.

SAP Accelerators by Syniti

Release Notes

Version 7.1.4

Software Release Date: 05/04/2020

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

SAP Accelerators by Syniti versions 7.1, 7.1.1, 7.1.2 and 7.1.3 were not released. The immediately prior release to 7.1.4 was version 7.0.6.

SAP Accelerators by Syniti 7.1.4 contains:

- New Feature
- Enhancements
- Resolved Issues
- Known Issues
- Enhancement Requests from the User Base

NOTE: If you are upgrading from 7.0.6 or below, you may need to migrate your security settings to use centralized security. Users of ISA and Mass Maintenance (formerly dspCompose) must update security roles when upgrading to 7.1.4. Refer to the Centralized Security Migration Manual for important information about using security in the DSP in version 7.1.4 and later. Consult this manual BEFORE updating to 7.1.4, as an analysis of current security assignments must be completed before the SAP Accelerators can be updated.

NOTE: The following SAP products are compatible with the DSP 7.1.4 release:

- SAP Information Platform Services 4.2 SP6
- SAP Data Services 4.2 SP12
- SAP Information Steward 4.2 SP12

However, these are not compatible with MS SQL Server 2019. For full DSP integration with these products running on MS SQL Server 2019, clients must wait until SAP releases MS SQL Server 2019 compatible versions. This is currently anticipated at the end of Q2 2020.

Align Column Encryption State for key Target Source column in Collect Before Upgrade

A new feature was introduced in DSP 7.1.4 whereby the SAP connection settings on a Collect Target Source are moved to a dedicated Data Source Registry record. During upgrade, the following DataGarage dgTargetSource table columns are used to create the new DSPCommon Data Source Registry records.

Database	Table	Column	Database	Table	Column
DataGarage	dgTargetSource	SAPPassword	DSPCommon	ttDataSourceRegistry	SAPPassword
DataGarage	dgTargetSource	SAPUserID	DSPCommon	ttDataSourceRegistry	SAPUserID
DataGarage	dgTargetSource	Instance	DSPCommon	ttDataSourceRegistry	SAPSystemID
DataGarage	dgTargetSource	RfcNameSpace Option	DSPCommon	ttDataSourceRegistry	RfcNameSpaceOption
DataGarage	dgTargetSource	SAPSystemNumber	DSPCommon	ttDataSourceRegistry	SAPSystemNumber
DataGarage	dgTargetSource	Client	DSPCommon	ttDataSourceRegistry	SAPClient
DataGarage	dgTargetSource	SAPServerHost	DSPCommon	ttDataSourceRegistry	SAPApplicationServer
DataGarage	dgTargetSource	Language	DSPCommon	ttDataSourceRegistry	SAPLanguage
DataGarage	dgTargetSource	SAPMsgServerHost	DSPCommon	ttDataSourceRegistry	SAPMessageServer
DataGarage	dgTargetSource	SAPLogonGroup	DSPCommon	ttDataSourceRegistry	SAPLogonGroup

As a result of these changes, BEFORE UPGRADING to version 7.1.4, you must review and confirm that the encryption state of these two sets of columns matches. If you do not confirm that the encryption state is identical in these two sets of columns, mixed data could be saved in the column when the DSP is upgraded. Access the *Data Source Column Encryption* page in System Administration. The Status field indicates issues with encryption that must be corrected before upgrade.

New Feature

Enhanced Migration Reporting

Data Quality is the analytical component of the DSP® that facilitates enhanced migration reporting on the target data staged in preparation for loading into the target system. It allows business users to:

- Establish data quality thresholds and view data quality scores and status
- Organize and display quality metric reports via web access or other formats for process improvement
- Identify and send errors (via workflow notifications) to business users for remediation prior to loading to the target system

Data Quality is delivered with a standard set of reports. Users can also create custom reports to fit their business needs. Refer to Use Enhanced Migration Reporting for more information.

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.

