Syniti Solutions Centralized Security

Migration Manual

BackOffice Associates, LLC, d/b/a Syniti
www.syniti.com
info@syniti.com

Contents

Overview

This document describes how user security is applied in DSP 7.1 and later. Upgrades from versions 7.0.6 or below to 7.1 or above may require changes to a client's security roles.

This document contains the following sections:

- Centralized Security Model Introduction
- Manual Migration vs. Using the Utility
- Manual Migration
- Install and Configure the Centralized Security Migration Utility
- Determine Migration Approach
- Pre-upgrade Steps: Migration Scenario: 1 to 1 Migration
- Post-Upgrade Steps: Migration Scenario: 1 to 1 Migration
- Pre-Upgrade Steps: Migration Scenario: Consolidate
- Post-Upgrade Steps: Migration Scenario: Consolidate

Centralized Security Model Introduction

In DSP releases of 7.0.6 and earlier, an administrator would manage a user's access to application functionality and content from within system administration and the individual applications. For example, to grant a user access to dspCompose, administrative tasks were required in both dspCompose and System Administration. This fragmented approach resulted in these challenges:

- New-user onboarding and change of user access was not efficient.
- Users responsible for user onboarding needed training in all DSP applications that were being used.
- Integration of DSP with third-party identity management tools was limited and, without extensive customization, would still require actions to be performed within DSP.

With the centralized security model introduced with 7.1, a user's access to both application functionality and content is managed in System Administration.

Refer to Set Security for an overview of the updated process.

Role Types Drive User Access

To support this functionality, 7.1 also introduces a Role Type concept. There are three role types:

- **Standard** roles allow access to both application functionality via WebApp Groups AND Content via Security Definition Key Value assignments.
- **Application** roles only allow access to application functionality via WebApp Group assignment.
- **Content** roles only allow access to Content via Security Definition Key Value assignment.

As in previous versions, users are given access to applications through assignment to WebApp groups. In 7.1, users are assigned to WebApp groups directly, or are assigned to a Standard or Application security role that has the WebApp group assigned.

Separate User Provisioning Tasks

Syniti recommends that Application and Content access is provisioned through separate security roles. With 7.1, it is now possible to create security roles that ONLY permit application functionality access to be granted. This will offer the most efficient method by which to maintain security. Users who administer content can be assigned to the System Administration ContentKeySecurity WebApp group. Users who administer application access can be assigned to the System Administration User Management WebApp group.

Security Definitions Restrict Access to Content and Run Rules

Security definitions that restrict access to content and that run rules when certain security-related events occur have been added to the platform. Use a security definition to:

- Assign a key to limit a user's access to content.

NOTE: Security definitions are assigned to Content and Standard security roles. When a user is assigned to a role, the key value(s) assigned to the role's security definition(s) restrict the user's access to that content only.

- Tie rules to events, so that for example, when a user is removed from a security role, the user is removed from associated template roles in dspCompose.

Delivered security definitions cannot be updated, but users can register custom security definitions for custom WebApps. Refer to Delivered Security Definitions and Register Custom Security Definitions for more information.

Automatic Updates to User Access to Content with Security Definition Events

Security definition events provide the capability to assign users to application content that previously required direct application maintenance. When a specific security-related task is performed in DSP, these events run stored procedures that insert, update or delete data specific to a user and piece of application content. For example, when a user is deleted from a security role, the user is also unassigned from the relevant application content items as a result of the security definition event rules.

The DSP is delivered with security definition events. Refer to Delivered Security Definitions for more information.

NOTE: There is no change to the existing security definition functionality that allows security definitions to be assigned to a WebApp page and for the data on the page to be filtered based upon the user Security Definition Key value assignments.

New WebApp Groups

The following WebApp groups have been added. For a complete list of delivered WebApp Groups, refer to Delivered WebApp Groups.

WebApp	WebApp Group
Assemble	• **PowerUserLite** — Enables users to create, change, delete and execute CranPort Packages. Users cannot change any Assemble configuration-related settings. • **ExecutionOnly** — Enables users to execute CranPort packages only, not to create or edit them.
Automate	• **PowerUserLite** — Enables users to add tables to Target Sources and to build and run packages. • **ExecutionOnly** — Enables users to execute Automate Interfaces only. Users cannot create or edit them.
Common	• **AdvancedDeveloper** — Intended to be used for Migration Advanced Developers. It enables users to maintain module-specific settings, maintain data sources, and add automation engine tasks. • **AnalyzeLite** — Enables users to execute profiling, tracing and duplicate detection activities. • **UserCredentials** — Designed to be used by Integrate Roles, allowing users to maintain their user-specific application credentials.
dspConduct™	• **UserManager** — Access to the *User Settings* page in dspConduct to update a user's workflow notification settings and back up user information.
Integrate	• **ExecutionOnly** — Ability to post in Integrate, but not to activate or deactivate templates or processes.
Map	• **FieldAndValueMapper** — Enables users to maintain Field and Value Mapping. Intended for use by non-migration developer resources who are responsible for documenting mappings requirements. • **PowerUserLite** — Enables users to perform all Field and Value Mapping activities needed to build a data object end to end. It's recommended for use by Migration Developers. Users with this Group cannot change any Map configuration-related settings.
System Administration	• **ContentKeySecurity** — Provides restricted access to a type of security user, usually a SME or Data Steward, that can: o Create security roles with a Role Type of Content and o Assign security definition key values to users, and to security roles with Role Types of Standard and Content • **DesignerPlus** — Provides experienced DSP users with access to some advanced System Admin setup and configuration tasks. • **JobMonitoring** — Provides users with comprehensive access to DSP Monitoring pages. • **UserManagement** — Provides restricted access to security, only allowing access to the pages used to create users and assign them to roles.

Target Design	• **PowerUserLite** — Enables users to perform all Data Design activities needed to build a data object end to end. It's recommended for use by Migration Developers. Users cannot change any Console or Target Design configuration-related settings and cannot create Waves, Process Areas, or Objects.
Transform	• **ExecutionOnly** — Designed to be used by: o A user whose role is to only process data objects or o Users that are running migration load cycles from within non-development environments. Users in this WebApp group can: • Execute Objects, Targets, Sources, Rules and Reports • Publish / Unpublish Objects / Targets / Sources and Reports • Segment Reports • Assign users to reports or report segments.

New Security Roles

- The following security roles have been added to the platform:
  - **Governance Business User—**users assigned this role can be added to WebApp groups that allow them to submit requests and process roles in dspCompose and dspConduct and to receive reports and remediate failures with dspMonitor. Users with the Governance Business User have access to all DSP Data Governance Application functionality intended for use by end users. Depending upon which applications are in scope for a project, this role will need to be tailored to meet project requirements.
  - **Governance Developer—**users assigned this role can be added to WebApp groups that allow them to register data sources, add system types, configure templates, and perform other development and configuration tasks in Collect, Common, Construct, Assemble, dspCompose, dspConduct, dspMonitor, Integrate, Sys Admin. Users with the Governance Developer role have PowerUser access across all the DSP Data Governance Applications and most shared cross application components (Common, Collect and Integrate). They also have wide access to System Administration functionality. They do not have access to maintain DSP Security. Depending upon which applications are in scope for a project, this role will need to be tailored to meet project requirements.
  - **Migration Business User—**users assigned this role can be added to WebApp groups that allow them to maintain data design and field / value mapping. They should also be able to view the migration reports to which they have been assigned.
  - **Migration Developer Advanced—**users assigned this role can be added to WebApp groups that allow them to have access to all waves, process areas, objects, targets and sources and can set up security for dspMigrate. Users with the Migration Developer Advanced role are senior resources on a project and are responsible for not only designing, developing and executing data objects from start to finish, but also for troubleshooting, supporting other

consultants and managing some platform level settings that control DSP's behavior. Users with this access must have a deep understanding of the DSP platform and associated implementation methodology.

- **Migration Developer Lite**—users assigned this role can be added to WebApp groups that allow them to configure dspMigrate but cannot set up security. Users with the Migration Developer Lite role are developers on a project that are responsible for designing, developing and executing data objects from start to finish. This role should permit them to perform all tasks required to design, build and execute the data objects they are responsible for. Users assigned this role should have limited access to any setup / configuration areas of DSP, including Console where they are not permitted to alter the Wave setup, because such changes impact project scope and should be determined by the project lead.
- **Migration Executer**—users assigned this role can be added to WebApp groups that allow them to have limited access to perform tasks within a designated wave and process area. Users with the Migration Executer role can view data design, field/value mappings and execute Transform / Integrate processes. This role is intended for use on projects that have a multi-tier DSP environment where changes made in the development environment are transported into the Quality / Production instances. This role is also intended for use by projects that have a team that is responsible solely for executing the migration process.
- **Security Administrator**—users assigned this role can be added to WebApp groups that allow them to either manage security and users or manage DSP Add-ons. Users with the Security Administrator role can maintain all aspects of the DSP security layer. They can create roles, security definitions and custom WebApp groups. They can also create users and assign them roles. This is a privileged role and must be assigned to only a few select users.

- The *Security Role Compare* page has been added so that users can compare security roles to determine the groups and pages to which certain security roles have access. Refer to Compare Security Roles for more information.

Refer to Set Security for an overview of the updated process.

Security Reports

- User Security reports have been added to System Administration to provide details about how centralized security is configured, including:
  - All users in the platform
  - All security roles in the platform
  - WebApp Groups assigned to security roles
  - The pages and content security roles can access
  - The pages and content users can access
  - Security roles assigned to users
  - The Security Administration Reconciliation with Governance Applications report has been added to show instances where a user's security is out of sync between a WebApp and security settings set in System Administration. The report compares a user's access to dspConduct Positions, dspMonitor Groups and dspCompose Template Roles within the

individual applications with the expected access based upon user assignment to security roles that have associated Security Definition Key Values and User Specific Security Definition Key Values. Refer to Compare User Access to Content Between WebApps and System Administration for more information.

For an overview of security changes for these applications, watch the following videos.

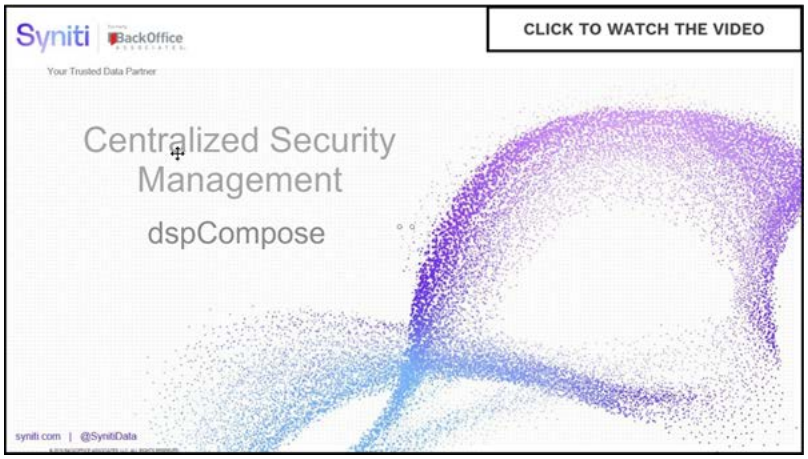
- Changes to dspConduct Positions for 7.1 and later

Syniti | BackOffice ASSOCIATES
Your Trusted Data Partner
CLICK TO WATCH THE VIDEO
Centralized Security Management
dspConduct
syniti.com | @SynitiData

- Changes to dspMonitor Groups for 7.1 and later

Syniti | BackOffice ASSOCIATES
Your Trusted Data Partner
CLICK TO WATCH THE VIDEO
Centralized Security Management
dspMonitor
syniti.com | @SynitiData

- Changes to dspCompose Template Roles for 7.1 and later



As a result of these changes, user assignment to and removal from the items indicated above is no longer performed in native applications. Instead, users must be granted access to these items via Content Roles or via direct assignment to users using User Specific Security Definitions.

When upgrading from DSP 7.0.6 or below to DSP 7.1 or above, clients need to be aware of the changes to the DSP application security model to do the following: -

- Define Content Role structure needed to support ongoing User Management activities
- Change operational processes in such a way that User access to the application content above is managed via Content Roles or User Specific Security Definitions.
- Migrate Application Content

Manual Migration vs. Using the Utility

For small installations with a low number of different application content items, the migration can be done manually. There is no need to install the Centralized Security Migration Utility. Refer to *Manual Migration* for more information

For larger installations, the Centralized Security Migration Utility as defined in this User Guide can be used to support the migration. This application is installed BEFORE the system is upgraded to DSP 7.1 (or above). This will allow detailed analysis and planning of the future security setup. The tasks to be performed before the upgrade are included in the Pre-upgrade Steps sections. Tasks to be performed after the upgrade are included in the Post-upgrade Steps sections. Refer to *Install and Configure the Centralized Security Migration Utility* for more information.

Manual Migration

Watch the Central Security Manual Migration video.

After upgrading to 7.1 or above, review the security content you currently have in your system.

Select **Admin** > **Security** > **Security Management** > **User Security Report**s and click the **Security Reconciliation in Governanc**e link to access the _Security Administration Reconciliation with Governance Applications_ report.

Use this report to analyze the current content that is found within the various applications. The report displays the WebApp, the details about the content, and the user assigned to it.

The Status column indicates whether content is found within the application, but does not exist in System Administration, which means that it's not found within the central security model in the DSP.

To allow the users access to the content, follow the steps as outlined in the online help below. Create all security roles needed to support current assignments.

1. Create a security role with the Type of Content manually.
2. Assign Security Definition Keys to the security role.
3. Assign Users to the Security Role.

Refer to Set Security for more information.

Install and Configure the Centralized Security Migration Utility

Install the Utility BEFORE upgrading to DSP 7.1 or above.

Download the Utility

The Centralized Security Migration Application is obtained by opening a support ticket at support.boaweb.com and requesting a download link.

Install Utility

Perform the following steps to install the Utility:

1. Unzip the file **CENTRAL_SECURITY_MIGRATION_UTILITY.zip**.
2. Navigate to the folder **CENTRAL_SECURITY_MIGRATION_UTILITY\Databases.**
3. Copy the following folders:
   - **Apps**
   - **Install**
4. Paste them into the DSP Databases folder that is located within the DSP installation directory (for example, C:\Program Files (x86)\BOA\DSP\Databases).
5. Navigate to the folder **\BOA\DSP\Databases\Install**
6. Run the following .bat file **INSTALL_PKG_CENTRAL_SECURITY_MIGRATION_UTILITY.bat.**

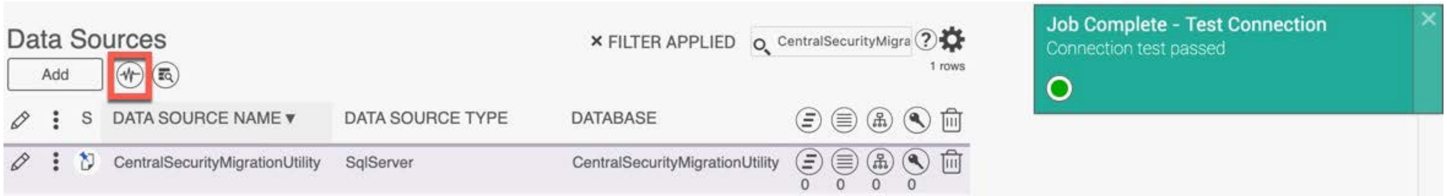
Set Up the Utility

Once the Utility has been installed, the following steps must be performed before the utility can be used. These steps must be performed in the DSP by an Administrator:

1. Update Data Source Credentials
2. Add Utility to DSP Site Menu
3. Add Users to WebApp

Update Data Source Credentials

1. Select **Admin** > **Data Sources** in the *Navigation* pane.
2. Click **Vertical View** for the Data Source **CentralSecurityMigrationUtility**.
3. Update the following fields:
   - Server Address
   - User ID
   - Password
4. Click **Save**.
5. Click the **Test Connection** icon in the Page toolbar.

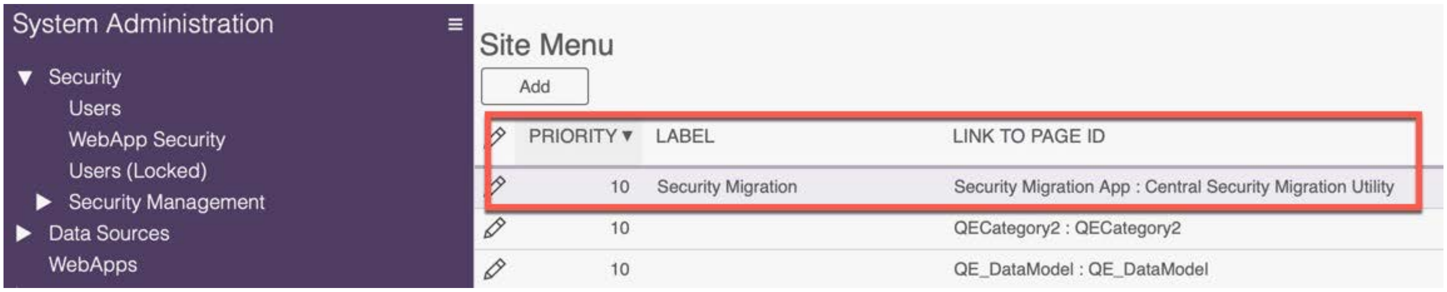


S	DATA SOURCE NAME ▾	DATA SOURCE TYPE	DATABASE
	CentralSecurityMigrationUtility	SqlServer	CentralSecurityMigrationUtility

Job Complete - Test Connection
Connection test passed

Add Utility to DSP Site Menu

1. Select **Admin** > **Configuration** > **Site Menu** in the *Navigation* pane.
2. Add the Security Migration Utility home page to the site menu.

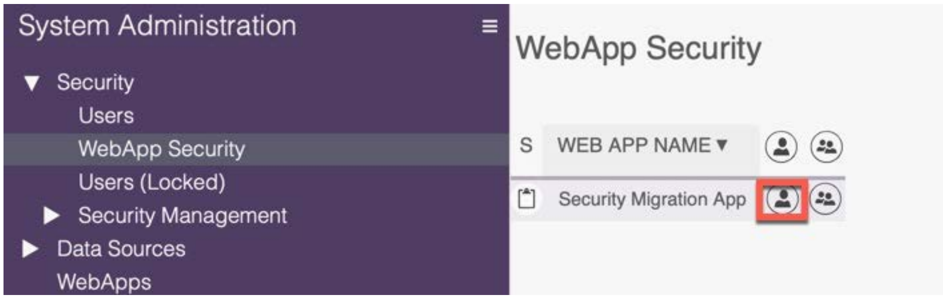


PRIORITY ▾	LABEL	LINK TO PAGE ID
10	Security Migration	Security Migration App : Central Security Migration Utility
10		QECategory2 : QECategory2
10		QE_DataModel : QE_DataModel

Add Users to WebApp

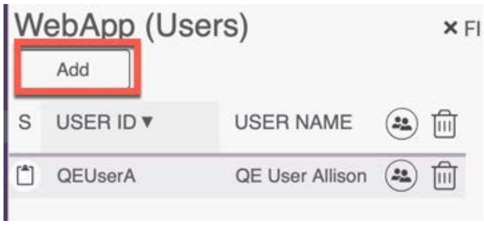
By default, the DSP Administrator user has access to the Security Migration App. If other users require access to perform the migration to centralized security, they must be added to the WebApp and associated WebApp groups.

1. Select **Admin** > **Security** > **WebApp Security** in the *Navigation* pane.
2. Click the **Users** icon for the **Security Migration App**.



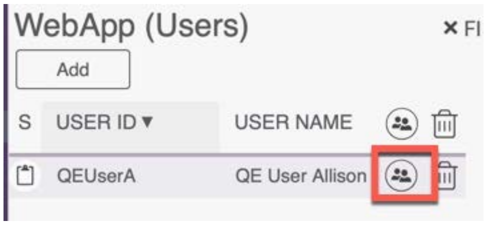
S	WEB APP NAME ▾
	Security Migration App

3. Select the user and click the **Add** button.

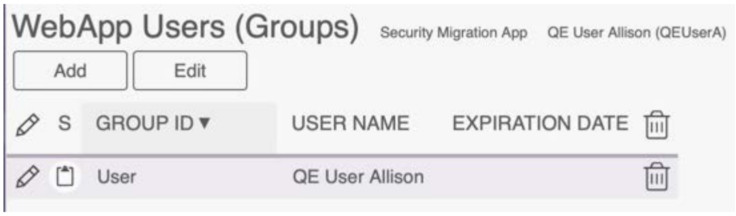


S	USER ID ▾	USER NAME
	QEUserA	QE User Allison

Then assign the user to the **User** WebApp Group.



S	USER ID ▾	USER NAME
	QEUserA	QE User Allison



WebApp Users (Groups) Security Migration App QE User Allison (QEUserA)

S	GROUP ID ▼	USER NAME	EXPIRATION DATE
	User	QE User Allison	

NOTE: After completing these steps, if you do not see the Security Migration link on the site menu, either log out of the DSP and log back in or clear cache.

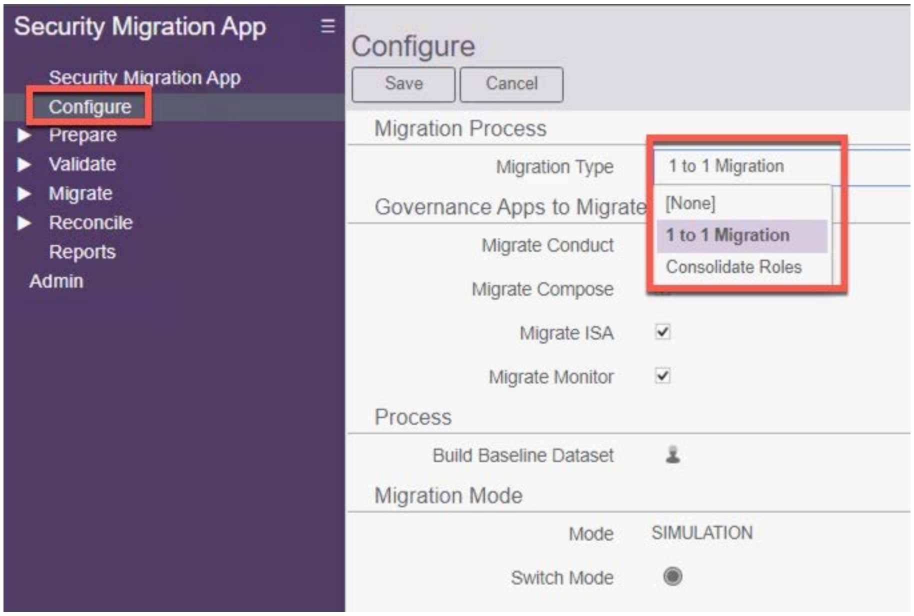
Determine Migration Approach

Watch the Security Migration Application Overview video:

CLICK TO WATCH THE VIDEO
Syniti BackOffice
Your Trusted Data Partner
Syniti eLearning
Security Migration Application Overview

The Central Security Migration Utility has been designed to support 2 scenarios:

1. Lift and Shift -> Migration Type ‘1 : 1 Migration’
2. Consolidate -> Migration Type ‘Consolidate Roles’



Migration Process

Migration Type: 1 to 1 Migration

Governance Apps to Migrate

Migrate Conduct

Migrate Compose

Migrate ISA ☑

Migrate Monitor ☑

Process

Build Baseline Dataset

Migration Mode

Mode: SIMULATION

Switch Mode ●

Scenario 1: Lift and Shift

This scenario is designed to create a 1:1 relationship between DSP Content Role and Governance Application content item. It then assigns users to the Content Roles based upon the user assignment to content within each governance application. This approach is the simplest and will result in a DSP instance's Security being fully aligned to each Governance Application. After the migration, day to day business will need to resume based upon usage of the new Centralized Security Model. Refer to Set Security in the online help for more information.

