Nasdaq

Nasdaq Calypso

Permissions & Authorizations User Guide

Version 18

Revision 5.0

February 2025

Approved

While reasonable efforts have been made to ensure that the contents of this document are accurate, the document is provided strictly "as is", and no warranties of accuracy are given concerning the contents of the information contained in this document, including any warranty that the document will be kept up to date. Nasdaq reserves the right to change details in this document without notice. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by Nasdaq or its employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

Document History

Revision	Published	Summary of Changes
1.0	February 2024	First revision for version 18.
2.0	March 2024	Updates for version 18 monthly release.
3.0	April 2024	Updates for version 18 monthly release.
4.0	May 2024	Updates for version 18 monthly release - Added group access permissions for Report Hierarchies, group name mapping for MSAD.
5.0	February 2025	Updates for version 18 monthly release - Added Data Authorization for Attribute Configuration Window.

This document provides information on User Access Control, data authorization, and auditing.

Table of Contents

1. Overview

1.1 Running Modes

Before running the deployment, your administrator will choose the running mode regarding access permissions and authorization, under `<calypso home>\tools\local-deployer\config\deployLocalConfig.properties`.

Access Permissions: set dataServer.tokens.CALYPSO_ACCESS_CONTROL_ENABLED=true

Authorization: set dataServer.tokens.CALYPSO_DATA_AUTHORIZATION_ENABLED=true

Audit mode and Access Permissions mode are enabled by default.

The running modes can also be set using the Calypso DevOps Center.

▶ Please refer to the *Calypso DevOps Center Installation Guide* for details on using the Calypso DevOps Center.

1.1.1 Access Permissions

When running in Access Permissions mode, you will need access permissions at the Function level and at the Data level, in order to carry out any activity.

Access permissions are granted to user groups. Part of this process is to define users and user groups.

Calypso uses role-based access permissions. The client creates roles, or groups, and allocates permissions to this role or group based on the tasks for that group. For instance a role may be created for front office USD FX trading. The administrator then assigns these roles to users; a user may have more than one role.

Permissions are available for all aspects of Calypso and can provide restrictions to operations, for instance saving a trade, as well as to data items, such as viewing a specific curve.

1.1.2 Authorization

When running in Authorization mode, any static data modification will have to be authorized by another user. You can choose what type of data should be authorized.

Some operations, for instance changing static data, can be configured to require two stages - the four eyes principle. This can be forced to be two different users.

1.1.3 Auditing

All changes to data within Calypso are audited; the audit trails are viewable with a Calypso report. Some data, such as trades and products are always audited, while others can be selectively audited. For instance, quotes may be audited just for the close values, or every change.

1.2 Logon/Authentication

Calypso uses HashiCorp Vault to control access to sensitive credentials and encrypt properties in the Calypso environment file directory.

Database, LDAP and Kerberos authentication are supported.

Authentication works on the principal of tokens. The Authentication Server is responsible for authenticating internal Calypso processes such as the user details and permissions, and then provides a token to the client. The client then uses the token to access the Calypso services. The token is sufficient to validate the access to the request. It is signed using a symmetric key and is validated on each request. It has a validity period after which the token expires. The token is refreshed periodically to ensure the session is active until the user logs out.

The Auth Server is the first server that should be started when starting Calypso.

1.2.1 Passwords

With the default authentication module, user credentials are checked against those managed by the Calypso Access Permission application and stored in the core database. This out-of-the box functionality provides the following features for each account on the account and the passwords:

Passwords can be:

- Forced to use digits or special characters.
- Forced to have a minimum length.
- Expired based on a period of time, for instance 30 days, or on the number of logins. For instance it is possible to create a one-time account.

You can also provide a custom password validation routine. Your routine could prevent a user from re-using a previous password or from choosing a "forbidden" password (dictionary words, etc.), for example. To do so, you would implement your validation routine using `tk.refdata.CustomPasswordValidator`.

▶ Refer to the *Calypso Developer's Guide* for information on implementing a custom password validation routine.

Accounts can be:

- Locked out after a period of disuse.
- Locked if more than a defined number of failed login attempts occur in sequence.
- Logged out after a period of inactivity.

All login attempts, both successful and failures, are audited and can be viewed in a Calypso report.

1.2.2 Microsoft Active Directory

Calypso's Microsoft Active Directory integration consists of two components. First, in order to configure access permissions, user identifiers must exist in Calypso. These can then be put into groups and Calypso specific access permissions can then be assigned. In order to import these users, a scheduled task has been provided which attempts to import both users and groups into Calypso’s database. This scheduled task can be repeated on a regular basis in order to synchronize users and groups as they are managed in MSAD. Once this access permission is configured, users then need to be authenticated against MSAD on login.

Note that any integration with an external identity system implies that management of that user is delegated to the external system expert.

1.2.3 Database Access

The database access password is encrypted in the configuration file using two-way encryption. The encryption algorithm can be the Calypso algorithm (TEA) or a replacement algorithm meeting the client's specifications.

1.2.4 Remoting

Calypso relies on SSL to ensure a secure remoting layer. Please refer to *Calypso Installation and Upgrade System Guide* for details on configuring SSL in the application server.

2. Access Permissions Window

The Calypso system provides the ability to specify and enforce user permissions by user group. Every user is a member of one or more groups, and each group has access to:

- A given set of individual application functions that can be executed (functions like save, delete and remove in most windows, and more)
- A given set of data (like books, filters, market data, and more)

In addition, trading books can be restricted by currency and product type, and the actions that the users can carry out throughout the life of the trades can be restricted by product type.

