

Florida **PALM**

Planning, Accounting, and Ledger Management

Florida PALM Security Access Management User Manual



**Florida
Department of
Financial
Services**

Revision History

Version	Date	Revision Notes
1.0	07/02/2021	Initial Version
2.0	08/23/2021	Updated contact information when adding a new SAM; Added how to approve and remove SOD conflicts; Added report fields and descriptions.
3.0	09/30/2021	Clarified instructions for Username/Route Control; Updated weblink to Agency Role Mapping Handbook, Added website location for the SAM Access Request and Acknowledgement form.
4.0	01/07/2022	Updated SOD Conflicts
5.0	01/28/2022	Updated and added Roles
6.0	02/08/2022	Updated Links and Route Control
7.0	06/21/2022	Updating Roles and SOD conflicts
8.0	12/29/2022	Adding auto-recon Roles
9.0	02/13/2023	Updated Role Names
10.0	10/03/2024	Updated language per CFO Memo #28 (July 19, 2024) for a New SAM, Inactivation of a SAM, Approving SOD conflicts; and updated DFS Role/PPL List Mapping for DFS GL Close Processor and DFS YEC GL Journal Processor.
11.0	04/24/2025	Updated language per CFO Memo #28 (March 19, 2025) with updated verbiage for requests to A&A for additional SAM end users based on end-use ratios. Update SOD approval conflict language.
12.0	7/1/2025	Update the language per CFO Memo #28 (July 1, 2025) to include the expanded responsibilities assigned to SAMs. All SAMs are now required to create an account in ServiceNow. Added information for SAM approvals of the end users access to ServiceNow account.

Table of Contents

Revision History	2
Table of Contents.....	3
Introduction to Security Access Management	4
Security Access Manager Identification	4
New Security Access Manager	5
Inactivation of Security Access Manager	5
Security Access Manager Training.....	5
Florida PALM Access Management	6
Navigation Elements in Florida PALM Access Management.....	7
Florida PALM Access.....	7
New End User	7
Identity Provider	8
End User Profile	8
Primary Permission List.....	9
Username/Route Control	10
Adding Florida PALM End User Roles	11
Removing Florida PALM End User Roles	12
Bank Security	13
Separation of Duties	13
Approving SOD Conflicts	13
Removing SOD Conflicts	16
Inactivating End Users	17
Updates to End User Name	18
Reports and Queries	18
Access Control Report.....	18
FLP_USER_ROLES_BY_PPL Query.....	19
Glossary.....	20
Florida PALM End User Role to System Role Matrix.....	21

Introduction to Security Access Management

The Department of Financial Services (DFS) delegated the Florida PALM Security Access Management responsibilities to individual agencies. Agencies will be responsible for managing end user access to functionality within Florida PALM. A Security Access Manager (SAM) has responsibilities to manage end user security within Florida PALM. This includes adding and removing roles and inactivating end user profiles. Agencies are assigned a primary and backup SAM to manage security role access for their agency's end users. The SAM accesses Florida PALM Access Management to maintain end user roles in Florida PALM.

Security Access Manager Identification

The agency Administrative Service Director, or designee, must appoint the agency SAM. The identified Florida PALM SAMs should meet the following qualifications:

- Understand who within the agency currently requires access to Florida PALM to perform their job responsibilities;
- Understand the type of access agency end users have within Florida PALM;
- Understand the functions agency end users perform in Florida PALM;
- Have the appropriate level of authority to act on behalf of the agency to make authorized Florida PALM access assignments.
- Complete the Florida PALM Security Access Manager training available in People First Learning Management System (LMS) – Florida PALM Training Highlights – SAM.
- Complete registration in Florida PALM Solution Center (FPSC) [Customer Portal – ServiceNow](#).

Security Access Manager Responsibilities

A SAM is responsible for maintaining role-based access to Florida PALM end users. SAMs cannot have processor, maintainer, or approver roles in Florida PALM. They can have view only and Query access for reporting purpose.

The SAM responsibilities include:

- Adding and removing role access based on the agency's internal procedures.
- Terminating end user accounts when an end user no longer requires access, e.g., end user separates from the agency.
- Updating end user accounts when role job duties change.
- Maintaining a list of end users and their access.
- Conducting and documenting at least a quarterly review of end users and their access for appropriateness.
- Notifying the Florida PALM Solution Center and Agency Identity Provider point of contact upon notice that an end user account has been compromised.
- Responding to Accounting and Auditing's (A&A) Governance Administrator inquiries when separation of duty conflicts are identified.
- Reviewing and approving or denying end user registration requests for the [Customer Portal ServiceNow](#) (FPSC), to validate the end user belongs to the correct agency group.

New Security Access Manager

To assign a new SAM, or update information for an existing SAM, the agency Administrative Services Director or equivalent must complete and sign the SAM Access Request and Acknowledgement form ([DFS-A0-2206](#)). The form can be found on the Forms Page of the Accounting & Auditing subsection on the MyFloridaCFO.com website. The completed form must be sent to A&A for approval at Access2PALM@myfloridacfo.com.

Before submitting the [DFS-A0-2206](#) form, the prospective SAM must have an account established in:

- [Florida PALM](#)
- [Florida PALM Identity Access Management \(IAM\) Tool](#)
- [Florida PALM Solution Center Customer Portal](#) - ServiceNow Application

The [Florida PALM End User Page](#) offers end user job aids to support each of the processes outlined above.:

Agencies must maintain one primary SAM and one backup SAM. A&A will approve an agency having more than two SAMs in accordance with the standard below:

- If an agency has less than 100 End Users, the agency cannot exceed two SAMs.
- If an agency has between 101 and 200 End Users, the agency cannot exceed three SAMs.
- If an agency has between 201 and 300 End Users, the agency cannot exceed four SAMs.
- If an agency has more than 301 End Users, the agency can have five SAMs.

To request an exception, contact Access2PALM@myfloridacfo.com.

TIP: Notify agency end users when a SAM changes; the Florida PALM Solution Center will not manage changes to end user role assignments.



Inactivation of Security Access Manager

SAMs who have separated from the state, moved to another agency, or changed job responsibilities should be inactivated. To inactivate an authorized SAM, the agency Administrative Services Director or equivalent must complete the Florida PALM Security Access Manager Form, select “Inactivate Current SAM” in Section 1, and email the completed and approved form to DFS A&A at Access2PALM@myfloridacfo.com to request SAM inactivation. The email should include the SAM’s name and the effective date for the inactivation.



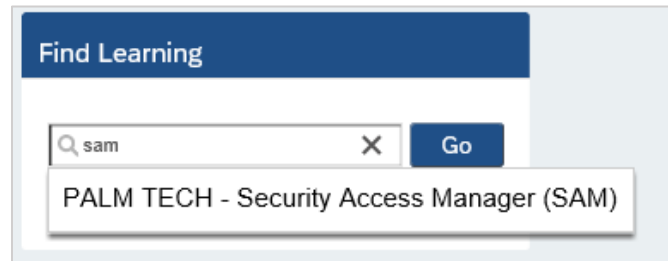
TIP: When deactivating a SAM, agencies may also need to remove their access from Florida PALM. Reference the “Inactivating End Users” section of this manual.