To use this method, start with *Pre-Upgrade Steps: Migration Scenario: 1 to 1 Migration.*

Scenario 2: Consolidate

In this scenario, analysis of Governance Content is done to determine the most efficient Content Role setup for future user management. For example, a Content Role that contains 1 Conduct Position, 10 Compose Template Roles and 1 Monitor Group could be created. A user could then be assigned to this Role and be automatically assigned to the content in all these governance applications.

Once a Content Security Model has been designed, new Custom Content Roles can be created. Existing Governance Content can then be mapped to the Custom Content Roles and decisions about user assignment to the roles made. After the migration, day to day business will need to resume based upon usage of the new Centralized Security Model. Refer to Set Security in the online help for more information.

To use this method, start with *Pre-Upgrade Steps: Migration Scenario: Consolidate*.

Pre-Upgrade Steps: Migration Scenario: 1 to 1 Migration

The tasks in this section must be performed BEFORE upgrading to 7.1.

1. Select Migration Scope
2. Build Dataset from Applications
3. Review Current Governance Content and User Access
4. Prepare Final Role Dataset
5. Validate Role Data Before Migration
6. Upgrade DSP

Watch the Central Security Migration Application One to One video for a demonstration of the steps in this section.

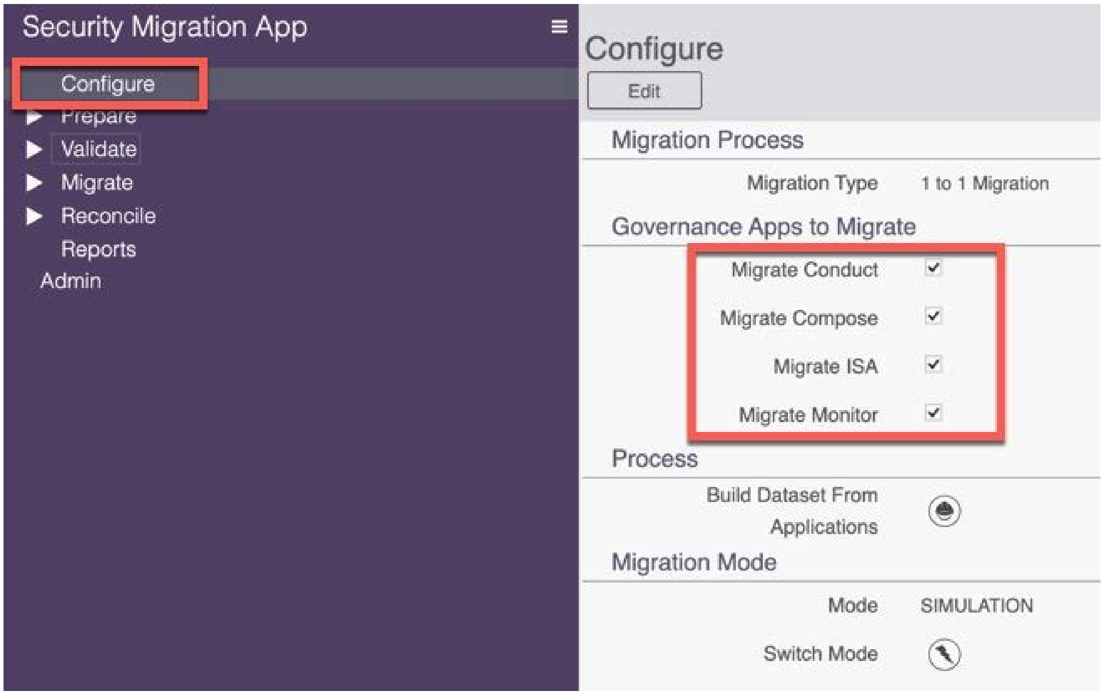
Step 1: Select Migration Scope

The migration to the Centralized Security Model impacts customers that use the following the DSP Solutions and associated content: -

- dspConduct
  - Positions
- dspMonitor
  - Groups
- dspCompose
  - Template Roles

From the configuration menu, select the applications to migrate to the Centralized Security Model.

NOTE: All DSP Solutions will adopt the new security model when upgrading to DSP 7.1 or above. The selections made here relate to the automatic migration of data to the new security model.



Migration Type 1 to 1 Migration

Migrate Conduct ☑

Migrate Compose ☑

Migrate ISA ☑

Migrate Monitor ☑

Mode SIMULATION

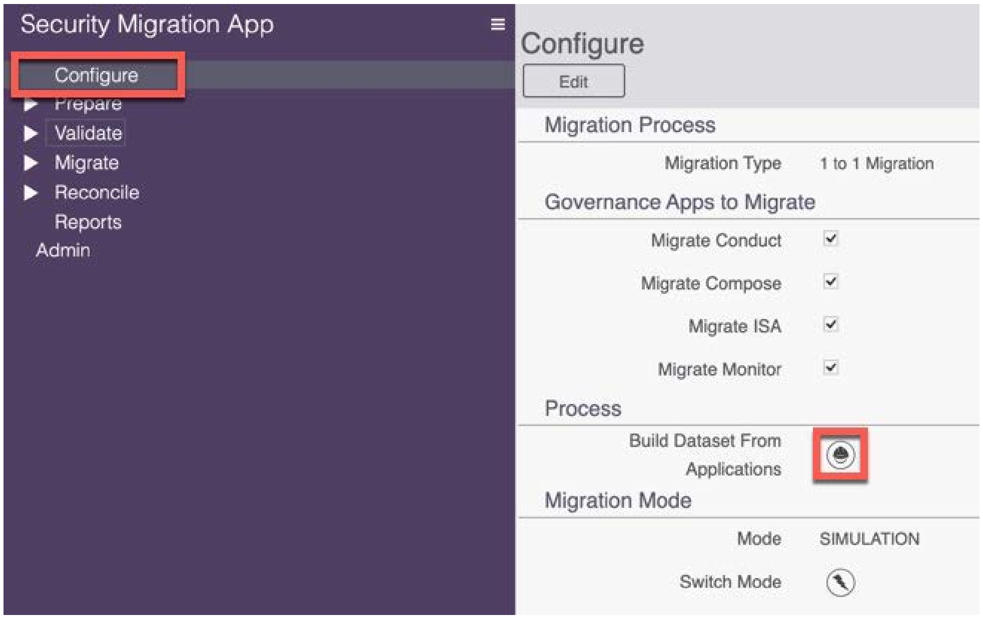
Step 2: Build Dataset From Applications

Set the **Migration Type** to **1 to 1 Migration** and click the **Build Dataset From Applications** button.

This runs a stored procedure that creates (within the Utility Staging Area, not in DSP) a single Content Role for every piece of content associated with applications selected in the previous step. This step also assigns the users assigned to the content to these roles.

Staging tables within the database CentralSecurityMigrationUtility:

- BaselineContentRoles
- BaselineContentRoleUsers



Configure

Migration Process

Migration Type: 1 to 1 Migration

Governance Apps to Migrate

Migrate Conduct ☑

Migrate Compose ☑

Migrate ISA ☑

Migrate Monitor ☑

Process

Build Dataset From Applications

Migration Mode

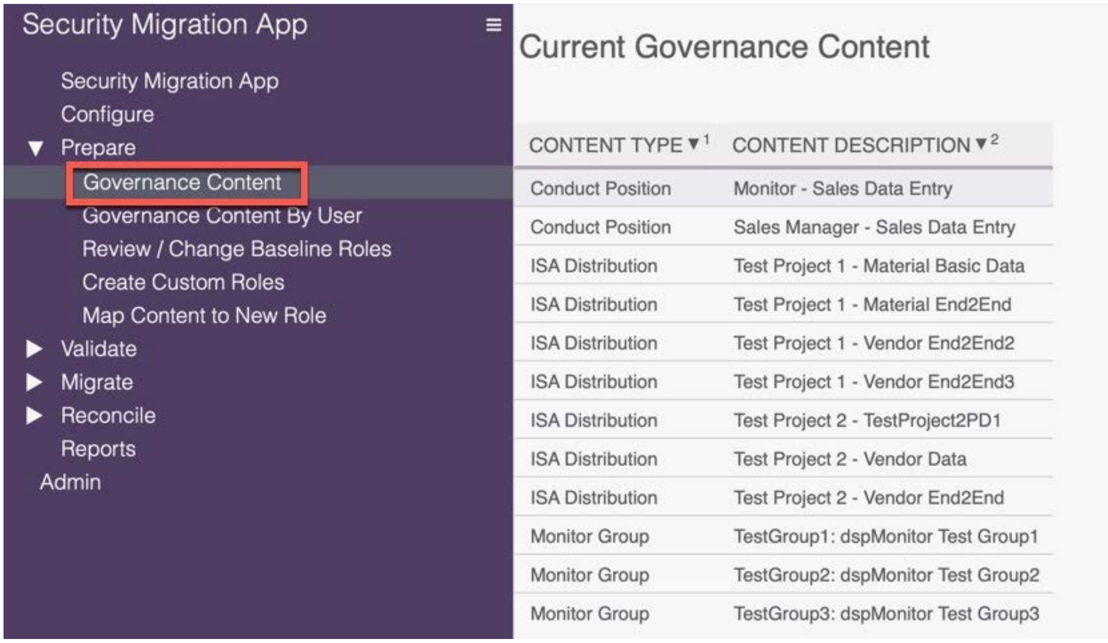
Mode: SIMULATION

Switch Mode

Step 3 Review Current Governance Content and User Access

In the Security Migration App, under the ‘Prepare’ Menu, review 2 reports to validate that the staged data contains the Content and User Content assignment that you’re expecting to migrate.

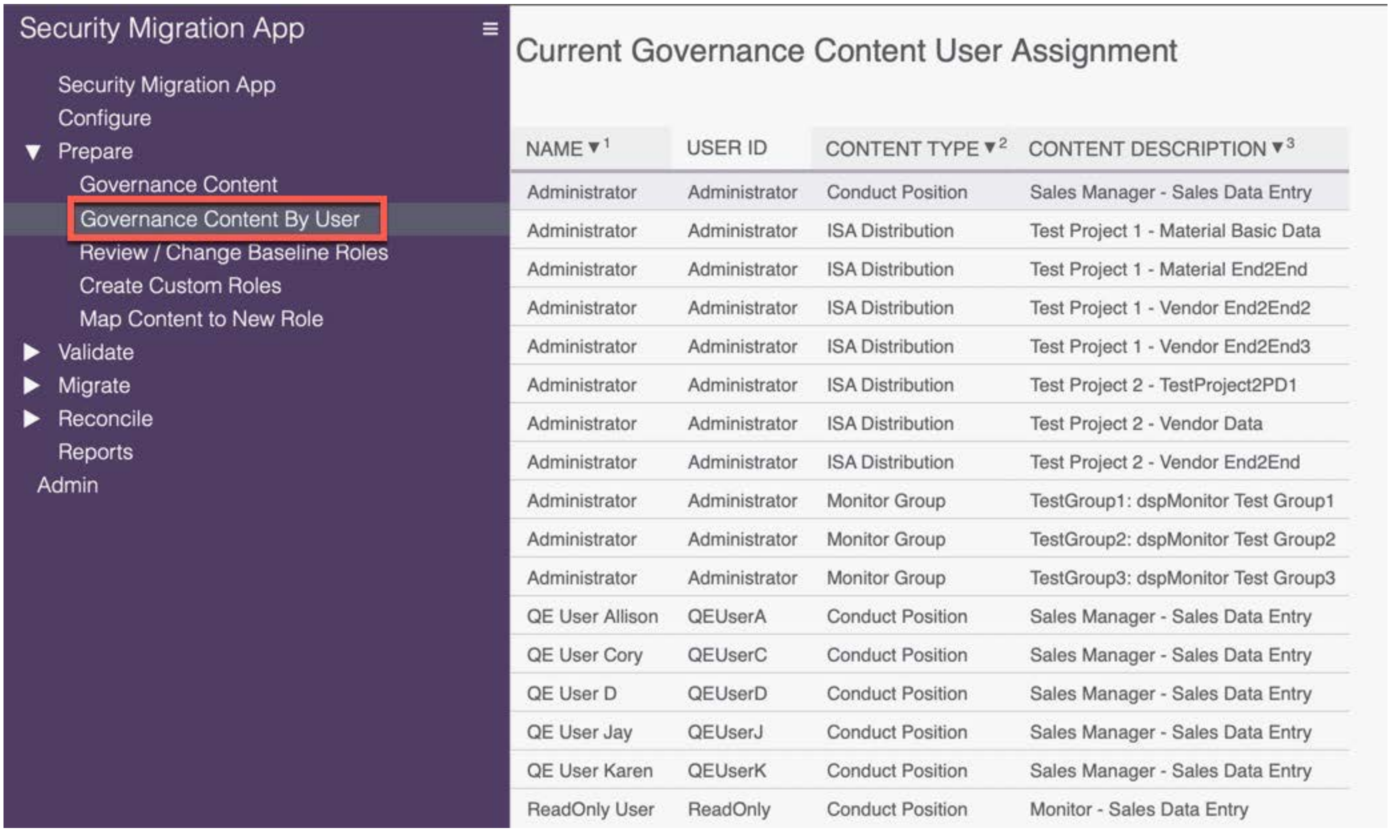
Select *Prepare > Governance Content* to view the Current Governance Content report, which shows all the content to be migrated to the new Content Roles.



Current Governance Content

CONTENT TYPE ▼1	CONTENT DESCRIPTION ▼2
Conduct Position	Monitor - Sales Data Entry
Conduct Position	Sales Manager - Sales Data Entry
ISA Distribution	Test Project 1 - Material Basic Data
ISA Distribution	Test Project 1 - Material End2End
ISA Distribution	Test Project 1 - Vendor End2End2
ISA Distribution	Test Project 1 - Vendor End2End3
ISA Distribution	Test Project 2 - TestProject2PD1
ISA Distribution	Test Project 2 - Vendor Data
ISA Distribution	Test Project 2 - Vendor End2End
Monitor Group	TestGroup1: dspMonitor Test Group1
Monitor Group	TestGroup2: dspMonitor Test Group2
Monitor Group	TestGroup3: dspMonitor Test Group3

Select Prepare > Governance Content By User to view the Current Governance Content User Assignment report, which shows all the User to Content assignments that currently exist within your DSP application and that will be migrated to the new Content Roles.



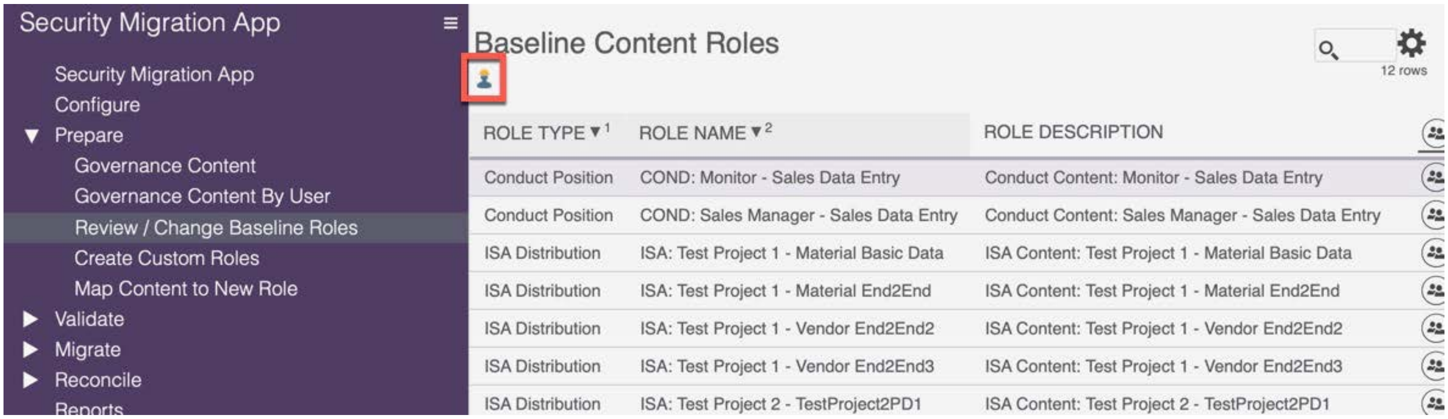
Current Governance Content User Assignment

NAME ▾ 1	USER ID	CONTENT TYPE ▾ 2	CONTENT DESCRIPTION ▾ 3
Administrator	Administrator	Conduct Position	Sales Manager - Sales Data Entry
Administrator	Administrator	ISA Distribution	Test Project 1 - Material Basic Data
Administrator	Administrator	ISA Distribution	Test Project 1 - Material End2End
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End2
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End3
Administrator	Administrator	ISA Distribution	Test Project 2 - TestProject2PD1
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor Data
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor End2End
Administrator	Administrator	Monitor Group	TestGroup1: dspMonitor Test Group1
Administrator	Administrator	Monitor Group	TestGroup2: dspMonitor Test Group2
Administrator	Administrator	Monitor Group	TestGroup3: dspMonitor Test Group3
QE User Allison	QEUserA	Conduct Position	Sales Manager - Sales Data Entry
QE User Cory	QEUserC	Conduct Position	Sales Manager - Sales Data Entry
QE User D	QEUserD	Conduct Position	Sales Manager - Sales Data Entry
QE User Jay	QEUserJ	Conduct Position	Sales Manager - Sales Data Entry
QE User Karen	QEUserK	Conduct Position	Sales Manager - Sales Data Entry
ReadOnly User	ReadOnly	Conduct Position	Monitor - Sales Data Entry

Step 4 Prepare Final Role Dataset

1. Select **Prepare** > **Review/Change Baseline Roles** in the *Navigation* pane to navigate to the *Baseline Content Roles* page.

2. Click the **Prepare Final Roles** button to transform the baseline role data into the format required for migration into DSP.

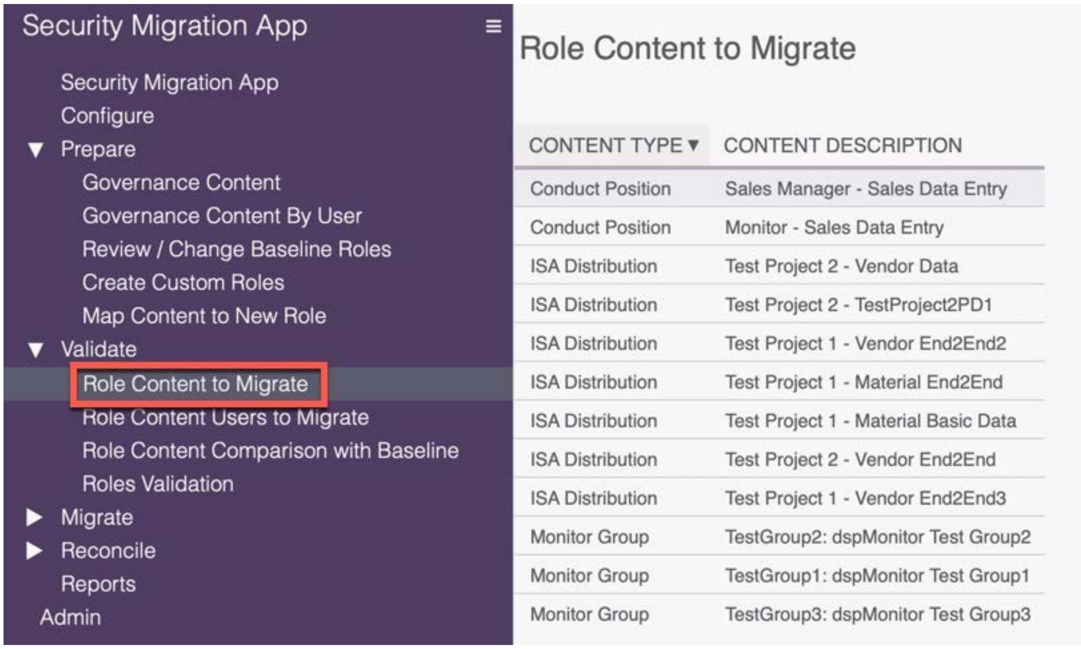


Baseline Content Roles

ROLE TYPE ▾ 1	ROLE NAME ▾ 2	ROLE DESCRIPTION
Conduct Position	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry
Conduct Position	COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry
ISA Distribution	ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data
ISA Distribution	ISA: Test Project 1 - Material End2End	ISA Content: Test Project 1 - Material End2End
ISA Distribution	ISA: Test Project 1 - Vendor End2End2	ISA Content: Test Project 1 - Vendor End2End2
ISA Distribution	ISA: Test Project 1 - Vendor End2End3	ISA Content: Test Project 1 - Vendor End2End3
ISA Distribution	ISA: Test Project 2 - TestProject2PD1	ISA Content: Test Project 2 - TestProject2PD1

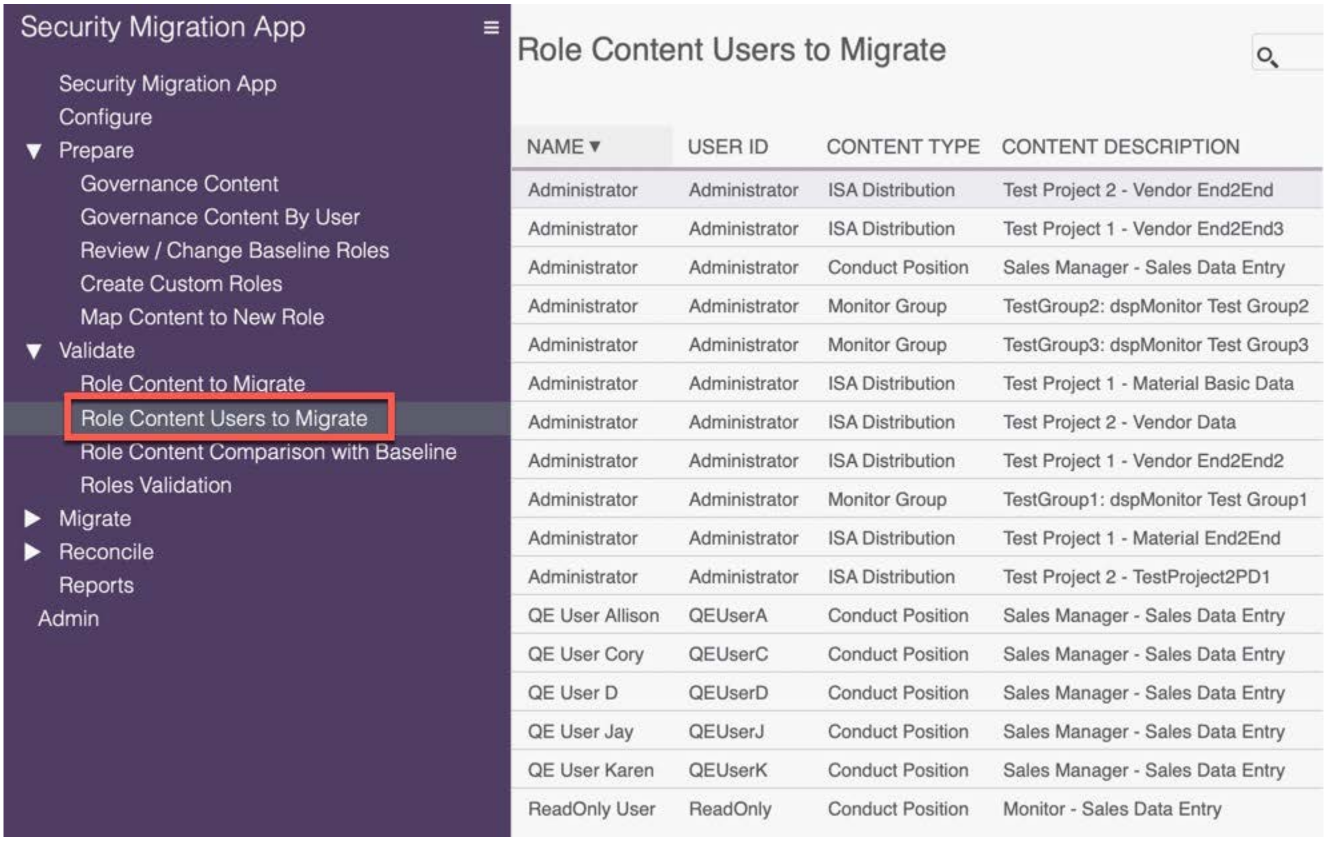
Step 5 Validate Role Data Before Migration

