There may be a scenario when a user (for example, Joe) can create and submit an access request for approval. Since Joe requested access for himself, Joe’s Manager would need to approve the request first. However, if the Manager decides to delegate the Manager Approval privilege to Joe, then Joe may be able to approve his own request (while acting as his Manager) if the AllowSelfApproval global option is set to true.

If the AllowSelfApproval global option is set to false, Joe cannot approve his own request.

The default value in the global option is set to false, which does not allow self approvals for delegatees.

Checking for ARM Privileges Using Custom Macros

The Access Request Manager supports the following ARM privileges that a user (delegator) can own and delegate:

- Request Access
- Manager Approval
- Access Approval
- Profile Approval

An ARM privilege determines the scope with which a user interacts within the Access Request Manager. For example, if a delegator has Access Approval, it means that this delegator is selected as an access approver for any grouping and entitlement assignment. If an access approver delegates his Access Approval privilege to a delegatee, the delegatee can approve or deny access requests on behalf of the delegator.

Custom macros are used to check whether or not delegators are entitled to delegate the ARM privileges. These custom macros are described further in this section.

Custom Macros to check for ARM Privileges of a Delegator

Request Access

A manager who has the Request Access privilege can delegate this privilege to his direct report. With this delegated privilege, the direct report (delegatee) can request access when acting as the manager (delegator). The delegatee can request access only for the direct reports of the delegator. For example, if David Larson delegates his ARM privileges to John Smith, then John Smith can request access only for David Larson’s direct reports.

The IsManagerRequestDelegationAvailable custom macro checks if the delegator is entitled to delegate the Request Access privilege.

Manager Approval

A manager who has the Manager Approval access privilege can delegate this privilege to his direct report. With this delegated privilege, the direct report (delegatee) can approve requests when acting as the manager (delegator). The delegatee can only approve pending requests for which the delegator is responsible. For example, if another user requests access for a direct report of David Larson, then David Larson does the first-level approval because he is the manager. With delegation enabled, the direct report (delegatee who has the Manager Approval privilege) does the first-level approval for David Larson (delegator).

The IsApproveAsManagerDelegationAvailable custom macro checks if the delegator is entitled to delegate the Manager Approval privilege.

Access Approval

Any user (delegator) who is specified as an access approver can delegate his Access Approval privilege to another user (delegatee). The delegatee can only approve pending requests that require the second-level approval of the delegator. For example, if Aaron Biggs delegates his Access Approval privilege to John Smith, then John Smith can approve pending requests for which Aaron Biggs is responsible.

The IsApproveAsApproverDelegationAvailable custom macro checks if the delegator is entitled to delegate the Access Approval privilege.

Profile Approval

When a user submits a new profile request, the profile approval follows the approval process described in the chapter *"Creating Profiles" on page 153*. The approver of the profile request can delegate this privilege in his absence.

The IsApproveAsManagerDelegationAvailable custom macro checks if the delegator is entitled to delegate the Profile Approval privilege.

Using Restriction Macros for Delegation

This section describes the restriction macros that limit what a logged-in user sees on the **DELEGATION ARM PRIVILEGES** screen.

Restriction on the Delegator Drop-Down Textbox for an Administrator

When the logged-in user is an administrator, the drop-down textbox for the owner search uses the Restrictions.Access Delegation Admin Profile Search to control which users appear in the search results. By default, there is no restriction.

Restriction on the Delegator Advanced Search for an Administrator

When the logged-in user is an administrator, the Advanced Search popup for the owner uses the Restrictions.Access Delegation Admin Advanced Search to control which users appear in the search results. By default, there is no restriction.

Restriction on the Delegatee Drop-Down Textbox

When the logged in user is an administrator, the Delegatee search for an ARM privilege shows all the users. For other users, the Delegatee search results only show the active users. The logged in user does not appear in the results.

The following macros are used for each ARM privilege:

- For Request Access, it is the Restrictions.Access Delegation Search Request Access Delegatee restriction macro.
- For Manager Approval, it is the Restrictions.Access Delegation Search Approve As Manager Delegatee restriction macro.
- For Access Approval, it is the Restrictions.Access Delegation Search Approve Access Delegatee restriction macro.
- For Profile Approval, it is the Restrictions.Access Delegation Search Approve Profile Delegatee restriction macro.

Restriction on the Advanced Search Popup

For the Delegatee Search, the results vary based on who is the logged in user. If the logged in user is an administrator, the Delegatee search for all the ARM privilege shows all the users without exception. However, for other users who log in, the Delegatee search results only show the active users except the logged in user. The following macros are used for each ARM privilege:

- For Request Access, it is the Restrictions.Access Delegation Advanced Search Request Access Delegatee restriction macro.

- For Manager Approval, it is the Restrictions.Access Delegation Advanced Search Approve As Manager Delegatee restriction macro.
- For Access Approval, it is the Restrictions.Access Delegation Advanced Search Approve Access Delegatee restriction macro.
- For Profile Approval, it is the Restrictions.Access Delegation Advanced Search Approve Profile Delegatee restriction macro.

Restriction on the History Tab

If the logged in user is an administrator, the user sees the delegation history for all the users on the **HISTORY** tab for whom delegation was done. For all other users, the **HISTORY** tab only shows the delegation history for the logged in user. This is enforced by the Restrictions.Access Delegation View History restriction macro.

Using Global Options for Delegation

The global options covered in this section enable the administrator to hide or show the ARM privileges, specify the maximum number of days for active delegation or customize the search controls for delegation.

Hide or Show the Delegation - ARM Privileges Link

The ARMPrivilegeDelegation global option shows the **DELEGATION - ARM PRIVILEGES** link when the value is true. If the value is changed to false, the link is hidden from the menu and delegation becomes unavailable.

Specifying the Maximum Number of Days for Active Delegation

The MaxARMPrivilegeDelegationDays global option allows the administrator to specify the maximum number of days during which delegation is active. The default number of days is seven in the global option. Delegation remains active for a maximum of seven days (default) from the start date and after the specified period, the delegatee cannot approve or deny any ARM privileges on behalf of the delegator.

Customizing the Search Controls

The Delegatee search controls includes a drop-down textbox and an Advanced Search popup. The drop-down textbox enables a string search while the Advanced Search provides a filtered search.

The drop-down textbox for the string search is enabled with the type-ahead feature. As you type, the search results appear in the drop-down list. global options are available for the individual drop-down that appear for every ARM privilege. Use the respective global option to change the number of characters at which the type-ahead feature is enabled and the maximum number of results that can appear. For information about the global options for the string search, see the section *“Customizing the Drop-Down TextBoxes Using Global Options”* .

The search control for the Advanced Search displays a popup with two sections: the top section contains the search fields and the bottom section shows the search results. The global options enable you to configure the fields for the search results. For information about the global options for the Advanced Search, see the section *“Customizing the Advanced Search Using Global Options”* .

Customizing the Drop-Down TextBoxes Using Global Options

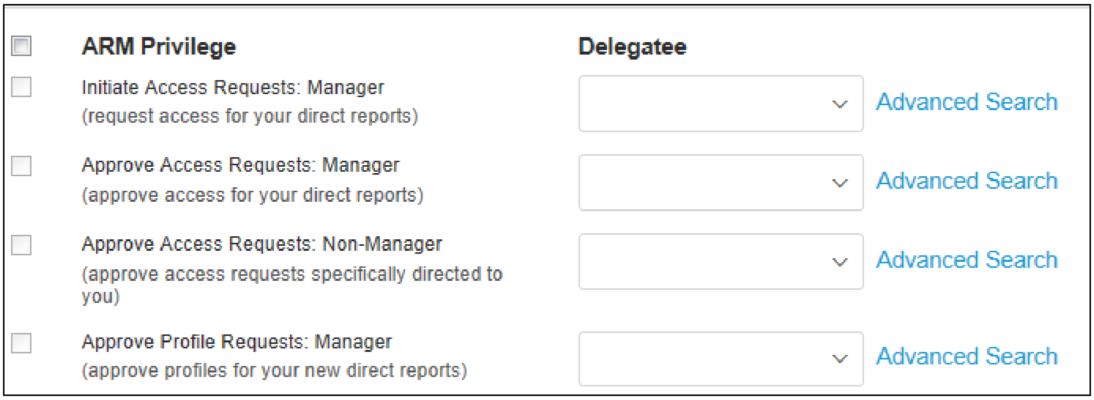
This section describes the global options available to customize the drop-down textbox for the delegatee search and the delegator search if an administrator logs in to delegate privileges of another user. The global options allow you to set the minimum number of characters required to initiate a query and the maximum number of options to present in the drop-down list.

