Information Builders

iWay

Omni Governance Console Administration User's Guide

Version 3.2 and Higher

January 07, 2020

Contents

Preface 9
Documentation Conventions 10
Related Publications 10
Customer Support 10
Help Us to Serve You Better 11
User Feedback 13
Information Builders Consulting and Training 13

1. Introducing the Administration Console 15
Overview 15
Key Features 15
Accessing the Administration Console 16
Understanding the Layout and Structure of the Administration Console 17
Components Menu. 17
Actions Menu. 18
Help Menu. 18
Content Area. 19
Footer. 19

2. Configuring Application Components 21
Sources 21
Source List. 22
Source Validation. 22
Source History. 23
Show Source. 23
Editing a Source. 25
Deleting a Source. 26
Views 26
View List. 28
Show View. 30
Creating a New View. 32
Editing a View. 33
Options 33

Option List. 34
Show Option. 34
Creating a New Option. 35
Editing an Option. 36
Tables 36
Table List. 37
Show Table. 37
Creating a New Table. 38
Editing a Table. 42
Editing a Column. 46
Global Column Editing. 47
Editing a Link. 47
Table Order 48
Table Order List. 49
Editing a Table Order. 50
Settings 50
Setting List. 52
Show Setting. 52
Creating a New Setting. 53
Editing a Setting. 54
Exceptions 54
Exception List. 55
Downloading and Uploading Metadata 55
Downloading Metadata. 55
Uploading Metadata. 57
Configuring 360 Viewer 59
Configuring Remediation Pages 71
Issues Page. 71
Case Issues Grid. 72
Ticket Issues Grid. 74
Filtering Panel on My Cases Tab. 77
Filtering Panel on All Cases Tab. 78
Number of Filtering Criteria Sections Expanded by Default. 79

Default Filtering on My Cases/All Cases Tab. 80
Switching ON/OFF of Multiselect Drop-down List on My Cases/All Cases Tabs. 85
Override Matching Page. 90
Instance Details Panel. 90
Case Properties Panel. 91
Manual Cleansing Page. 92
Workspace Panel. 93
Case Properties Panel. 95
General Issue Page. 96
Workspace Panel. 96
Case Properties Panel. 97
Issues Pop Up. 98
Domain Grid Configuration. 98
Breadcrumbs Configuration. 101
Sub-domains Configuration. 102

A. Enhanced Access Security: Column-Based and Row-Based 103
Overview 103
Configuring Enhanced Security 104
Enabling Enhanced Security 106
Configuring Column-based Security 109
Configuring Column Access. 109
Configuring Row-Based Access Security 116
Supporting Enhanced Security Using WSO2 Identity Server 120
Merging and Reorganizing Column Sets 120

B. Configuring Single Sign-On 123
Stopping the OGC Tomcat Service 124
Unzipping the Single Sign-On Delivery Package 124
Configuring the context.xml Properties File and Creating Backup Files 124
Editing the sso.properties File 125
Generating Certificates 126
Exporting Certificates 128
Editing the ogc-sp.xml File With Certificates and Properties .128

Configuring the SAML2 Identity Provider (SiteMinder) 131
Registering the Identity Provider Partnership Information and Certificate From the Identity Provider 131
Special Algorithms (Optional) 132
Restarting Apache Tomcat 133
Testing the New SAML2 SSO Sign On Page 134

C. Using MData, Synch, and WSO2 Administration 135

Functional Overview 135
Using the WSO2/MData-Synchronization Feature 135
Configuring Omni Server Mode. 135
Using the Synchronization. 136
Step 1: Initializing the Analysis for the Synchronization Process.. 137
Step 2: Analyzing the Progress.. 137
Step 3: Summarizing the Analysis.. 138
Step 4: Viewing the Details of the Analysis.. 138
Step 5: Customizing Roles or Users to be Synchronized (Optional). 139
Step 6: Customizing Policies to be Updated (Optional. 140
Step 7: Executing the Synchronization. 140
Step 8: Summarizing the Synchronization. 141
Developer Environment Considerations. 141

D. Configuring Omni Governance Console Roles From LDAP (Active Directory) 145

Overview 145
Prerequisites 145
Enabling Authorization Permission From OGC Using Group Names Through LDAP 146
Using the Active Directory (LDAP Server) System 150
Testing Logons to Omni Governance Console (OGC) 156

E. Custom Logos (Application Branding) 157

Rebranding Omni Governance Console Images With Custom Logos 157
Image Reference Catalog 158
Image 0 (logo_about.png). 159
Image 1 (logo_login.png) and Image 2 (logo_login_info.png). 160
Image 3 (logo_360viewer.png) and Image 4 (branding_bg_stripes.png). 161

Image 5 (remediation-strip.png) and Image 6 (logo_remediation.png). 161
Image 7 (op.ico). 162
Available Branding Locations 162
Understanding the Placement of Branding Assets 163

Preface

This documentation describes how to perform administration tasks for Omni Governance Console (OGC), which provides a web-based Administration console that you can use to configure the application.

How This Manual Is Organized

This manual includes the following chapters:

	Chapter/Appendix	Contents
1	Introducing the Administration Console	Introduces the Administration console, which is a component of the Omni Governance Console (OGC).
2	Configuring Application Components	Describes how to configure Omni Governance Console (OGC) application components using the Administration console.
A	Enhanced Access Security: Column-Based and Row-Based	Describes how to configure column-based access security and row-based access security in the Omni Governance Console (OGC).
B	Configuring Single Sign-On	Describes how to configure Single Sign-On (SSO) for Omni Governance Console (OGC).
C	Using MData, Synch, and WSO2 Administration	Describes the WSO2/MData Synchronization (Mdata-Synch) feature of reducing the configuration work of the administrator when a new subject arrives into the Omni-Gen Server (OGS) model and database, and when data structures are altered (for example, a type or name of a column has been changed).
D	Configuring Omni Governance Console Roles From LDAP (Active Directory)	Describes how to configure a WSO2 based LDAP connection and User Store which will eliminate the redundant data entry, and allow the Subject per Userid Authorizations to be obtained from the enterprise LDAP Server (Active Directory).
E	Custom Logos (Application Branding)	Describes how to apply branding or custom logos to your Omni Governance Console (OGC) application.

Documentation Conventions

The following table lists and describes the documentation conventions that are used in this manual.

Convention	Description
`THIS TYPEFACE` or `this typeface`	Denotes syntax that you must type exactly as shown.
this typeface	Represents a placeholder (or variable), a cross-reference, or an important term. It may also indicate a button, menu item, or dialog box option that you can click or select.
underscore	Indicates a default setting.
Key + Key	Indicates keys that you must press simultaneously.
{}	Indicates two or three choices. Type one of them, not the braces.
|	Separates mutually exclusive choices in syntax. Type one of them, not the symbol.
...	Indicates that you can enter a parameter multiple times. Type only the parameter, not the ellipsis (...).
. . .	Indicates that there are (or could be) intervening or additional commands.

Related Publications

Visit our Technical Documentation Library at *http://documentation.informationbuilders.com*. You can also contact the Publications Order Department at (800) 969-4636.

Customer Support

Do you have any questions about this product?

Join the Focal Point community. Focal Point is our online developer center and more than a message board. It is an interactive network of more than 3,000 developers from almost every profession and industry, collaborating on solutions and sharing tips and techniques. Access Focal Point at *http://forums.informationbuilders.com/eve/forums*.

You can also access support services electronically, 24 hours a day, with InfoResponse Online. InfoResponse Online is accessible through our website, *http://www.informationbuilders.com*. It connects you to the tracking system and known-problem database at the Information Builders support center. Registered users can open, update, and view the status of cases in the tracking system and read descriptions of reported software issues. New users can register immediately for this service. The technical support section of *http://www.informationbuilders.com* also provides usage techniques, diagnostic tips, and answers to frequently asked questions.

Call Information Builders Customer Support Services (CSS) at (800) 736-6130 or (212) 736-6130. Customer Support Consultants are available Monday through Friday between 8:00 a.m. and 8:00 p.m. EST to address all your questions. Information Builders consultants can also give you general guidance regarding product capabilities and documentation. Please be ready to provide your six-digit site code number (*xxxx.xx*) when you call.

To learn about the full range of available support services, ask your Information Builders representative about InfoResponse Online, or call (800) 969-INFO.

Help Us to Serve You Better

To help our consultants answer your questions effectively, be prepared to provide specifications and sample files and to answer questions about errors and problems.

The following tables list the environment information our consultants require.

Platform	
Operating System	
OS Version	
JVM Vendor	
JVM Version	

The following table lists additional questions to help us serve you better.

Request/Question	Error/Problem Details or Information
Did the problem arise through a service or event?	
Provide usage scenarios or summarize the application that produces the problem.	
When did the problem start?	
Can you reproduce this problem consistently?	
Describe the problem.	
Describe the steps to reproduce the problem.	
Specify the error message(s).	
Any change in the application environment: software configuration, EIS/database configuration, application, and so forth?	
Under what circumstance does the problem *not* occur?	

The following is a list of error/problem files that might be applicable.

- ❑ Input documents (XML instance, XML schema, non-XML documents)
- ❑ Transformation files
- ❑ Error screen shots
- ❑ Error output files
- ❑ Trace files
- ❑ Custom functions and agents in use

- Diagnostic Zip
- Transaction log

User Feedback

In an effort to produce effective documentation, the Technical Content Management staff welcomes your opinions regarding this document. Please use the Reader Comments form at the end of this document to communicate your feedback to us or to suggest changes that will support improvements to our documentation. You can also contact us through our website, *http://documentation.informationbuilders.com/connections.asp*.

Thank you, in advance, for your comments.

Information Builders Consulting and Training

Interested in training? Information Builders Education Department offers a wide variety of training courses for this and other Information Builders products.

For information on course descriptions, locations, and dates, or to register for classes, visit our website (*http://education.informationbuilders.com*) or call (800) 969-INFO to speak to an Education Representative.

Chapter 1

Introducing the Administration Console

This chapter introduces the Administration console, which is a component of the Omni Governance Console (OGC).

In this chapter:

- Overview
- Key Features
- Accessing the Administration Console
- Understanding the Layout and Structure of the Administration Console

Overview

Omni Governance Console (OGC) provides an Administration console that you can use to configure OGC.

The Administration console is only available after users log in to OGC. Only users who are first authenticated and authorized with the *System Administrator* role in the WSO2 Identity Server user store repository are allowed to access the OGC Administration console.

Key Features

The OGC Administration console provides a web-based interface to view and edit OGC configuration details (metadata).

The main operations that can be performed in the Administration console include the following:

- View and edit sources.
- View and edit views, create new views.
- View and edit options, create new options for table, view or source.
- View and edit tables, create new tables.
- View and edit columns.
- View and edit links.
- View and edit Table Order.

- View and edit settings, create new settings.
- Download and upload configuration (metadata.xml) files.

Note: All configuration options set, and all screen layouts defined by the metadata that the Administration console creates or edits are applied at a system-wide level. These options cannot be configured on a per-user basis.

For example, if the Administration console is used to create a grid display with *LastName* as column 1 and *FirstName* as column2, then all users viewing that display will see the columns in this order.

Accessing the Administration Console

Ensure that the user who is responsible for managing OGC metadata, modifying application options, and display definitions has the *System Administrator* role in the WSO2 Identity Server user store repository.

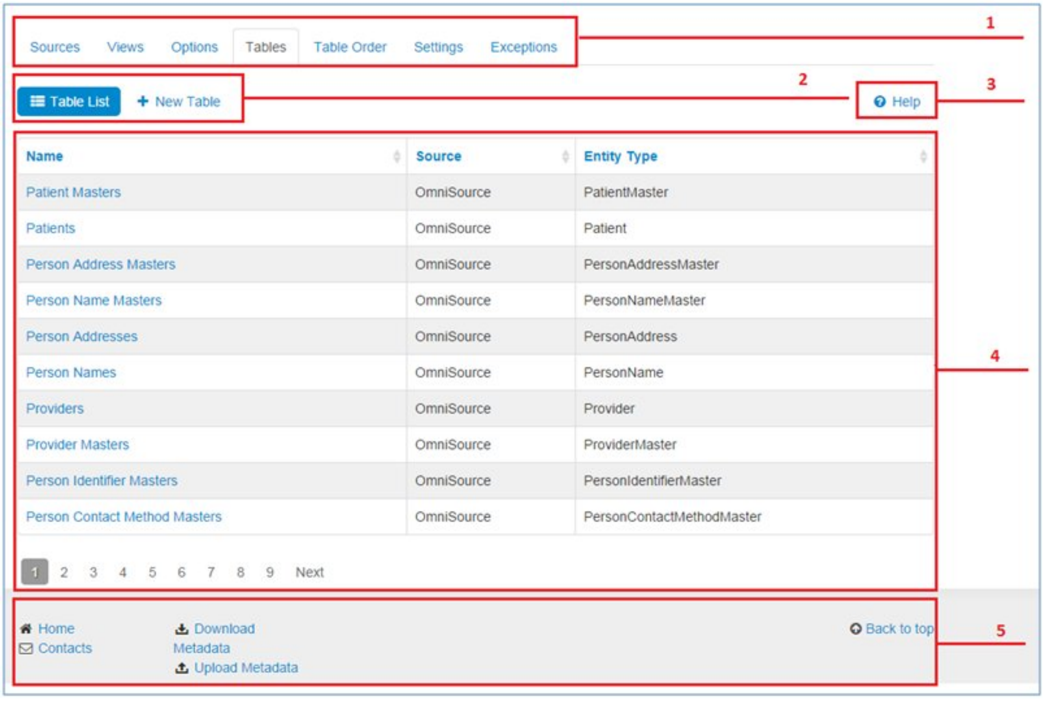
1. Enter the URL in your browser to access OGC. For example:

   ```
   https://ogcHostName:8443
   ```

2. Sign in to OGC with your valid user ID and password.
3. Click the *Administration* tab on the OGC menu bar.

Understanding the Layout and Structure of the Administration Console

All pages within the OGC Administration console are unified through a common page layout, as shown in the following image.



Each page contains the following areas:

1. Components menu
2. Actions menu
3. Help menu
4. Content area
5. Footer

Components Menu

The components menu includes the following tabs:

- ❑ Sources
- ❑ Views

- Options
- Tables
- Table Order
- Settings
- Exceptions

The following image shows the components menu with the Tables tab selected.

Actions Menu

The actions menu may vary depending on the specific page. Usually, the actions menu contains:

- List of items.
- Create item button.
- Edit item button.
- Delete item button.

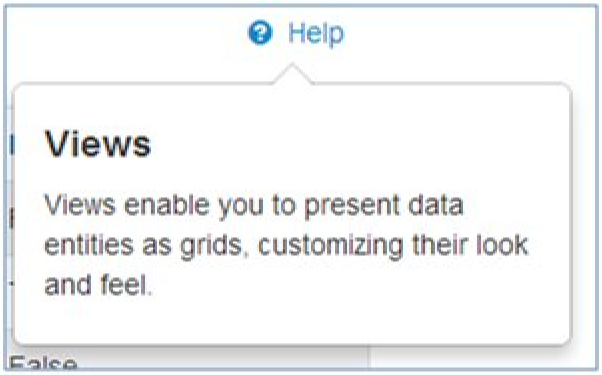
Detailed information about the actions menu is described throughout this documentation.

The following image shows the actions menu when the Tables tab selected in the components menu.

Help Menu

The Help menu describes the functionality of the corresponding activity. It is available within each tab for each action.

The following image shows the Help menu when the Views tab selected in the components menu.



Content Area

The content area is the main part of each page where administrators can view and edit metadata.

Detailed descriptions of different pages are provided throughout this documentation.

Footer

The footer contains links to the Home and Contacts pages, and links for downloading and uploading metadata. It also contains the *Back to top* link.

Chapter 2

Configuring Application Components

This section describes how to configure Omni Governance Console (OGC) application components using the Administration console.

In this chapter:

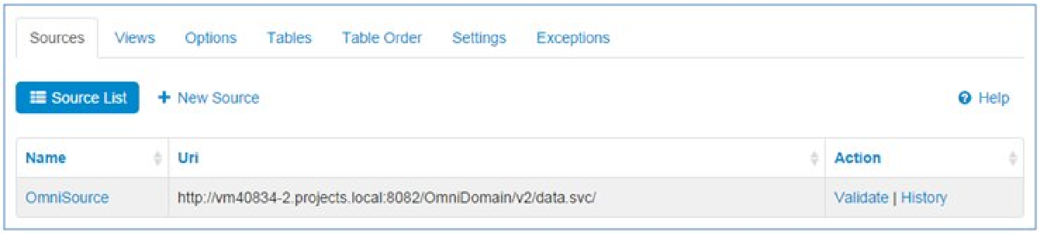
- Sources
- Views
- Options
- Tables
- Table Order
- Settings
- Exceptions
- Downloading and Uploading Metadata
- Configuring 360 Viewer
- Configuring Remediation Pages

Sources

Sources contain information about services that provide data and its metadata (data structure).

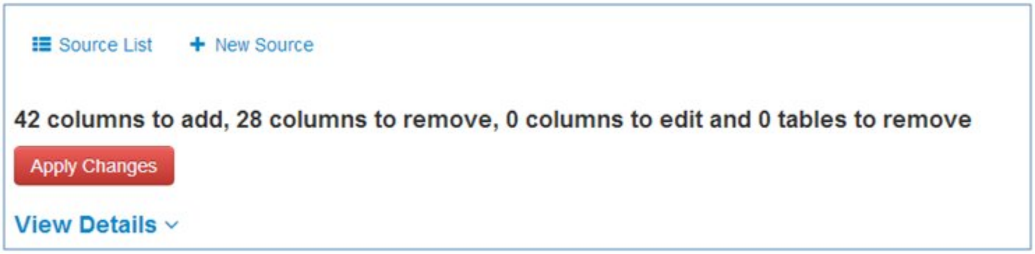
Source List

A list of all sources is displayed on the Source List page. On this page, it is also possible to validate source and view source updating history.

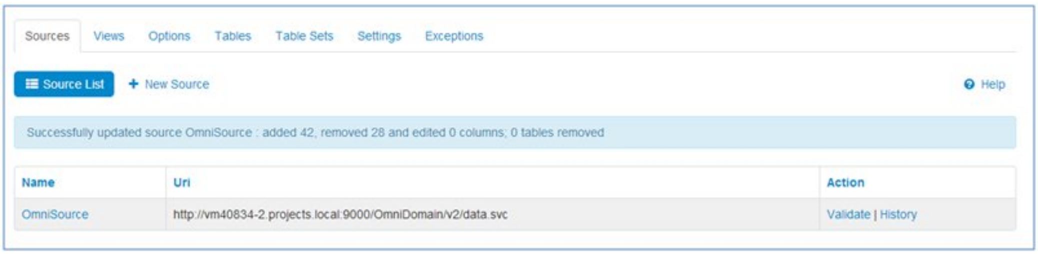


Source Validation

Administrators can validate a source by clicking the *Validate* link. Validation is necessary to check the source remote changes. It covers the cases when an additional column was added to a specific table on a remote source, removed from it, or its properties changed (*type*, *canFilter*, *canEdit*). After validation, all changes will be synchronized.

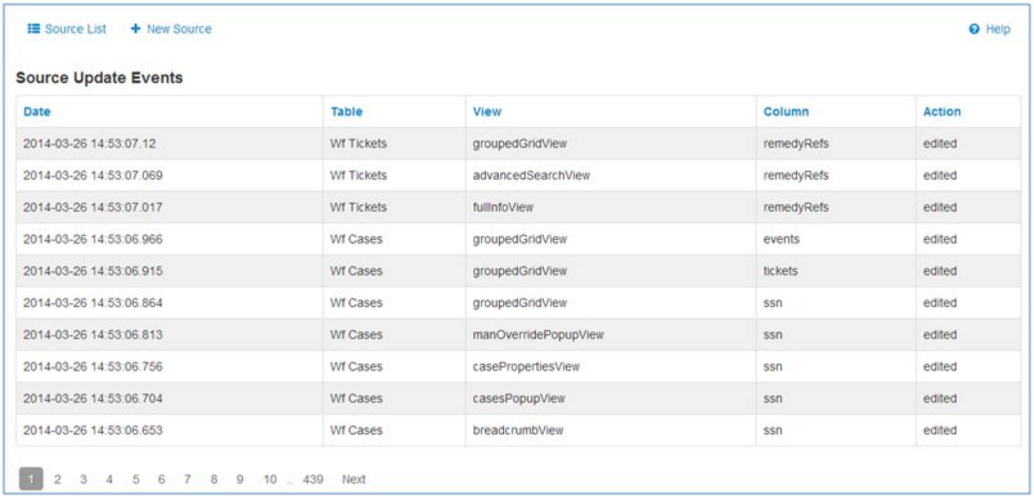


After clicking the *Apply Changes* button, the source will be updated, as shown in the following image.



Source History

Administrators can access the Source Update History page from the Source List page by clicking the *History* link. This page contains all update events after a source validation, as shown in the following image.



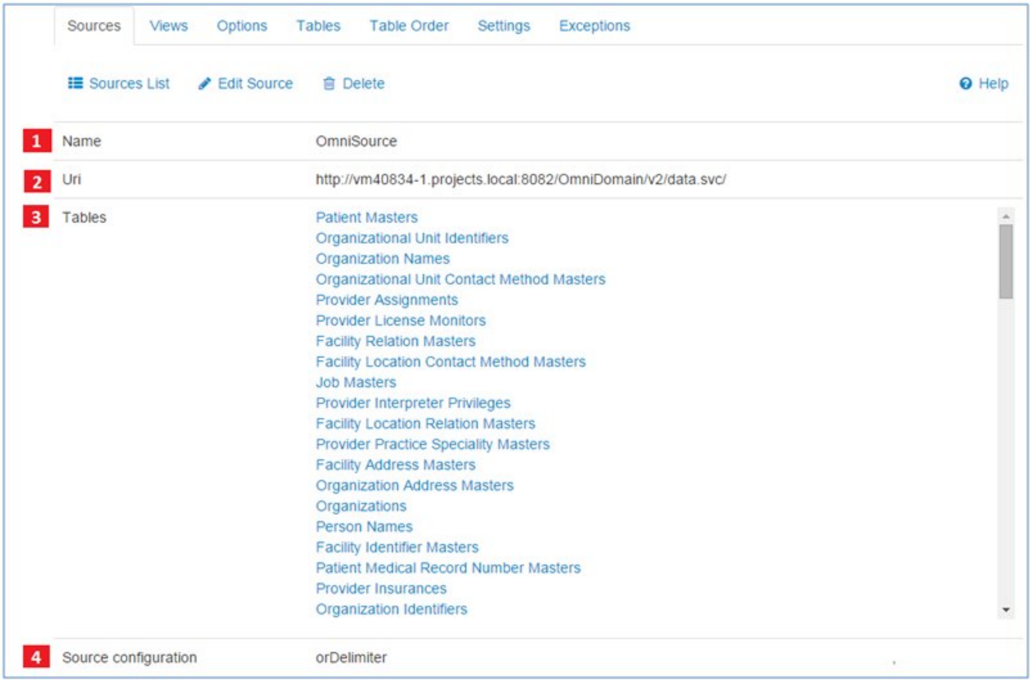
Date	Table	View	Column	Action
2014-03-26 14:53:07.12	Wf Tickets	groupedGridView	remedyRefs	edited
2014-03-26 14:53:07.069	Wf Tickets	advancedSearchView	remedyRefs	edited
2014-03-26 14:53:07.017	Wf Tickets	fullInfoView	remedyRefs	edited
2014-03-26 14:53:06.966	Wf Cases	groupedGridView	events	edited
2014-03-26 14:53:06.915	Wf Cases	groupedGridView	tickets	edited
2014-03-26 14:53:06.864	Wf Cases	groupedGridView	ssn	edited
2014-03-26 14:53:06.813	Wf Cases	manOverridePopupView	ssn	edited
2014-03-26 14:53:06.756	Wf Cases	casePropertiesView	ssn	edited
2014-03-26 14:53:06.704	Wf Cases	casesPopupView	ssn	edited
2014-03-26 14:53:06.653	Wf Cases	breadcrumbView	ssn	edited

Show Source

To view detailed information about a source, administrators should click the name of the source on the Source List page. The Show Source page contains the following information:

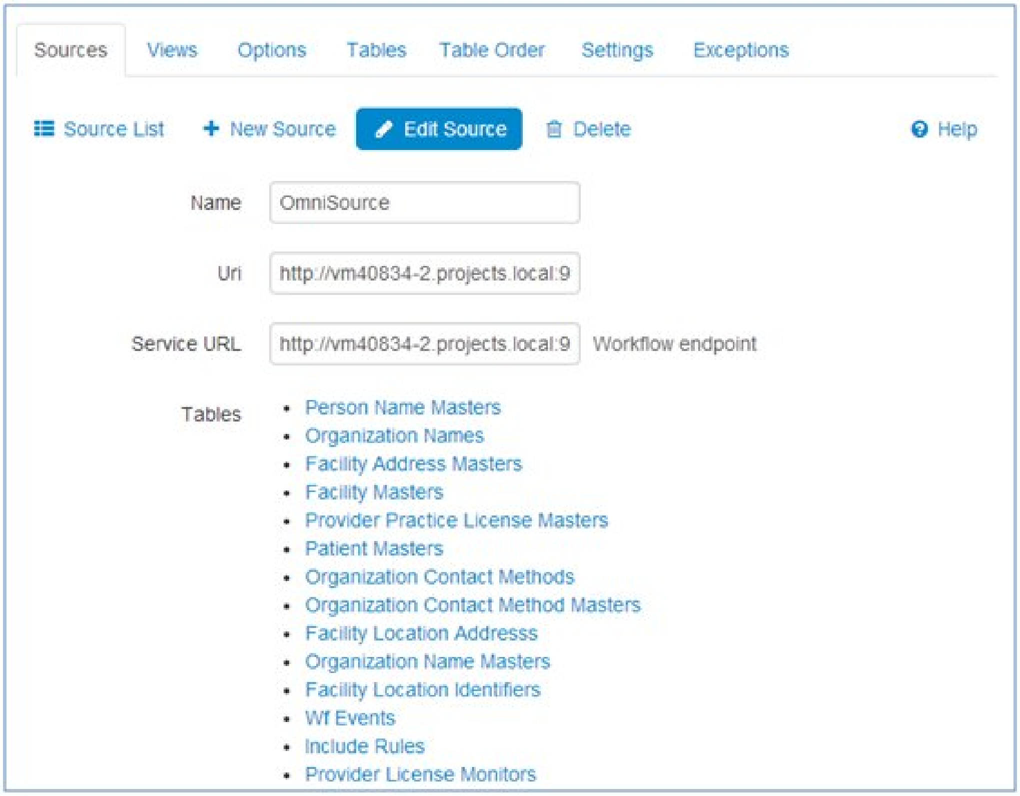
- Source name
- Uri
- Tables the source contains

- Source configuration



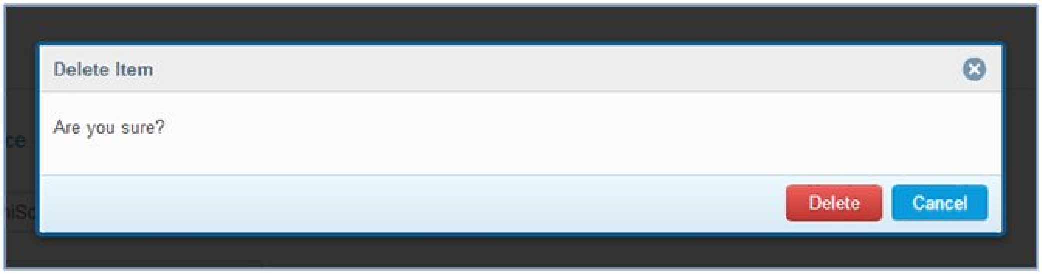
Editing a Source

The Edit Source page enables administrators to change source properties. However, some fields such as Uri and Tables cannot be edited. To navigate to this page, administrators should select the source that needs to be changed from the list and then click the *Edit Source* button.



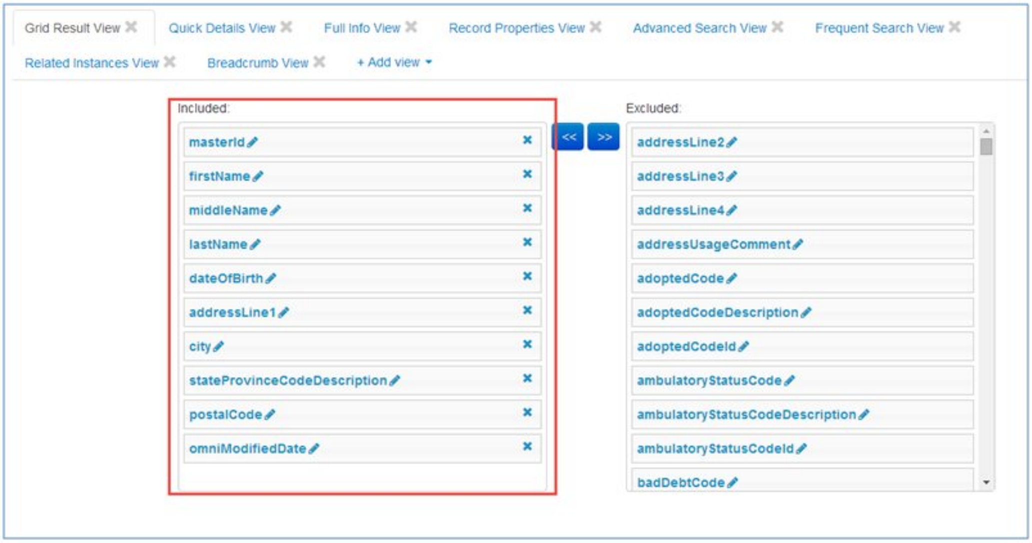
Deleting a Source

Administrators can delete an item by clicking the *Delete* button, which is available on the Show Source page, as shown in the following image.

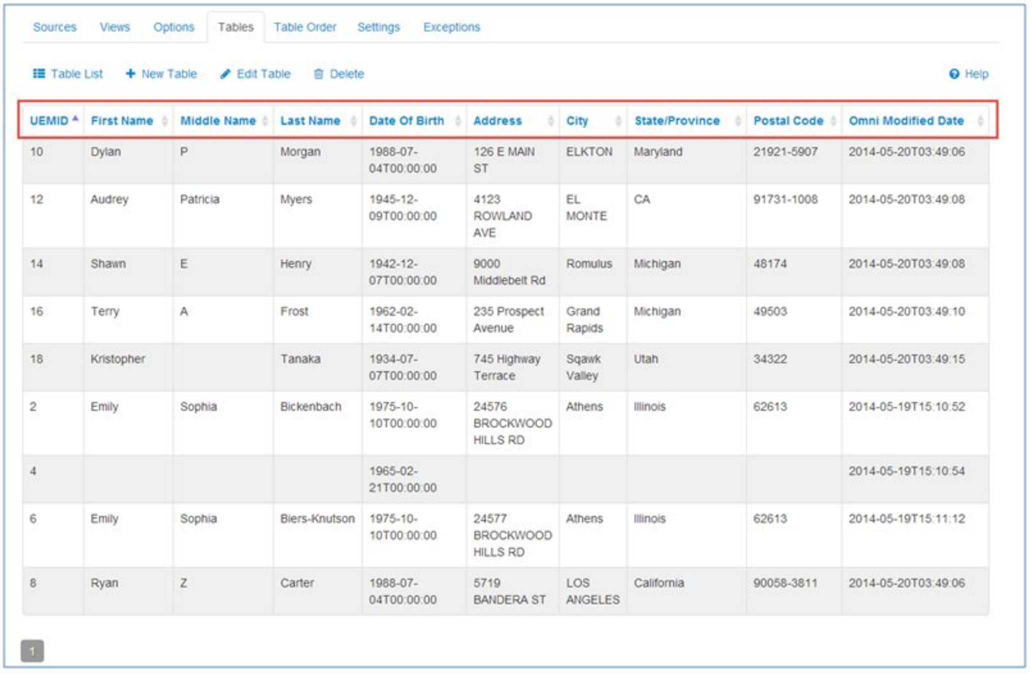


Views

Views are used to select/group columns for display in the main interface of Omni Governance Console (OGC).

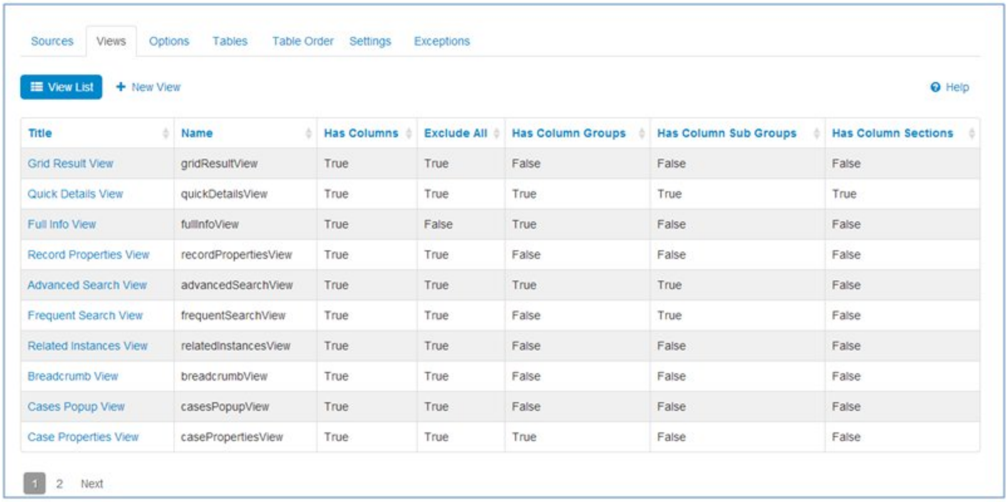


For example, the Grid Result View is used to represent the grid on the Show Table page, as shown in the following image.



View List

The list of all views is displayed on the View List page, as shown in the following image.



List of all views and its representation in the user interface is described in the following table.

View	Description
Grid Result View	**UI:** Columns that should be displayed in the tables on the 360 Viewer and 360 Details page. Also reflects Show Table page on Admin console. **Admin Tables:** Domain's (Party Master, Party) and Subdomain's tables (Addresses).
Quick Details View	**UI:** Columns that should be displayed in Preview Panel in the 360 Viewer and 360 Details tables. **Admin Tables:** Domain page table and Details 360 subdomain table (Preview Panel), also configure case and ticket pop-ups (Wf Cases, Wf Tickets, WF RemedyRef tables).

View	Description
Full info View	**UI:** Columns on Details 360, Master Comparison, Compare Source, Historic Master Comparison, Historic Compare Source, Remediation pages. **Admin Tables:** Domain's (Party Master, Party) and Subdomain's tables (Addresses).
Record Properties View	**UI:** Record properties on Master Comparison for current and historic records. **Admin Tables:** Domain's (Party Master, Party) tables.
Advanced search view	**UI:** Domain search, Instance search, and Issues Search. **Admin Tables:** Domain's (Party Master, Party) and Subdomain's tables (Addresses).
Frequent Search View	**UI:** Domain search, Instance search. **Admin Tables:** Domain's (Party Master, Party) tables.
Related Instances View	**UI:** Details 360 breadcrumb drop-down list for domain. **Admin Tables:** Domain's (Party Master, Party) and Subdomain's tables (Addresses).
Breadcrumb View	**UI:** Breadcrumbs throughout the entire application. **Admin Tables:** Domain's(Party Master, Party) and Subdomain's tables (Addresses).
Case Properties View	**UI:** Case properties area on remediation pages: Matching, Cleansing, General Issue. **Admin Tables:** WF Cases
Grouped Grid View	**UI:** Data Dictionary Code set grouped view. **Admin Tables:** Source Codes.
Case Issues Grid View	**UI:** Columns in Case's Grid on Issues Search page. **Admin Tables:** WF Cases, all Domain's (Party Master, Party) tables.

View	Description
Ticket Issues Grid View	**UI:** Columns in Ticket's Grid on Issues Search page (nested grids). **Admin Tables:** WF Tickets.
Manual Override Popup View	**UI:** Issue popups. **Admin Tables:** WF Remedy Refs table.
My Cases Filter View	**UI:** Filter by Cases and Filter by Tickets panel on My cases tab (Issue Search page) **Admin Tables:** WF Tickets, WF Cases
All Cases Filter View	**UI:** Filter by Cases and Filter by Tickets panel on All cases tab (Issue Search page). **Admin Tables:** WF Tickets and WF Cases.

Show View

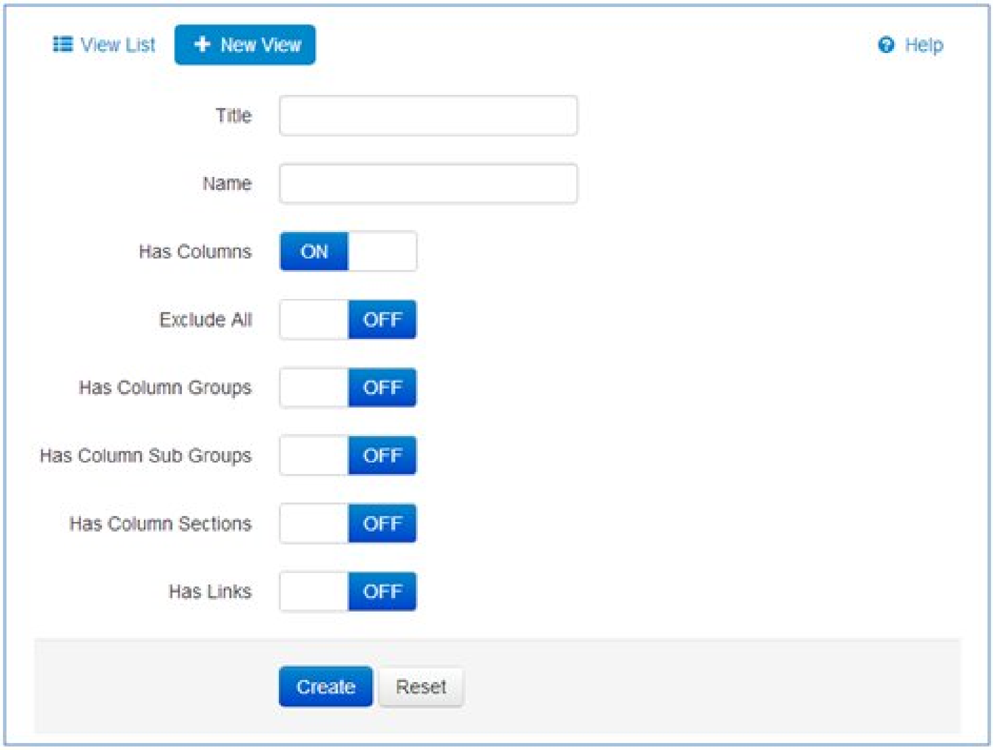
The Show View page can be reached by selecting any view from the list. It contains the following information about the selected view:

- View title
- View name
- If a view has columns
- If all columns must be excluded
- If a view has groups
- If a view has sub-groups
- If a view has sections
- If a view has links

More information about groups/sub-groups/sections will be provided in the following sections.

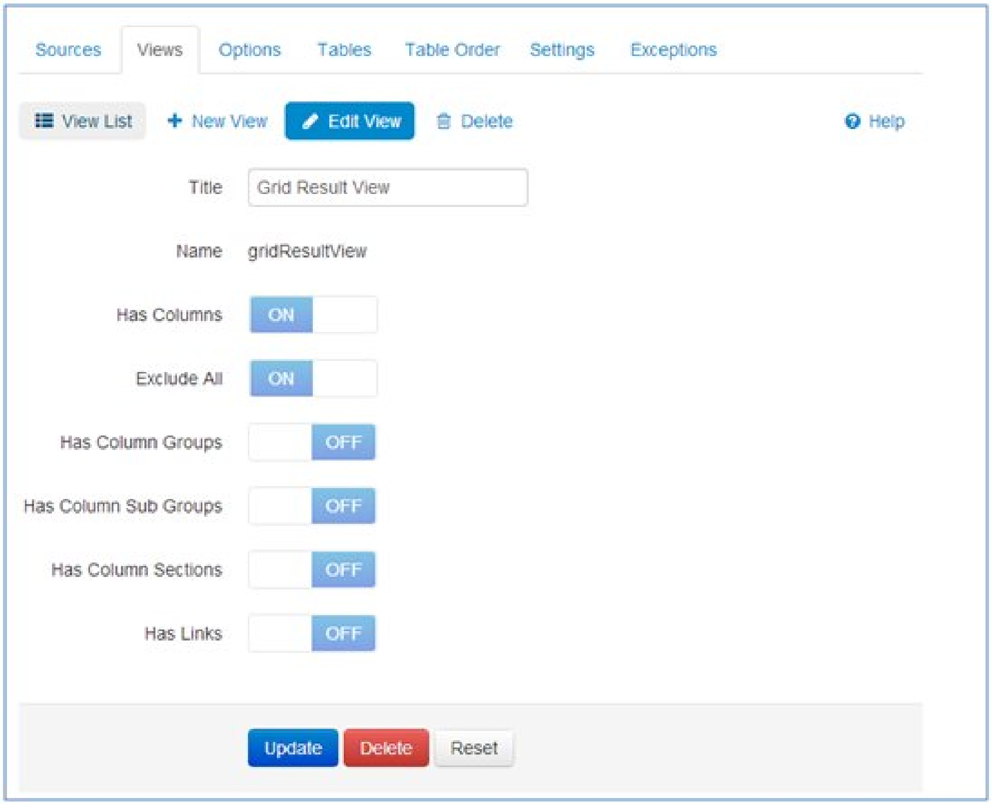
Creating a New View

Administrators can create a new view by clicking the *New View* button. The new view will not be used anywhere, but this functionality is available.



Editing a View

The Edit View page enables administrators to change a view. Administrators can navigate to this page from the Show View page by clicking the *Edit View* button. Note that the Name field cannot be edited.



Options

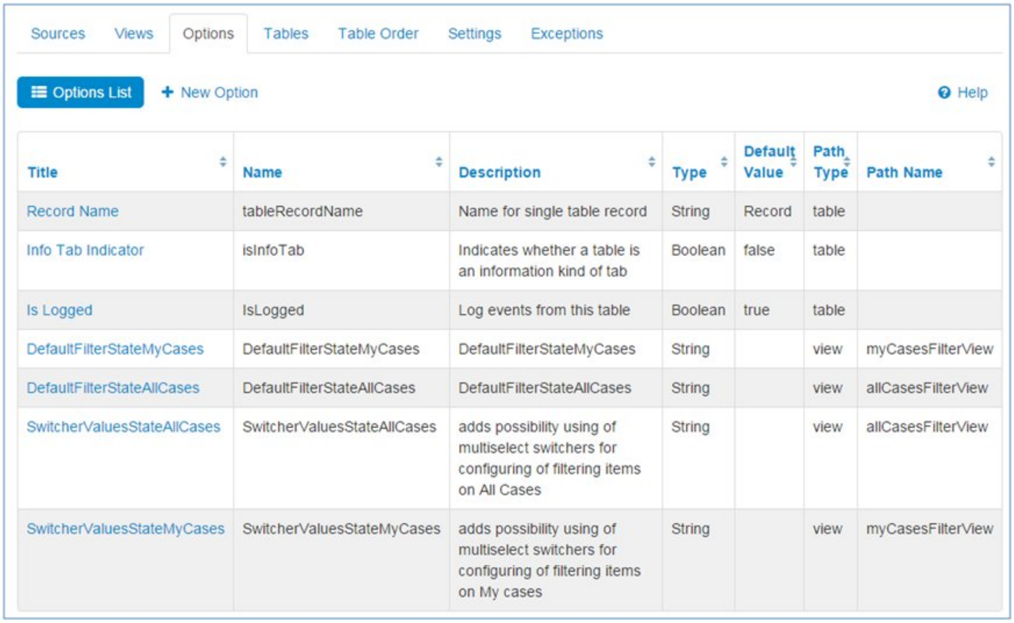
Options can be added for a table, source, or view. Each of these elements can store a custom value for the option. Currently, options are used to:

- Configure a name for single table record.
- Show or hide Info tabs.
- Switch logging on or off.
- Define a title for Default Filters.

