Syniti Solutions

Release Notes

Version 7.1

Software Release Date: 11/14/19

BackOffice Associates, LLC
12000 Findley Road
Suite 200
Johns Creek, GA 30097

T +1 770-246-1287
F +1 770-246-1289
info@boaweb.com
www.boaweb.com

Contents

Overview

Syniti Solutions 7.1 contains:

- Enhancements
- Resolved Issues

NOTE: Version 7.1 introduces a new centralized security model and users of dspMonitor, dspConduct and dspCompose must update security roles when upgrading to 7.1. Refer to the *Syniti Solutions Centralized Security Migration Manual* for important information about using security in the DSP in version 7.1. Consult this manual BEFORE updating to 7.1.

Enhancements

Data Stewardship Platform (DSP®)

System Administration

Centralized Security

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 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 have been added to the platform that restrict access to content and that run rules when certain security-related events occur. 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, ISA, 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 Addons. 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.

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, ISA Distributions, 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 Valus. Refer to Compare User Access to Content Between WebApps and System Administration for more information.
- A new set of report pages are available under Security Management, called Security Pages, to allow Security Administrators to see what pages are assigned to which WebApp groups, Security roles and Security Definitions. This new set of reports enables users to effectively and efficiently create new custom security roles and to grant security access to appropriate security roles. Refer to View Security by Page for more information.

Add Multiple Users Quickly with User Role Staging

- The *User Roles Staging* page has been added so that Administrators can stage user role assignments, either manually or using Excel Integration. Staging user roles allows a user to add multiple user role assignments in one process. Processing the records in this staging table adds and removes role assignments for selected users. If the roles have any security definition key values with associated events, these events will be run. Refer to Stage User Roles for more information.

Additional Enhancements

- The DSP is now delivered with a set of encrypted columns, such as passwords and connection strings. This feature allows Security and Data Source Administrators to monitor columns where encryption is either required or suggested for encrypted. Refer to Monitor Columns for Encryption for more information.
- The following tasks that were once performed in Common are now performed in System Administration:
  - Assign an Expiration Date to a User
  - Reset a User's Password
  - Send a Temporary Password to a New User

NOTE: The ability update the text in the password reset email has been removed. Additionally, the View Log In History icon has been removed from the *Users* page. This information is now accessible in System Administration Logs.

- To maintain consistency across DSP pages, the E Mail Address field on the *Users* page now displays as Email Address.
- The Excel Integration feature for mass user creation on the *Users* page now has additional fields available, facilitating the completing of users' profiles. Previous fields available: UserID, Name, Password, Anonymous and Language ID New fields available: UserID, Name, WindowsUserName, ExpirationDate, Anonymous, Telephone, TelephoneExtension, EMailAddress, LanguageID, DefaultPageID, StyleID and LocaleID
- The Security Definition menu and all sub-pages are now nested under a new menu option, titled Security Management. Under this menu, Security Administrators are now able to better manage security related to the platform and individual applications. They are also able to gain deeper insights into the overall DSP security setup.

DSP Add-ons

- When creating custom WebApp groups with DSP Add-ons, an Administrator user can use two new methods to quickly add pages and page permissions to it:
  - Copy a WebApp group to use the pages and page permissions (the ability to view, add, update or delete records on a page) as the basis for the new WebApp group.
  - Use Excel Integration on the *Group Pages* page to import a spreadsheet of pages and permissions for the new WebApp group.

    Refer to Customize Security Using DSP Add-Ons for more information.
- Custom WebApp groups created using DSP Add-Ons can now be updated after they are published. After the group is published, the Administrator user can:

  - Assign new pages to the WebApp group
  - Delete pages from the WebApp group
  - Change page permissions
  - Change security roles assigned to the WebApp group
  - Rename the WebApp group
  - Delete the WebApp group

- WebApp groups added in DSP Add-ons are no longer deleted on upgrade. In previous versions, users were required to republish any WebApp Groups created in DSP Add-ons after upgrade.
- Users can now CTS custom WebApp groups added to delivered WebApps that were created in DSP Add-ons.