Security Access Manager Training

Training for managing end user access for Florida PALM as a SAM is available on the [PeopleFirst Learning Management System](#)¹. Search for “PALM TECH – Security Access Manager (SAM)”

¹ <https://peoplefirst.myflorida.com/peoplefirst>

training for a security overview, creating an end user profile, managing end user access, and reviewing end user access for separation of duty conflicts.



Find Learning

Q sam X Go

PALM TECH - Security Access Manager (SAM)

Figure 1: Training Search



TIP: The SAM training must be completed prior to the SAM performing access management responsibilities.

Florida PALM Access Management

Florida PALM access is managed through a Tool called Florida PALM Access Management. SAMs perform their work primarily through this tool. It allows a SAM to add and remove Florida PALM access.

Open the [Florida PALM Access Management²](https://fin.flpalm.myfloridacfo.gov/enduser/) tool using Chrome (preferred), Firefox, or Edge internet browser. Select your agency from the drop-down list and then click Log In.



FloridaPALM
Planning, Accounting, and Ledger Management

Please Select Your Agency.

Department of Financial Services

LOG IN

Figure 2: Florida PALM Access Management Log In

² <https://fin.flpalm.myfloridacfo.gov/enduser/>

Navigation Elements in Florida PALM Access Management

After logging into Florida PALM Access Management, you will reach the Florida PALM Access Management Dashboard. From here, you can access the functionality through easy-to-use menus. Below is a screenshot of the menu and an explanation of each menu item.

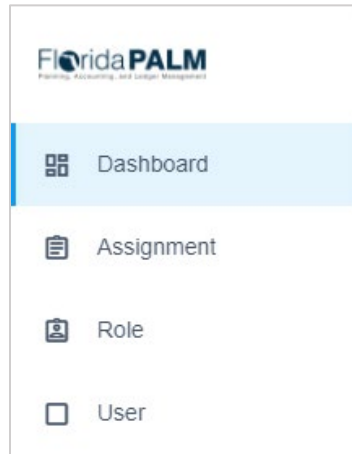


Figure 3: Florida PALM Access Management Menu

- **Dashboard** – Displays the welcome page
- **Assignment** –Use this page to view the Florida PALM system roles assigned to a Florida PALM End User Role.
- **Role** – Displays a list of Florida PALM End User Roles. If a role is selected to view, the Assignment(s) under this role will be displayed. Use this page to view the end users assigned to a role within your agency.
- **User** – Displays a list of Florida PALM end users within your agency. Use this page to activate and remove end user roles, update Business Unit security, and inactivate an end user profile.

Florida PALM Access

New End User

A new end user needs to be added to their Agency's Identity Provider (IDP). The end user must then log in to Florida PALM; this will auto-generate an account on Florida PALM. If the end user is not added to the IDP, the end user will not be able to log in to Florida PALM. End users who have logged in to create an account, will have limited access to Florida PALM until the following updates are made by the SAM within Florida PALM Access Management:

- Primary Permission List (PPL)
- Username/Route Control (Agency GL Journal Approver role only)
- Florida PALM End User Roles
- Bank Security

The below diagram depicts the steps required to establish a new end user in Florida PALM.

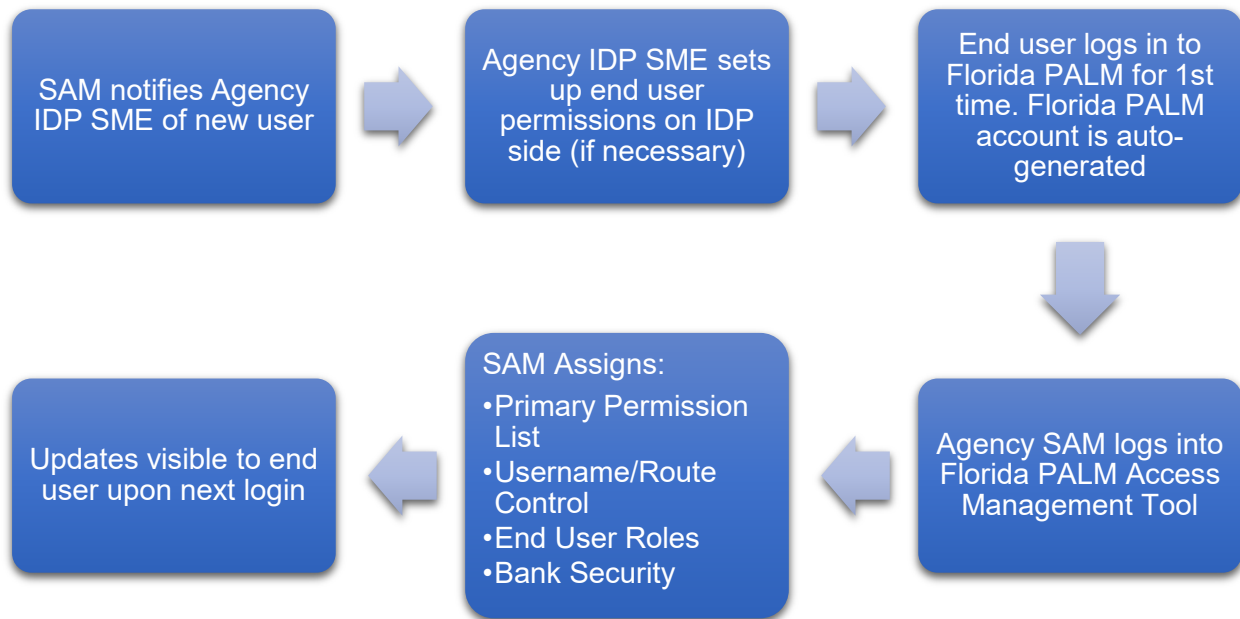


Figure 4: New End User Diagram



TIP: Changes within the Florida PALM Access Management System are updated immediately in Florida PALM.

Identity Provider

The Florida PALM Identity Access Management (IAM) system is integrated with all agencies in a manner that allows end users to authenticate using their own agency credentials. In this model the agencies act as the “IDP”. Hence the IDP is simply the agency end user directory service that contains the end user credentials and authenticates the end users on behalf of Florida PALM.

Agencies will be responsible for identity management and authentication controls, e.g., password and policies, for their end users, as well as for configuring and maintaining their identity provider interface with Florida PALM. If your agency changes your agency identity provider, please contact the Florida PALM Solution Center.

For end users to gain access to Florida PALM the agency IDP must grant them access and roles must be assigned by the SAM.



TIP: If an end user cannot access Florida PALM, coordinate with the IDP SME to confirm the end user has been added to the agency’s IDP.