- ❑ Adding of multiselect switchers to My/All Filter cases.

Option List

The list of all options is displayed on the Option List page, as shown in the following image.



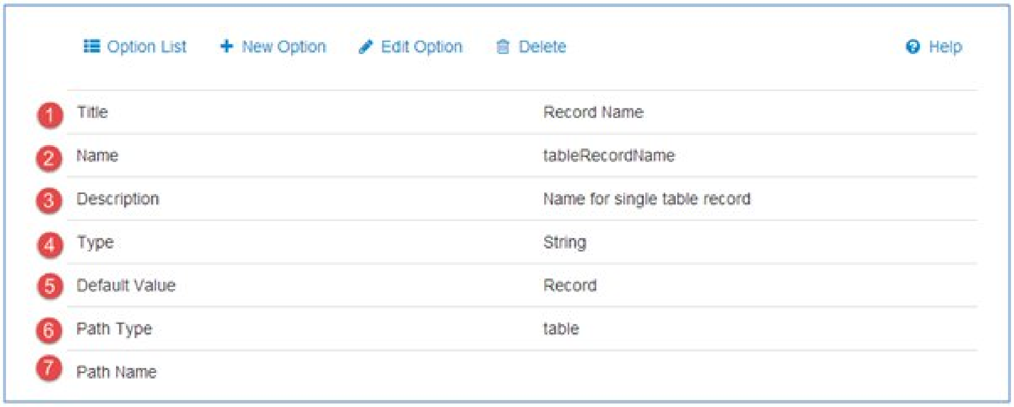
Title	Name	Description	Type	Default Value	Path Type	Path Name
Record Name	tableRecordName	Name for single table record	String	Record	table	
Info Tab Indicator	isInfoTab	Indicates whether a table is an information kind of tab	Boolean	false	table	
Is Logged	IsLogged	Log events from this table	Boolean	true	table	
DefaultFilterStateMyCases	DefaultFilterStateMyCases	DefaultFilterStateMyCases	String		view	myCasesFilterView
DefaultFilterStateAllCases	DefaultFilterStateAllCases	DefaultFilterStateAllCases	String		view	allCasesFilterView
SwitcherValuesStateAllCases	SwitcherValuesStateAllCases	adds possibility using of multiselect switchers for configuring of filtering items on All Cases	String		view	allCasesFilterView
SwitcherValuesStateMyCases	SwitcherValuesStateMyCases	adds possibility using of multiselect switchers for configuring of filtering items on My cases	String		view	myCasesFilterView

Show Option

When administrators select any option from the list, the Show Option page is displayed. This page contains the following information about the selected option:

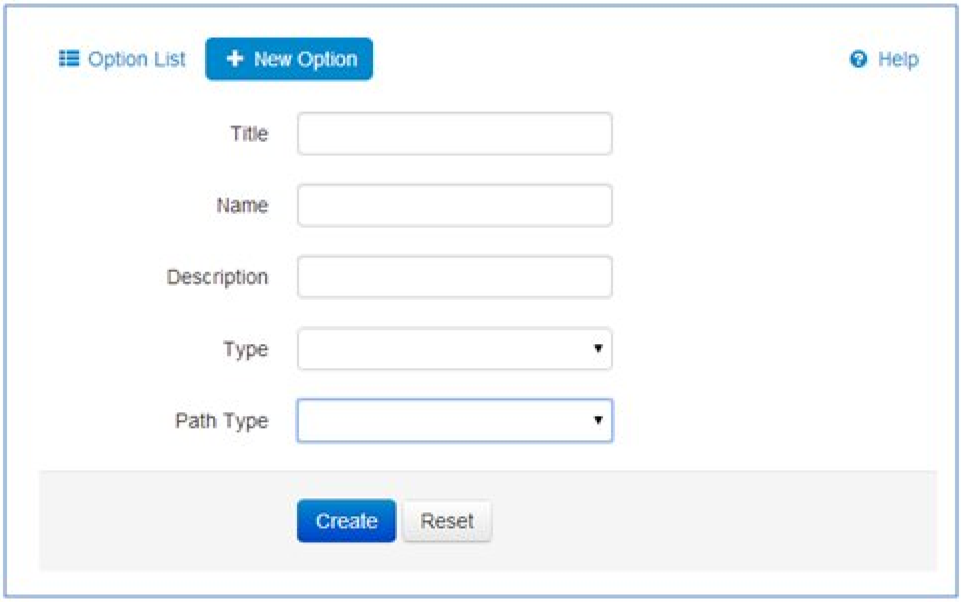
- ❑ Option title
- ❑ Option name
- ❑ Option description
- ❑ Option type
- ❑ Option default type
- ❑ Type of component

- ❑ Name of view (if required)



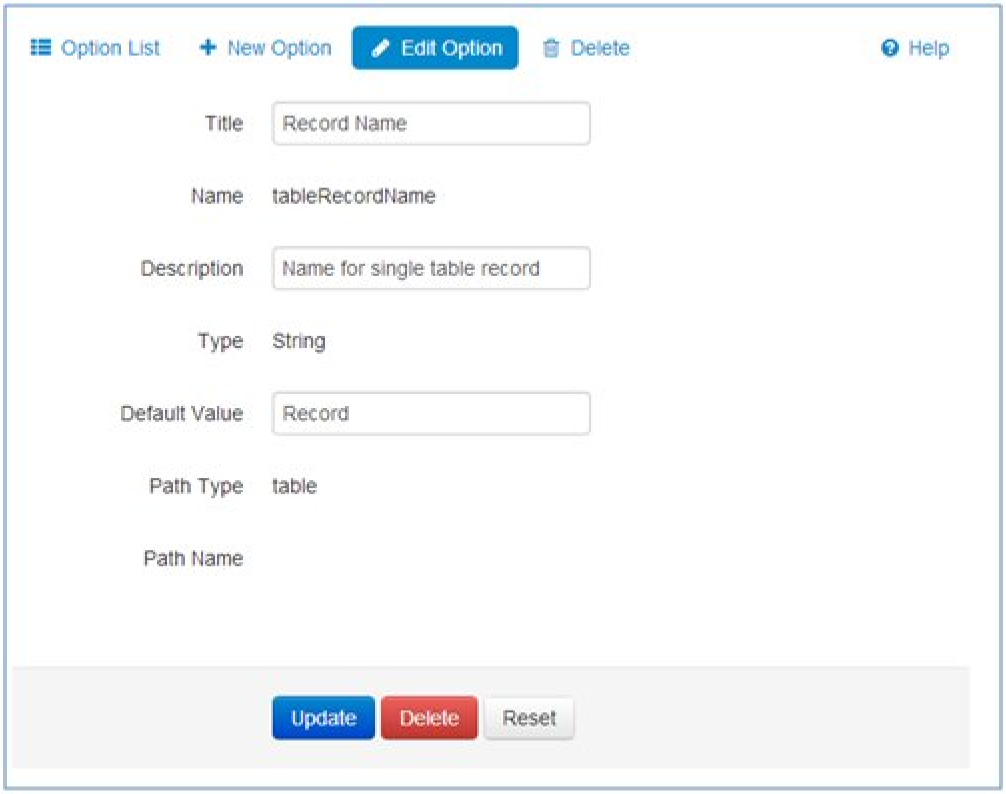
Creating a New Option

Administrators can create a new option on the New Option page by clicking the corresponding button on the Option List page, as shown in the following image.



Editing an Option

The Edit Option page enables administrators to modify an option. Administrators can navigate to that page from the Show Option page by clicking the *Edit Option* button, as shown in the following image.



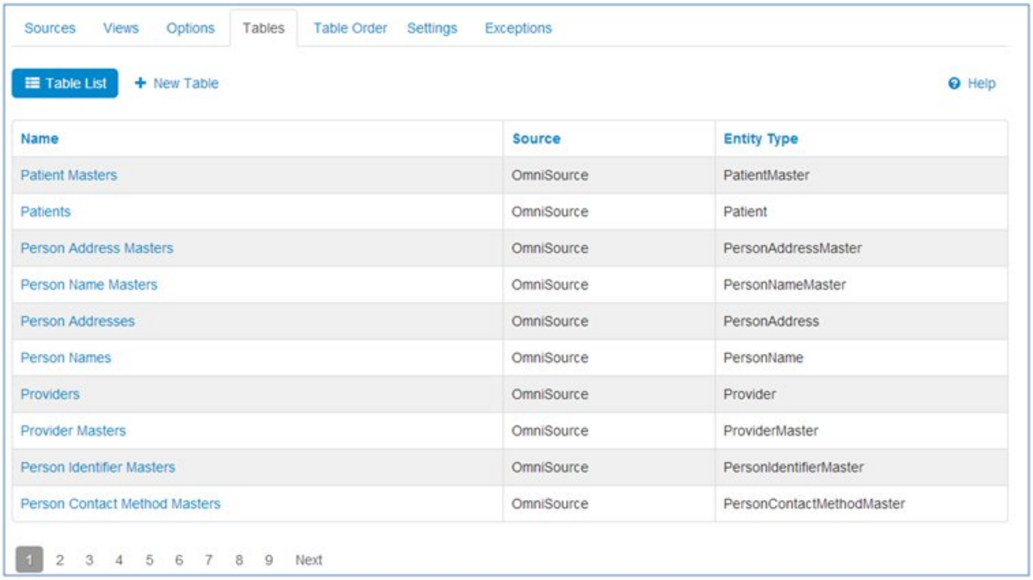
Note that the Name and Type fields cannot be modified.

Tables

Tables represent all available entities (for example, Patient Master, its Addresses, Provider Master, and so on).

Table List

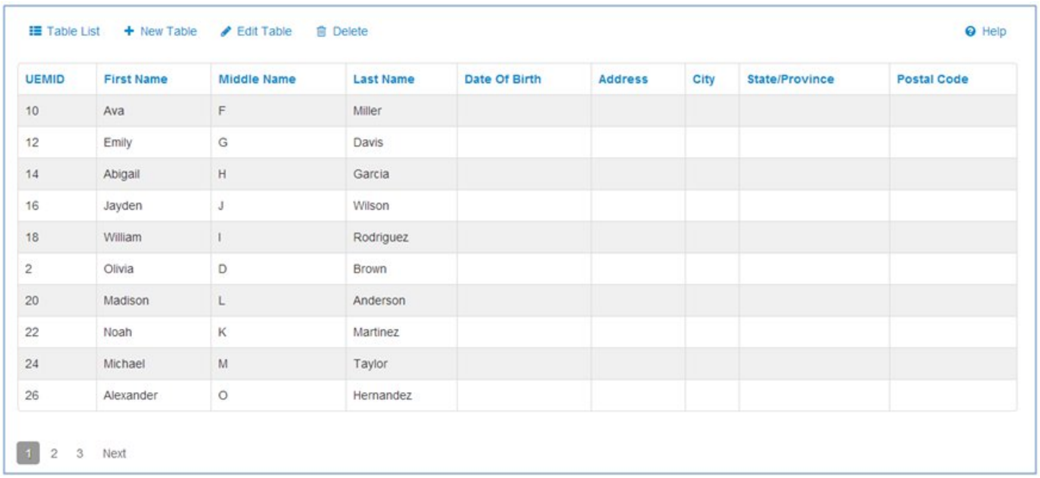
The list of all tables is displayed on the Table List page, as shown in the following image.



Name	Source	Entity Type
Patient Masters	OmniSource	PatientMaster
Patients	OmniSource	Patient
Person Address Masters	OmniSource	PersonAddressMaster
Person Name Masters	OmniSource	PersonNameMaster
Person Addresses	OmniSource	PersonAddress
Person Names	OmniSource	PersonName
Providers	OmniSource	Provider
Provider Masters	OmniSource	ProviderMaster
Person Identifier Masters	OmniSource	PersonIdentifierMaster
Person Contact Method Masters	OmniSource	PersonContactMethodMaster

Show Table

When administrators select a table from the list, the Show Table page is displayed. This page contains information about the selected table, as shown in the following image.



UEMID	First Name	Middle Name	Last Name	Date Of Birth	Address	City	State/Province	Postal Code
10	Ava	F	Miller					
12	Emily	G	Davis					
14	Abigail	H	Garcia					
16	Jayden	J	Wilson					
18	William	I	Rodriguez					
2	Olivia	D	Brown					
20	Madison	L	Anderson					
22	Noah	K	Martinez					
24	Michael	M	Taylor					
26	Alexander	O	Hernandez					

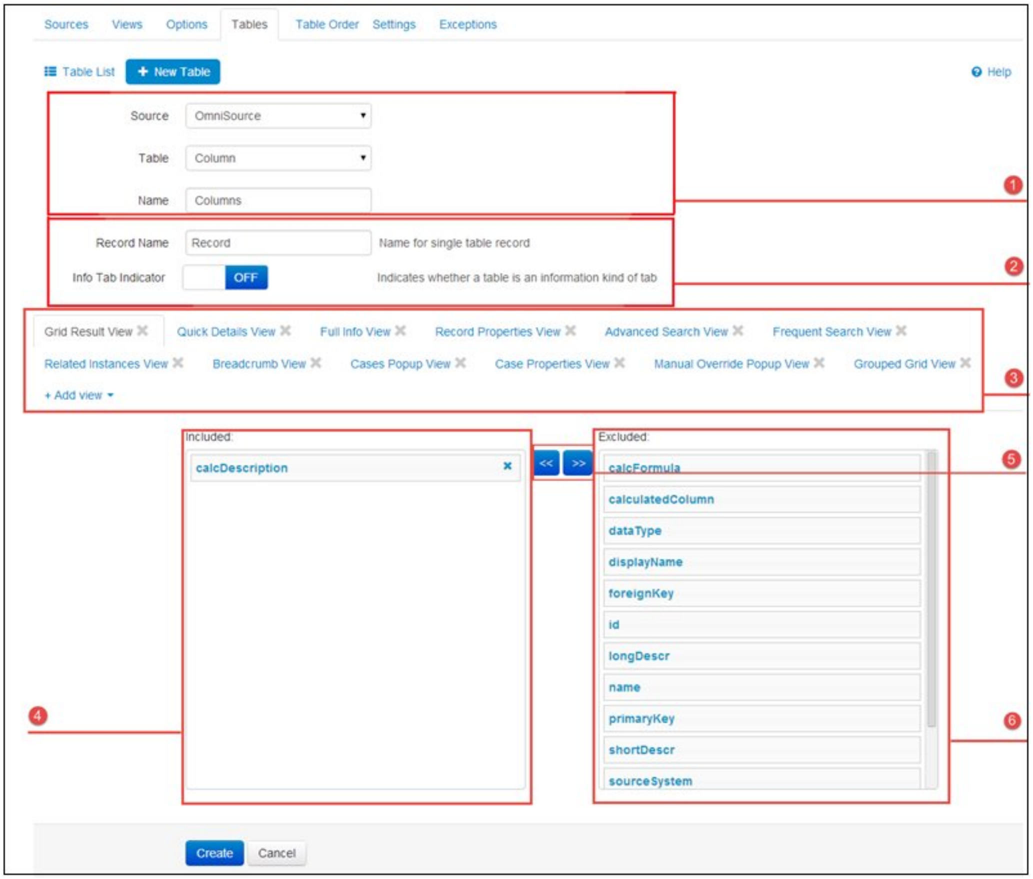
Creating a New Table

Administrators can create a new table on the New Table page by clicking the corresponding button on the Show Table page.

The New Table page contains the following sections:

1. Table properties
2. Table options
3. View tabs
4. Included columns
5. Include all/Exclude all buttons
6. Excluded columns

Columns can be added in the Included section by dragging and dropping, or deleted by clicking the "x" icon.



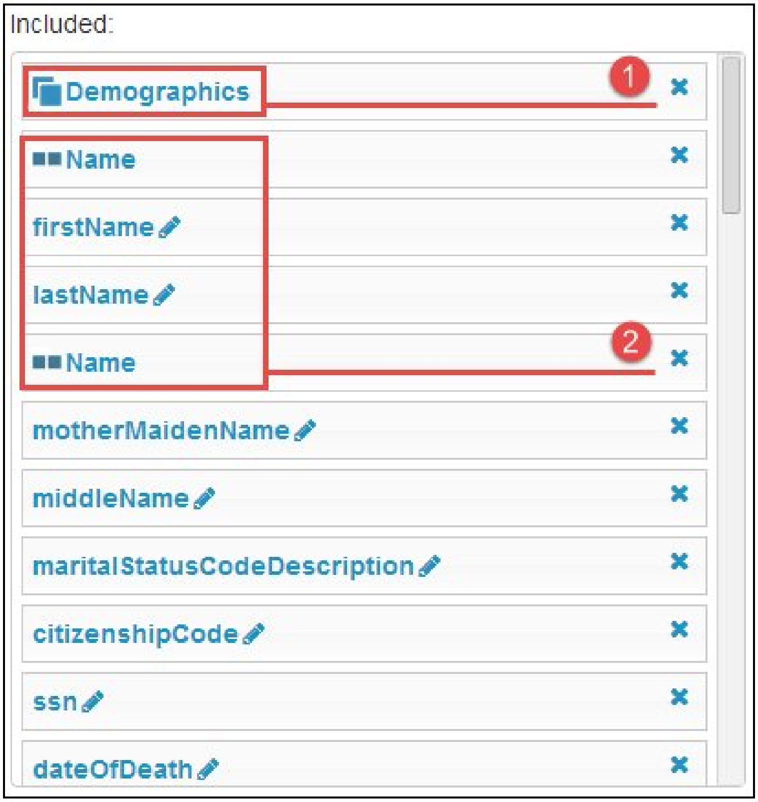
Some views have groups/sub-groups/sections. To create a new group/sub-group/section, administrators should choose the appropriate value from the drop-down list (if the view allows having groups/sub-groups/sections), type the name, and then press *Enter*.

Groups allow administrators to unite columns.

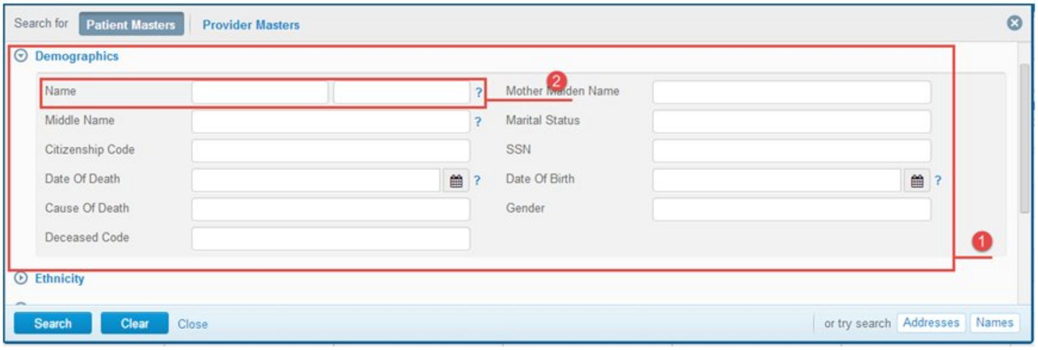
Sub-group is used to display a key-value pair, which is why a sub-group must contain two columns.

A section is an additional grouping in the group.

For example, the Patient Master table has groups (1) and subgroups (2) in the Quick Details View.

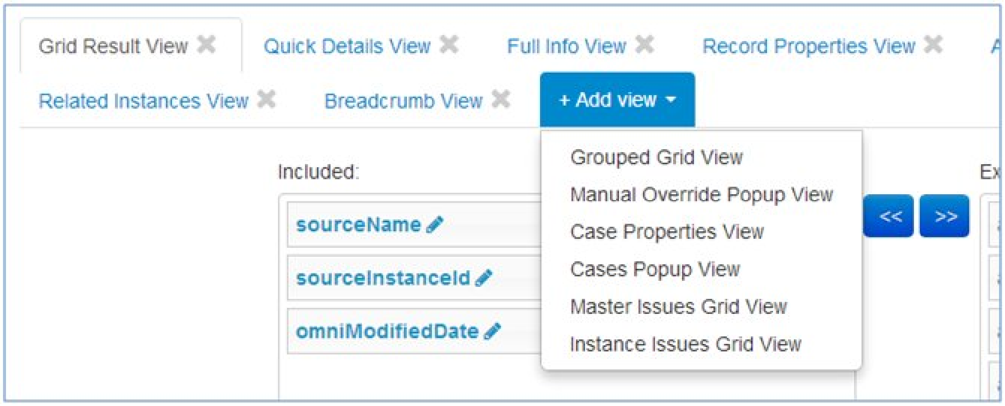


The following image shows the Advanced Search dialog.



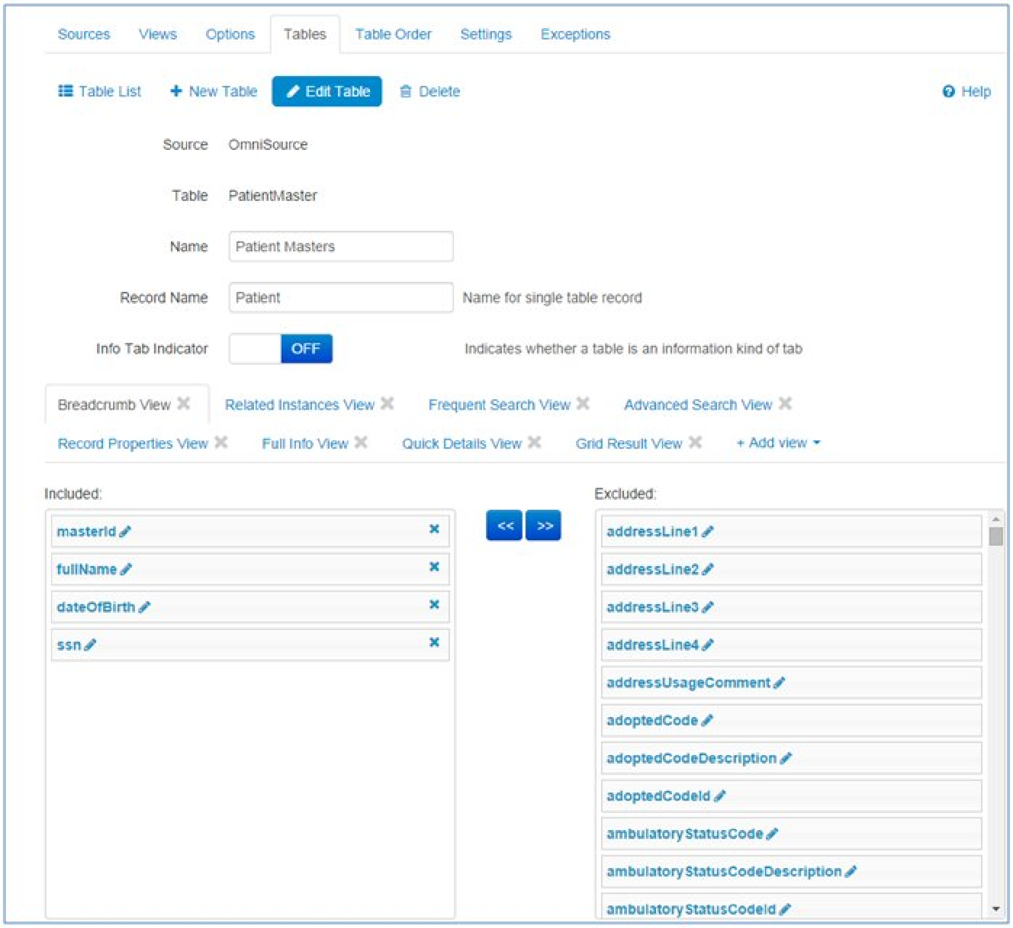
Created items are validated before they are updated to the table. Sub-group tags must contain two columns. In addition, the Grid Result View must have at least one column included. If validation fails, an appropriate message is displayed and the table is not updated.

View tabs can be closed and restored from +Add view drop-down list, as shown in the following image.

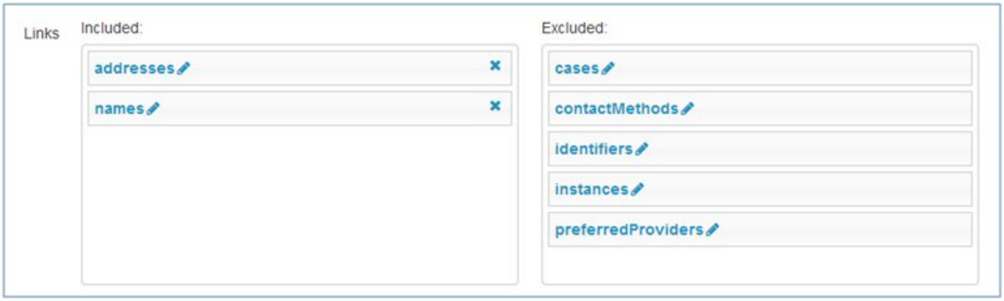


Editing a Table

The Edit Table page looks similar to the New Table page. To navigate to the Edit Table page, administrators must select a table from the list and click the *Edit Table* button. Note that the Source and Table fields cannot be edited. Administrators can enable the Info Tab Indicator to represent Info tabs for a particular table.



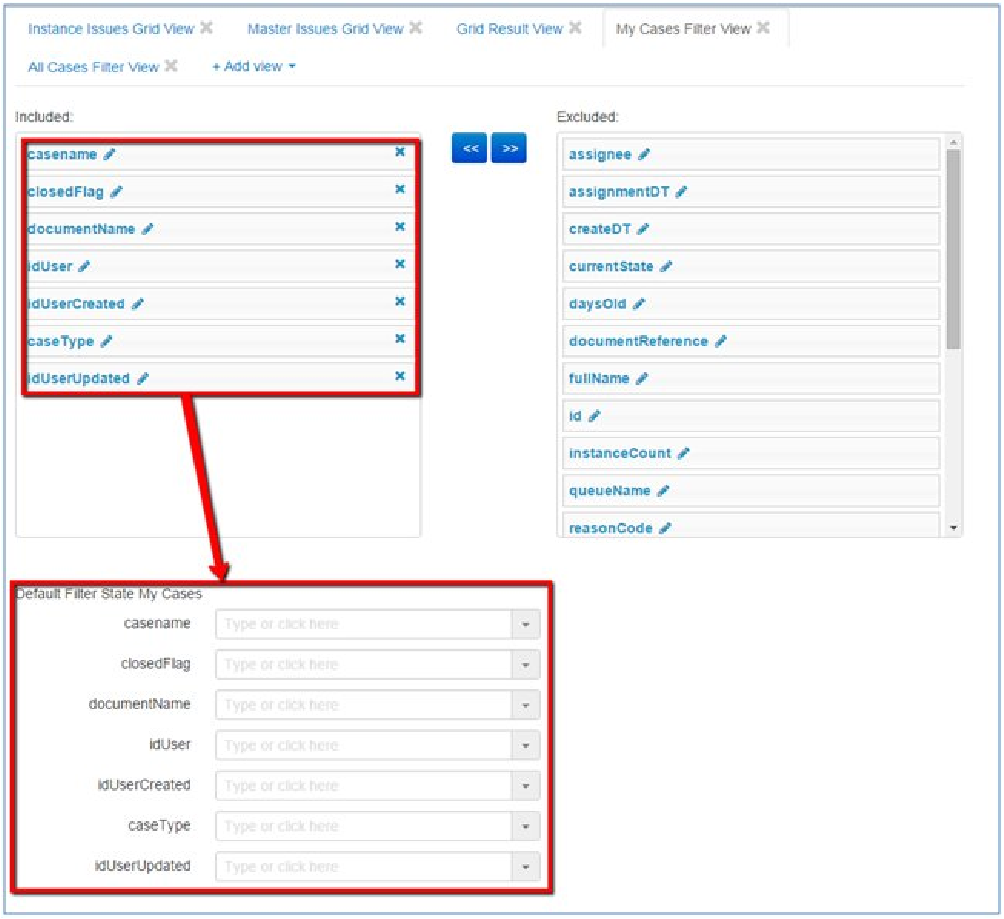
Some views have links. The Links section is displayed after the Columns section.



Columns and links can be added in the Included section by dragging and dropping, or deleted by clicking the "x" icon. Tables displayed in the Links section are represented within the application as subdomains/sub-sub domains.

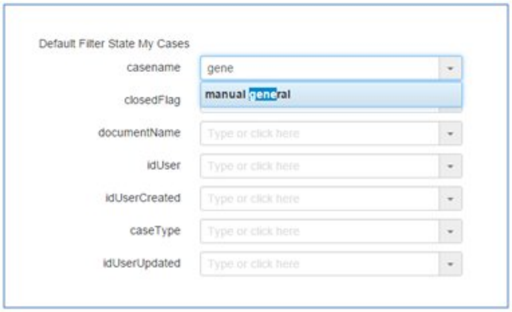
When new options for a View are created, they are displayed on the corresponding View tab after the Columns and Links sections.

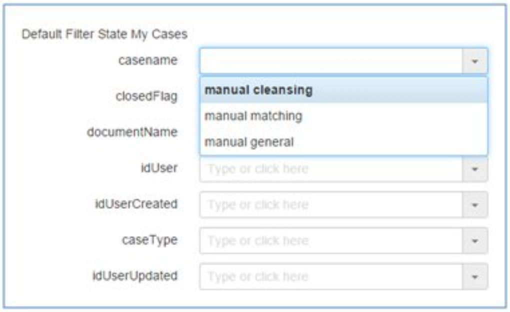
For example, the following image shows Default Filtering on the WF User Cases table.



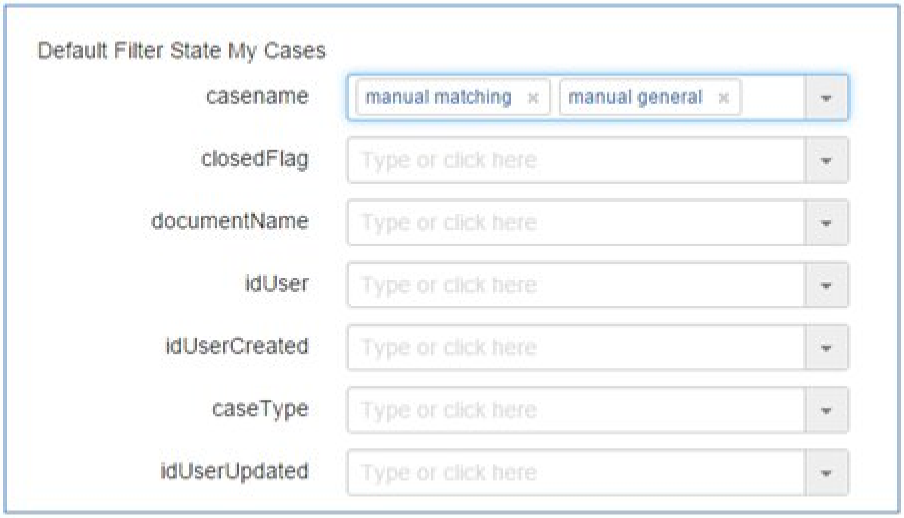
Columns that are placed in the Included section of the My/All cases filter view are displayed in the Default Filtering section as well. If a column is moved to the Excluded section, the column will automatically disappear from the Default Filtering section.

The administrator can select any required value for the field from the drop-down list. Or the administrator can start typing within the field itself to view results that satisfy the filtering criteria.





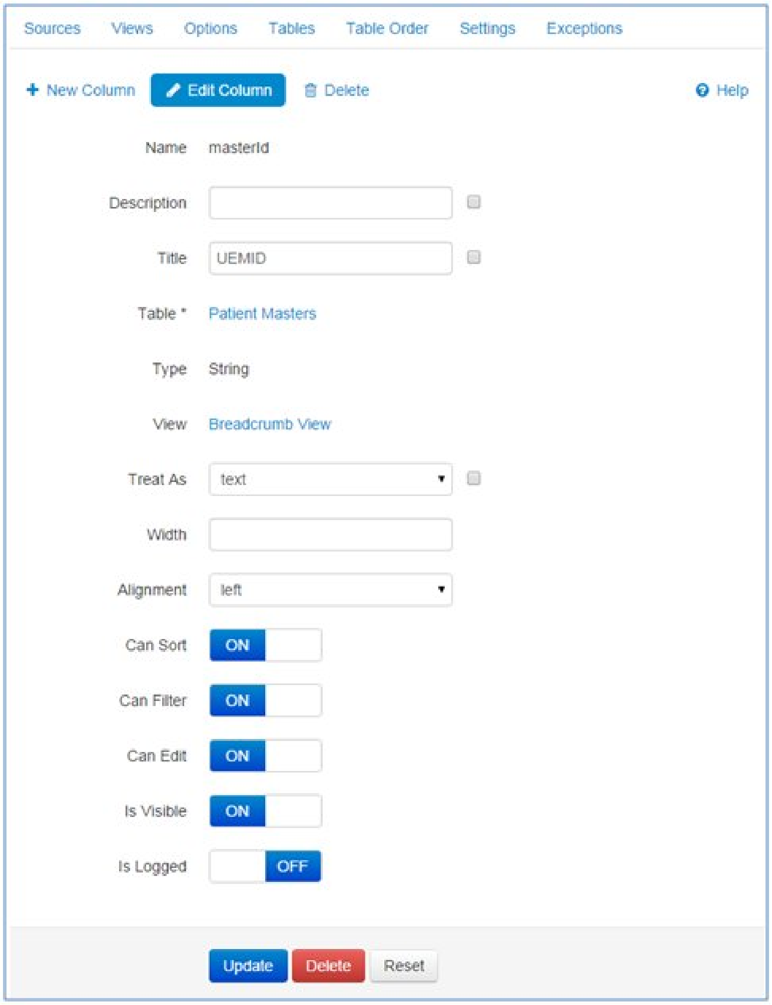
More than one value can be selected for one field if required.



After the required values are set, the administrator can click *Update* to apply the changes.

Editing a Column

Columns can be edited from the Edit Column page, by clicking on the pencil icon for a corresponding column in the table.



Several fields, such as Name, Table, Type, and View are not available for editing. The Table and View fields are hyperlinks to corresponding items.

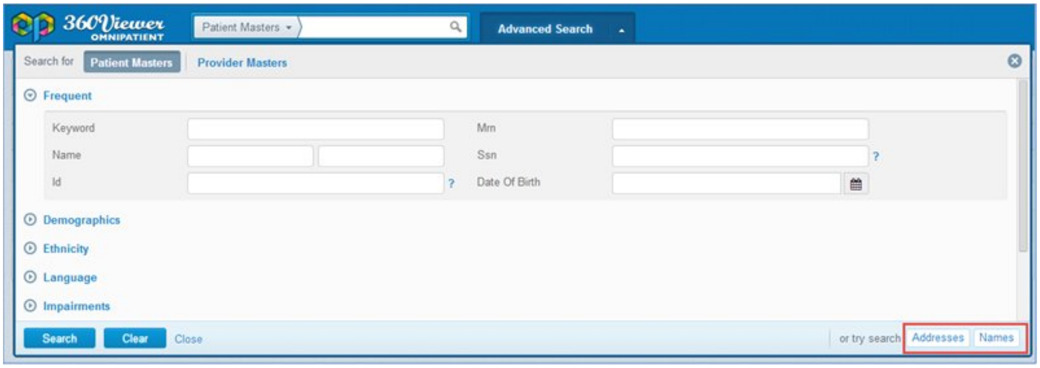
In addition, it is possible to create or delete a current column by clicking the corresponding button.

Global Column Editing

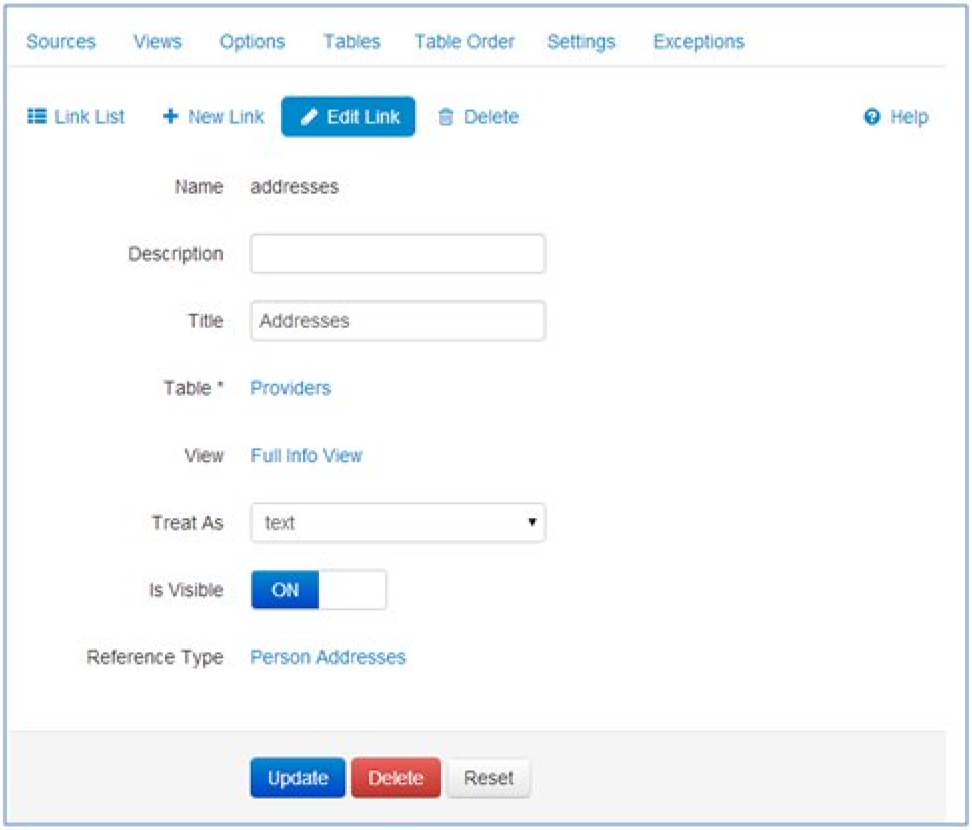
There is an *Update in all views* check box near some fields on the Edit Column page. When selected, the appropriate column will be updated in all views for the corresponding table. For example, if an administrator changes a description in the Patient Masters table with this option selected, then the description will be changed in all views for the Patient Masters table.

Editing a Link

Links represent sub-domains. Links are used, for example, in the Advanced Search dialog. They allow searching by sub-domain parameters of a record. Links are laos used on the Details 360 page, where they display sub-domain tabs.



Link can be edited from the Links section on the Edit Table page, by clicking on the pencil icon.



Several fields, such as Name, Table, Type, and View are not available for editing. The Table and View fields are hyperlinks to corresponding items.

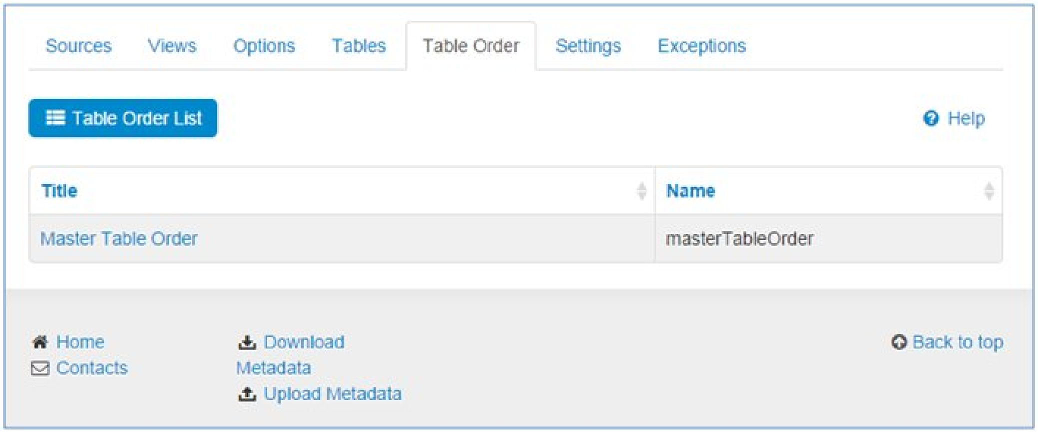
In addition, it is possible to create or delete a current link by clicking the corresponding button.

Table Order

Table Order is a group of Domain tables. Domains included in the Domains drop-down list are displayed based on the order defined in Table Order.

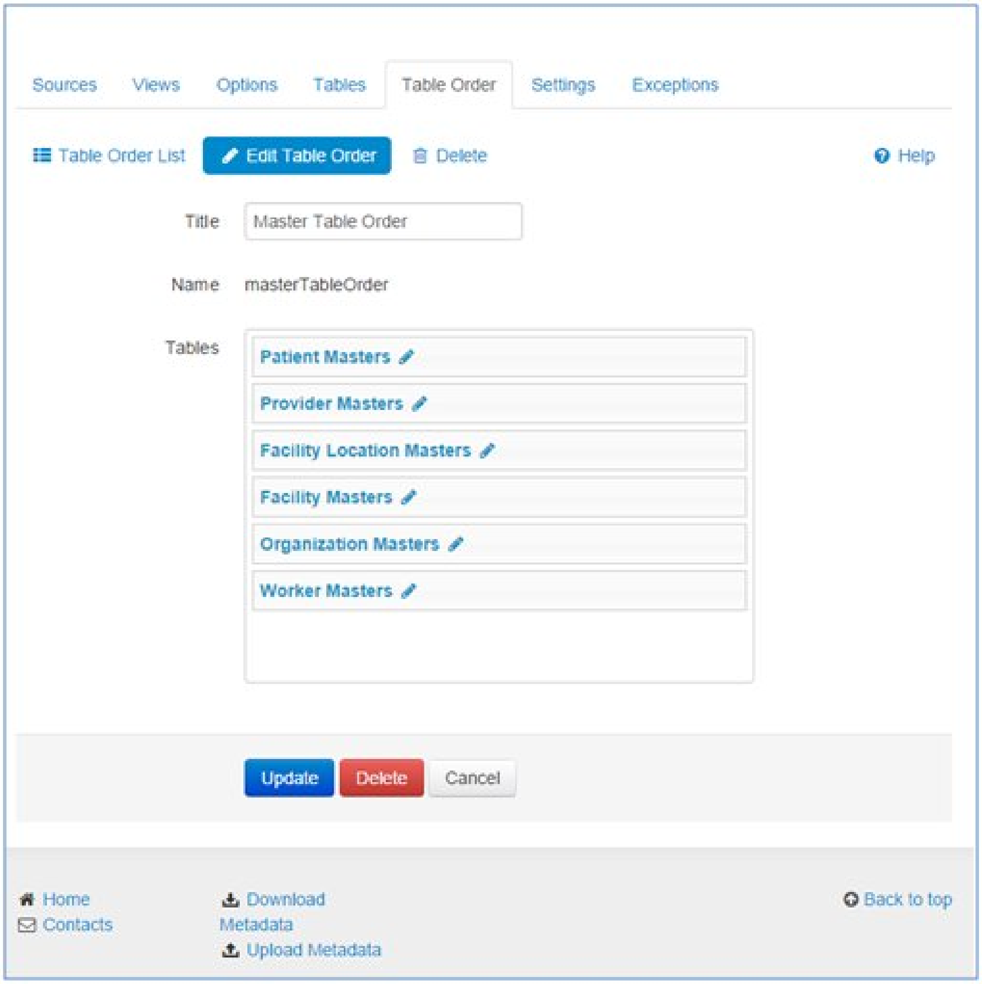
Table Order List

A list of all table orders is displayed on the Table Order List page, as shown in the following image.