The default XML is as follows:

```
<dropdown-properties minimum-query="2" maximum-results="20" />
```

Figure shows the Delegatee drop-down textbox for each ARM privilege that you can configure.

Figure 65: Delegatee Drop-Down Textbox



□	ARM Privilege	Delegatee	
□	Initiate Access Requests: Manager (request access for your direct reports)		Advanced Search
□	Approve Access Requests: Manager (approve access for your direct reports)		Advanced Search
□	Approve Access Requests: Non-Manager (approve access requests specifically directed to you)		Advanced Search
□	Approve Profile Requests: Manager (approve profiles for your new direct reports)		Advanced Search

For Request Access, use the Actions.AccessDelegation.RequestAccessSearch global option.

For Manager Approval, use the Actions.AccessDelegation.ApproveManagerSearch global option.

For Access Approval, use the Actions.AccessDelegation.ApproveAccessSearch global option.

For Profile Approval, use the Actions.AccessDelegation.ApproveProfileSearch global option.

If an administrator logs in, the administrator can delegate the ARM privileges of another user by searching for that user using the drop-down textbox. This drop-down textbox is configurable using the Actions.AccessDelegation.AdminSearch global option.

Customizing the Advanced Search Using Global Options

This section describes the global options available to customize the Advanced Search for the Delegatee column of each ARM privilege and for the delegator search when you log in as an administrator.

The default XML for each configuration is as follows:

```
<grid-columns>

  <column model-name="FirstName" label="First Name" />

  <column model-name="LastName" label="Last Name" />

  <column model-name="Department" label="Department" />

  <column model-name="Location" label="Location" />

  <column model-name="ManagerID" label="Manager" />

  <column model-name="JobCode" label="Job Code" />

</grid-columns>
```

When you click on **Advanced Search**, a search popup appears similar to *Figure 63*. The search fields in the bottom section of the Advanced Search are configurable using the respective global option for each ARM privilege.

For Request Access, use the Actions.AccessDelegation.RequestAccessAdvanced global option.

For Manager Approval, use the Actions.AccessDelegation.ApproveManagerAdvanced global option.

For Access Approval, use the Actions.AccessDelegation.ApproveAccessAdvanced global option.

For Profile Approval, use the Actions.AccessDelegation.ApproveProfileAdvanced global option.

If an administrator logs in, the administrator can delegate the ARM privileges of another user by searching for that user using the Advanced Search control. The fields in the search results section of the Advanced Search popup are configurable using the Actions.AccessDelegation.AdminAdvanced global option.

Configuring the IsAccessDelegationDisabled Global Option

Using the **IsAccessDealegationDisabled** global option you can enable or disable the delegation of ARM privileges. The default values include:

Config Name — IsAccessDelegationDisabled

Config Type — Text

Config value — False

Description — This configurable variable allows the administrators to disable the ability for users to delegate their ARM privileges. Specifying the values as True disables delegation. The value False or any other value enables delegation.

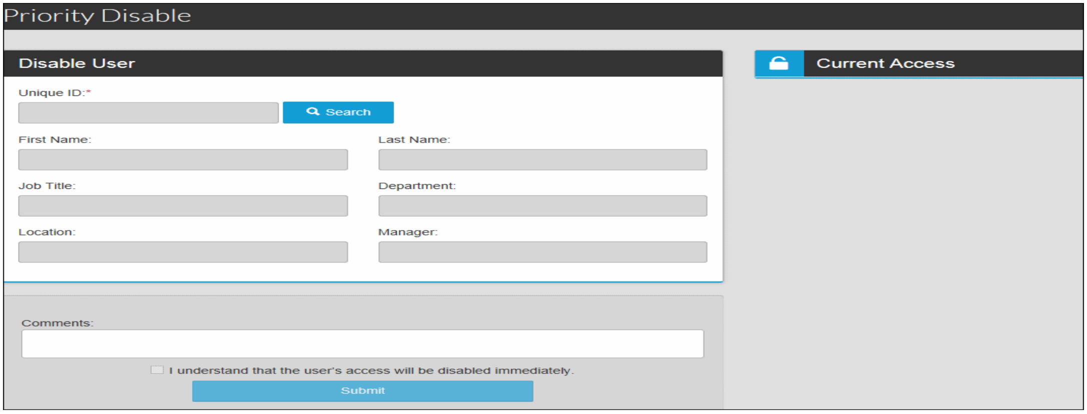
If you set the value to True, all the fields in the **Delegate ARM Privileges** screen are disabled.

Chapter 12:Disabling Access For Terminated Users

This chapter describes how to immediately disable access for users who are being terminated.

To disable access for a user, go to the main menu and under **Admin**, select **Priority Disable.** The **Disable User** screen appears, as shown in *Figure 66*.

Figure 66: Disabling Access with Priority Disable



Click the Search icon to search for the user whose profile needs to be disabled. The **Search Control** popup enables you to select the profile using the search criteria.

Enter any comments you may have, and select the checkbox to **Submit.**

Configuring the Search Control Popup

The **Search Control** popup appears when you search for unique identifiers on the **Disable User** screen. Use the **DisableUserSearchOption** global option to configure the fields that appear on the **Search Control** popup. Refer to *"Configuring Global Options" on page 27* that describes how to edit the global option.

The default values for the **DisableUserSearchOption** are as follows:

- **Heading** — This header appears in the search panel. The default value is Find User.
- **KeyColumn** — ProfileUID is the unique field to search on from the Profile table.
- **IsSingleSelect** — Reserved for future use. The default value is true.
- **RestrictionConfigurationName** — DisableUserSearchRestriction is the name of the default global option that contains a **clause** column. This clause column accepts a custom macro or a SQL clause. Define your restriction in the custom macro and reference the custom macro in the **clause** column. The restriction gets implemented when you search for a user using the **Search Control** screen.

- **ROWSPERRESULTPAGE** — Enter the number of rows to display in the results grid. The default value is 5.
- **RESULTCOLUMNS**: ProfileUID, FirstName, LastName, Location, Department, StartDate. These fields appear in the results grid.

Table 23: DisableUserSearchOption Default Values

Column-name	Order	Visible	Label	Control
ProfileUID	0	True	Employee ID	Text
FirstName	1	True	First Name	Text
LastName	2	True	Last Name	Text
StartDate	3	True	Start Date	DateTime

In the absence of the DisableUserSearchOption global option, the search control uses the default Multiusersearchoption2 global option. The default restriction used with Multiusersearchoption2 is the restriction macro that is specified in the MultiUserSearchRestriction2 global option.

Using the DisableUserSearchRestriction to Implement Restriction

The DisableUserSearchRestriction global option enables you to create a custom macro to implement a restriction for the DisableUserSearchOption. The default values include:

- **NAME**: Priority Disable Restriction
- **VISIBLE**: False
- **LABEL**: Terminated Employees
- **CLAUSE**: Accepts a custom macro or a SQL clause
- **DEFAULTVALUES**: True

Chapter 13: Setting Up Email Notifications

This chapter describes how to configure email notifications that are sent when a request is submitted for approval, using the **CONFIGURE EMAIL TEMPLATES.**

Email notifications are sent to all the relevant users: the requesters, the Business Managers (first-level approvers), and the second-level approvers who participate in the approval of a request.

Note: The Business Managers by default are the first-level approvers.

The **CONFIGURE EMAIL TEMPLATES** offers default email templates for Access Requests, Profile Requests, Grouping Definition, Priority Disable, and Delegation as shown in Table 24 .

Table 24: The Default Email Templates for Notification

Default Email Type	Sent To	Notification is Sent
AccessApproval	Requesters, Business Managers, Second-level approvers	If an access item is approved, notification is sent with information about the access item and the approver. **Note:** Notifications are sent for every access item in a request. For example, if a requester submits a request with three access items and an approver approves two of them, notifications are sent for each approved access item.
AccessDenial	Requesters, Business Managers, Second-level approvers	If an access item is denied, notification is sent with information about the access item and the approver. **Note:** Notifications are sent for every access item in a request. For example, if a requester submits a request with three access items and an approver denies two, notifications are sent for each denied access item.
RequestSubmission	Requester	When a request is submitted.