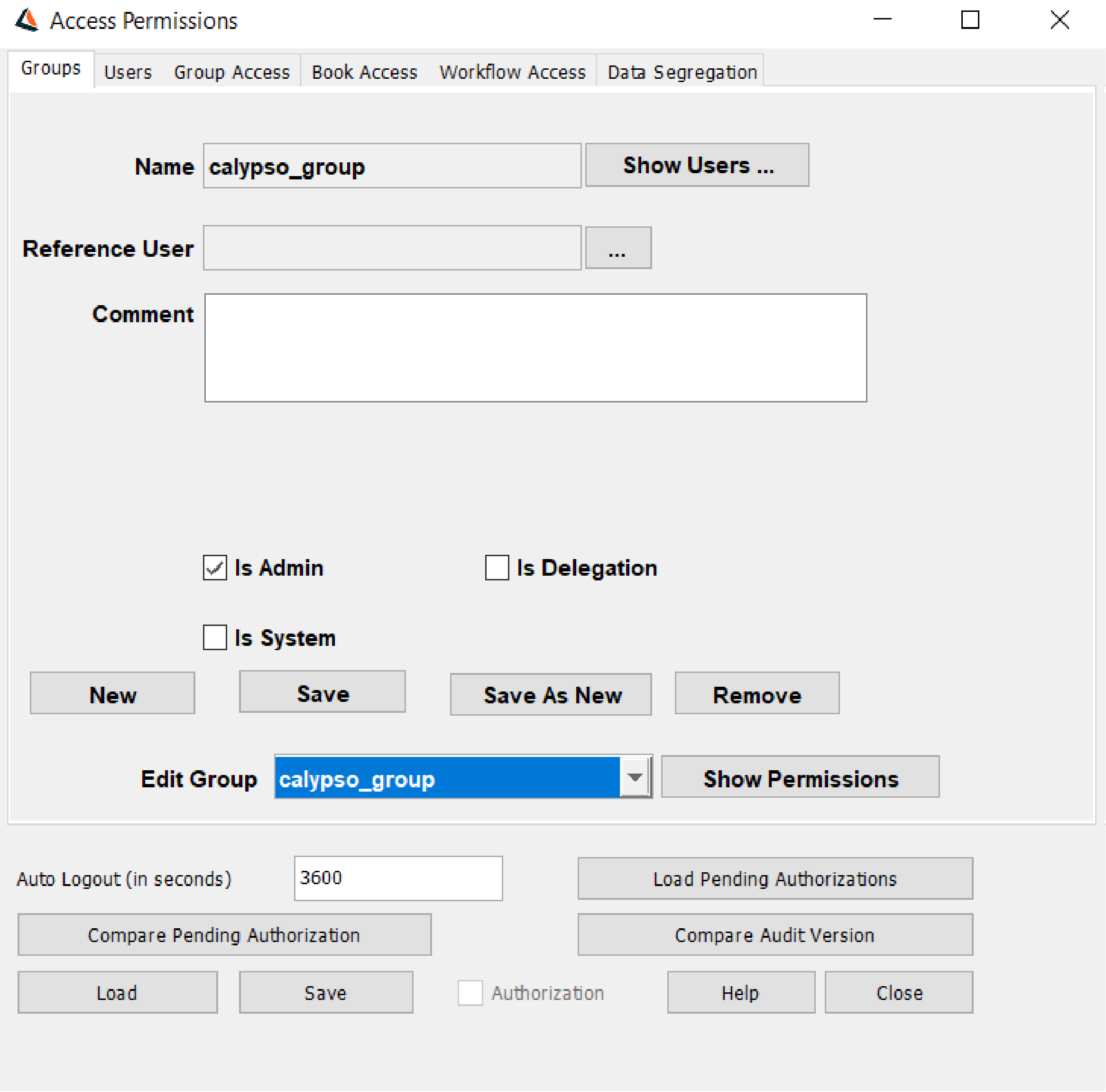
This section describes how to setup groups, users, and associated permissions.

Note that users will need to get permission from the administrator of the system to read and modify access permissions when the Access Permissions mode is enabled.

2.1 Configuring Access Permissions

Access permissions are specified using the Access Permissions window.

From the Calypso Navigator, choose **Configuration > User Access Control > Access Permissions** (menu action `refdata.AccessPermissionWindow`) to invoke the Access Permissions window.



Name: calypso_group

Reference User:

Comment:

☑ Is Admin □ Is Delegation

□ Is System

Edit Group: calypso_group

Auto Logout (in seconds): 3600

□ Authorization

Access Permissions Window

- Click **Load** to load access permission data if they are not already loaded.

  You can also click **Load** to refresh access permission data.
- To specify access permissions:
  - Create a group using the Groups panel and, if enabled, in Microsoft Active Directory. The Groups panel is selected by default.

    ▶ See Specifying Groups for details.
  - Select the Users panel to specify the users that belong to a given group. If Active Directory support is enabled, use Active Directory to specify users and establish User/Group relationships.

    ▶ See Specifying Users Using Calypso and Specifying Users Using MS Active Directory for details.

- Select the Group Access panel to associate permissions with a given group.

  ▶ See Specifying Group Permissions for details.

- Select the Book Access panel to specify restrictions on the books.

  ▶ See Specifying Book Permissions for details.

- Select the Workflow Access panel to specify restrictions on the actions that the users can carry out throughout the life of the trades.

  ▶ See Specifying Workflow Permissions for details.

» Click **Save** to save your changes, then click **Close** to close the Access Permissions window.

Note that some panels have their own **Save** button. So click the local **Save** button where available to save local changes. When you are done with all the local changes, click the general **Save** button at the bottom of the window.

Auto Logout

You can enter a number of seconds in the "Auto Logout (in seconds)" field, after which a user session will be automatically ended if it is inactive, and provided there are no pending changes to be saved. Enter 0 to disable the auto logout capability.

Authorization Mode

☑ Authorization

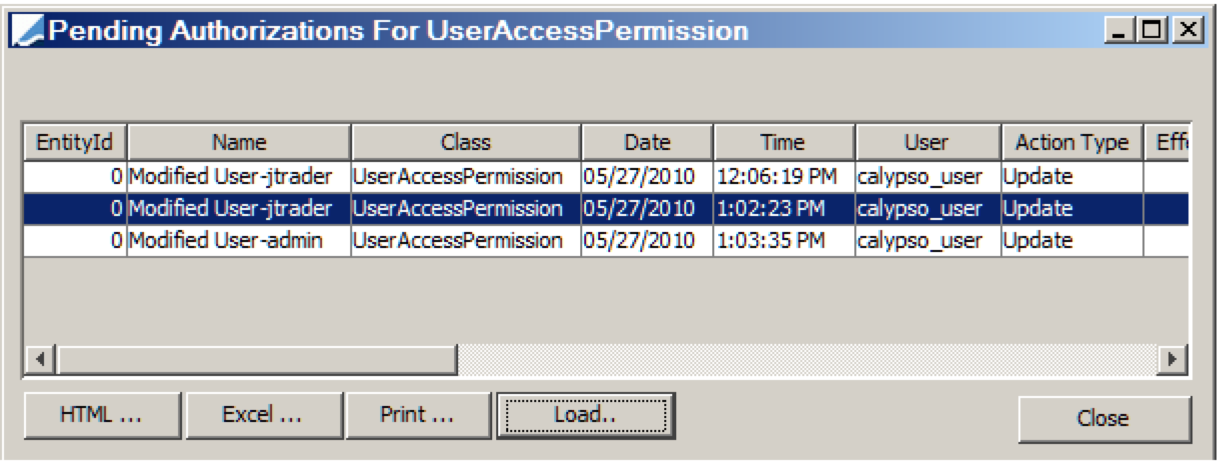
When running Access Permissions in Authorization mode, the Authorization checkbox will appear checked and grayed out. Any modifications must be authorized by an Authorization User. An Authorization User is a user who has permission to authorize modifications, and who is different from the user who actually made the modifications.

To run Access Permissions in Authorization mode, you must add UserAccessPermission to the *classAuthMode* domain from the Calypso Navigator using **Configuration > System > Domain Values** (menu action `refdata.DomainValueWindow`).

▶ See Data Authorization documentation for additional information the Authorization mode.

The following commands apply when Access Permissions is running in Authorization mode.