Editing a Table Order

The Edit Table Order page is accessible from the Table Order List page by clicking the *Table Order* link and then clicking *Edit Table Order*, as shown in the following image.



Orders can be changed by dragging boxes to the required position and then clicking *Update*.

Settings

Settings are global variables for configuration per whole application. For now, settings are used to configure the following items:

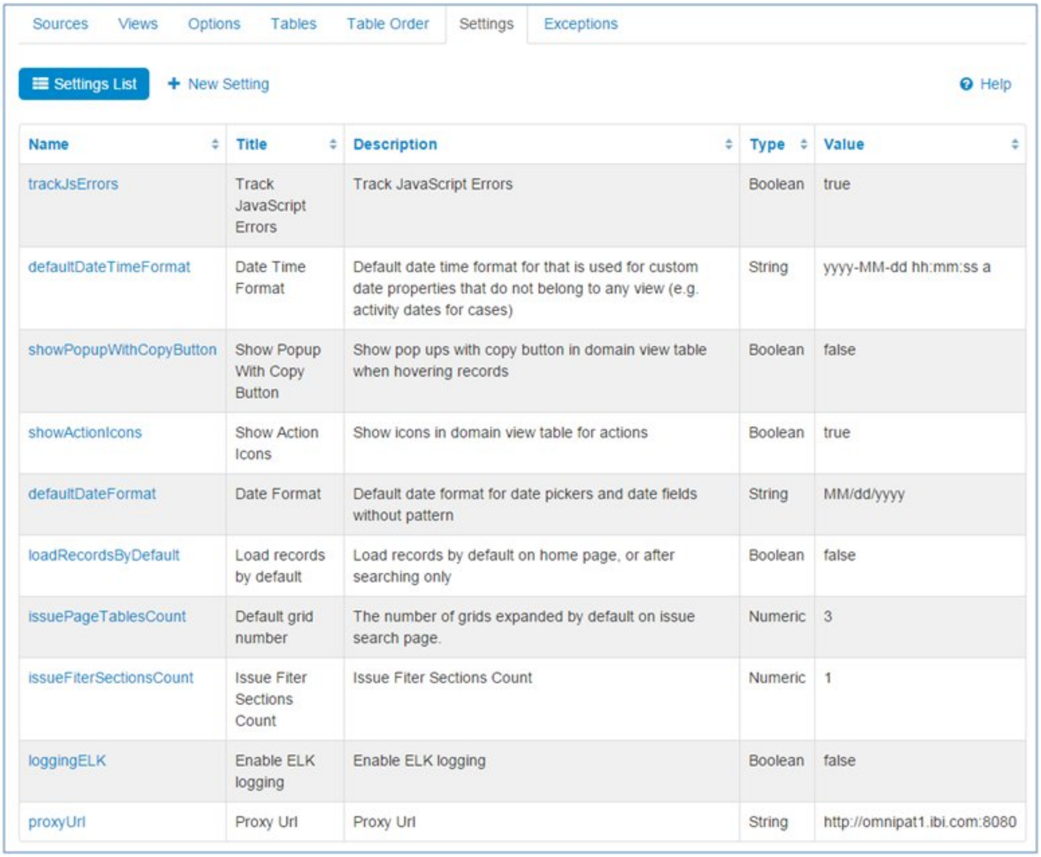
- Default date format for date pickers and date fields.

- Default date time format for that is used for custom date properties that do not belong to any view (for example, activity dates for cases).
- Defining view of links for actions column in domain view table.
- Track JavaScript Errors.
- Show pop ups with copy button in domain view table when hovering records.
- Load records by default on home page, or after searching only.
- The number of tables expanded by default on issue search page.
- Defining of the number of filter sections count.
- Enabling the ELK logging functionality.
- Setting the proxy URL.
- Defining the default display of sections on the Master comparison page.

For example, administrators can change the default date format value to *dd MM yyyy*, and all date fields will be represented in this format.

Setting List

The list of all settings is displayed on the Setting List page, as shown in the following image.



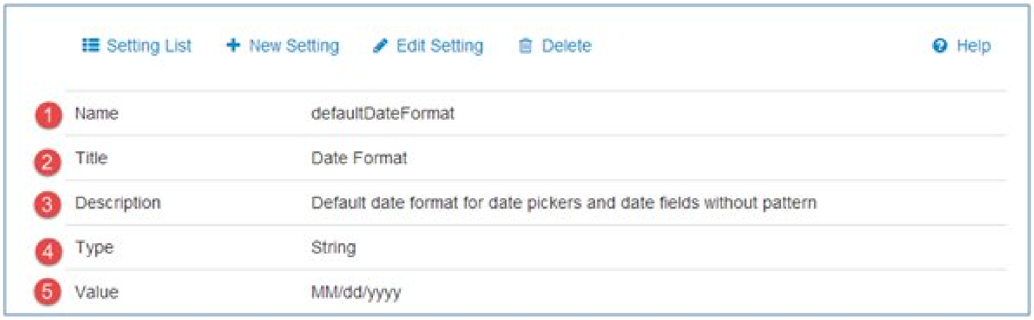
Name	Title	Description	Type	Value
trackJsErrors	Track JavaScript Errors	Track JavaScript Errors	Boolean	true
defaultDateTimeFormat	Date Time Format	Default date time format for that is used for custom date properties that do not belong to any view (e.g. activity dates for cases)	String	yyyy-MM-dd hh:mm:ss a
showPopupWithCopyButton	Show Popup With Copy Button	Show pop ups with copy button in domain view table when hovering records	Boolean	false
showActionIcons	Show Action Icons	Show icons in domain view table for actions	Boolean	true
defaultDateFormat	Date Format	Default date format for date pickers and date fields without pattern	String	MM/dd/yyyy
loadRecordsByDefault	Load records by default	Load records by default on home page, or after searching only	Boolean	false
issuePageTablesCount	Default grid number	The number of grids expanded by default on issue search page.	Numeric	3
issueFiterSectionsCount	Issue Fiter Sections Count	Issue Fiter Sections Count	Numeric	1
loggingELK	Enable ELK logging	Enable ELK logging	Boolean	false
proxyUrl	Proxy Url	Proxy Url	String	http://omnipat1.ibi.com:8080

Show Setting

Administrators can navigate to the Show Setting page by selecting the corresponding setting from the list. The Show Setting page provides the following information about the selected setting:

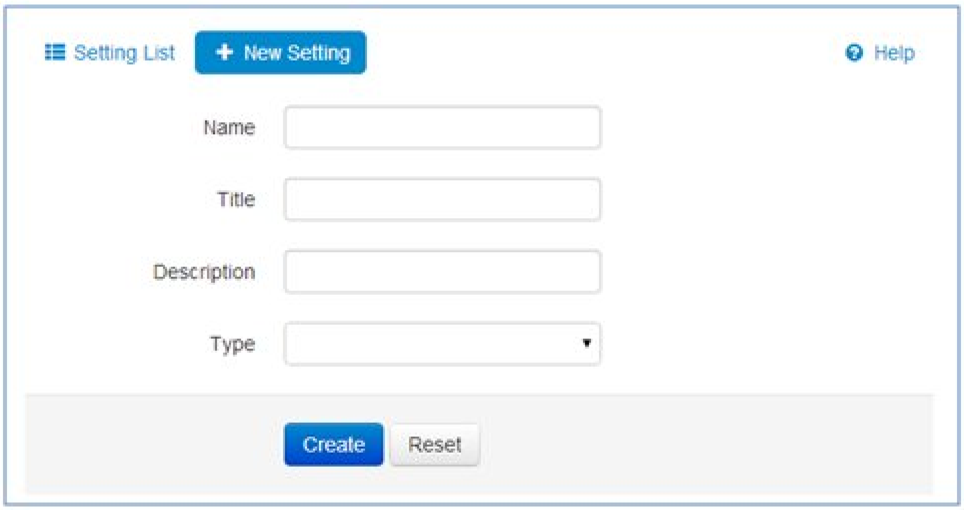
- Setting name
- Setting title
- Setting description
- Setting type

- Setting value



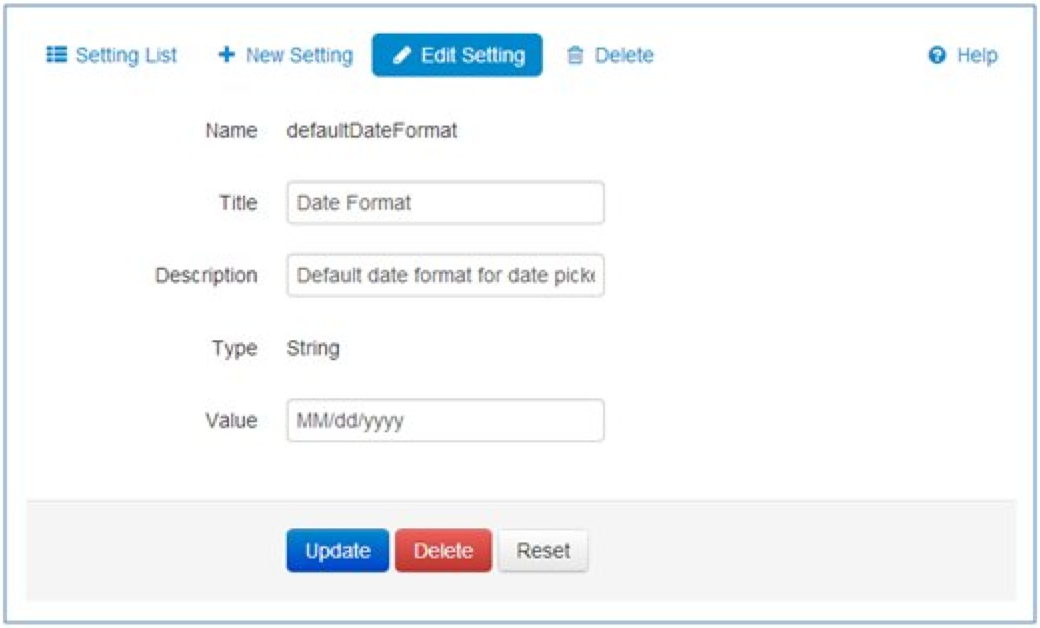
Creating a New Setting

Administrators can create new setting on the New Setting page by clicking the corresponding button on the Show Setting page, as shown in the following image.



Editing a Setting

The Edit Setting page enables administrators to change the properties of a setting. Administrators can navigate to that page by clicking the corresponding button on the Show Setting page, as shown in the following image.



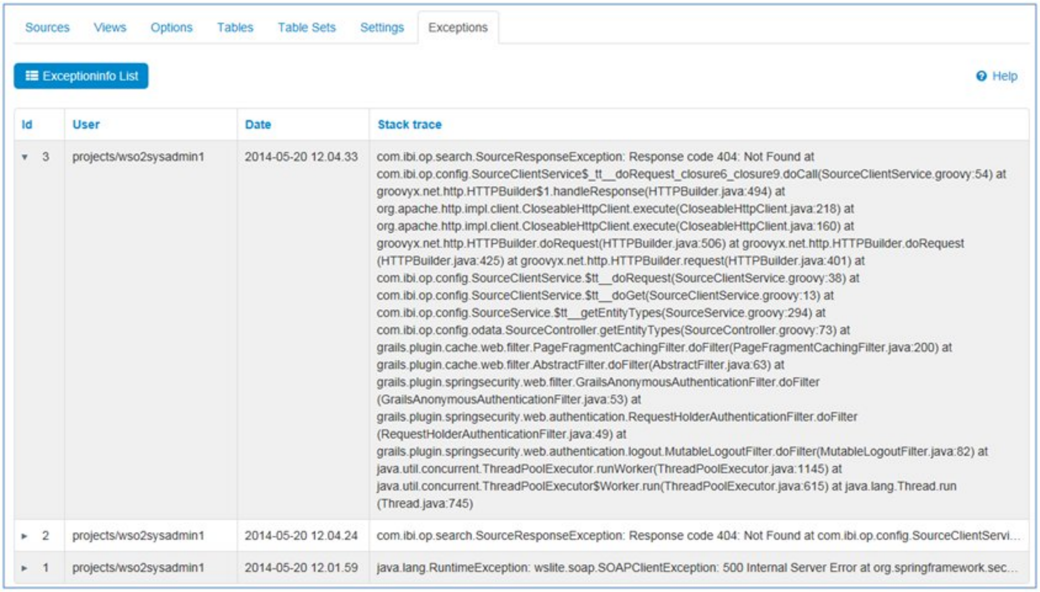
Note that the Name field and Type field cannot be edited.

Exceptions

The Exceptions tab contains information about all errors that have occurred in the application. When an error occurs, a user receives an exception ID on the error page, and an administrator can the error condition based on this ID.

Exception List

The list of all exceptions is displayed on the Exception info List page, as shown in the following image. This page is used to provide information for Omni Governance Console (OGC) support and developers in the event of an error occurrence.



Downloading and Uploading Metadata

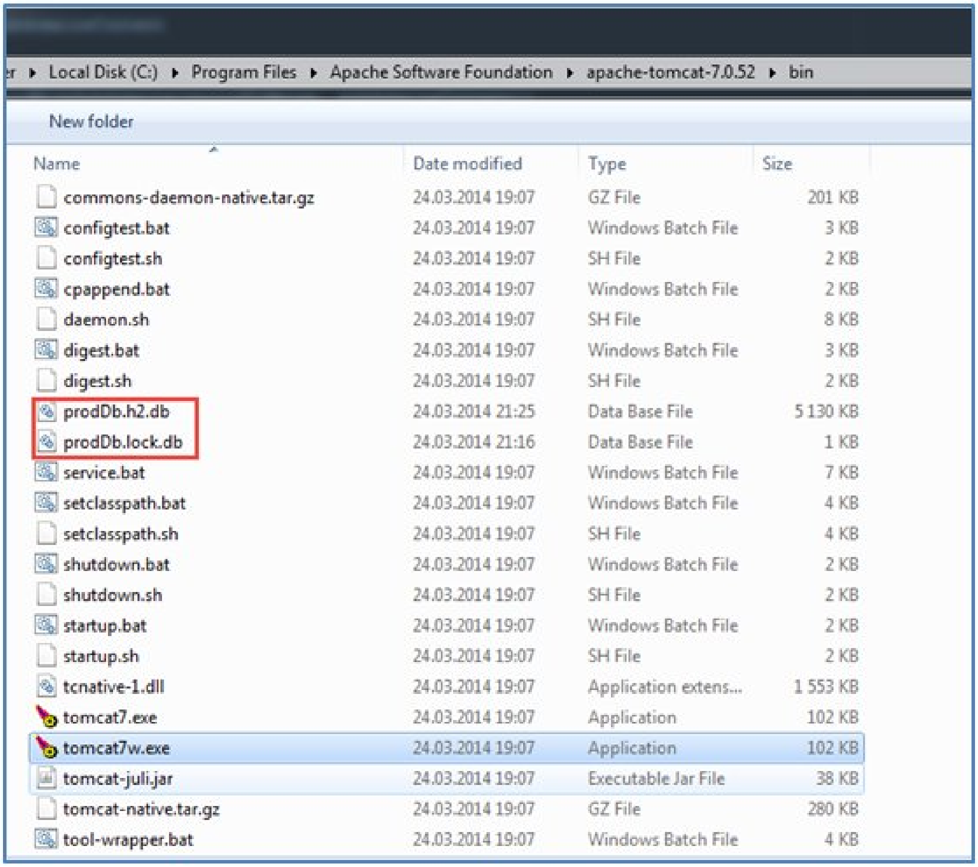
This section describes how to download and upload metadata.

Downloading Metadata

Metadata provides the configuration values for the Omni Governance Console (OGC) application. It describes what sources, domains, and sub-domains (from services, views, settings, and so on) are used within the application. Metadata is stored in XML format in a file-based database.

A *metadata.xml* file is read into and is validated while it populates the OGC configuration database, and initializes application settings.

The configuration database is stored in two files, as shown in the following image.



The database is created during the first deployment of OGC when an existing configuration database (prodDb.h2.db) is not present.

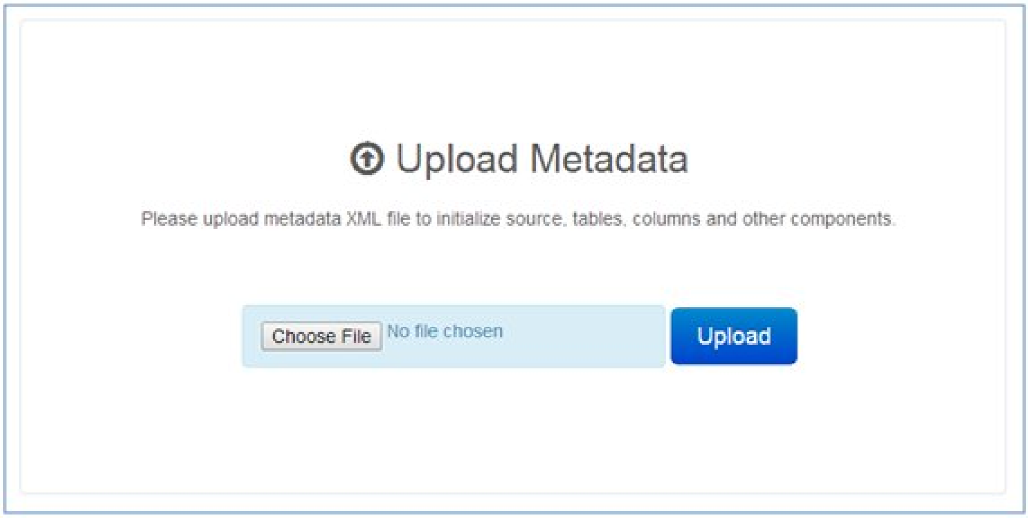
Administrators can download the runtime database of metadata stored as prodDB.h2.db (as shown in the above image) and convert it into a readable metadata XML file by clicking the *Download Metadata* link.

The download link is displayed in the footer of the page, as shown in the following image.

Uploading Metadata

You can configure an application from metadata that is stored in an XML file. There are three scenarios for uploading metadata:

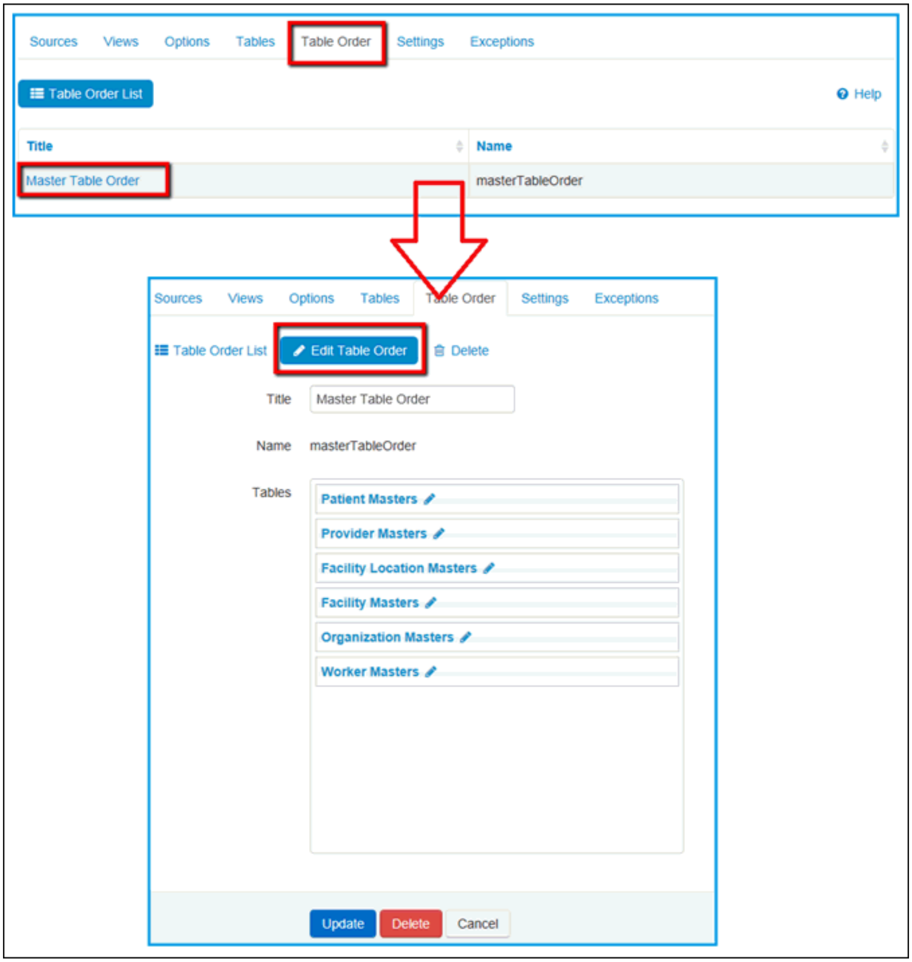
1. Upon the first deployment of the application, when the configuration database is empty. After authorization, the first log in attempt by a user with the System Administrator role will be redirected to the Upload Metadata page. Here, the administrator will be able to select the configuration file that will be provided separately.
2. It is possible to upload metadata without redeployment, when the application is already configured, by clicking the *Upload Metadata* link. It is advisable to do this only if the data structure has not changed, and only some columns or views were edited. Otherwise, the application may crash. In this case, follow the instructions in the third scenario.
3. If remote services were upgraded and the data structure was changed (the application can no longer function), using the second scenario will not work. In that case, stop the application, remove the configuration database, and follow the instructions in the first scenario.



Before uploading, the file is validated to ensure that the format is correct. If the format is incorrect or thee file is empty, an error message appears, as shown in the following image.

Configuring 360 Viewer

To configure the order of domains in the Domain drop-down list, click the Table Order tab and then click *Master Table Order*. You can change the order of the Domains by dragging the domain boxes and then clicking *Update*.



For configuring table columns (Home, Search pages) edit the particular table and include or exclude the necessary columns in the Grid Result View. Each domain has its own set of columns that configures to the appropriate Master tables (Patient Master, Provider Master, Worker Master, and so on), as shown in the following image.

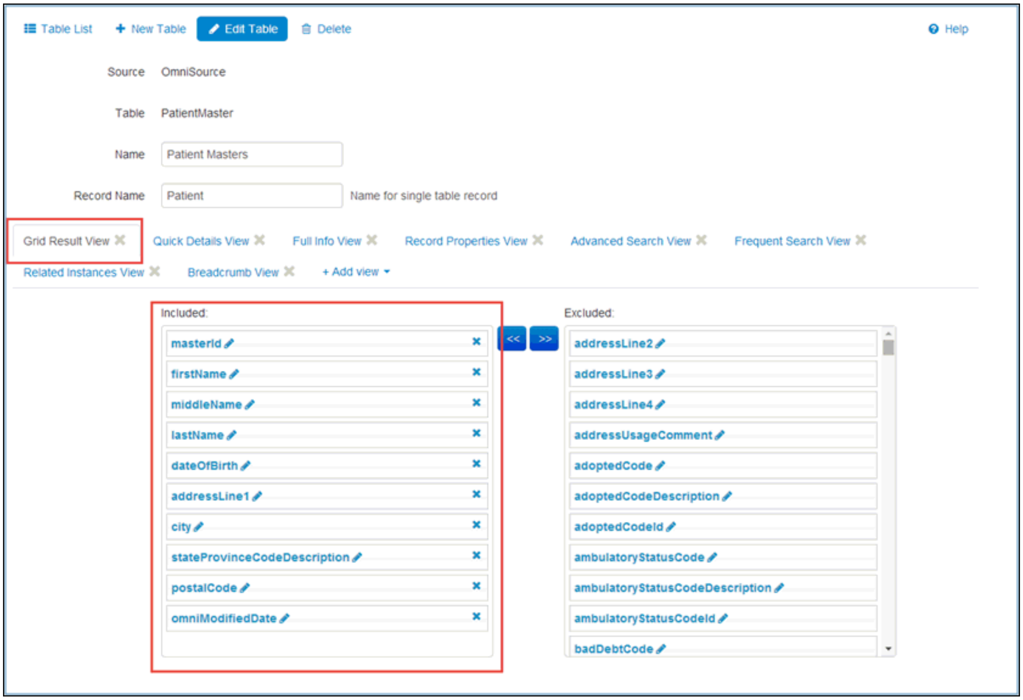
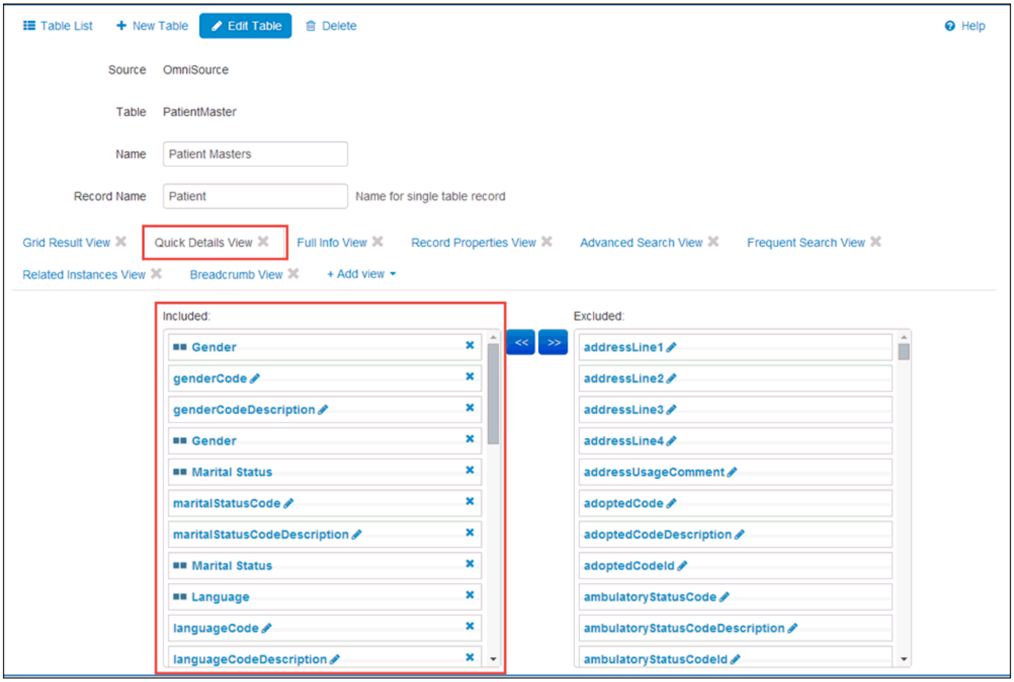
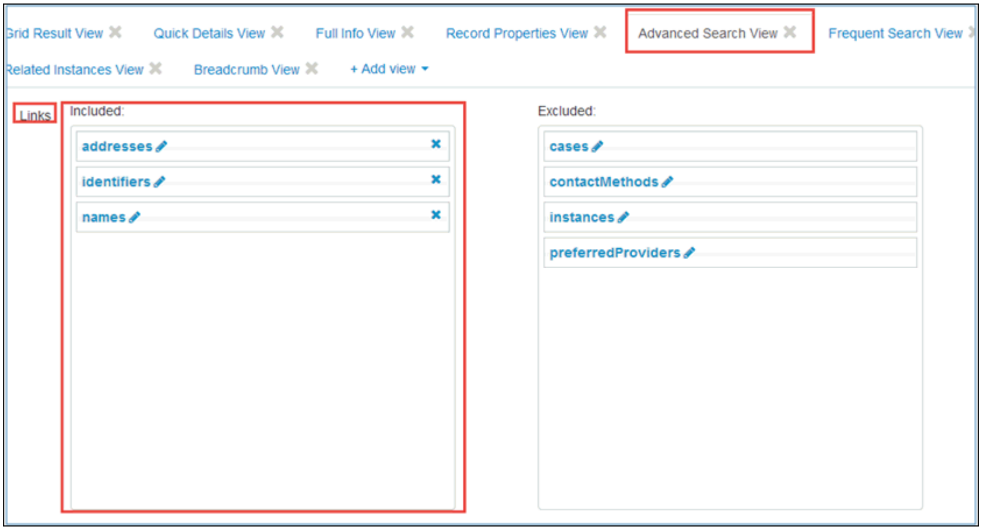


Table List
New Table
Edit Table
Delete
Help
Source OmniSource
Table PatientMaster
Name Patient Masters
Record Name Patient
Name for single table record
Grid Result View
Quick Details View
Full Info View
Record Properties View
Advanced Search View
Frequent Search View
Related Instances View
Breadcrumb View
+ Add view
Included:
masterId
firstName
middleName
lastName
dateOfBirth
addressLine1
city
stateProvinceCodeDescription
postalCode
omniModifiedDate
Excluded:
addressLine2
addressLine3
addressLine4
addressUsageComment
adoptedCode
adoptedCodeDescription
adoptedCodeId
ambulatoryStatusCode
ambulatoryStatusCodeDescription
ambulatoryStatusCodeId
badDebtCode

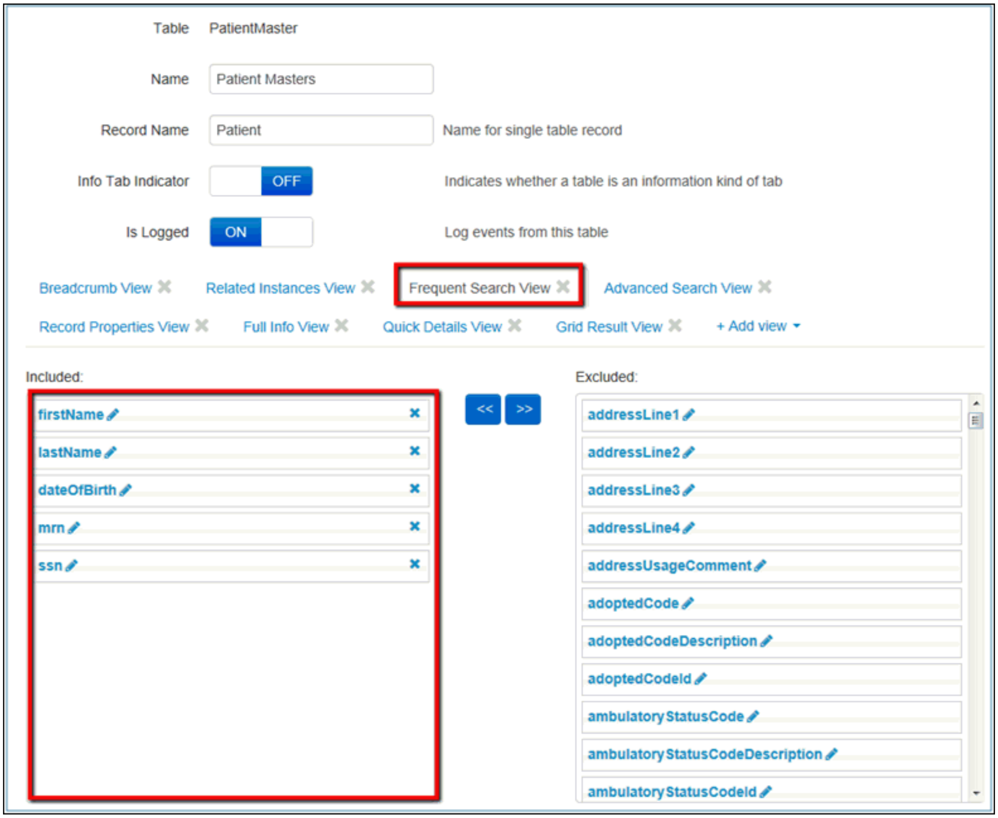
To configure columns for record details, edit the appropriate table and include or exclude the necessary columns in the Quick Details View.



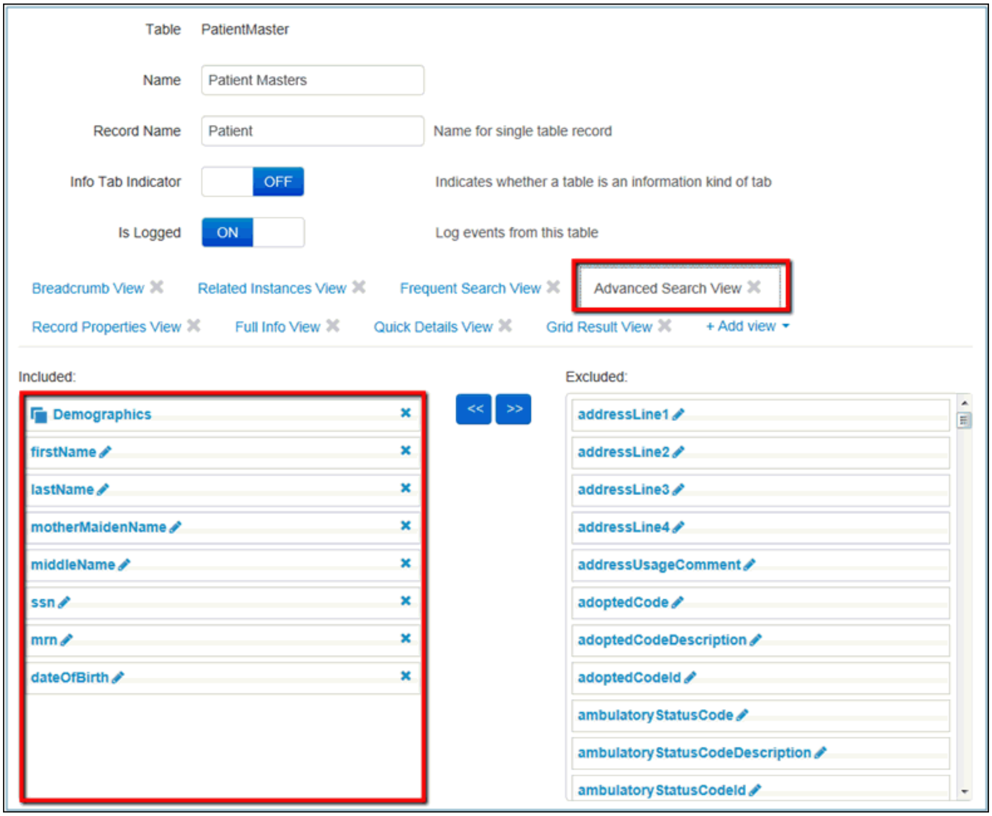
To configure subdomain links for advanced search panels, include or exclude the necessary links in the Advanced Search View tab for the corresponding domain table.



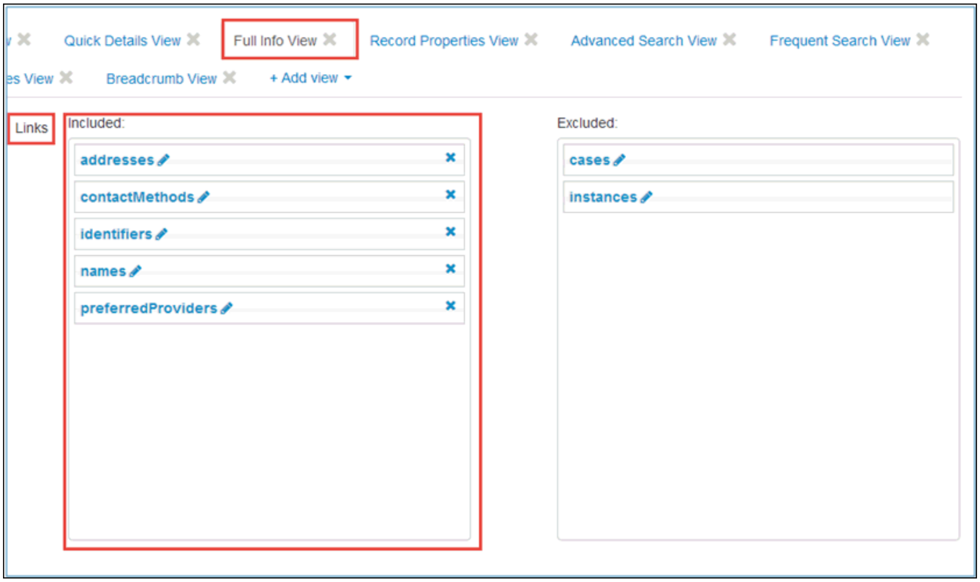
To configure fields in the Frequent Search View, include or exclude the necessary columns, as shown in the following image.



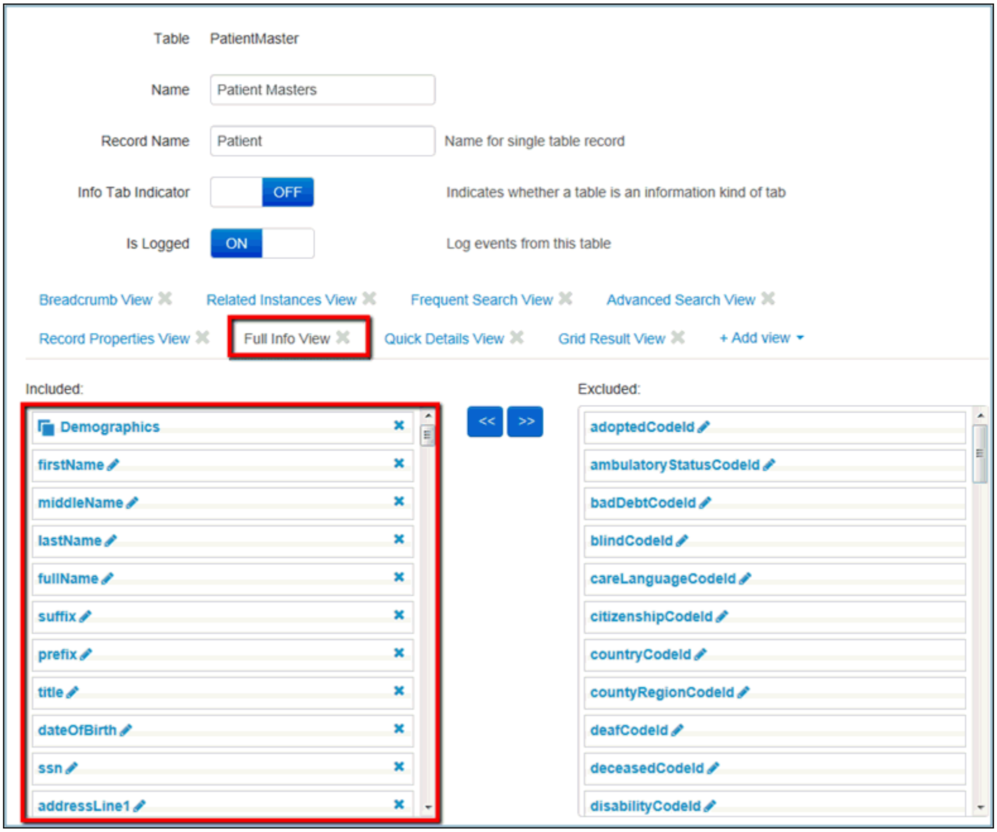
To configure all Advanced Search sections (except Frequent section) and their attributes, include or exclude the necessary columns in the Advanced Search View, as shown in the following image.



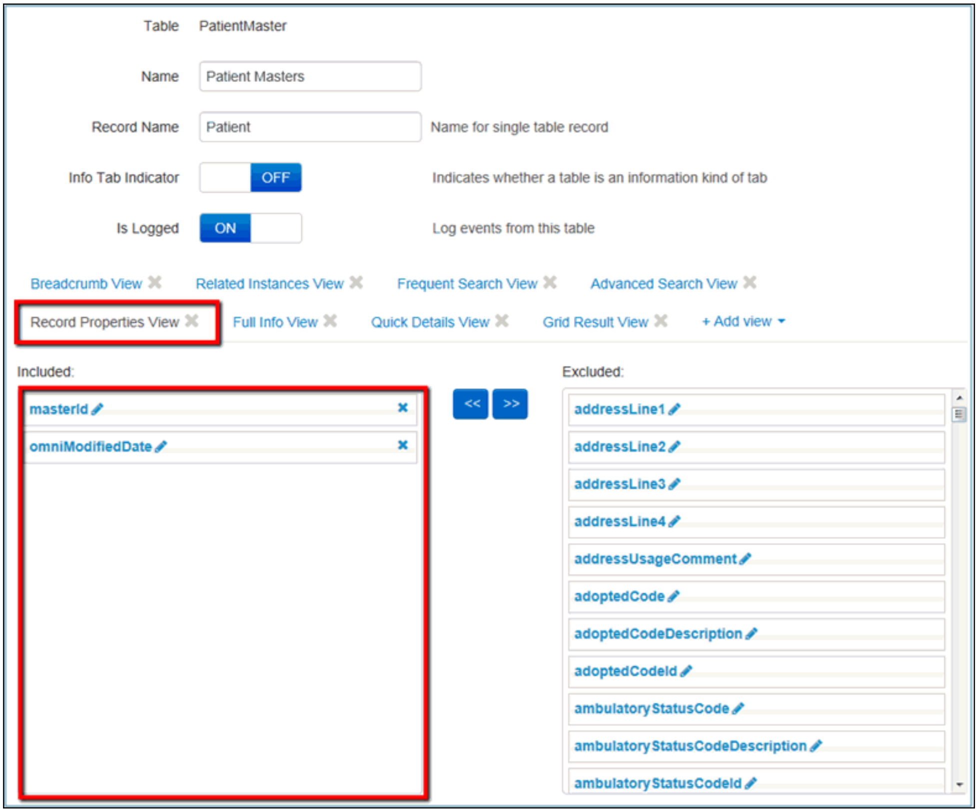
To configure subdomains for Details 360 and Master Comparison pages, edit the Master table and include or exclude the necessary links in the Full Info View tab, as shown in the following image.



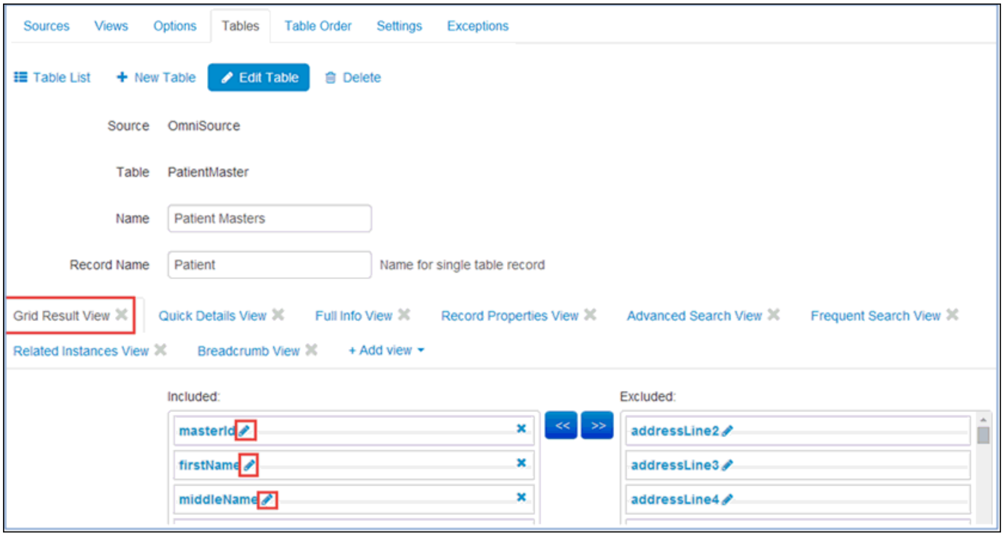
In the Full Info View tab, you can configure sections and their attributes for Domain or Subdomain (for example, Details 360, Master Comparison, and Compare Source pages) by including or excluding the necessary columns, as shown in the following image.