End User Profile

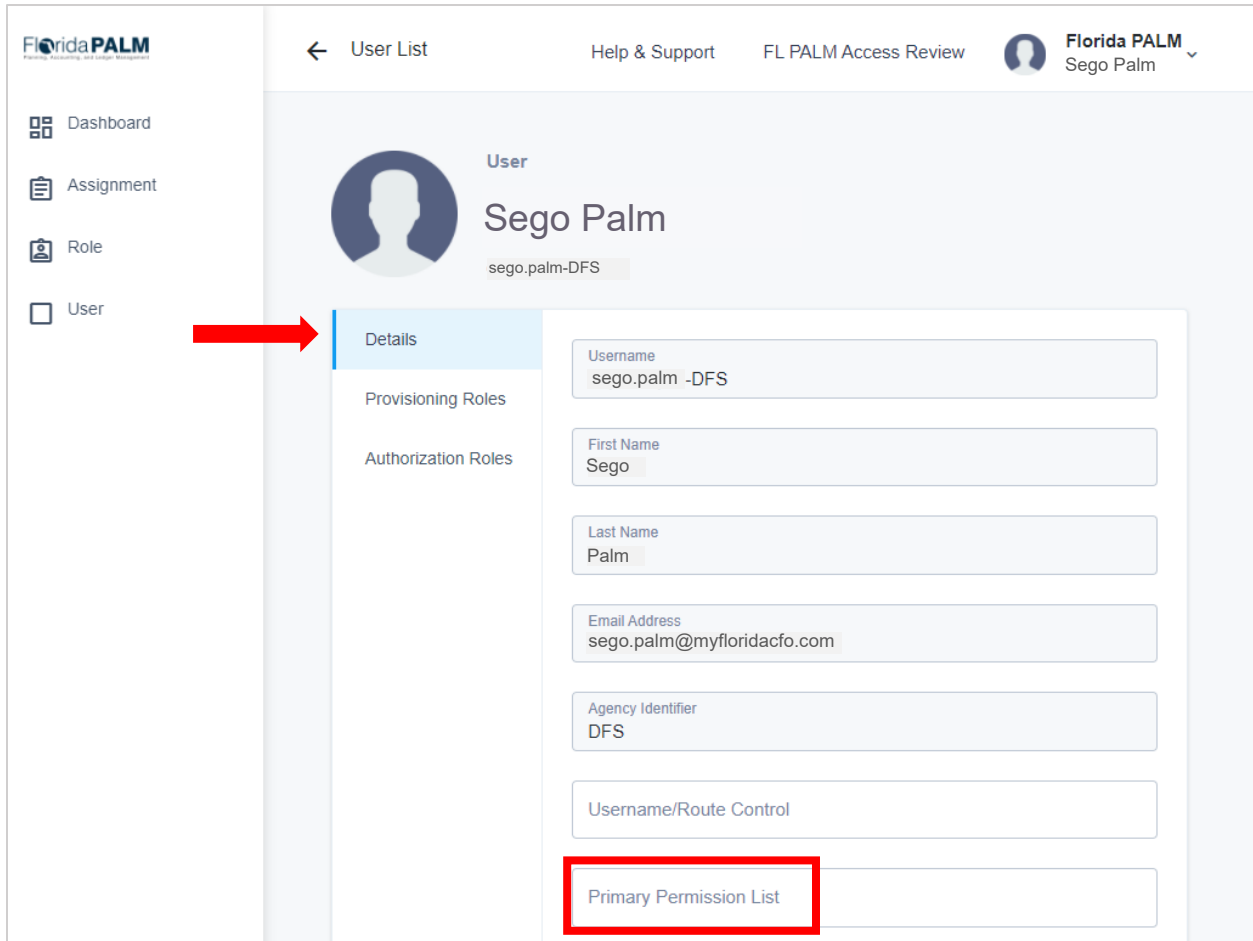
An end user is required to login to Florida PALM before a SAM can assign a Florida PALM End User Role. The new end user may establish the User Profile by logging into Florida PALM using

their agency provided end user ID and password. The end user ID and Password will be the same values the end user uses to sign into their agency computer. If the agency requires multi-factor authentication, the end user will be directed to an additional screen to confirm their identity.

Primary Permission List

When adding a new agency end user or updating an existing end user to Florida PALM Access Management, the SAM will need to enter the Primary Permission List (PPL). The PPL field is required for each new end user. A PPL allows the end user to perform functions on behalf of your agency (i.e., Business Unit) or other agencies. For example, certain end users within the Department of Revenue perform functions for other agencies; these end users would have a PPL to represent the agencies for whom they are performing work.

To add the PPL to a new end user, log into the Florida PALM Access Management tool and click “User” from the left menu bar. Search and select the new end user. Select the “Details” tab and enter the PPL. For security purposes, the PPL was provided individually to each agency. If you need assistance obtaining your agency PPL, contact your agency Tier 0 Support or the Florida PALM Solution Center.



The screenshot shows the Florida PALM Access Management interface. On the left is a navigation menu with options: Dashboard, Assignment, Role, and User. The 'User' option is selected. The main content area shows the 'User List' header with links for 'Help & Support' and 'FL PALM Access Review'. Below this is a user profile for 'Sego Palm' with the email 'sego.palm-DFS'. The 'Details' tab is selected, indicated by a red arrow. The 'Details' tab contains fields for Username (sego.palm -DFS), First Name (Sego), Last Name (Palm), Email Address (sego.palm@myfloridacfo.com), Agency Identifier (DFS), Username/Route Control, and Primary Permission List. The 'Primary Permission List' field is highlighted with a red box.

Figure 5: Entering PPL



TIP: If applicable, an end user performing activities on behalf of other agencies must update the PPL and change it back after completing the activities.

Username/Route Control

The Username/Route Control field is required when an end user has been assigned either the Agency GL Journal Approver role or the DFS YEC GL Journal Approver role. This field allows the end user to approve journals for the respective Business Unit. End users who have been assigned the Agency GL Journal Approver role without updating the Username/Route Control, will not have access to their role functions. If the new end user has not been assigned the Agency GL Journal Approver role, leave the Username/Route Control field blank in Florida PALM Access Management.

The Username/Route Control field is a combination of the end user's username (the first field on the Details tab for the user), a backslash (/), and the assigned PPL, **with the agency identifier replaced with "BU"**. For security purposes, the PPL was provided individually to each agency. If you need assistance obtaining your agency PPL or business unit, contact your agency Tier 0 Support or the Florida PALM Solution Center.

Example:

Username: JOE.SMITH-EXM

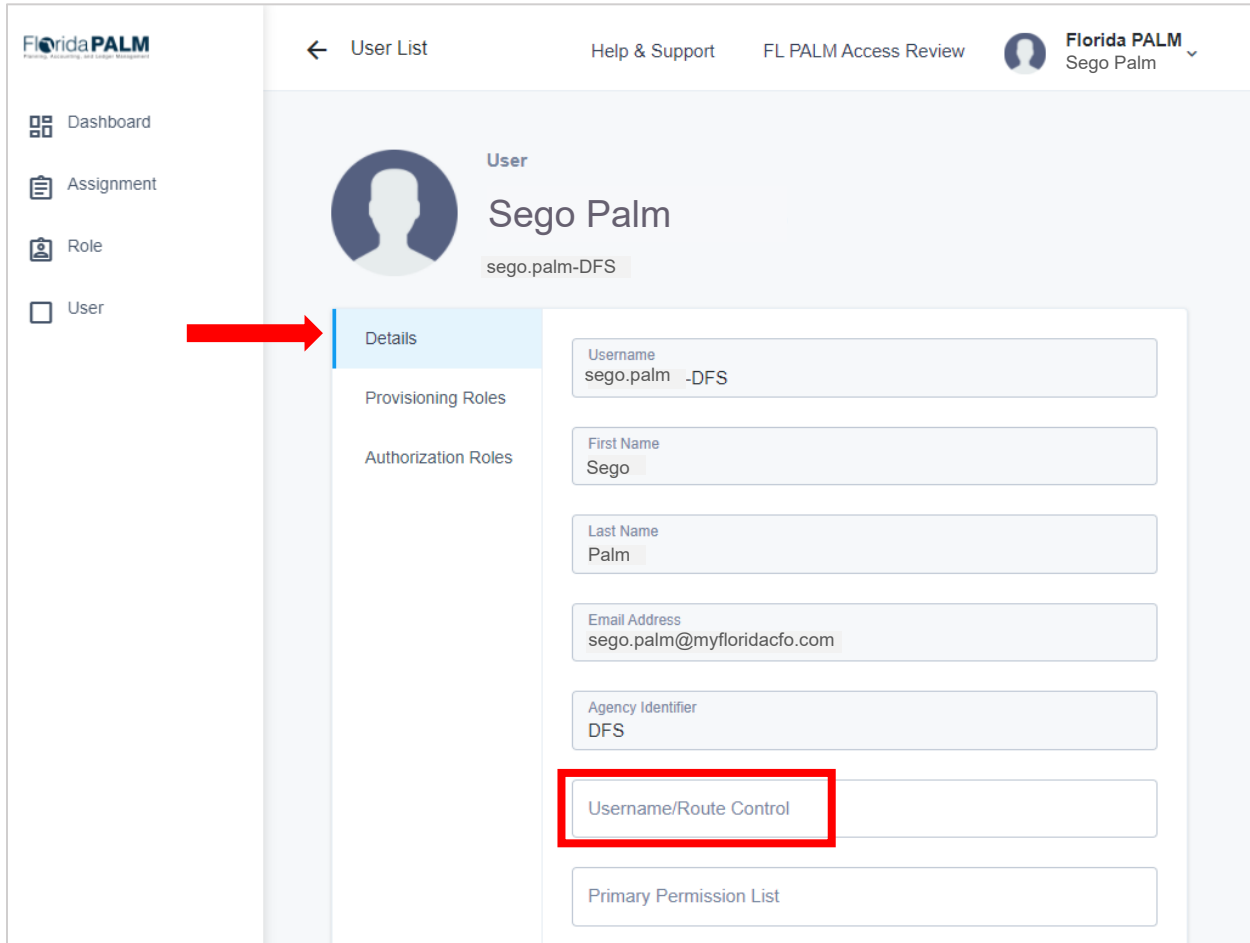
PPL: FLP_EXM_12345

Username/Route Control: JOE.SMITH-EXM/FLP_BU_12345

To add the Username/Route Control value to a new end user, log into the Florida PALM Access Management tool and click "User" from the left menu bar. Search and select the new end user. Select the "Details" tab and enter the Username/Route Control value. If you need assistance obtaining the PPL, please contact your agency Tier 0 Support or the Florida PALM Solution Center.



TIP: If removing the Agency GL Journal Approver role from an end user, the Username/Route Control value must also be removed.



The screenshot displays the 'User List' interface. On the left, a sidebar contains navigation links: Dashboard, Assignment, Role, and User. The 'User' link is selected. The main area shows the 'User' profile for 'Sego Palm' with the email 'sego.palm-DFS'. A red arrow points to the 'Details' tab in the sub-menu. The 'Details' tab is active, showing a form with the following fields: Username (sego.palm -DFS), First Name (Sego), Last Name (Palm), Email Address (sego.palm@myfloridacfo.com), Agency Identifier (DFS), and Username/Route Control (highlighted with a red box). Below these fields is a 'Primary Permission List' section.

Figure 6: Entering a Username/Route Control

Adding Florida PALM End User Roles

In the Florida PALM Access Management tool, the SAM adds a Florida PALM End User Role to the end user which grants them access to the functionality assigned to that role. The SAM may use the [Agency Role Mapping Handbook³](https://myfloridacfo.com/docs-sf/florida-palm-libraries/resources/approach-documents/agency-role-mapping-handbook84a77cf6dcaa4014a4bb40dc0bc308eb.pdf?sfrsn=180d3c09_14) found on the Florida PALM website for a list of Florida PALM End User Roles and separation of duty conflicts. Each Florida PALM End User Role breaks down into one or more System Roles that describe the specific functionality each Florida PALM End User Role grants the end users. Please reference the Florida PALM End User Role to [System Role Matrix](#) for a list of Florida PALM End User Role and assigned System Roles to confirm the functionality your end users have been assigned. SAMs will only see System Roles when running the FLP_USER_ROLES_BY_PPL query.

To add Florida PALM End User Roles to an end user, click “User” in the left menu bar. Search and select the end user. Select the “Provisioning Roles” tab and click “Add Provisioning Roles”.

³https://myfloridacfo.com/docs-sf/florida-palm-libraries/resources/approach-documents/agency-role-mapping-handbook84a77cf6dcaa4014a4bb40dc0bc308eb.pdf?sfrsn=180d3c09_14

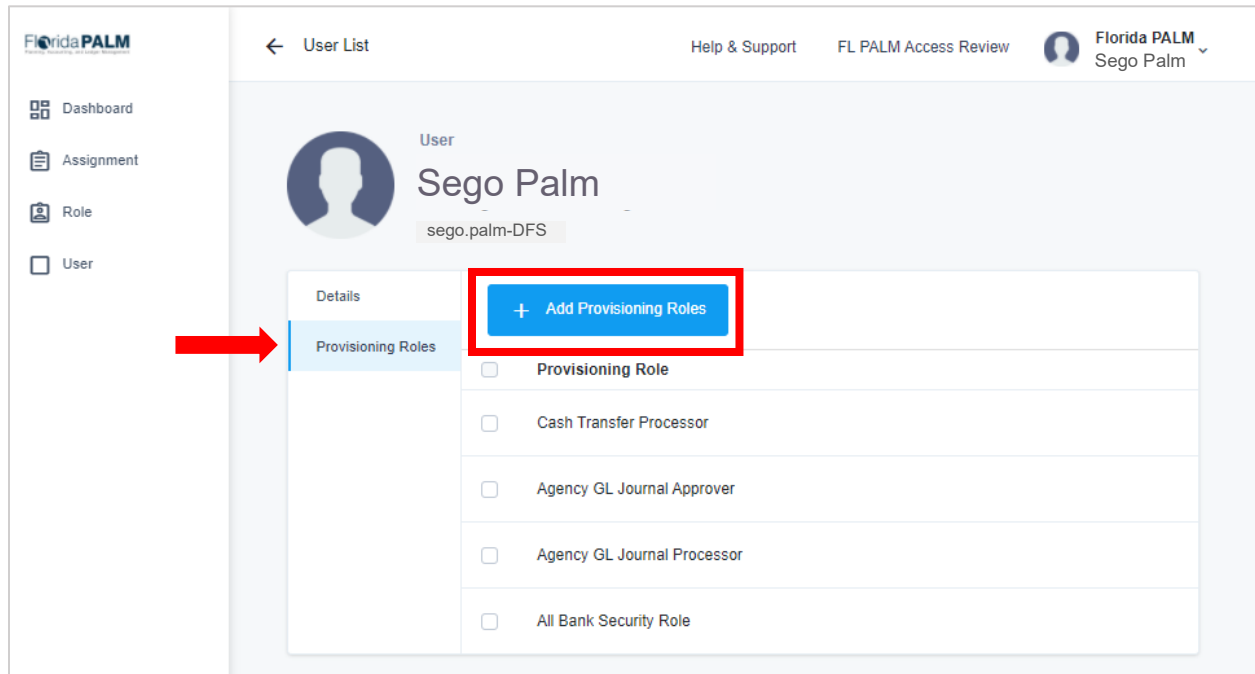


Figure 7: Add Provision Roles

Search and select the role to add. Click Save. Click Save again when prompted.