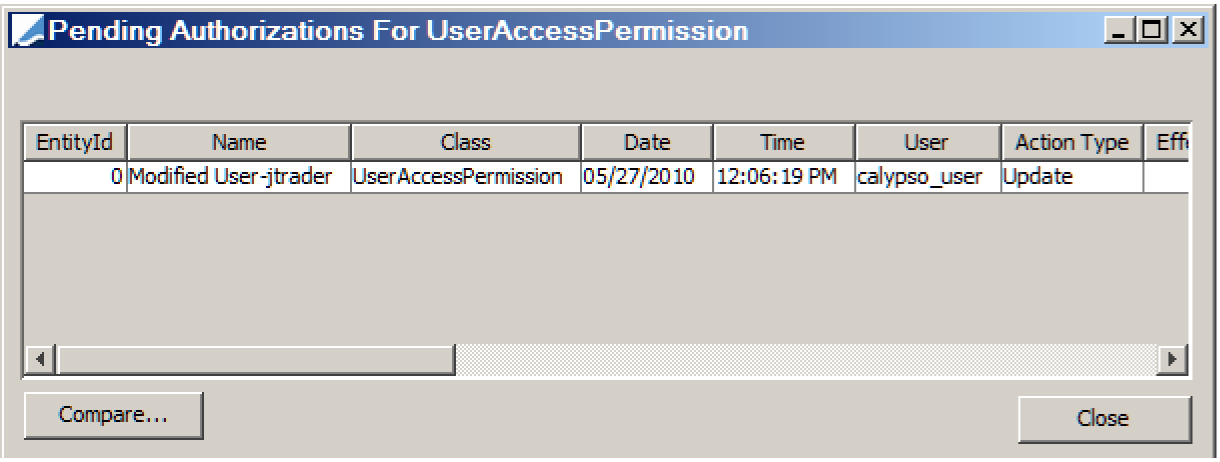
» Click **Load Pending Authorizations** to load the list of changes to Access Permissions that are pending authorization as shown below:


Pending Authorizations For UserAccessPermission

EntityId	Name	Class	Date	Time	User	Action Type	Eff
0	Modified User-jtrader	UserAccessPermission	05/27/2010	12:06:19 PM	calypso_user	Update	
0	Modified User-jtrader	UserAccessPermission	05/27/2010	1:02:23 PM	calypso_user	Update	
0	Modified User-admin	UserAccessPermission	05/27/2010	1:03:35 PM	calypso_user	Update	

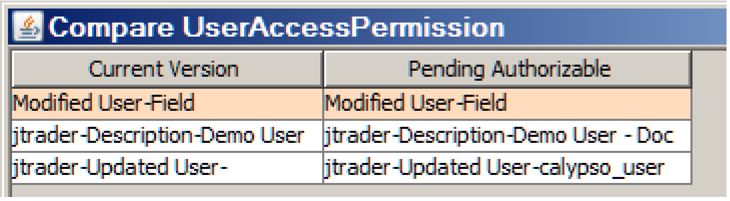
Click **Close** when you are done.

» Click **Compare Pending Authorization** to load the list of changes to Access Permissions that are pending authorization and compare with the previous version.


Pending Authorizations For UserAccessPermission

EntityId	Name	Class	Date	Time	User	Action Type	Eff
0	Modified User-jtrader	UserAccessPermission	05/27/2010	12:06:19 PM	calypso_user	Update	

Select a row, then click **Compare** to display the differences with the previous version as shown below.

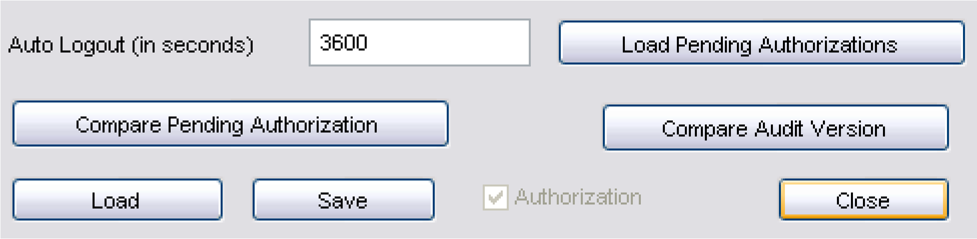

Compare UserAccessPermission

Current Version	Pending Authorizable
Modified User-Field	Modified User-Field
jtrader-Description-Demo User	jtrader-Description-Demo User - Doc
jtrader-Updated User-	jtrader-Updated User-calypso_user

Click **Close** when you are done.

Audit Mode

The system runs in Audit mode by default.

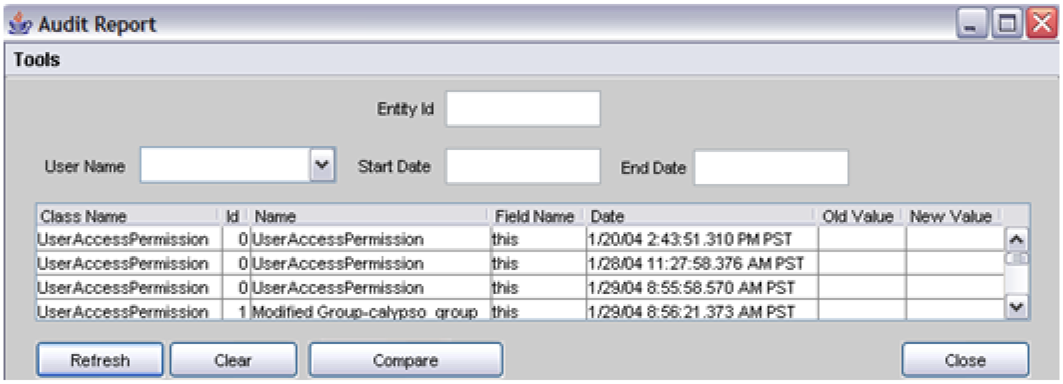


Auto Logout (in seconds): 3600

▶ See Data Auditing documentation for information the Audit mode.

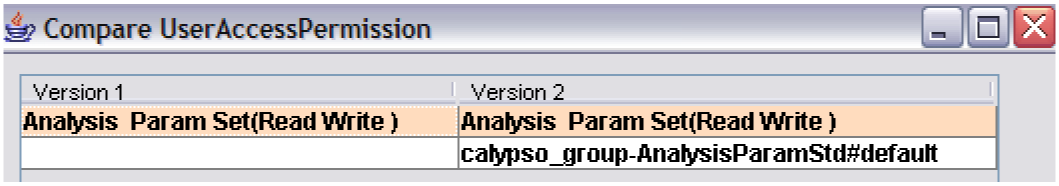
The following command applies when Access Permissions is run in Audit mode.

» Click **Compare Audit Version** to bring up the Audit Report for Access Permissions as shown below.



Class Name	Id	Name	Field Name	Date	Old Value	New Value
UserAccessPermission	0	UserAccessPermission	this	1/20/04 2:43:51.310 PM PST		
UserAccessPermission	0	UserAccessPermission	this	1/28/04 11:27:58.376 AM PST		
UserAccessPermission	0	UserAccessPermission	this	1/29/04 8:55:58.570 AM PST		
UserAccessPermission	1	Modified Group-calypso_group	this	1/29/04 8:56:21.373 AM PST		

Enter selection criteria and click **Refresh** to load the corresponding audit records. Select a record and click **Compare** to display differences with the previous version as shown below.

