DSP - psaSecureAD User Guide

Version: 2.1

Date: 2020/04/28

Legal Disclaimer

Contents

Document Receiver

Company	Privileged
Clients with active Syniti Consulting Services Engagement	

Document Owner

Publisher		
Syniti Solutions Management Team		
Contact	**Telephone**	**E-Mail**
Kurt Vandergriend		Kurt.Vandergriend@Syniti.com

Document History

Version	Date	Update reason	Author	Reviewer
1.0	2018/11/01	Initial Version	Kurt Vandergriend	
2.0	2019/06/01	Added Role Construction and Encryption functionality	Kurt Vandergriend	
2.1	2020/02/01	Upgrades for DSP 7.1, added custom Security Definitions for Conduct, Compose, Monitor, and ISA	Kurt Vandergriend	

1 Introduction

psaSecureAD is a Professional Service Accelerator that adds:

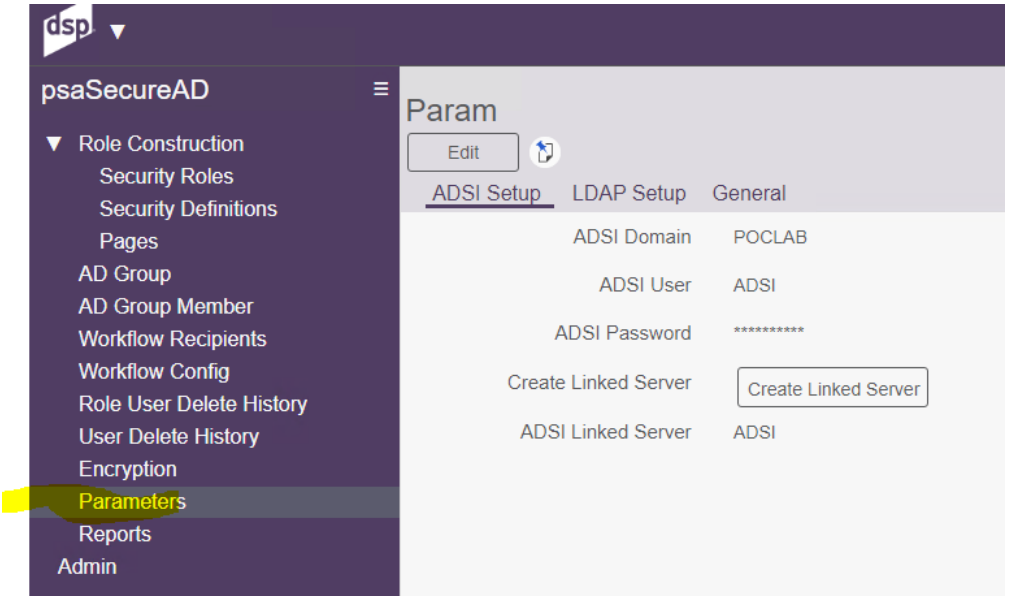
1) Active Directory integration for DSP User creation/expiration (Authentication)
2) Active Directory integration for User Security Role assignments/deletions (Authorization)
3) Seamless construction of custom Security Roles
4) Role security integration for Conduct, Monitor, Compose, and ISA
5) Easier maintenance and monitoring of password encryption

Since psaSecureAD controls all security definitions in DSP, only System Administrators should be granted access to this PSA.

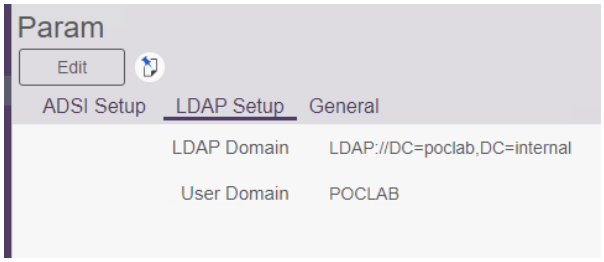
2 psaSecureAD Parameter Configuration

2.1 ADSI and LDAP Configuration

Active Directory integration is an optional feature within psaSecureAD. If this functionality is needed, AD integration must first be configured in the Parameters page.