To configure the Record Properties section attributes, include or exclude the necessary columns in the Record Properties View, as shown in the following image.

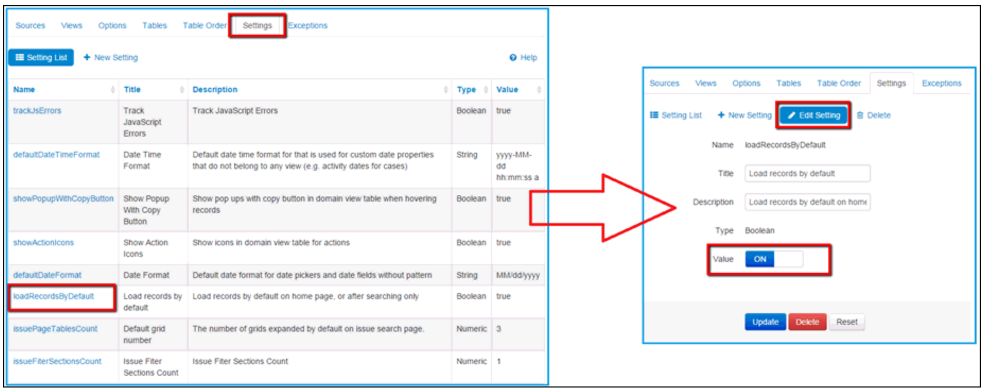


To configure the size, alignment of columns, and the columns to be sorted and filtered, click the pencil icon (Edit) in Grid Result View, as shown in the following image.



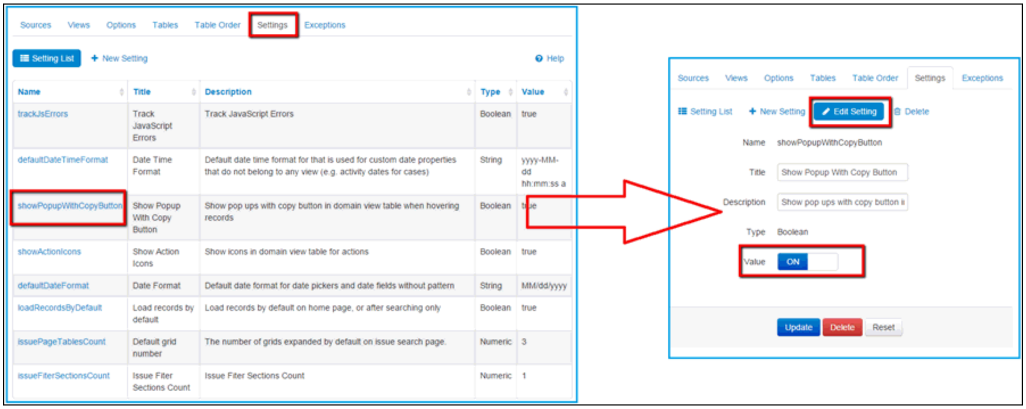
To select the default state of the Home Page, click the Settings tab, select the *Load records by default* setting from the list, and then edit the parameters accordingly.

If you wish to display the grid on the page by default, select *ON* in Value field and then click *Update*. Otherwise, select *OFF*.



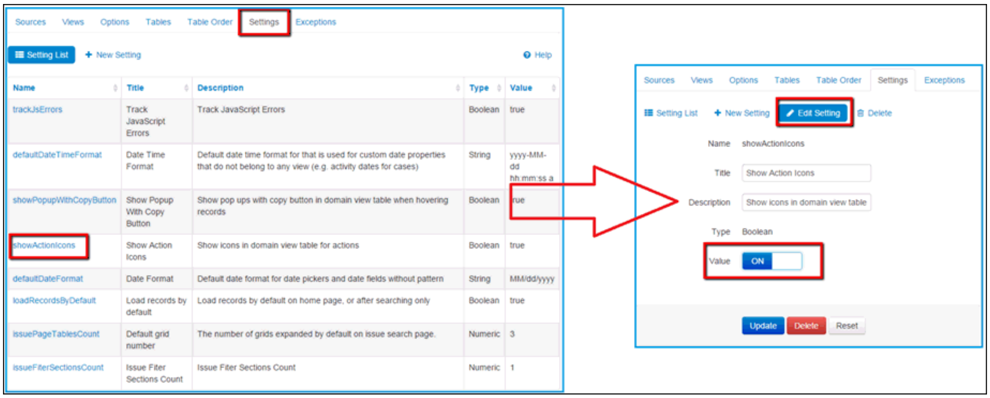
To configure the Copy button in Popup windows, click the *showPopupWithCopyButton* setting in the Settings tab and edit it accordingly.

If you wish to display the Copy button, select *ON* in Value field and then click *Update*. Otherwise, select *OFF*.



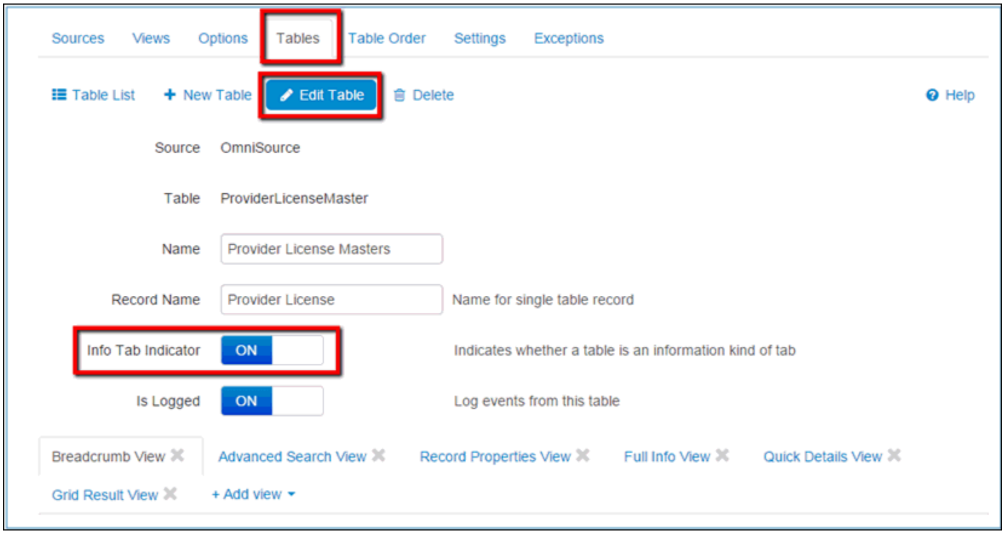
To configure the Master comparison and Details 360 display screens, click the Settings tab, then click the *showActionIcons* link from the list and edit it accordingly.

To display the Master comparison and Details 360 as icons, set the Value parameter to *ON*, and then click *Update*. Otherwise, to display them as links, set the Value parameter to *OFF* and then click *Update*.

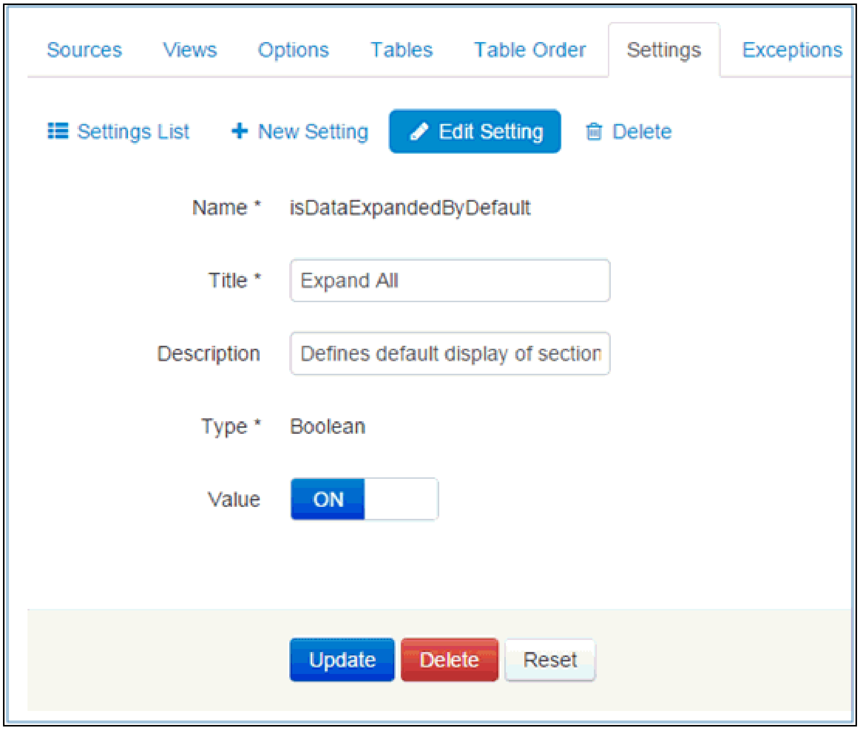


To configure the display of information tabs, click the Tables tab, select the required table from the list, and edit it accordingly.

To display the table as an Information tab, set the Info Tab Indicator parameter to *ON*. Otherwise, to display the table as an ordinary sub-domain, set the Info Tab Indicator to *OFF*.



You can configure the default display of sections on the Master Comparison page. All sections on Master Comparison page can be collapsed or expanded by default. It can be configured using the setting *IsDataExpandedByDefault*, as shown in the following image.



If you want all sections to be expanded by default, set the Value parameter to *ON*. Otherwise, set the Value to *OFF* to collapse all sections by default.

Configuring Remediation Pages

This section describes the configurations for the remediation pages.

Issues Page

The Administration panel is available for users with the System Administrator role.

You must first identify which grid on the Issues page needs to be configured.

- If the Parent grid needs to be configured, click the Tables tab and select the *WF Cases* table from the list of tables.
- If the Inline grid needs to be configured, click the *WF Tickets* table from the list of tables.

Case Issues Grid

The Case Issues Grid view is responsible for the looks and appearance of the Case Grid in the All Cases and My cases tab of the Issues Search page. The view consists of the following parts:

- general
- domain

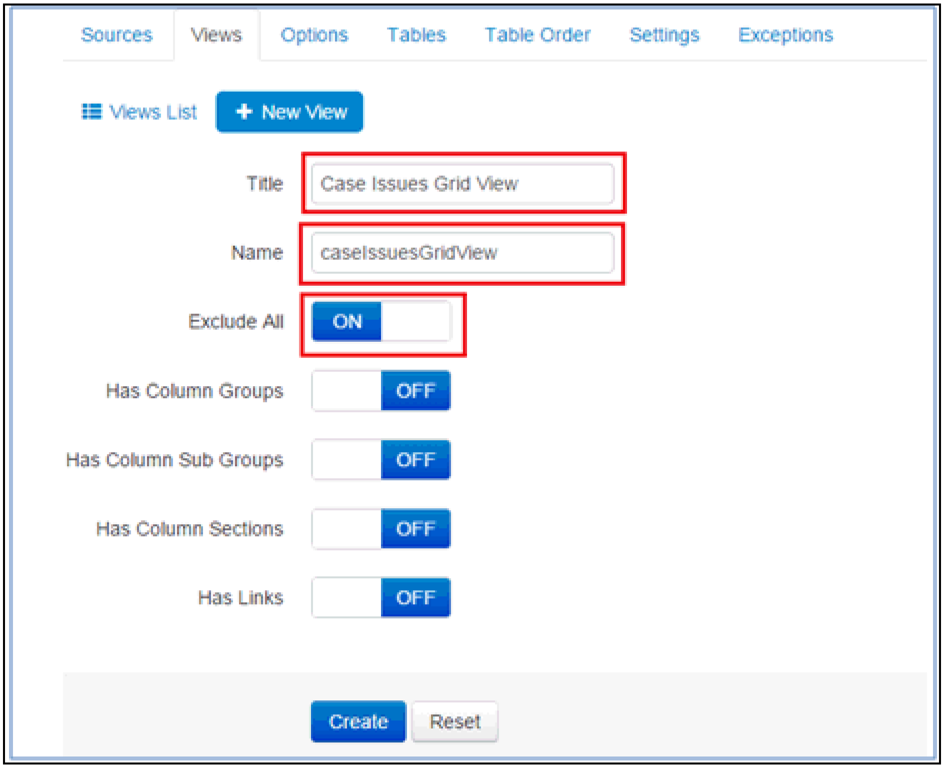
The general-related part includes columns which are common for all domains and configurations in the main Included section of the Case Issues Grid view.

The domain columns are displayed next to the general columns in the grid and can each be preconfigured for the current user domain.

In order to configure how the Case grids appear on the Issues Search page, click the Tables tab and select *WF Cases* from the list of tables. The table should consist of the following views:

- My filter Issues Grid
- All Filter Issues Grid
- Advanced Search View
- Case Issues Grid View

First, check if the current metadata contains a particular view in Views List. If the Case Issues Grid View is not created yet, delete the existing Master Issues Grid View, then click the *New View* button and fill in the required fields, as shown in the following image.

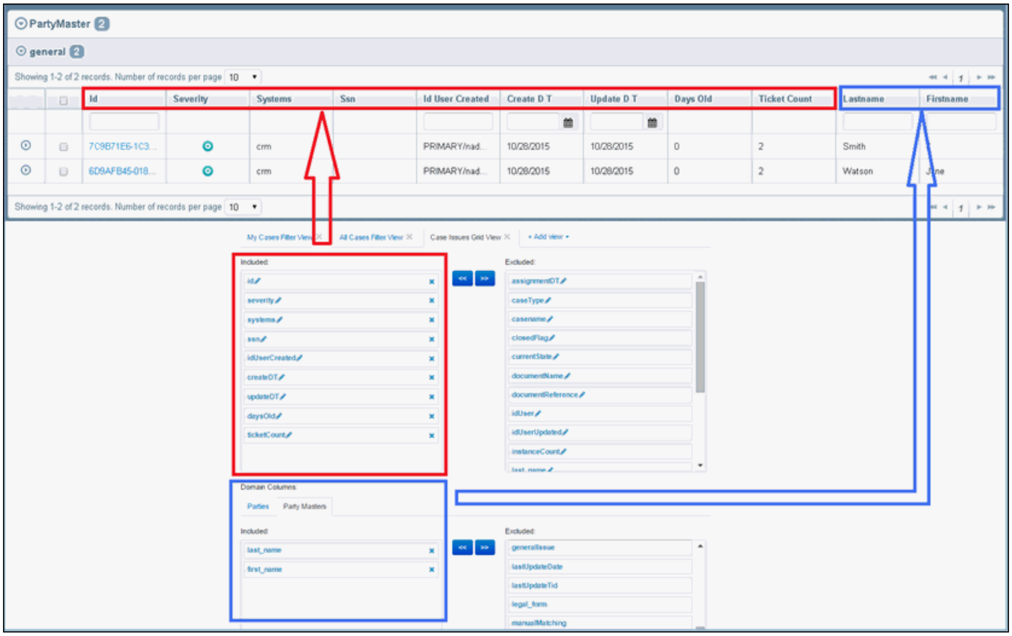


Click *Create* and then click the Tables tab, open the *WF Cases* table, and click *Edit Table*.

Add the required Views from the *Add View* drop-down list and exclude any that are not required.

To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view.

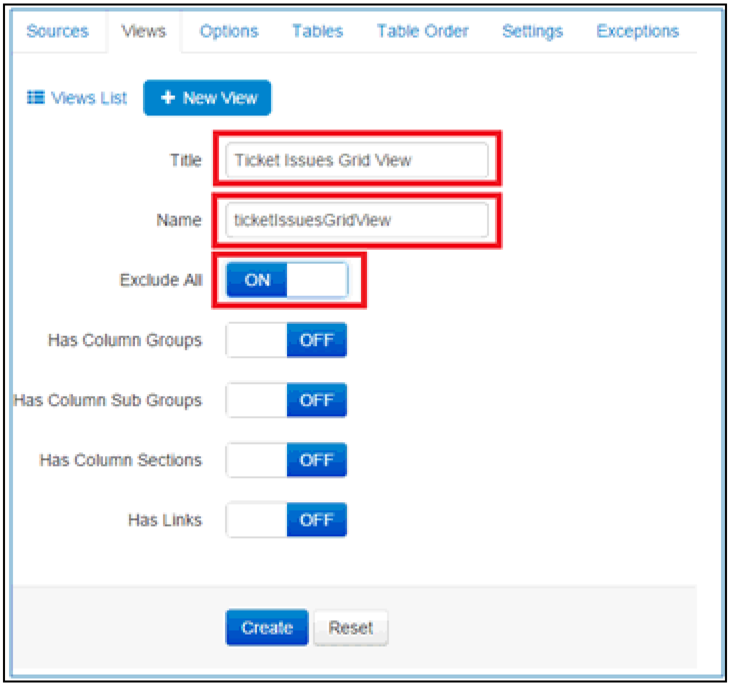


Ticket Issues Grid

The Ticket Issues Grid View is responsible for how the Inline grid appears, which is used to display Ticket details. In order to configure the Inline grids in the Issues Search page, click the Tables tab and select *WF Tickets* from the list of tables. That table should consist of the following views:

- ❑ My filter Issues Grid
- ❑ All Filter Issues Grid
- ❑ Ticket Issues Grid View.

Check if the current metadata contains a particular View in Views list. If the Ticket Issues Grid View is not created yet, delete the existing Instance Issues Grid View, then click the *New View* button and fill in the required fields, as shown in the following image.

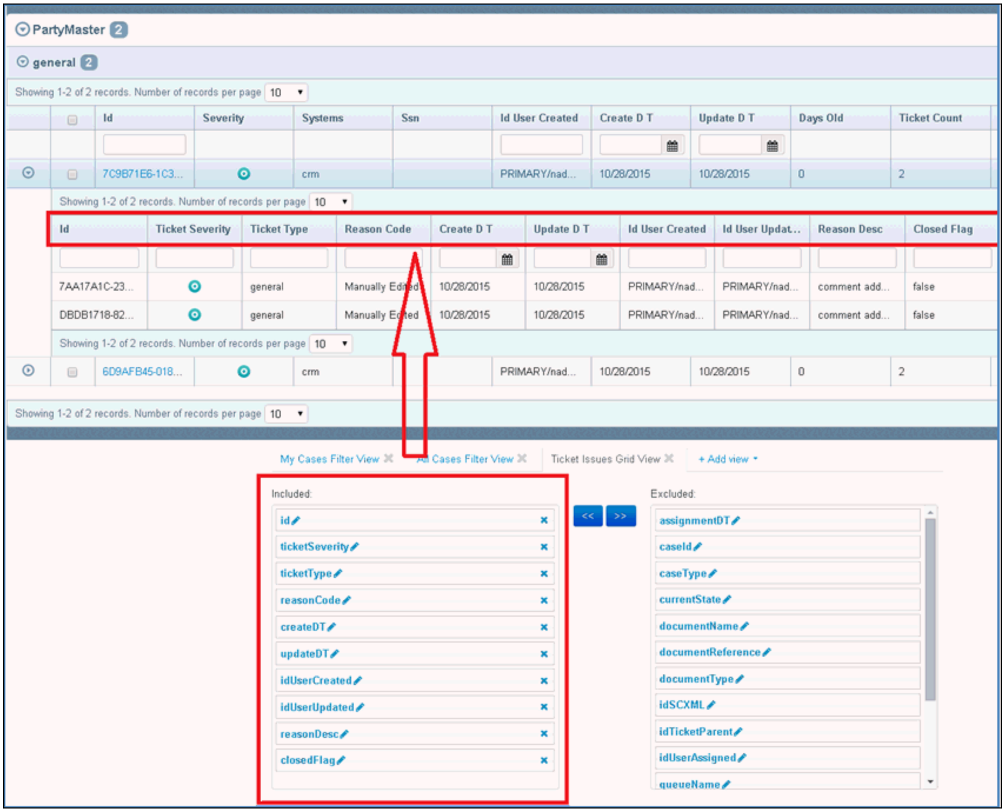


Click *Create*, and click Tables tab, then open the *WF Tickets* table and click *Edit Table*.

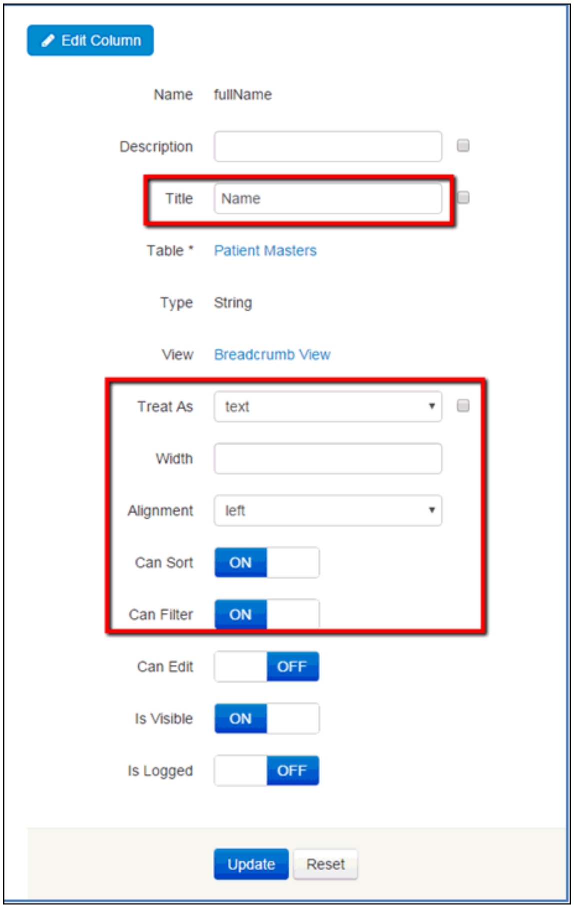
Add the required Views from the *Add View* drop-down list and exclude any that are not required.

To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view.



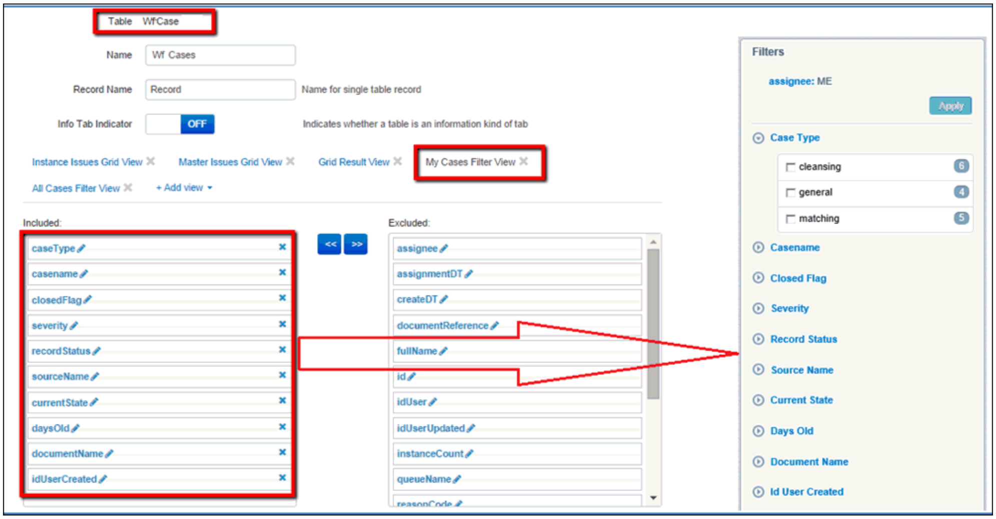
The configuration of nested columns (for example, display name, sortable, filterable) are available by clicking the pencil (edit) icon for the appropriate columns and updating the corresponding options.



Filtering Panel on My Cases Tab

In order to configure the Filtering Panel for cases on the Issues page, click the Tables tab and then click *WF Cases* from the list of tables. If the Filtering panel for tickets needs to be configured, then the *WF Tickets* table should be edited.

The My Cases Filter View is responsible for the list of filtering criteria displayed in the Filtering panel of the My Cases tab, as shown in the following image.



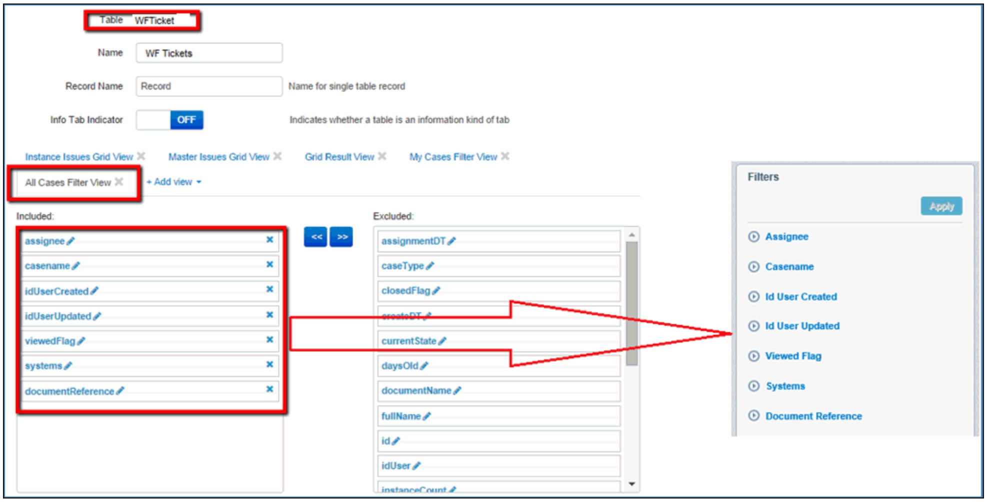
To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view.

Filtering Panel on All Cases Tab

In order to configure the Filtering Panel for cases on the Issues page, click the Tables tab and then click *WF Cases* from the list of tables. If the Filtering panel for tickets needs to be configured, then the *WF Tickets* table should be edited.

The All Cases Filter View is responsible for the list of filtering criteria displayed in the Filtering panel of the All Cases tab.



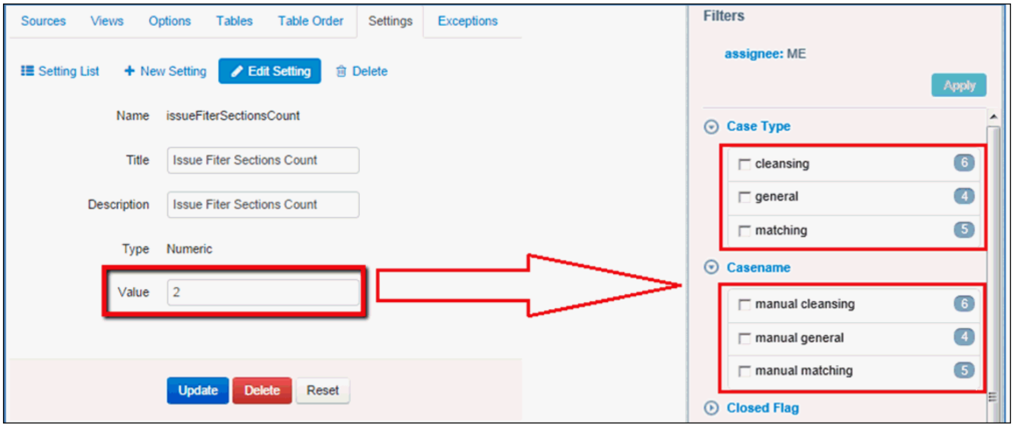
To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view.

Number of Filtering Criteria Sections Expanded by Default

In order to change the number of Filtering criteria sections expanded by default, click the Settings tab and select *Issue Filter Sections Count* from the list.

The number entered in the Value field corresponds to the number of sections to be expanded by default in the Filtering Panel of the Issues page.



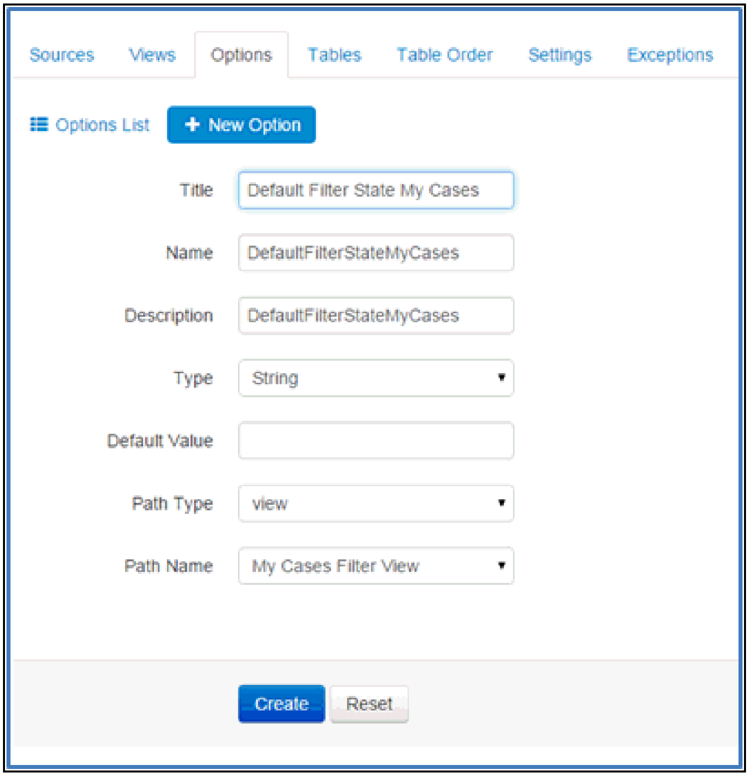
This setting is applied to Filtering panels on both the My Cases and All Cases tabs.

Default Filtering on My Cases/All Cases Tab

In order to have default filters in the issue search page, you must create the following options accordingly:

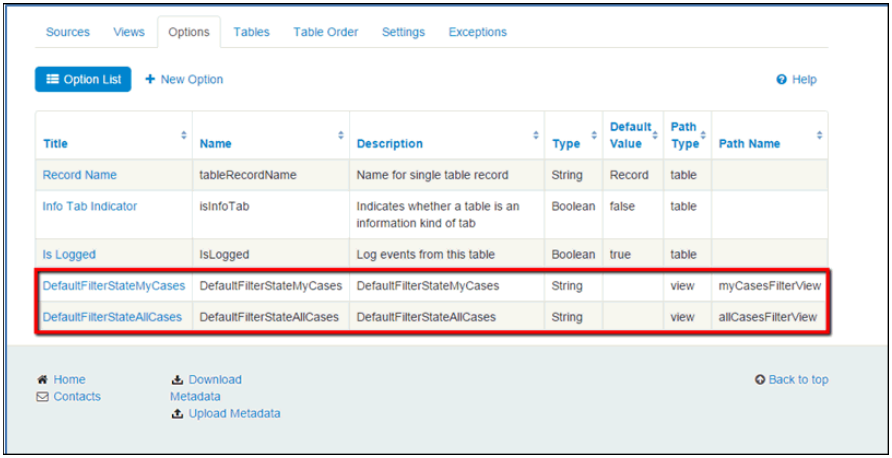
- DefaultFiltersMyCases

❑ DefaultFiltersAllCases



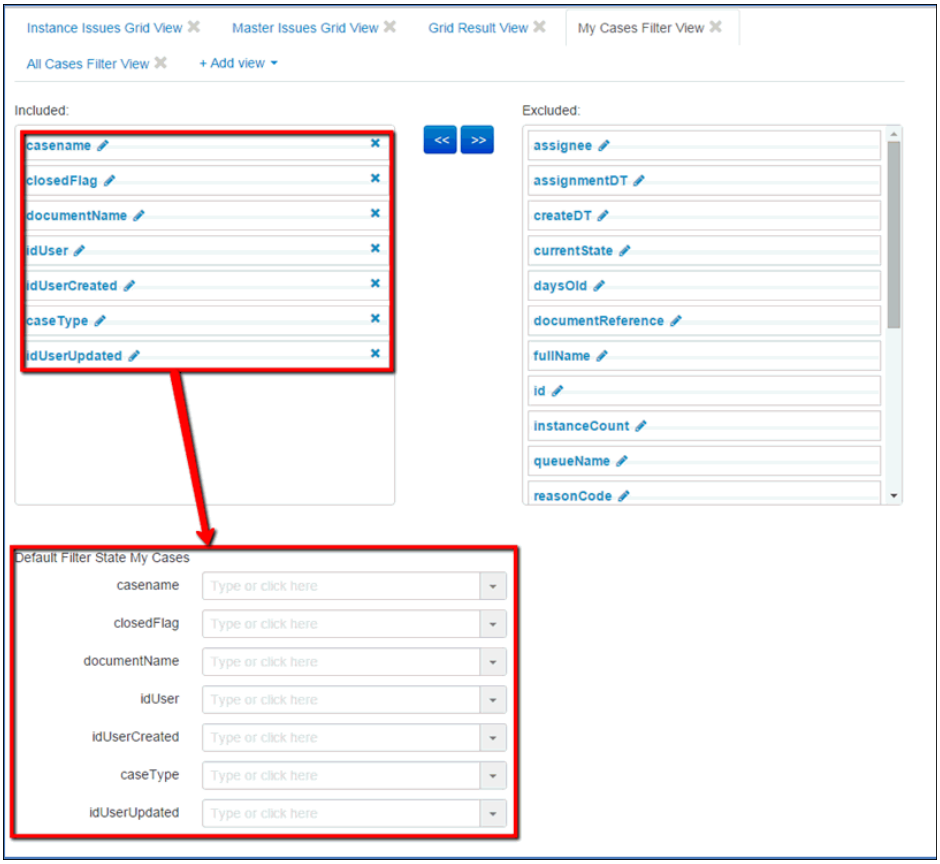
You must perform the same steps for the All Cases tab.

When the options are created, they will appear in a list of options, as shown in the following image.



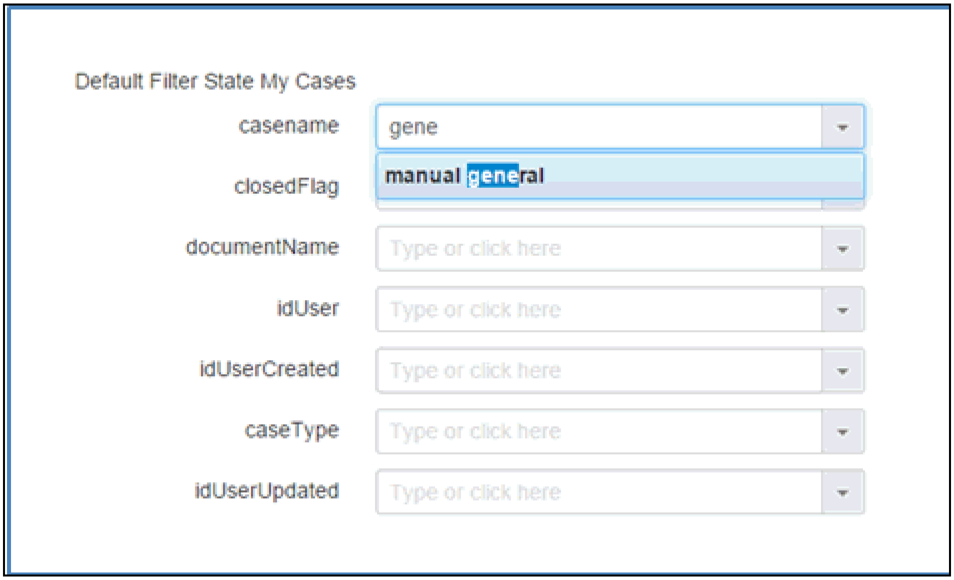
After the options have been added, add the required values to the default filtering section for the corresponding tab of the WF Cases table.

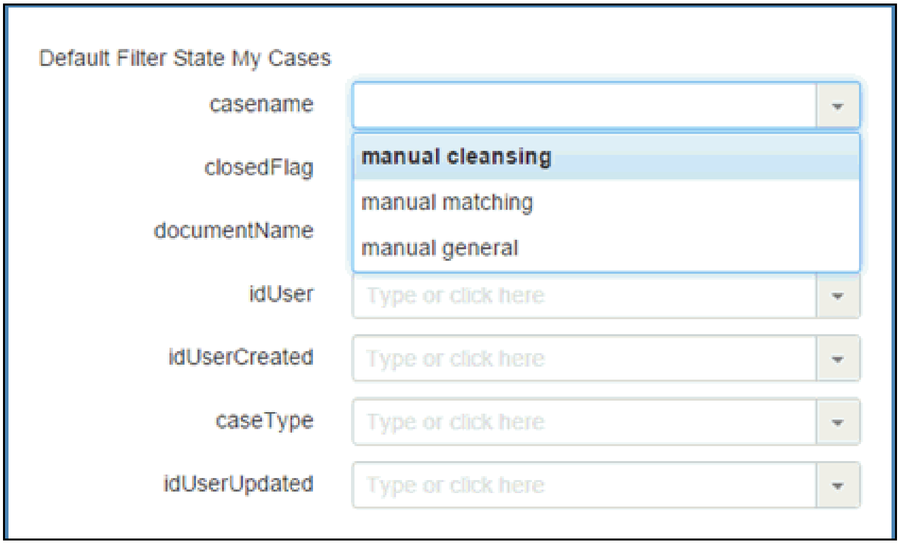
The following image shows the columns that are in the Included section of the My Cases and All Cases filter view.



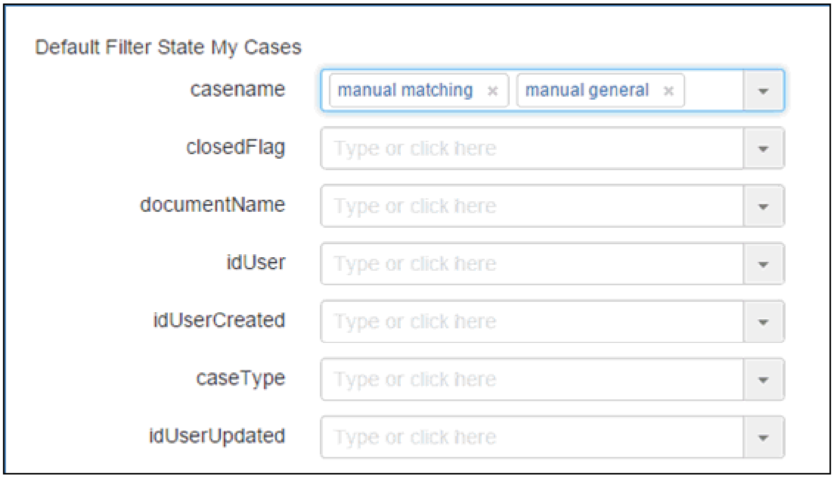
If a column is moved to the Excluded section, it will automatically disappear from the Default Filtering section.

You can select any required value for the field from the drop-down list. You can also start typing in the field and then select any of the results that meet your criteria, as shown in the images below.





More than one value can be selected per field if needed:



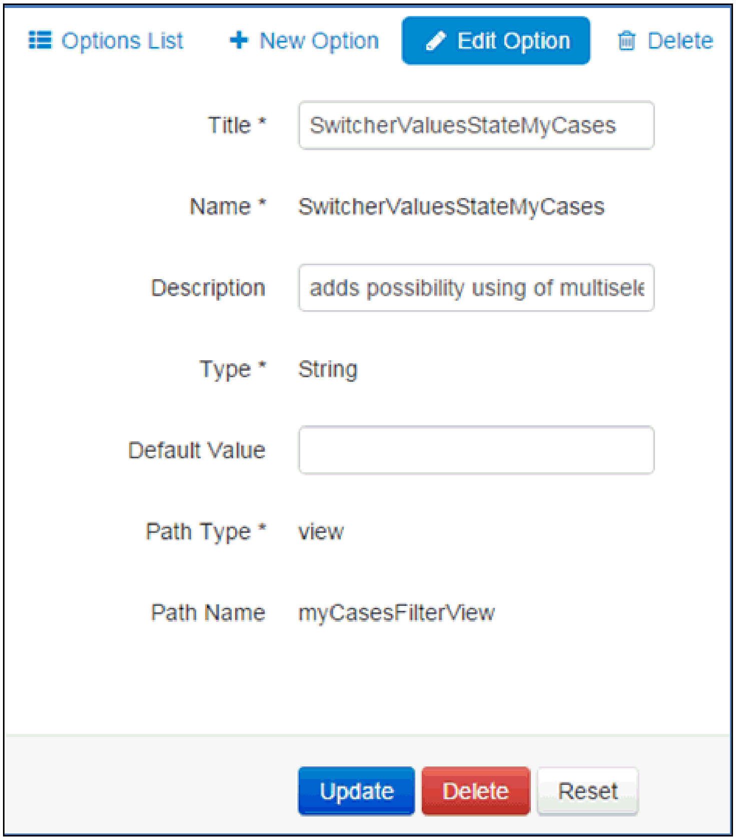
After the required values are set, click *Update* to apply the changes.