The details of the Roles / Content and users to migrate can be reviewed in the following reports, located under the 'Validate' menu:



Role Content to Migrate

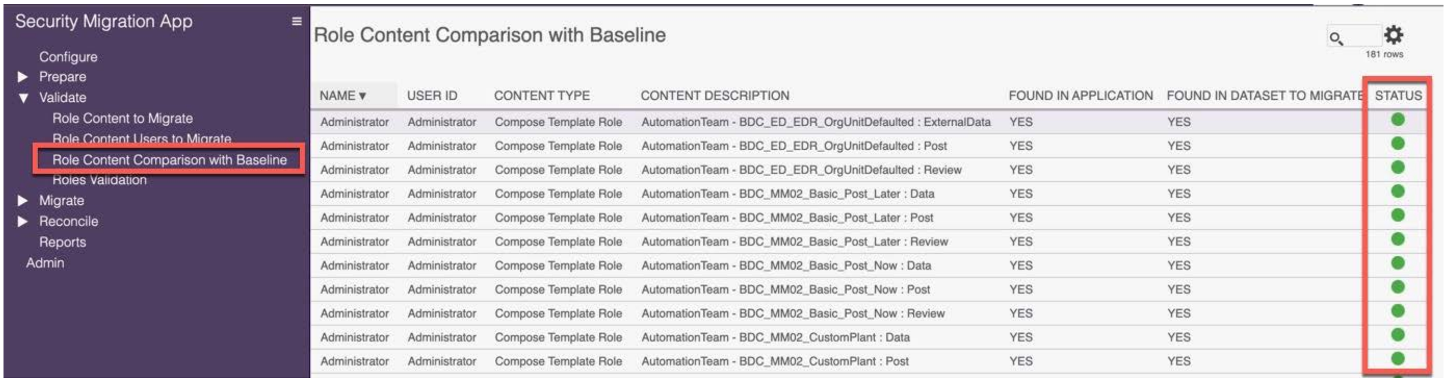
CONTENT TYPE ▾	CONTENT DESCRIPTION
Conduct Position	Sales Manager - Sales Data Entry
Conduct Position	Monitor - Sales Data Entry
ISA Distribution	Test Project 2 - Vendor Data
ISA Distribution	Test Project 2 - TestProject2PD1
ISA Distribution	Test Project 1 - Vendor End2End2
ISA Distribution	Test Project 1 - Material End2End
ISA Distribution	Test Project 1 - Material Basic Data
ISA Distribution	Test Project 2 - Vendor End2End
ISA Distribution	Test Project 1 - Vendor End2End3
Monitor Group	TestGroup2: dspMonitor Test Group2
Monitor Group	TestGroup1: dspMonitor Test Group1
Monitor Group	TestGroup3: dspMonitor Test Group3



Role Content Users to Migrate

NAME ▾	USER ID	CONTENT TYPE	CONTENT DESCRIPTION
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor End2End
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End3
Administrator	Administrator	Conduct Position	Sales Manager - Sales Data Entry
Administrator	Administrator	Monitor Group	TestGroup2: dspMonitor Test Group2
Administrator	Administrator	Monitor Group	TestGroup3: dspMonitor Test Group3
Administrator	Administrator	ISA Distribution	Test Project 1 - Material Basic Data
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor Data
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End2
Administrator	Administrator	Monitor Group	TestGroup1: dspMonitor Test Group1
Administrator	Administrator	ISA Distribution	Test Project 1 - Material End2End
Administrator	Administrator	ISA Distribution	Test Project 2 - TestProject2PD1
QE User Allison	QEUserA	Conduct Position	Sales Manager - Sales Data Entry
QE User Cory	QEUserC	Conduct Position	Sales Manager - Sales Data Entry
QE User D	QEUserD	Conduct Position	Sales Manager - Sales Data Entry
QE User Jay	QEUserJ	Conduct Position	Sales Manager - Sales Data Entry
QE User Karen	QEUserK	Conduct Position	Sales Manager - Sales Data Entry
ReadOnly User	ReadOnly	Conduct Position	Monitor - Sales Data Entry

In the 1 : 1 migration scenario, the comparison of what is proposed to be migrated compared to the applications current status should be the same as there is no consolidation of roles being done.



Role Content Comparison with Baseline

181 rows

NAME ▾	USER ID	CONTENT TYPE	CONTENT DESCRIPTION	FOUND IN APPLICATION	FOUND IN DATASET TO MIGRATE	STATUS
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_ED_EDR_OrgUnitDefaulted : ExternalData	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_ED_EDR_OrgUnitDefaulted : Post	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_ED_EDR_OrgUnitDefaulted : Review	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Later : Data	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Later : Post	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Later : Review	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Now : Data	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Now : Post	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Now : Review	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_CustomPlant : Data	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_CustomPlant : Post	YES	YES	●

Step 6 Upgrade DSP

After the steps in this section are completed, DSP can be upgraded to version 7.1 or above.

Post-Upgrade Steps: Migration Scenario: 1 to 1 Migration

These second set of steps must be performed AFTER the update to 7.1 to complete the migration to centralized security.

7. Synchronize Security Definition Keys
8. Change Migration Mode to Live
9. Validate the Roles
10. Migrate the Roles
11. Assign Users to Roles
12. Review Migration Status
13. Reconcile System Admin Security with Application Security

Step 7 Synchronize Security Definition Keys

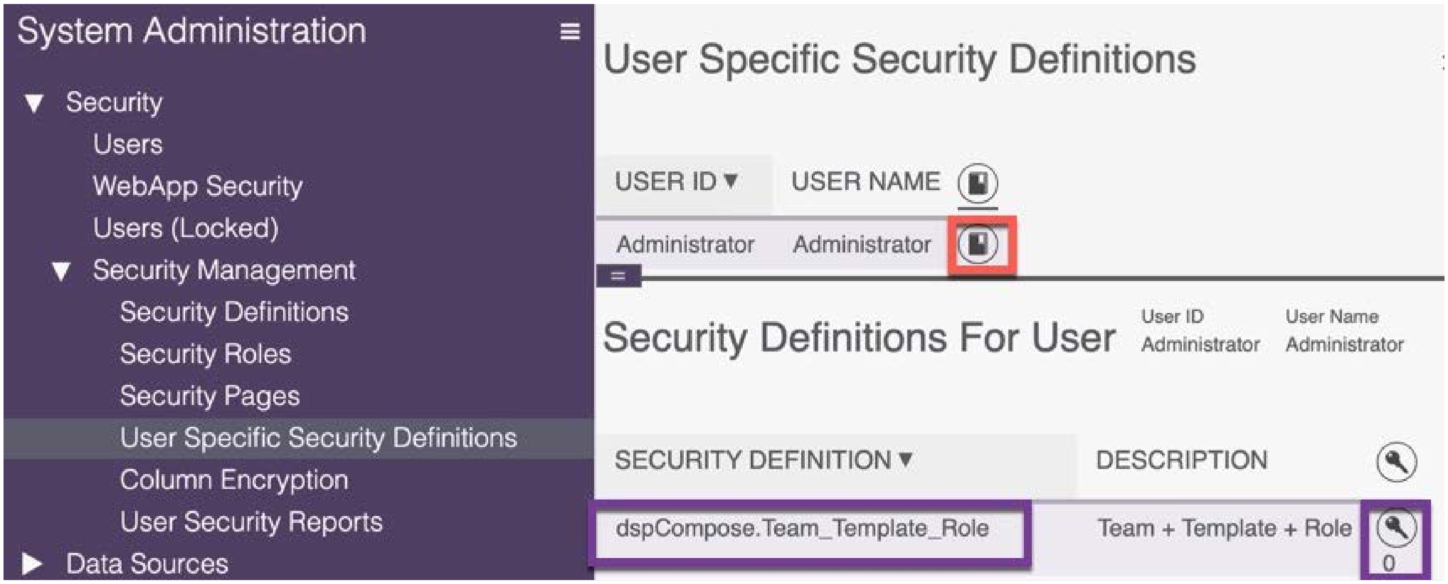
In order to seed the new Security Definitions with the data from each application, a DSP administrator must:

1. Log in to DSP.
2. Select **Admin** > **Security** > **Security Management** > **User Specific Security Definitions** in the *Navigation* pane.
3. Click the **Definitions** icon for the Administrator user.
4. Perform the following, depending on the application security that is being migrated to central security:

NOTE: Opening the *User Specific Keys* page as described in the following sections runs a plugin that synchronizes the DSP security tables with each individual application.

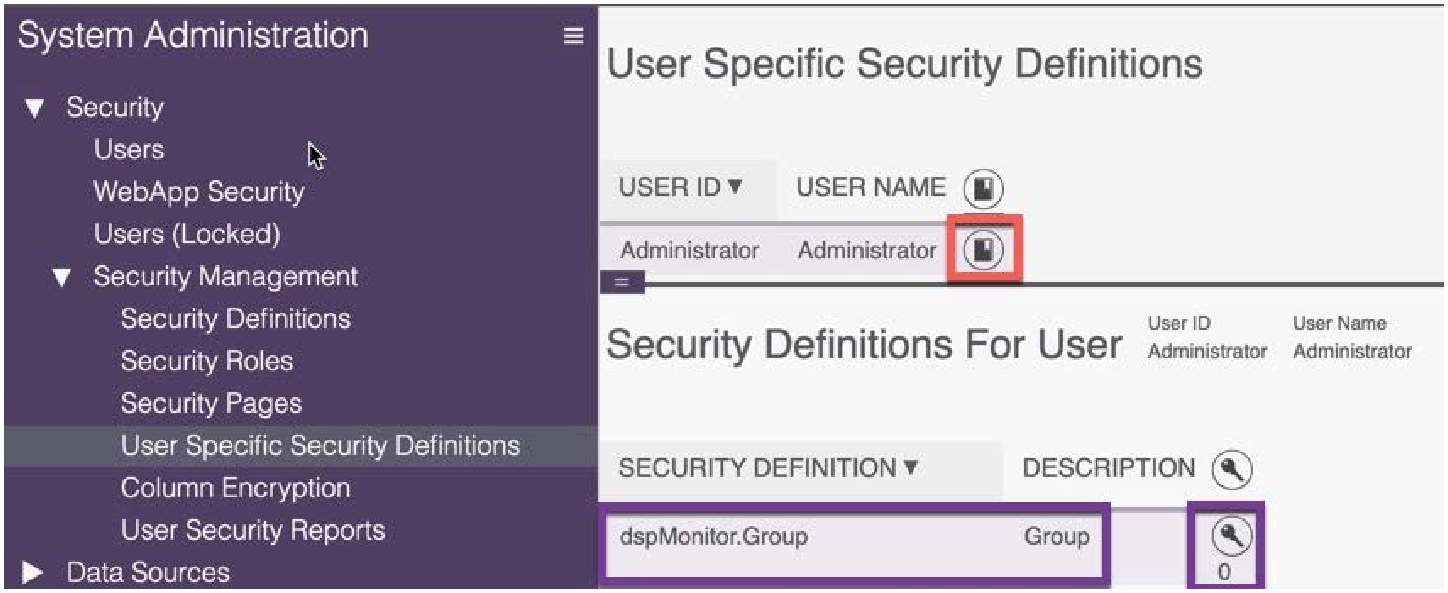
Synchronize dspCompose

Click the **Keys** icon for the **dspCompose.Team_Template_Role** security definition on the *Security Definitions for User* page.



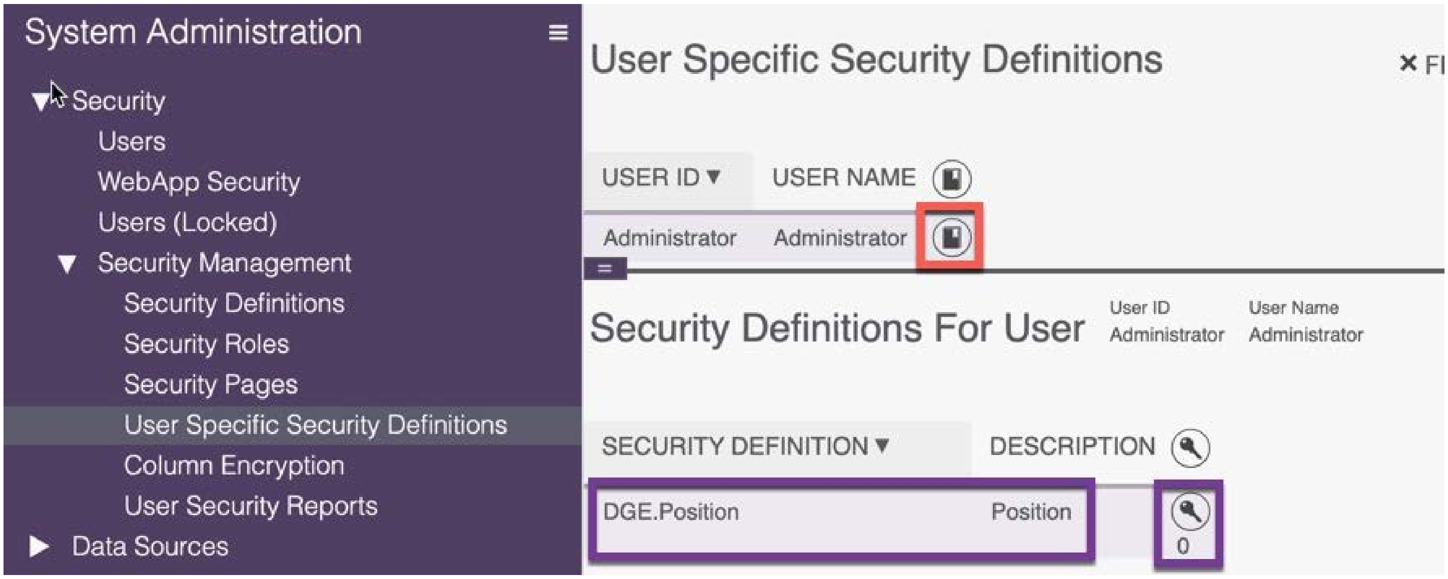
Synchronize dspMonitor

Click the **Keys** icon for the **dspMonitor.Group** security definition on the *Security Definitions for User* page.



Synchronize dspConduct

Click the **Keys** icon for the **DGEPosition** security definition on the *Security Definitions for User* page.



User Specific Security Definitions

USER ID ▼	USER NAME
Administrator	Administrator

Security Definitions For User

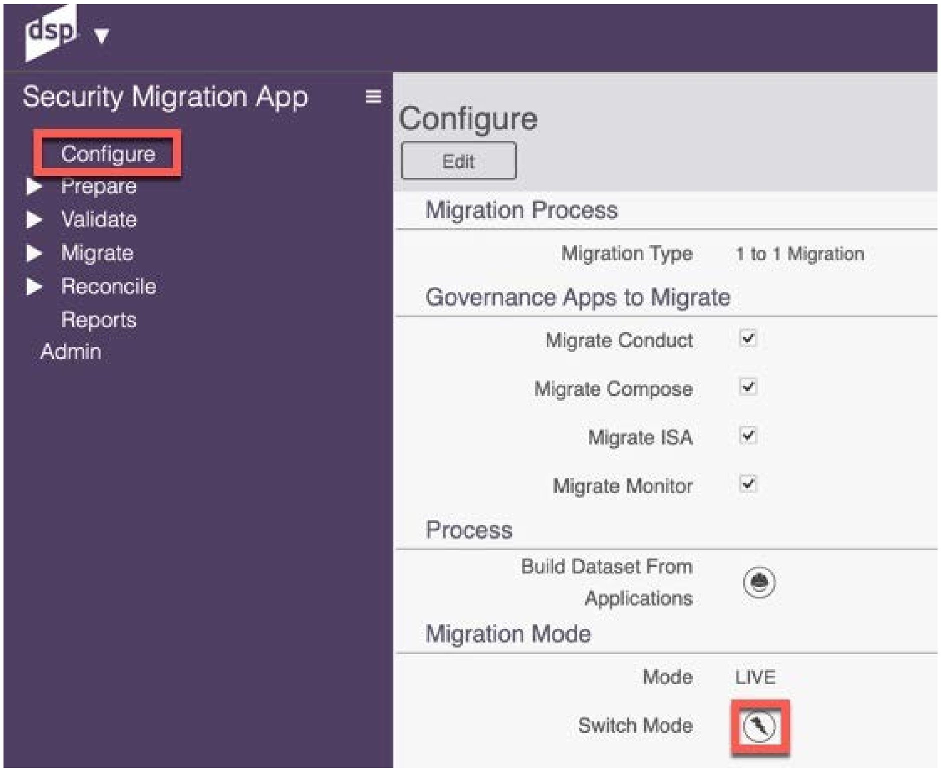
User ID: Administrator
User Name: Administrator

SECURITY DEFINITION ▼	DESCRIPTION	
DGE.Position	Position	0

Step 8 Change Migration Mode to Live

By default, the utility is installed in SIMULATION mode. This mode does not allow any migration into the underlying DSP security tables. It does, however, allow all the planning and preparation work to be done BEFORE DSP is upgraded to version 7.1 or above.

After upgrade from a DSP version of 7.0.6 or below to DSP 7.1 or above, the utility can be switched into LIVE mode. Making this switch activates functionality that enables the migration to take place.



Configure

Migration Process

Migration Type 1 to 1 Migration

Governance Apps to Migrate

Migrate Conduct ☑

Migrate Compose ☑

Migrate ISA ☑

Migrate Monitor ☑

Process

Build Dataset From Applications ●

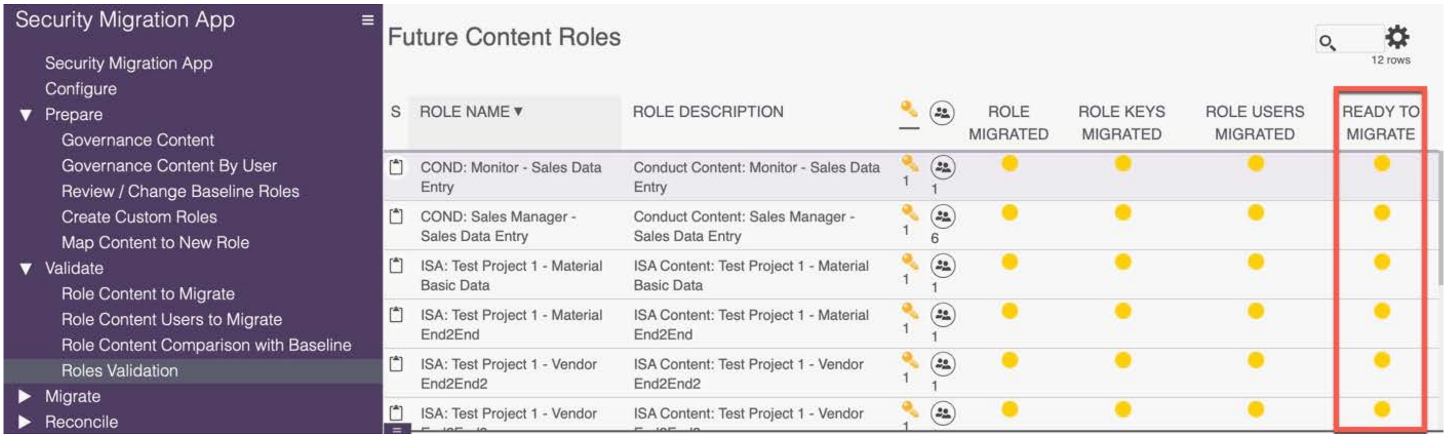
Migration Mode

Mode LIVE

Switch Mode

Step 9 Validate the Roles

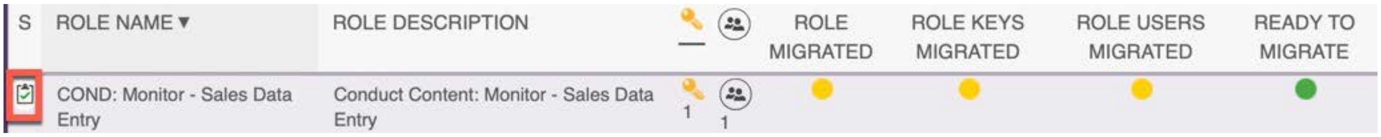
Before a Role can be migrated, it must pass some basic validations and the 'Ready to Migrate' indicator must be set to 'Green'.



Future Content Roles

S	ROLE NAME ▾	ROLE DESCRIPTION			ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	●	●	●	●
	COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	1	6	●	●	●	●
	ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	1	1	●	●	●	●
	ISA: Test Project 1 - Material End2End	ISA Content: Test Project 1 - Material End2End	1	1	●	●	●	●
	ISA: Test Project 1 - Vendor End2End2	ISA Content: Test Project 1 - Vendor End2End2	1	1	●	●	●	●
	ISA: Test Project 1 - Vendor	ISA Content: Test Project 1 - Vendor	1		●	●	●	●

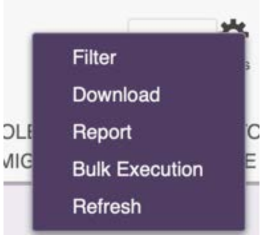
Trigger the validations for a single role by clicking the **Validate Record** icon.

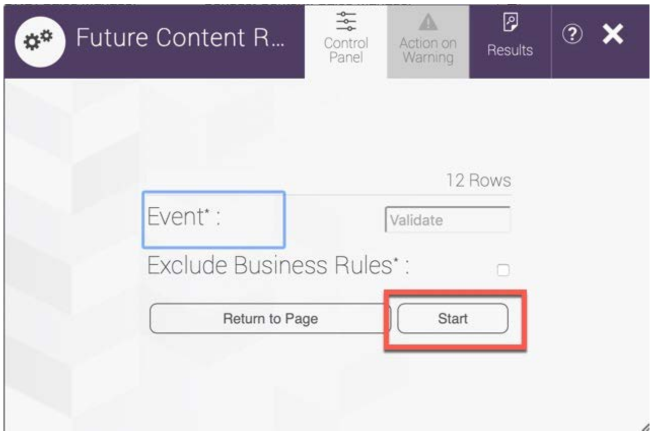


S	ROLE NAME ▾	ROLE DESCRIPTION			ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	●	●	●	●

Trigger the validations to run on multiple roles using the Bulk Execution feature.

Click the **More Actions** (small gear) icon and select **Bulk Execution**.





12 Rows

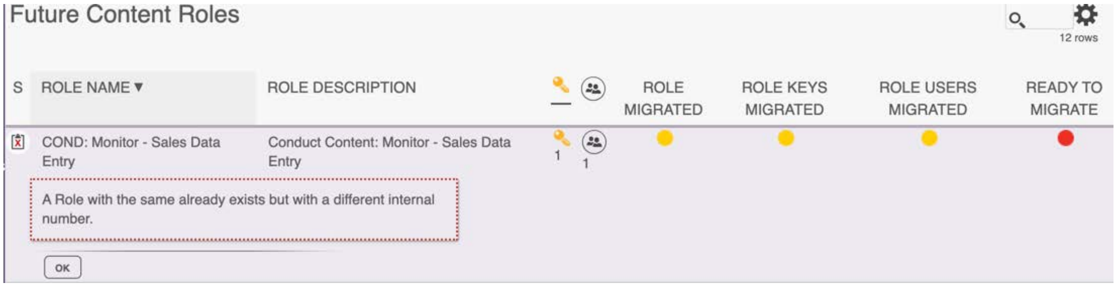
Event* : Validate

Exclude Business Rules* : □

The following validation checks are performed:

- Checks that a Role with same name but different internal GUID does not already exist.
- Checks that the Content Assigned to a Role has a Security Key assigned to it.