Table 24: The Default Email Templates for Notification

Default Email Type	Sent To	Notification is Sent
ManagerApproval	Business Manager (first-level approver)	If the requester is other than the Business Manager of the recipient, then the Business Manager receives notification for first-level approval. **Note**: Notification is sent for every single recipient selected in a request. For example, Business Managers receive two notifications if two of their direct reports are selected in a single request. If Business Managers submit requests for their direct reports, the first-level approval is complete.
SecondaryApproval	Second-level approvers	Once the first-level approval is complete, notification is then sent to all second-level approvers.
ProfileRequestSubmission	Requester	When a profile request is submitted.
ProfileApproval	Business Managers	When an approval is required for a new profile.
ProfileApproved	Requester	When a profile is approved.
ProfileDenied	Requester	When a profile is denied.
GroupingDefinitionRequestSubmission	Requester	When a grouping definition request is submitted.
GroupingDefOwnerPending	Requester	When a grouping definition is pending approval from a grouping owner.
GroupingDefApproverPending	Requester	When a grouping definition is pending approval from an approver.
GroupingDefSolicitOwner	Owner (if first-level approver)	Solicits the owner to take action on the pending approval.
GroupingDefSolicitApprover	Second-level approvers	Solicits the approver to take action on the pending approval.
GroupingDefapprove	Requester, Owner, Second-level approvers	When a grouping definition request is approved.
GroupingDefDeny	Requester, Owner, Second-level approvers	When a grouping definition request is denied.

Table 24: The Default Email Templates for Notification

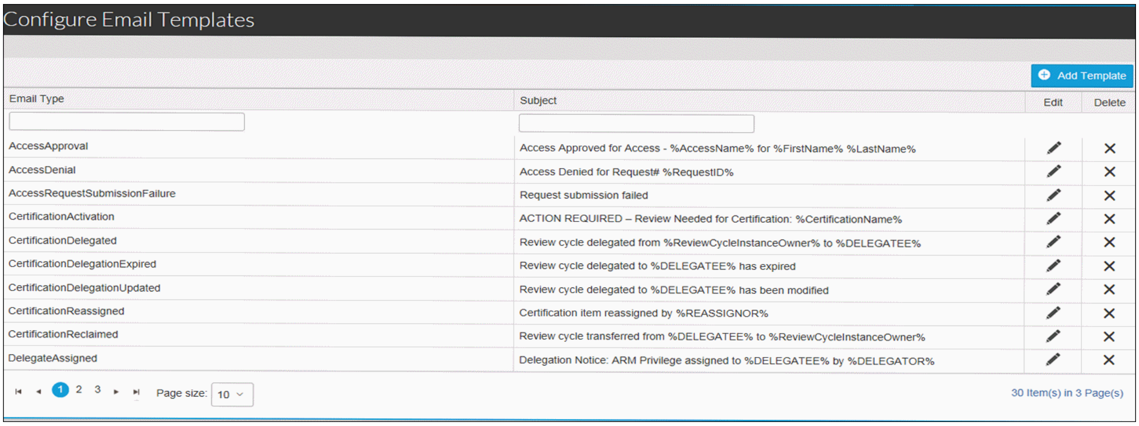
Default Email Type	Sent To	Notification is Sent
GroupingDefComplete	Requester	When all the approval are done and the grouping definition is completed.
PriorityDisableRequestSubmission	Requester	When a request is submitted to disable access for a terminated user.
DelegateAssigned	Delegators and Delegatees	When delegation is enabled
DelegateWithdrawn	Delegators and Delegatees	When delegation is disabled

Editing a Default Email Template

To add a new template or to customize an existing template, follow these steps:

1. From the main menu, select **CONFIGURATION > EMAIL TEMPLATES**. The **CONFIGURE EMAIL TEMPLATES** appears as shown in *Figure 67*.

Figure 67: Email Templates Manager

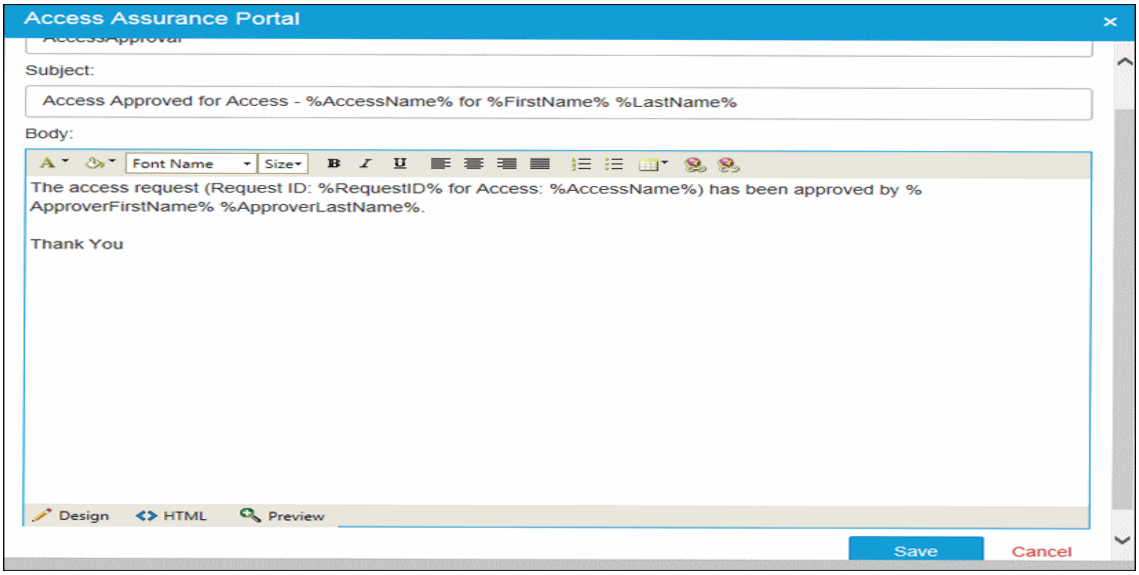


Configure Email Templates

Email Type	Subject	Edit	Delete
AccessApproval	Access Approved for Access - %AccessName% for %FirstName% %LastName%	✎	✕
AccessDenial	Access Denied for Request# %RequestID%	✎	✕
AccessRequestSubmissionFailure	Request submission failed	✎	✕
CertificationActivation	ACTION REQUIRED – Review Needed for Certification: %CertificationName%	✎	✕
CertificationDelegated	Review cycle delegated from %ReviewCycleInstanceOwner% to %DELEGATEE%	✎	✕
CertificationDelegationExpired	Review cycle delegated to %DELEGATEE% has expired	✎	✕
CertificationDelegationUpdated	Review cycle delegated to %DELEGATEE% has been modified	✎	✕
CertificationReassigned	Certification item reassigned by %REASSIGNOR%	✎	✕
CertificationReclaimed	Review cycle transferred from %DELEGATEE% to %ReviewCycleInstanceOwner%	✎	✕
DelegateAssigned	Delegation Notice: ARM Privilege assigned to %DELEGATEE% by %DELEGATOR%	✎	✕

2. Click on **ADD TEMPLATE** to add a new template or click the Edit icon ✎ to edit an existing template. The template allows you to add or edit the subject and the body text of the email template. For example, *Figure 68* appears if you click the Edit icon.

Figure 68: Add New Email Template



Subject:

Access Approved for Access - %AccessName% for %FirstName% %LastName%

Body:

The access request (Request ID: %RequestID% for Access: %AccessName%) has been approved by %ApproverFirstName% %ApproverLastName%.

Thank You

Add or customize the following fields, depending on your action:

Subject: Enter the topic of the email you want to display to the requester or the approver.

Body: Enter the message you want to send as a notification. The email template macros specified in the %<macros may be used>% retrieve information from the Profile table.

3. Click **Save** to save the message or **Cancel** to reset to the previous message.

Chapter 14: Customizing the Access Request Manager User Interface

This chapter describes how to customize the Access Request Manager user interface using the AccessReqMgrResources.resx resource file. This resource file is found in the [installation-folder]\CoreARMS\App_GlobalResources folder. Use any text editor to edit the resource file.

The resource file enables you to customize the text displayed for buttons, tabs, and dialog boxes for a specific language or culture by editing the <name>/<value> pair of the XML data tag in the resource file.