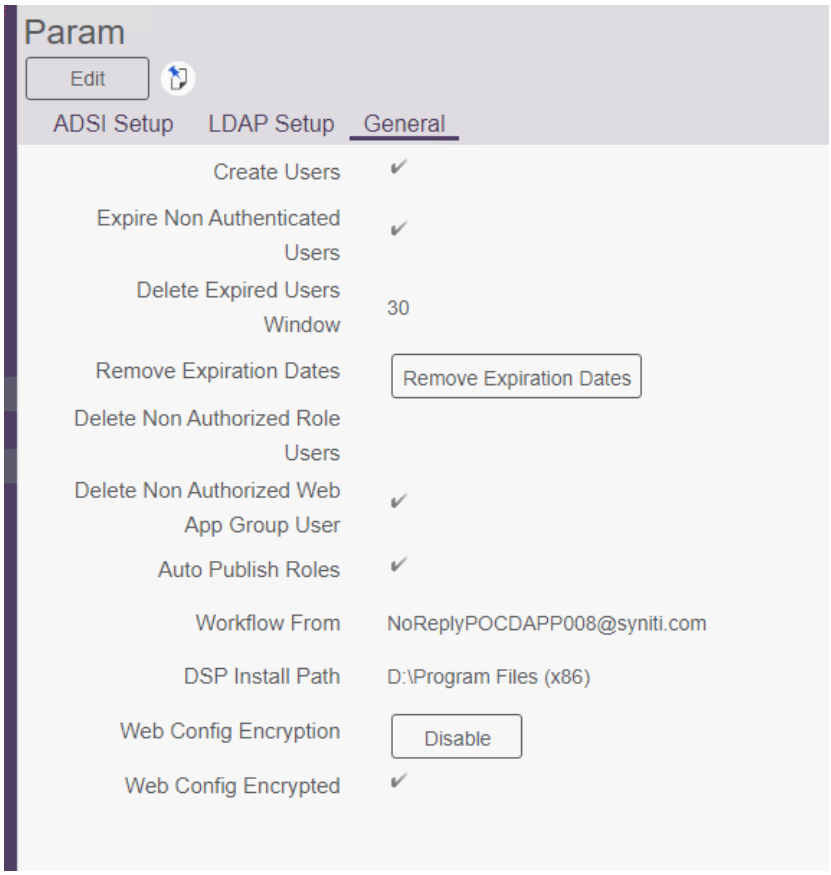
1) In the ADSI Setup tab, enter the following:
    a. ADSI Domain: This is the Domain of where the Active Directory read-only login was created.
    b. ADSI User: AD Account created to read Active Directory. The Account only needs to be a member of "Domain Users."
    c. ADSI Password: Password for the 'ADSI User' AD Account
2) Click on the “Create Linked Server” button to create the Linked Server based on information populated above. NOTE: the DSP application login must have SQL admin rights in order for this step to work. Once this step is complete, SQL admin rights are no longer needed for the DSP application login



3) In the LDAP Setup tab, populate the required fields:
   a. LDAP Domain: If you do not know what to enter here, you can run 'dsquery * -limit 1' from a command prompt. Prefix the results of that with 'LDAP://' and enter that into this field. Or contact the Active Directory administrator for this value.
   b. User Domain: This field must be populated if DSP Integrated Authentication is turned on, and you want psaSecureAD to auto populate the "Windows User Name" field when Users are created.

2.2 General Settings

In the General Settings tab, you should not have to change anything from the initial installation settings. Here is an explanation of what these fields do:



1) Create Users: The "Create Users" flag will automatically create DSP Users that are members of an AD Group. If not checked, DSP Users must be added manually before Role Users will be added automatically. If both this field and the 'Expire Authenticated Users' flag are checked, Users not in any of the AD Groups listed will be expired, but not deleted until the 'Delete Expired Users Window' duration has passed.

2) Expire Non-Authenticated Users: Check this field if you wish psaSecureAD to expire DSP Users who are not in an AD Group.

3) Delete Expired Users Window: Number of days after a DSP User is expired before the DSP User will be deleted.

4) Remove Expiration Dates: This button removes the 'Expiration Date' for all DSP Users. This should only be done if mistakes were made in psaSecureAD configuration, and User access needs to be restored. You still need to fix the configuration before the next service page run, or Users may get expired again.