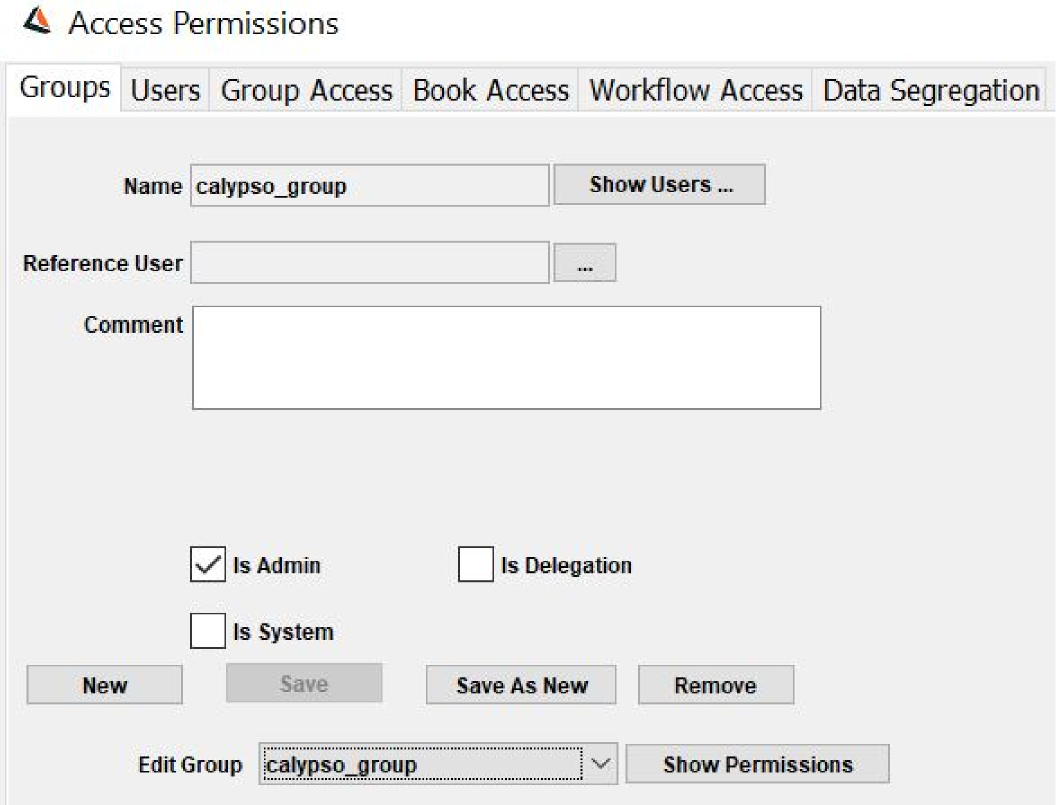


Version 1	Version 2
Analysis Param Set(Read Write)	Analysis Param Set(Read Write)
	calypso_group-AnalysisParamStd#default

Click **Close** when you are done.

2.2 Specifying Groups

Select the Groups panel to specify groups. A group is a collection of users that share common tasks, and therefore share common access permissions.



Name: calypso_group

Reference User:

Comment:

☑ Is Admin □ Is Delegation

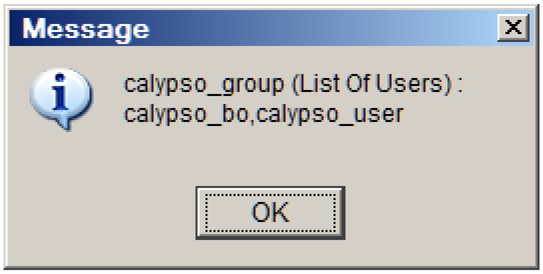
□ Is System

Edit Group: calypso_group

Select a group from the Edit Group field to load an existing group.

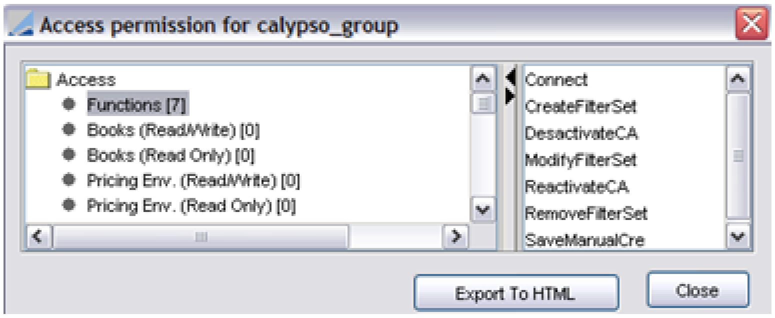
- Click **New** to create a new group. This will clear the Groups panel. Enter the fields as applicable. The fields are described below.
- Then click the local **Save** button to save your changes. You will be prompted to enter a group name. If MS Active Directory is enabled, the Group name must match the function group specified in Active Directory to allow the Calypso system to function correctly.

  It is recommended to also click the general **Save** button before proceeding to another panel.
- Click **Show Users** to view the users associated with the group currently selected as shown below.

  calypso_group (List Of Users) :
  calypso_bo,calypso_user

  You can assign users to a group using the Users panel.
- Click **Show Permissions** to view the permissions associated with the group currently selected as shown below.



Access permission for calypso_group

- Access
  - Functions [7]
  - Books (Read/Write) [0]
  - Books (Read Only) [0]
  - Pricing Env. (Read/Write) [0]
  - Pricing Env. (Read Only) [0]

Connect
CreateFilterSet
DesactivateCA
ModifyFilterSet
ReactivateCA
RemoveFilterSet
SaveManualCre

You can assign permissions to a group using the Group Access panel.

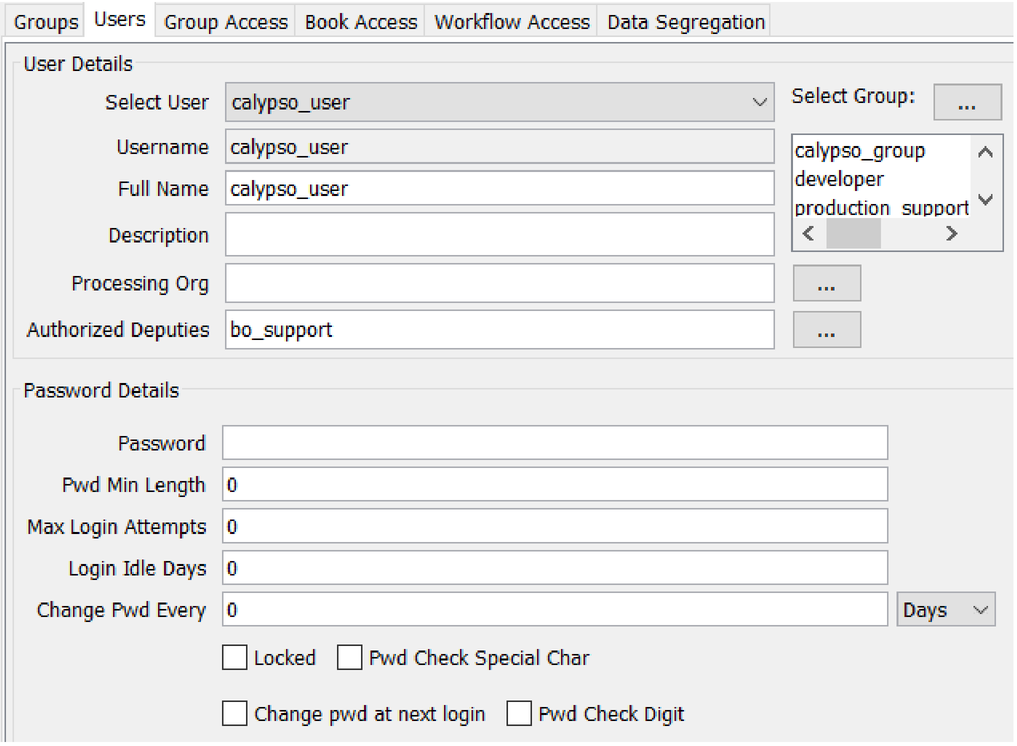
Field	Description
Reference User	Click the ... to select a reference user (optional). The reference user is used when copying the properties of a group to another group: • Main Entry Config • User Viewer Column properties • User Default Config • Task Station Config
Comment	Enter a free-text comment (optional).
Filter Set	No longer used. May produce undesired effects if used. This field will be removed from the application in a future release.
Read Only Filter Set	No longer used. May produce undesired effects if used. This field will be removed from the application in a future release.
Is Admin	Check the "Is Admin" checkbox to grant administrator privileges to the users of the group. You can also grant administrator privileges to a user by adding the user to the "admin" group. Note that the "admin" group does not need the "Is Admin" checkbox to be checked.
Is Delegation	Check the "Is Delegation" checkbox to indicate that users from that group can delegate their access permissions to another user as needed. ⓘ **[NOTE: A delegated group *cannot* be a system group, and *should not* be an admin group]** Access Permissions delegations can be configured using **Configuration > User Access Control > Delegation Window**. ▶ See Access Permission Delegation for details.
Is System	Check the "Is System" checkbox to prevent recording login information for the users of that group. Note that other information will be audited.