If any of these fails, an error message displays. If the record passes validation, it is set to 'Ready to Migrate' and available to migrate.



Future Content Roles

12 rows

S	ROLE NAME ▼	ROLE DESCRIPTION	🔑	👥	ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
☒	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	●	●	●	●

A Role with the same already exists but with a different internal number.

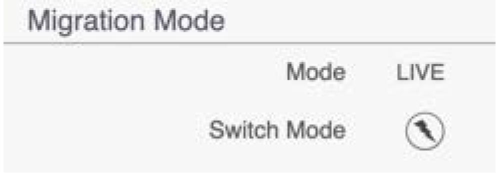
OK

NOTE: If a validation fails with the message above, ensure you've synchronized the DSP Security Definitions with each application for which the security is being migrated. Refer to *Step 7 Synchronize Security Definition Keys* for more information.

Step 10 Migrate Roles

Only Roles that have passed validation are available for migration. These roles have a green indicator in the 'Ready To Migrate' column.

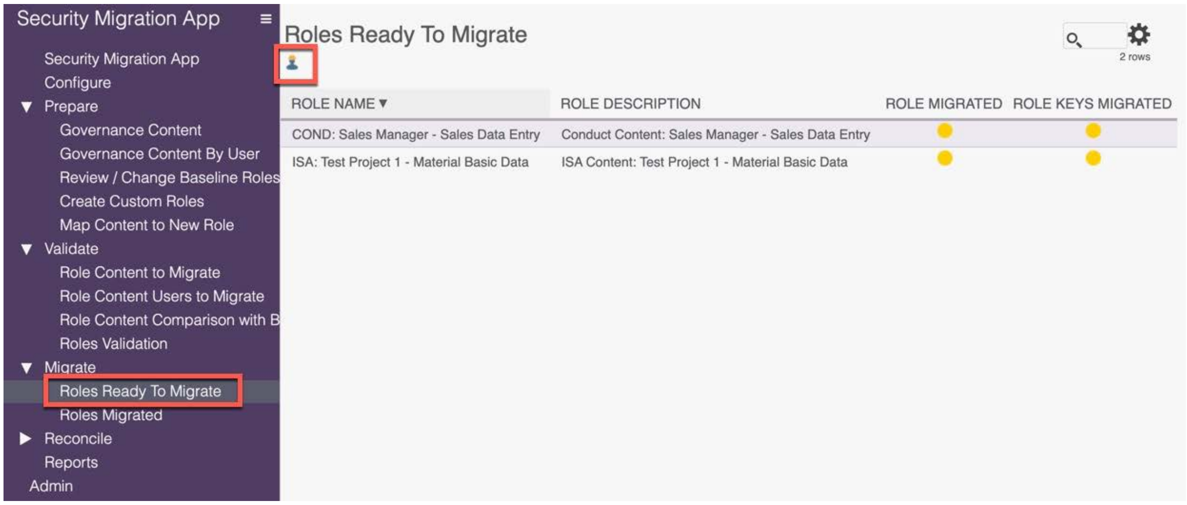
NOTE: Configuration 'Migration Mode' MUST be set to 'LIVE' in order to perform the migration tasks. Refer to *Step 8 Change Migration Mode to Live* for more information.



Migration Mode

Mode: LIVE

Select one or more records and click the **Migrate Role** button.



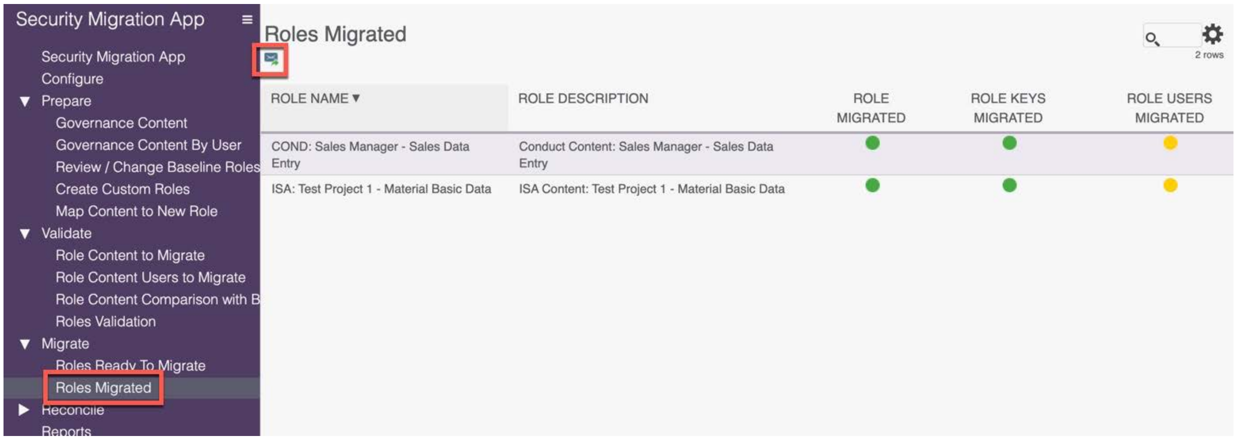
ROLE NAME ▾	ROLE DESCRIPTION	ROLE MIGRATED	ROLE KEYS MIGRATED
COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	●	●
ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	●	●

TIP! It's advisable to migrate a couple of roles end to end first and then check the results. Once the process has been confirmed to work as intended, the rest of the roles can be migrated.

Step 11 Assign Users to Roles

Once a Role and its Role Keys Value (Content) has been migrated, the User Role Staging functionality can be used to assign users to roles.

1. To populate the user role staging, select **Migrate** > **Roles Migrated** in the navigation pane.
2. Select user records.
3. Click the **Send to User Role Staging** button in the Page toolbar.



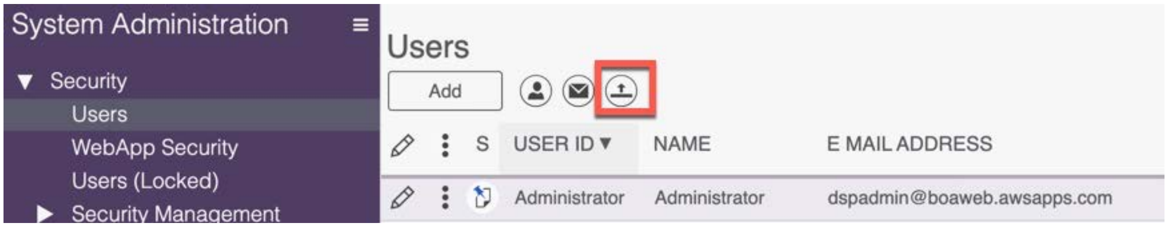
Roles Migrated

ROLE NAME ▾	ROLE DESCRIPTION	ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED
COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	🟢	🟢	🟡
ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	🟢	🟢	🟡

NOTE: This functionality pushes the User to Assignment Records to the User Role Staging table. From here, they can be assigned to the Role and any associated content as needed.

NOTE: In the 1 : 1 migration scenario, the expected outcome is that user access to governance content is unchanged.

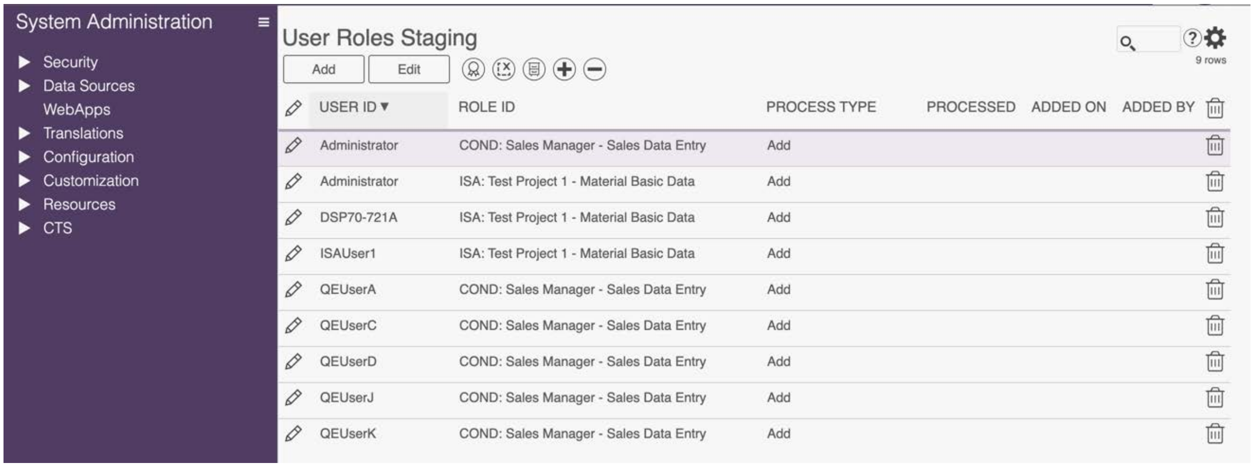
4. Select **Admin** > **Security** > **Users** in the *Navigation* pane.
5. Click the **User Role Staging** button.



Users

S	USER ID ▾	NAME	E MAIL ADDRESS
	Administrator	Administrator	dspadmin@boaweb.awsapps.com

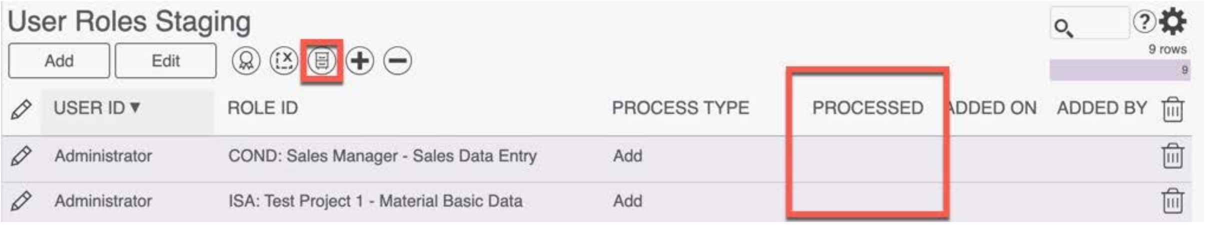
The User to Role assignment records are pushed into the Staging table and are available to process with process type ‘ Add’. Before adding users, validate the records.



USER ID ▾	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
Administrator	COND: Sales Manager - Sales Data Entry	Add			
Administrator	ISA: Test Project 1 - Material Basic Data	Add			
DSP70-721A	ISA: Test Project 1 - Material Basic Data	Add			
ISAUser1	ISA: Test Project 1 - Material Basic Data	Add			
QEUserA	COND: Sales Manager - Sales Data Entry	Add			
QEUserC	COND: Sales Manager - Sales Data Entry	Add			
QEUserD	COND: Sales Manager - Sales Data Entry	Add			
QEUserJ	COND: Sales Manager - Sales Data Entry	Add			
QEUserK	COND: Sales Manager - Sales Data Entry	Add			

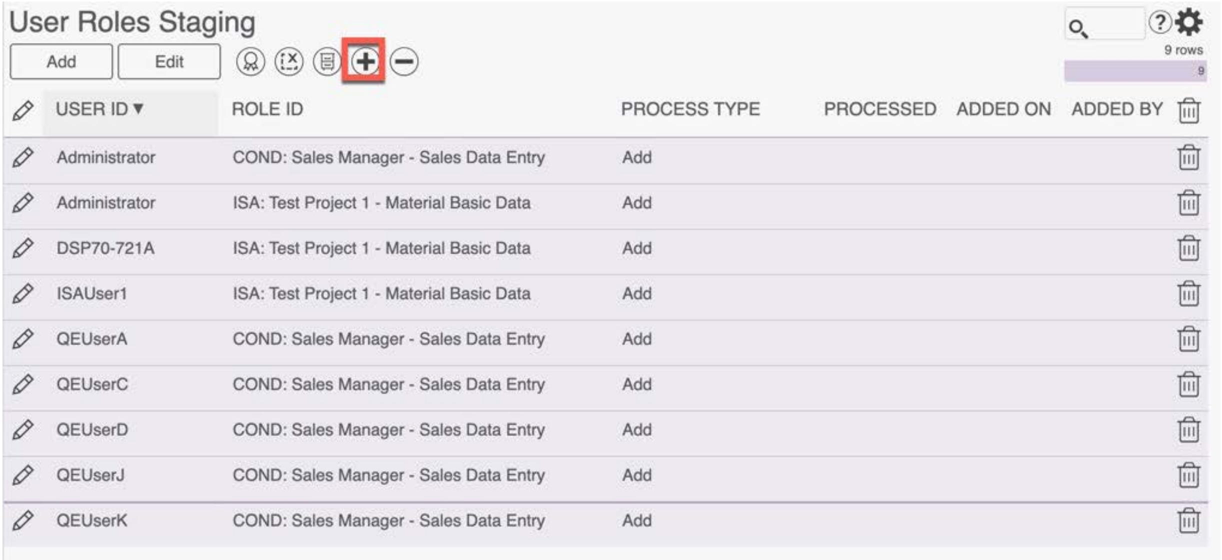
Validate all records to check that a user has not already been assigned to the role. If the user is already assigned, a check mark displays in the Processed column.

These records do not need to be assigned and can be removed by clicking the **Remove Processed** button.



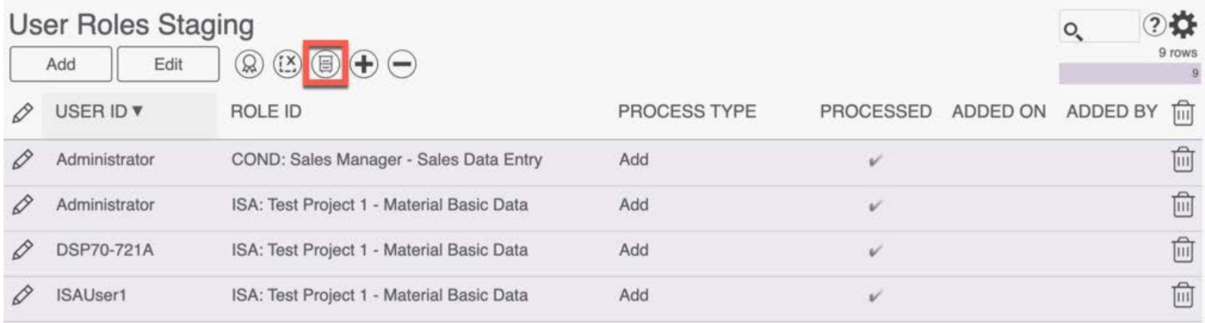
USER ID ▾	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
Administrator	COND: Sales Manager - Sales Data Entry	Add			
Administrator	ISA: Test Project 1 - Material Basic Data	Add			

Users can be assigned to the Role by selecting one or more records and then clicking the *Add Role* button.



	USER ID ▼	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
	Administrator	COND: Sales Manager - Sales Data Entry	Add			
	Administrator	ISA: Test Project 1 - Material Basic Data	Add			
	DSP70-721A	ISA: Test Project 1 - Material Basic Data	Add			
	ISAUser1	ISA: Test Project 1 - Material Basic Data	Add			
	QEUserA	COND: Sales Manager - Sales Data Entry	Add			
	QEUserC	COND: Sales Manager - Sales Data Entry	Add			
	QEUserD	COND: Sales Manager - Sales Data Entry	Add			
	QEUserJ	COND: Sales Manager - Sales Data Entry	Add			
	QEUserK	COND: Sales Manager - Sales Data Entry	Add			

The processed records can be removed by pressing the **Remove Processed** button.

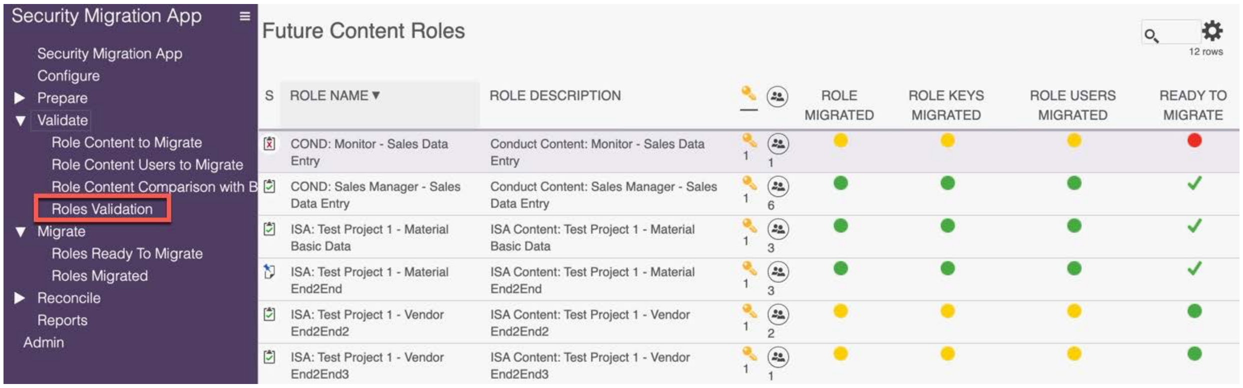


	USER ID ▼	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
	Administrator	COND: Sales Manager - Sales Data Entry	Add	✓		
	Administrator	ISA: Test Project 1 - Material Basic Data	Add	✓		
	DSP70-721A	ISA: Test Project 1 - Material Basic Data	Add	✓		
	ISAUser1	ISA: Test Project 1 - Material Basic Data	Add	✓		

Step 12 Review Migration Status

To check the overall status of the role migration, navigate to the *Future Content Roles* page by selecting **Validate** > **Roles Validation** in the *Navigation* pane.

Validate the records manually or via Bulk Execution.

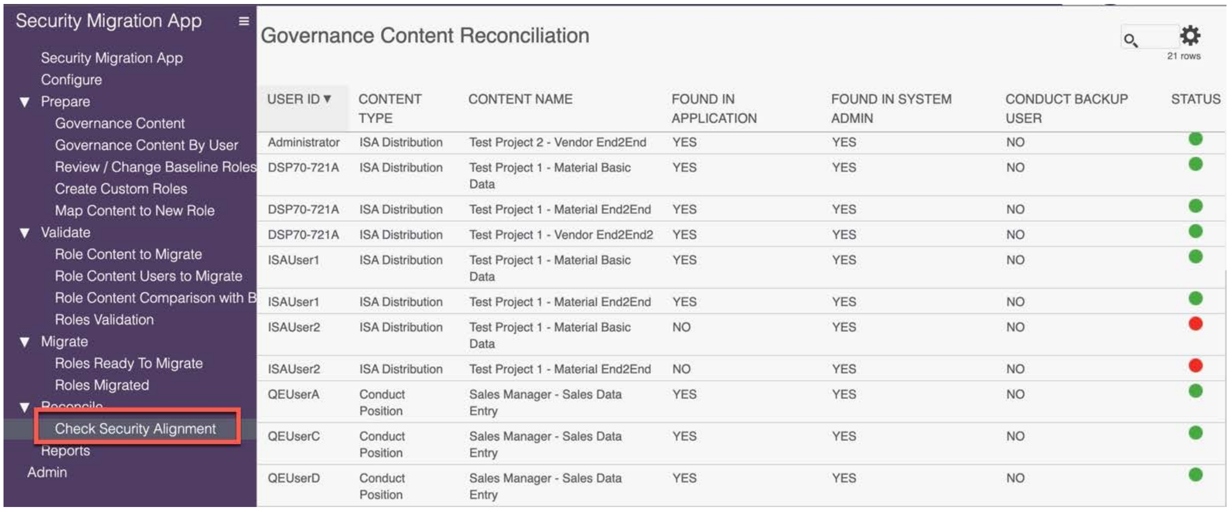


S	ROLE NAME ▼	ROLE DESCRIPTION			ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	🟡	🟡	🟡	🔴
	COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	1	6	🟢	🟢	🟢	✓
	ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	1	3	🟢	🟢	🟢	✓
	ISA: Test Project 1 - Material End2End	ISA Content: Test Project 1 - Material End2End	1	3	🟢	🟢	🟢	✓
	ISA: Test Project 1 - Vendor End2End2	ISA Content: Test Project 1 - Vendor End2End2	1	2	🟡	🟡	🟡	🟢
	ISA: Test Project 1 - Vendor End2End3	ISA Content: Test Project 1 - Vendor End2End3	1	1	🟡	🟡	🟡	🟢

Step 13 Reconcile System Admin Security with Application Security

Once the migration of the roles and user role assignment has been completed, review the Governance Content Reconciliation report. This report shows User Content Access based upon System Administration Security Setup and the User Content Access that is actually assigned within each governance application.

Once the migration is complete, these should be aligned. Any misalignment may indicate that there have been some failures during the synchronization of Security to the various applications or that some roles have not been fully created.



Governance Content Reconciliation

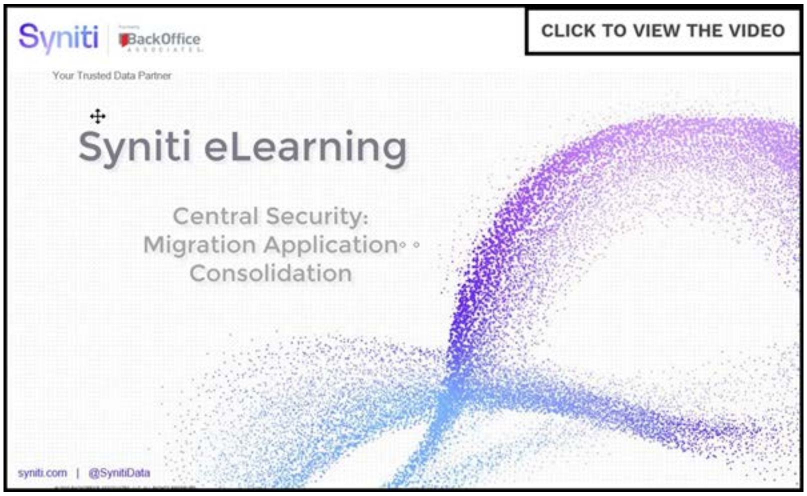
USER ID ▼	CONTENT TYPE	CONTENT NAME	FOUND IN APPLICATION	FOUND IN SYSTEM ADMIN	CONDUCT BACKUP USER	STATUS
Administrator	ISA Distribution	Test Project 2 - Vendor End2End	YES	YES	NO	🟢
DSP70-721A	ISA Distribution	Test Project 1 - Material Basic Data	YES	YES	NO	🟢
DSP70-721A	ISA Distribution	Test Project 1 - Material End2End	YES	YES	NO	🟢
DSP70-721A	ISA Distribution	Test Project 1 - Vendor End2End2	YES	YES	NO	🟢
ISAUser1	ISA Distribution	Test Project 1 - Material Basic Data	YES	YES	NO	🟢
ISAUser1	ISA Distribution	Test Project 1 - Material End2End	YES	YES	NO	🟢
ISAUser2	ISA Distribution	Test Project 1 - Material Basic Data	NO	YES	NO	🔴
ISAUser2	ISA Distribution	Test Project 1 - Material End2End	NO	YES	NO	🔴
QEUserA	Conduct Position	Sales Manager - Sales Data Entry	YES	YES	NO	🟢
QEUserC	Conduct Position	Sales Manager - Sales Data Entry	YES	YES	NO	🟢
QEUserD	Conduct Position	Sales Manager - Sales Data Entry	YES	YES	NO	🟢

Pre-Upgrade Steps: Migration Scenario: Consolidate

The tasks in this section must be performed BEFORE upgrading to 7.1.