5) Delete Non-Authorized Role Users: This should be checked so that Users are deleted from Roles when they are removed from Active Directory groups

6) Delete Non-Authorized WebApp Group User: Enabling this is highly recommended if you want Role User membership to have complete control of DSP security, otherwise Role Security is compromised.

7) Auto Publish Roles: Enabling this is highly recommended if you want Role User membership to have complete control of DSP security.

8) Workflow From: This field is optional. If it is blank, the 'workflow from' address will be taken from the Default Email Address field in 'Admin > Configuration > Parameters.'

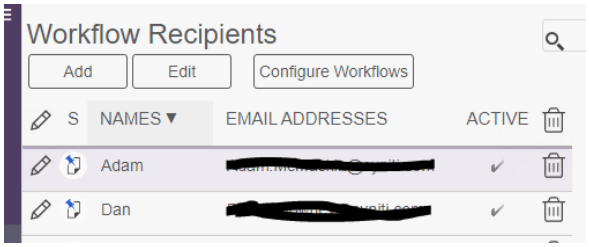
9) DSP Install Path: The path of the DSP install folder is required in order for encryption of the web.config file to work. Do not include the BOA\DSP portion of the path. Entering the \ at the end of the path is optional.

10 Web Config Encryption: This will encrypt the Web.config file on the DSP application server. The "Encrypt" and "Decrypt" option will toggle based on the "Web Config Encrypted" field value.

11) Web Config Encrypted: This field will be automatically updated as the "Web Config Encryption" button is toggled. If the encryption state is incorrect, update this field to the correct value.

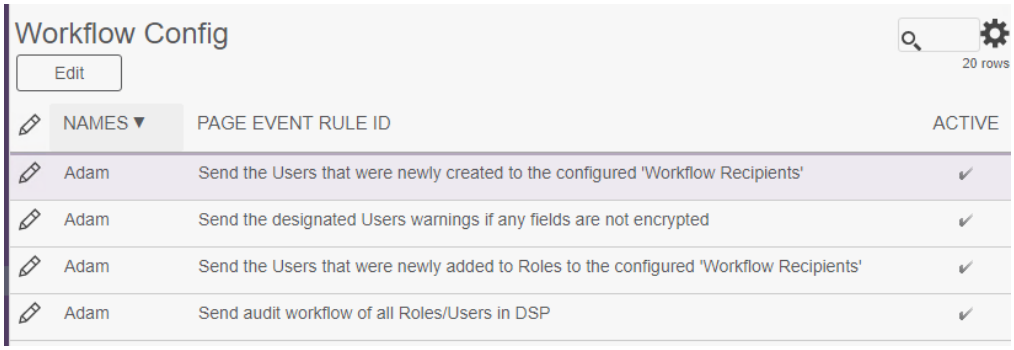
3 Workflow Settings

3.1 WorkFlow Recipients



In the Workflow Recipients page, enter the Names and email addresses of any System Administrators, or security auditors that need to be made aware of key events.

3.2 Workflow Config



Any Workflow Recipients entered will automatically be added to the Workflow Config page, with all events checked. Uncheck any event that the recipient does not wish to be notified about. Events with Workflows are as follows:

a) Users that were newly created

b) Users that were newly added to DSP Roles

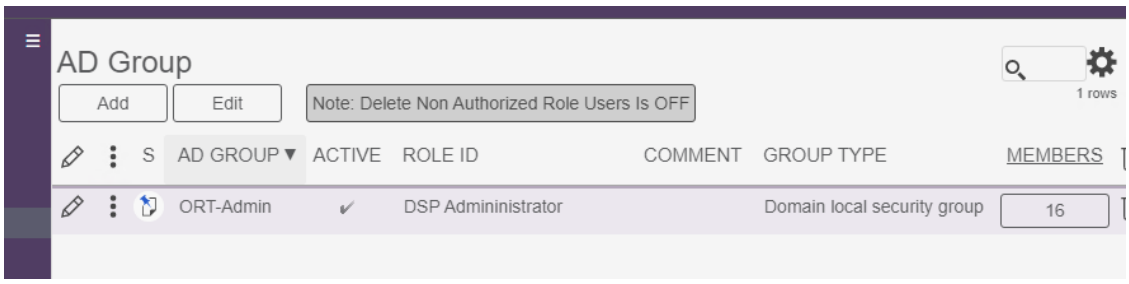
c) Weekly audit of active Users and their Roles in DSP

d) Warnings if any of the Password fields in DSP are not encrypted

4 Active Directory Group Setup

Active Directory integration is an optional feature within psaSecureAD. If this functionality is needed, AD integration must first be configured in the Parameters page (see section 2.1).