Switching ON/OFF of Multiselect Drop-down List on My Cases/All Cases Tabs

To enable fields with multiselect drop-down lists on the Filtering Panel Issue search page, you must create the following options:

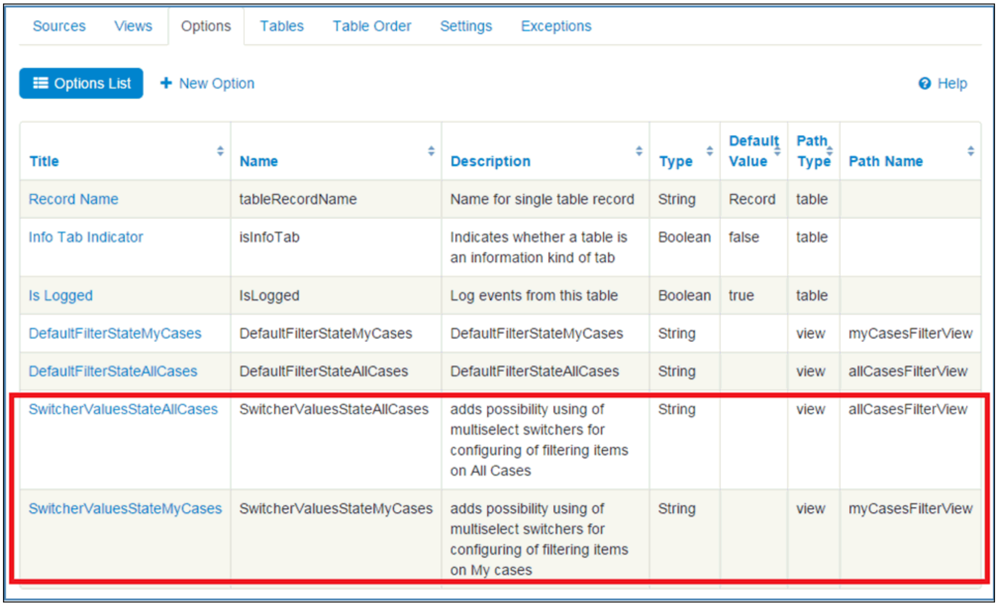
- SwitcherValuesStateAllCases

- SwitcherValuesStateMyCases



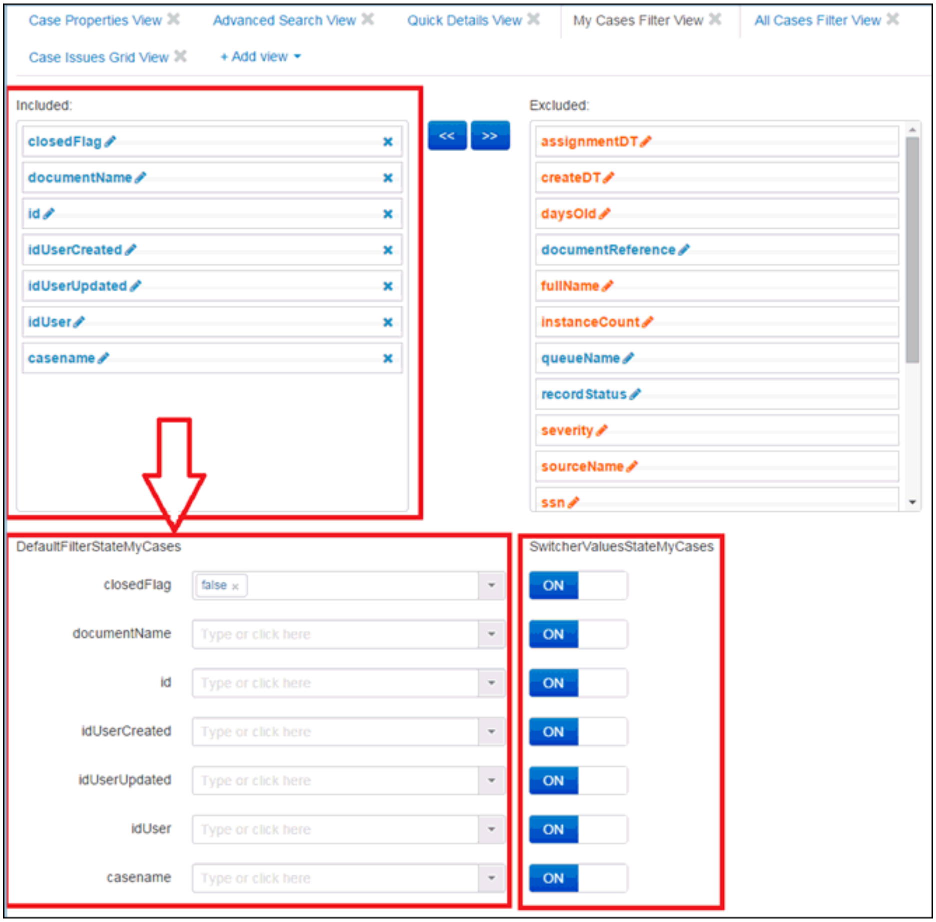
You must also create the same options in the All Cases tab.

When the options are created, they will appear in the list of options, as shown in the following image:



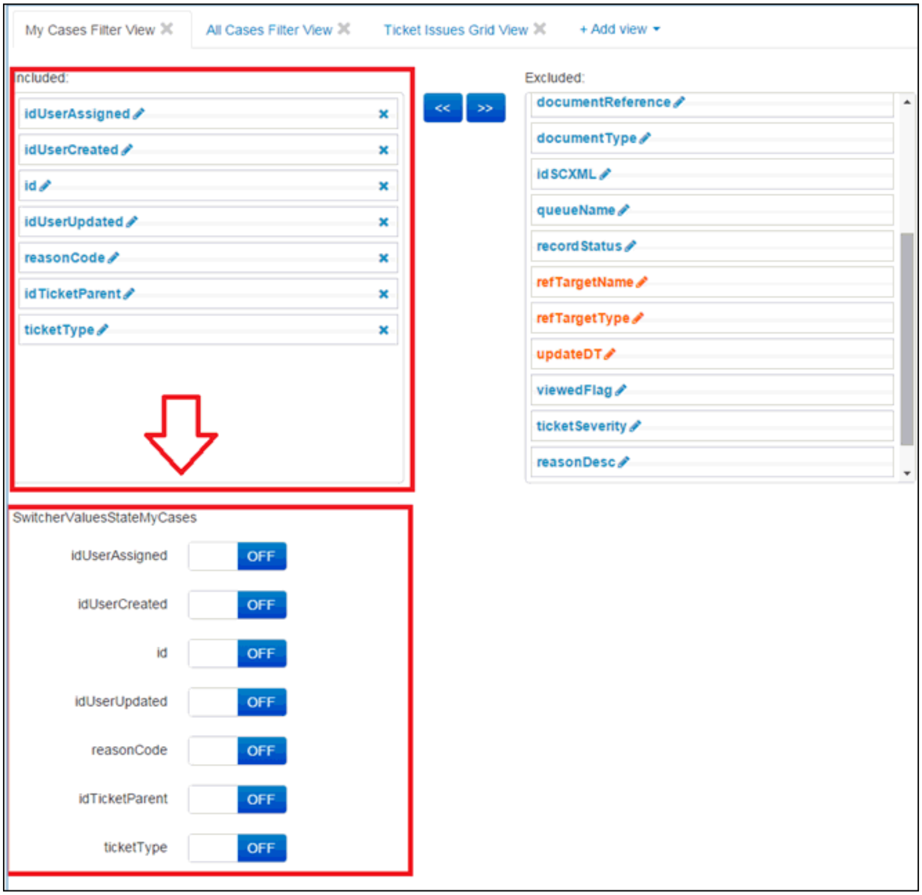
Title	Name	Description	Type	Default Value	Path Type	Path Name
Record Name	tableRecordName	Name for single table record	String	Record	table	
Info Tab Indicator	isInfoTab	Indicates whether a table is an information kind of tab	Boolean	false	table	
Is Logged	IsLogged	Log events from this table	Boolean	true	table	
DefaultFilterStateMyCases	DefaultFilterStateMyCases	DefaultFilterStateMyCases	String		view	myCasesFilterView
DefaultFilterStateAllCases	DefaultFilterStateAllCases	DefaultFilterStateAllCases	String		view	allCasesFilterView
SwitcherValuesStateAllCases	SwitcherValuesStateAllCases	adds possibility using of multiselect switchers for configuring of filtering items on All Cases	String		view	allCasesFilterView
SwitcherValuesStateMyCases	SwitcherValuesStateMyCases	adds possibility using of multiselect switchers for configuring of filtering items on My cases	String		view	myCasesFilterView

After the options have been added, switch the WF Cases or WF Tickets to either *ON* or *OFF* for each multiselect drop-down list option. Columns that are in the Included section of the My cases or All cases filter views of the WF Cases table will automatically appear in the Default Filtering section along with the multiselect switches, as shown in the following image:



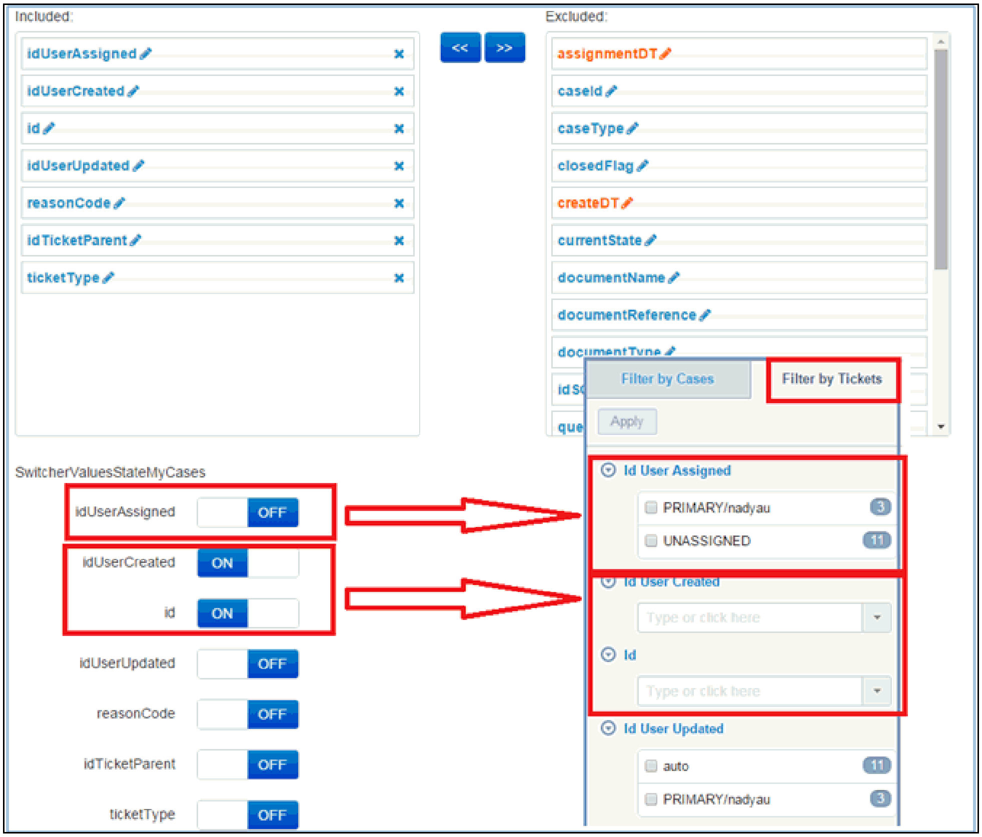
The Default setting of the multiselect switch is set to *OFF*, and the UI of the fields are displayed with check boxes. If a column is moved to the Excluded section, then it will automatically disappear from the Default Filtering section.

The Multiselect switches appear only for the WF Tickets table and display the appropriate views, as shown in the following image.



After the required values are set, click *Update* to apply the changes.

The Filtering Panel on the Issues Search page reflects the preconfigured settings on the appropriate view of the Administration page, as shown in the following image.



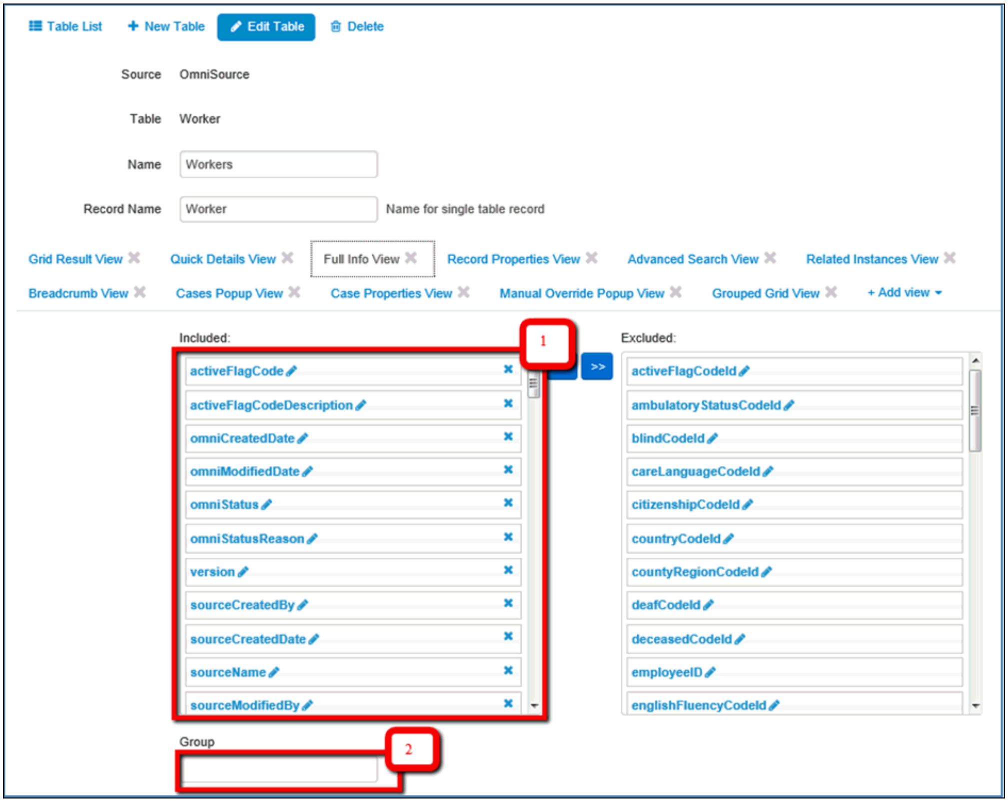
Override Matching Page

The Administration panel is available for users with the System Administrator role.

Instance Details Panel

To configure the Instance Details panel, click the Tables tab and select an Instance table (for example, Provider, Worker, and so on).

The table consists of many views. Click *Full Info View*, as shown in the following image.



To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

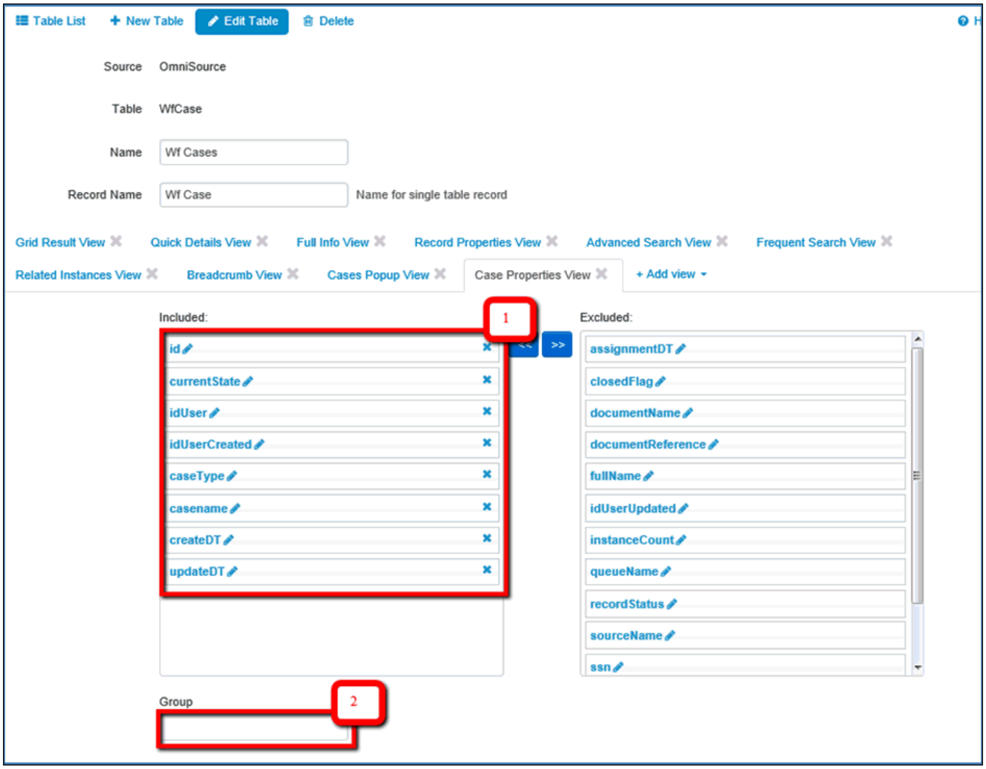
Click the *X* icon if you wish to exclude a column from the view (1).

If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

Case Properties Panel

You can configure the Case Properties panel in the Override Matching page. The WF Cases table can be found in the list of tables, and the view that needs to be configured is the Case Properties View.

Note: Configuring the Case Properties View affects all Remediation case pages, including: Override matching, manual cleansing, and General Issue cases.



To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view (1).

If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

Note: For this view, the names of groups will not be displayed. A horizontal line will appear instead.

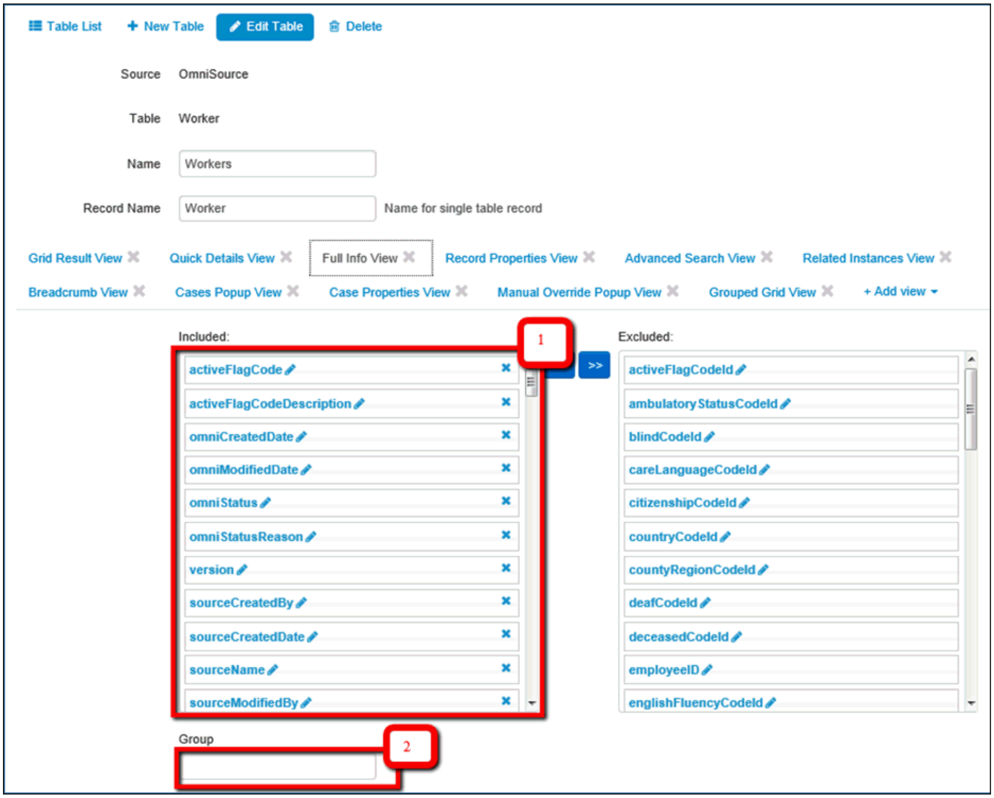
Manual Cleansing Page

The Administration panel is available for users with the System Administrator role.

Workspace Panel

To configure the Workspace panel, click the Tables tab and select an Instance table (for example, Provider or Worker).

The table consists of many views. Click *Full Info View*, as shown in the following image.



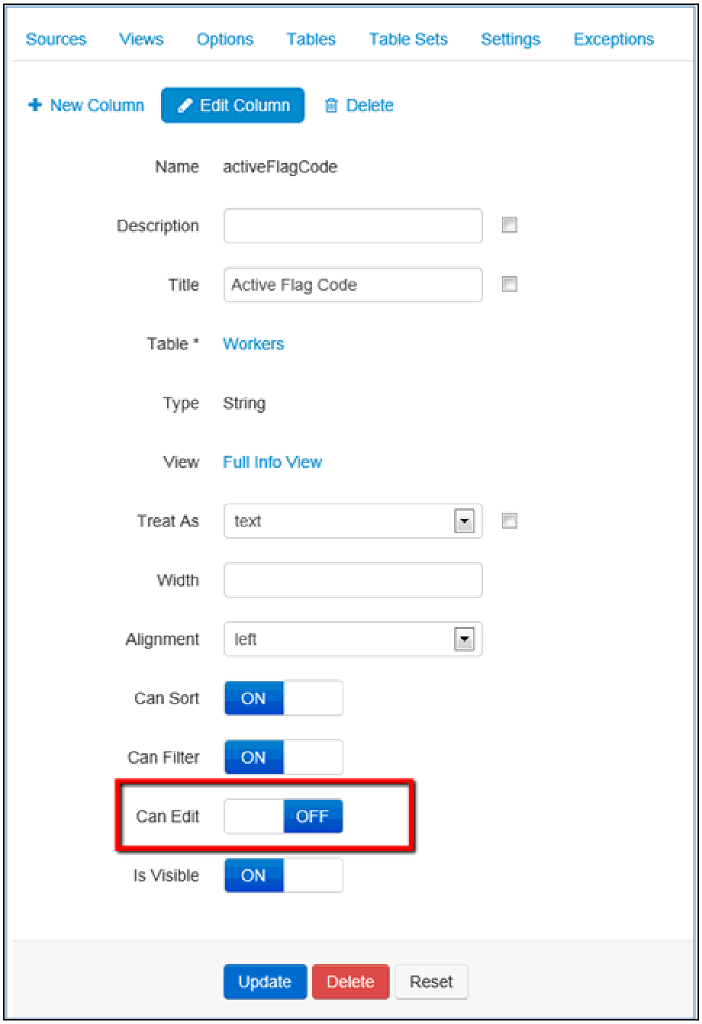
To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view (1).

If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

Ability to Allow/Prohibit Editing for Fields

To configure the ability to edit fields in the workspace panel, edit the nested columns (for example, display name, sortable, or filterable). This can be done by clicking the pencil (edit) icon for the corresponding columns in the Full Info View of the selected table and updating its parameters accordingly.

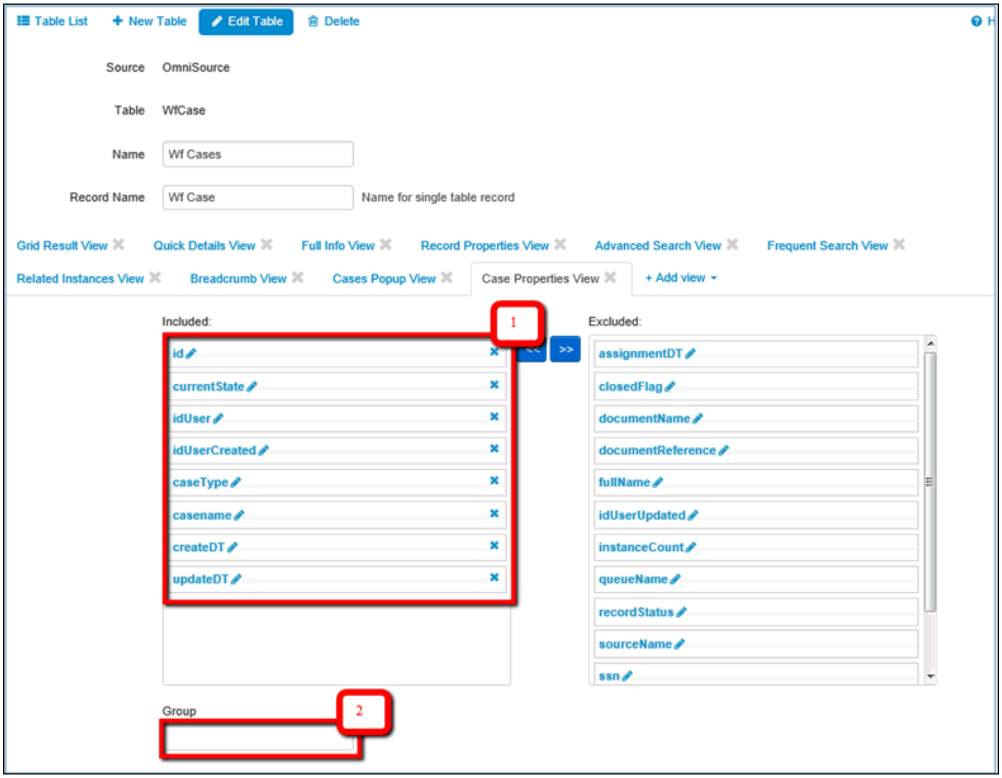


If a field needs to be disabled for editing, select the *OFF* option. Otherwise, select ON if there are no changes.

Case Properties Panel

You can configure the Case Properties panel in the Manual Cleansing page. The WF Cases table can be found in the list of tables, and the view that needs to be configured is the Case Properties View.

Note: Configuring this view affects all Remediation case pages, including: Override matching, manual cleansing, and General Issue cases.



To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view (1).

If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

Note: For this view, the names of groups will not be displayed. A horizontal line will appear instead.

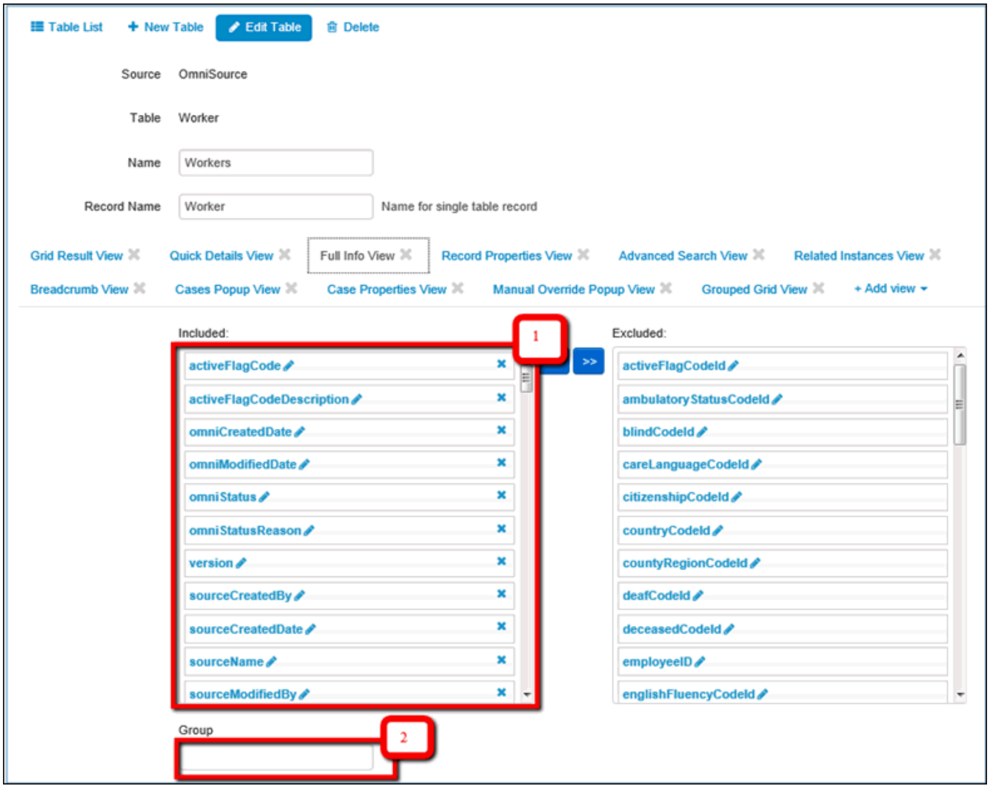
General Issue Page

The Administration panel is available for users with the System Administrator role.

Workspace Panel

To configure the Workspace panel for the General Issue of the Instance record, click the Tables tab and select an Instance table (for example, Provider or Worker).

The table consists of many views. Click *Full Info View*, as shown in the following image.



To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view (1).

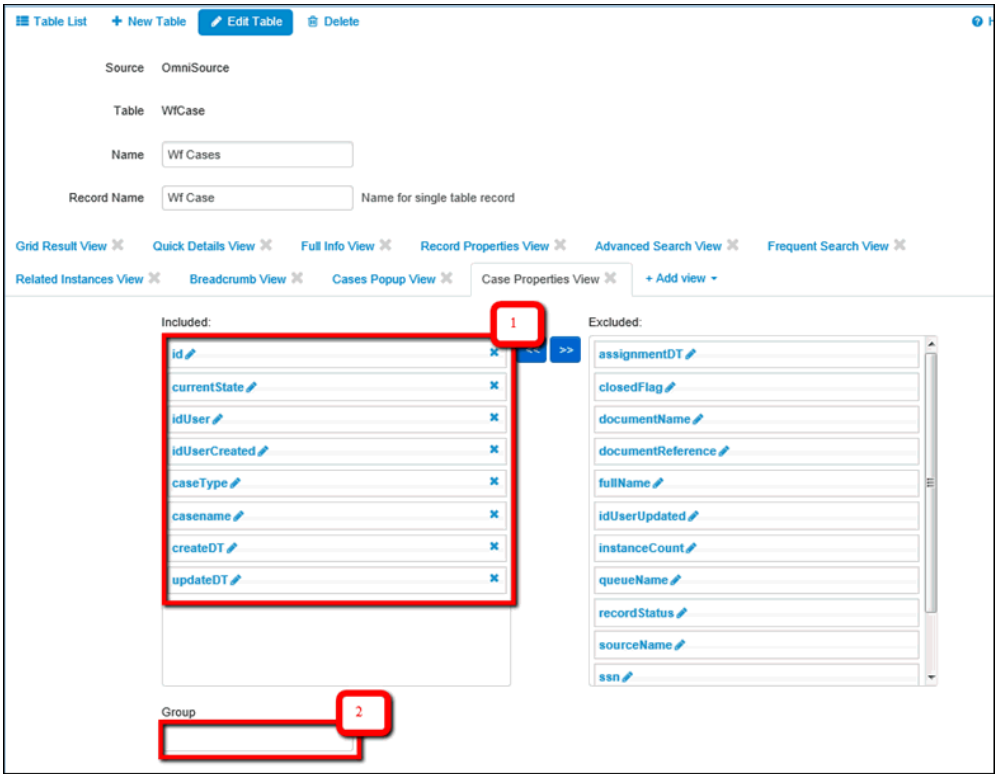
If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

Note: When the Workspace panel of the General Issue page for the Golden record needs to be configured, follow the same steps mentioned above. However, the Master table must be edited (for example, Provider Masters or Patient Masters).

Case Properties Panel

You can also configure the Case Properties panel in the General Issue page. The WF Cases table can be found in the list of tables, and the view that needs to be configured is the Case Properties View.

Note: Configuring this view affects all Remediation case pages, including: Override matching, manual cleansing, and General Issue cases.



To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

Click the *X* icon if you wish to exclude a column from the view (1).

If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

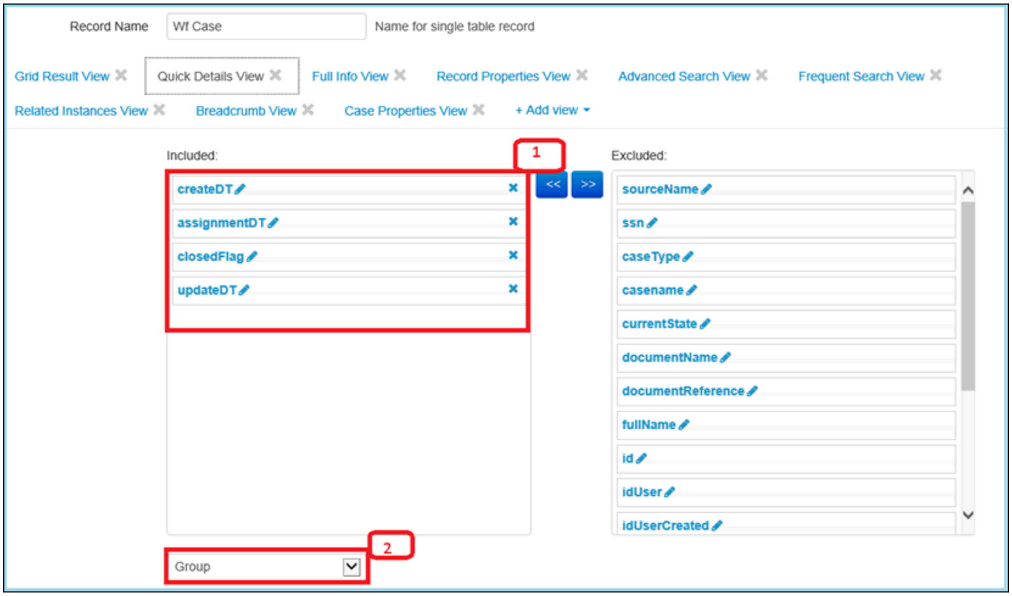
Note: For this view, the names of groups will not be displayed. A horizontal line will appear instead.

Issues Pop Up

The Administration panel is available for users with the System Administrator role.

To configure the Issues pop up, click the Tables tab and select an Instance table (for example, Provider or Worker) from the WF Case list of tables.

The consists of many views. Click *Quick Details View*.



To rearrange the columns in the view, drag the required column from the Excluded section to the Included section, especially if you wish to include the column in the view.

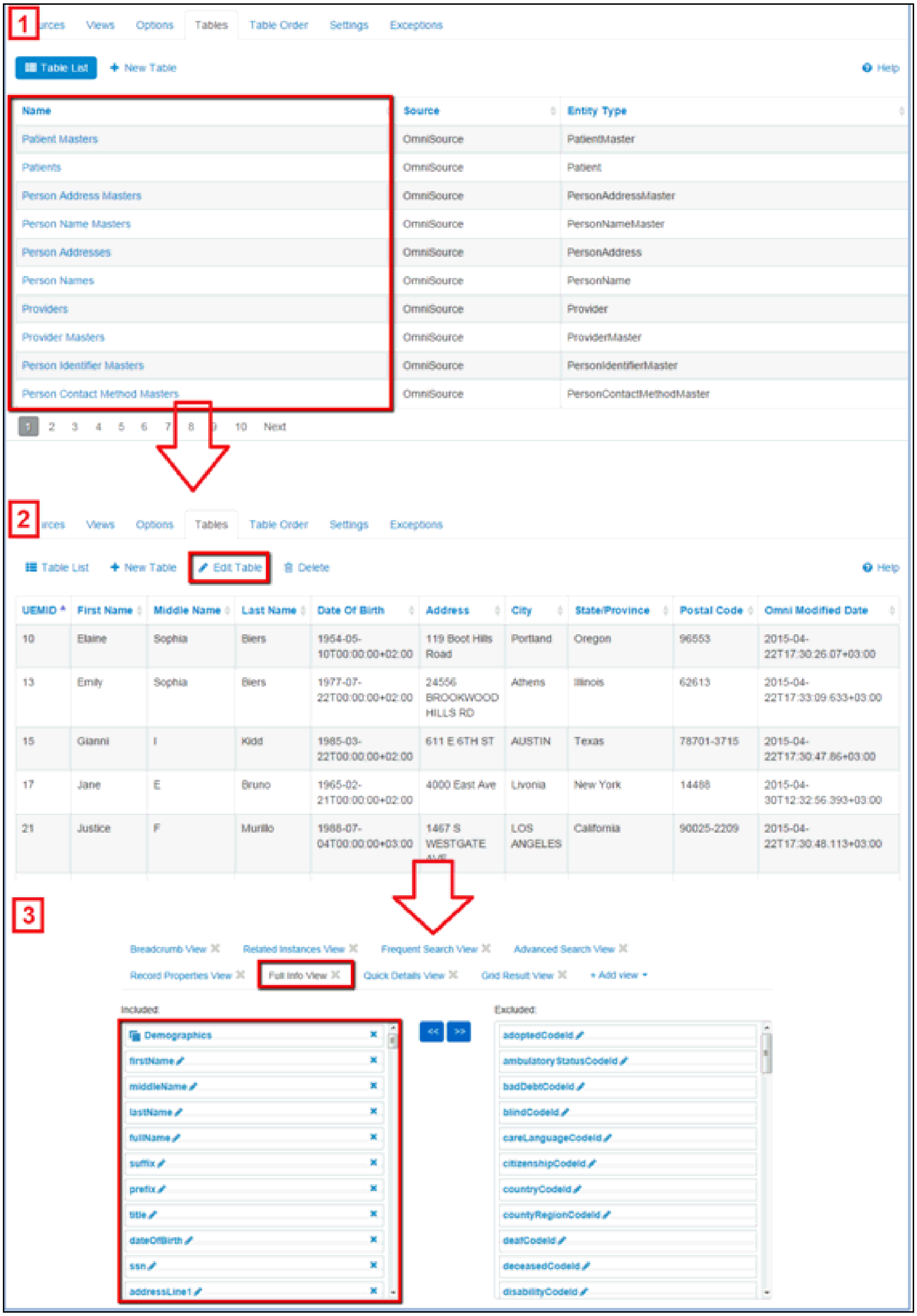
Click the *X* icon if you wish to exclude a column from the view (1).

If you wish to separate the columns into Groups, add the appropriate group to the Included section (2).

Domain Grid Configuration

To configure sections and their attributes, include or exclude the necessary columns in the Full Info View of the appropriate table.

The following image shows the steps required to configure the domain grid.

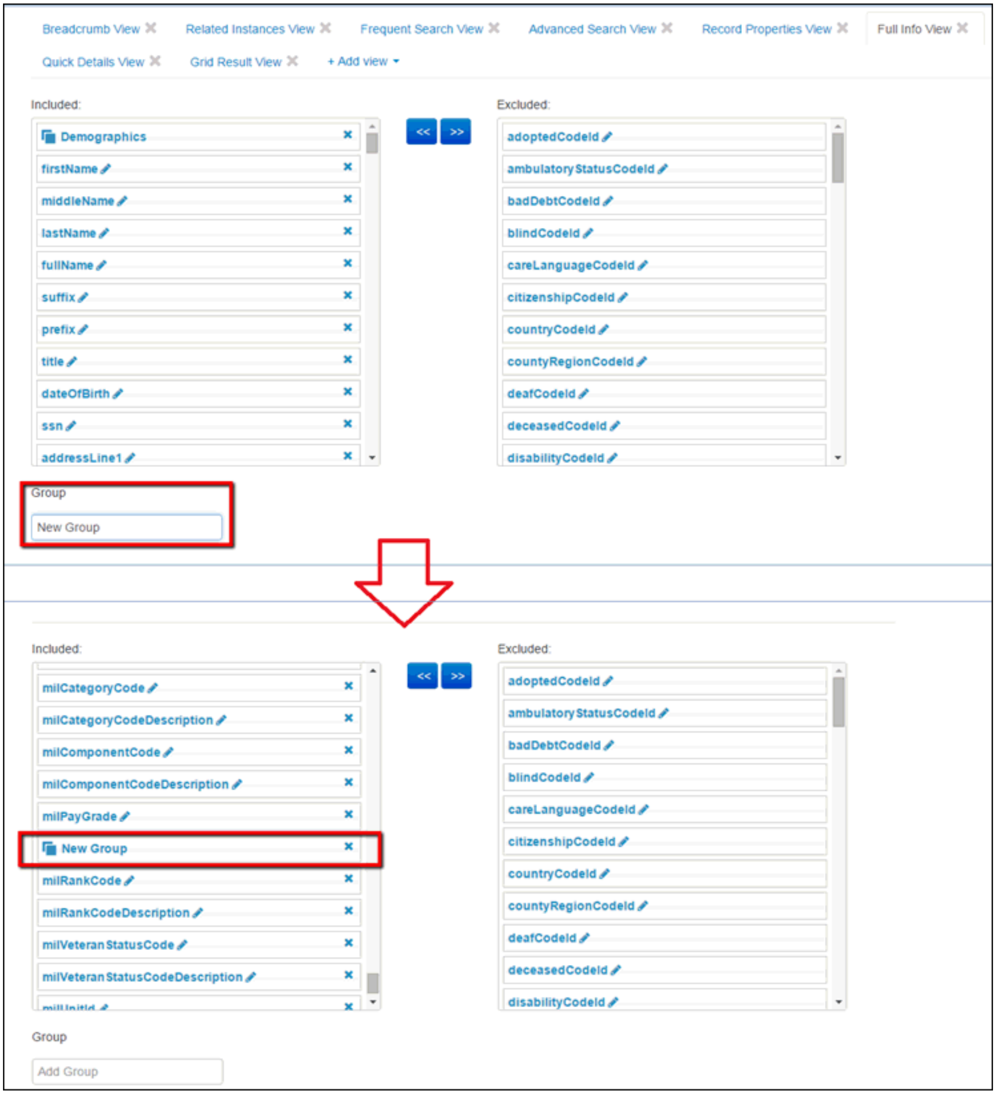


1. Find the required table in the list of tables.

2. Edit the table.
3. Click *Full Info View*

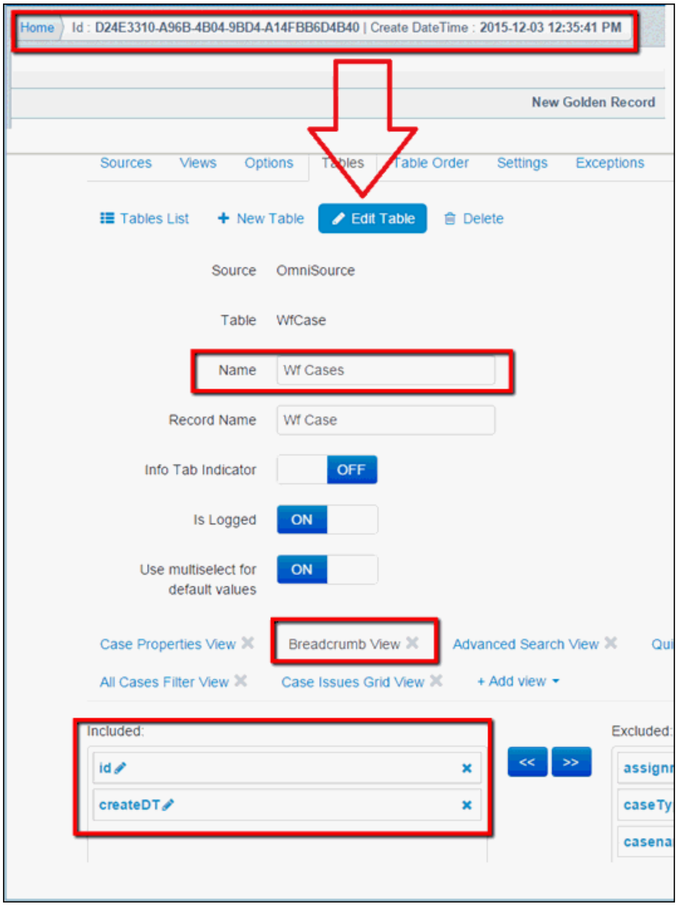
To divide the fields on the page into sections, edit the Group field and press *Enter* (Full Info view). The header of the section will be added into the list of included columns.

Drag the header and drop it above the columns that are required for the section.



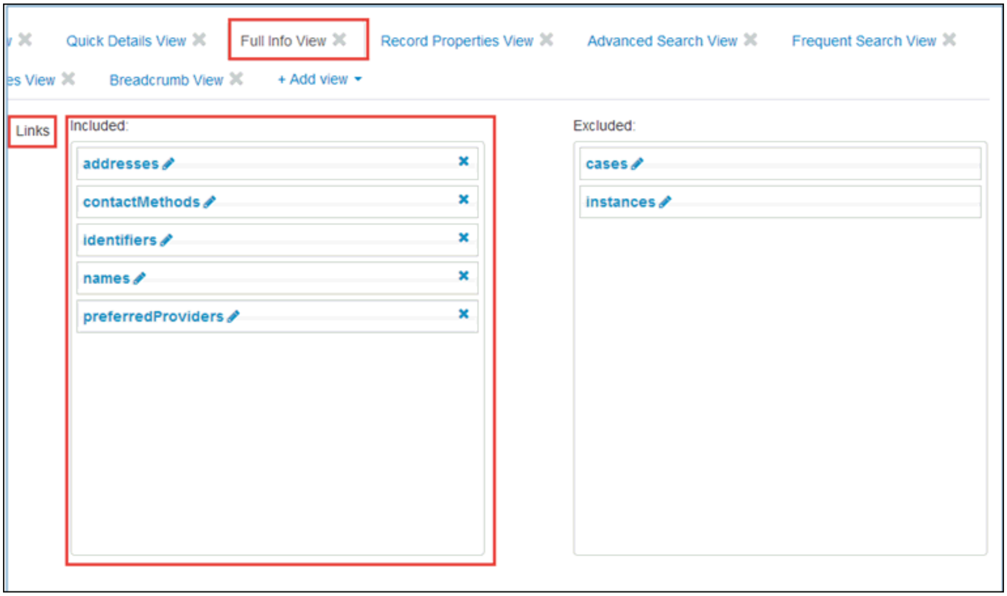
Breadcrumbs Configuration

Breadcrumbs are configured through the Breadcrumb View in the WF Case table, as shown in the following image.