Field	Description
	This should be used for groups where the users run servers and engines so that they do not get locked out. You can also use the environment properties ACCOUNT_LOGINS_NOT_AUDITED and DISABLE_LOGIN_AUDIT to achieve the same results.

2.3 Specifying Users Using Calypso

Select the Users panel to create user login accounts that can access the Calypso system, and to assign users to groups.

[NOTE: To work with users when using MS Active Directory for authentication, refer to Specifying Users Using MS Active Directory. When using Active Directory, the User/Group relationship and User management functions are both controlled by Active Directory]

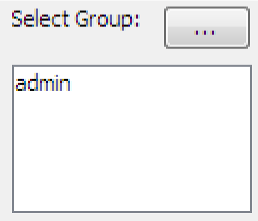


Select User: calypso_user
Username: calypso_user
Full Name: calypso_user
Description:
Processing Org:
Authorized Deputies: bo_support
Select Group: calypso_group, developer, production, support

Password:
Pwd Min Length: 0
Max Login Attempts: 0
Login Idle Days: 0
Change Pwd Every: 0 Days

□ Locked □ Pwd Check Special Char
□ Change pwd at next login □ Pwd Check Digit

- Use the Select User drop down to choose an existing User to modify.
- Click **New** to create a new user. This will clear the Users panel. Enter the fields as applicable. The fields are described below.
- Click the Select Group button (**...**) to assign the user to one or more groups. You will be prompted to select groups.



Select Group: ...

admin

The selected groups will appear in the field below the Groups box (e.g., admin in the above example).

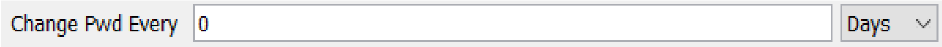
- Enter a Password in accordance with your organization's standards.
- Enter the Minimum Password Length.
- Enter the Maximum number of failed login attempts before the system locks out the User.
- Login Idle Days displays the maximum number of number of days without a login before the system locks out the user. The system can lock the user in two ways:
  - Trigger by the user trying to login and already pass the idle days.
  - Configure the LOCK_INACTIVE_USERS scheduled task, which does not have any parameters, to run daily to lock the user passing the idle days.
- Change Pwd Every specifies the interval in days or the number of logins between forced password changes.
- Click **Save** to save your changes. You will be prompted to enter a user name.

  It is recommended to also click the Access Permission window's **Save** button at the bottom of the window before proceeding to another panel.

[NOTE: Calypso saves the user name to the database in lower case]

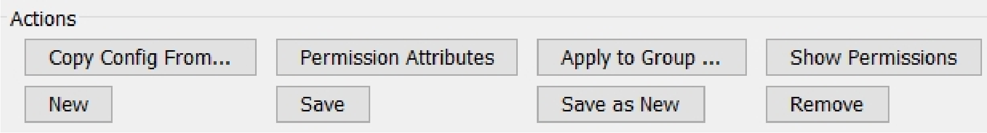
Additional available actions are described below.

Fields	Description
Full Name	Enter the user's full name (mandatory).
Password	Enter a password for the user (mandatory). The user will be able to change the password after logging in. ▶ Please refer to Change Password documentation for details.
Description	Enter a free-text description of the user (optional).
Processing Org	Click the **...** button next to the Processing Org field to select a set of processing organizations (optional). Use Shift+Click or Ctrl+Click to select multiple processing orgs. **[NOTE: If the ModifyOnlyProcessingOrgTrade and ViewOnlyProcessingOrgTrade functions are granted, the user will only have access to the trades in the books associated with those processing orgs in Trade Report, Cash Flow Report, Account Enrichment, Trade Blotter and Trade Selector]** Also, if the ModifyOnlyProcessingOrgStaticData and the ViewOnlyProcessingOrgStaticData

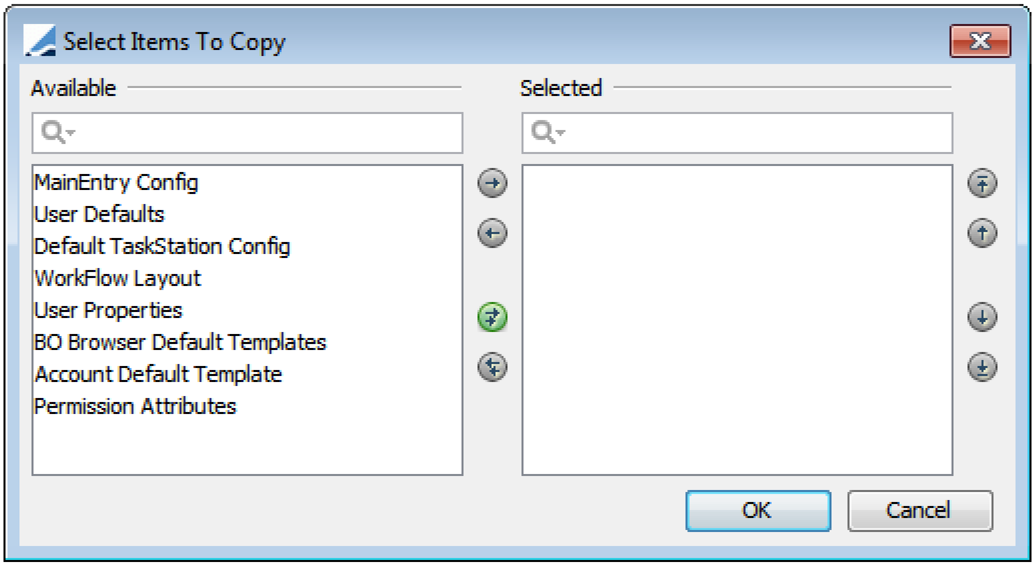
Fields	Description
	functions are granted to the user's group, the user will only be able to view and modify static data of the processing organizations specified here.
Authorized Deputies	Select users to whom the user can delegate his or her access permissions as needed. The deputy must have access to the group defined with "Is Delegation" checked, and must have access to the Applications required to perform the actions (Navigator for example). Access Permissions delegations can be configured using **Configuration > User Access Control > Delegation Window**. ▶ See Access Permission Delegation for details.
Pwd Min Length	Enter the minimum length of the password (optional). You can also provide a custom password validation routine. Refer to the *Calypso Developer's Guide* for information on implementing a custom password validation routine.
Change Pwd Every	 Change Pwd Every 0 Days Enter a number and then select Days or Logins from the drop down selector to set the interval in days or number of logins that are permitted between forced password changes. You can also use the environment property **MAX_SESSIONS_PER_APP_PER_USER** to limit the number of times the users can login.
Max Login Attempts	Enter the maximum number of failed login attempts allowed before the user is automatically locked out (optional). Enter 0 for no limit. If the user reaches that maximum, the Locked checkbox will be checked automatically, and an administrator will have to unlock the user, so that the user can access the system again. ▶ See Resetting Login Info for information on unlocking a user.
Login Idle Days	Enter the number of idle days allowed before the user is locked (optional). Enter 0 for no limit. If the user does not login for the specified number of days, the Locked checkbox will be checked automatically, and an administrator will have to unlock the user, so that the user can access the system again. ▶ See Resetting Login Info for information on unlocking a user.
Last Login Date	Last successful login date, retrieved from the user information.
Number of Att	Number of failed attempts since the last successful login, retrieved from the user information. The number of failed attempts is only recorded when Max Login Att is set.
Pwd Change Date	Last date the password has been changed, retrieved from the user information.
Locked	Check the Locked checkbox to prevent the user from accessing the system. The locking date will appear in the Locked Since field in the Status group.

