DSP 7.1.4 Centralized Security

Migration Manual

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

Syniti | BackOffice ASSOCIATES

Contents

Overview

This document describes how user security is applied in DSP 7.1.4 and later. Upgrades from versions 7.0.6 or below to 7.1.4 or above may require changes to a client's security roles.

This document contains the following sections:

- DSP Centralized Security Model Introduction
- Manual Migration

DSP 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 Mass Maintenance (formerly dspCompose), administrative tasks were required in both Mass Maintenance 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 7.1.4, 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, 7.1.4 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 7.1.4, 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 7.1.4, 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 Mass Maintenance.

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.

Security Reports

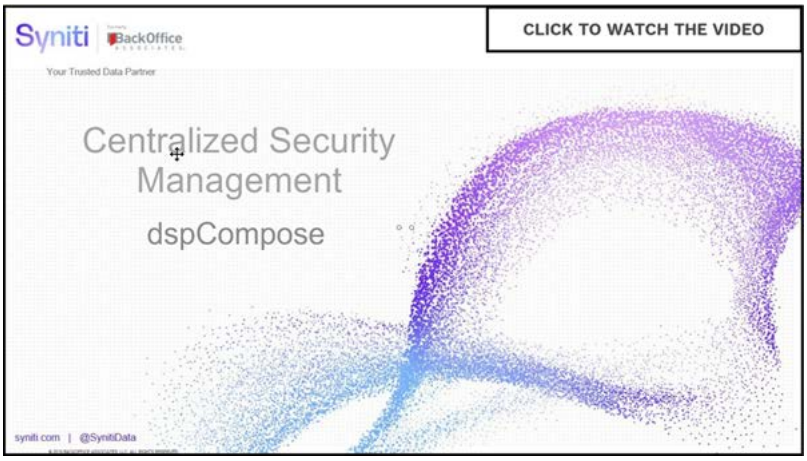
- User Security reports have been added to System Administration to provide details about how centralized security is configured, including:
    - All users in the platform
    - All security roles in the platform
    - WebApp Groups assigned to security roles
    - The pages and content security roles 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 ISA Distributions, dspMonitor Groups and Mass Maintenance 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 Information Steward Accelerator Distributions for 7.1.4 and later

- Changes to Mass Maintenance Template Roles for 7.1.4 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 7.1.4 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

Watch the Central Security Manual Migration video.

After upgrading to 7.1.4 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.