Common

- The JDE System Type model is no longer delivered with the product.
- The trace level setting is used to indicate when the DSP should log information about DSP processes. This severity is now set to Debugging Disabled (0) for Common and dspCompose debug logs. Refer to Configure Debug Logs Settings for more information.
- The new *User Calendar* page allows users to view and change the calendar for a user, either individually or in bulk by utilizing Excel Integration pages. In dspConduct, the pages that use that use Calendar ID (for example, the *Position User, User Position* and *My Positions* pages) were updated to continue to work.

dspMigrate™

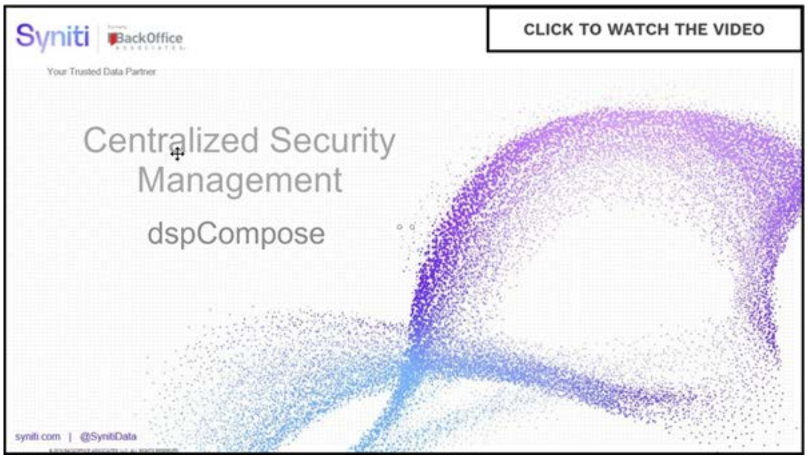
Transform

Users can now purge inactive target report segments that do not have records returned on all reports. The segments with no records display on the *All Business Reports (All Waves and Process Areas)* page until they are manually purged. Refer to Purge Inactive Segments for more information.

dspCompose

- From DSP release 7.1 onwards, users will no longer be able to be assigned to a Template or Template Roles from directly within dspCompose. It will still be possible to view user assignments to Positions. It will also no longer be possible to copy a user's template role assignment, this functionality. Instead, users will have to be assigned the corresponding Security Definition Key Value, either directly to their user, or via the assignment of their user to a Role that contains the key value. Watch the video for an overview of changes to dspCompose template roles for

7.1.



- The order of items in the dspCompose Navigation menu has changed. The Configuration menu in dspCompose contains:
  - Roles
  - Org Units
  - Users
  - Change Request Status
  - Archives
- The Setup menu contains:
  - Parameters
  - External Data Email Accounts
  - Workflow Message
  - Email Validation
  - Request Status
  - Mass Change Exclude Column
- The Troubleshooting menu contains
  - Request Role (Finish Download)
  - Roles (Execute)
  - Data Services Job Executor
- When a user is copied in dspCompose, the user no longer inherits dspCompose Template Roles from the user selected in the 'Copy User ID' field. Only org unit assignments are copied to the new user. Refer to Copy Org Unit Assignments for more information.

dspMonitor

- Users will no longer be able to be assigned to Monitor Groups from directly within dspMonitor. It will still be possible to view user assignments to Groups. Instead, users will have to be assigned the corresponding Security Definition Key Value, either directly to their user, or via the assignment of their user to a Role that contains the key value. Watch the video for an overview of changes to dspMonitor groups for 7.1.

Your Trusted Data Partner

CLICK TO WATCH THE VIDEO

Centralized Security Management dspMonitor

syniti.com | @SynitiData

- The *Data Quality Score Thresholds* page is now accessible via dspMonitor > Configuration > Data Quality Score Thresholds.

dspConduct

Permissions on pages assigned to the dspConduct Read Only WebApp group have been updated so that read only access is applied correctly.