Advanced Data Migration

Console

When adding a wave to the *Wave: Process Areas* page, if a Target System (which is on the *Vertical* View) was not selected prior to saving the record, a warning message displayed. If the user canceled the record at this time, the record still saved and allowed the wave to be further configured. This error caused issues later in the migration process because target reports are not generated until a Target System value is set. To alleviate this issue, the insert method for the *Wave: Process Areas* page was changed from Horizontal Insert / Switch to Vertical to Horizontal / Switch to Vertical, which requires the *Vertical* View to be saved in order for the data entered on the *Horizontal* View to be saved, i.e., requires a user to select a Target System before the wave record can be saved.

Map

To improve the user experience, the Submit and Submit All events on the *Field Mappings* page now run in the background instead of in the foreground.

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 / Process Areas)* page until they are manually purged. Refer to Purge Inactive Segments in the online help for more information.

Information Steward Accelerator (ISA)

- From DSP release 7.1.4 onwards, users will no longer be able to be assigned to a Project Distribution from directly within Information Steward Accelerator. It will still be possible to view user assignments to Project Distributions. 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 ISA Distributions for 7.1.4.
- Several fields were added to the Excel Summary spreadsheet that is distributed to users in a Project Distribution:
  - Rule description
  - Custom attribute name and value associated with the rule
  - Connection and comment on the rule field with Implication and Recommendation
  - HTML-formatted Rule Binding description, allowing the user to link to an external source

Mass Maintenance (formerly dspCompose)

- From DSP release 7.1.4 onwards, users will no longer be able to be assigned to a Template or Template Roles from directly within Mass Maintenance. 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. 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 do Mass Maintenance template roles for 7.1.4.
- The order of items in the Mass Maintenance Navigation menu has changed. The Configuration menu in Mass Maintenance 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 Mass Maintenance, the user no longer inherits Mass Maintenance 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 in the online help for more information.
- The Mass Maintenance *Navigation* pane displays as expected after a user expands the *Navigation* pane and later performs a page refresh.

Syniti Data Replication (formerly DBMoto)

- The DSP is now compatible with Syniti Data Replication 9.6.3. When upgrading to DSP 7.1.4, an additional step is required to upgrade Syniti Data Replication to 9.6.3.
- 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.
- To more tightly integrate Syniti Data Replication functionality into the DSP, the following updates have been made:
  - DSP functionality has been updated so that the Syniti Data Replicator Service no longer stops and then restarts when building and refreshing packages. The application now builds and refreshes packages without starting and stopping.
  - Where Clause functionality has been updated for the DBMoto Download package type so that running Syniti Data Replication filters records as expected. Previously, the Where Clause Override field in the DSP was not passed into the Syniti Data Replication replication Where Clause. Now, both the Where Clause Override and the Client fields are added to the Replication.

    NOTE: The DBMoto Mirror package type only filters based on SAP Client. Other filters must be manually added within the Syniti Data Replication Management Center as a Visual Basic script.
  - When a user clicks the Build package button on the *Tables* page in Collect, Syniti Data Replication creates the replication but does not run it.
  - Refreshing a DBMoto Download package type runs the package without also rebuilding it.

Data Stewardship Platform (DSP®)

- The Migration Developer security role in previous versions of the product is now called System Administrator.
- The DSP, including SSIS, is now compatible to run on MS SQL Server 2019. Additionally, MS SQL Server 2014 is no longer a supported platform for the DSP.
- If SSIS packages are used in Collect on a SQL Server 2019 environment, SQL Server Data Tools for Visual Studio 2017 (SSDT for VS 2017) must be installed.
- The delivered Security Role Governance Developer has had the System Administration JobMonitoring WebApp group added to it. This provides users assigned to this Security role with comprehensive access to DSP Monitoring pages.
- Electronic Signature authentication enhancements include:

- The logic for deciding when to render the Electronic Signature panel has been updated so that the panel always appears if custom authentication is enabled, regardless of whether the user has a basic authentication password.
- When determining whether to accept the credentials entered on the Electronic Signature panel, the logic first checks if the password matches the basic credentials password. Otherwise, it checks for custom authentication, if enabled.
- To show unencrypted columns that needed to be reviewed, the DSP sent a daily email and a pop-up message displayed within the DSP. The pop-up message was superfluous and therefore has been removed.