Fields	Description
	▶ See Resetting Login Info for information on unlocking a user. This checkbox is automatically checked if the user reaches the maximum number of failed login attempts, or does not log in for the specified number of idle days. ⓘ **[NOTE: A user will not be automatically locked if the Access Permissions mode is not enabled]**
Change pwd at next login	Select the "Change pwd at next login" checkbox to force the user to change his or her password at the next login.
Pwd Check Digit	Select the "Pwd Check Digit" checkbox to force users to use at least one number character in their password.
Pwd Check Special Char	Select the "Pwd Check Special Char" checkbox to force users to use at least one special character (for example "?") in their password.

Available Actions



- You can click **Copy Config From** to apply a number of configurations from a given user to the currently selected user. You will be prompted to select a user, then use the selector to choose the configuration(s) you wish to copy:

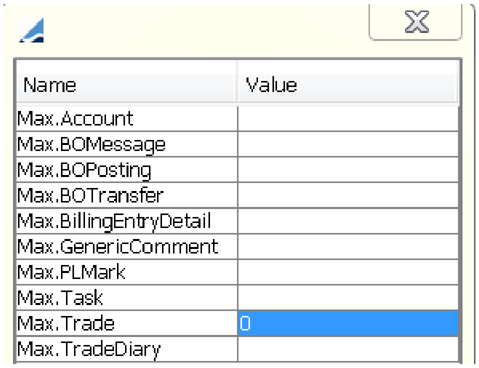


  - MainEntry Config is no longer used.
  - User Defaults applies to default values for trade entry.
  - Default TaskStation Config applies to the Task Station.

- Workflow Layout applies to the workflow graph configuration.
- User Properties applies to the Users panel in Access Permissions. It allows setting default fields from another user.
- BO Browser Default Templates applies to the BO Browser.
- Account Default Template applies to the Account definition.
- Permission Attributes applies to user attributes.

» You can click **Apply to Group** to apply the current settings to all the users of a given group. You will be prompted to select a group.

» You can click **Permission Attributes** to set User attributes.



Name	Value
Max.Account	
Max.BOMessage	
Max.BOPosting	
Max.BOTransfer	
Max.BillingEntryDetail	
Max.GenericComment	
Max.PLMark	
Max.Task	
Max.Trade	0
Max.TradeDiary	

The following attributes can be set:

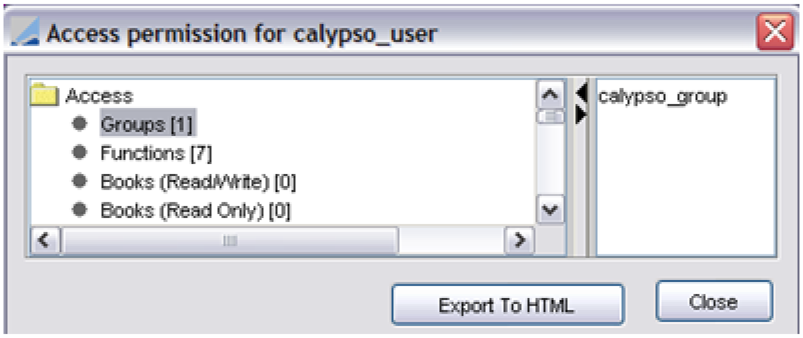
- Max.Account – The maximum number of Accounts to return.
- Max.Balance - The maximum number of balance positions loaded by the Balance report and the Balance Activity report (default is 100000).
- Max.BOAudit – The maximum number of BOAudit records to return.
- Max.BOMessage – The maximum number of BO messages to return.
- Max.BOPosting – The maximum number of BO postings to return.
- Max.BOTransfer – The maximum number of BO transfers to load in Reports.
- Max.BillingEntryDetail - The maximum number of billing details to load in Reports.
- Max.GenericComment – The maximum number of generic comments to load in reports.
- Max.InventoryPosition - The maximum number of inventory position to load in reports.
- Max.OfficialPLMark – The maximum number of Official P&L Marks that can be loaded in the Official P&L Mark report.
- Max.PLMark – The maximum number of P&L Marks that can be loaded in the PLMark report.
- Max.PaymentSetup - The maximum number of Valid Payment configurations to be loaded in the Valid Payment Setup window.

- Max.PendingModif - Used in Authorization Audit window. If the number of elements retrieved is greater than this limit, the process is stopped and an error is thrown. (This check is not in place for admin users.)
- Max.ManualSdi – The maximum number of Manual SDIs that can be loaded in the Browse panel of the Manual SDI window and Cash Manual SDI window.
- Max.Task – The maximum number of tasks to return.
- Max.Trade – The maximum number of trades to return.
- Max.TradeDiary – The maximum number of Trade Diary Records to return.
- Max.TradeIdLoad - The maximum number of Trade IDs that can be loaded into memory.

If an attribute is not available for selection, you can add it to the domain *userAccessPermAttributes*.

The domain `UnVersionedCacheableObject` contains `Value = UserAccessPermissionSQL._cache`. It allows refreshing the read-only data server cache in case any User attribute is modified.

» You can click **Show Permissions** to view the groups associated with the user currently selected as shown below.