For example, change the <value> string as indicated:

```
<data name="lblRequiredField" xml:space="preserve">

    <value>What are you acting as?</value>

    <comment>Required label</comment>

</data>
```

Customize the <value> tag to display new text:

```
<data name="APPROVAL_ACTING_AS" xml:space="preserve">

    <value>Acting As:</value>

    <comment>Required label</comment>

</data>
```

The **APPROVE REQUESTS** screen shows “**Acting As”** as the new text.

Displayed Text in the Resource File

Table 25 lists the displayed text available to you for editing in the resource file.

Table 25: Strings in the Resource File

Name	Displayed Text	Type	Location
APPROVAL_ACCESS_ NO_LONGER_EXISTS	Access has been deleted.	Message appears in the **ACCESS** column if an access level was deleted before approval.	**REQUEST DETAILS**

Table 25: Strings in the Resource File

Name	Displayed Text	Type	Location
APPROVAL_ACTING_AS	Acting As:	Help Text	**APPROVE REQUESTS**
APPROVAL_APP_NO_ LONGER_EXISTS	Application has been deleted.	Message appears in the **APPLICATION** column if an application was deleted before approval.	**REQUEST DETAILS**
DELEGATION_SELECT_ ALL_TOOL_TIP	Select or Deselect all	Tool Tip	**DELEGATE ACCESS PRIVILEGES**
DROPDOWN_SELECT_ TEXT	----------Select----------	Text displayed in a drop-down list	As needed
PENDING_APPROVAL_ TEXT	Requests Pending Approval	Label for the grid that shows the pending requests	**APPROVAL QUEUE**

For additional information about the Multi Language Framework (MLF), refer to *The Access Assurance Suite Implementation Guide.*

Customize Interface

The Customize Interface page is used to design the Login, Navigation, and Landing Page screens based on images, colors, and background you select.

Login

The Login screen can be customized with a background, welcome message, and logo.

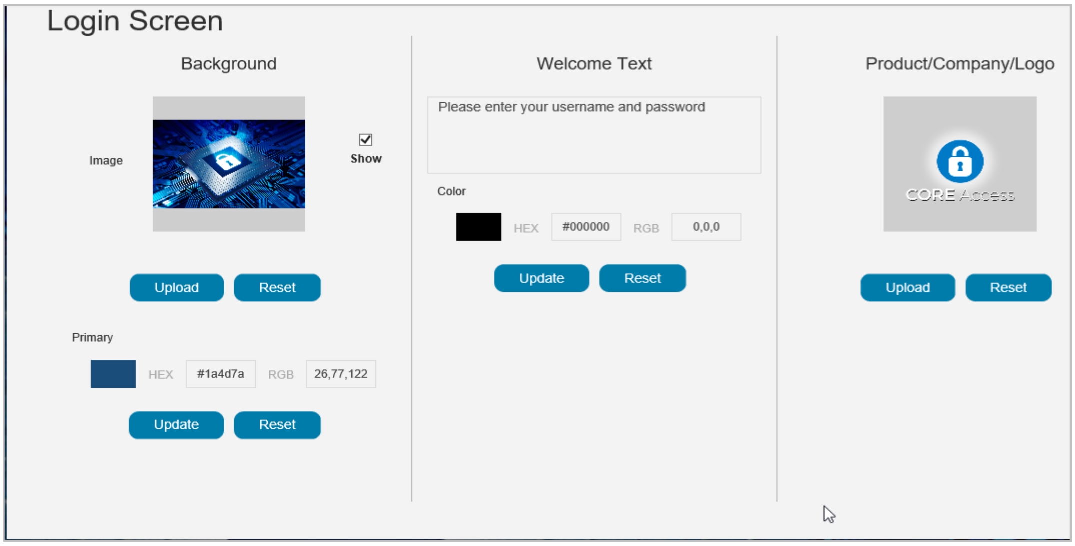
To customize the Login screen:

1. From the Admin menu, select Customize Interface.
2. Select the Login tab.
3. For the *Background*, click the Image icon to select a customized image from the Choose File dialog, then click OK. Press F5 to refresh, there is no need to log in again.

   NOTE: images must be at least 512 Bytes (no max. requirement) in .jpg,.png,.gif, or .jpeg format.
4. Select the Show checkbox, then click Upload to upload the selected image. Note: Click Reset to revert to previous image.
5. Click the Hex color icon to select a color from the palette, then click Update.
6. For the *Welcome Text*, enter a custom message in the text box.
7. Click the Hex color icon to select a color from the palette, then click Update.
8. For the Product/Company/Logo, click the image icon to select a customized image from the Choose File dialog, then click OK.

   Click Upload to upload the selected image.
   NOTE: Click Reset to revert to previous image.

Figure 70: Login



Login Screen

Background

Image ☑ Show

Primary: HEX #1a4d7a RGB 26,77,122

Welcome Text

Please enter your username and password

Color: HEX #000000 RGB 0,0,0

Product/Company/Logo

Navigation

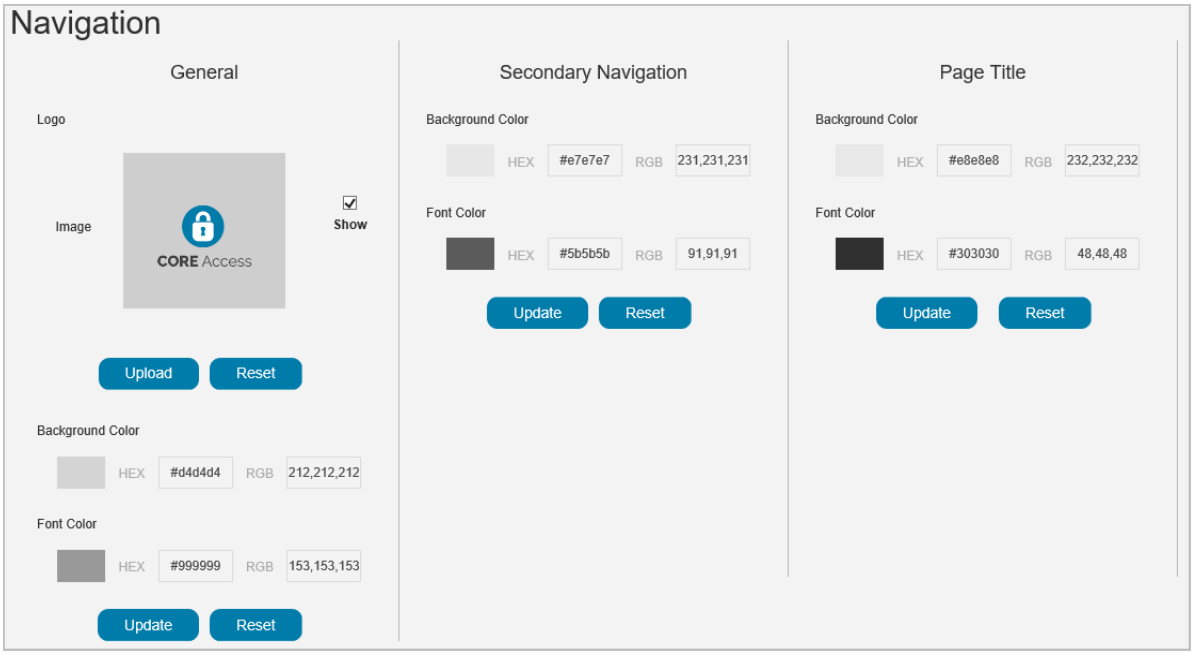
The Navigation screen can be customized with a logo and background colors for secondary navigation and page titles.

To customize the Navigation screen:

1. From the Admin menu, select Customize Interface.
2. Select the Navigation tab.
3. For the *General* design, click the Image icon to select a customized image from the Choose File dialog, then click OK. Press F5 to refresh, there is no need to log in again.

   NOTE: images must be at least 512 Bytes (no max. requirement) in .jpg,.png,.gif, or .jpeg format.
4. Select the Show checkbox, then click Upload to upload the selected image.
   Note: Click Reset to revert to previous image.
5. Click the Hex color icon to select a color from the palette, then click Update.
6. For the *Secondary Navigation*, click the Background Color and Font Color icons to select a color from the palette, then click Update.
7. For the *Page Title*, click the Background Color and Font Color icons to select a color from the palette, then click Update.

