Syniti Solutions

Release Notes

Version 7.1.1

Software Release Date:12/16/2019

Contents

Overview

NOTE: If you are upgrading from 7.0.6 or below to 7.1 or above, you may need to migrate your security settings to use centralized security. Users of Data Quality (formerly dspMonitor), Master Data Management (formerly dspConduct), ISA and Mass Maintenance (formerly dspCompose) must update security roles when upgrading to 7.1. Refer to the Centralized Security Migration Manual for important information about using security in the DSP in version 7.1 and later. Consult this manual BEFORE updating to 7.1, as an analysis of current security assignments must be completed before the DSP can be updated.

Syniti Solutions 7.1.1 contains.

- Enhancements
- Resolved Issues

Enhancements

As part of the Syniti rebranding effort, the temporary license email, which is sent to users who request a temporary license to log in to the DSP, has been updated from no-reply@boaweb.com to no-reply@syniti.com.

Data Stewardship Platform (DSP®)

System Administration

- To help streamline user management security, User Management was added to delivered security roles. The User Management role includes access to the UserManagement and ContentKeySecurity WebApp Groups. Users assigned to this role can create security roles with a Role Type of Content. They can also assign security definition key values to users and to security roles with Role Types of Standard and Content. The role restricts access to security, only allowing access to the pages used to create users and assign them to Application roles. Refer to Delivered Security Roles for more information.

- To improve security, the following columns were hidden for the FieldAndValueMapper WebApp Group:

  - Refresh
  - ExportFieldMappings
  - ImportFieldMappings
  - SyncFromTargetDesign
  - UserColumnNotDefined
  - RemoveValues
  - Process
  - Build Reports
  - BuildReportsWithRemediation

- Create

- CreateAllRules

- TargetTableImport

- Hard-coded UCVs were replaced with a generic webUserSecurityUcv that points to the cMap ztPageGroupColumnStatus table. If entries for AutoGen pages' columns are included in the cMap ztPageGroupColumnStatus table, the generic webUserSecurityUcv will provide correct results. All cMap page-specific UCV registrations were replaced with webUserSecurityUcv, which checks against all aspects of user security.

Syniti Data Replication (formerly DBMoto)

The DSP is now compatible with Syniti Data Replication version 9.6.1. New DSP installations now default to the 64-bit version of Syniti Data Replication; the 32-bit version of Syniti Data Replication has been removed from the DSP installer.

Resolved Issues

With Google Chrome version 78, check boxes on Horizontal pages did not work properly; the check box was made invisible and an image rendered on top. Therefore, users were unable to update the check box. This issue has been fixed where check boxes work as expected in Google Chrome version 78. [DSP70-834]

Mass Maintenance (formerly dspCompose)

The User Template Role Access page in Mass Maintenance has been updated to remove functionality to grant and deny users access to templates at a global level as this method of assigning security is not compatible with the centralized security management introduced in 7.1. [DSP70-799]

Master Data Management (formerly dspConduct)

- Fixed an error that caused a process to fail when the user clicked the Create Control Table button on the Scenario Role Task page under certain conditions. If another ScenarioRoleTask with the "Active In Scenario Role" flag unchecked is associated to the same Task as the ScenarioRoleTaskPage being processed, Invalid column name 'FieldName' errors displayed and the process failed. The failure occurred because the Control Table was created with only the key fields, missing all the non-key fields. With the fix, the Create Control Table button creates and populates the control table including both key fields and non-key fields and the process ends successfully. [DSP70-813]

- In previous versions, when copying a position, that position's users could be copied to the new position. Since 7.1, users are assigned to positions using centralized security, and can no longer be assigned to positions as part of the position copy process. [DSP70-823]

Data Stewardship Platform (DSP®)

An issue occurred where the DSP displayed a red "service stopped" icon even when all services were running. This issue occurred when the database and app servers were not located in the same time zone. With the fix, this difference in time zones no longer triggers the "service stopped" icon to display. [DSP70-831]

Collect

- An issue occurred in the Vertical view of the Target Sources page when users populated the SAP Settings with data that included the string 'PWD'. When a user clicked the Test SAP Connection button, this error displayed:
Test SAP Logon Failed: Argument Length must be greater than zero.
With this fix, including the string 'PWD' in the SAP connection information no longer triggers the Test SAP Logon Failed: Argument Length must be greater than zero error message. [DSP70-844]

- An issue occurred with the Test Connection process on the Collect Targets page where, when more than one Cransoft Service was running in the General Queue and the user clicked Test Connection for a target, an error message displayed:
Internal Error - Object reference not set to an instance of an object. An unhandled exception occurred during the execution of the plugin.
Supporting views have been changed to prevent the issue. With this fix, the exception no longer occurs and the Test Connection process completes as expected. [DSP70-500]

System Administration

- The Role Content Access Download report displays the friendly name of the key assigned to a role. However, the table joined in this report is SecurityDefinitionKeyValue, which has a two-column key for some components, such as Mass Maintenance. The view used to create this report was modified to de-duplicate the values for multi-column key assignments. [DSP70-814]

- An issue occurred on the Security Role Compare page where the page and group comparisons were displaying incorrect results. With this fix:

  o The Role Page Comparison Dynamic SQL determines the Access Matches based upon the page's inclusion in both roles, and based upon the Allow Select/Insert/Update and Delete indicators. If the page is not found in one of the roles, then the Access Matches field is set to NO.

  o The Role Group Comparison Dynamic SQL determines the Access Matches based upon the page's inclusion in both groups. If the group is not found in one of the roles, then the Access Matches field is set to NO. [DSP70-816]

Last Updated on 12/16/2019