- Starting with DSP release 7.1.4, the Exclude Client Fields check box on the *Vertical* View for a system type on the *System Type Import* page in Common is checked by default. If this check box is not checked and the system type is built with the client included, all target tables and check tables include this field. This means that every lookup table will become a multi-value key value mapping, which diminishes the visibility of true multi-value key lookup tables. Users can uncheck the box to include Client fields if needed.

Collect

- The Connection Type field on the *Target Sources* page now supports a Connection Type of IG Universal Connect as expected. Previously, when IG Universal Connect was selected as the Connection Type, the following error message displayed: “Target Source has Data Services connection type and the Source connection type is not compatible. Correct the Source "Connection Type" or the Source "Data Services Connection Type.” The webTargetSource_ConnectionTypeDataServicesIDVal view was modified to reflect support for the Connection Type of IG Universal Connect.

- Custom Source Connection Types added in Collect are no longer deleted on upgrade.

  To support this functionality, the DSP Supplied check box has been added to the following pages in Collect to indicate those items that are delivered with the DSP and cannot be deleted:

  - Connection Types
  - Source Connection Types
  - Connection Type Data Conversion

- Previously, the Collect Target Source Data Services test connection process sometimes failed when the Target Source type was SAPAPPSERVER. The following features were added to prevent failure of the connection test for this Target Source type:

  - The Connection Settings button on the *Vertical* View of the *Target Sources* page is disabled when the Data Services connection type is SAP Application.
  - A validation error displays on the *Target Sources* page if the source connection type and Data Services connection type do not align (for example, if the source connection type is SAPAPPSERVER, then the Data Services connection type must be SAP Application).

  - A validation error displays on the *Target Sources* page if the source connection type does not align with the Data Services package types registered for that Target Source (for example, if the source connection type is ORACLE, the Data Services package type cannot be DataServicesRFC).

- The Collect Parameter option Maximum Connections on the SDR Settings tab of the *Parameters-Collect* page in Common has been deprecated.

- The AddedOn field on the *Job Detail* page's *Vertical* View now displays date and time, so users can review failed records from the Test Connection Service page in time sequence order.

- The performance of Collect extracts using the SAP RFC and BOA RFC package types has been significantly improved. This performance improvement was achieved through faster data parsing and the use of bulk insert functionality.

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 Mass Maintenance debug logs. Refer to Configure Debug Logs Settings in the online help 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.

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 in the online help 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.

Online Help

- A new topic was added: Create Custom Authentication Plugins
- Updates were made to the following topics to improve clarity:
  - Append Utility Columns to All Tables
  - Allow Mapping of Utility Columns
- Added this note to the Validation Rules topic to clarify the use of Warning validations:

NOTE: When creating an event that will be called indirectly, do not use Warning validations. Use Error validations. Warnings are intended for user interaction. Validations running on events used as business rules of the type WebApp Event or WebApp Event (Private), or as Event Tasks added to a job, are non-interactive. In these cases, validations are only used to stop the business rules of the event from running (or, in this case of a 'Run On Validate Fail' set of rules, to allow the business rules to run). Refer to Set Parameters for a Public WebApp Event, Create a WebApp Event (Private) Business Rule in the online help, and the *Job Queue (Task)* page for more information.

- Added topic Track - Changes Per Week.

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 in the online help 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

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

Centralized Security

In DSP releases of 7.0.6 and below, the management of a user's access to different application functionality and content is done from within System Administration and the individual applications. For example, to grant a user access to Mass Maintenance, 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 in the online help 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 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 offers 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 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 in the online help 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 in the online help 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 in the online help.

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.

WebApp	WebApp Group
	• **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.
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: • Create security roles with a Role Type of Content and • 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.