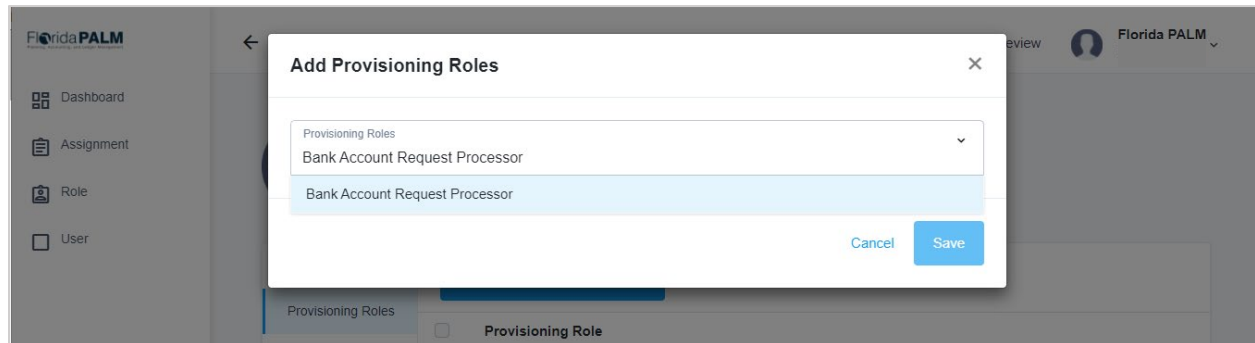


Figure 8: Saving New Provisioning Roles



TIP: When searching for roles, you must type the role name exactly as it appears in the Agency Role Mapping Handbook.

Removing Florida PALM End User Roles

When a SAM is notified an end user's responsibilities and roles have changed, the SAM must promptly update the end user's access. The SAM may remove roles in the Florida PALM Access Management tool which removes the end users' access to functionality assigned to that role. To remove Florida PALM End User Roles, click "User" in the left menu bar. Search and select the end user. Select the "Provisioning Roles" tab. Click the check box next to the appropriate role(s) and click "Remove." A warning pop-up window will appear, click "Remove."

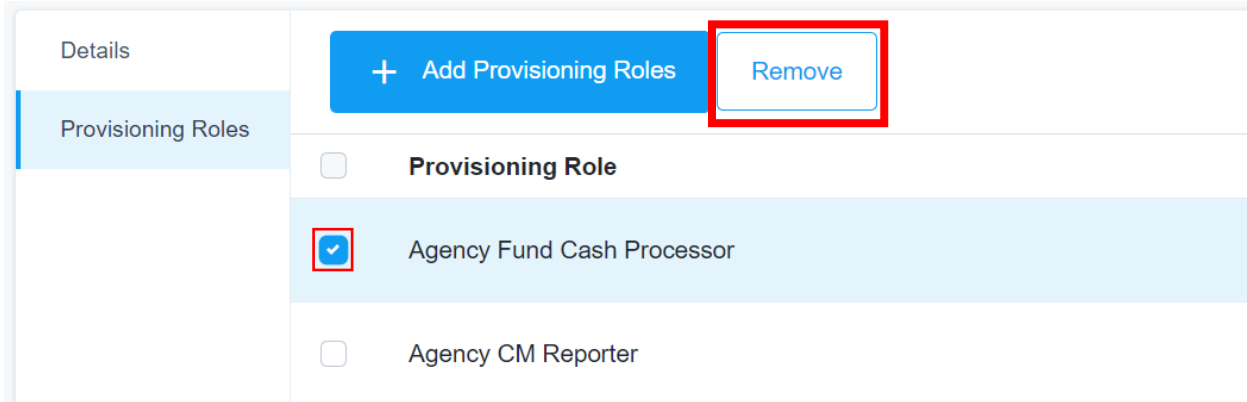


Figure 9: Remove Business Roles

Bank Security

When adding a new agency end user or updating an existing end user to Florida PALM Access Management, the SAM will need to setup the end user's Bank Security. Bank Security provides an end user access to **their** agency's bank accounts to perform necessary functions, such as view bank data on applicable transactions, (e.g., deposits and payments), and view banking reports. Depending on the Bank Security selected, it also allows the end user to perform functions on behalf of other agencies. For example, certain end users within DFS perform banking functions for other agencies; these end users would have a Bank Security to represent the agency **for whom** they are performing work.

To add the Bank Security to a new end user, the SAM will follow the steps outlined in the "Adding Florida PALM End User Roles" section of this manual. If you need assistance obtaining your agency Bank Security role name, contact your agency Tier 0 Support or the Florida PALM Solution Center.

Separation of Duties

Separation of duties (SOD) identifies which roles must not be assigned to the same end user. These rules are put in place to avoid granting an end user access to roles that cause regulatory, internal, or financial control issues with a single position.

The SAM may reference the Agency Role Mapping Handbook to determine the appropriate end user roles needed for the employee along with the SOD conflicts.

The SAM will validate there are no SOD conflicts as outlined in the Agency Role Mapping Handbook. If SOD conflicts occur, an explanation and compensating controls must be submitted to DFS A&A for approval at Access2PALM@myfloridacfo.com.

Approving SOD Conflicts

If DFS A&A determines an access combination is appropriate for the situation, despite a SOD violation, DFS A&A will grant the exception with comments and add an Exception Expiration Date. DFS A&A expects agencies to understand that SOD conflicts are not allowed to continue indefinitely. Prior to approval, agencies must provide a plan to mitigate the conflict within the period for which the exception has been granted. Exceptions are typically granted for 60 – 90 days.