Figure 71: Navigation



Navigation

General

Logo

Image ☑ Show

Background Color HEX #d4d4d4 RGB 212,212,212

Font Color HEX #999999 RGB 153,153,153

Secondary Navigation

Background Color HEX #e7e7e7 RGB 231,231,231

Font Color HEX #5b5b5b RGB 91,91,91

Page Title

Background Color HEX #e8e8e8 RGB 232,232,232

Font Color HEX #303030 RGB 48,48,48

Landing Page

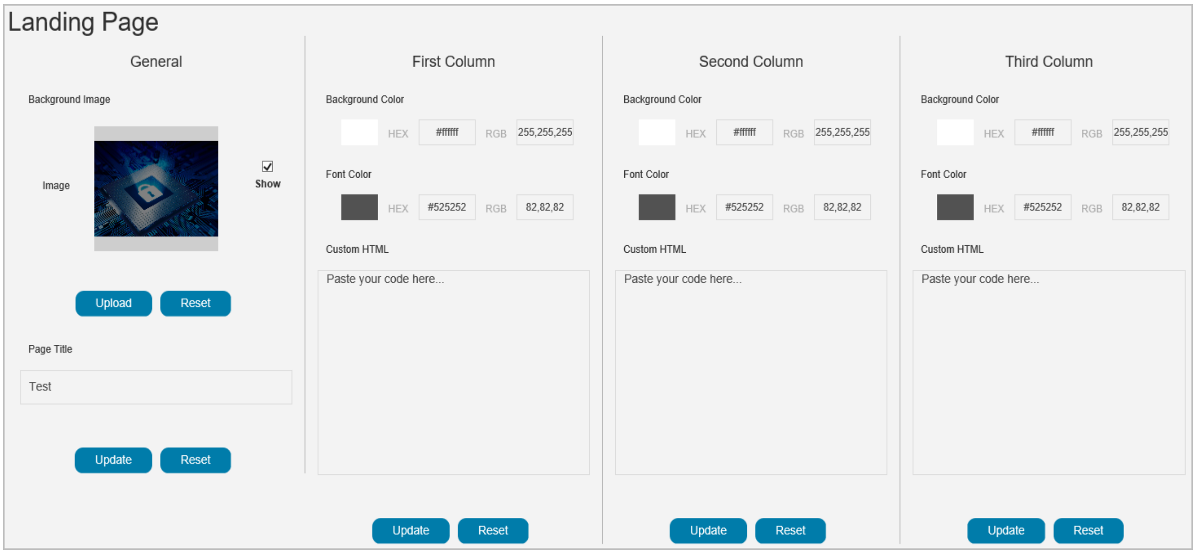
The Landing Page screen can be customized with a logo and background colors for secondary navigation and page titles.

To customize the Landing Page screen:

1. From the Admin menu, select Customize Interface.
2. Select the Landing Page tab.
3. For the *General* design, click the Image icon to select a customized image from the Choose File dialog, then click OK. Press F5 to refresh, there is no need to log in again.

   NOTE: images must be at least 512 Bytes (no max. requirement) in .jpg,.png,.gif, or .jpeg format.
4. Select the Show checkbox, then click Upload to upload the selected image.
   Note: Click Reset to revert to previous image.
5. Enter a Page Title in the text provided, then click Update.
6. For the *First, Second, and Third Column*s, click the Background Color and Font Color icons to select a color from the palette,
7. Enter any safe HTML code in the text box, then click Update.
   NOTE: Only safe HTML code is rendered on the Landing Page.

Figure 72: Landing Page



Landing Page

General

Background Image

Image ☑ Show

Page Title

Test

First Column

Background Color HEX #ffffff RGB 255,255,255

Font Color HEX #525252 RGB 82,82,82

Custom HTML

Paste your code here...

Second Column

Background Color HEX #ffffff RGB 255,255,255

Font Color HEX #525252 RGB 82,82,82

Custom HTML

Paste your code here...

Third Column

Background Color HEX #ffffff RGB 255,255,255

Font Color HEX #525252 RGB 82,82,82

Custom HTML

Paste your code here...

Chapter 15: Managing Access to the Access Request Manager Web Screens

This chapter describes the communities and entitlements that are available to access the Access Assurance Portal.

It also describes how to restrict access to the Access Request Manager web screens based on entitlements, using the **SECURITY ADMINISTRATOR**.

This chapter includes the following sections:

- *“Communities and Entitlements in the Access Assurance Portal” on page 140*
- *“Securing Access to Web Screens in the Access Request Manager” on page 145*

Adding Communities and Entitlements

If you need to add new communities or entitlements, refer to the *Support_Note* document in the www/ Docs folder.

Communities and Entitlements in the Access Assurance Portal

Communities and entitlements enable you to access web screens within the Access Assurance Portal. These communities and entitlements are briefly described in this section. Please note that some communities and entitlements only apply to Core Security products which may or may not be licensed in your environment.

Community

A community is a set of users that have a common set of privileges. The Access Assurance Portal supports the following communities:

- Everyone
- Managers
- Owners
- Approvers
- ARM Admins
- Business Users
- Compliance Analysts
- Compliance Users
- IDM Admins

When users authenticate into the Access Assurance Portal, a macro determines the community to which the users belong by matching the community to their Active Directory group membership. To match a community to an Active Directory group, you must create a corresponding group with the same name in the Active Directory Domain. For more information about configuring Active Directory groups, refer to the chapter *“Configuring the Access Request Manager” on page 21*.

Table 26 lists the community and the corresponding AD group.

Table 26: Communities and their AD Groups

Community	AD Group
Approvers	Approvers
ARM Admins	ARM Admins
Managers	Managers
Business Users	Business Users
Compliance Analysts	Compliance Analysts
Compliance Users	Compliance Users
Everyone	All users in Active Directory
IDM Admins	IDM Admins
Owners	Owners

Entitlements

Entitlements determine the menu items that appear on the Access Assurance Portal and the web screens displayed to the user.

The Access Assurance Portal supports the following entitlements:

- Basic Access
- Manager
- Owner
- Approver
- ARM Admin
- Business User
- Compliance Analyst
- Admin
- IDM Admin

An entitlement consists of zero or more communities. For example, the Business Manager entitlement consists of the Business Managers community. At installation, the default entitlements are mapped to the menu items.

Table 27 lists the default for entitlements, the related communities, AD Groups, and the associated menu items in the Access Assurance Portal.

Table 27: Entitlements with the Related Communities, AD Groups and Menu Items (Sheet 1 of 3)

Entitlement	Community	AD Group	Main Menu Item
Access.Find	Everyone	Everyone	**ACCESS >** **REQUEST ACCESS FOR OTHERS** **REQUEST ACCESS FOR MYSELF**
Basic Access	Everyone	All users in Active Directory	**VIEW REQUESTS**
Role.Approvechange	Approvers and Admins	Approvers and Admins	**APPROVE REQUESTS**
Access.Approvechange	Approvers and ARM Admins	Approvers and ARM Admins	**APPROVE REQUESTS**

Table 27: Entitlements with the Related Communities, AD Groups and Menu Items (Sheet 2 of 3)

Entitlement	Community	AD Group	Main Menu Item
ARM Admin	ARM Admins	ARM Admins	**ACCESS >** **VIEW REQUESTS** **APPROVE REQUESTS** **PRIORITY DISABLE** **ADMIN >** **SECURITY ADMIN** **MANAGE ACCESS CATALOG** **MANAGE CATEGORIES** **CONFIGURATION >** **SECURE FIELDS** **EMAIL TEMPLATES** **GLOBAL OPTIONS** **MACROS** **MANAGE CONTENT** **MIGRATION UTILITY** **PICK LIST**
Entitlement.Catalog	Owners and ARM Admins	Owners and ARM Admins	**ADMIN >** **> MANAGE ACCESS CATALOG**
Role.Catalog	Owners and ARM Admins (or a user-defined community with equivalent collection of entitlements)	Owners and ARM Admins	**ADMIN >** **> MANAGE ACCESS CATALOG**
Business User	Business Users	Business Users	**ACCESS >** **REQUEST ACCESS FOR OTHERS** **REQUEST ACCESS FOR MYSELF** **VIEW REQUESTS** **DELEGATE >** **ARM PRIVILEGES** **REVIEW CYCLES** **MY CERTIFICATIONS**

Table 27: Entitlements with the Related Communities, AD Groups and Menu Items (Sheet 3 of 3)

Entitlement	Community	AD Group	Main Menu Item
Compliance Analyst	Compliance Analysts	Compliance Analysts	Admin > Core Compliance > ReviewCycles Delegate > Review Cycles Admin > Manage Contents Configure > Global Options Email Templates Macros
Admin	ARM Admins	ARM Admins	Admin > Admin Manager
			Admin > Enable Users Secure Fields Migration Utility
IDM Admin	IDM Admins	IDM Admins	Identity Map > Identity Mapping Data Collection Data Feeds Entitlement Mapping Mapping Overview Mapping Reports Configuration > Manage Content
			Admin > Collection Data Collection Data Feeds
			> Mapping Identity Mapping Entitlement Mapping Manage Content

For example, a user who belongs to the Managers AD group is in the Managers community. Since the Managers community resides in the Manager entitlement, all menu items associated with this entitlement are displayed to the user. If a user belongs to multiple groups, the user sees all the related menu items.