From DSP release 7.1 onwards, users will no longer be able to be assigned to a Position from directly within dspConduct. It will still be possible to view user assignments to Positions. Instead, users will have to be assigned the corresponding Security Definition Key Value, either directly to their user, or via the assignment of their user to a Role that contains the key value. Watch the video for an overview of changes to dspMonitor groups for 7.1.

Your Trusted Data Partner

CLICK TO WATCH THE VIDEO

Centralized Security Management dspConduct

syniti.com | @SynitiData

Resolved Issues

dspConduct™

- There were several dspConduct dashboards that did not include archived data. The impacted charts referenced the views webDashboard_RequestMinStartTimeSel and webDashboard_RequestMaxFinishedOnSel. This issue has been fixed by replacing the table ttRequestRoleLog (active requests) with apiRequestRoleLogAllSel (active and archived) in these two views. [DSP70-698]
- An issue occurred where the Count Metrics displayed week counts that did not take the year into consideration, so two years with week x would both display, causing each year's Count Metrics to display a different week count. With this fix, the dashboard shows the correct number of week / year records. [DSP70-707]

dspMigrate™

Transform

Fixed an issue where a target report, target source report, or target Data Services report did not display on the *All Business Reports (All Waves and Process Areas)* page in certain cases. If the report had segments, but there were no records returned for the segments, the segments were deleted in error. With the fix, when a segment is added and users are assigned to it, even if a report has no records for a segment, the segment is not removed. Additionally, segmented reports display on the A*ll Business Reports (All Waves and Process Areas)* page, even if the target report segment contains no records. Segments with no records must be purged to be removed. Refer to Purge Inactive Segments for more information. [DSP70-552]

Map

Previously, when a duplicate source table was added to the *Target Sources* page, the validation rule should have prompted the user to override the source table name. Instead, the validation rule failed. The validation rule has been fixed to properly prompt the user to override the duplicate source table name. [DSP70-776]

dspCompose™

When using comparison approvals, the *Approve* page did not display all changes to the data entry page in certain cases. If the data entry page contained a list box, and the list box was updated to the value None, the *Approve* page did not display an arrow next to the list box, indicating that a change had been made. With the fix, an arrow displays next to list boxes with this update on the *Approve* page. [DSP70-696]

Data Stewardship Platform (DSP®)

An issue occurred where, when users enabled page logging for a data source and performed concurrent actions that produced log files, a concurrency error caused those log files to be written to a fallback file path. This frequently produced a logging file path error message. With this fix, the NLog versions were replaced in the library, which stabilized the concurrency error that was forcing the logging files to write to the fallback file path. [DSP70-759]

System Administration

An issue occurred when users registered a security definition and added more than one key column for a multi-part key. In these instances, the system created duplicate entries in the SecurityDefinitionKeyValue table and incorrectly processed the multi-part keys. Old values for multi-part keys are now properly removed when the security definition's key columns are modified.

In addition to this fix, a System Provided flag has been added to delivered security definitions. Security definitions with this flag cannot be changed by users. Refer to Register Security Definitions for more information. [DSP70-743]

Integrate

In previous versions, if multiple background posts were executed from Integrate, they ran single threaded (one at a time). These postings worked this way because they were saved with a JobQueue GroupName of 'Integrate - Post,' which indicated to DSP that they should be run single threaded. With this fix, the Integrate 'Process Name' is used for the JobQueue GroupName, and now posts related to different processes run in parallel. [DSP70-671]

dspTrack

With User Management being moved from Common to System Administration, a new method to default a calendar to dspTrack users was designed by creating new the security definition events Plan Role and Project Role. Now, when a user is assigned to a role containing a Security Definition Key Value that belongs to one of these security definitions, or when a Security Definition Key Value that belongs to one of these security definitions is added to the user, the calendar defined by the **Default Plan Calendar** field on the *Parameters* page in dspTrack is assigned to users with no calendar set.

Last Updated on 11/13/2019