4.1 Active Directory Group



1) Enter any Active Directory Groups that are used to control User creation or DSP User Role assignment.

a) AD Group: The name of the Active Directory Group. As soon as a Group is entered, the Distinguished Name of the group will be read from the connection. This information can be seen in the vertical view.

b) Active: The "Active" flag must be checked, and either "Create Users" checked in Parameters or "RoleID" populated before psaSecureAD will change anything.

c) RoleID: This is an optional field, depending on the requirements (Authentication or Authorization):

- If RoleID is populated, the members of the AD Group will automatically be inserted/deleted from the specified DSP Role. This is providing both Authentication and Authorization via the AD Groups that are entered. The "Create Users" field in Parameters should also be checked to ensure the DSP Users exist when adding them to a Role.

  - Enter a separate AD Group for every DSP Role where Users need to be assigned

- If Not populated, psaSecureAD will only create/expire Users in/not in this AD Group. It will not assign Users to DSP Roles. This is only providing Authentication via the AD Group entered. In this scenario, only one AD Group can be entered.

  - Enter only one AD Group

d) Comment: Enter any comment as needed

e) Group Type: This is automatically populated

f) Members: displays members of the Active Directory Group (refreshed every 10 minutes)

4.2 AD Group Member

The AD Group Member page displays all AD Group members for all AD Groups.

4.3 Deletion History

History of Users deleted from roles and Users deleted from DSP via AD Groups can be viewed on the "Role User Delete History" and "User Delete History" pages.

5 Role Construction

DSP comes delivered with several standard Security Roles. However, there are many cases where custom security requirements require creation of new Security Roles. Role Construction in psaSecureAD provides seamless and secure integration with the DSP Framework in accomplishing this.

5.1 Role Construction Page

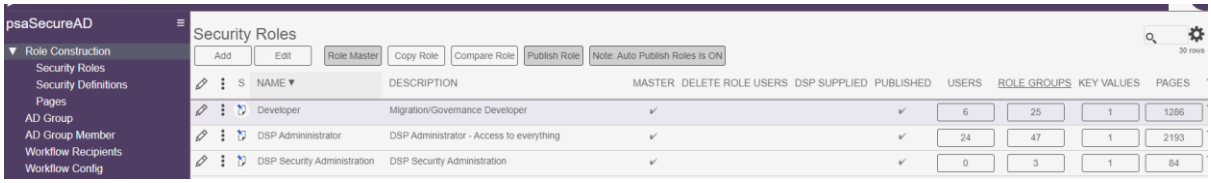
The Role Construction page is the starting point for viewing and constructing all Security Roles. psaSecureAD comes delivered with three custom Security Roles. NOTE: Any Roles that exist in the DSP Framework are automatically pulled into psaSecureAD.

The delivered custom Roles are:

1) Developer: This is a true “Developer” role, that has access to all Development activities in Migrate, Conduct, Compose, Monitor, etc. (license permitting). It does not have access to any security functionality.

2) DSP Administrator: This is the full DSP Admin access, including security.

3) DSP Security Administration: This is access to DSP security related functionality only. It does not have access to development activities.



Field descriptions for this page are as follows:

1) Name: Name of the Security Role. Enter the name as desired

2) Description: Description of the Security Role

3) Master: If "Master" is checked, psaSecureAD becomes the master of data associated with that Role. This means changes in the Framework will be deleted if not made in psaSecureAD first, and any data in the Framework will not be copied to psaSecureAD. Ultimately, all Roles should be checked as "Master" using the Role Master toolbar button.

4) Delete Role Users: Check this button if you do not want this Role to be assigned to anyone. This can be used if an existing Role does not meet security requirements, and should never be used.

5) DSP Supplied: This field is display only, and indicates if the Role was supplied by the Framework, or created in psaSecureAD.

6) Published: This check box is dynamic, and indicates if the Role maintained in psaSecureAD matches what is in the DSP Framework.

7) Users: List all Users currently assigned to this Role. Note that User assignment to Roles only occurs in psaSecureAD if the Active Directory functionality is in use.