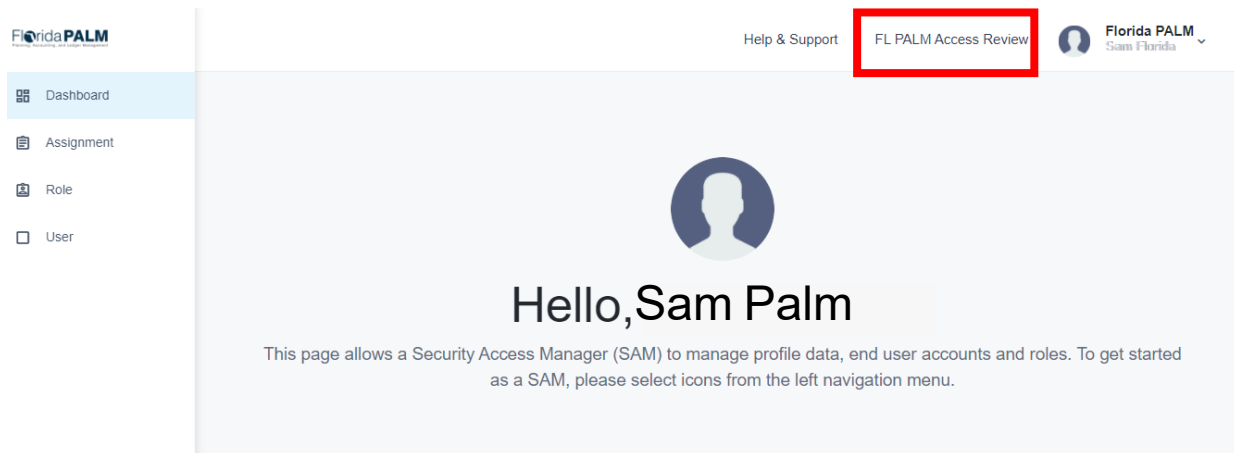


Figure 10: FL PALM Access Review link

The Violations page will provide a list of end user names and the associated SOD conflict under the “Policy” column.

☰ sam.florida-dfs) ▾

My Tasks

Violations

Active Closed

Filter table...
Q

User	Policy	Owner	Expiration Date
Security.Smith (security.smith-DFS)	SOD Conflict 8	DFS-Delegated-Admin	07/29/2021
Palm.Trees (palm.trees-DFS)	SOD Conflict 7	DFS-Delegated-Admin	07/29/2021
Orange.Grove (orange.grove-DFS)	SOD Conflict 7	DFS-Delegated-Admin	07/29/2021
Ally.Gator (ally.gator-DFS)	SOD Conflict 13	DFS-Delegated-Admin	07/29/2021

Figure 11: The Violations page

The below table provides the policy name and the associated role conflicts.

Table 1: Policy Names and Conflicting Roles

Policy Name	Role	Conflicting Role
SOD Conflict 3	Agency Requestor	DFS Bank Account Maintainer
SOD Conflict 6	DFS Bank Account Maintainer	DFS Book to Bank Reconciliation Processor
SOD Conflict 8	DFS Bank Reconciliation Processor	DFS Book to Bank Reconciliation Processor
SOD Conflict 9	Agency Requestor	DFS Correspondence Processor
SOD Conflict 10	Agency CRA Processor	DFS CRA Payment Cancellation Processor
SOD Conflict 11	DFS Bank Reconciliation Processor	DFS Investment Accounting Processor
SOD Conflict 12	Agency GL Journal Processor	DFS Investment Journal Approver
SOD Conflict 14	Agency Query Writer	DFS Query Writer
SOD Conflict 17	Agency Requestor	DFS Bank Reconciliation Processor
SOD Conflict 18	DFS Bank Account Maintainer	DFS Treasury GL Journal Processor
SOD Conflict 19	DFS Bank Reconciliation Processor	DFS CM Accounting Approver
SOD Conflict 20	DFS Bank Reconciliation Processor	DFS Treasury GL Journal Processor

Select the appropriate row. A comment may be added by clicking “Add Comment.” Click “Grant Exception”.

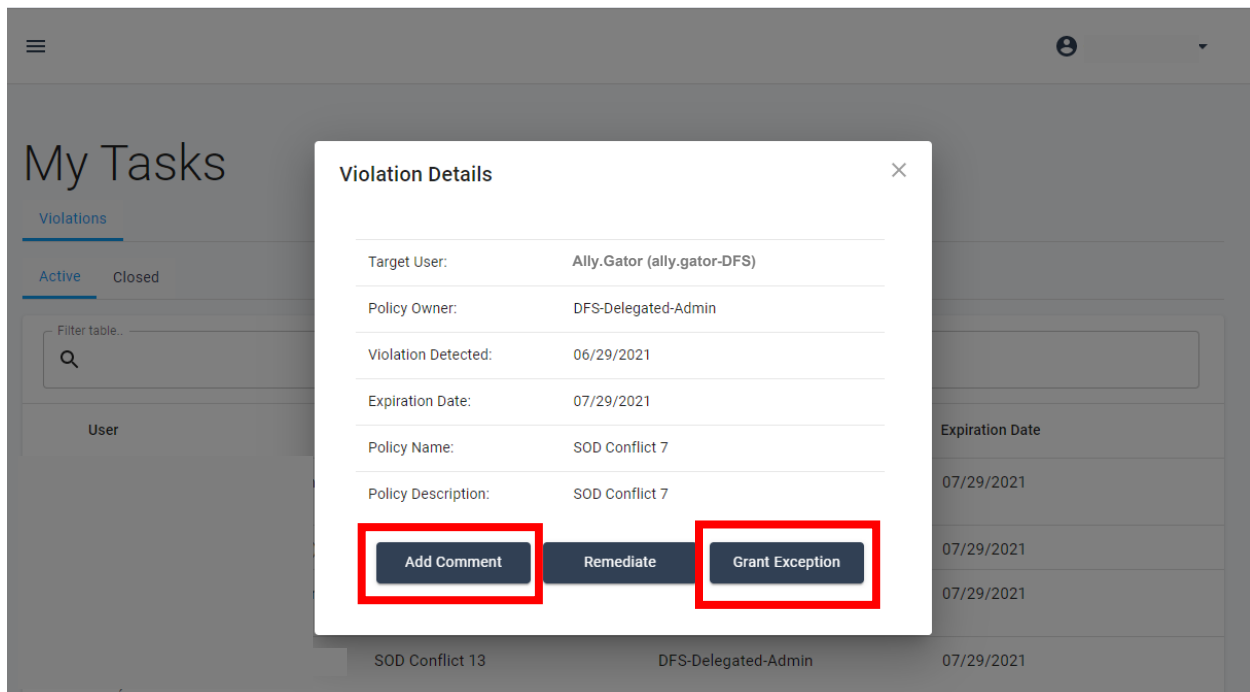


Figure 12: Add Comment and Grant Exception button

Enter a reason description and update the 'Exception Expiration Date' to a future date. The system automatically defaults to the current date; however, it needs to be updated to at least one day in the future. Click Submit Exception to accept the SOD conflict.

Violation Details

Target User: Ally.Gator (ally.gator-DFS)

Policy Owner: DFS-Delegated-Admin

Violation Detected: 06/29/2021

Expiration Date: 07/29/2021

Policy Name: SOD Conflict 8

Policy Description: SOD Conflict 8

Add Comment Remediate Hide Exception

Reason
Approved by A&A

Exception Expiration Date: 07/15/2021

Submit Exception

Figure 13: Submitting an Exception

Removing SOD Conflicts

If DFS A&A determines a SOD access combination is inappropriate, the A&A Governance Administrator can remediate the SOD violation immediately. The A&A Governance Administrator will select the “FLPALM Access Review” link on the top of the “Access Management” page to open a new window. Within the Violations page, select the appropriate name. Select the “Remediate” button to remove all conflicting roles from the end user.