Sub-domains Configuration

To configure subdomains in the Add New Document page, edit the Document table and include or exclude the required links in the Full Info View, as shown in the following image.



Appendix A

Enhanced Access Security: Column-Based and Row-Based

This section describes how to configure column-based access security and row-based access security in the Omni Governance Console (OGC).

In this appendix:

- Overview
- Configuring Enhanced Security
- Enabling Enhanced Security
- Configuring Column-based Security
- Configuring Row-Based Access Security
- Supporting Enhanced Security Using WSO2 Identity Server
- Merging and Reorganizing Column Sets

Overview

As of Omni-Gen version 3.6, enhanced security for the 360 Viewer and Remediation applications in the Omni Governance Console (OGC) is available in two forms (Column-based access security and Row-based access security).

- Column-based access security provides the ability to restrict access to any column in any table to any user.

  For example, all data stewards would see six columns of data in a 360 view of a subject, while finance managers would also see a seventh, restricted access data column, such as Revenues Received.

- Row (or column criteria)-based access security provides the ability to restrict the display of rows in any table where the value of the content in any column is a configurable value.

  For example, the rows of customer master records displayed for regional managers can be restricted to the rows where the Region column contains a value that is specific to the region of the manager.

By default, Column-based access security and Row-based access security are disabled and can be enabled independently as required.

Configuring Enhanced Security

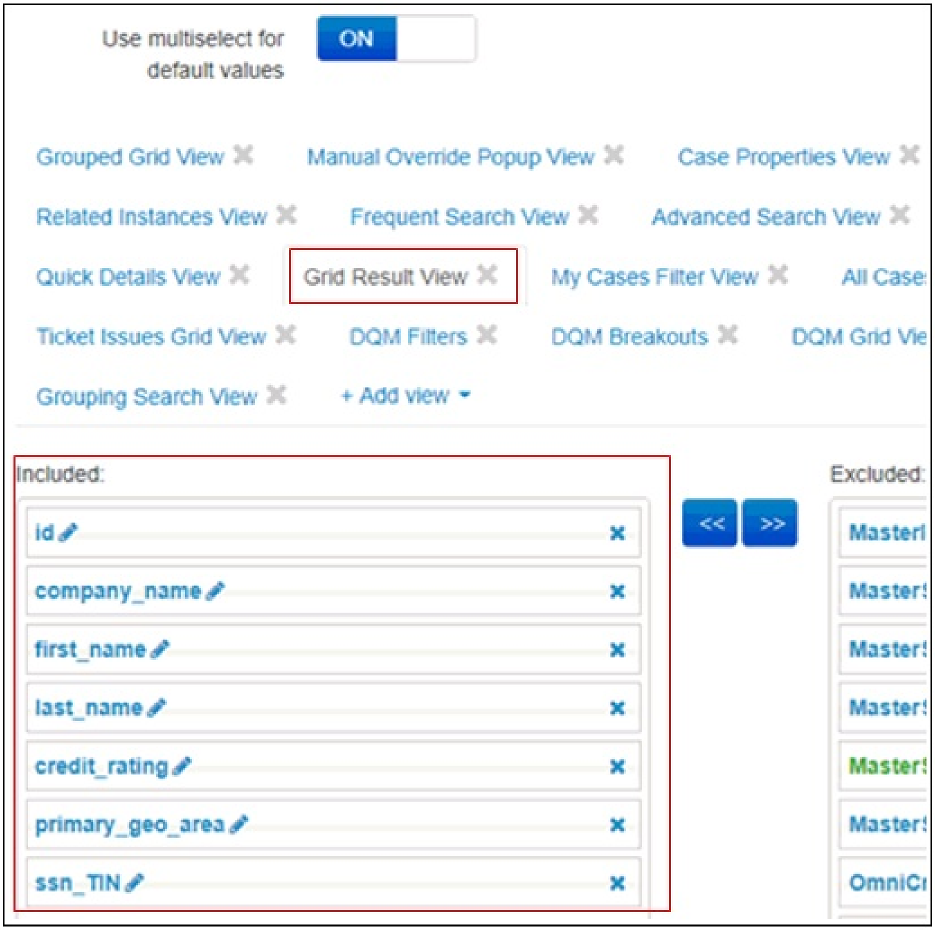
This section provides an example that describes how to configure enhanced security using the Administration console.

After deploying a deployment bundle that was created using Omni Designer, log in to the Omni Governance Console (OGC) and click the *Administration* tab on the OGC menu bar. The Administration console opens. Click the *Tables* tab, which is used to configure metadata (MData) views in an *MData.xml* file.

The MData is used to describe the OGC home page of a typical Subject master. From the Administration console, you can access the existing MData by clicking *Table*, selecting *SupplierMaster*, *Edit Table*, and then clicking *Grid Result View*. In this example, the following columns are included by default:

- id
- company_name
- first_name
- last_name
- credit_rating
- primary_geo_area

❑ ssn_TIN



The following is a list of users who have WSO2 roles of *Internal/domain.SupplierMaster* and *Internal/domain.Supplier*, which provides them access to the Supplier domain:

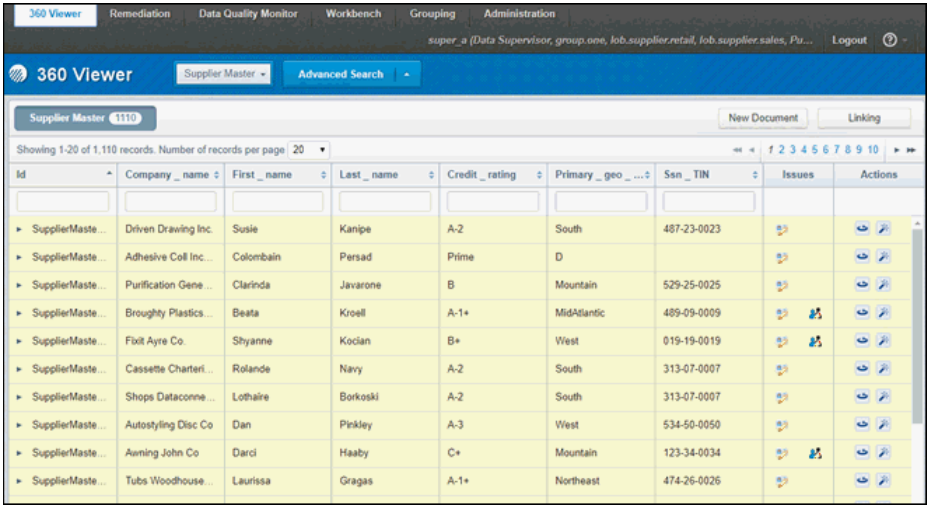
❑ PRIMARY/Super_a

❑ PRIMARY/Super_b

❑ PRIMARY/ds_a

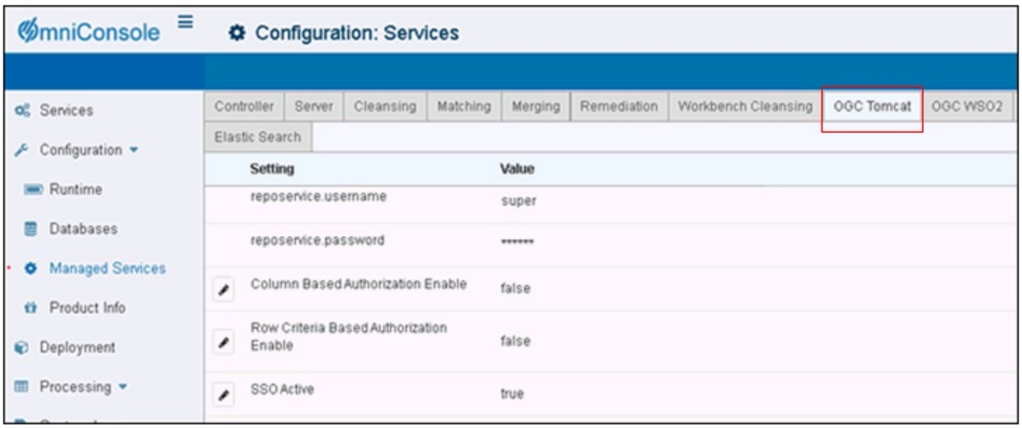
❑ PRIMARY/ds_b

Upon logging in to the Omni Governance Console (OGC), the following screen is displayed, which shows the seven columns defined when enhanced security is disabled.



Enabling Enhanced Security

By default, column-based access security and row-based access security are disabled. However, each security type can be enabled independently. The corresponding settings are available in the Omni Console (Configuration, Managed Services) under the OGC Tomcat tab, as shown in the following image.



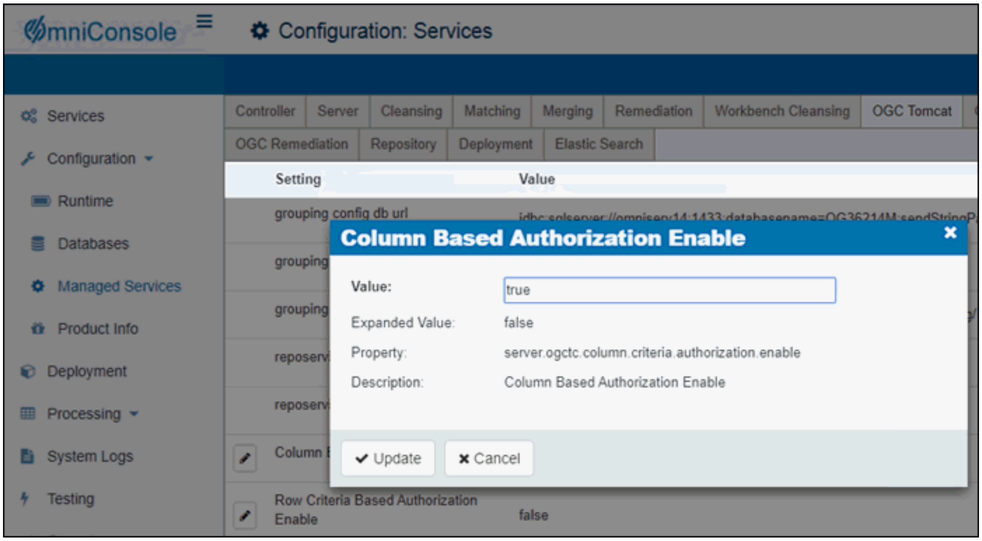
The settings are listed and labeled as follows:

- Column Based Authorization Enable

❑ Row Criteria Based Authorization Enable

To enable individual or both enhanced security settings:

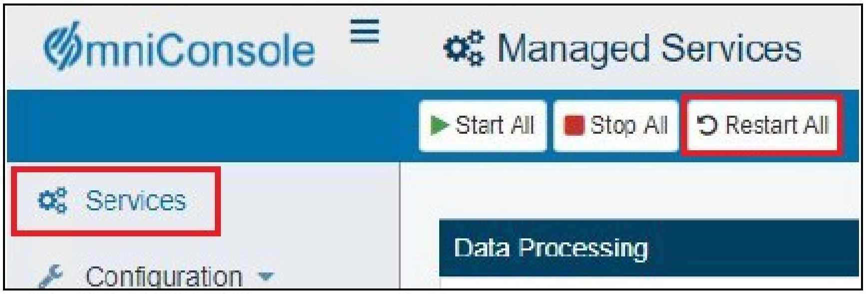
1. Click the corresponding pencil icon to the left of the security setting.
2. Change the value from *false* to *true*.
3. Click *Update*, as shown in the following image.



After the setting has been updated (enabled), a message indicating a successful update is displayed in a green banner, as shown in the following image.

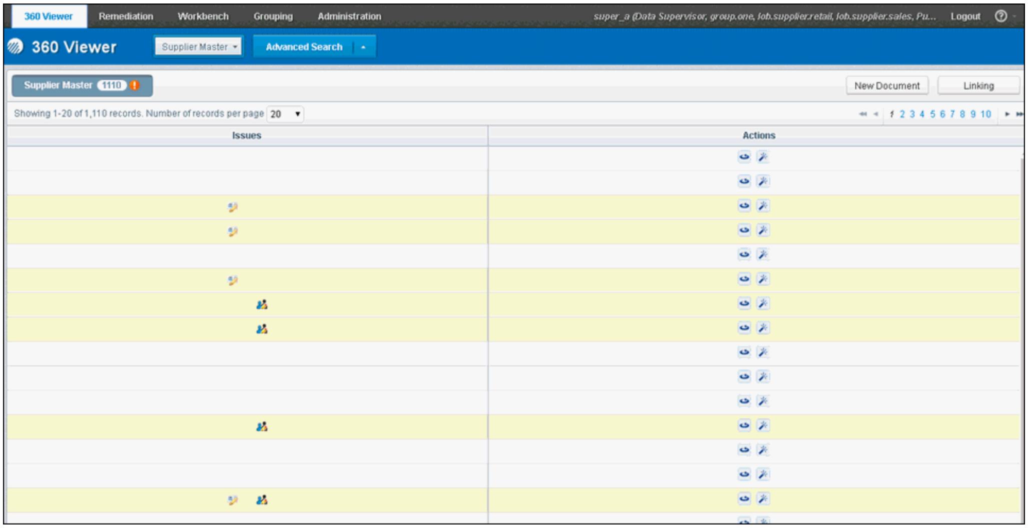
4. Close the green banner by clicking the X icon, which is located on the right-hand side of the banner.
5. Click *Services* in the left pane of the Omni Console.

The Managed Services pane opens, as shown in the following image.



6. click *Restart All*
7. After restarting, log on to the Omni Governance Console (OGC), which now has column or row-based security enabled, depending on the settings you specified in the Omni Console.

   The following image shows the 360 Viewer with columns not enabled for access and not displayed. To display columns, you must enable them per Table, View, and user with the Enhanced Security management tool.

   Note: Only the columns or rows with access allowed are displayed. Issues and actions are not columns. Rather they are navigation aids.

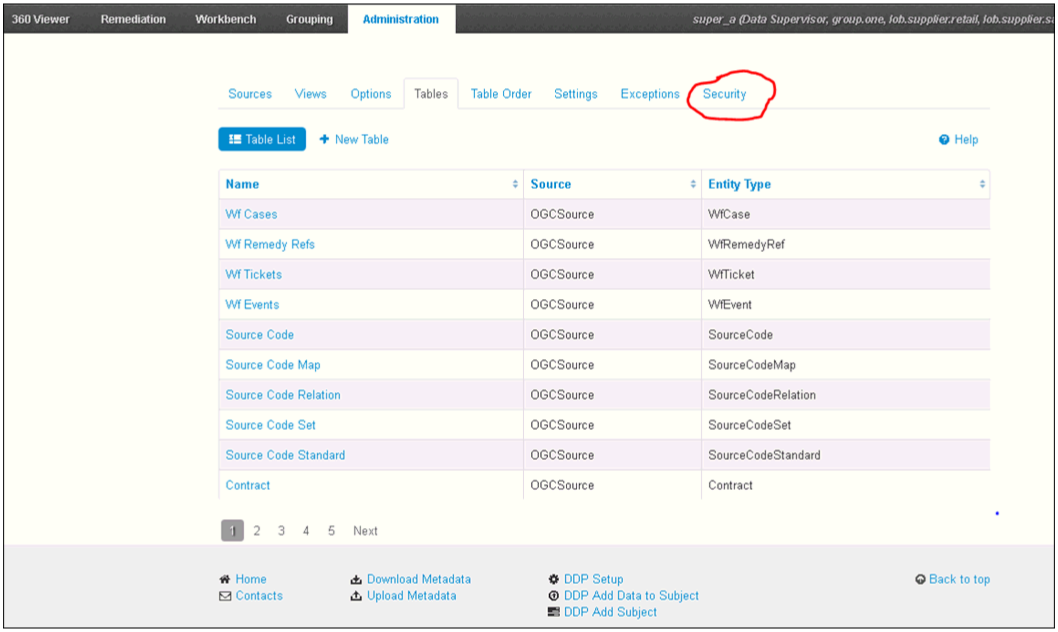
   The following list describes a sample configuration using the four users that were mentioned previously.

   - All four users should see five of the seven columns.

- Only user *Super_a* is cleared to access the two sensitive columns (*credit_rating* and *ssn_TIN*).
- User *Super_b* can see the five columns and the *ssn_TIN* column.

Configuring Column-based Security

The Security tab appears in the Administration console when either or both switches are enabled, as shown in the following image.



Click the Security tab to open the Enhanced Security management tool. This tool is used to configure access to any column or row in all OGC tables (screens) for specific users.

Configuring Column Access

The Enhanced Security management tool consists of the following sections:

- domains list (located on the left pane)
- column sets editor (located on the right pane)

From the domains list, you can select a specific domain to access and configure its data.

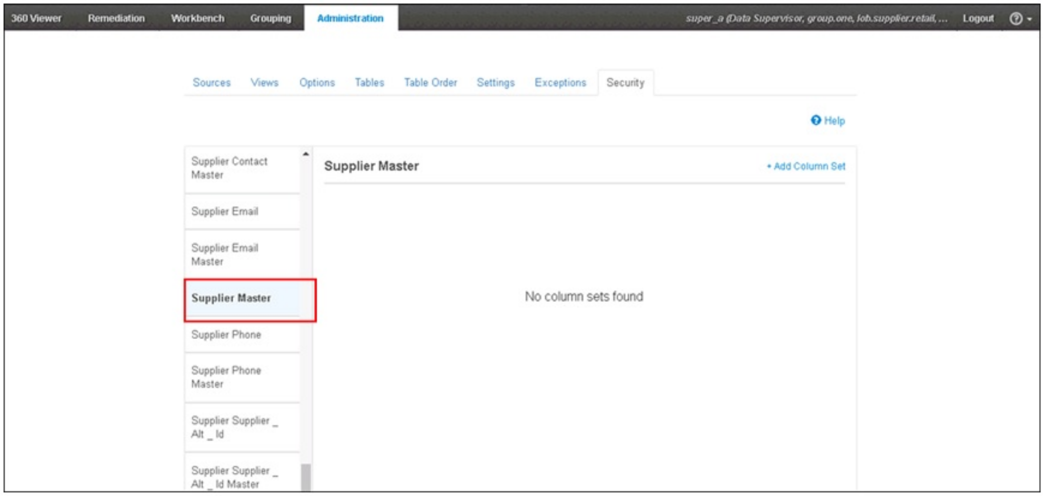
Using the column sets editor, the security administrator can create a set of columns that will be visible to a specific user.

Procedure: How to Add a New Column Set

If there are no column sets created for a specific domain, the *No column sets found* message appears.

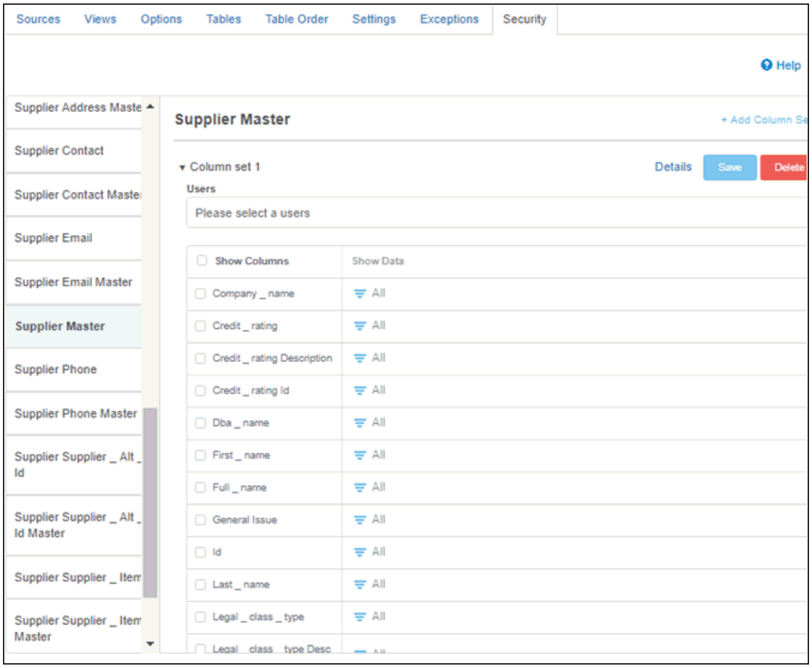
To add a new column set:

1. From the domains list in the left pane, scroll down and click the domain (subject or sub collection) to which you want to grant column access (for example, Supplier Master), as shown in the following image.



2. Click *Add Column Set*.

A new column set appears with the list of available columns for the selected domain, as shown in the following image.



A new column set consists of the following:

- Column selection list
- Row criteria selectors
- Save and Delete buttons

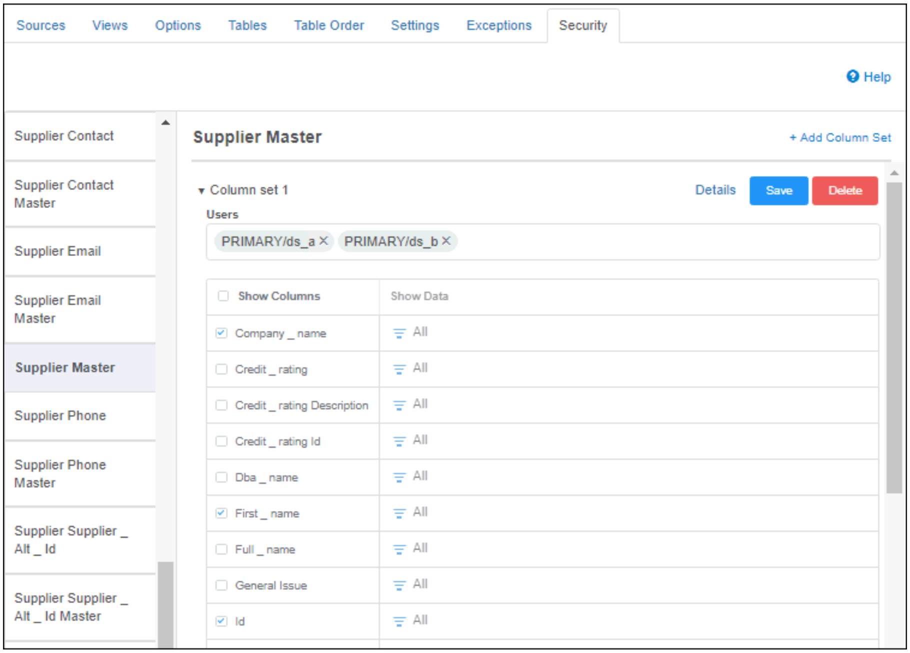
Note that the validation is active and notifies you that at least one user name and one column must be selected for the created column set.

3. Select the check box for each column you want to allow access.
4. Click the Users drop-down list to view a list of available users.
5. Select the user(s) that you want to grant access to the column set of selected columns.

   For example, to configure the first column set, select the check box for the five non-sensitive columns, and enter the two most restricted view user IDs (for example, *ds_a* and *ds_b*).

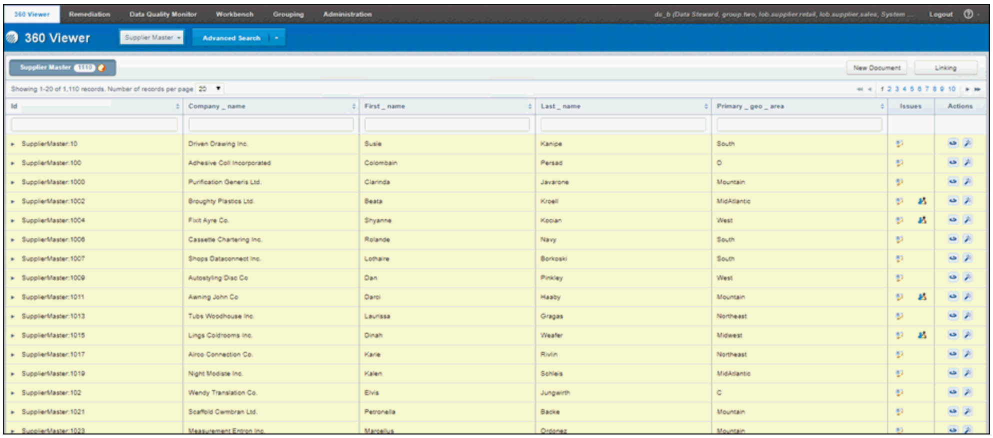
6. Click *Save*.

7. Expand the desired column set name (for example, *Column set 1*) to view the users and columns within the column set, as shown in the following image.

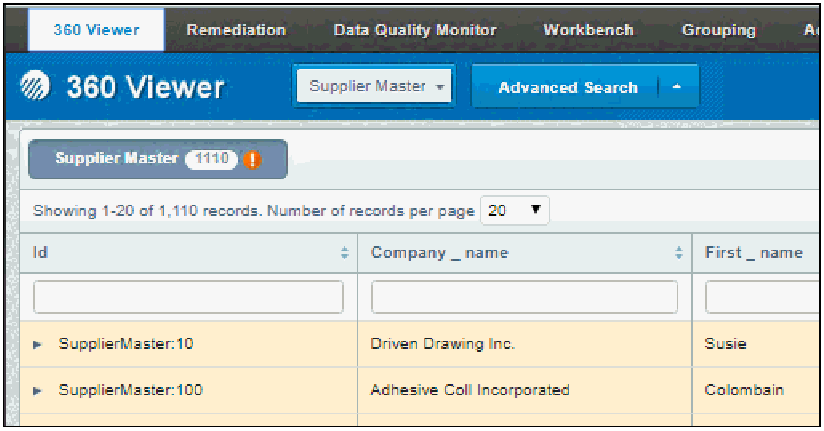


8. Confirm your changes to the users or columns, and then click *Save*.

9. Log on to OGC as one of the newly configured users (for example, *ds_a* or *ds_b*) and verify that the 360 Viewer has allowed the configured access results (for example, the five columns that were just specified), as shown in the following image.



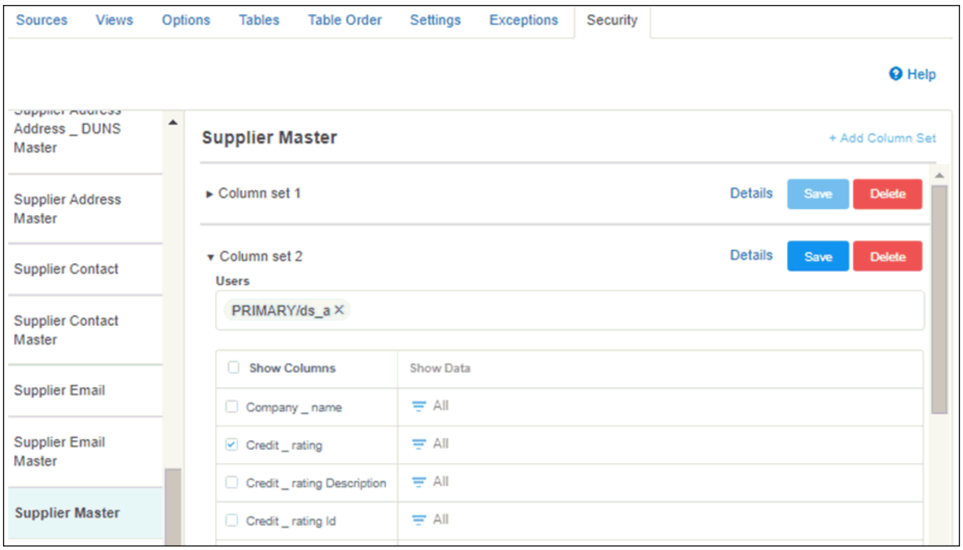
Note the orange exclamation icon, which appears next to the user ID, as shown in the following image.



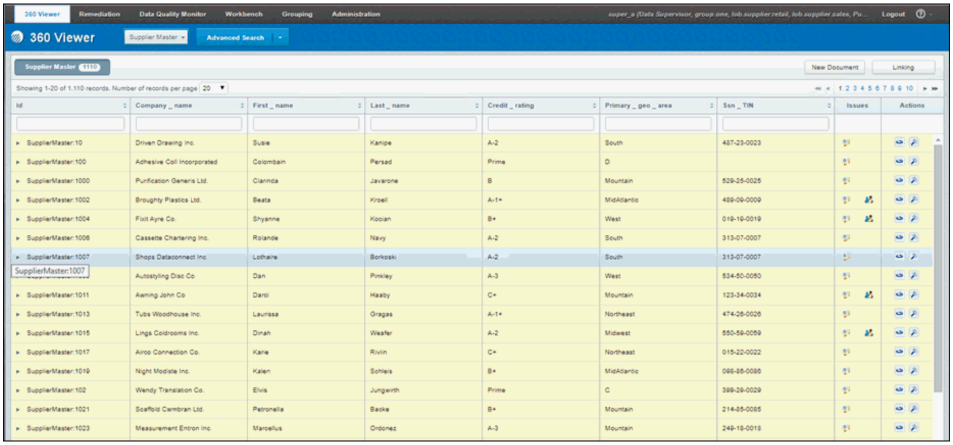
This icon indicates that data may be restricted due to security purposes.

10. Enter two more column sets allowing the appropriate user access to the data.

    For example, add *Column set 2* to the *Supplier Master* domain, and allow the *PRIMARY/super_a* user access to seven columns, the same five configured in *Column set 1*, in addition to *credit_rating* and *ssn_TIN*, as shown in the following image.

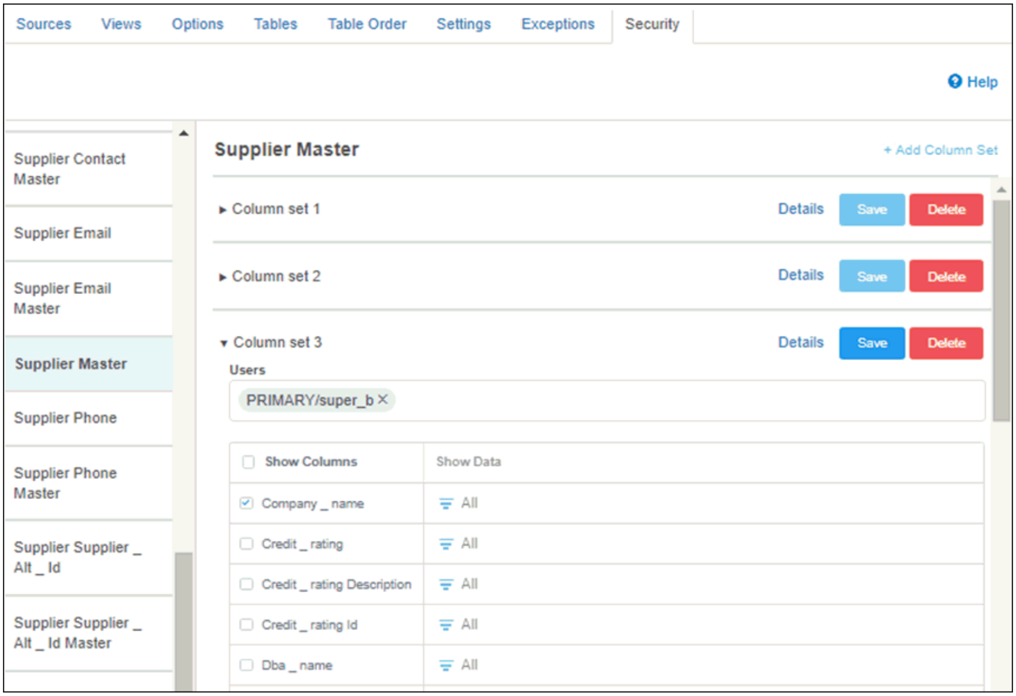


11. Log on to OGC as the *PRIMARY/super_a* user and verify access to the seven configured columns, as shown in the following image.

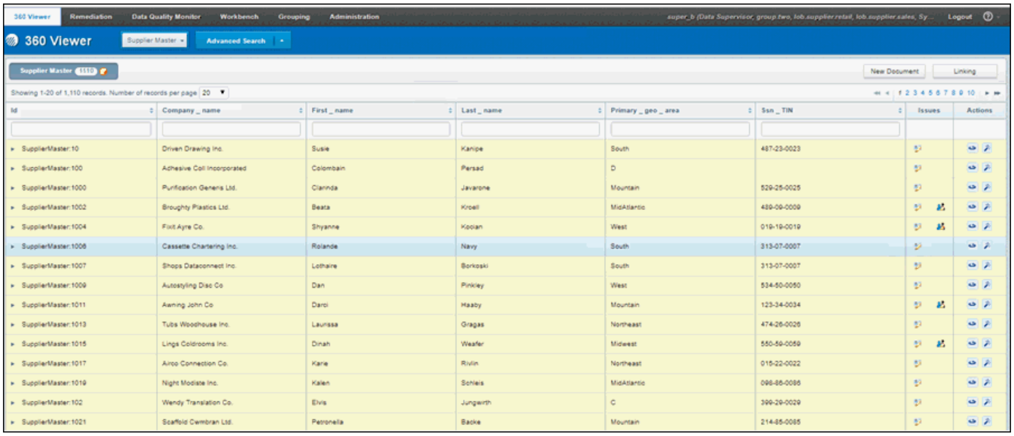


12. Add *Column set 3* to the *Supplier Master* domain, as shown in the following image.

13. Allow the *PRIMARY/super_b* user access to *ssn_TIN* in addition to the five columns granted in the *Supplier Master* domain for *Column set 1*, as shown in the following image.



14. Log on to OGC as the *super_b* user to verify that the sixth column, *ssn_TIN*, is accessible, as shown in the following image.



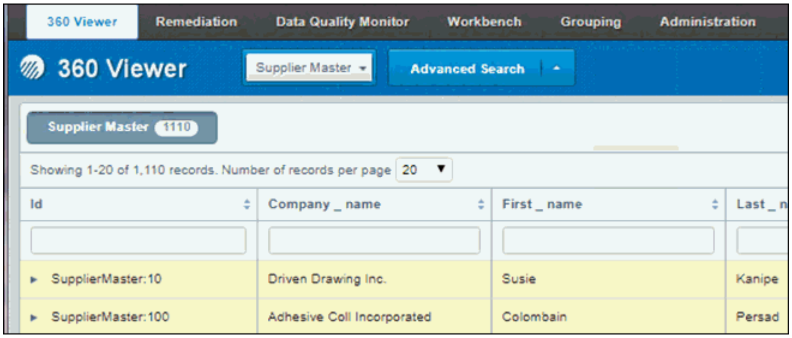
Note that a single column set can be configured for multiple users.

The selection of specific values is not required (for example, all values for a specific column are selected and displayed). However, if it is necessary to restrict or allow visibility of specific values for specific users, then the individual configurations must be configured via row-based access security.

Configuring Row-Based Access Security

Row-based access security allows you to see only the rows whose value in a specified column meets a configured value(s). For example, if user *ds_b* wants to display suppliers whose geographical area equals South or West.

In this example, all views regardless of which columns are allowed access for a specific user, a total of 1,110 records in the Supplier Master domain have been reported, as shown in the following image.



Before proceeding with using the Show Data column in the Enhanced Security management tool to configure row-based access security, the *Row Criteria Based Authorization Enable* setting must be set to *true* in the Omni Console. To enable this setting from the Omni Console, click *Configuration*, select *Managed Services*, click the *OGC Tomcat* tab, and then change the switch to *true*. When you have finished enabling this setting, click *Services* in the left pane, and then click *Restart All*.

Procedure: How to Configure Row-based Access Security

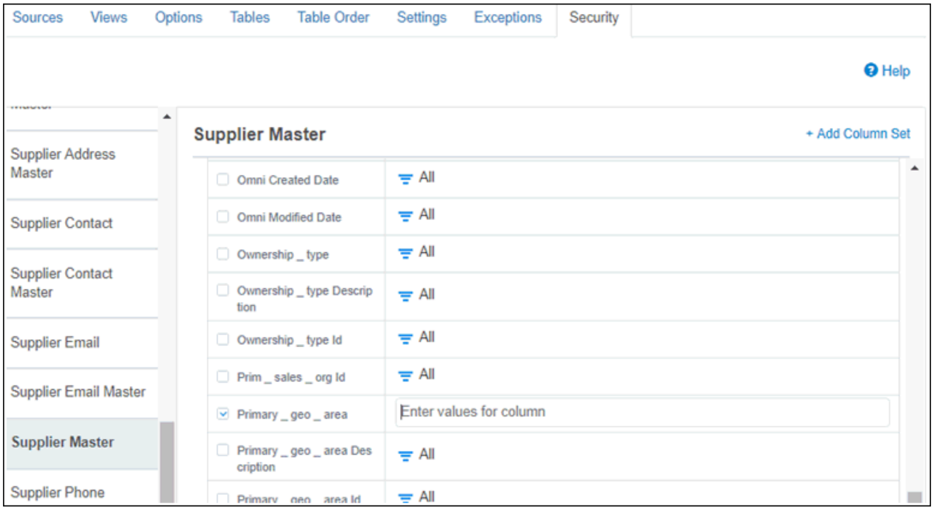
To configure row-based access security:

1. From the Security tab in the Administration section of the Omni Governance Console (OGC), select the desired domain (for example, Supplier Master).

   Note that in this example, there are three other Supplier Master Column sets.

2. Expand the desired Column set (for example, *Column set 2*).

3. Scroll down the column list until you find the set where you can enter values into the row (for example, *Primary_geo_area*) and expand the corresponding Show Data column, as shown in the following image.



4. Enter a value (for example, *West*) and press *Enter*.

   The resulting value is displayed like a filter. For example:

```
‘<column name> equals: <value1, value2…>'
```

5. Click *Save*.

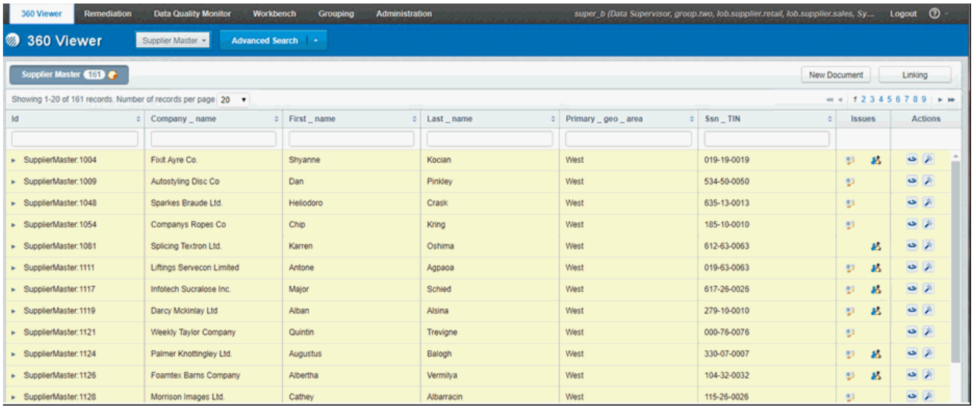
   Note that in an upcoming release, a drop-down list with available values for specific columns will be implemented.

   To delete a created or edited Column set, click the *Delete* button.

Procedure: How to Remove Individual Access Security Rules

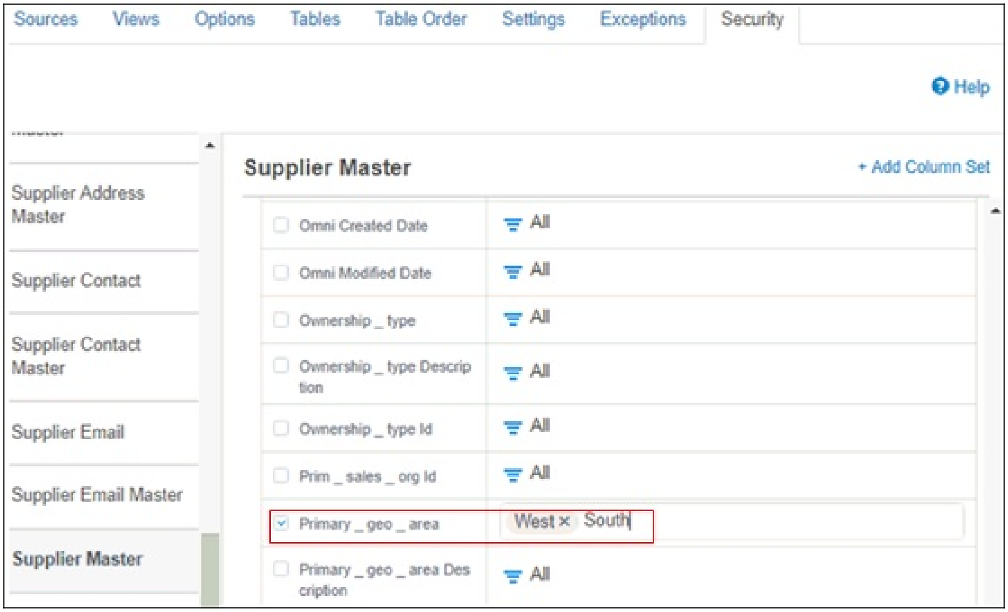
To remove individual access security rules:

Log on to the Omni Governance Console as *PRIMARY/super_b* to view the six columns configured to be displayed, but only for the rows where *Primary_geo_area=West*, as shown in the following image.

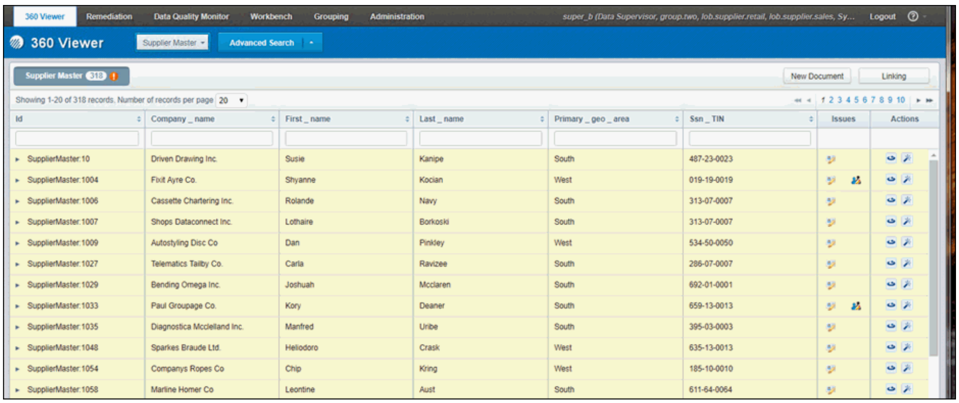


Note that in the Supplier Master Count display, 1,110 records (rows) are no longer accessible, but rather only 161, which meet the *Primary_geo_area=West* criteria.

Note also that you can include more than one criteria value in the Show Data column for any displayed column. The criteria values are automatically evaluated using the OR operand to determine the display of each row. For example, the following image shows the second value of *South* being entered for *Primary_geo_area*.



The resulting search criteria, West or South displays 318 Supplier Master rows, as shown in the following image.