1. Select Migration Scope
2. Build Dataset From Applications
3. Review Current Governance Content and User Access
4. Create Custom Roles
5. Map Governance Content to Custom Roles
6. Validate Role Data Before Migration
7. Upgrade the DSP

Watch the Central Security Migration Application Consolidation video for a demonstration of the steps in this section.



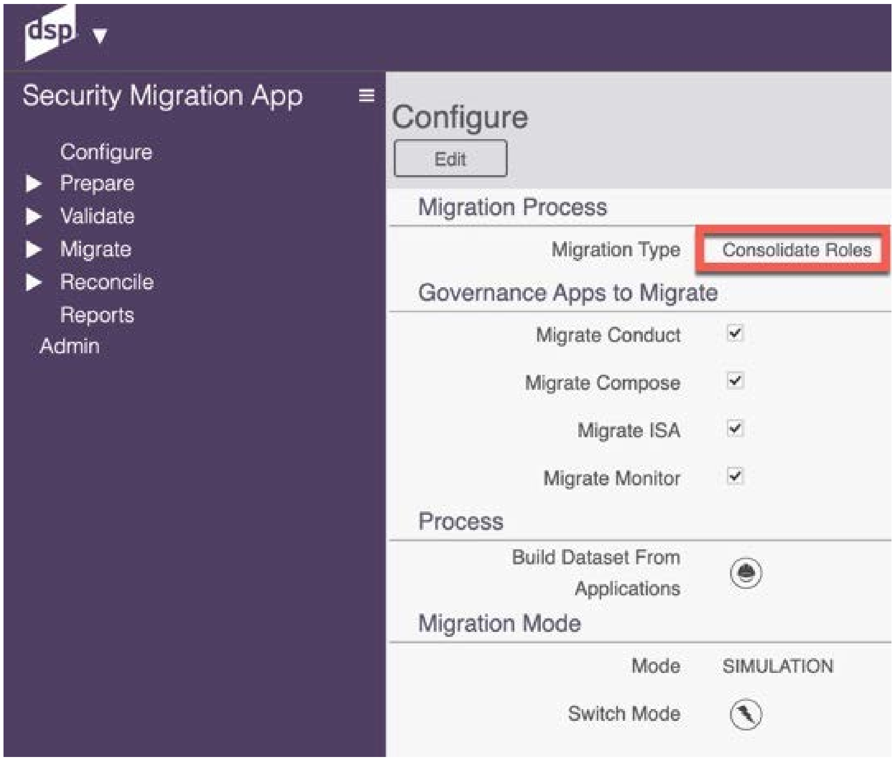
Step 1: Select Migration Scope

The migration to the Centralized Security Model impacts customers that use the following DSP Solutions and associated content:

- dspConduct
  - Positions
- dspMonitor
  - Groups
- dspCompose
  - Template Roles

From the configuration menu, select the applications that you want to migrate to the Centralized Security Model.

NOTE: All DSP Solutions will adopt the new security model when upgrading to DSP 7.1 or above. The selections made here relate to the automatic migration of data to the new security model.



Migration Process

Migration Type: Consolidate Roles

Governance Apps to Migrate

Migrate Conduct ☑

Migrate Compose ☑

Migrate ISA ☑

Migrate Monitor ☑

Process

Build Dataset From Applications

Migration Mode

Mode: SIMULATION

Switch Mode

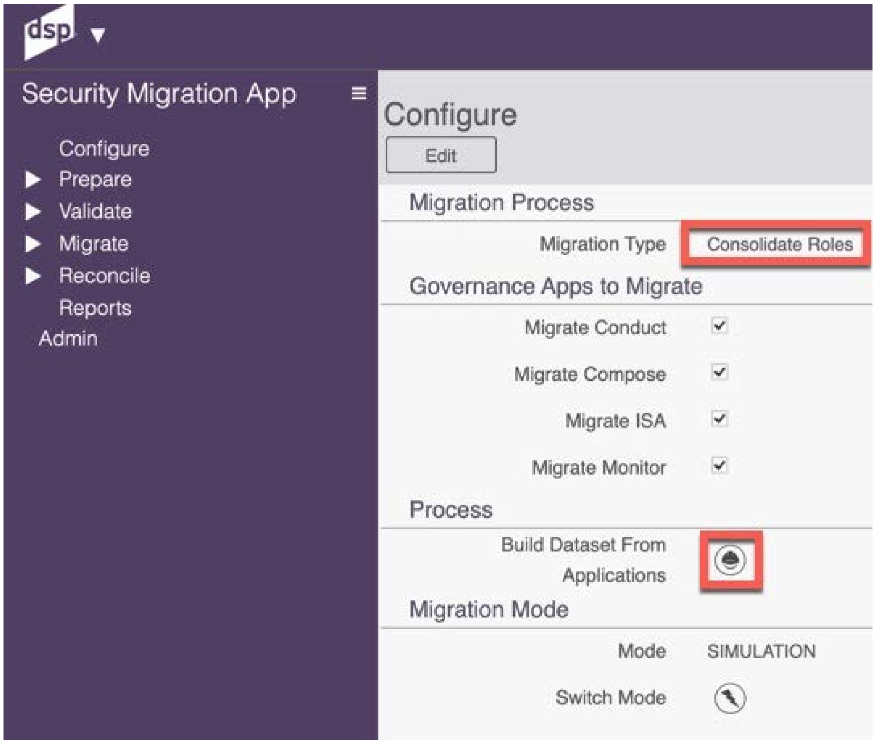
Step 2: Build Dataset From Applications

In this scenario, set the **Migration Type** to **Consolidate Roles** and then click the **Build Dataset from Application**s button.

This runs a stored procedure that creates (within the Utility Staging Area, not in DSP) a single Content Role for every piece of content associated with applications selected in the previous step. This step also assigns the users assigned to the content to these roles.

Staging tables within the database CentralSecurityMigrationUtility:

- BaselineContentRoles
- BaselineContentRoleUsers



Migration Process

Migration Type: Consolidate Roles

Governance Apps to Migrate

Migrate Conduct ☑

Migrate Compose ☑

Migrate ISA ☑

Migrate Monitor ☑

Process

Build Dataset From Applications

Migration Mode

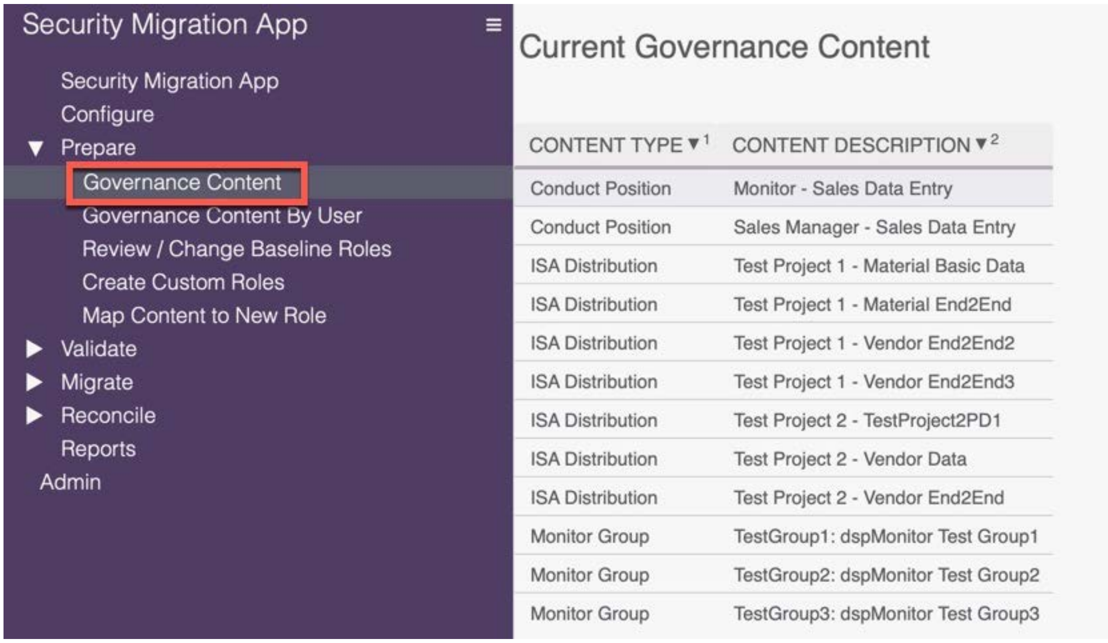
Mode: SIMULATION

Switch Mode

Step 3 Review Current Governance Content and User Access

Under the 'Prepare' Menu, there are 2 reports that can reviewed to validate that the staged data contains the Content and User Content assignment that you're expecting to migrate.

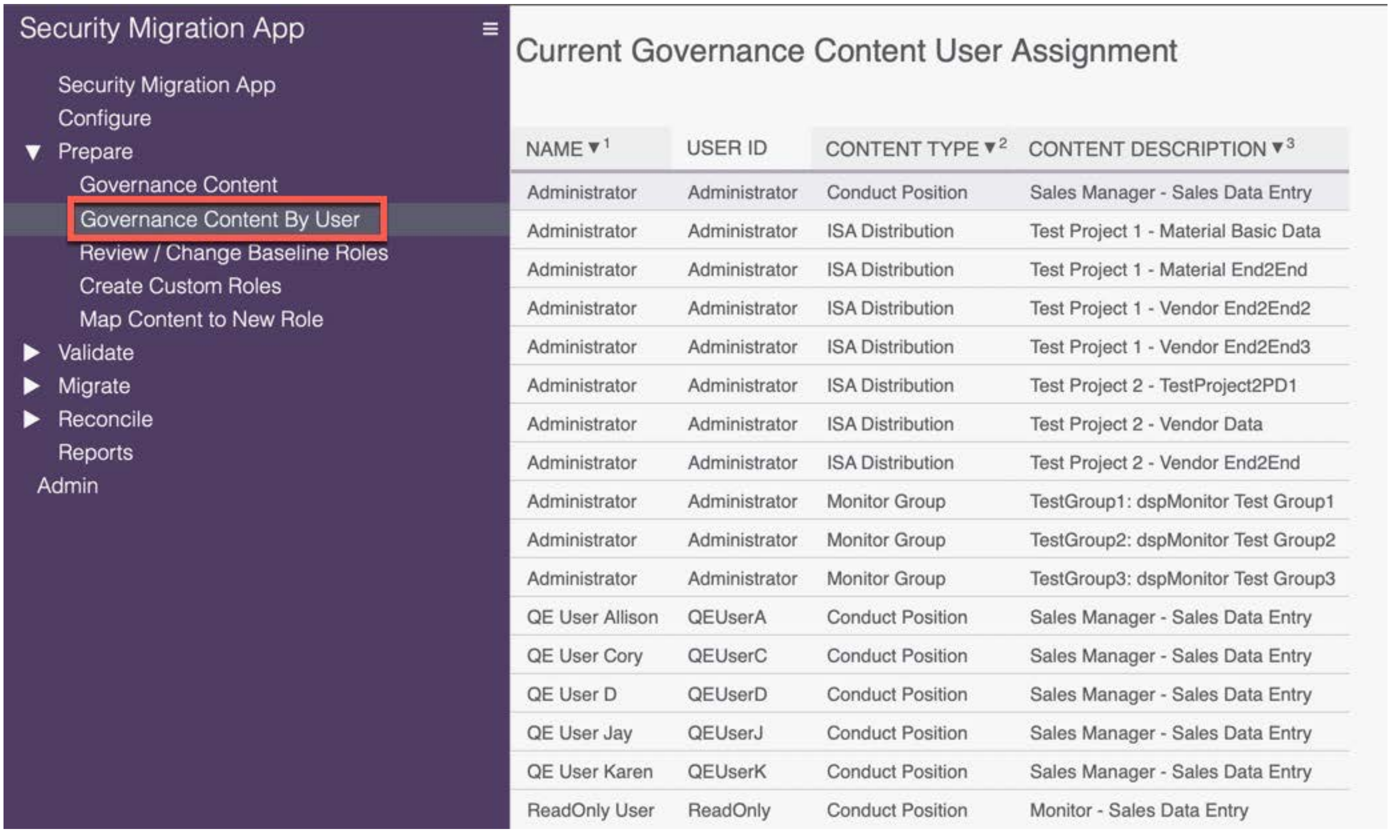
Select **Prepare** > **Governance Content** to view all the content to be migrated to the new Content Roles.



Current Governance Content

CONTENT TYPE ▼1	CONTENT DESCRIPTION ▼2
Conduct Position	Monitor - Sales Data Entry
Conduct Position	Sales Manager - Sales Data Entry
ISA Distribution	Test Project 1 - Material Basic Data
ISA Distribution	Test Project 1 - Material End2End
ISA Distribution	Test Project 1 - Vendor End2End2
ISA Distribution	Test Project 1 - Vendor End2End3
ISA Distribution	Test Project 2 - TestProject2PD1
ISA Distribution	Test Project 2 - Vendor Data
ISA Distribution	Test Project 2 - Vendor End2End
Monitor Group	TestGroup1: dspMonitor Test Group1
Monitor Group	TestGroup2: dspMonitor Test Group2
Monitor Group	TestGroup3: dspMonitor Test Group3

Select **Prepare > Governance Content By User** to view all the User to Content assignments that currently exist within your DSP applications and that will be migrated to the new Content Roles.

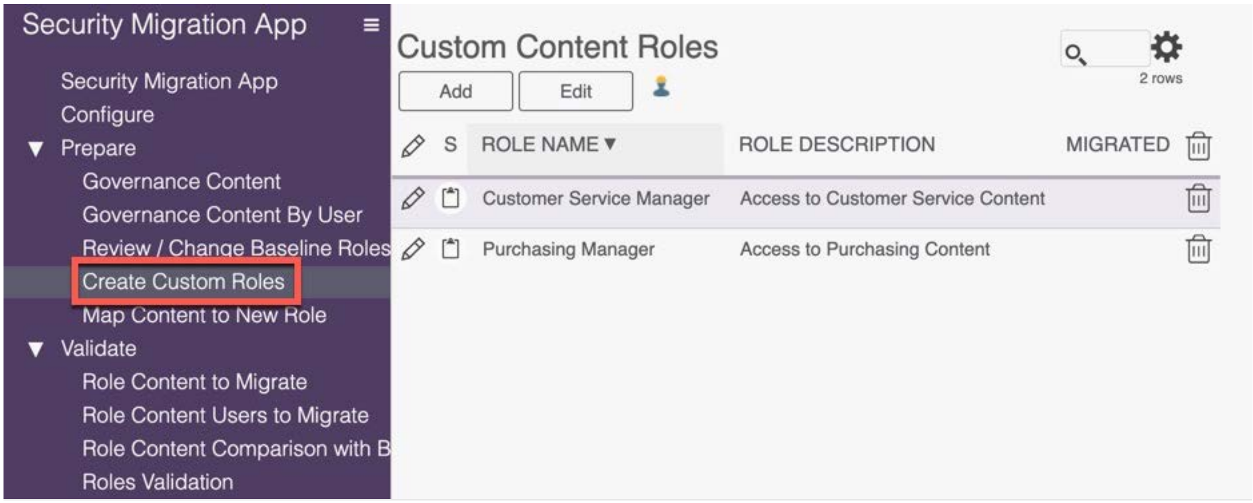


Current Governance Content User Assignment

NAME ▼ 1	USER ID	CONTENT TYPE ▼ 2	CONTENT DESCRIPTION ▼ 3
Administrator	Administrator	Conduct Position	Sales Manager - Sales Data Entry
Administrator	Administrator	ISA Distribution	Test Project 1 - Material Basic Data
Administrator	Administrator	ISA Distribution	Test Project 1 - Material End2End
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End2
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End3
Administrator	Administrator	ISA Distribution	Test Project 2 - TestProject2PD1
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor Data
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor End2End
Administrator	Administrator	Monitor Group	TestGroup1: dspMonitor Test Group1
Administrator	Administrator	Monitor Group	TestGroup2: dspMonitor Test Group2
Administrator	Administrator	Monitor Group	TestGroup3: dspMonitor Test Group3
QE User Allison	QEUserA	Conduct Position	Sales Manager - Sales Data Entry
QE User Cory	QEUserC	Conduct Position	Sales Manager - Sales Data Entry
QE User D	QEUserD	Conduct Position	Sales Manager - Sales Data Entry
QE User Jay	QEUserJ	Conduct Position	Sales Manager - Sales Data Entry
QE User Karen	QEUserK	Conduct Position	Sales Manager - Sales Data Entry
ReadOnly User	ReadOnly	Conduct Position	Monitor - Sales Data Entry

Step 4 Create Custom Roles

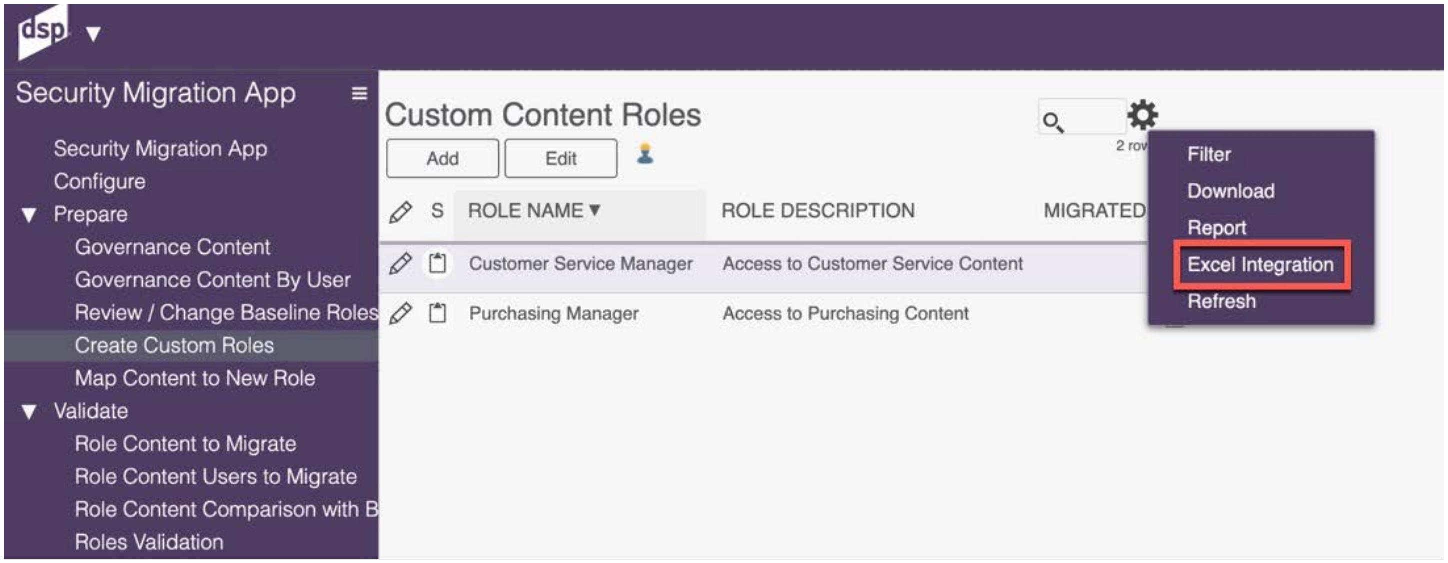
Custom Content roles can be added manually via the user interface, as shown below.



Custom Content Roles

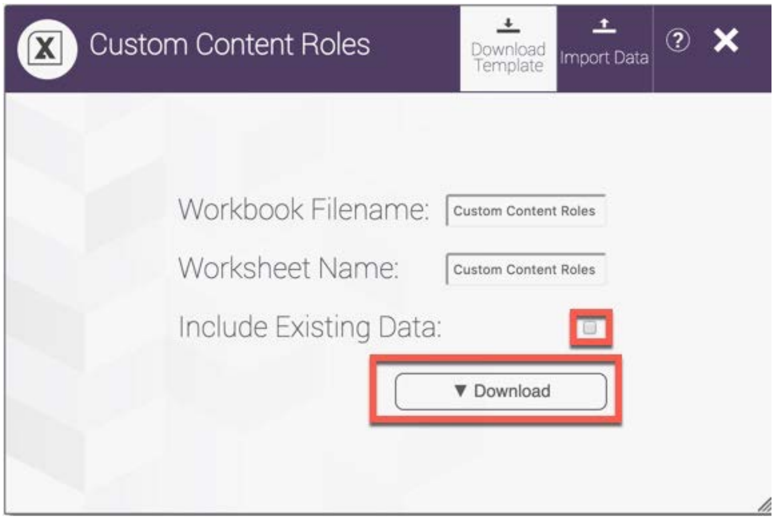
S	ROLE NAME ▼	ROLE DESCRIPTION	MIGRATED
	Customer Service Manager	Access to Customer Service Content	
	Purchasing Manager	Access to Purchasing Content	

Alternatively, DSP Excel Integration functionality can be used to mass upload the required roles.



S	ROLE NAME	ROLE DESCRIPTION	MIGRATED
	Customer Service Manager	Access to Customer Service Content	
	Purchasing Manager	Access to Purchasing Content	

An Excel template with or without data can be downloaded.

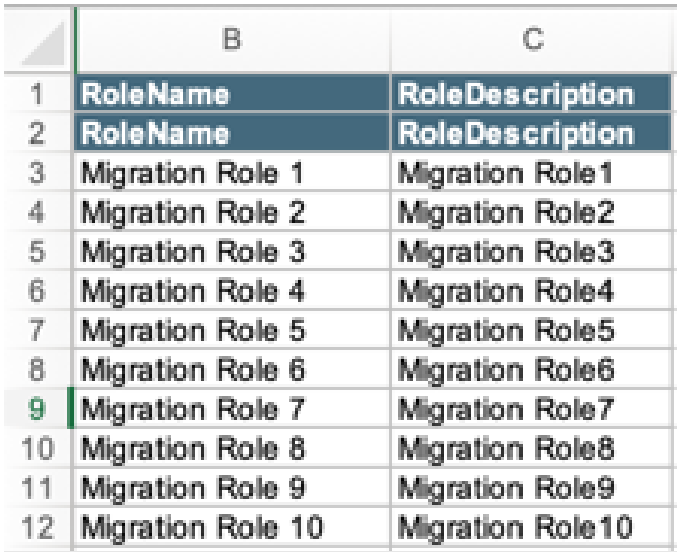


Workbook Filename: Custom Content Roles

Worksheet Name: Custom Content Roles

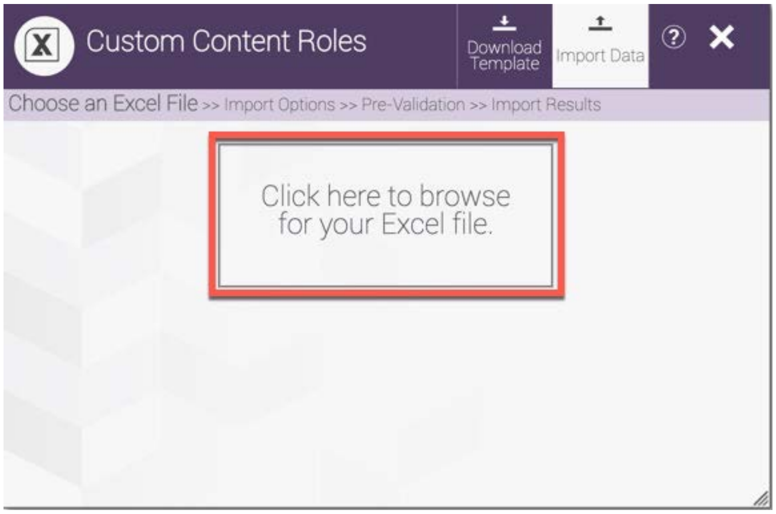
Include Existing Data: □

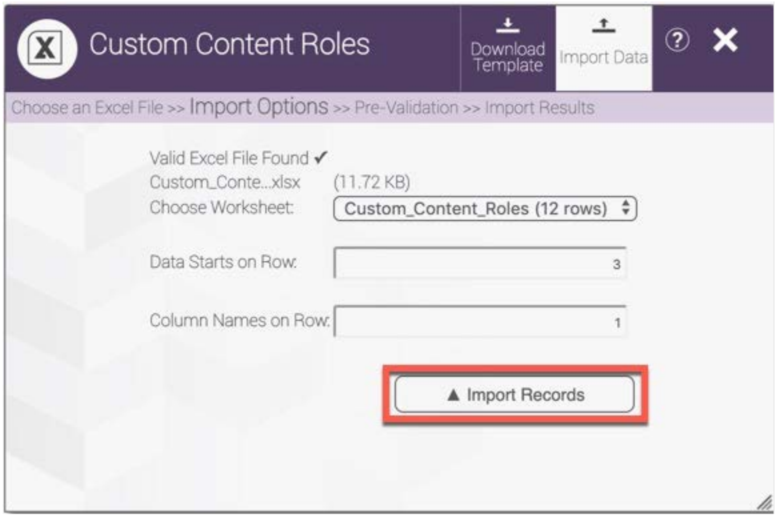
The Excel template can then be populated with the new roles.