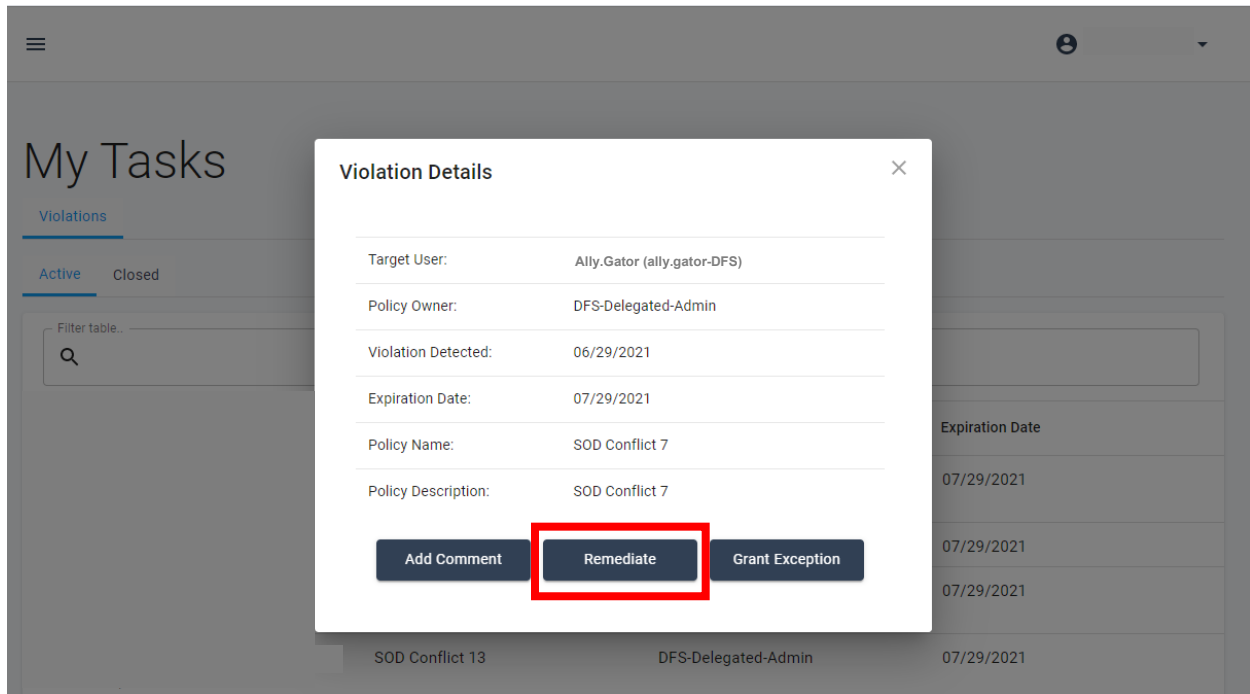


Figure 14: Remediate button

Inactivating End Users

When a SAM is notified, an end user is separating from the agency or responsibilities have changed where access to Florida PALM is no longer required, the SAM must inactivate the end user. Inactivating an existing end user requires removing all roles, Username/Route Control, PPL, and entering a status of "Inactive." The steps below depict how to inactivate an end user in Florida PALM Access Management. The Florida PALM profile remains active in Florida PALM however, without assigned roles, they cannot perform functions in Florida PALM. The end user may be removed from the agency IDP to remove access from Florida PALM.

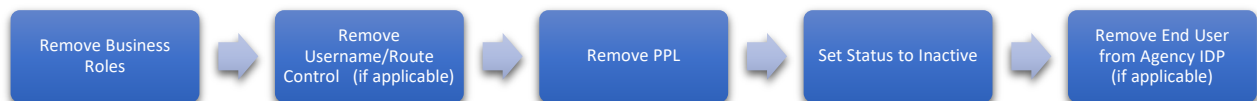


Figure 15: Inactivate End User Steps Diagram

To inactivate an end user, navigate to the Provisioning Roles tab for the appropriate end user. Select all roles and click "Remove" to remove all assigned roles. Florida PALM Access Management will request confirmation to remove the roles, click "Remove."

Click the "Details" tab and remove values within the "Username/Route Control" and "PPL" fields. In the "Status" field, enter "Inactive". Click "Save" to save all changes. The end user is now inactivated.

The screenshot shows the 'User List' page in the Florida PALM Security Access Management system. The user 'Sego Palm' is selected, and the 'Details' tab is active. The 'Username' field is 'sego.palm'. The 'First Name' is 'Sego' and the 'Last Name' is 'Palm'. The 'Email Address' is 'sego.palm@myfloridacfo.com'. The 'Agency Identifier' is 'DFS'. The 'Username/Route Control' field is highlighted with a red box. The 'Primary Permission List' field is highlighted with a red box. The 'Status' field is 'Inactive' and is also highlighted with a red box.

Figure 16: Removing Values Within Username/Route Control and PPL fields

Updates to End User Name

If an end user needs to change their first or last name, or update an email address, the end user should first close out or complete of any open journals in their workflow. Then, the SAM will then inactivate their profile and create a new profile with their name change and/or email address.

Note: When a new account is created, end user roles, bank security, PPL and Route Control will need to be added to the new account. Additionally, any personalization (Tiles, Favorites) saved in the inactivated account will not carry over to the new account.

Reports and Queries

Reports are available to support SAMs in monitoring and auditing Florida PALM end user access.

Access Control Report

The Access Control Report is a list of end users, status, and Florida PALM End User Roles. The report is used to help monitor, add, and remove end users' access.

To access the report, navigate: (<https://fin.flpalm.myfloridacfo.gov/reporting>) > Access Control Report menu button > Select the preferred report type (online, PDF, or CSV) > Enter Secret Key

The Agency Secret Key is a unique key provided to each agency. Please contact the Florida PALM Solution Center if you do not currently have the Agency Secret Key. Below is a list of report fields and descriptions

⁴ <https://fin.flpalm.myfloridacfo.gov/reporting>

Table 2: Access Control Report

Field	Field Description
Username	Username of the end user
Primary Permission List	End users' PPL which allows the end user to perform functions on behalf of your agency (i.e., Business Unit) or other agencies.
Status	Current status of the end user (i.e., Active, Inactive)
Business Role	Florida PALM End User Role assigned to the end user which grants them access to the functionality assigned to that role
System Role	System roles describing the specific functionality each Florida PALM End User Role grants the end user.
Date User Created	Date the end user created their profile in Florida PALM
Last Logon	Date the end user last logged into Florida PALM
Date Role Assigned	Date the Florida PALM End User Role was assigned to the end user
Date Role Removed (Last Action Taken)	Date the Florida PALM End User Role was removed from the end user. This is the most recent action taken on the Florida PALM End User Role.
Date User Disabled	Date end user was set to 'Inactive' Status
SAM	SAM username who assigned the Florida PALM End User Role on the Date Role Assigned field

FLP_USER_ROLES_BY_PPL Query

Florida PALM provides a query listing all current end users, PPL, and System Roles. The query is accessed by logging into Florida PALM (<https://fin.flpalm.myfloridacfo.gov>) and navigating to the below pages:

Florida PALM > Main Menu > Reporting Tools > Query > Query Viewer

Search for the FLP_USER_ROLES_BY_PPL query.