Supporting Enhanced Security Using WSO2 Identity Server

After saving the settings, the appropriate roles are created and added to the corresponding users in the WSO2 Identity Server (WSO2 IS).

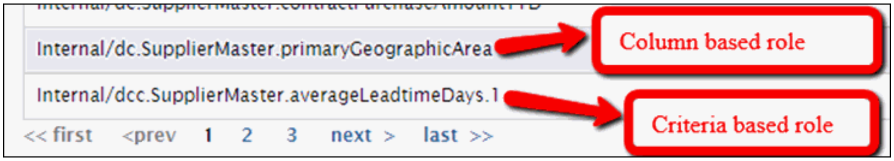
Roles that are defined for column security have the following naming convention:

```
Internal/dc.[domainName].[columnName]
```

Roles that are defined for criteria/row security have the following naming convention:

```
Internal/dcc.[domainName].[columnName].[criteriaValue]
```

The following image shows sample security roles in the WSO2 IS.



If required, you can create those roles manually in the WSO2 IS by following the naming conventions. The corresponding column set(s) will be created in the Administration console.

If a column set is no longer required, you can click the Delete button so that all related column set roles will be deleted from the corresponding users in the WSO2 IS.

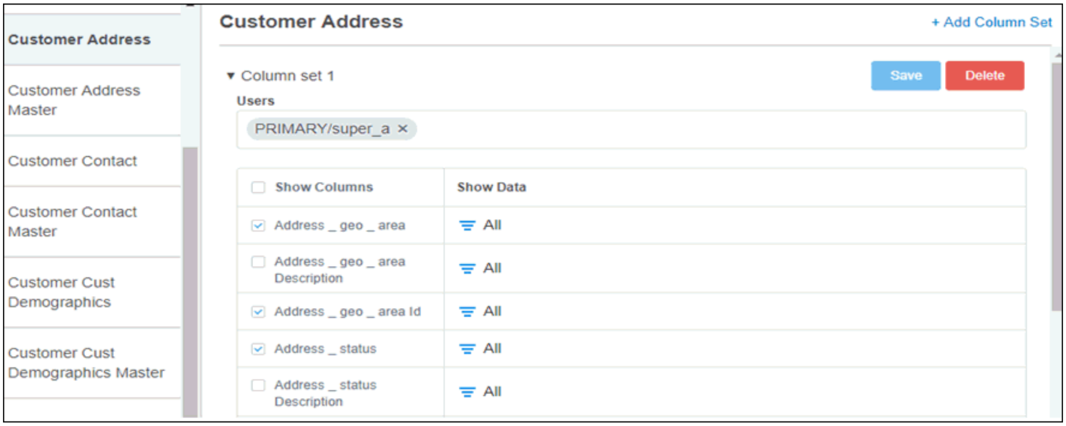
Note: Created roles will still exist in the WSO2 IS, but they will not affect the user interface because they are unassigned.

Merging and Reorganizing Column Sets

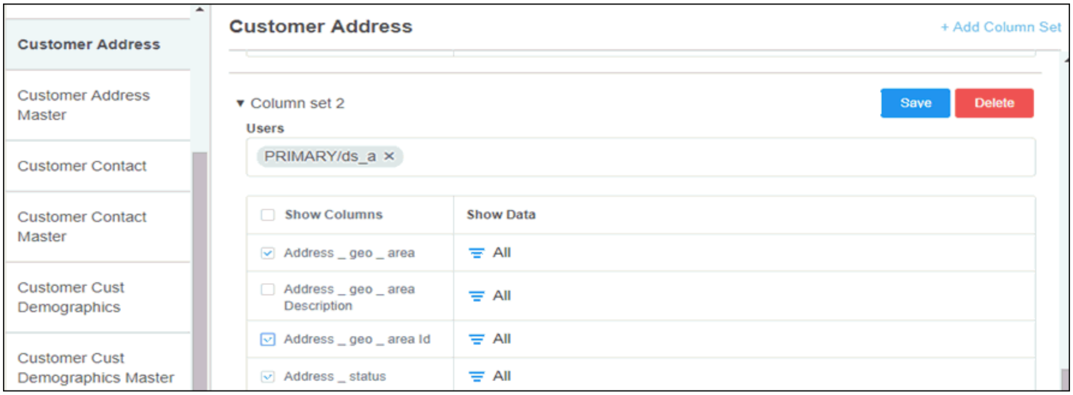
Created column sets can automatically be merged into one after refreshing the page, especially if the same columns and/or the same values were selected or entered for different columns sets.

Column sets can be reorganized if, for example, two column sets with the same visible columns were created for different users.

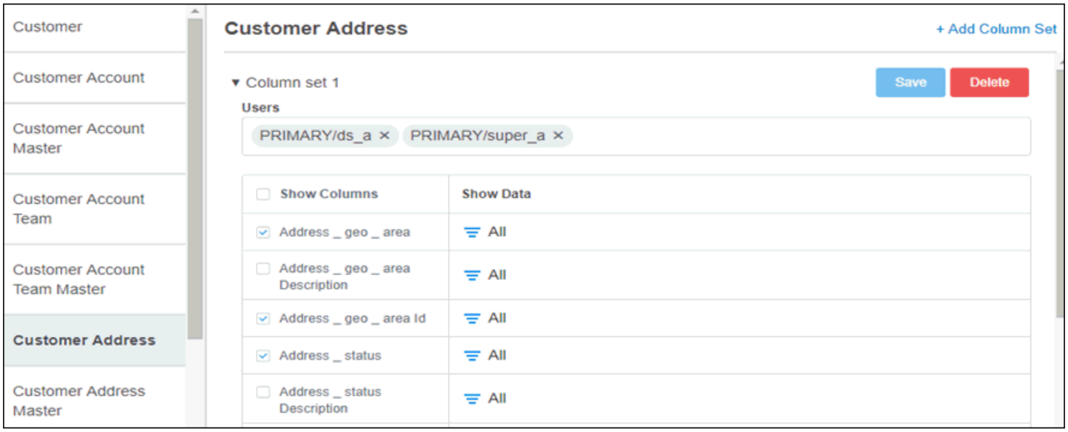
For example, the first column set below, shows the columns selected for the user *PRIMARY/ super_a*.



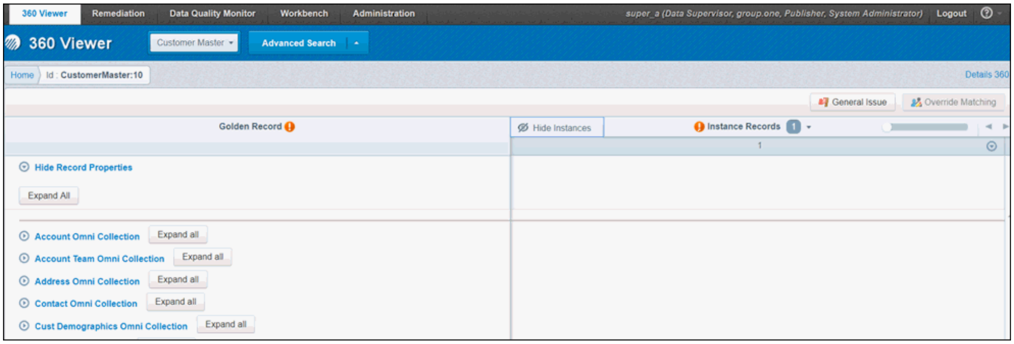
The following image shows the second column set, showing the same columns selected for the user *PRIMARY/ds_a*.



As a result, one column set will be displayed when both users and shared columns are selected, as shown in the following image.



Users are alerted if data access is restricted when an icon containing an exclamation mark in an orange circle is displayed. This notification is displayed on pages with limited access to data, as shown in the following image.



Note that two *data access is limited* notifications appear in the above image. The first notification on the left is for the records in the Golden Records frame (from the Supplier Master table). The second notification on the right is for the records in the Instances frame (from the Supplier Table).

Appendix B

Configuring Single Sign-On

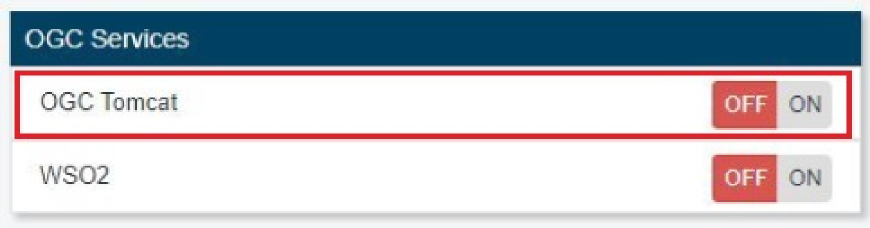
This section describes how to configure Single Sign-On (SSO) for Omni Governance Console (OGC).

In this appendix:

- Stopping the OGC Tomcat Service
- Unzipping the Single Sign-On Delivery Package
- Configuring the context.xml Properties File and Creating Backup Files
- Editing the sso.properties File
- Generating Certificates
- Exporting Certificates
- Editing the ogc-sp.xml File With Certificates and Properties
- Configuring the SAML2 Identity Provider (SiteMinder)
- Registering the Identity Provider Partnership Information and Certificate From the Identity Provider
- Special Algorithms (Optional)
- Restarting Apache Tomcat
- Testing the New SAML2 SSO Sign On Page

Stopping the OGC Tomcat Service

Before continuing, ensure that the *OGC Tomcat* service is stopped in the Omni Console, as shown in the following image.



Unzipping the Single Sign-On Delivery Package

Unzip the *ogc_sso.zip* archive file to the following folder of your installation:

```
\omnigen\omniGenData
```

This will create the following subdirectory, which contains two .xml files:

```
\omnigen\omniGenData\sso
```

Note: As of Omni-Gen version 3.10.0 and higher, the two .xml files in this subdirectory are included in the release packaging (in `\omnigen\OmniGenData\sso`), which avoids the need to install these files manually.

Configuring the context.xml Properties File and Creating Backup Files

Navigate to the following directory:

```
\omnigen\OmniGovConsole\conf
```

Verify that the *context.xml* file located in this directory has the following property definition in place, is uncommented, and is consistent with your Omni Governance Console (OGC) installation.

```
<!-- SSO testing -->
<Environment override="true" type="java.lang.String"
value="\omnigen\OmniGenData\sso\sso.properties"
name="ssoConfigPropertiesFile"/>
```

You can also copy this property definition from the *context_snip* file from the SSO delivery location, edit accordingly, and paste it into your *context.xml* file.

If they already exist, create backup copies of the following sso-related files, which are located in the `\omnigen\OmniGenData\sso` directory:

- sso.properties
- ogc-sp.xml

For example, create a backup copy of the *sso.properties* file as *sso.properties.save0402* in the `\omnigen\OmniGenData\sso` directory. Repeat this for the *ogc-sp.xml* file.

Editing the sso.properties File

Navigate to the following directory:

```
\omnigen\OmniGenData\sso
```

The *sso.properties* file that is located in this directory should be structured as follows:

```
active = true (a)
userDomain = ibi (j)
SSO_DOMAIN_1 = PRIMARY (b)
SSO_DOMAIN_2 = iway (b)
SSO_DOMAIN_3 = ibi (b)
keyManager.storeFile = file:/C:\omnigen\omnigendata\sso\wso2carbon.jks (c)
keyManager.storePass = wso2carbon
keyManager.passwords.wso2carbon = wso2carbon (d)
keyManager.passwords.wso2sign = wso2carbon
keyManager.passwords.wso2encr = wso2carbon
keyManager.defaultKey = wso2carbon
metadata.sp.file = \omnigen\omnigendata\sso\ogc-sp.xml (e)
metadata.sp.defaults.local = true
metadata.sp.defaults.alias = test.ibi.com (f)
metadata.sp.defaults.signingKey = wso2sign (g)
metadata.sp.defaults.encryptionKey = wso2encr (h)
metadata.providers.idp = \omnigen\omnigendata\sso\wso2-idp.xml (i)
```

Perform the following steps:

1. Either change the definitions **(j)** and **(b)** in your existing *sso.properties* file, adding the password entries **(d)** for *encr* and *sign* if necessary, and verifying that items **(a)** through **(i)** are correct, or copy the *sso.properties* file from the SSO delivery location, and change the domain names **(j)**, **(b)**, and so on, to reflect your environment.
2. Ensure that the *keyManager.storeFile* value **(c)** above includes the *file:* prefix as per Linux and Windows instances. For example, on Windows:

   ```
   keyManager.storeFile=file:/C:\omnigen\omnigendata\sso
   ```

3. Verify that the *keyManager.passwords* names (for example, *wso2sign* and *wso2encr*) match the *-alias* values entered when the certificates are being generated. For example:

   ```
   keyManager.passwords.wso2sign = wso2carbon
   keyManager.passwords.wso2encr = wso2carbon
   ```

4. Ensure that the fully qualified path and file name is entered in the following line:

```
metadata.sp.file = \omnigen\omnigendata\sso\ogc-sp.xml
```

5. Ensure that the alias specification **(f)** matches the value of the *EntityId* in the Identify Provider (IdP) (for example, SiteMinder or ADFS) and the alias when specified in the *ogc-sp.xml* file. For example:

```
metadata.sp.defaults.alias = test.ibi.com
```

6. Edit the proper key values **(g)** and **(h)** that will be used in *Generating Certificates* on page 126. For example:

```
metadata.sp.defaults.signingKey = wso2sign
metadata.sp.defaults.encryptionKey = wso2encr
```

7. Ensure that the path to the sso-related files and the corresponding file name is correct. For example:

```
metadata.providers.idp = \omnigen\omnigendata\sso\wso2-idp.xml
```

8. Save the *sso.properties* file when you are finished making your changes.

Generating Certificates

To generate certificates:

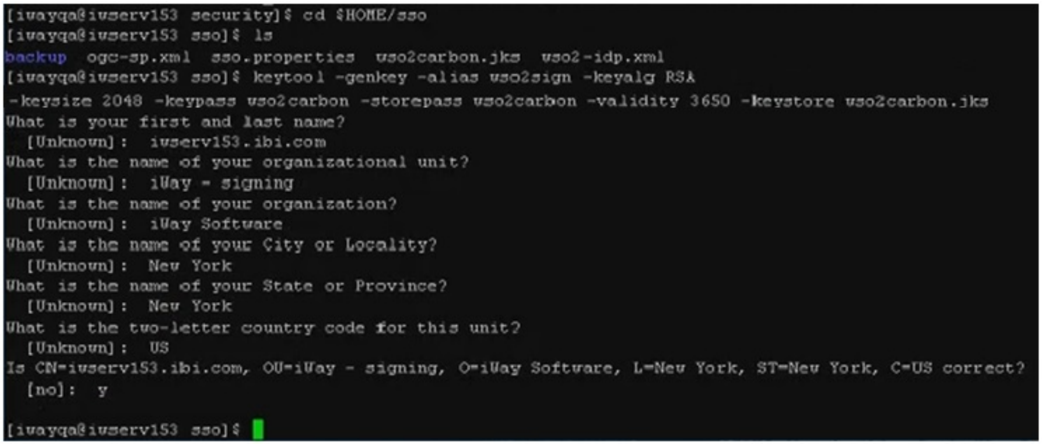
1. Verify that the *keytool* command is in your path.
2. Use the *keytool* command to generate a new signature processing certificate.
3. Navigate to the \sso subfolder. For example:

```
\omnigen\omnigendata\sso
```

4. Type the following:

```
keytool –genkey –alias wso2sign –keyalg RSA –keysize 2048 –keypass
wso2carbon -storepass wso2carbon -validity 3650 -keystore wso2carbon.jks
```

5. Respond to the questions prompted by the *keytool* command using your site details, as shown in the following example:



```
[iwayqa@iwserv153 security]$ cd $HOME/sso
[iwayqa@iwserv153 sso]$ ls
backup  ogc-sp.xml  sso.properties  wso2carbon.jks  wso2-idp.xml
[iwayqa@iwserv153 sso]$ keytool -genkey -alias wso2sign -keyalg RSA
-keysize 2048 -keypass wso2carbon -storepass wso2carbon -validity 3650 -keystore wso2carbon.jks
What is your first and last name?
  [Unknown]:  iwserv153.ibi.com
What is the name of your organizational unit?
  [Unknown]:  iWay - signing
What is the name of your organization?
  [Unknown]:  iWay Software
What is the name of your City or Locality?
  [Unknown]:  New York
What is the name of your State or Province?
  [Unknown]:  New York
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=iwserv153.ibi.com, OU=iWay - signing, O=iWay Software, L=New York, ST=New York, C=US correct?
  [no]:  y

[iwayqa@iwserv153 sso]$
```

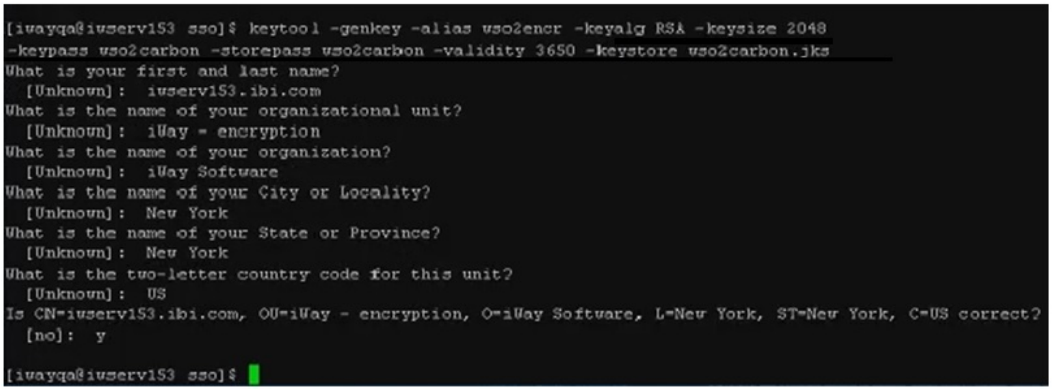
6. Reply to the question *What is your first and last name?* with your Omni Governance Console (OGC) server's host name (for example, *iwserveribi.com*).

7. Use the *keytool* command to generate a new encryption certificate.

8. From the \sso subfolder, type the following:

```
keytool –genkey –alias wso2encr –keyalg RSA –keysize 2048 –keypass
wso2carbon -storepass wso2carbon -validity 3650 -keystore wso2carbon.jks
```

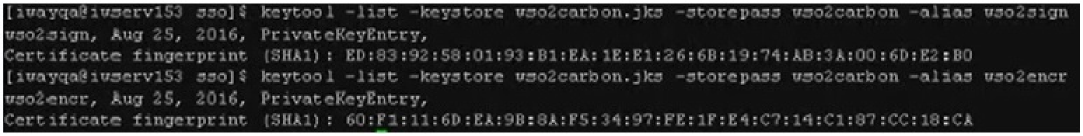
9. Reply to the question *What is your first and last name?* with your Omni Governance Console (OGC) server's host name (for example, *iwserveribi.com*).



```
[iwayqa@iwserv153 sso]$ keytool -genkey -alias wso2encr -keyalg RSA -keysize 2048
-keypass wso2carbon -storepass wso2carbon -validity 3650 -keystore wso2carbon.jks
What is your first and last name?
  [Unknown]:  iwserv153.ibi.com
What is the name of your organizational unit?
  [Unknown]:  iWay - encryption
What is the name of your organization?
  [Unknown]:  iWay Software
What is the name of your City or Locality?
  [Unknown]:  New York
What is the name of your State or Province?
  [Unknown]:  New York
What is the two-letter country code for this unit?
  [Unknown]:  US
Is CN=iwserv153.ibi.com, OU=iWay - encryption, O=iWay Software, L=New York, ST=New York, C=US correct?
  [no]:  y

[iwayqa@iwserv153 sso]$
```

10.Type the `keytool -list` command, as shown in the following example:



```
[ivayqa@ivserv153 sso]$ keytool -list -keystore wso2carbon.jks -storepass wso2carbon -alias wso2sign
wso2sign, Aug 25, 2016, PrivateKeyEntry,
Certificate fingerprint (SHA1): ED:83:92:58:01:93:B1:EA:1E:E1:26:6B:19:74:AB:3A:00:6D:E2:B0
[ivayqa@ivserv153 sso]$ keytool -list -keystore wso2carbon.jks -storepass wso2carbon -alias wso2encr
wso2encr, Aug 25, 2016, PrivateKeyEntry,
Certificate fingerprint (SHA1): 60:F1:11:6D:EA:9B:8A:F5:34:97:FE:1F:E4:C7:14:C1:87:CC:18:CA
```

11.Verify that the certificates are stored in the proper keystore (under `\omnigen\omnigendata\sso`).

Exporting Certificates

To export certificates:

1. Navigate to the \sso subfolder. For example:

   ```
   \omnigen\omnigendata\sso
   ```

2. Type the following:

   ```
   keytool -exportcert -keystore wso2carbon.jks -storepass wso2carbon
   -alias wso2sign -file wso2sign.crt -rfc
   ```

   This will generate a certificate in RFC style for signature processing in the `\omnigen\OmniGenData\sso` directory named *wso2sign.crt*.

3. From the \sso subfolder, type the following:

   ```
   keytool -exportcert -keystore wso2carbon.jks -storepass wso2carbon
   -alias wso2encr -file wso2encr.crt -rfc
   ```

   This will generate a certificate in RFC style for encryption processing in the `\omnigen\OmniGenData\sso` directory named *wso2encr.crt*.

Editing the ogc-sp.xml File With Certificates and Properties

To edit the *ogc-sp.xml* file with certificates and properties:

1. Edit the *ogc-sp.xml* file.

   The following is a sample *ogc-sp.xml* file for reference.

   Note that there are two long, multi-line strings in the `<ds:X509Certificate>` tags. These are the certificates that will be overwritten with the site-specific certificates that were created in *Generating Certificates* on page 126. Shortened versions of the certificates are shown in this sample for demonstration purposes. The actual certificates will be much larger.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="test.ibi.com"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
<md:SPSSODescriptor AuthnRequestsSigned="true"
WantAssertionsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:Extensions>
            <idpdisco:DiscoveryResponse
xmlns:idpdisco="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
protocol" Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-
protocol" Location="http://localhost:8080/spring-security-saml/login/
auth/alias/localhost?disco=true"/>
        </md:Extensions>
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
MIIDoTCCAomgAwIBAgIEf6nJDTANBgkqhkiG9w0BAQsFADCBgDELMAkGA1UEBhMCVVMxETAPB
gNV
Ykym9tOG+m21eC5LgRX+qyfB+XE7OP24N/
ccKYuJkcQdJKnJCFxgdC3xl45EfaEFh5bQ0UOZzzSM
cyNApOW+qssSOxRJyWbqAEOx3SxE
</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:KeyDescriptor use="encryption">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
MIIDpzCCAo
+gAwIBAgIEIuaEgzANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCVVMxETAPBgNV
0MaUTCLU1X94XcQJQ8zskBLSSw2jrf9rvGzBMHJrTphJGl0RluIpJWu0fWFhNRRxq61FwZzRl
53j
5pHGZ2yxcPWefW05qqjX/ZZWkx8rxH/YnTvA
         </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-POST" Location="http://iwserv153.ibi.com:8080/ogc/saml/
SingleLogout/alias/test.ibi.com"/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-Redirect" Location="http://iwserv153.ibi.com:8080/ogc/
saml/SingleLogout/alias/test.ibi.com"/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:SOAP" Location="http://iwserv153.ibi.com:8080/ogc/saml/
logout/SingleLogout/test.ibi.com"/>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
```

```
 <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</
md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-POST" Location="http://iwserv153.ibi.com:8080/ogc/
saml/SSO/alias/test.ibi.com" index="0" isDefault="true"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-Artifact" Location="http://iwserv153.ibi.com:8080/ogc/
saml/SSO/alias/test.ibi.com" index="1" isDefault="false"/>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

2. Navigate to the following directory:

   ```
   \omnigen\omnigendata\sso
   ```

3. Open the *wso2sign.crt* file.

   The long multi-line string between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` is the actual certificate . Copy and paste it into the *ogc-sp.xml* file between the `<ds:X509Certificate>` tags, which are below the `<md:KeyDescriptor use="signing">` tag. When pasting, ensure that you overwrite the entire existing string that is currently there.

4. Open the *wso2encr.crt* file from the \sso directory.

   The long multi-line string between `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` is the actual certificate . Copy and paste it into the *ogc-sp.xml* file between the `<ds:X509Certificate>` tags, which are below the `<md:KeyDescriptor use="encryption">` tag. When pasting, ensure that you overwrite the entire existing string that is currently there.

5. Still editing the *ogc-sp.xml* file, edit the *EntityID* field, which is located at the top of the file.

   Set the value to the value used in the *sso.properties* file. For example:

   ```
   <md:EntityDescriptor entityID="test.ibi.com"
   ```

6. Edit the five URLs which refer to the *EntityID* field.

   There are three `SingleLogoutService` tags and two `AssertionConsumerService` tags.

7. Change all five of the default *test.ibi.com* strings to your *EntityID* value specified in the *sso.properties* file. For example:

   ```
   <md:EntityDescriptor entityID="test.ibi.com"
   ```

   The five strings are located at the bottom of the *ogc-sp.xml* file as follows:

```
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-POST" Location="http://iwserv153.ibi.com:8080/ogc/saml/
SingleLogout/alias/test.ibi.com"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-Redirect" Location="http://iwserv153.ibi.com:8080/ogc/
saml/SingleLogout/alias/test.ibi.com"/>

<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:SOAP" Location="http://iwserv153.ibi.com:8080/ogc/saml/
logout/SingleLogout/test.ibi.com"/>

<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-POST" Location="http://iwserv153.ibi.com:8080/ogc/
saml/SSO/alias/test.ibi.com" index="0" isDefault="true"/>

<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:
2.0:bindings:HTTP-Artifact" Location="http://iwserv153.ibi.com:8080/ogc/
saml/SSO/alias/test.ibi.com" index="1" isDefault="false"/>
```

8. In these same URL strings, change the five host name instances (for example, *iwserv153.ibi.com*) to your actual OGC host name that is being used.
9. Save the *ogc-sp.xml* file and give it to the Identity Provider (IdP) administrator.

Configuring the SAML2 Identity Provider (SiteMinder)

The SAML2 Identity Provider (IdP) administrator (or other SAML2 IdP administrator) creates the partnership and returns the partnership *idp.xml* file.

Registering the Identity Provider Partnership Information and Certificate From the Identity Provider

1. Copy the *idp.xml* file received from the SiteMinder Identity Provider (IdP) administrator into the following directory:

   ```
   \omnigen\OmniGenData\sso
   ```

2. Edit the *sso.properties* file, which is located in the same directory.
3. Change line **(i)** as tagged in *Editing the sso.properties File* on page 125, defining *metadata.providers.idp* to the exact, fully qualified file name of the *idp.xml* file that the SiteMinder IdP administrator has provided to you.

   For example:

   ```
   metadata.providers.idp = \omnigen\OmniGenData\sso\wso2-idp.xml
   ```

4. Ensure that the first line in the *sso.properties* file is set as follows:

   ```
   active=true
   ```

5. Save the *sso.properties* file.

Special Algorithms (Optional)

If the use of special blocking and signing algorithms is required (for example, to support a change of the signing algorithm to RSA with SHA256, and support AES-256 blocking algorithm), then perform the following steps to add the Java Cryptography Extensions *local_policy.jar* and *US_export_policy.war*.

Note: If Java version 1.8 is being used, then skip to step 4.

1. In your Java installation (`\jre\lib\security` directory) and in all of the Java installations in use by Omni Governance Console (OGC), SiteMinder Identity Provider (IdP), and the SiteMinder Policy Server (they are most likely already in Java used by the Identity Provider and the Identity Provider's Policy Server):
    a. Rename the original *local_policy.jar* file to:

    ```
    local_policy_orig_jar.out
    ```

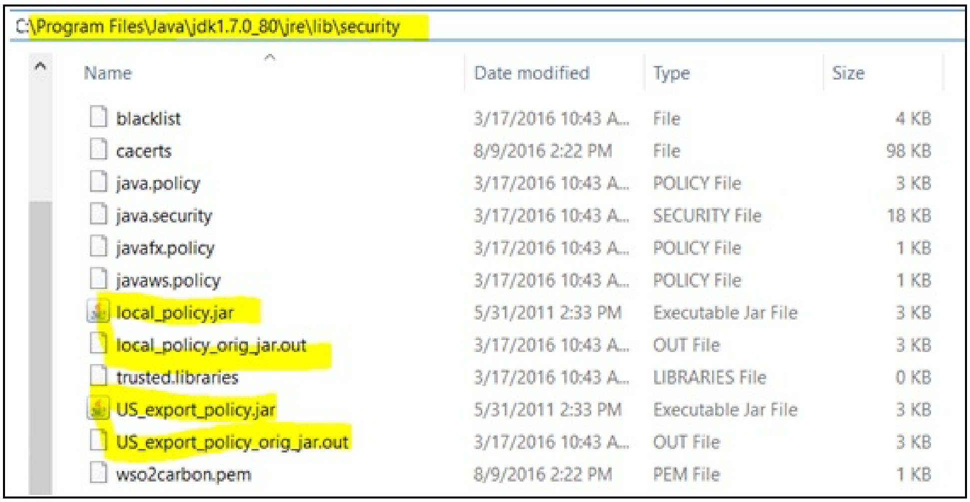
    b. Rename the original *US_export_policy.jar* file to:

    ```
    US_export_policy_orig_jar.out
    ```

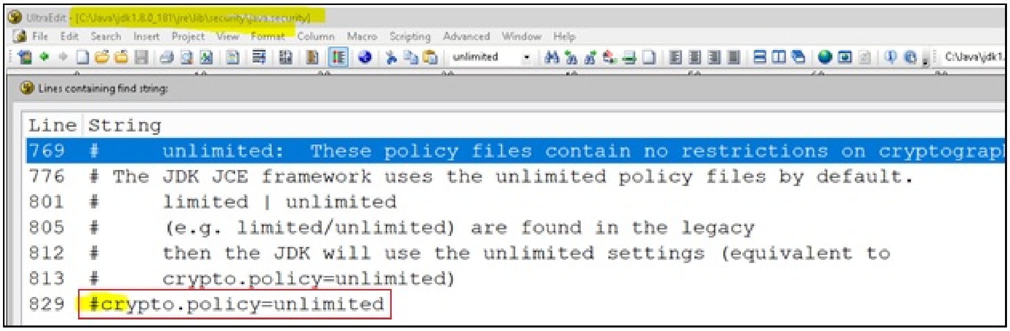
2. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files (*local_policy.jar* and *US_export_policy.jar*) directly from the Oracle website, and store them in the following directory of your Java installation:

    ```
    \jre\lib\security
    ```

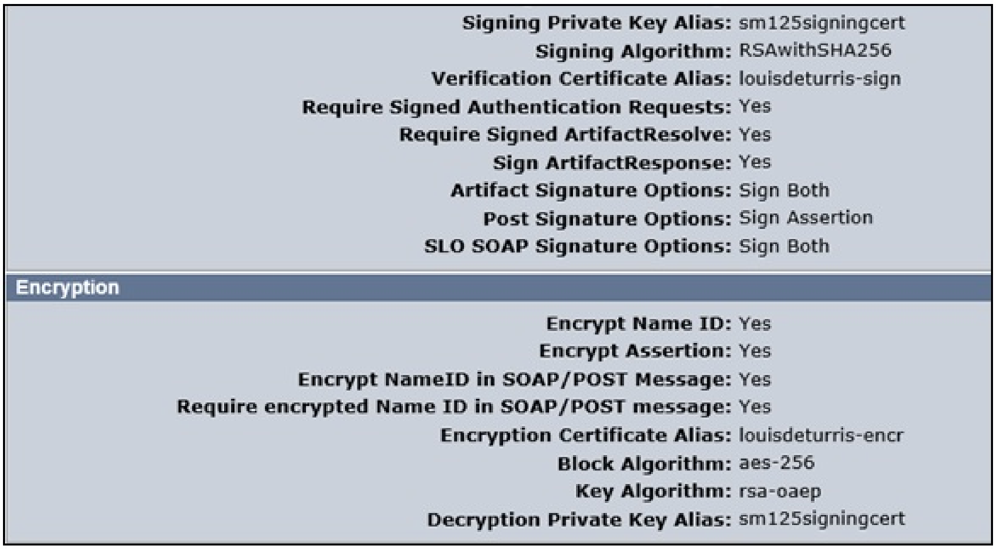
    For example, you should have a `\security` subfolder that is structured as shown in the following image.



3. For Java version 1.8, uncomment the `crypto.policy` setting, which is located in `\java\jdk1.8.0_181\jre\lib\security\java.security`, as shown in the following image.



4. Issue a request for the SiteMinder IdP administrator to reconfigure the partnership with the required algorithms, as shown in the following image.



No additional changes to OGC properties or to the generated certificates are required.

Restarting Apache Tomcat

To restart Apache Tomcat:

1. Delete or save the log files in the following directory:

   `\omnigen\OmniGovConsole\logs`

2. Delete the following `\Work` subfolder and all of its contents:

   `\omnigen\OmniGovConsole\Work`

3. Start the *OGC Tomcat* service in the Omni Console.

Testing the New SAML2 SSO Sign On Page

To test the new SAML2 SSO sign on page:

1. From a browser, clear the cache and try to connect and login to Omni Governance Console (OGC) with your regular URL.

   Instead of the original Omni-Gen Console login page, you should be rerouted to the Identify Provider's (ADFS or SiteMinder) login page.

2. Log in with your SSO credentials.

Appendix C

Using MData, Synch, and WSO2 Administration

This appendix describes the WSO2/MData Synchronization (Mdata-Synch) feature of reducing the configuration work of the administrator when a new subject arrives into the Omni-Gen Server (OGS) model and database, and when data structures are altered (for example, a type or name of a column has been changed). The whole synchronization process has been reduced to double-clicking on the OGC Administration Panel while allowing you to do some basic customization to the synchronization process.

Previously, all users had to go through a set of manual steps in the OGC Administration Panel and in several WSO2 IS Administration panels to make the OGC application consistent with the change(s) made to the data structure.

In this appendix:

- Functional Overview
- Using the WSO2/MData-Synchronization Feature

Functional Overview

MData-Synch consists of the following parts:

- Interaction with OmniDomain to synchronize the internal data structure (referred to as MData) of OGC.
- Interaction with WSO2 to synchronize permissive mechanisms of the OGC application.

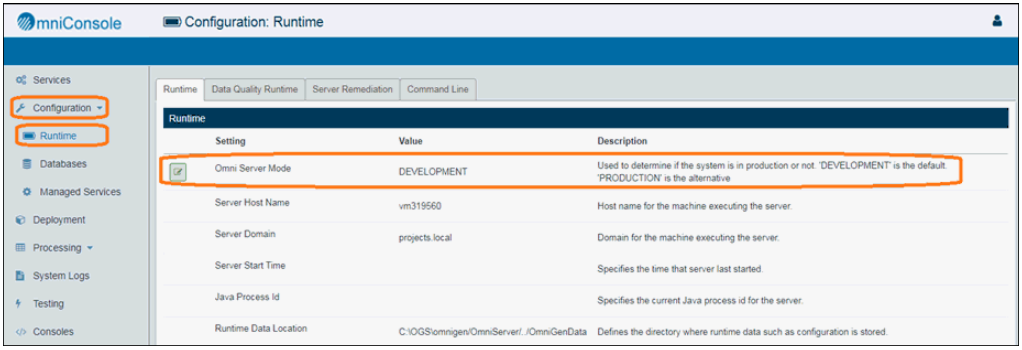
Using the WSO2/MData-Synchronization Feature

This section describes the prerequisites and synchronization usage of the WSO2/MData feature.

Configuring Omni Server Mode

This section describes how configure the Omni Server Mode setting in the Omni Gen Server (OGS).

The synchronization functionality is intended for use only in OGS DEVELOPMENT mode, where you must configure the Omni Server Mode setting to *DEVELOPMENT*, as shown in the following image.



Note: If the OGS is unresponsive (for example, it is not started or in error), the Sync functionality is disabled.

Using the Synchronization

When a new model contains a new subject(s), or a change to the structure of a current subject, a synchronization between the updated data structure and the structure previously existing in OGC is required.

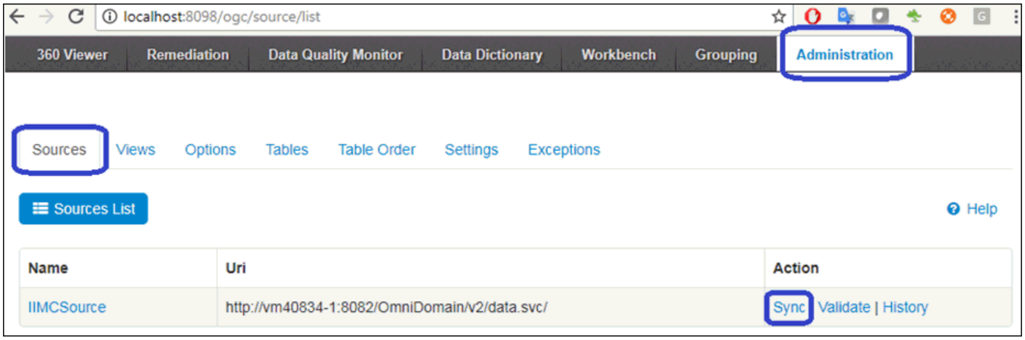
Initialization of the synchronization process is performed using OGC and consists of the following parts:

- Analysis for the sync (and optional customization)
- Actual synchronization using the results of the analysis

The following procedure shows a sample workflow of actions for a user to accomplish the synchronization.

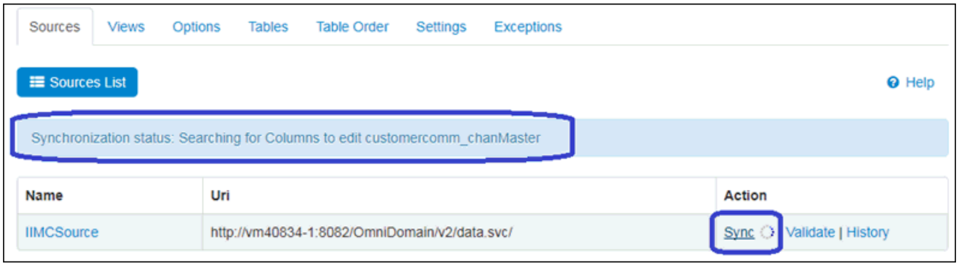
Step 1: Initializing the Analysis for the Synchronization Process.

Using your browser, connect to the OGC Logon page, log on with the credentials containing the System_Administrator role, and then navigate to the Sources tab from Administration, and click the *Sync* link, as shown in the following image.



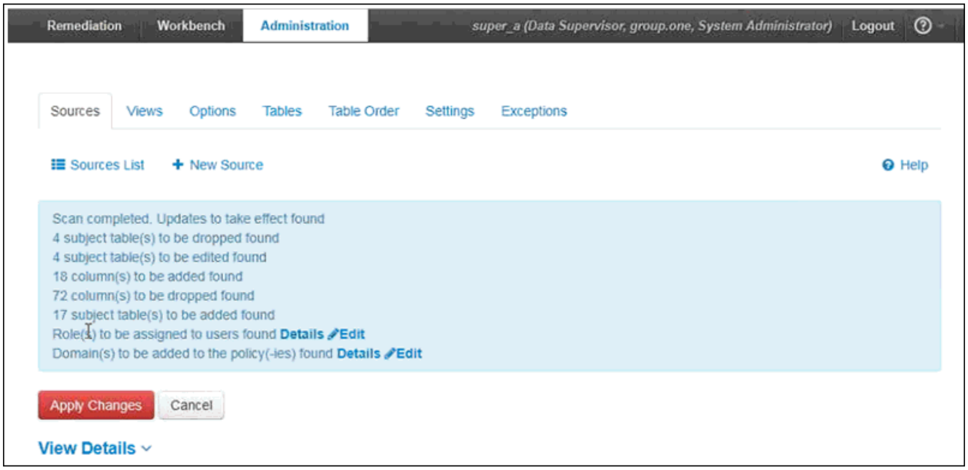
Step 2: Analyzing the Progress.

The analysis for the synchronization process begins, where the status bar displays the dynamic progress of the status, as shown in the following image.



Step 3: Summarizing the Analysis.

After the analysis is complete, a summary on the proposed synchronization appears, as shown in the following image.

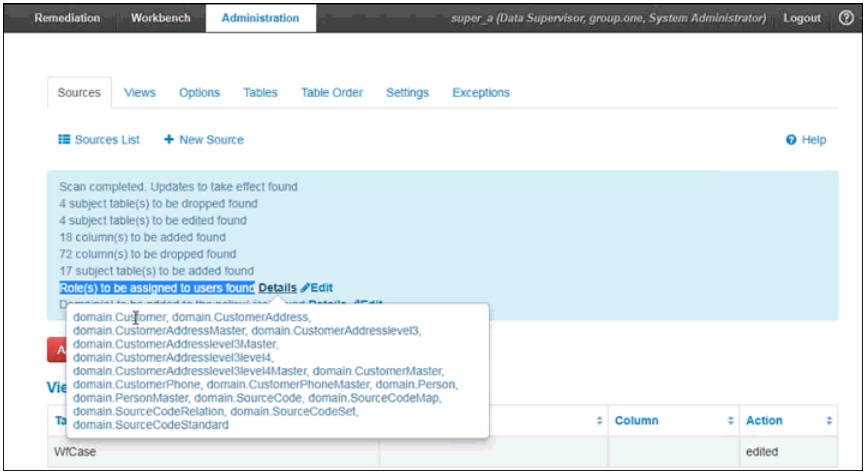


Step 4: Viewing the Details of the Analysis.

You can view the details on the potential update by expanding the *View Details* link.

Note: *View Details* refers only to the action modifying the OGC MData structure. To view the details for WSO2 modification, click the *Details* link near the respective summary items, as shown in the following image.

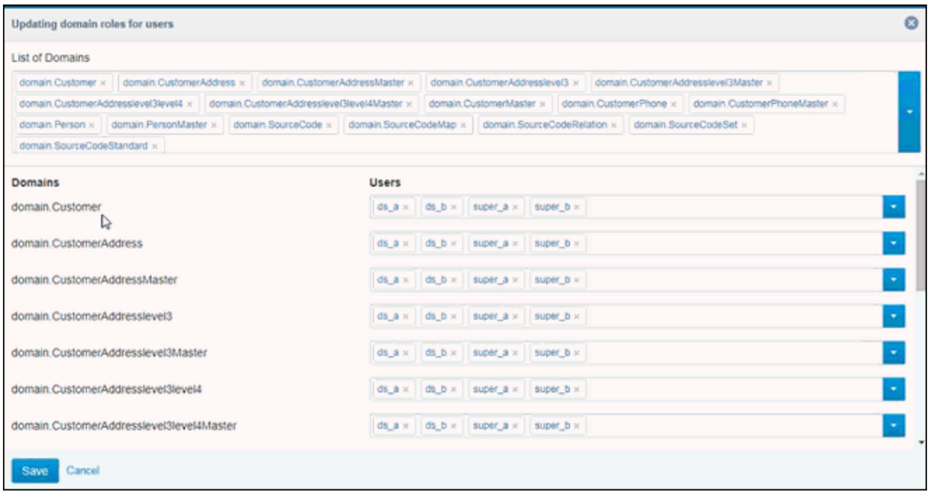
The following image shows a sample entry after clicking *Details* from *Role(s) to be assigned to users found*.