	B	C
1	RoleName	RoleDescription
2	RoleName	RoleDescription
3	Migration Role 1	Migration Role1
4	Migration Role 2	Migration Role2
5	Migration Role 3	Migration Role3
6	Migration Role 4	Migration Role4
7	Migration Role 5	Migration Role5
8	Migration Role 6	Migration Role6
9	Migration Role 7	Migration Role7
10	Migration Role 8	Migration Role8
11	Migration Role 9	Migration Role9
12	Migration Role 10	Migration Role10

The data can then be imported.


Custom Content Roles
Download Template
Import Data
Choose an Excel File >> Import Options >> Pre-Validation >> Import Results
Click here to browse for your Excel file.



Choose an Excel File >> Import Options >> Pre-Validation >> Import Results

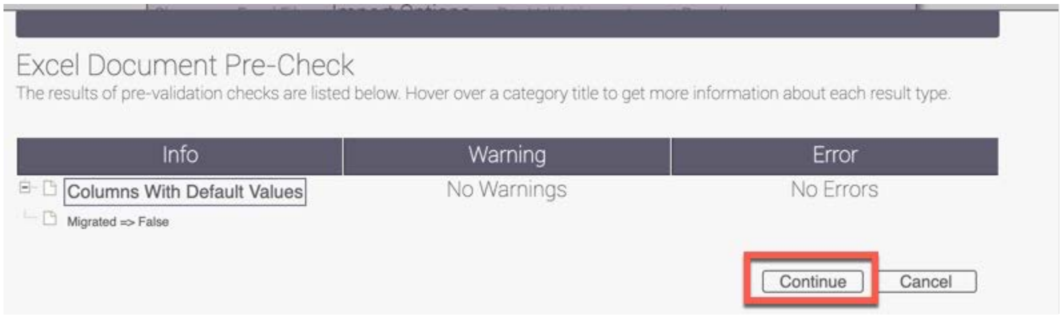
Valid Excel File Found ✓

Custom_Conte...xlsx (11.72 KB)

Choose Worksheet: Custom_Content_Roles (12 rows)

Data Starts on Row: 3

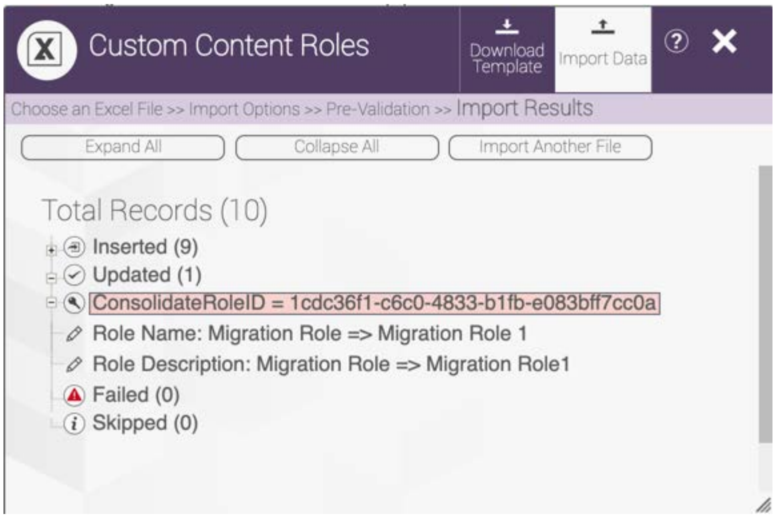
Column Names on Row: 1



Excel Document Pre-Check

The results of pre-validation checks are listed below. Hover over a category title to get more information about each result type.

Info	Warning	Error
Columns With Default Values Migrated => False	No Warnings	No Errors



Choose an Excel File >> Import Options >> Pre-Validation >> Import Results

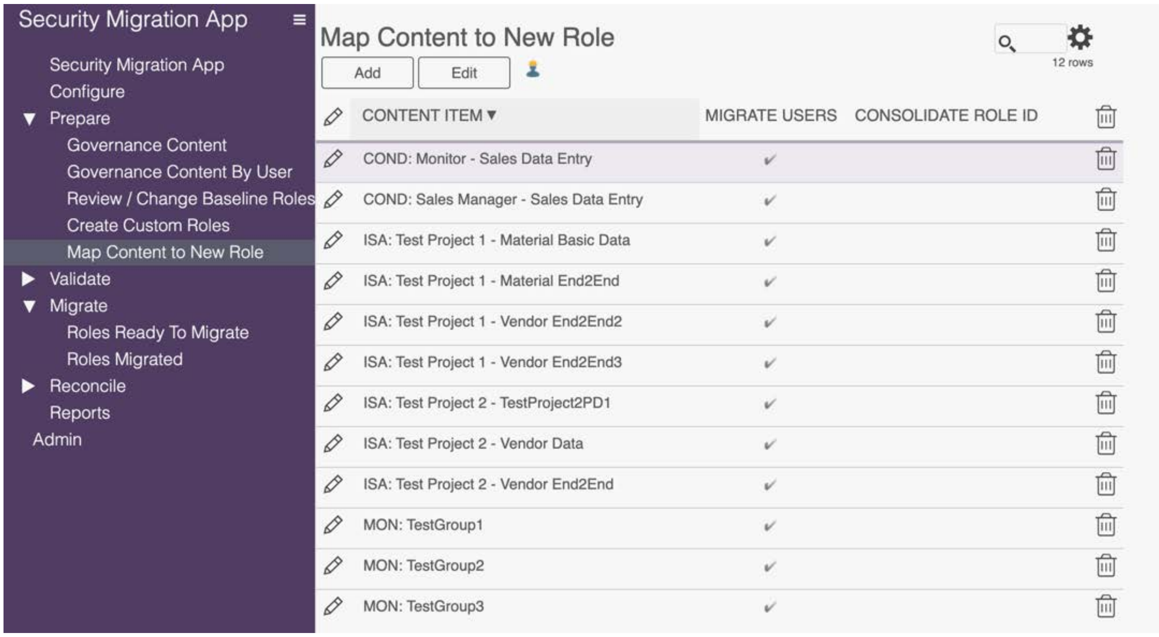
Total Records (10)

- Inserted (9)
- Updated (1)
  - ConsolidateRoleID = 1cdc36f1-c6c0-4833-b1fb-e083bff7cc0a
    - Role Name: Migration Role => Migration Role 1
    - Role Description: Migration Role => Migration Role1
- Failed (0)
- Skipped (0)

Step 5 Map Governance Content to Custom Roles

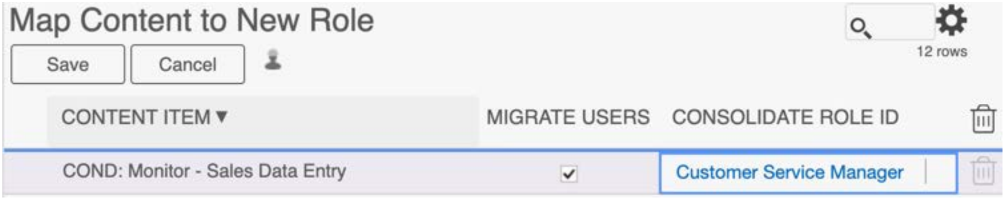
The *Map Content to New Role* page is populated with all Governance Content from select applications. This page allows governance content to be mapped to multiple roles. If the Migrate Users column is checked, the users on the content are migrated to the mapped role.

Careful consideration is needed with regard to this check box, because it could result in users gaining access to content that they did not previously have. Validation reports are available to compare the results of this mapping against existing setup.



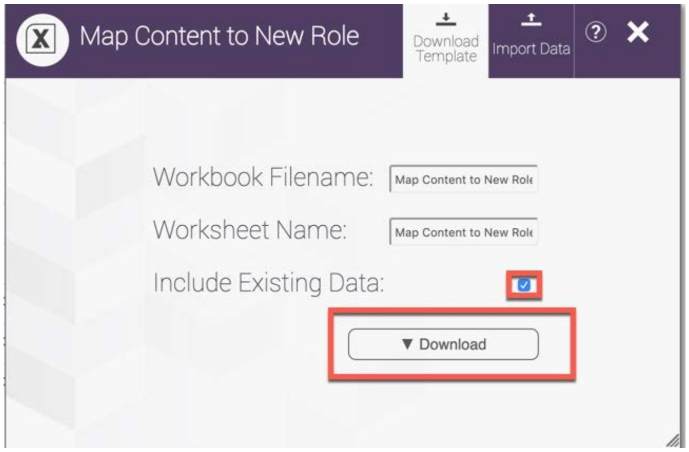
CONTENT ITEM ▼	MIGRATE USERS	CONSOLIDATE ROLE ID
COND: Monitor - Sales Data Entry	✓	
COND: Sales Manager - Sales Data Entry	✓	
ISA: Test Project 1 - Material Basic Data	✓	
ISA: Test Project 1 - Material End2End	✓	
ISA: Test Project 1 - Vendor End2End2	✓	
ISA: Test Project 1 - Vendor End2End3	✓	
ISA: Test Project 2 - TestProject2PD1	✓	
ISA: Test Project 2 - Vendor Data	✓	
ISA: Test Project 2 - Vendor End2End	✓	
MON: TestGroup1	✓	
MON: TestGroup2	✓	
MON: TestGroup3	✓	

Content can be manually mapped to any role that exists in DSP or a newly created Custom Role.



CONTENT ITEM ▼	MIGRATE USERS	CONSOLIDATE ROLE ID
COND: Monitor - Sales Data Entry	☑	Customer Service Manager

Alternatively, the Content to Role mapping can be done in Excel and then uploaded.

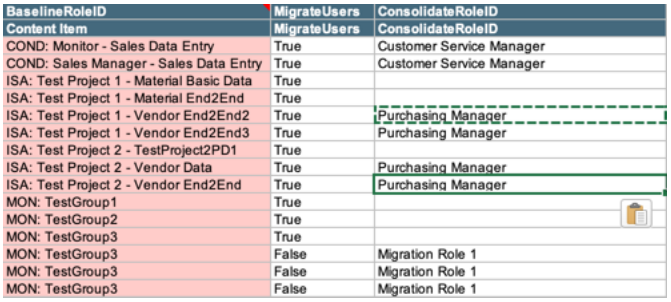


Workbook Filename: Map Content to New Role

Worksheet Name: Map Content to New Role

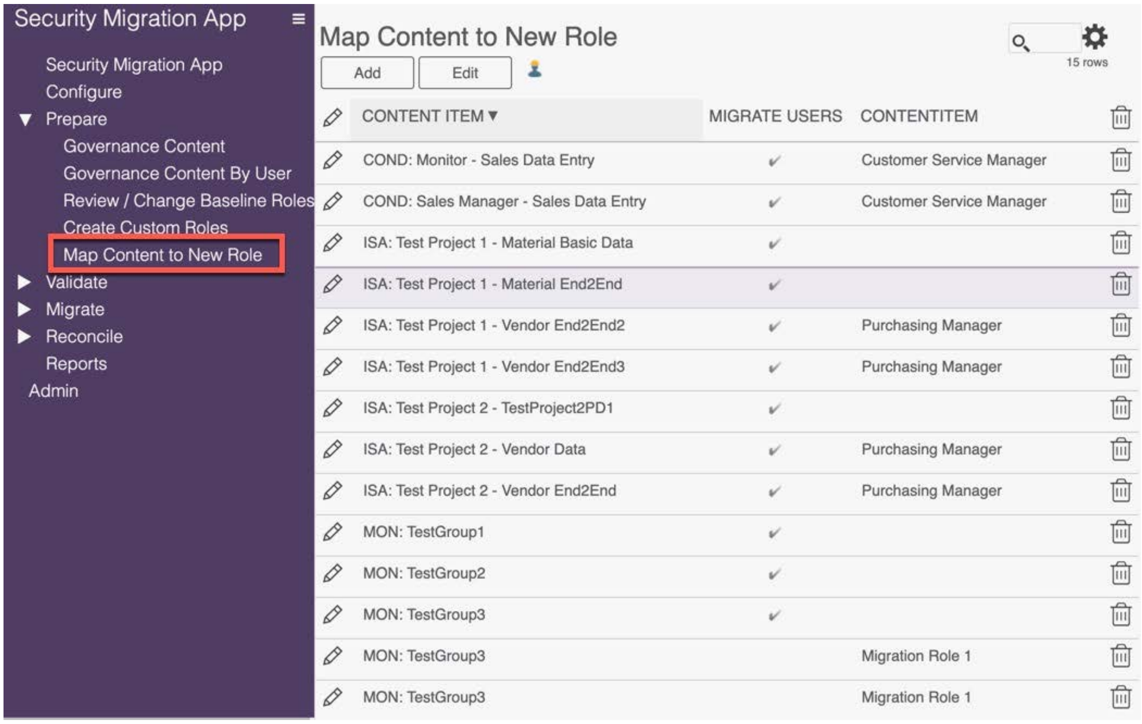
Include Existing Data: ☑

Prepare the data.



BaselineRoleID	MigrateUsers	ConsolidateRoleID
Content Item	MigrateUsers	ConsolidateRoleID
COND: Monitor - Sales Data Entry	True	Customer Service Manager
COND: Sales Manager - Sales Data Entry	True	Customer Service Manager
ISA: Test Project 1 - Material Basic Data	True	
ISA: Test Project 1 - Material End2End	True	
ISA: Test Project 1 - Vendor End2End2	True	Purchasing Manager
ISA: Test Project 1 - Vendor End2End3	True	Purchasing Manager
ISA: Test Project 2 - TestProject2PD1	True	
ISA: Test Project 2 - Vendor Data	True	Purchasing Manager
ISA: Test Project 2 - Vendor End2End	True	Purchasing Manager
MON: TestGroup1	True	
MON: TestGroup2	True	
MON: TestGroup3	True	
MON: TestGroup3	False	Migration Role 1
MON: TestGroup3	False	Migration Role 1
MON: TestGroup3	False	Migration Role 1

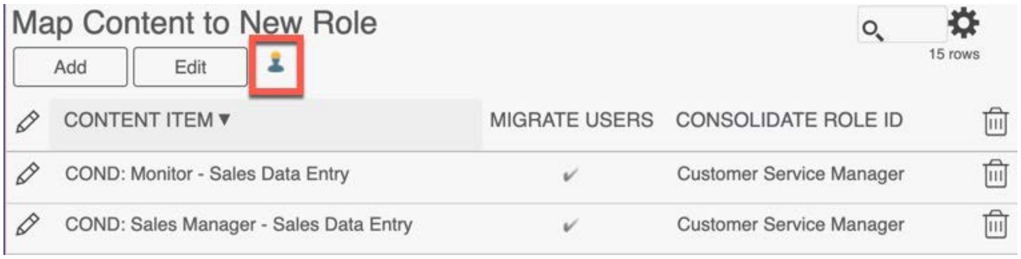
Then upload it.



Map Content to New Role

CONTENT ITEM ▼	MIGRATE USERS	CONTENTITEM
COND: Monitor - Sales Data Entry	✓	Customer Service Manager
COND: Sales Manager - Sales Data Entry	✓	Customer Service Manager
ISA: Test Project 1 - Material Basic Data	✓	
ISA: Test Project 1 - Material End2End	✓	
ISA: Test Project 1 - Vendor End2End2	✓	Purchasing Manager
ISA: Test Project 1 - Vendor End2End3	✓	Purchasing Manager
ISA: Test Project 2 - TestProject2PD1	✓	
ISA: Test Project 2 - Vendor Data	✓	Purchasing Manager
ISA: Test Project 2 - Vendor End2End	✓	Purchasing Manager
MON: TestGroup1	✓	
MON: TestGroup2	✓	
MON: TestGroup3	✓	
MON: TestGroup3		Migration Role 1
MON: TestGroup3		Migration Role 1

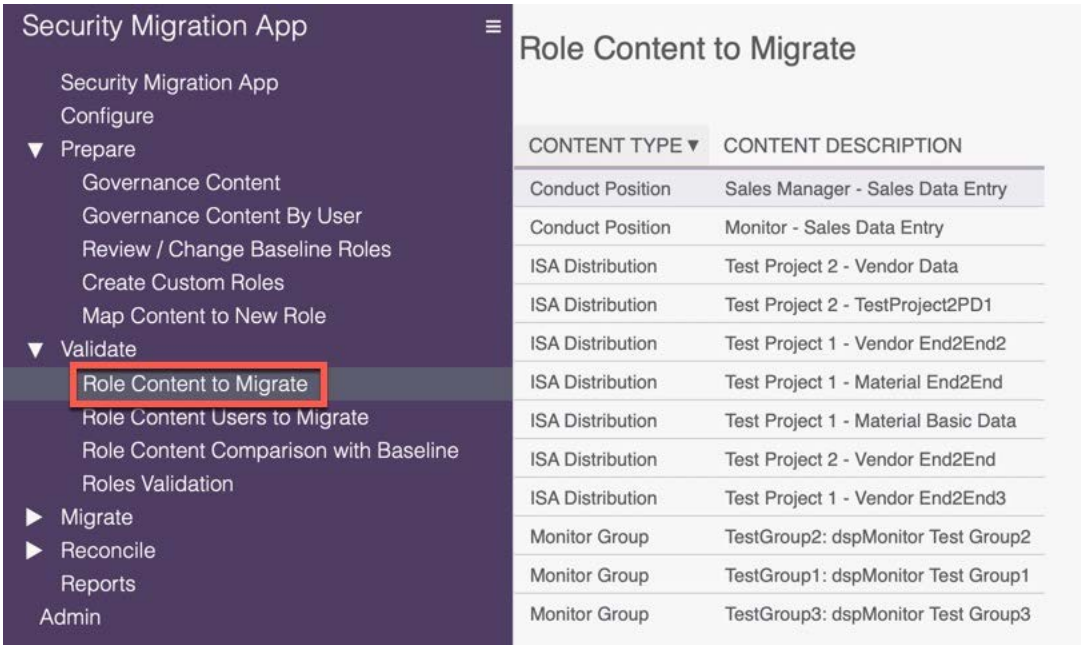
Once the Content to Role mapping has been completed, create the final role dataset by clicking the **Prepare Final Role** button.



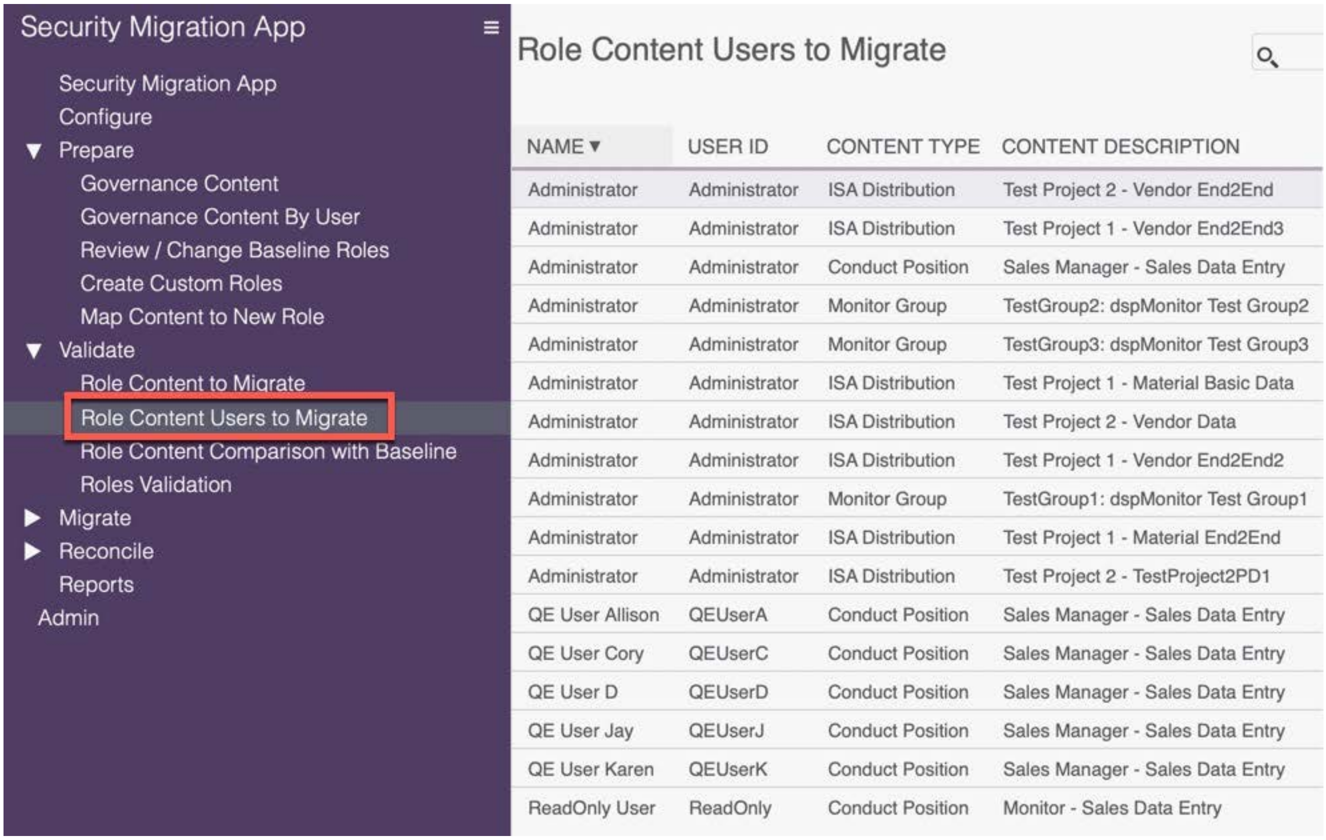
CONTENT ITEM ▾	MIGRATE USERS	CONSOLIDATE ROLE ID
COND: Monitor - Sales Data Entry	✓	Customer Service Manager
COND: Sales Manager - Sales Data Entry	✓	Customer Service Manager

Step 6 Validate Role Data Before Migration

The details of the Roles / Content and users to migrate can be reviewed in the following reports.