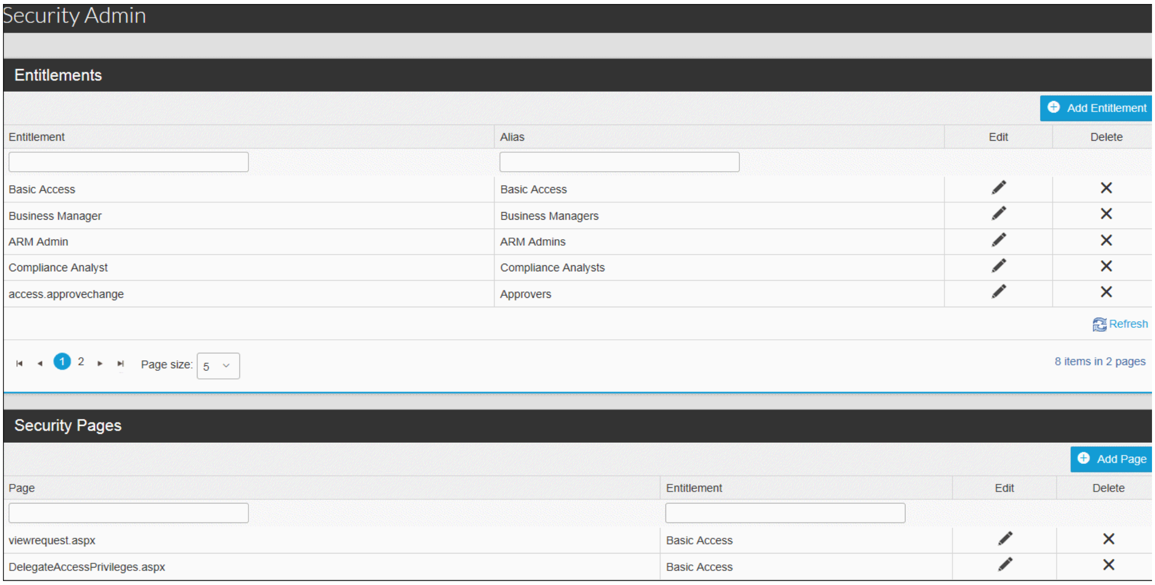
Securing Access to Web Screens in the Access Request Manager

The entitlements also determine the web screens displayed to the user. Follow the steps in this section to give access to specific web screens in the Access Request Manager.

Note: The default is no access.

1. From the main menu, select **Security Admin** under **Admin** The **Security Admin** screen appears as shown in *Figure 73*.

Figure 73: Managing Access with the Security Administrator



Security Admin

Entitlements

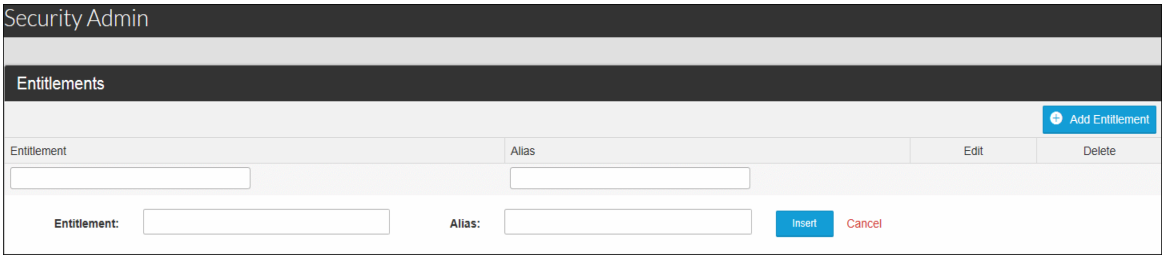
Entitlement	Alias	Edit	Delete
Basic Access	Basic Access	✎	✕
Business Manager	Business Managers	✎	✕
ARM Admin	ARM Admins	✎	✕
Compliance Analyst	Compliance Analysts	✎	✕
access.approvechange	Approvers	✎	✕

Security Pages

Page	Entitlement	Edit	Delete
viewrequest.aspx	Basic Access	✎	✕
DelegateAccessPrivileges.aspx	Basic Access	✎	✕

2. Click **Add Entitlement**. A screen appears for you to add the entitlement and an alias, as shown in *Figure 74*.

Figure 74: Add Entitlement



Security Admin

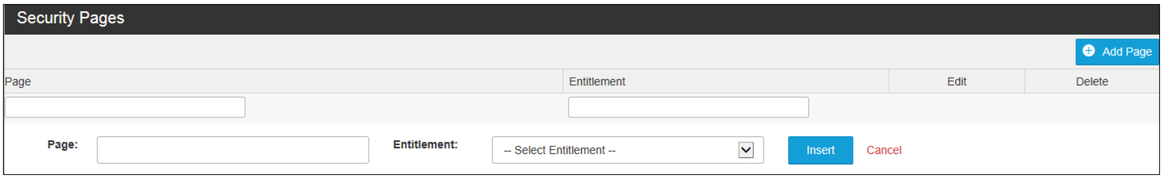
Entitlements

Entitlement	Alias	Edit	Delete

Entitlement: Alias:

3. Enter the **Entitlement** into textbox, such as Business Manager. Enter an **Alias**, such as Business Managers. Click **Insert**.
4. Click **Add Page** to assign a web screen to the entitlement you just added. Enter the web screen in the **Page** field to which you want to enable access, as shown in *Figure 75*.

Figure 75: Add the Web Screen



For example, add accessrequest.aspx. Select the **ENTITLEMENT** alias from the drop-down list, for example Business Managers. Select **INSERT** to add the web screen to the **SECURITY PAGES**. Only those users who belong to the Business Managers community can see the screen you added.

Entitlement and Web Screen Pairs in the Access Request Manager

Table 28 lists the default entitlement and web screen pairs in the Access Request Manager.

Table 28: Web Screens and the Entitlements

Entitlement	Web Screen
Basic Access	viewrequest.aspx
Access.approvechange	approvalqueue.aspx
ARM Admin	disableuser.aspx
ARM Admin	globalconfigurationmanager.aspx
ARM Admin	manageemailtemplates.aspx
ARM Admin	picklistadmin.aspx
ARM Admin	admin/viewrequest.aspx
ARM Admin	securityadmin.aspx
ARM Admin	editemailtemplate.aspx
Role.approvechange	approvalqueue.aspx
Role.Catalog	Manage Access Catalog
Entitlement.Catalog	Manage Access Catalog

Adding Web Screens For a New Entitlement

If, for example, you want to add a new Active Directory group, such as HR Managers and provide access to the Priority Disable screen so they can disable access for a terminated user, follow these steps:

1. Create HR Managers in the Active Directory domain.
2. Add the HR Managers AD group to the AD account of all HR Managers who you want to allow to use the Priority Disable web screen.

3. Create an HR Managers community and add the HR Managers AD group to it.
4. Create an HR Manager entitlement and add the HR Managers community to it.
5. Assign the **PRIORITY DISABLE** menu item to the new HR entitlement. To do this, Follow the steps in *“Configuring Menu Items to the Access Assurance Portal Menu using Menu.XML File” on page 148*.
6. Follow the steps in *“Securing Access to Web Screens in the Access Request Manager” on page 145* to add the web screen disableuser.aspx for the HR Manager entitlement.

Configuring Menu Items to the Access Assurance Portal Menu using Menu.XML File

Overview

As part of Access Assurance Suite 9.0, the portal menus are integrated within the application. This document details the menus shipped out of the box as well as how the menus can be customized.