Below is a list of query fields and descriptions

Table 3: Query fields and descriptions

Field	Field Description
Username	Username of the end user
Primary Permission List	End users' PPL which allows the end user to perform functions on behalf of your agency (i.e., Business Unit) or other agencies.
System Role	Florida PALM system roles describing the specific functionality each Florida PALM End User Role grants the end user.
Last Sign on Date and Time	Date and time the end user last logged into Florida PALM

Glossary

Common terms used within, and specific to, Florida PALM.

Table 4: Glossary of Terms

Term	Definition
Business Role	Managed Role in Florida PALM Access Management tool. It contains one or multiple Florida PALM System Roles and displays on reports.
Florida PALM Access Management	Tool used by SAMs to maintain end user roles in Florida PALM.
Florida PALM Identity Access Management Reporting	Reporting tool used by SAMs to help monitor and audit end users' access.
System Role	Assignment or Managed Assignments in Florida PALM Access Management tool. These translate into PeopleSoft roles
Identity Provider (IDP)	Agency IDP where authentication takes place (Ex.: username/password/MFA)
IDP Subject Matter Expert (SME)	Technical resource at the agency who establishes integration with Florida PALM and can assist in agency related login issues, e.g. login credentials, password expiration, user information changes.
Primary Permission List (PPL)	PPL allows the end user to perform functions on behalf of an agency (i.e., Business Unit)
Security Access Manager (SAM)	Responsible person who manages the Florida PALM access for agency end users
Separation of Duties (SOD) Conflicts	Identifies which roles must not be assigned to the same end user
Solution Center	Team providing information and support to Florida PALM users. Can be contacted by phone or email: FLPALM_Solutions@myfloridacfo.com 877-352-7256 (877-FLA-PALM) rings to 850-410-9011

Florida PALM End User Role to System Role Matrix

Table 5: Florida PALM End User Role to System Role Matrix

Florida PALM End User Role Name	Role Type	System Role
Agency GL Journal Approver	Agency	FLP_AGENCY_GL_JOURNAL_APPR_1 FLP_GL_VIEWER
Agency GL Journal Processor	Agency	FLP_AGENCY_GL_JOURNAL_PROC FLP_GL_VIEWER
Agency Deposit Reporter	Agency	FLP_AR_REPORTER FLP_AR_VIEWER
DOR Agency Exception Processor	Agency	FLP_AGENCY_AR_PAYMENT_PROC FLP_AR_REPORTER FLP_AR_VIEWER
Agency Banking Reporter	Agency	FLP_CM_REPORTER
Agency Requestor	Agency	FLP_AGENCY_TREAS_CORRESPND_PRO C FLP_CM_REPORTER
Cash Transfer Approver	Agency	FLP_AGENCY_CM_PAYMENT_APPR FLP_AGENCY_CM_CASH_TRNSFR_APPR FLP_CM_REPORTER
Agency CRA Processor	Agency	FLP_AGENCY_CM_CRA_PROC FLP_CM_REPORTER FLP_GL_REPORTER FLP_GL_VIEWER
Agency Query Writer	Agency	AGENCY_QUERY_WRITER
Agency COA Maintainer	Agency	FLP_AGENCY_COA_MAINTAINER
DFS COA Maintainer	DFS	FLP_STATE_COA_MAINTAINER FLP_GL_REPORTER FLP_GL_VIEWER
DFS Investment Journal Approver	DFS	FLP_STATE_GL_JOURNAL_APPR FLP_GL_VIEWER

Florida PALM End User Role Name	Role Type	System Role
DFS GL Close Processor	DFS	FLP_STATE_GL_JOURNAL_PROC FLP_STATE_GL_CLOSE_PROC FLP_GL_REPORTER FLP_GL_VIEWER
DFS GL Reconciliation Processor	DFS	FLP_STATE_GL_JOURNAL_PROC FLP_GL_REPORTER FLP_GL_VIEWER
DFS Deposit Processor	DFS	FLP_STATE_AR_PAYMENT_PROC FLP_AR_REPORTER FLP_AR_VIEWER
DFS Deposit Approver	DFS	FLP_STATE_AR_PAYMENT_APPROVER FLP_AR_REPORTER FLP_AR_VIEWER
DFS Bank Reconciliation Processor	DFS	FLP_STATE_BANK_STMT_RECON_PROC FLP_CM_REPORTER FLP_AR_REPORTER FLP_AR_VIEWER FLP_AP_REPORTER FLP_AP_VIEWER
DFS CM Accounting Approver	DFS	FLP_STATE_CM_ACCOUNTING_APPR
DFS Bank Account Maintainer	DFS	FLP_STATE_BANK_ACCOUNT_MAINT FLP_CM_REPORTER
DFS Correspondence Processor	DFS	FLP_STATE_TREAS_CORRESPND_APPR FLP_CM_REPORTER
DFS Transfer Approver	DFS	FLP_STATE_CASH_TRANSFER_APPR FLP_STATE_CM_PAYMENT_APPR FLP_CM_REPORTER
DFS Book to Bank Reconciliation Processor	DFS	FLP_STATE_BOOK_TO_BANK_RECON FLP_CM_REPORTER
DFS Investment Accounting Processor	DFS	FLP_STATE_DM_ACCOUNTING_MAINT
DFS Investment Reporter	DFS	FLP_STATE_DM_REPORTER

Florida PALM End User Role Name	Role Type	System Role
DFS Treasury GL Journal Processor	DFS	FLP_STATE_GL_JOURNAL_PROC FLP_AGENCY_ALLOCATION_PROC FLP_GL_REPORTER FLP_GL_VIEWER
DFS Investment Override Processor	DFS	FLP_STATE_GL_JOURNAL_PROC FLP_GL_INV_OVERRIDE_PROC FLP_GL_REPORTER FLP_GL_VIEWER
DFS CRA Payment Cancellation Processor	DFS	FLP_STATE_TREAS_PYMT_CNCL_APPR
DFS Query Writer	DFS	DFS_QUERY_WRITER
Cash Transfer Processor	DFS or Agency	FLP_AGENCY_CASH_TRANSFER_PROC FLP_AGENCY_CM_PAYMENT_REQUEST FLP_CM_REPORTER
GL Reporter	DFS or Agency	FLP_GL_REPORTER FLP_GL_VIEWER
AP Reporter	DFS or Agency	FLP_AP_REPORTER FLP_AP_VIEWER
DFS Investment Viewer	DFS	FLP_STATE_DM_VIEWER
ReportDistAdmin	DFS	ReportDistAdmin
DFS YEC GL Journal Processor	DFS	FLP_STATE_GL_JOURNAL_PROC FLP_GL_VIEWER FLP_GL_REPORTER
DFS YEC GL Journal Approver	DFS	FLP_AGENCY_GL_JOURNAL_APPR_1 FLP_GL_VIEWER FLP_GL_REPORTER
DFS Reconciliation Processor	DFS	FLP_RCN_065_QRY, FLP_RCN_066_QRY, FLP_RCN_107_QRY, FLP_RCN_014_QRY, FLP_RCN_027_QRY
DFS Reconciliation Reporter	DFS	FLP_RCN_065_QRY, FLP_RCN_066_QRY, FLP_RCN_107_QRY, FLP_RCN_014_QRY, FLP_RCN_027_QRY