8) Role Groups: List all WebApp Groups assigned to the Role

9) Key Values: Lists all Security Definition Key Values assigned to the Role

10) Pages: Lists all Pages assigned to the Role

11) Role Master: This toolbar field will flag ALL Roles in psaSecureAD as the "Master." If "Auto Publish Roles" is also turned on, psaSecureAD will have complete control over Security Roles, and any changes made via the Framework will be removed.

12) Copy Role: This will copy the hi-lighted Role to a new designated Role, including all WebApp Groups, their Pages, and Security Definition Key Values.

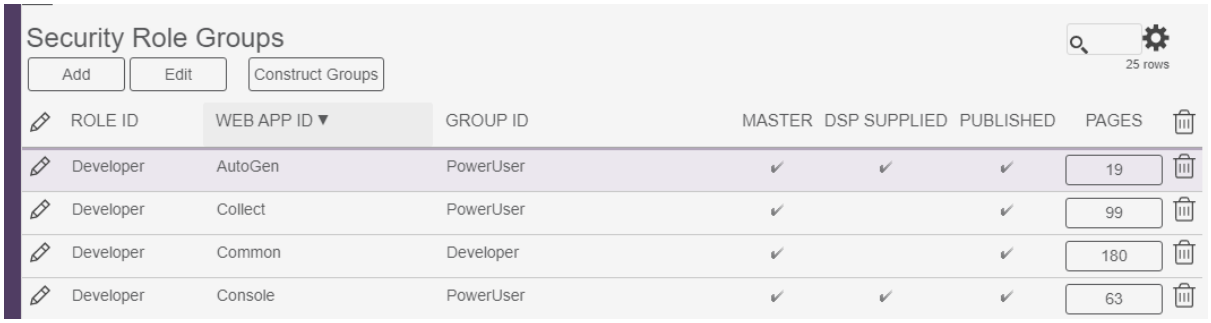
13) Compare Role: This allows you to compare security access for one Role with another Role. It can compare both WebApp Groups, and Page access.

14) Publish Role: If the Master field is checked, this provides an option to manually publish the Role from psaSecureAD to the Framework. Otherwise it will get published automatically every 10 minutes.

15) Note Auto Publish Role is ON: This is displaying the current configuration for publishing Roles, warning you that any changes made in psaSecureAD will override what is in the Framework.

5.2 Security Role Groups Page

The Role Groups page is where WebApp Groups are maintained for a Role, and links to WebApp Group Page maintenance.



1) Add/delete WebApp groups as needed

2) Master: Indicates that psaSecureAD is the "Master" of this WebApp Group. Master is automatically copied from the Role if all associated Roles are also the master in psaSecureAD. You will not be able to check Master field is all Roles tied to the WebApp Group are not the Master in psaSecureAD.

3) DSP Supplied: This field is display only, and indicates if the Role was supplied by the Framework, or created in psaSecureAD.

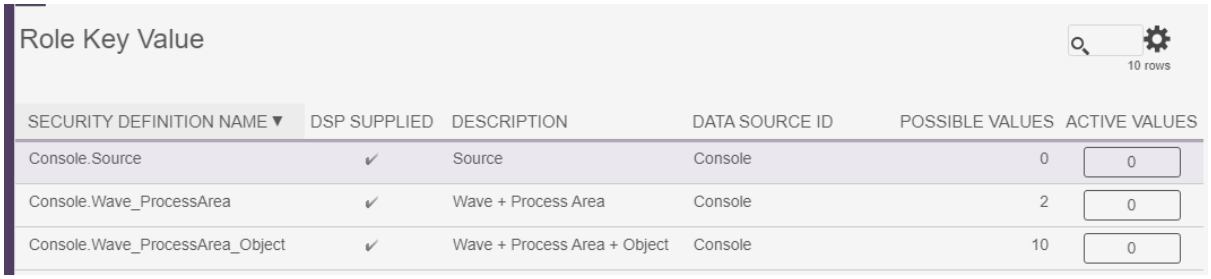
4) Published: This check box is dynamic, and indicates if the Role maintained in psaSecureAD matches what is in the DSP Framework.

5) Pages: Displays the number of Pages in this WebApp Group, and links to the WebApp Groups page for maintenance of Pages in that Group.