Main Navigation

The Access Assurance Portal comes with the menus listed in Table 29:

Table 29: Access Assurance Portal Menus

Parent ID	ID	Text	URL	Weight	Required Entitlements	Target
	Access	ACCESS		20		
	Certification	CERTIFICATION		30		
	Password	PASSWORD		40		
	Admin	Admin		50		
	IdentityMap	IDENTITY MAP		60		
	Configuration	CONFIGURATION		70		
Access	Request Access for Myself	Request Access for Myself	~/AccessRequest/Access/ManageMyAccess	20	Access Request:access.find	
Access	Request Access for Others	Request Access for Others	~/AccessRequest/Access/ManageUsersAccess	30	Access Request:access.find	
Access	View Requests	View Requests	~/Areas/AccessRequest/viewrequest.aspx	40	Access Request:Basic Access	
Access	Approve Requests	Approve Requests	~/Areas/AccessRequest/approvalqueue.aspx	50	Access Request:access.approvechange", "Access Request:role.approvechange	
Access	Delegate Approvals	Delegate Approvals	~/AccessRequest/Actions/AccessDelegation	60	Access Request:Business Manager", "Access Request:access.approvechange	
Certification	Delegate Certifications	Delegate Certifications	~/AccessCertification/Delegation/CertificationDelegation	100	Access Certification:Business User","Access Certification:Compliance Analyst	
Certification	My Certifications	My Certifications	~/Areas/AccessCertification/AAPortal.aspx?MetricID=AACertificationTaskList	110	Access Certification:Business User	
Certification	Review Certification Cycles	Review Certification Cycles	~/Areas/AccessCertification/AAPortal.aspx?MetricID=ReviewCycle	120	Access Certification:Compliance Analyst	
Password	Password Reset	Password Reset	/Core/WebSamples/AccessOptions/HTML/PasswordCourier/default.asp	200		
Admin	Admin Manager	Admin Manager	/Core/CustMgrs/AccountCourier/Default.asp	300	Courion Suite:Admin	adminMgrWindow
Admin	Customize Interface	Customize Interface	/admin/customize	310	Access Request:ARM Admin	
Admin	Enable Users	Enable Users	/Core/toolbox/enable_users.asp	320	Courion Suite:Admin	adminMgrWindow
Admin	Priority Disable	Priority Disable	~/Areas/AccessRequest/disableuser.aspx	340	Access Request:ARM Admin	
Admin	Security Admin	Security Admin	~/Areas/AccessRequest/admin/securityadmin.aspx	350	Access Request:ARM Admin	
Admin	Documentation	Documentation	~/Documentation/documentation.html	360	Access Request:ARM Admin	
IdentityMap	Data Collection	Data Collection	~/DataCollection/DataCollectionWizard/Index?ruleType=Collection	400	Data Mapping:IDM Admin	
IdentityMap	Data Feeds	Data Feeds	~/Areas/DataMapping/DataFeeds.aspx	410	Data Mapping:IDM Admin	
IdentityMap	Entitlement Mapping	Entitlement Mapping	~/DataCollection/DataCollectionWizard/Index?ruleType=Mapping	420	Data Mapping:IDM Admin	
IdentityMap	Identity Mapping	Identity Mapping	~/Areas/DataMapping/Rules.aspx	430	Data Mapping:IDM Admin	
IdentityMap	Mapping Overview	Mapping Overview	~/Areas/DataMapping/Dashboard.aspx	440	Data Mapping:IDM Admin	
IdentityMap	Mapping Reports	Mapping Reports	~/Areas/DataMapping/Reports.aspx	450	Data Mapping:IDM Admin	
Configuration	Email Templates	Email Templates	~/Areas/AccessRequest/admin/manageemailtemplates.aspx	500	"Access Request:ARM Admin", "Access Certification:Compliance Analyst	
Configuration	Global Options	Global Options	~/Areas/AccessRequest/admin/globalconfigurationmanager.aspx	510	"Access Request:ARM Admin", "Access Certification:Compliance Analyst	
Configuration	Macros	Macros	~/Areas/AccessRequest/admin/managemacros.aspx	520	"Access Request:ARM Admin", "Access Certification:Compliance Analyst	
Configuration	Manage Content	Manage Content	~/Areas/DataCollection/ManageIDU.aspx	530	" Data Mapping:IDM Admin", "Access Request:ARM Admin", "Access Certification:Compliance Analyst	
Configuration	Migration Utility	Migration Utility	/Core/toolbox/migration.asp	540	Courion Suite:Admin	adminMgrWindow
Configuration	Pick List	Pick List	~/Areas/AccessRequest/admin/picklistadmin.aspx	550	Access Request:ARM Admin	

Customizing the Navigation using XML file

The Core Server Administrator can Add/Remove/Update the menu items in the menu Navigation by using Menu.xml which is located in [Core-installation-folder]\CourionARMS\App_Data.

Following are the key attributes for the menu.xml:

a. Id (required): Unique Identifier of the Menu Item. Use an existing ID if you are updating a menu item and a new ID if you are adding a new menu item. The ID can also be used as the parentid when adding a child menu item.

The Id must be unique and must not exist in the out of the box menus or in any other menu.xml menus.

b. Text (required): Text displayed for the menu.

c. url: URL to navigate to on menu click.

d. weight: The weight is used to determine the display order of the menu items.

- For top level menu items the higher the weight the more to the right the menu appears. For e.g.: Menu1 has weight 10 & Menu2 has weight 20. If I want another menu item in between them I can use the weight 15.
- For child menu items the lighter items float on the top, and the heavier items sink to the bottom.
- This is NOT required. If no weights are specified for added menu items, then the new menu items appear to the right (top-level menus) or below (child menu) existing menu item, and appear in the order in which they appear in the menu.xml file.

The weight should be unique. If two menu items have the same weight, the first one wins and only the first one gets created.

For e.g.:

Scenario 1: We create two menus using the menu.xml as below.

```
<add id="TopLevelMenu1" weight= "70" text="Top Level Menu 1" url="http://
www.coresecurity.com" target="_blank" />
<add id="TopLevelMenu2" weight= "70" text="Top Level Menu 2" url="http://www.
coresecurity.com" target="_blank" />
```

Only TopLevelMenu1 will get created.

Scenario 2: We create a menu using the menu.xml but assign it a weight of an existing menu item.

```
<add id="TopLevelMenu1" weight= "20" text="Top Level Menu 1" url="http://www.
coresecurity.com" target="_blank" />
```

The menu item won’t get created, because a menu item with weight 20 already exists.

e. cssClass: The css class to use.

f. target: The target window to open the link. I.e., “_blank” will open in a new browser window. “adminMgrWindow“ will open in the Admin Manager window. The target attribute is simply the ‘name’ attribute in the standard javascript api:

g. http://www.w3schools.com/jsref/met_win_open.asp

h. enabled: reserved for future use.

i. requiredEntitlements: A semi-colon separated list of entitlements for the menu. For e.g.: `requiredEntitlements="Access Request:Business Manager;Access Request:Access Approver"`

j. image: reserved for future use.

k. parentId (required if modifying an existing child node, or adding a child node): Use this for specifying parent nodes for child nodes.

Adding a New Top Level Menu

A new menu item can be added to the existing menu navigation by adding an ‘add’ node to the menu.xml. You can set any of the above attributes in the add node.

For e.g.:

```
<add id="TopLevelMenu" weight= “70” text="Top Level Menu" url="http://
www.coresecurity.com" target="_blank" />
```

Adding a New Child Menu

A new child menu item can be added using the same ‘add’ node. You can set any of the above attributes in the add node. Please ensure you have specified a parentId that the child menu item should be listed under.

For e.g.:

```
<add id="ChildMenu" weight= “71” text="Child Menu" url="http://www.coresecurity.com"
target="_blank" parentId="TopLevelMenu"/>
```

Adding a New Child to an existing Top Level Menu

If you are adding a child menu item to an existing menu item, you can follow the same steps as mentioned above. Additionally, set the parentId as the Id of the existing menu item.

Removing a Menu

An existing menu item can be removed by adding a ‘remove’ node to the menu.xml. The only attribute this node needs is the id of the menu to be removed. Please note only top level menu items can be removed. Doing so removes the parent and all dependent child menus. You cannot remove a child menu alone.

NOTE: Top level menus must not contain spaces. Including a space in a top level menu may cause it to wrap, resulting on the text becoming partially hidden. Child nodes can contain spaces, and should display properly.