Step 5: Customizing Roles or Users to be Synchronized (Optional)

By default, four users (*ds_a*, *ds_b*, *super_a*, and *super_b*) are granted all the new domain roles (for example, permission to access the new domains or subjects).

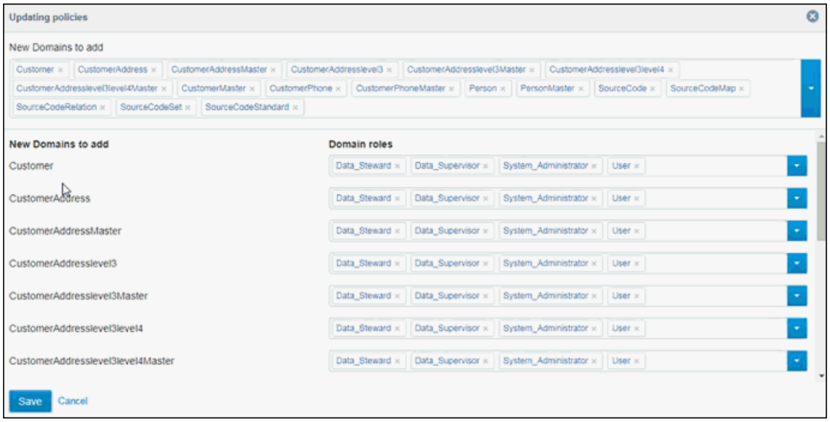
To customize those defaults, click *Edit*. A dialog allowing refinement of the assigned domain roles appears. The user can then add or remove new domain roles and users, as well as the relations between them, as shown in the following image.



Step 6: Customizing Policies to be Updated (Optional

By default, each new domain role will be added to all the role sections in policies.

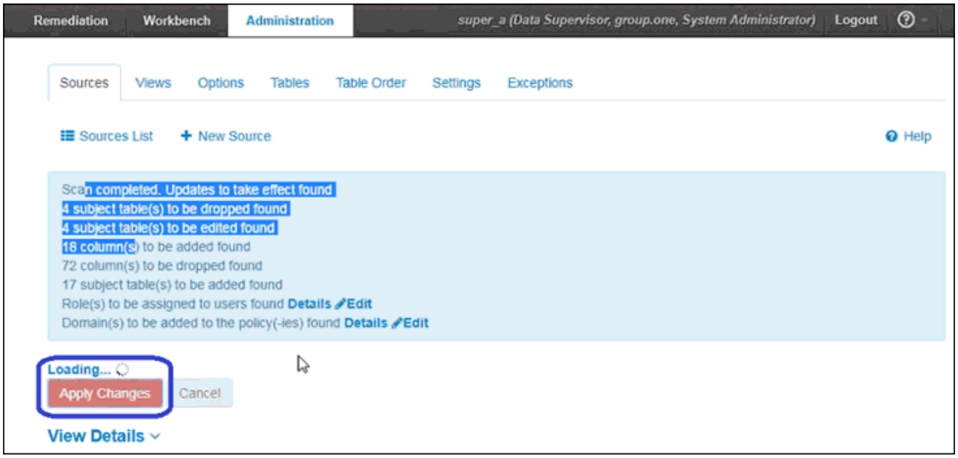
To change the default settings, click *Edit*. A dialog defining which domain roles will refer to what role sections in all policies appears. The user can match the new domain roles to the regular roles, as shown in the following image.



Step 7: Executing the Synchronization

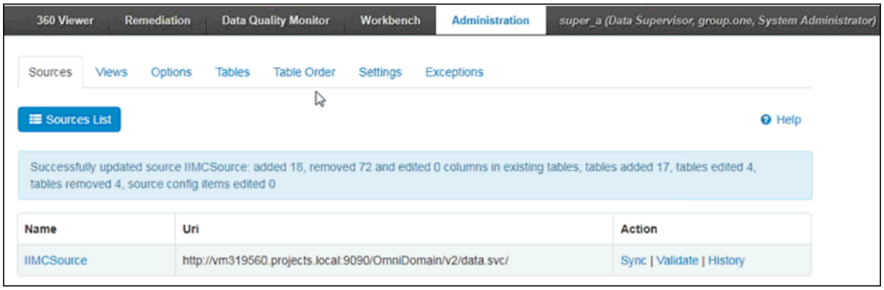
To start the actual synchronization process, click *Apply Changes*.

A Loading message appears, as shown in the following image.



Step 8: Summarizing the Synchronization

When the synchronization is complete, a summary appears displaying the synchronization details, as shown in the following image.



The OGC Application should now be completely in sync with the new OGS data structure, and fully functional in using the new data.

Developer Environment Considerations

When using the synchronization functionality from a developer environment (for example, IntelliJ IDEA, Eclipse, and so on) with OGS deployed on secured gateway (HTTPS), the configuration of SSL certificates should take place as described in this section.

Note: The following procedure should be performed *only* if you are running it in your integrated development environment (IDE).

1. Add the new VM argument to your running configuration. For example:

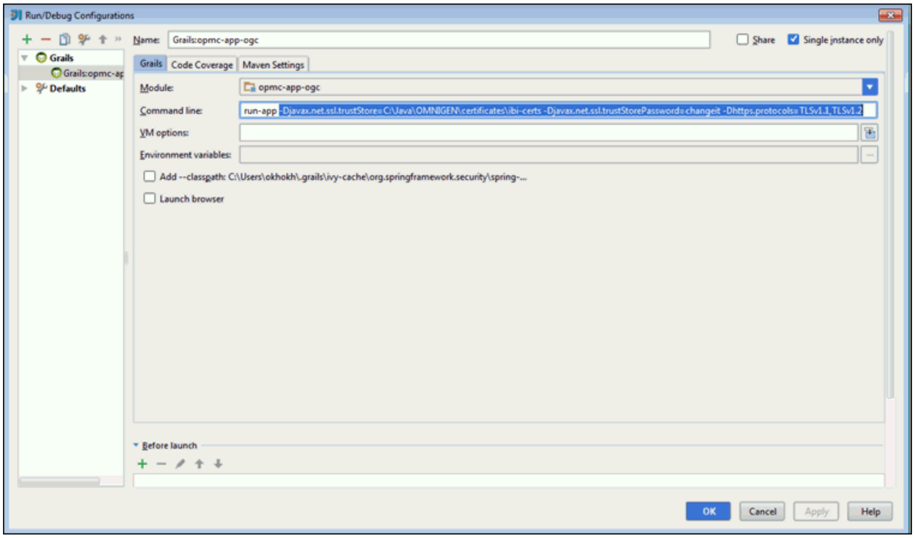
```
-Djavax.net.ssl.trustStore=[path_to_certificates]\ibi-certs -
Djavax.net.ssl.trustStorePassword=changeit -
Dhttps.protocols=TLSv1.1,TLSv1.2
```

   where:

   ibi-certs

   Is the name of the key storage.

2. Open *Run\Debug Configurations* and append the new arguments to the Command line field, as shown in the following image.



3. Copy the required certificate from the OGS location to your computer. For example:

   `..\[OGS_HOME_DIR]\omnigen\OmniGenData`

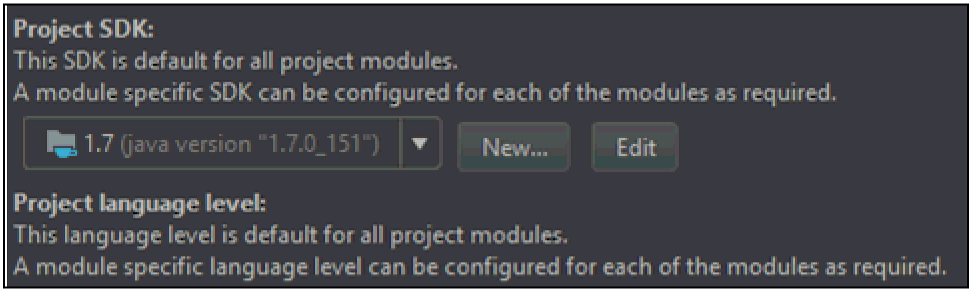
   Ensure that the following files are copied:

   - ibi-certs
   - omnigenstore
   - omnigenstore.pem

   Note: The certificate can change from time to time. If this happens, you must update them.

4. You must install JDK 1.7 with an update higher than 99, otherwise requests will fail even with correct certificates.

5. After installation is complete, open *File*, select *ProjectStructure*, and then ensure that Project SDK is configured to the proper location, as shown in the following image.



Appendix D

Configuring Omni Governance Console Roles From LDAP (Active Directory)

This appendix describes how to configure a WSO2 based LDAP connection and User Store which will eliminate the redundant data entry, and allow the Subject per Userid Authorizations to be obtained from the enterprise LDAP Server (Active Directory).

In this appendix:

- Overview
- Prerequisites
- Enabling Authorization Permission From OGC Using Group Names Through LDAP
- Using the Active Directory (LDAP Server) System
- Testing Logons to Omni Governance Console (OGC)

Overview

In prior versions, Omni-Gen/Omni-Governance Console supported username authentication and authorization using WSO2_is. The WSO2 repository consisted of a local repository of users and permissions, and groups of users stored in LDAP servers (for example, MS Active Directory). Until now, only user names and authentication requests/responses were obtained by OGC over an LDAP connection. User names which belonged to groups in the enterprise AD, and made available to the Identity Server of OGC, WSO2_IS, each had to be manually re-authorized in WSO2_IS using the WSO2_IS Administration console.

The following sections detail how to configure a WSO2 based LDAP connection and User Store, which eliminates the redundant data entry, and allows the Subject per UserID Authorizations to be obtained from your enterprise LDAP Server (Active Directory).

Prerequisites

The following list describes the prerequisites prior to configuring the OGC roles from LDAP.

- The username and password of an authorized LDAP user.
- The LDAP parameter values on your LDAP server, equivalent to the parameters on the Add New User Store form, for a typical MS Active Directory system, as shown in the following section.

Enabling Authorization Permission From OGC Using Group Names Through LDAP

This section describes how to enable authorization permission from OGC using Group Names through LDAP.

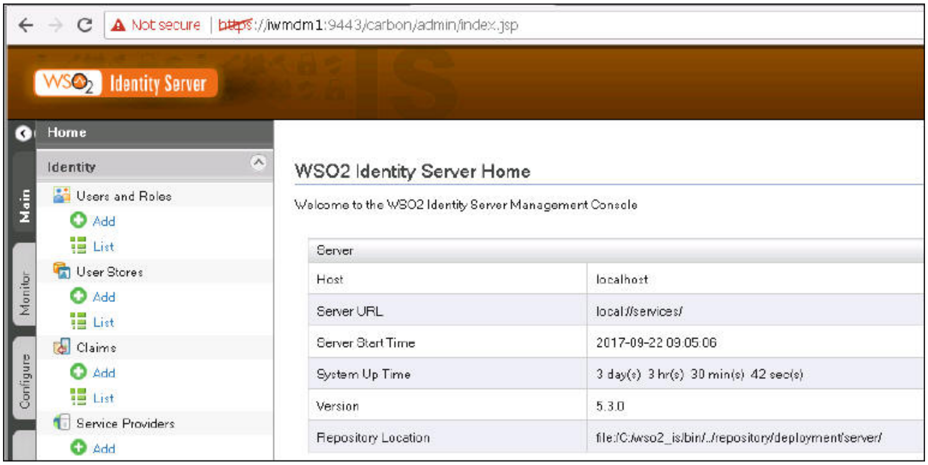
Procedure: How to Enable Authorization Permission from OGC Using Group Names Through LDAP

1. Connect to the WSO2_IS system administration console. For example:

   `https://`*`your-wso2hostname`*`:9443`

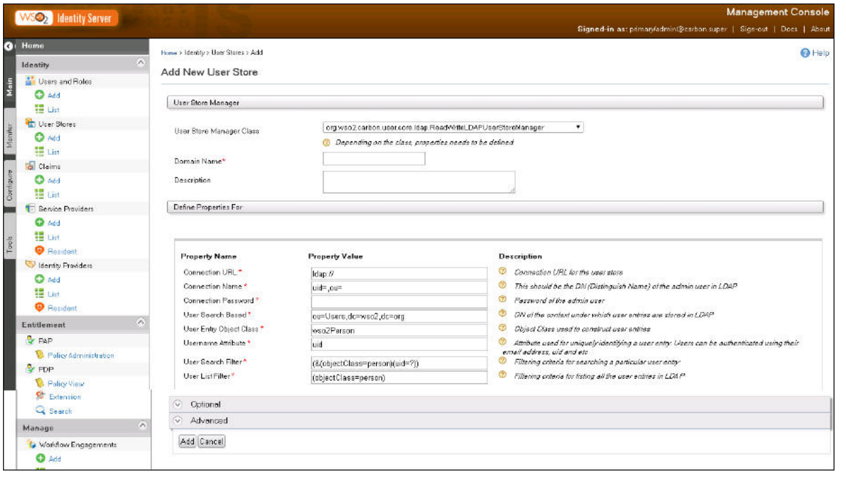
2. From the WSO2 homepage, log on with the WSO2_IS username and password of the administrator.

   The WSO2 Identity Server opens, as shown in the following image.



3. Click the Main tab at the left edge of the window.
4. Click *Identity*, select *User Stores*, and then click *Add*.

The Add New User Store window appears, as shown in the following image.



5. Complete the fields in the Property Value section.

   Note: The example below is based on configuring an LDAP connection to an MS Active Directory server.

6. Change the User Store Manager Class drop-down list to:

   `org.wso2.carbon.user.core.ldap.ReadOnlyLDAPUserStoreManager`

7. In the Domain Name field, enter a value for your domain name of your user name (for example, OGCUSERS).

   Note: This domain name will be used by all users logging in to OGC. Their user names will be entered as:

   OGCUSERS/*corporate_userid*

8. Enter the equivalents from the table below as defined on your Active Directory system.

Parameter	Value
Connection URL*	`ldap://iwadc-vm.iwaydev.ibi.com:389`
Connection Name*	`CN=Administrator,CN=Users,DC=iwaydev,DC=ibi,DC=com`
Connection Password*	`(Enter this last!)`

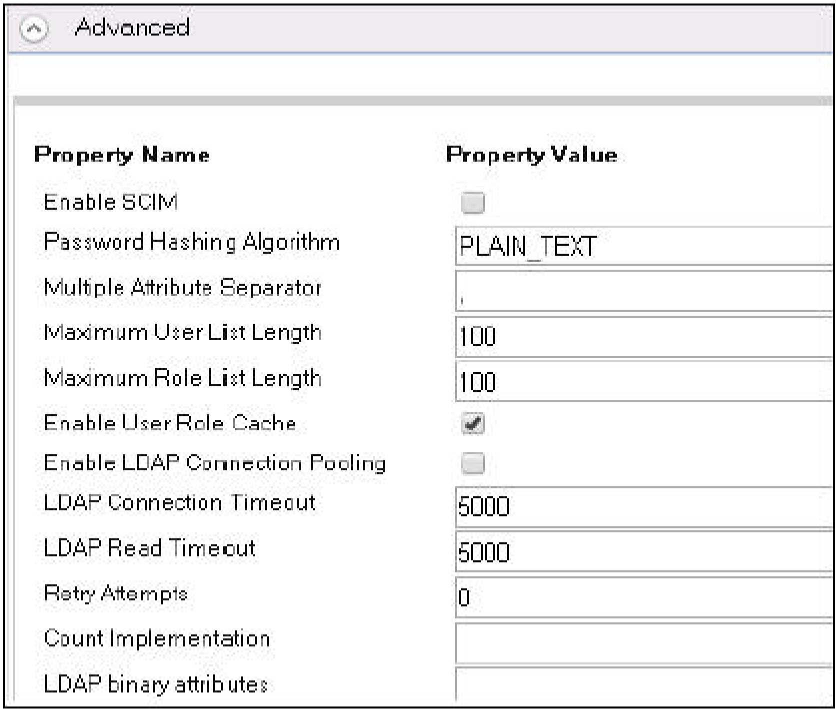
Parameter	Value
User Search Base*	`CN=Users,DC=iwaydev,DC=ibi,DC=com`
Username Attribute*	`sAMAccountName`
User Search Filter*	`(&(objectClass=user)(sAMAccountName=?))`
User List Filter*	`(&(objectClass=user)(memberOf=CN=OGCUSERS,CN=Users,DC=iwaydev,DC=ibi,DC=com))`

Note: An asterisk denotes a required field.

9. Expand *Optional* and then enter the following values into the corresponding fields:

Parameter	Value
User DN Pattern	(Nothing, leave blank)
Display name attribute	`sAMAccountName`
Read Groups	Select the check box.
Group Search Base	`CN=Users,DC=iwaydev,DC=ibi,DC=com`
Group Name attribute	`cn`
Group Search Filter	`(&(objectClass=group)(cn=?))`
Group List Filter	`(objectClass=group)`
Role DN Pattern	(Nothing, leave blank)
Membership Attribute	`member`
Member of Attribute	(Nothing, leave blank)
Enable Escape Characters at User Login	Select the check box.

10. Leave the Advanced section as is, as shown in the following image.



11. Enter the password in the Connection Password field.
12. Scroll down to the bottom of the form and click *Add*.
13. Confirm the information that appears in the User Stores are being Updated pop-up window.
14. Click the *Main* tab, select *User Stores*, and then click *List*.

    The new User Store Name (for example, OGCUSERS) appears.

15. Click *Users*.

    The new User Store Name also appears in the ALL USER STORE DOMAINS drop-down list, as well as the new domain users with the User Store name prefix which are listed in the name listl.

Using the Active Directory (LDAP Server) System

The following example uses Object names and LDAP parameters as used in a Microsoft Active Directory system. The LDAP server administrator must know the corresponding Object names when using a non-MS Active Delivery system.

1. Use Remote Desktop to access your Active Directory host (for example, to `wadc-vm.iwaydev.ibi.com`), and log on using your LDAP-Administrator user name and password.

   For example:

   - Username: **Administrator**

   - Password: **(LDAP authorized Password)**

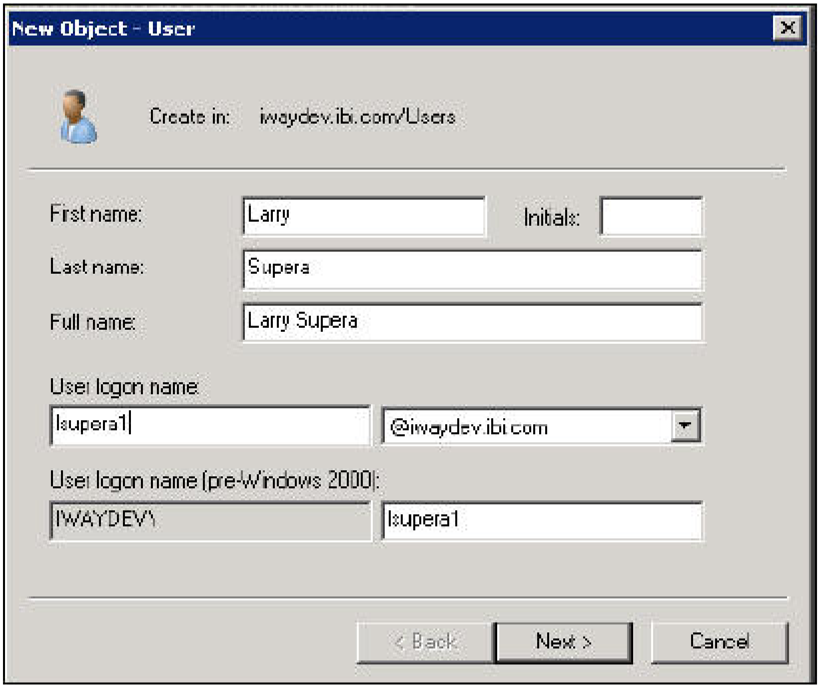
2. Click *Start*, select *Administrative Tools*, and then click *Active Directory Users and Computers*.

3. Identify the corporate or privileged UserName and proceed to *Create Groups in Active Directory*.

   If you do not have a corporate UserName, you must create one by performing the following steps:

   a. From the Active Directory Navigation Bar on the left pane, right-click *Users*, select *New*, and click *Users*.

b. Enter the required information in the First name, Last Name, Full name, and User logon name fields, as shown in the following image.



c. Click *Next*.

d. Enter and confirm the password, clear the *User must change password* check box, and select the *Password never expires* check box.

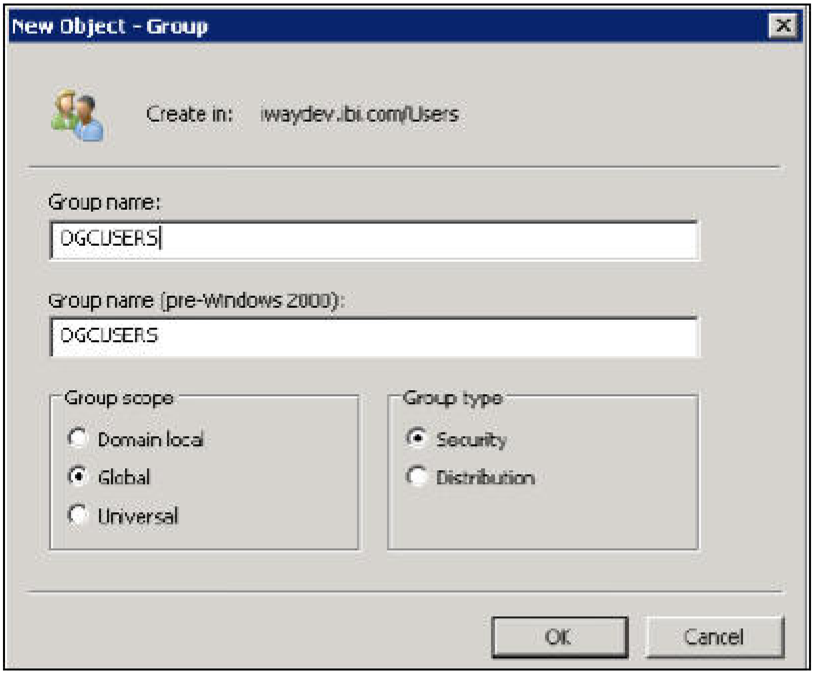
e. Click *Next*, and then click *Finish*.

Procedure: How to Create Groups in Active Directory

To create groups in the Active Directory, perform the following one-time steps:

1. Right-click *Users*, select *New*, and then click *Group*.
2. Enter the Group name or use the same name as your LDAP connection (for example, OGCUSERS).
3. In the Group scope section, select the *Global* radio button.

4. In the Group type section, select the *Security* radio button.



5. Click *OK*.
6. Repeat steps 1 - 5 for each of the following group names:
   - Data_Supervisor
   - Data_Steward
   - User
   - System_Administrator
7. If your OmniGen Model includes the Customer subject, repeat steps 1 - 5 for each of the following group names:
   - domain.Customer
   - domain.CustomerMaster
8. Repeat the two domain.group creations for each Mastered subject in your OmniGen Model.

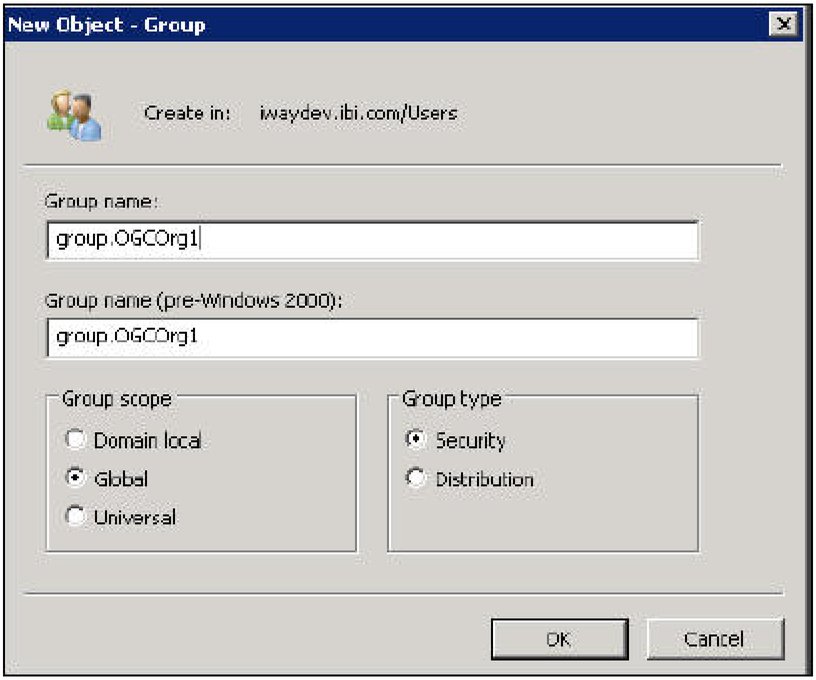
   For example, if Subject = Vendors, then create the groups domain.Vendors and domain.VendorsMaster.

9. Create the Supervisor and Steward Group(s).

   The hierarchical Supervisor & Steward Remediation Case resolution featured in OGC allows for a Data_Steward to resolve a case, at which time the case is automatically reassigned to that Data_Supervisor of the Steward for Approval and Closure.

   If you are not using this feature, proceed to step 10. Otherwise, if you will use the hierarchical Supervisor and Steward Remediation Case resolution feature in OGC, you must create an OGC-Org Group for each group by performing the following steps:

   a. Create a group (for example, group.OGCOrg1), as shown in the following image.



   b. Repeat the above step for Creating (AD) groups for as many Data_Supervisor with Data_Steward(s) groups (or teams) that exist.

10. Designate the user to be a member of the Omni Users Group whose members will be allowed to log on to OGC. For example, make the user a member of the OGCUSERS group.

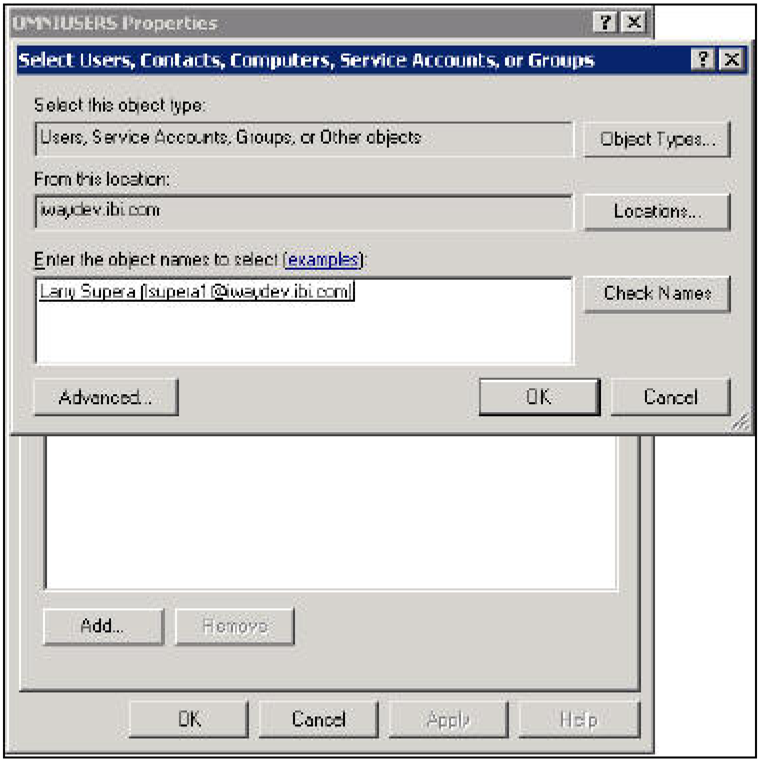
    To designate a user:

    a. Right-click *OGCUSERS*, select *Properties*, and then click *Members*.

    b. Click *Add*.

    c. Enter the first name or Login ID into the *Enter the object names to select* field.

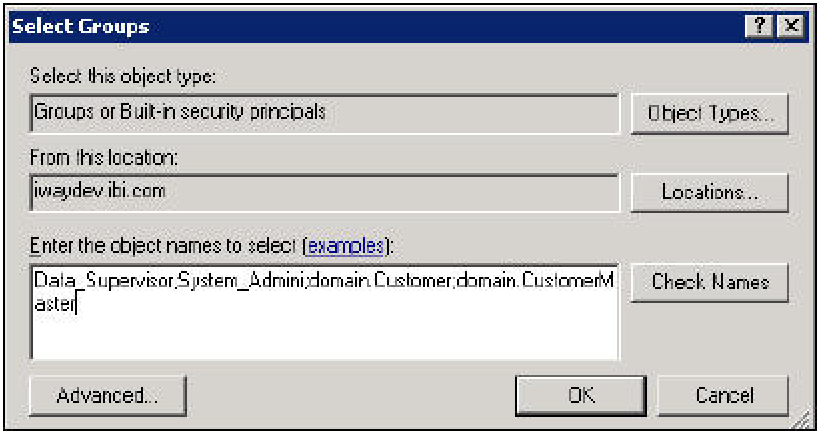
d. Click *Check Names*, as shown in the following image.



e. Click *OK*.

f. Click *Apply*, then click *OK*.

You can add the user to multiple Groups by separating them with a semi-colon, as shown in the following image.



11. Within the Omni Users Group, designate a user to be a member of only *one* of the following three groups:

- ❑ Data_Supervisor
- ❑ Data_Steward
- ❑ User

12. If the user is to be an OGC_Administrator (and has the Administration tab on their own OGC menu), designate that user a member of the System_Administration group. Otherwise, proceed to the next step.

13. Designate the user to be a member of both domain groups for each subject they can access.

    For example, designate them to be a member of domain.CustomerMaster for access to the Customer Master records, and a member of domain.Customer to grant access to Customer Instance records.

    For instance, if the user is to have access to Vendors, designate that user to be a member of domain.Vendors and of domain.VendorsMaster, and so on.

    Note: If you are using the Supervisor or Steward(s) groups, perform the following steps as many times as necessary.

    a. Designate only *one* Data_Supervisor (a user who is a member of the Data_Supervisor group) a member of group.OGCOrg1.

b. Designate *all Data_Stewards who are supervised* by the Data_Supervisor above, a member of the Data_Supervisor's Group (for example, a member of group.OGCOrg1).

Testing Logons to Omni Governance Console (OGC)

This section describes how to test logons to OGC after creating OGC roles from LDAP.

Procedure: How to Test Logons to OGC

To test your logon of OGC:

1. Connect to OGC by entering the following into your browser:

   `http://`*`yourhostname`*`:9090/ogc`

2. Perform the following test 1.

   a. Enter your username and password credentials. For example:

      Username: **UserSuperv1**

      Password: **PassSuperv123**

   b. Verify that the 360 Viewer, Remediation, and Administration consoles are shown.

   c. Verify that the 360 Viewer shows the Customer Master records.

3. Perform the following test 2.

   a. Enter your username and password credentials. For example:

      Username: **UserSuperv1**

      Password: **PassSuperv123**

   b. Verify that the 360 Viewer and Remediation consoles are shown, but not the Administration console.

   c. Verify that the 360 Viewer shows the Customer Master records.

Appendix E

Custom Logos (Application Branding)

This section describes how to apply branding or custom logos to your Omni Governance Console (OGC) application.

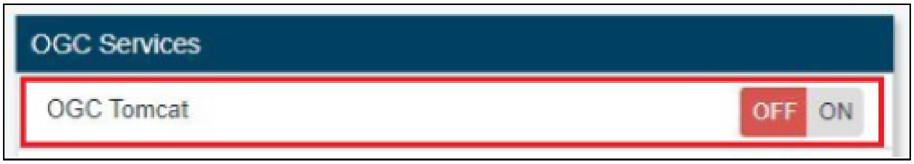
In this appendix:

- Rebranding Omni Governance Console Images With Custom Logos
- Image Reference Catalog
- Available Branding Locations
- Understanding the Placement of Branding Assets

Rebranding Omni Governance Console Images With Custom Logos

To rebrand Omni Governance Console (OGC) images with custom logos:

1. Prepare your custom logo image(s) as .png files with transparent backgrounds and image resolutions, as defined in *Image Reference Catalog* on page 158.
2. Log out of your current OGC session.
3. Ensure that the *OGC Tomcat* service is stopped in the Omni Console, as shown in the following image.



4. Use the File Explorer on your system and the information in *Image Reference Catalog* on page 158 to navigate to the image you want to replace.
5. Rename the image file you want to replace by adding the _*orig* suffix to its file name.

   For example, rename logo_login.png as logo_login_orig.png.

6. Copy your custom logo image file, which must be named according to the corresponding value in the File Name column, in *Image Reference Catalog* on page 158.

   For example, copy

   <your_custom_image_source>\logo_login.png

to

`…\images\logos\login\logo_login.png`

7. Start the *OGC Tomcat* service in the Omni Console.
8. Log in to OGC and view the new custom logo images.

Image Reference Catalog

The following table provides a reference catalog for all of the image locations that can be rebranded. Corresponding screenshots showing the image assets are also provided for reference purposes following this table.

Image	**File Name**	**Path**	**Resolution**	**Color Depth**	**Description**
0	logo_about.png	...\images \logos \about_dialog	280x40	32	About dialog logo
1	logo_login.png	...\images \logos\login	280x40	32	Login page main logo
2	logo_login_info. png	...\images \logos\login	177x49	32	Login page bottom logo
3	logo_360viewer .png	...\images \logos \360viewer	295x39	32	360Viewer logo
4	branding_bg_str ipes.png	...\images \logos \360viewer	1x100	24	360Viewer header background
5	remediation-strip.png	...\images \logos \remediation	1x100	24	Remediation logo
6	logo_remediatio n.png	...\images \logos \remediation	305x39	32	Remediation header background

Image	File Name	Path	Resolution	Color Depth	Description
7	op.ico	...\images \logos	48x48	32	Website icon (tab icon in browser)

Image 0 (logo_about.png)

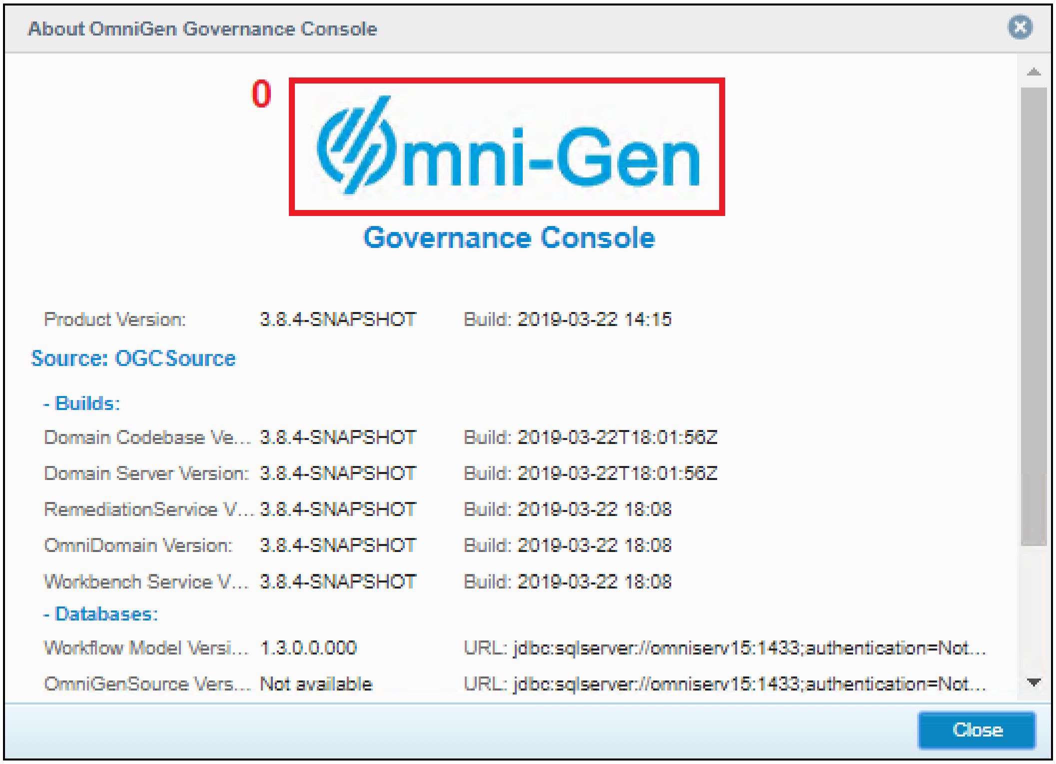


Image 1 (logo_login.png) and Image 2 (logo_login_info.png)

Image 3 (logo_360viewer.png) and Image 4 (branding_bg_stripes.png)

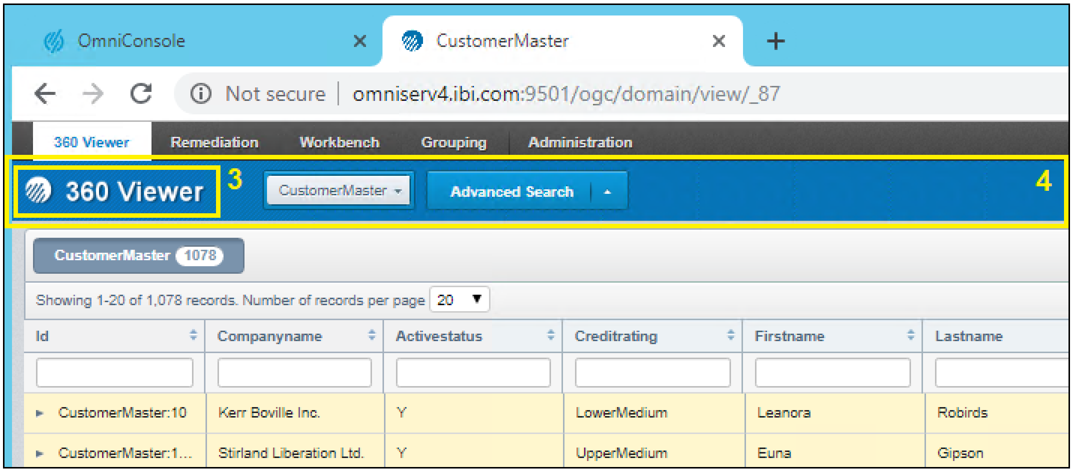


Image 5 (remediation-strip.png) and Image 6 (logo_remediation.png)

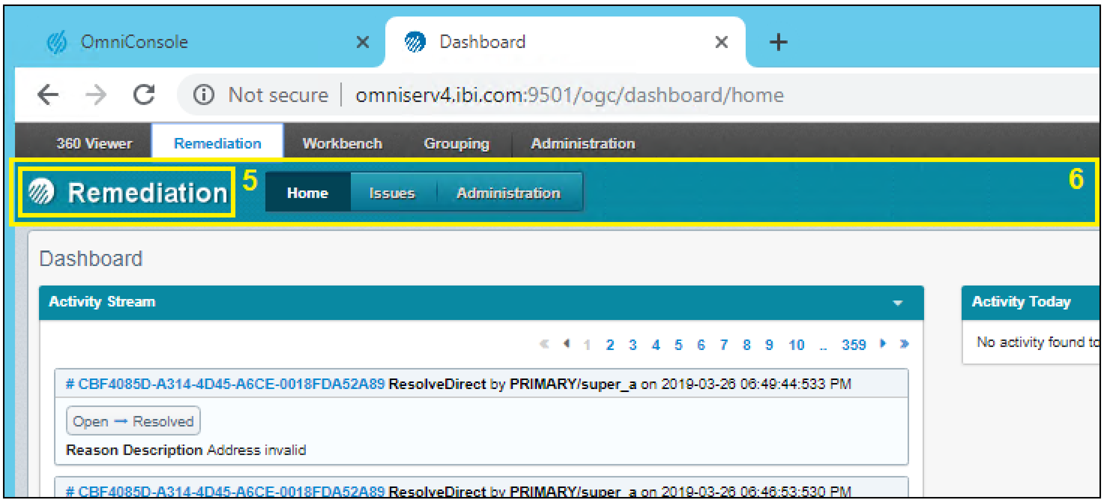
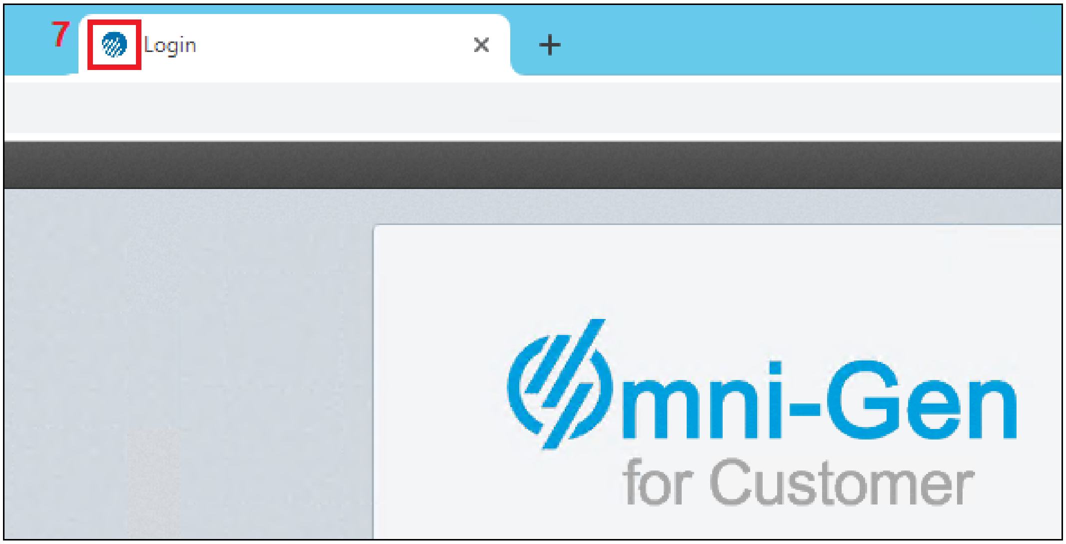


Image 7 (op.ico)



Available Branding Locations

Omni Governance Console (OGC) has screen spaces on several pages where image files are rendered. A collection of these images are stored as a theme in a set of subfolders.

By default, this JNDI location of the set of replaceable images is defined in the *context.xml* file, which is located in the following directory of your OGC installation:

```
\omnigen\omniGenData\OmniGovConsole\data\conf\context.xml
```

The *context.xml* file contains the following entry:

```
<!-- Omni Branding -->
<Environment override="true"
value="C:/omnigen/OmniGenData/OmniGovConsole/data/ogc_theme/"
type="java.lang.String"
name="brandingFolderPath"/>
```

The `brandingFolderPath` points to a set of folders, one folder per page on which there are locations for customizable logos.

If no branding changes are made, then the default OGC theme stored in the above default location is rendered.

Understanding the Placement of Branding Assets

The names of the *ogc_theme* subfolders and the names of the image files are predefined, as per the *Path* values specified in the table in *Image Reference Catalog* on page 158.

Feedback

Customer success is our top priority. Connect with us today!

Information Builders Technical Content Management team is comprised of many talented individuals who work together to design and deliver quality technical documentation products. Your feedback supports our ongoing efforts!

You can also preview new innovations to get an early look at new content products and services. Your participation helps us create great experiences for every customer.

To send us feedback or make a connection, contact Sarah Buccellato, Technical Editor, Technical Content Management at *Sarah_Buccellato@ibi.com.*

To request permission to repurpose copyrighted material, please contact Frances Gambino, Vice President, Technical Content Management at *Frances_Gambino@ibi.com.*

Information Builders

iWay

Omni Governance Console Administration User's Guide

Version 3.2 and Higher

DN3502342.1219

Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898