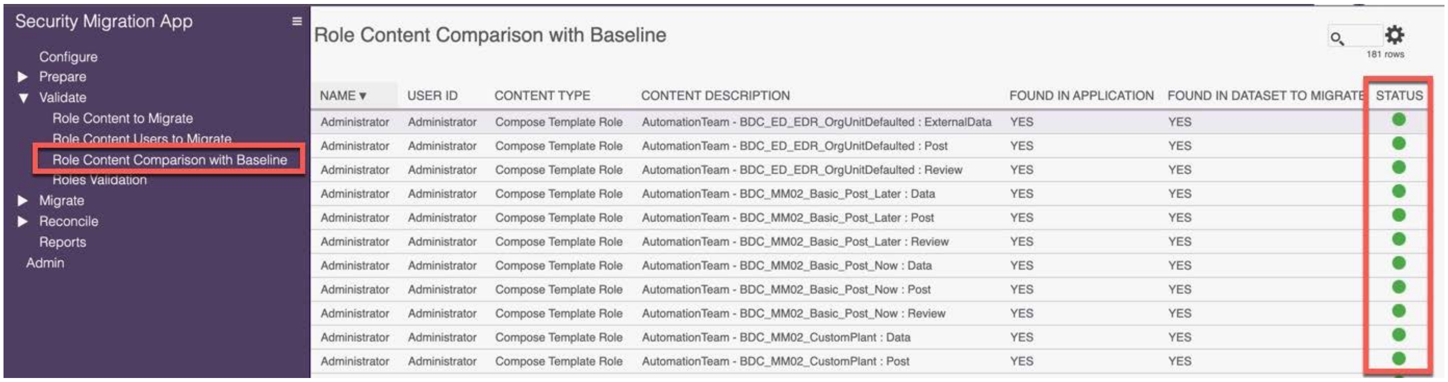
CONTENT TYPE ▾	CONTENT DESCRIPTION
Conduct Position	Sales Manager - Sales Data Entry
Conduct Position	Monitor - Sales Data Entry
ISA Distribution	Test Project 2 - Vendor Data
ISA Distribution	Test Project 2 - TestProject2PD1
ISA Distribution	Test Project 1 - Vendor End2End2
ISA Distribution	Test Project 1 - Material End2End
ISA Distribution	Test Project 1 - Material Basic Data
ISA Distribution	Test Project 2 - Vendor End2End
ISA Distribution	Test Project 1 - Vendor End2End3
Monitor Group	TestGroup2: dspMonitor Test Group2
Monitor Group	TestGroup1: dspMonitor Test Group1
Monitor Group	TestGroup3: dspMonitor Test Group3



Role Content Users to Migrate

NAME ▼	USER ID	CONTENT TYPE	CONTENT DESCRIPTION
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor End2End
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End3
Administrator	Administrator	Conduct Position	Sales Manager - Sales Data Entry
Administrator	Administrator	Monitor Group	TestGroup2: dspMonitor Test Group2
Administrator	Administrator	Monitor Group	TestGroup3: dspMonitor Test Group3
Administrator	Administrator	ISA Distribution	Test Project 1 - Material Basic Data
Administrator	Administrator	ISA Distribution	Test Project 2 - Vendor Data
Administrator	Administrator	ISA Distribution	Test Project 1 - Vendor End2End2
Administrator	Administrator	Monitor Group	TestGroup1: dspMonitor Test Group1
Administrator	Administrator	ISA Distribution	Test Project 1 - Material End2End
Administrator	Administrator	ISA Distribution	Test Project 2 - TestProject2PD1
QE User Allison	QEUserA	Conduct Position	Sales Manager - Sales Data Entry
QE User Cory	QEUserC	Conduct Position	Sales Manager - Sales Data Entry
QE User D	QEUserD	Conduct Position	Sales Manager - Sales Data Entry
QE User Jay	QEUserJ	Conduct Position	Sales Manager - Sales Data Entry
QE User Karen	QEUserK	Conduct Position	Sales Manager - Sales Data Entry
ReadOnly User	ReadOnly	Conduct Position	Monitor - Sales Data Entry

In the consolidate role migration scenario, the comparison of what is proposed to be migrated compared to the existing applications could result in users having access to content that they do not currently have. Alternatively, it might result in them having access based upon current application assignments, but then having the DSP security setup misaligned to this.



Role Content Comparison with Baseline

NAME ▼	USER ID	CONTENT TYPE	CONTENT DESCRIPTION	FOUND IN APPLICATION	FOUND IN DATASET TO MIGRATE	STATUS
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_ED_EDR_OrgUnitDefaulted : ExternalData	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_ED_EDR_OrgUnitDefaulted : Post	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_ED_EDR_OrgUnitDefaulted : Review	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Later : Data	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Later : Post	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Later : Review	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Now : Data	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Now : Post	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_Basic_Post_Now : Review	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_CustomPlant : Data	YES	YES	●
Administrator	Administrator	Compose Template Role	AutomationTeam - BDC_MM02_CustomPlant : Post	YES	YES	●

Step 7 Upgrade DSP

At this point, DSP can be upgraded to version 7.1 or above.

Post-Upgrade Steps: Migration Scenario: Consolidate

These second set of steps must be performed AFTER the update to 7.1 to complete the migration to centralized security.

8. Synchronize Security Definition Keys
9. Change Migration Mode to Live
10. Validate the Roles
11. Migrate Roles
12. Assign Users to Roles
13. Review Migration Status
14. Reconcile System Admin Security with Application Security

Step 8 Synchronize Security Definition Keys

In order to seed the new Security Definitions with the data from each application, a DSP administrator must:

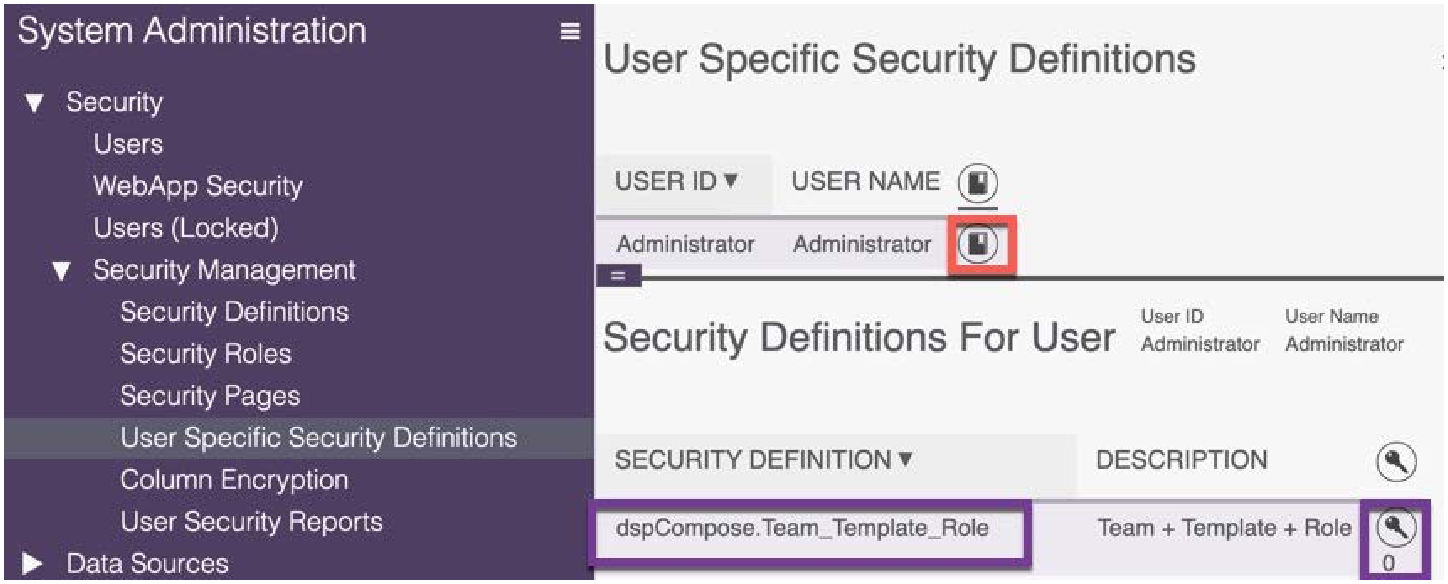
1. Log in to DSP.
2. Select **Admin** > **Security** > **Security Management** > **User Specific Security Definitions** in the *Navigation* pane.
3. Click the **Definitions** icon for the Administrator user.

Perform the following, depending on the application security that is being migrated to central security:

NOTE: Opening the *User Specific Keys* page as described in the following sections runs a plugin that synchronizes the DSP security tables with each individual application.

Synchronize dspCompose

Click the **Keys** icon for the **dspCompose.Team_Template_Role** security definition on the *Security Definitions for User* page.



User Specific Security Definitions

USER ID ▼	USER NAME
Administrator	Administrator

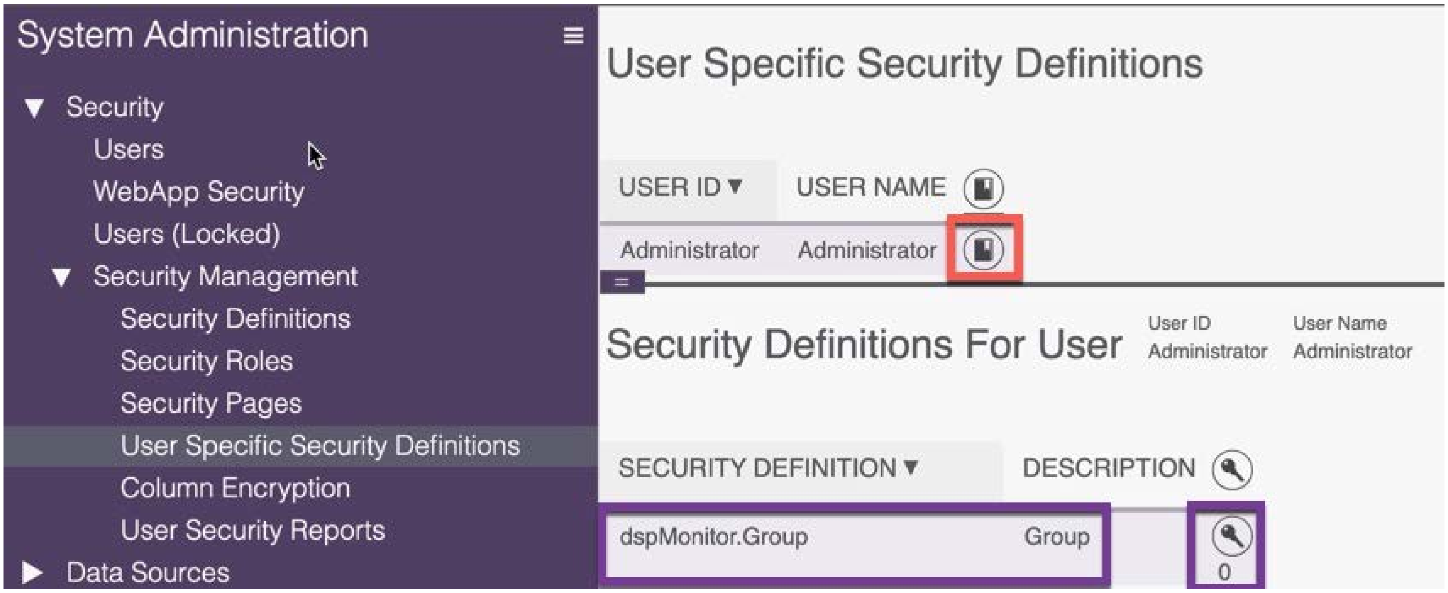
Security Definitions For User

User ID: Administrator
User Name: Administrator

SECURITY DEFINITION ▼	DESCRIPTION	
dspCompose.Team_Template_Role	Team + Template + Role	0

Synchronize dspMonitor

Click the **Keys** icon for the **dspMonitor.Group** security definition on the *Security Definitions for User* page.



User Specific Security Definitions

USER ID ▼	USER NAME
Administrator	Administrator

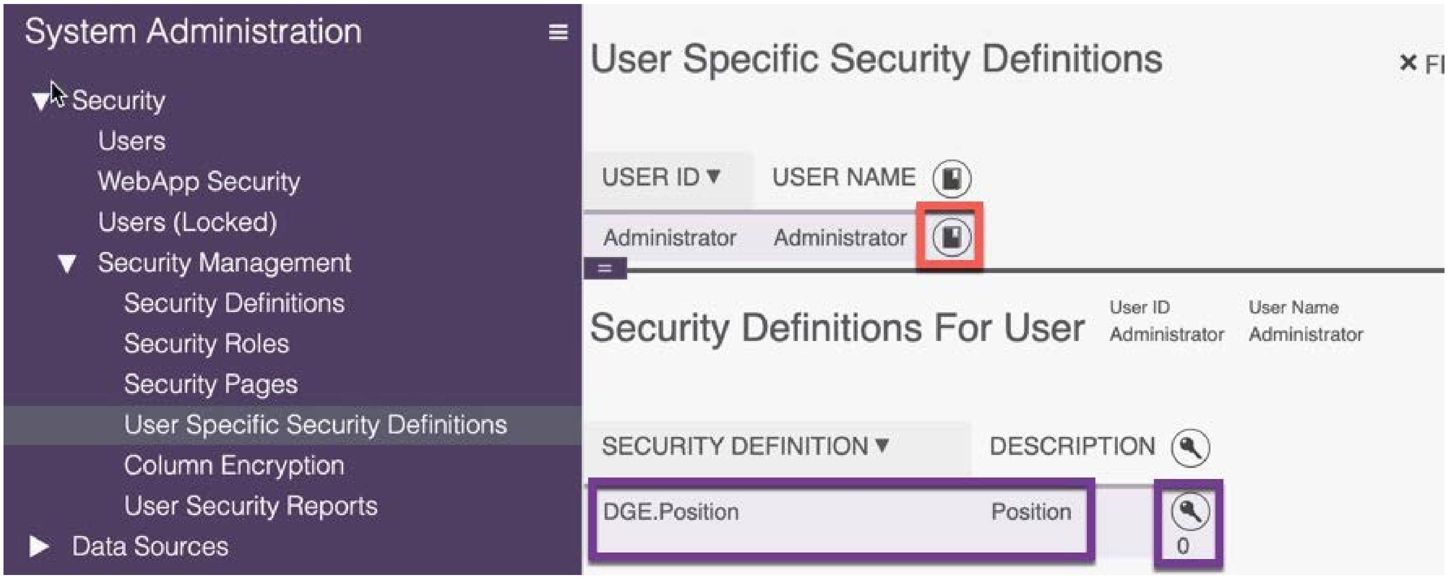
Security Definitions For User

User ID: Administrator
User Name: Administrator

SECURITY DEFINITION ▼	DESCRIPTION	
dspMonitor.Group	Group	0

Synchronize dspConduct

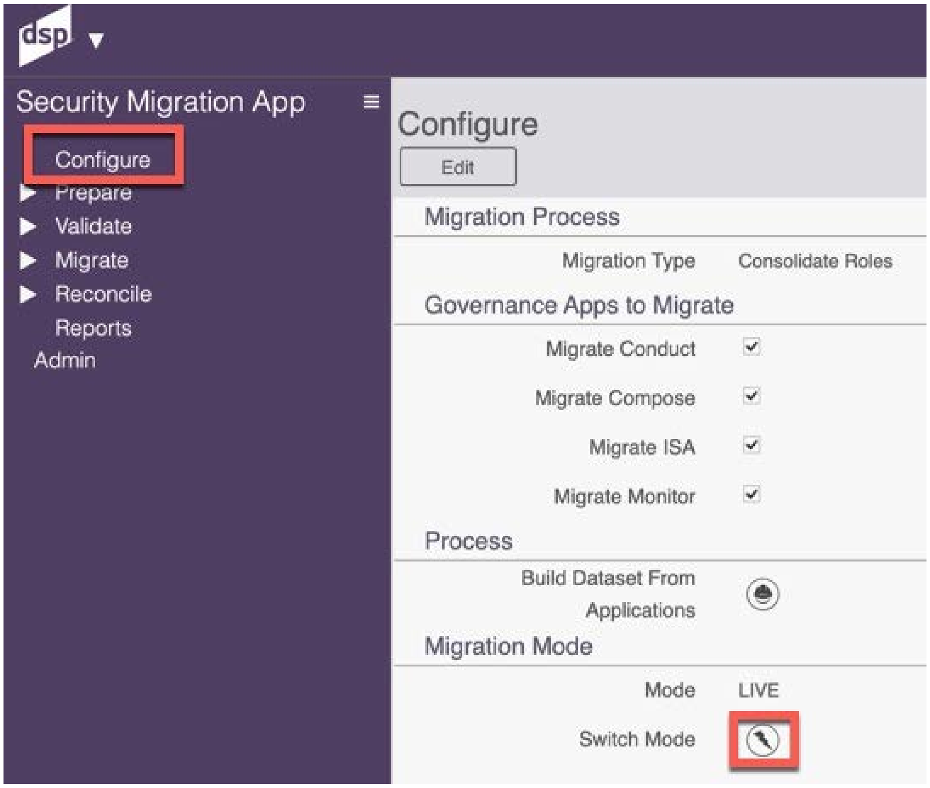
Click the **Keys** icon for the **DGEPosition** security definition on the *Security Definitions for User* page.



Step 9 Change Migration Mode to Live

By default, the utility is installed in SIMULATION mode. This mode does not allow any migration into the underlying DSP security tables. It does, however, allow all the planning and preparation work to be done BEFORE DSP is upgraded to version 7.1 or above.

After upgrade from a DSP version of 7.0.6 or below to DSP 7.1 or above, the utility can be switched into LIVE mode. Making this switch activates functionality that enables the migration to take place.



Configure

Migration Process

Migration Type: Consolidate Roles

Governance Apps to Migrate

- Migrate Conduct ☑
- Migrate Compose ☑
- Migrate ISA ☑
- Migrate Monitor ☑

Process

Build Dataset From Applications

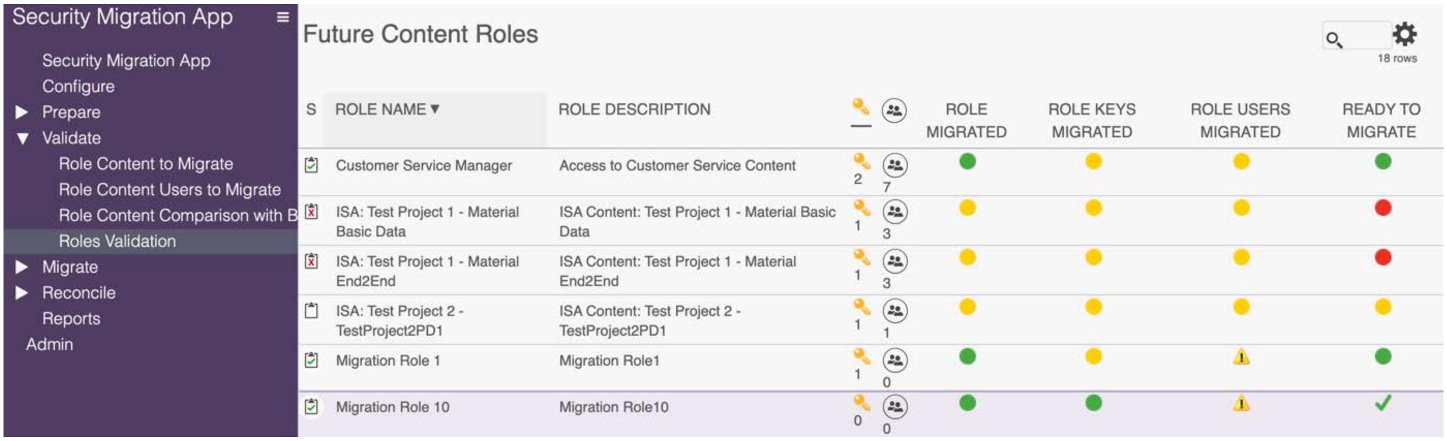
Migration Mode

Mode: LIVE

Switch Mode

Step 10 Validate the Roles

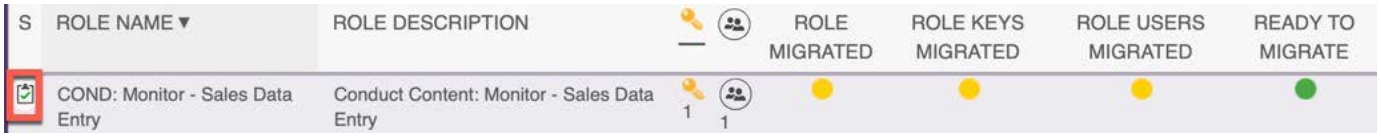
Before a Role can be migrated, it must pass some basic validations and the 'Ready to Migrate' indicator must be set to 'Green'.



Future Content Roles

S	ROLE NAME ▾	ROLE DESCRIPTION	🔑	👥	ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
	Customer Service Manager	Access to Customer Service Content	2	7	🟢	🟡	🟡	🟢
	ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	1	3	🟡	🟡	🟡	🔴
	ISA: Test Project 1 - Material End2End	ISA Content: Test Project 1 - Material End2End	1	3	🟡	🟡	🟡	🔴
	ISA: Test Project 2 - TestProject2PD1	ISA Content: Test Project 2 - TestProject2PD1	1	1	🟡	🟡	🟡	🟡
	Migration Role 1	Migration Role1	1	0	🟢	🟡	⚠	🟢
	Migration Role 10	Migration Role10	0	0	🟢	🟢	⚠	✓

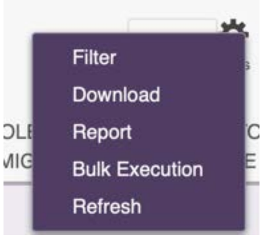
Trigger the validations for a single role by clicking the **Validate Record** icon.

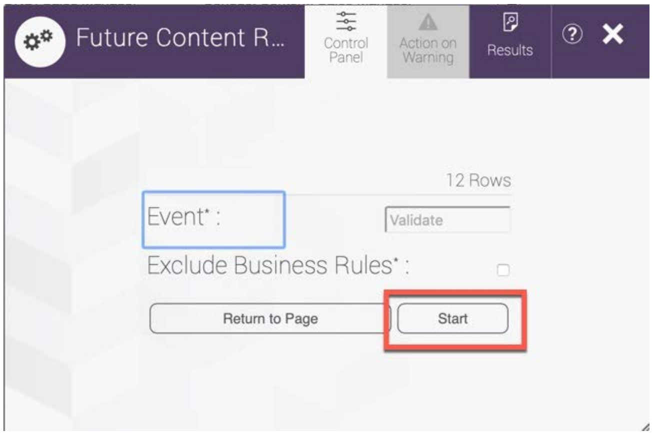


S	ROLE NAME ▾	ROLE DESCRIPTION	🔑	👥	ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	🟡	🟡	🟡	🟢

Trigger the validations to run on multiple roles using the Bulk Execution feature.

Click the **More Actions** (small gear) icon and select **Bulk Execution**.





12 Rows

Event* :

Validate

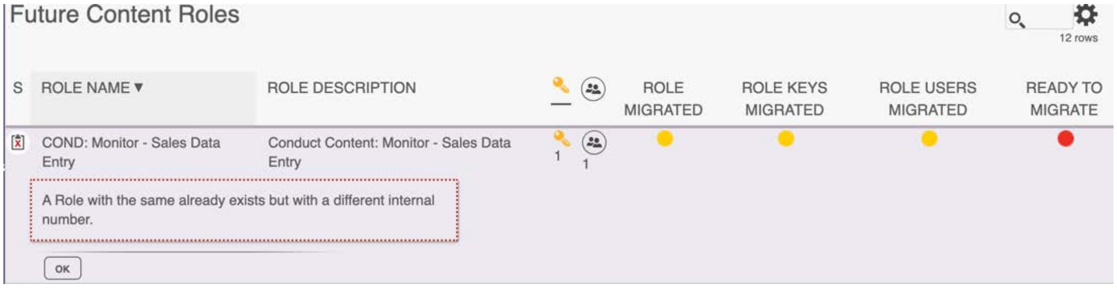
Exclude Business Rules* : □

Return to Page | Start

The following validation checks will be performed:

- Checks that a Role with same name but different internal GUID does not already exist.
- Checks that the Content Assigned to a Role has a Security Key assigned to it.