For e.g.:

```
<remove id="TopLevelMenu" />
```

If you want to remove one child menu from a parent menu, then you must remove the parent menu, then recreate it and all child menus that you want to keep.

For e.g., if you have the parent menu “Actions” and you want to remove the menu for “Password Reset”, then you would need to REMOVE the “Actions” menu (which also removes all items on the Actions menu) and then:

<add id=”Actions1” test=”ACTIONS”>

And then add all the child menu items except “Password Reset”, creating unique id’s for each.

Updating a Menu

An existing menu item in the existing menu navigation can be updated by adding an ‘update’ node to the menu.xml. Set the id to the node that you want to modify. You can modify the following attribute: Text, URL, Target and RequiredEntitlements..

For e.g.:

```
<update id="Access Request" text="Request New Access" url="http://
www.coresecurity.com"/ target="_blank" requiredEntitlement="Business Manager;Resource
Owner;ARM Admin” >
```

Chapter 16: Creating Profiles

This chapter describes how to add a new profile and the items for creating and approving a new profile. It includes the following sections:

- *“Configuring Items to Add a New Profile” on page 154*
- *“Configuring DefaultApproverProfileUID Global Option” on page 155*
- *“Approval Workflow for New Profiles” on page 156*
- *“Access Request Approval Workflow for a New Profile” on page 157*

Configuring Items to Add a New Profile

A requester can create a new profile by launching the Profile Manager through the **ACTIONS > CREATE/ MODIFY PROFILE** link.

Use the **PROFILEMANAGERURL** global option to provide the link to Profile Manager. The default URL contains the following link:

```
http://SERVERNAME/Core/AccountCourier/
default.asp?Workflow=WORKFLOW&
```

Replace the SERVERNAME with the correct machine name, and update the WORKFLOW with the name of the default Core Provisioning® or custom workflow.

This link does not appear by default since the Is Profile Manger custom macro is set to false. The link appears only when the Is Profile Manager custom macro resolves to true.

The Profile Manager connects to the default Core Provisioning® workflow, which enables you to create or modify a profile. Any Core Provisioning® or custom workflow that you create needs to satisfy the following requirements:

- Point to the Profile table to enable adding of a new profile with a unique ProfileUID.
- Create a row in the IdentityMap table that points to the newly created ProfileUID.
- Call the CreateProfileChangeRequest stored procedure.

The requester can submit a request for the newly created profile. The request status, however, remains on hold until the profile is approved and the Active column in the Profile table is set to true.

Providing a Label for the Profile Manager Link

Use the **PROFILEMANAGERURLLABEL** global option to change the default **ADD USER** label.

Configuring DefaultApproverProfileUID Global Option

Use the **DEFAULTAPPROVERPROFILEUID** global option to configure an approver, by inserting this value in to the GlobalConfigValues table. Navigate to the GlobalConfigValues table in the [installation-folder], and add the following values: DefaultApproverProfileUID in the ConfigName column, the approver ProfileUID in the ConfigValue column, and Text in the ConfigType column.

Approval Workflow for New Profiles

A Manager can create a profile for a user through the **ACTIONS** > **CREATE/MODIFY PROFILE** screen. A profile approval may include the following scenarios:

- If the Manager specifies a Manager ID on the **CREATE/MODIFY PROFILE** screen for the AccountCourier® workflow, the profile approval is sent to the specified Manager.
- If the Manager (requester) specifies his own ProfileUID as the ManagerID, then the approval is sent to the requester’s Manager.
- If the Manager does not specify a Manager ID, the approval is sent to an approver specified in the **DEFAULTAPPROVERPROFILEUID** global option. To specify a value, refer to the section *“Configuring DefaultApproverProfileUID Global Option” on page 155*.
- If the Manager does not specify a Manager ID, and there is no approver configured through the **DEFAULTAPPROVERPROFILEUID** global option, then the profile approval is sent to the requester’s Manager.

Note: Based on the scenarios, notifications are sent accordingly to the requesters and recipients. However, if the Manager specifies one or more approvers, the profile approval is sent only to the specified approvers overriding the above scenarios.

Access Request Approval Workflow for a New Profile

If the Manager requests access for the new profile that he created, the profile needs to be approved first. Once the profile is approved, the access request workflow for a new profile follows these steps:

1. Manager B creates a profile for a direct report. A notification is sent to Manager A (Manager of Manger B) to approve the profile.
2. Meanwhile, Manager B requests access for the direct report. The access request is On Hold until the profile is approved.
3. Manager A approves the profile request. Once the profile is approved, the following action may result:
   - The access request is automatically approved if there is no access approver defined for the second-level approval. This happens since the Manager requested access and, hence, the first-level is automatically approved.
   - The access request remains pending if an access approver is defined. The request is approved if the access approver approves it.

Appendix A: Obsolete Macros and Global Options

This appendix lists the Access Request Manager macros and global options that are included with the installation, but have been obsolete as of Release 8.2 or 8.3.

Obsolete Macros

The following macros have been obsolete as of Release 8.2 or 8.3:

- AccessRequest.ProfileID
- Get AccessCatalog Default Restriction v2
- Get AccessCatalog Default Restriction
- Get AccessCatalog Delegator As Resource Owner Restriction
- Get AccessCatalog Individual Contributor Restriction
- Get AccessCatalog Manager Restriction
- Get AccessCatalog Resource Owner Restriction
- Get Default Delegator Restriction
- Get Default Restriction
- Get Delegator As Individual Contributor Restriction
- Get Delegator As Manager Restriction
- Get Delegator As Resource Owner Restriction
- Get Individual Contributor Restriction
- Get Manager Restriction
- Get Multi-User Search Checkbox Restriction
- Get Profile Info
- Get Resource Owner Restriction
- Get LoggedInUser Role

Obsolete Global Options

The following global options have been obsolete as of Release 8.2 or 8.3:

- ApproveAsApproverSearchOption
- ApproverAsApproverSearchRestriction
- ApproveAsManagerSearchOption
- ApproveAsManagerSearchRestriction
- FindDelegatorSearchOption
- FindDelegatorSearchRestriction
- ProfileApprovalSearchOption
- RequestAsManagerSearchOption
- RequestAsManagerSearchRestriction
- RequestAsResourceOwnerSearchRestriction

Index

A
Access Approval 120
Access approver 53, 83
Access Assurance Portal 7
  authenticate 23
Access Assurance Portal Menus 149
access entitlement
  add 59
Access Keys 8
access privilege
  Request as Business Manager 120
access request 10, 12
Active Directory groups 22
add
  access entitlement 59
  macro 93
  profile 153, 154
administrator 7
Approval workflow 10
approval workflow 81, 113
approve
  profile 153
  role 58
approver 10
  first-level 83, 129
  second-level 83, 129
assign
  tags 62

B
bulk request 19

C
Configuring Menu Items to the Access Assurance Portal Menu 148
Courion Request Service 22
create
  profile 153
custom macros 120

D
Definition approver 53
definition approver 82
delegatees 113
delegation 113
  audit 126
  authorized users 113
delegators 113
disable
  role 58

E
edit
  email template 131
  macro 93
  role 57
Edit Complex Value editor 29
email template
  edit 131
Email Templates Manager 26
enable
  role 58
Entitlement 141

F
first-level approver 83, 129
Function 140

G
global configuration
  add, GlobalConfigValues table 31
  complex 28
  drop-down 33
  edit 28
  grid 31
  text 28
  views 33
Global Configuration Manager 26
global configurations 27
GlobalConfigValues table 27

M
macro
  add 93
  delete 96
  edit 93, 96
Macro Configuration 26
Manage Access Catalog 26
Manage User Access workflow 10
Manager Approval 120
Menu
  removing 151
  updating 151
Menu.XML 148

N
New Child Menu
  adding 150
New Top Level Menu
  adding 150
notifications 129

O
Obsolete Global Options 137, 160
Obsolete Macros 135, 159

P
Pick List Admin 44
Pick List Configuration 26
picklist 43, 44
  default values 45
picklists
  add 46
  defaults 45
  values 45
policy violation checking
  of access requests 17

profile
  add 153, 154
Profile Approval 120
profile approval 156

R
recipient 10
request 10, 12
Request Access 120
Request Details window 20
request workflow 63, 73, 113
requester 10
resource file 133
role
  approve 58
  disable 58
  edit 57
  enable 58
role owner 51

S
second-level approver 83, 129
Security Admin 26

T
tags
  assign 62

X
XML data tag 133
XML file 149