WebApp	WebApp Group
Transform	• **ExecutionOnly** — Designed to be used by: • A user whose role is to only process data objects or • 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 Mass Maintenance to receive reports and remediate failures with Mass Maintenance. 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, Mass Maintenance 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 Mass Maintenance. 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 Advanced Data Migration 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 in the online help 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 ISA Distributions and Mass Maintenance Groups 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 in the online help for more information.

To access the reports, select **Admin** > **Security** > **Security Management** > **User Security Reports**.

- 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 in the online help 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 in the online help for more information.

Additional Enhancements

- 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 to 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.
- 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 in the online help for more information.
- 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.
- The following pages have been modernized by utilizing fly-out pages, enabling users to access the pages with fewer clicks:
  - Security Role Key Values
  - User Specific Keys

Resolved Issues

- An issue occurred when performing an import of an .xlsx Excel file: a column with both an Excel format of Number and a defined number of decimal places was sporadically imported with additional decimal places (this was not an issue for .xls Excel files). For instance, an entry of 16.44 on the spreadsheet was imported as 16.44000001 in SQL Server. This issue was resolved by updating the third party library (ExcelDataReader) used by Assemble. [DSP70-905]
- 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]

Advanced Data Migration

Map

- An issue occurred when attempting to auto-generate a full construction page using the Sync to Map functionality on the *Targets* page. Validation rules failed to run when the values for the target lookup table did not match the associated values for the target table. The full construction page is now auto-generated without error. [DSP70-877]
- Auto-generated list boxes failed to store selected values correctly when the lookup table contained more than one target field. Validation rules run as expected and full construction pages are auto-generated as expected. [DSP70-877]
- 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]

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 / 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 *All Business Reports All Waves / 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 in the online help for more information. [DSP70-552]

Information Steward Accelerator

- ISA sends reports to users via email for the purpose of resolving data quality issues. The reports include an Excel attachment with a Summary sheet and an additional sheet for each individual rule binding. Previously, the Excel attachment did not include the Implication and Recommendation fields included in the report definition. Those fields now display as a comment on each associated rule on the Summary sheet; they also display as a comment on the first column name (cell A1) of each individual Rule Binding sheet. [DSP70-619]

- Currently, users can exclude 0-count Rule Binding failure records from an Excel Summary email attachment, improving readability and focus. Release 7.1.4 extends that functionality to notification emails as well. [DSP70-640]
- An issue occurred with the Rebuild Rule Binding Columns check box on the Basic Settings tab of the *Parameters* page. If the setting was unchecked, an error occurred. This issue is corrected. [DSP70-885]
- Updating a table/view in Information Steward requires associated rule bindings to be removed and then added again after the change. This action caused duplicate rule binding IDs to be generated for a rule, and multiple records to display on the *Report Data Viewer* page after the rule was run in IS and the Collect package was refreshed. Multiple records no longer display on the *Report Data Viewer* page. [DSP70-966]

Mass Maintenance

- 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]
- 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 7.1.4. [DSP70-799]

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]
- 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]
- The following issues with Electronic Signature authentication have been corrected:
  - Upon proper configuration, Electronic Signature now works with Integrated Authentication. Refer to Use Electronic Signature with Integrated Authentication in the online help for more information.
  - Custom authentication no longer allows locked users to log in to the DSP (for example, previously, they could make unlimited guesses at the custom login credentials).
  - The login attempt count is now correct when basic and custom authentication are both enabled.
  - Users are no longer forced to reset their passwords when they do not already have a password to reset.
  - The Integrated Authentication Variable Name option was removed from the *Parameters* page, resolving potential security issues. [DSP70-771]