If any of these fails, an error message displays. If the record passes validation, it is set to 'Ready to Migrate' and available to migrate.


Future Content Roles

12 rows

S	ROLE NAME ▾	ROLE DESCRIPTION			ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
☒	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	●	●	●	●

A Role with the same already exists but with a different internal number.

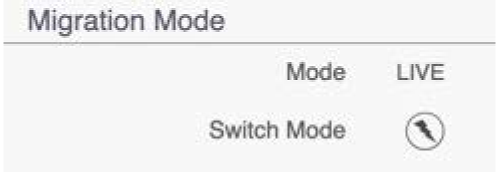
OK

NOTE: If a validation fails with the message above, ensure you've synchronized the DSP Security Definitions with each application for which the security is being migrated. Refer to *Step 8 Synchronize Security Definition Keys* for more information.

Step 10 Migrate Roles

Only Roles that have passed validation are available for migration. These roles have a green indicator in the ‘Ready To Migrate’ column.

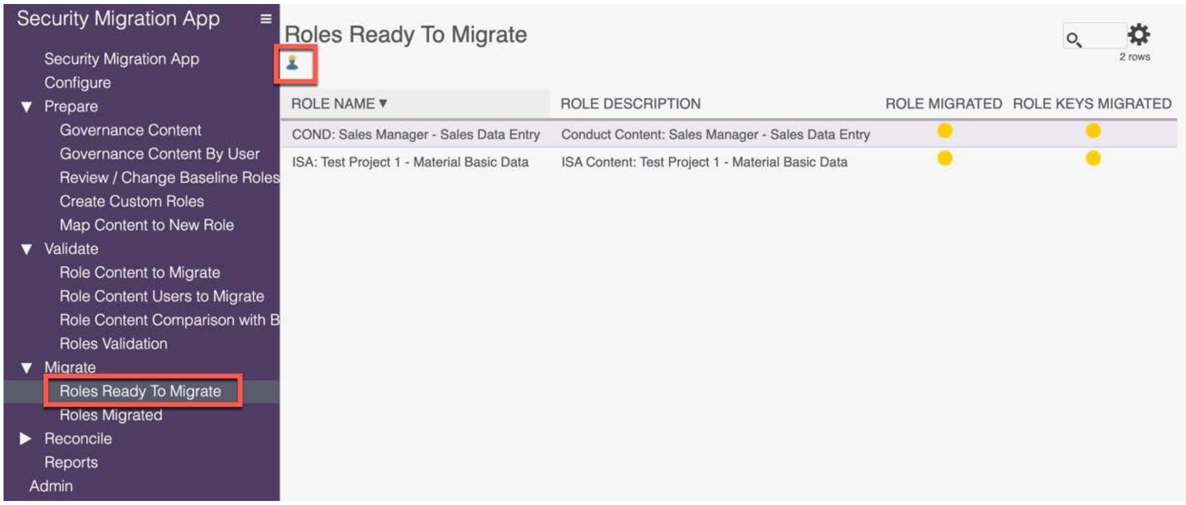
NOTE: Configuration ‘Migration Mode’ MUST be set to ‘LIVE’ in order to perform the migration tasks. Refer to *Step 9 Change Migration Mode to Live* for more information.



Migration Mode

Mode LIVE

Select one or more records and click the **Migrate Role** button.



Roles Ready To Migrate

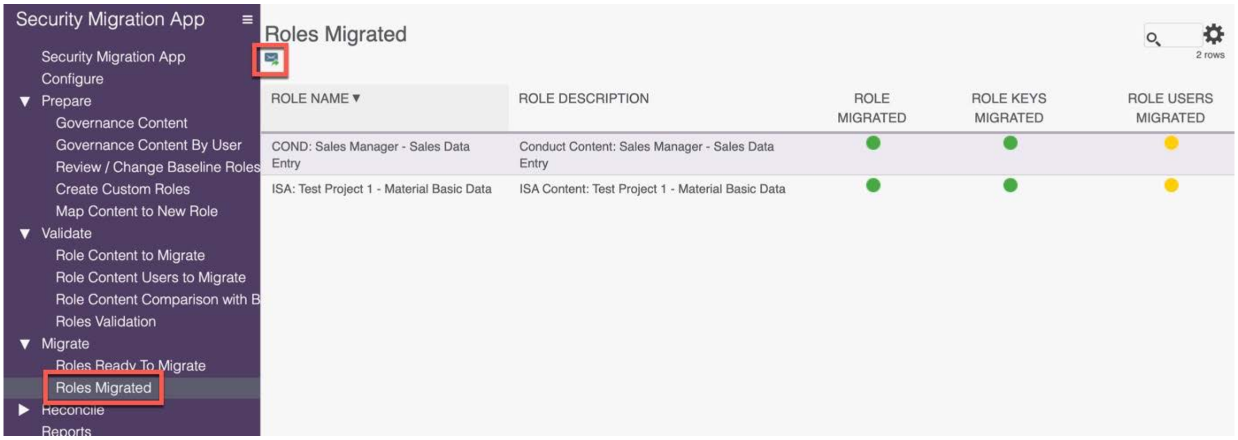
ROLE NAME ▾	ROLE DESCRIPTION	ROLE MIGRATED	ROLE KEYS MIGRATED
COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	●	●
ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	●	●

TIP! It’s advisable to migrate a couple of roles end to end first and then check the results. Once the process has been confirmed to work as intended, the rest of the roles can be migrated.

Step 11 Assign Users to Roles

Once a Role and its Role Keys Value (Content) has been migrated, the User Role Staging functionality can be used to assign users to roles.

1. To populate the user role staging, select **Migrate** > **Roles Migrated** in the navigation pane.
2. Select user records.
3. Click the **Send to User Role Staging** button in the Page toolbar.

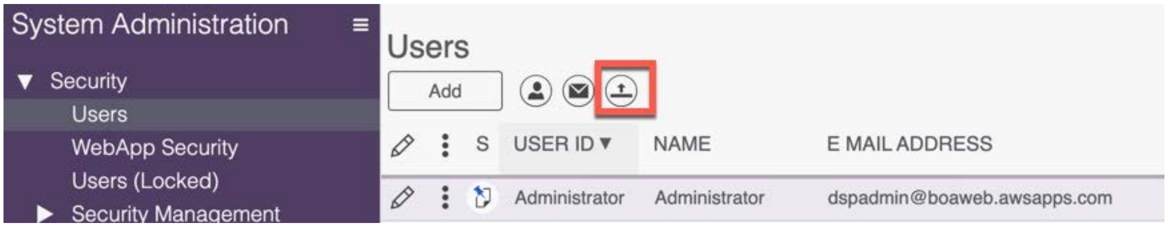


Roles Migrated

ROLE NAME ▾	ROLE DESCRIPTION	ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED
COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	●	●	●
ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	●	●	●

This functionality pushes the User to Assignment Records to the User Role Staging table. From here, they can be assigned to the Role and any associated content to which they need to be assigned.

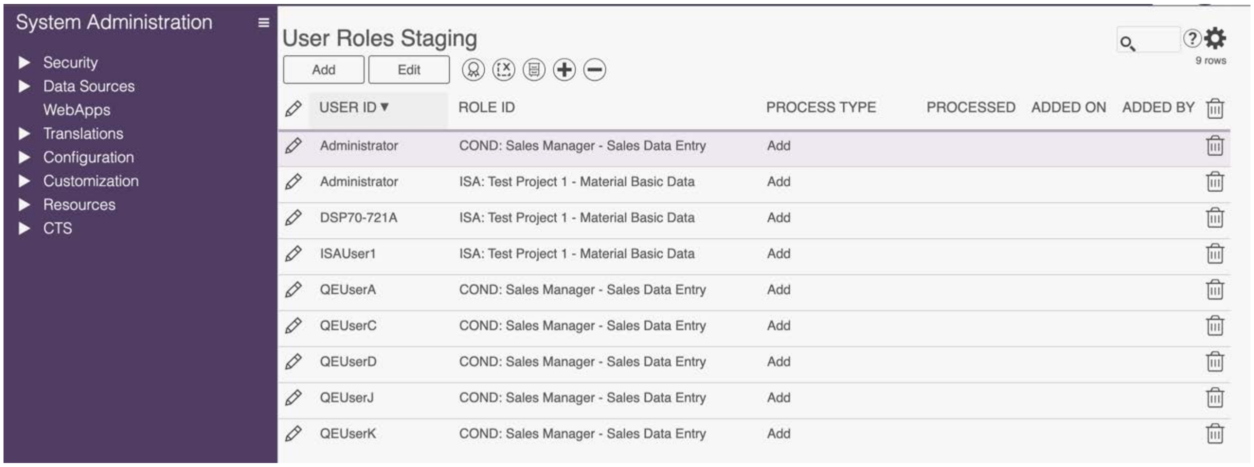
1. Select **Admin** > **Security** > **Users.**
2. Click the **User Role Staging** button.



Users

S	USER ID ▾	NAME	E MAIL ADDRESS
	Administrator	Administrator	dspadmin@boaweb.awsapps.com

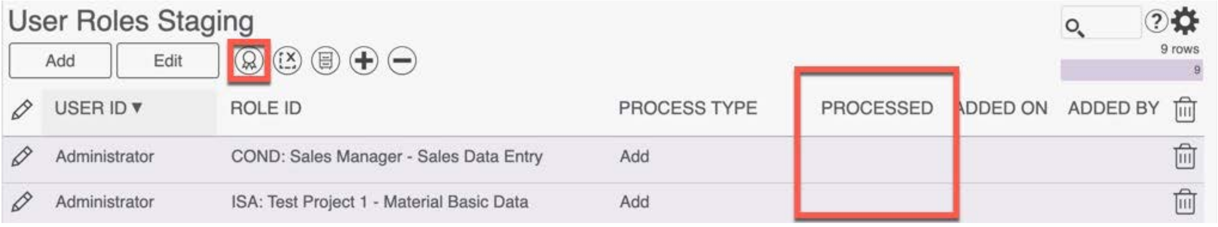
The User to Role assignment records are pushed into the Staging table and are available to process with process type ‘ Add’. Before adding users, validate the records.



User Roles Staging

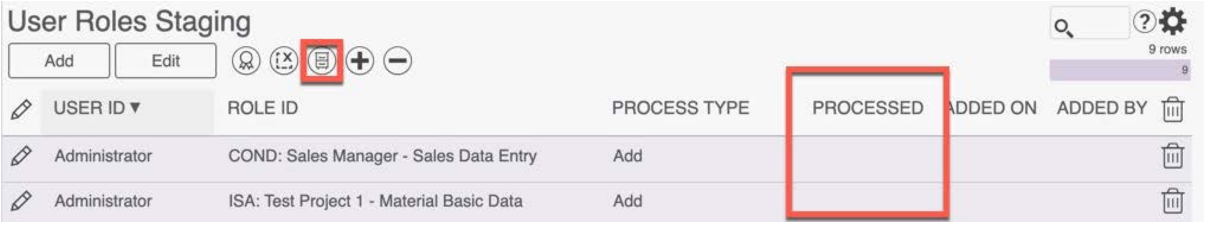
USER ID ▾	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
Administrator	COND: Sales Manager - Sales Data Entry	Add			
Administrator	ISA: Test Project 1 - Material Basic Data	Add			
DSP70-721A	ISA: Test Project 1 - Material Basic Data	Add			
ISAUser1	ISA: Test Project 1 - Material Basic Data	Add			
QEUserA	COND: Sales Manager - Sales Data Entry	Add			
QEUserC	COND: Sales Manager - Sales Data Entry	Add			
QEUserD	COND: Sales Manager - Sales Data Entry	Add			
QEUserJ	COND: Sales Manager - Sales Data Entry	Add			
QEUserK	COND: Sales Manager - Sales Data Entry	Add			

Validate all records to check that a user has not already been assigned to the role. If the user is already assigned, a check mark with appear in the Process column.



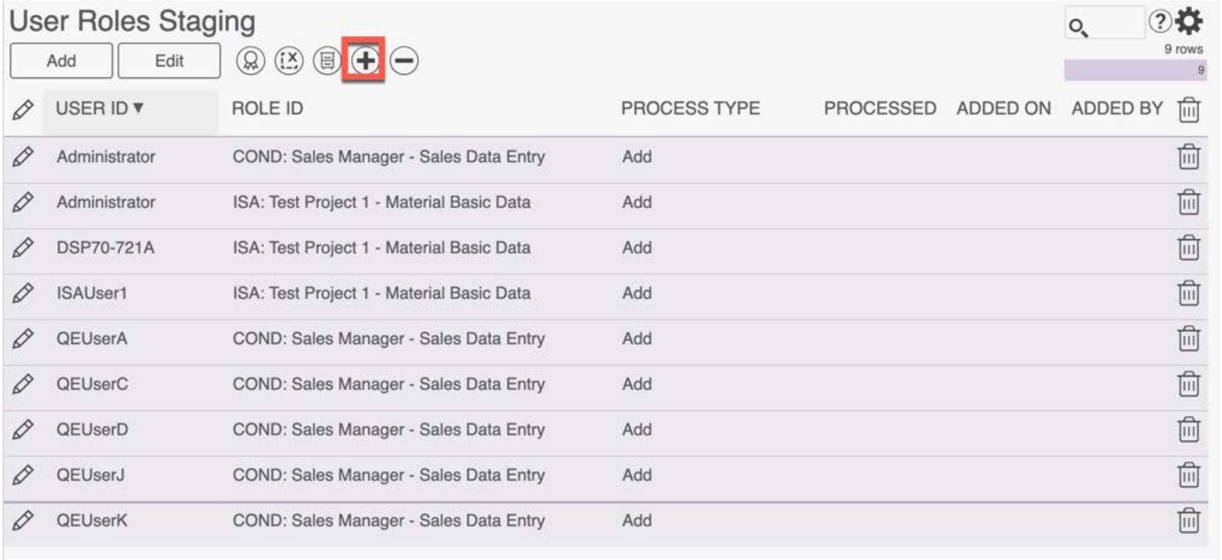
	USER ID ▼	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
	Administrator	COND: Sales Manager - Sales Data Entry	Add			
	Administrator	ISA: Test Project 1 - Material Basic Data	Add			

These records do not need to be assigned and can be removed by clicking the **Removed Processed** button.



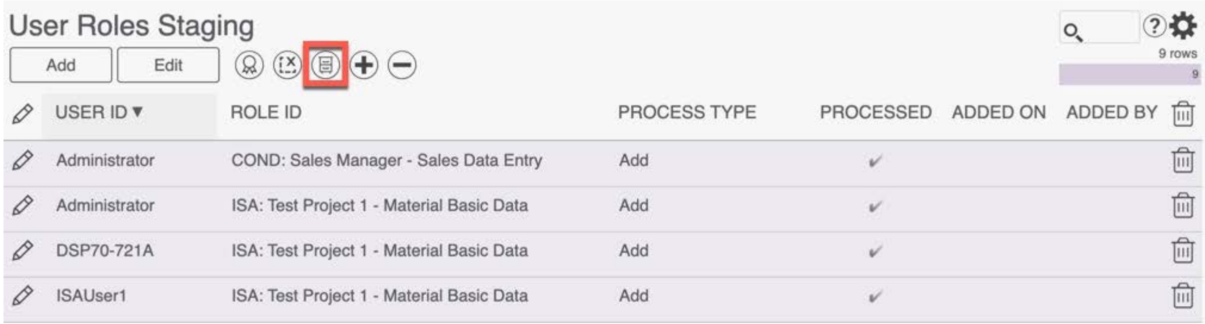
	USER ID ▼	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
	Administrator	COND: Sales Manager - Sales Data Entry	Add			
	Administrator	ISA: Test Project 1 - Material Basic Data	Add			

Users can be assigned to the Role by selecting one or more records and then clicking the **Add Role** button.



	USER ID ▼	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
	Administrator	COND: Sales Manager - Sales Data Entry	Add			
	Administrator	ISA: Test Project 1 - Material Basic Data	Add			
	DSP70-721A	ISA: Test Project 1 - Material Basic Data	Add			
	ISAUser1	ISA: Test Project 1 - Material Basic Data	Add			
	QEUserA	COND: Sales Manager - Sales Data Entry	Add			
	QEUserC	COND: Sales Manager - Sales Data Entry	Add			
	QEUserD	COND: Sales Manager - Sales Data Entry	Add			
	QEUserJ	COND: Sales Manager - Sales Data Entry	Add			
	QEUserK	COND: Sales Manager - Sales Data Entry	Add			

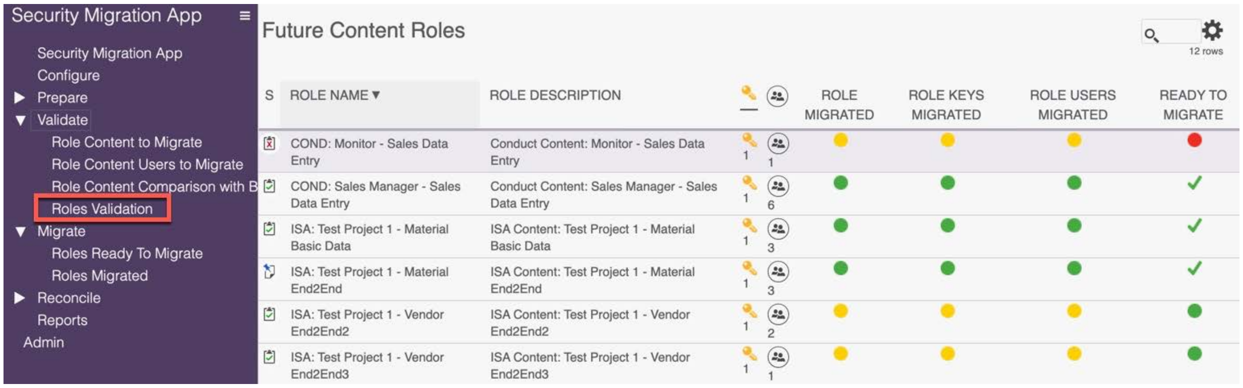
The processed records can be removed by clicking the **Remove Processed** button.



	USER ID ▼	ROLE ID	PROCESS TYPE	PROCESSED	ADDED ON	ADDED BY
	Administrator	COND: Sales Manager - Sales Data Entry	Add	✓		
	Administrator	ISA: Test Project 1 - Material Basic Data	Add	✓		
	DSP70-721A	ISA: Test Project 1 - Material Basic Data	Add	✓		
	ISAUser1	ISA: Test Project 1 - Material Basic Data	Add	✓		

Step 12 Review Migration Status

To check the overall status of the role migration, select **Validate** > **Roles Validation** to validate the records manually or via Bulk Execution.



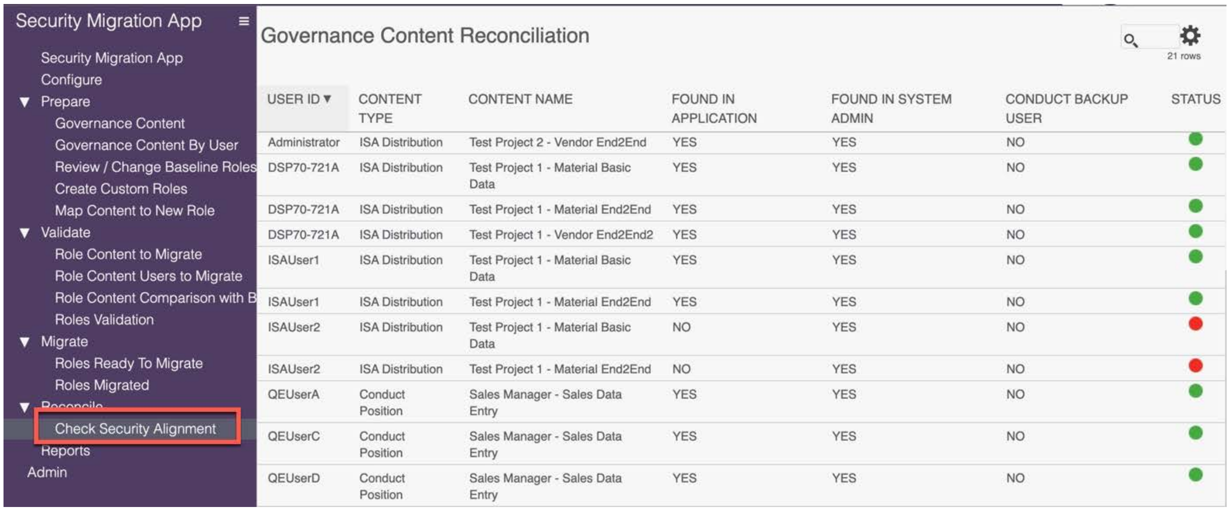
Future Content Roles

S	ROLE NAME ▼	ROLE DESCRIPTION	🔑	👥	ROLE MIGRATED	ROLE KEYS MIGRATED	ROLE USERS MIGRATED	READY TO MIGRATE
☒	COND: Monitor - Sales Data Entry	Conduct Content: Monitor - Sales Data Entry	1	1	🟡	🟡	🟡	🔴
☑	COND: Sales Manager - Sales Data Entry	Conduct Content: Sales Manager - Sales Data Entry	1	6	🟢	🟢	🟢	✓
☑	ISA: Test Project 1 - Material Basic Data	ISA Content: Test Project 1 - Material Basic Data	1	3	🟢	🟢	🟢	✓
↻	ISA: Test Project 1 - Material End2End	ISA Content: Test Project 1 - Material End2End	1	3	🟢	🟢	🟢	✓
☑	ISA: Test Project 1 - Vendor End2End2	ISA Content: Test Project 1 - Vendor End2End2	1	2	🟡	🟡	🟡	🟢
☑	ISA: Test Project 1 - Vendor End2End3	ISA Content: Test Project 1 - Vendor End2End3	1	1	🟡	🟡	🟡	🟢

Step 13 Reconcile System Admin Security with Application Security

Once the migration of the roles and user role assignment has been completed, review the following report. This report shows User Content Access based upon System Administration Security Setup and the User Content Access that is assigned within each governance applications.

Once the migration is complete, these should be aligned and therefore, any misalignment may indicate that there have been some failures during the synchronization of Security to the various applications or that some roles have not been fully created.



Governance Content Reconciliation

USER ID ▼	CONTENT TYPE	CONTENT NAME	FOUND IN APPLICATION	FOUND IN SYSTEM ADMIN	CONDUCT BACKUP USER	STATUS
Administrator	ISA Distribution	Test Project 2 - Vendor End2End	YES	YES	NO	🟢
DSP70-721A	ISA Distribution	Test Project 1 - Material Basic Data	YES	YES	NO	🟢
DSP70-721A	ISA Distribution	Test Project 1 - Material End2End	YES	YES	NO	🟢
DSP70-721A	ISA Distribution	Test Project 1 - Vendor End2End2	YES	YES	NO	🟢
ISAUser1	ISA Distribution	Test Project 1 - Material Basic Data	YES	YES	NO	🟢
ISAUser1	ISA Distribution	Test Project 1 - Material End2End	YES	YES	NO	🟢
ISAUser2	ISA Distribution	Test Project 1 - Material Basic Data	NO	YES	NO	🔴
ISAUser2	ISA Distribution	Test Project 1 - Material End2End	NO	YES	NO	🔴
QEUserA	Conduct Position	Sales Manager - Sales Data Entry	YES	YES	NO	🟢
QEUserC	Conduct Position	Sales Manager - Sales Data Entry	YES	YES	NO	🟢
QEUserD	Conduct Position	Sales Manager - Sales Data Entry	YES	YES	NO	🟢