6) Construct Groups: This tool bar button takes you to the WebApp Groups page where all WebApp Groups can be maintained.

5.3 Key Values Page

The Key Values page is where Security Definition Key Values are assigned to Roles.



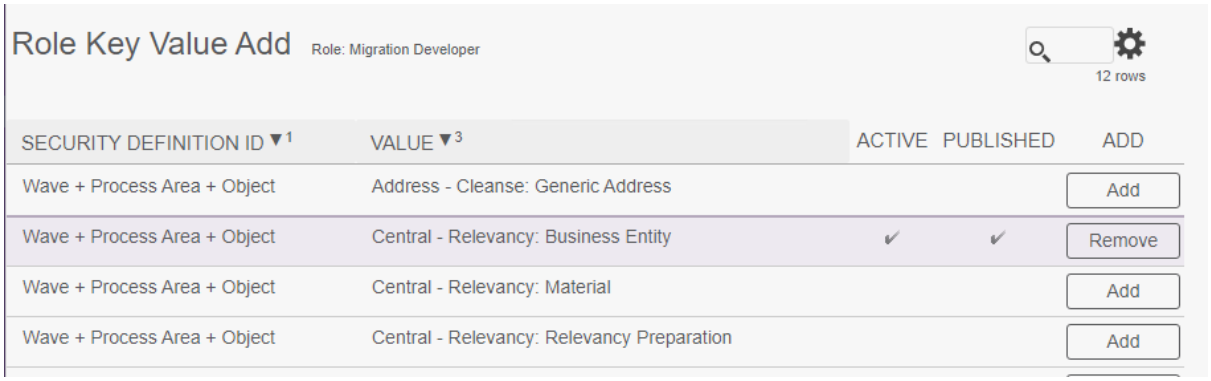
1) Security Definitions are automatically pulled from the Framework, and some custom Security Definitions are provided by psaSecureAD (see Security Definitions section).

2) Possible Values: Displays the number of Values that are available to be assigned for this Security Definition. Note that clicking on the "Active Values" button will re-generate the list of available values if changes have made.

3) Active Values: Display the number of Values that are active for this Security Definition. Click on this button to activate/delete Values.

5.4 Role Key Value Add Page

This is where Security Definition Key Values are added and removed from a Security Role.



SECURITY DEFINITION ID ▼1	VALUE ▼3	ACTIVE	PUBLISHED	ADD
Wave + Process Area + Object	Address - Cleanse: Generic Address			Add
Wave + Process Area + Object	Central - Relevancy: Business Entity	✔	✔	Remove
Wave + Process Area + Object	Central - Relevancy: Material			Add
Wave + Process Area + Object	Central - Relevancy: Relevancy Preparation			Add

1) Value: Displays the description of the Value

2) Active: Indicates if Value is active for the Role or not

3) Published: Indicates if the active/non- active status is published to the Framework. Publishing occurs automatically every 10 minutes, or it can be done manually on the Role Construction page.

4) Add/Remove: Used to add or remove the Value from the Role. Note that you will not be able to add/remove a Value until the previous change is published to the Framework.

5.5 Pages

The “Pages” page is an auditing tool where all DSP Pages are listed, and displays all of the following:

1) Roles: All Roles that have access to this Page. The lower pane will also display Users assigned to those Roles.

2) Groups: All WebApp Groups assigned to this Page

3) Security Definitions: All Security Definitions registered to this Page

4) Menu Links: All Menu links that have access to this Page

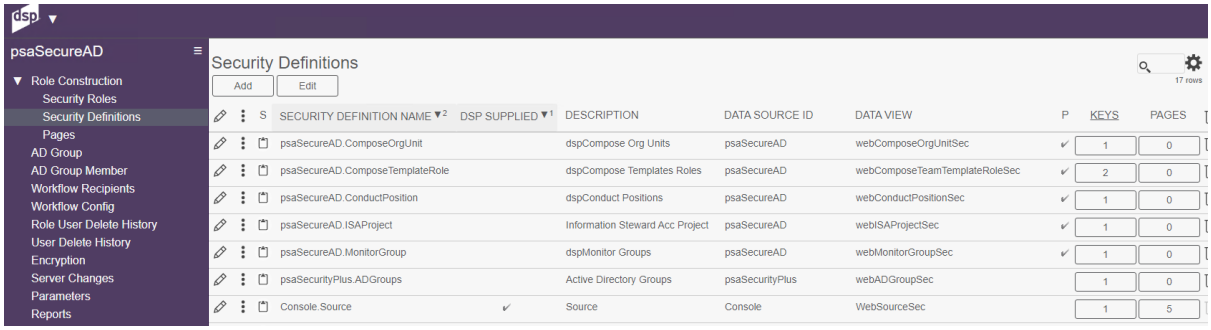
5) Paths: The detailed Menu/Column Path(s) that can be taken to get to this Page

6 Security Definitions

Security Definitions provide more granular control of DSP security than page-level access.