- A DSP-delivered CTS configuration for the DSPCommon WebApp has been updated. In a previous release, the System Type table ztSystemTypeTableFieldCheckTable was deprecated. In this release, this table has been removed from the CTS configuration. [DSP70-861]
- A DSP-delivered CTS configuration for the Transform WebApp has been updated. The Relationship of ttWaveProcessAreaObject to ttWaveProcessAreaObjectTarget now has the EnableCTS setting checked. [DSP70-861]
- An issue occurred when importing a System Type using a System Type Model where if there were duplicate data type mappings for the conversion from the data type used in the model to SQL Server then the import created duplicated records in the ztSystemTypeTableField table. With this fix, duplicate records are no longer created in the System Type. [DSP70-830]
- An issue occurred in several System Type tables, including ztSystemTypeJoin and ztSystemTypeJoinField, where the tables did not have primary keys or foreign key relationships. This caused performance impacts and prevented records from being deleted when a System Type was deleted. With this fix, all ztSystemType* tables have the required primary keys and foreign key relationships, and System Type deletion cascades successfully. [DSP70-851]
- If the password for a data source resulted in an encrypted value longer than 128 characters, the Common Service page "Service - DataServices Status" failed with a message of "Failed to enable constraints. One or more rows contain values violating non-null unique or foreign-key constraints." With the fix, the field length has been updated, and the Service page runs as expected. [DSP70-867]

DSP Upgrade Impact:

When upgrading from DSP 7.0.6 or below to 7.1.4 or above, Collect target sources that include SAP connection details will automatically have the saved connection string details converted into a new Data Source of type SAP Application Server. The newly created SAP Application Server Data Source will then be assigned to the Collect target source. After upgrading, it's important to review and test all Collect target sources to ensure they function correctly. [DSP70-740]

Collect

- An issue occurred with building Data Services packages. When adding a Where Clause to a table in Collect and then building a Data Services RFC package, the Where Clause was not added to the job initially; a second build was required. A similar issue occurred when building an SAP RFC package. The issue has been fixed and these packages now build as expected. [DSP70-837]
- An issue occurred when adding a target source with connection type SAPAPPSERVER on the *Target Sources* page and attempting to build an RFC package for a table using this target source. The package build failed. The issue has been corrected and the build now completes as expected. [DSP70-962]
- Collect was writing Data Services packages to the incorrect repository. Several changes were made to fix this issue:
  - The *Target Sources - DataServices Connection* page is now read only. The data services connection information is now retrieved from the *Data Source Registry* page in Common.

- A validation rule was added to the *Tables* and *Target Sources* pages to ensure that the SAP DataSource is populated on the *Target Sources* page if one or more RFC packages are registered (on the *Tables* page).
- A new Data Services connection type, Oracle12c, was added.
- An error with the Test Connection button on the *Targets* page was fixed. Previously, when the Data Source was registered on the *Targets* page and then renamed or removed from the *Data Sources* page in System Administration, an error displayed when the user clicked the Test Connection button on the *Targets* page.
- Logging for namespace override options was added to Common. If the SAP Namespace check box on the *Data Source Registry* page is not checked, DSP checks for a value in the Rfc Name Space Option field on the *Parameters-Collect* page. If a value is not set, the DSP overrides the logging configuration settings with “namespace." [DSP70-807]

- 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]

- An issue occurred with the DBMoto Download package type where, when users clicked Refresh on Collect Source, the job timed out. The code for this package type has been rewritten to prevent parallel sessions, which was the issue that caused the timeouts. With this fix, DBMoto Download jobs build as expected. [DSP70-790]

- An issue occurred when a Schedule Services service page executed during a CranPort package refresh. If the target contained both Syniti Data Replication and CranPort tables, the service page job failed because the service page process was not able to access the CranPort tables specified in the underlying view.

  The service page table view has been altered so that the deadlock no longer occurs. Running a Schedule Services job simultaneously with a CranPort package refresh no longer causes the Schedule Services job to fail. The concurrently running jobs now execute as expected. [DSP70-791]

- An issue occurred with the Advanced View Builder tool in Collect where, when a user built views for a given database, the views were created with the where clause on every column whose value related to the SAP Client and/or Language field. This rendered the view unusable. The workaround was to use the View Builder tool in

Common. The issue has been corrected, so using the Advanced View Builder tool in Collect builds a view as expected. [DSP70-902]