6.1 Security Definitions Page

The Security Definitions page is where custom Security Definitions are maintained, and Security Definitions from the Framework are displayed.



Note that there are 5 custom Security Definitions delivered with psaSecureAD. All five of these can be used for DSP version 7.0.6 and earlier, creating complete Role secure functionality for Conduct, Monitor, Compose, ISA security objects, or any other security object created in DSP. The 5 delivered Security Definition's Values can be assigned to Roles, such that these security objects are controlled via Role Security (they do not have to be maintained separately).

1) Conduct Positions

2) Monitor Groups

3) Compose Templates

4) Compose Org Units

5) ISA Projects:

For DSP versions 7.1 and later, only the psaSecureAD.ComposeOrgUnit Security Definition is needed.

Field definitions for this page are as follows:

1) Security Definition Name: Naming convention is <WebAppName.<Object>

2) DataSourceID: Where the Security Definition Data View is maintained

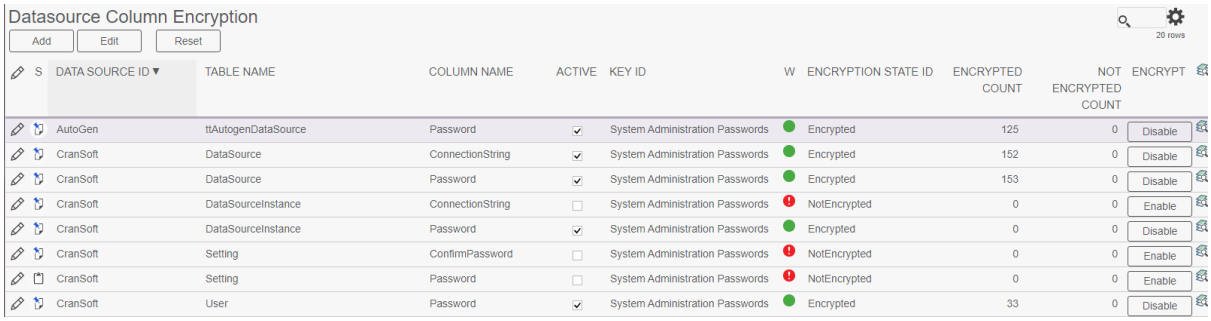
3) Data View: The name of the view that defines the Key Values

4) P: Indicates a stored procedure is registered to execute the assignment of Key Values to Roles (already provided for the 5 custom Security Definitions).

5) Pages: Displays the Pages where the Security Definition is registered.

7 Encryption

psaSecureAD Column encryption ensures that all password fields stay encrypted. It allows maintenance of all encryption on one page, field-level validation that data is encrypted, and Workflow warnings if fields are not encrypted. It also allows reset of the encryption state in the event that mixed-state encryption existed for a column.



1) Active: Means the field should be encrypted, and that workflow warnings will be sent to workflow recipients if any row is not encrypted.

2) W: Red or Green light indicating full encryption (green), or data not encrypted (red)

3) Encrypted Count: Count of rows that are encrypted

4) Not Encrypted Count: Count of rows that are not encrypted

5) Encrypt: Click on Enable or Disable to enable/disable encryption. A few situations where data may need to be temporarily decrypted: to verify a password, or to enter a new Datasource in Common

6) View Data: allows you to view Password data without going into SQL Server.

7) Reset: This toolbar button sets the Encryption State to Encrypted for this record. This is needed in the situations where the Encryption State is incorrectly set to not Encrypted, and there are encrypted values, or a mixture of encrypted and non-encrypted values. Once the record is “reset” to Encrypted, then manually click Disable to decrypt all values, then Enable to get all values encrypted.