- An issue occurred where, when a user tested a connection and the test failed for either a target or a target source, the service page execution ended without testing the remaining connections. The issue has been corrected, so that when a connection fails, service page execution continues and completes testing on all connections. Each record in the dgTarget or dgTargetSource tables updates with the appropriate connection status, depending on the outcome of each connection test. [DSP70-561]
- The Build View process on the *Advanced View Builder* page in Collect completes without an error message and drops every SQL Server view in the database for views. DSP is then unable to recreate the views since they no longer exist in the DATABASE FOR TABLES list box. To prevent all views from being deleted, a safety check was added to prevent the DATABASE FOR VIEWS and the DATABASE FOR TABLES fields from being in the same database: a view selected from the DATABASE FOR VIEWS list box is removed as an option from the DATABASE FOR TABLES list box. The same is true for a database selected from the DATABASE FOR TABLES list box. [DSP70-878]
- With the absence of a NUMERIC data type rule, Collect defaulted to the ANY data type, which uses nvarchar with the same length as the source field. If the source data contained a value that was at the character maximum for numeric and was negative, the value caused an error. To fix this issue, a NUMERIC data type rule was added to the SQLSERVER *Source Connection Type* page and is formatted the same way as the DECIMAL data type rule. [DSP70-464]
- In previous versions of DSP, Collect copied and used connection information from the assigned target source into the dgTarget and dgTargetSource tables. If the target source was required to connect to an SAP application (rather than database), the SAP Connection details were also populated on the target source record and stored in the dgTargetSource table. To ensure that connection information is stored in a central location, this release introduced the following changes:
    - Collect no longer copies target and target source connection information into dgTarget and dgTargetSource tables. Instead, Collect uses the connection information stored within the Common *Data Source Registry* page.
    - The ConnectionString column has been removed from the dgTarget and dgTargetSource tables.
    - Instead of entering the SAP Connection details on the target source record, users must select the Common Data Source Registry connection associated with the relevant SAP application / client.
        - With this change, the following columns within dgTargetSource have been removed or made read-only:
            - Client
            - Instance
            - Language
            - RfcNameSpaceOption
            - SAPLogonGroup
            - SAPMsgServerHost

  - SAPPassword
  - SAPServerHost
  - SAPSystemNumber
  - SAPUserID [DSP70-740]

Common

The View Builder tool in Common has been used as a workaround when the Advanced View Builder tool in Collect does not function properly. The Advanced View Builder tool in Collect now functions properly. [DSP70-902]

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]
- An issue has been fixed for 64-bit DSP instances that prevented non-dialog SAP users from creating Integrate BAPI/RFC Templates and posting an Integrate process. With this fix, using SAP non-dialog users/service accounts in Integrate is supported, so long as the user has correct SAP authorizations. [DSP70-915]
- An issue occurred in 32-bit DSP environment when the same non-dialog SAP user account was used in multiple different data sources, each with different SAP logon languages. This issue occurred when a user posted using one connection ID in language A and then, when that process had completed, attempted to post a second process using a second connection ID in language B. The second post failed, generating an error message: Please logon with a dialog user. This issue has been corrected so that the second background process now completes as expected. [DSP70-872]

System Administration

- An issue occurred when the Set Password And Notify User button on the *Users* page was clicked for a UserID that contained spaces. As a result, the following error message displayed when the user tried to log in with the UserID and temporary password: "The website could not finish processing the current request due to an unexpected system error." The issue has been fixed; the error message no longer displays in this scenario if the UserID contains spaces. [DSP70-926]
- 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 Custom Security Definitions in the online help for more information. [DSP70-743]
- 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:
  - 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.
  - 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]

Known Issues

In ISA, if the name of the view that is bound to the rule contains a period, columns will not download after the rule runs. Remove periods from view names in IS.

Enhancement Requests From the User Base

- As the result of feedback from the online help, the SQL Server Health Charts topic in the online help was updated to include more detailed information about the Memory Overview Chart.
- As the result of feedback from the online help, the *User Template Filter* page was updated to include more detailed information about the VALUE field.

Last Updated on 5/5/2020