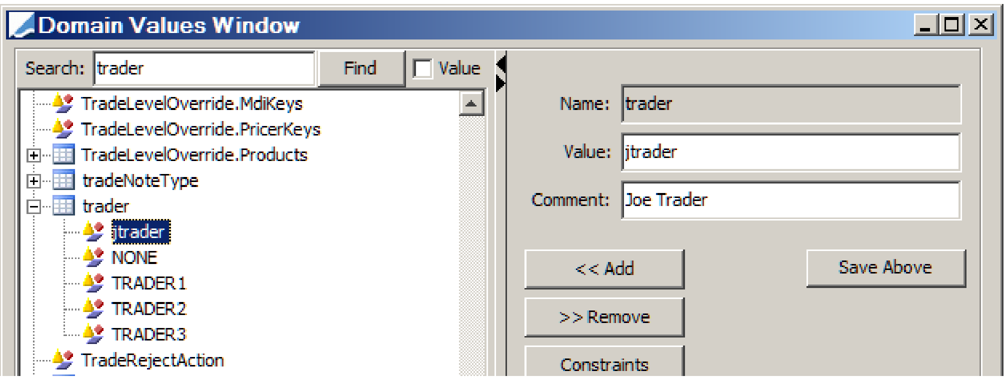
You can assign permissions to a group using the Group Access panel.

» You can click **Remove** to delete a user. Note that it will also delete all private templates associated with the user.

2.3.1 Registering Users

Trader

If a newly created user is a trader, you must add it to the *trader* domain using **Calypso Navigator > Configuration > System > Domain Values** (menu action `refdata.DomainValueWindow`).



Search: trader

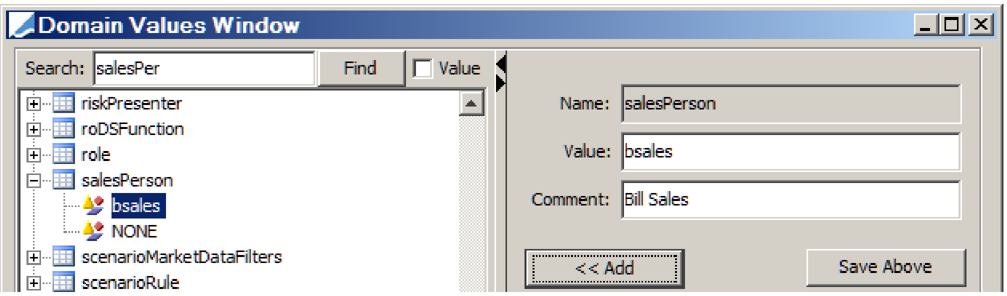
Name: trader

Value: jtrader

Comment: Joe Trader

Sales Person

If a newly created user is a sales person, you must add it to the *salesPerson* domain using **Calypso Navigator > Configuration > System > Domain Values** (menu action `refdata.DomainValueWindow`).



Search: salesPer

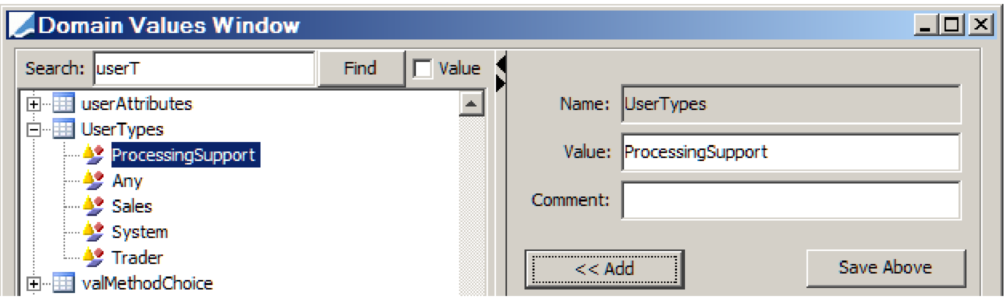
Name: salesPerson

Value: bsales

Comment: Bill Sales

Other User Types

You can assign other user types to a given user using **Calypso Navigator > Configuration > User Access Control > User Defaults** (menu action `refdata.UserDefaultsWindow`). User types are retrieved from the *UserTypes* domain.



Search: userT

Name: UserTypes

Value: ProcessingSupport

Comment:

2.3.2 Resetting Login Info

A user can be locked (the Locked checkbox is checked) after one of the following actions, and only if the Access Permissions mode is enabled:

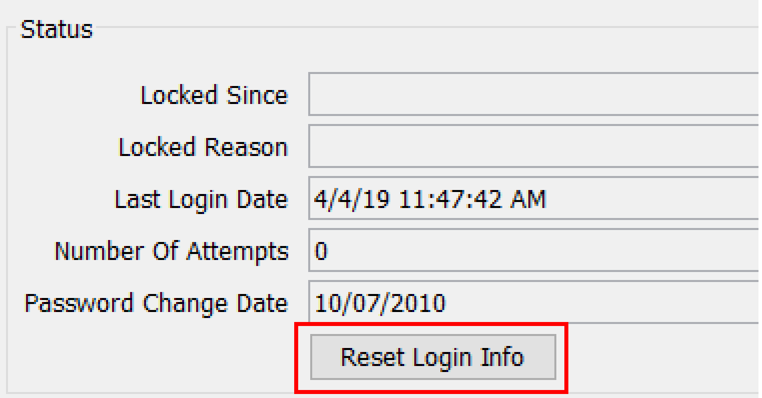
- Reaching the maximum number of failed login attempts

- Reaching the number of idle days
- Being locked by an administrator

Only an administrator can unlock the user, so that the user can access the system again.

Do the following to unlock a user:

» Load the user and click **Reset Login Info**.



Status

Locked Since

Locked Reason

Last Login Date 4/4/19 11:47:42 AM

Number Of Attempts 0

Password Change Date 10/07/2010

» Then click the local **Save** button to save the user, and click the general **Save** button at the bottom of the window.

2.4 Specifying Users Using MS Active Directory

2.4.1 Overview

Calypso's Microsoft Active Directory integration consists of two components. First, in order to configure access permissions, user identifiers must exist in Calypso. These can then be put into groups and Calypso specific access permissions can then be assigned. In order to import these users, a scheduled task has been provided which attempts to import both users and groups into Calypso's database. This scheduled task can be repeated on a regular basis in order to synchronize users and groups as they are managed in MSAD. Once this access permission is configured, users then need to be authenticated against MSAD on login.

Note that any integration with an external identity system implies that management of that user is delegated to the external system expert.

When using MS Active Directory to manage user access to Calypso, the following changes occur:

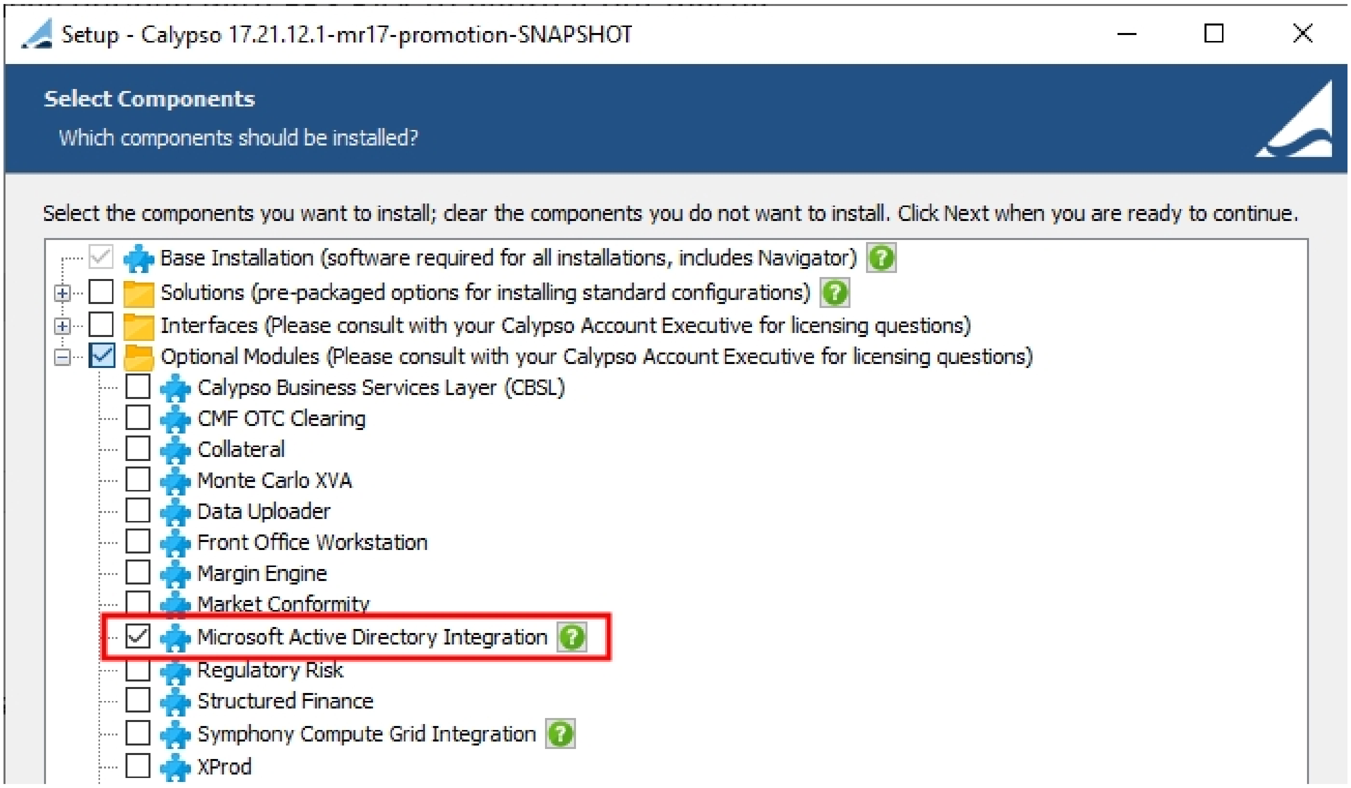
- Because Active Directory manages a number of user functions, the comparable Calypso functionality is disabled. The following fields, checkboxes, and buttons are disabled:
  - Fields: Select Group, Password, Pwd Min Length, Change Pwd Every
  - Checkboxes: Pwd Check Special Char, Change pwd at next login, Pwd Check Digit
  - Buttons: New, Save As New, Remove
- Administrators will insert, update, and delete user credentials using Active Directory, not the Users tab of the Access Permissions window.

- Administrators manage the remaining user functions (manual locking, Permission Attributes, Apply to Group, Copy Config From, Processing Org, etc.) on the Users tab of the Access Permissions window.
- Group names follow local Active Directory naming conventions. Group names specified in Calypso must exist in Active Directory.
- Administrators will manage user/group relationships using Active Directory.
- Audit Records are maintained using a user's domain/user_name.
- Active Directory is used to authenticate Calypso logins.

2.4.2 Enabling MS Active Directory Support in Calypso

If your site uses Microsoft Active Directory, you have the option to use the MSAD LDAP service to perform user authentication in Calypso.

You can enable Active Directory support in Calypso by selecting the optional module "Microsoft Active Directory Integration" in the Calypso Installer.



Setup - Calypso 17.21.12.1-mr17-promotion-SNAPSHOT

Select Components

Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

- ☑ Base Installation (software required for all installations, includes Navigator)
- ⊞ □ Solutions (pre-packaged options for installing standard configurations)
- ⊞ □ Interfaces (Please consult with your Calypso Account Executive for licensing questions)
- ⊟ ☑ Optional Modules (Please consult with your Calypso Account Executive for licensing questions)
  - □ Calypso Business Services Layer (CBSL)
  - □ CMF OTC Clearing
  - □ Collateral
  - □ Monte Carlo XVA
  - □ Data Uploader
  - □ Front Office Workstation
  - □ Margin Engine
  - □ Market Conformity
  - ☑ Microsoft Active Directory Integration
  - □ Regulatory Risk
  - □ Structured Finance
  - □ Symphony Compute Grid Integration
  - □ XProd

Step 1 – Grant the Active Directory user access to the Admin page of the Data Server.

» Create a group called "AdmServer" in MSAD and add the user to it.

Step 2 – Configure users and Calypso function groups in Microsoft Active Directory.

Step 3 – Remove all existing users from the Calypso database.

- Start Calypso without enabling MSAD.
- Run the scheduled task SYNCLDAPUSER. It will remove all existing users from the database and populate the database with the users configured in MSAD (from Step 1).

  ▶ See Synchronizing the MS Active Directory for details on SYNCLDAPUSER scheduled task.
- Shut down Calypso.

Step 4 – Define user names and passwords in Calypso.

- Set the environment properties as follows:
  - CLIENTUSER=<user name as defined in MSAD>
  - CLIENTPASSWD=<password defined for the user in MSAD>
  - AutoPrependDomain

    always – Always prepend the Windows domain to the user name typed (from Calypso Navigator login window) when running on Windows.

    true – Prepend if necessary, i.e. when running on Windows and the username entered does not contain '\' ("ny_calypso\jsmith"), then prepend the domain name.

    not set or any other value – Do not prepend.

Step 5 – Enable MSAD authentication.

- Modify the configuration file "`resources/Core.DataServer.clientconfig.xml`" as follows:
  - Add "enableMSAD" to the "depends–on" property in the DSConnection bean.
  - Uncomment the enableMSAD bean.

Before:

```
<bean id="DSConnection" class="com.calypso.tk.service.DSConnection" lazy-init="true" init-
method="init" destroy-method="stopSession" depends-on="ClientBeans">
```

```
<!--
<bean id="enableMSAD" class="com.calypso.security.auth.callback.CalypsoClientCallbackHandler">
<property name="msadEnabled" value="true" />
</bean>
-->
```

After:

```
<bean id="DSConnection" class="com.calypso.tk.service.DSConnection" lazy-init="true" init-
method="init" destroy-method="stopSession" depends-on="enableMSAD,ClientBeans">
```

```
<bean id="enableMSAD" class="com.calypso.security.auth.callback.CalypsoClientCallbackHandler">
<property name="msadEnabled" value="true" />
</bean>
```

» Modify the configuration file "`resources/appConfig/authserver.properties`" as follows:

Add:

```
calypso.ldap.enabled=true
calypso.ldap.parseusername=true
```

To restrict authentication to LDAP users only. add:

```
calypso.ldap.authflag.required=true
```

[NOTE: After making configuration changes, you must re-deploy your application servers using the Local Deployer or the DevOps Center. Please refer to the *Calypso Installation Guide* for details]

Step 6 – Replace Calypso security with MSAD security.

LDAP authentication is available out-of-the-box. The following environment properties should be set in the Environment:

- MSAD_URL=<LDAP hostname>
- MSAD_BIND_DN=<username as defined in MSAD>
- MSAD_BIND_CREDENTIAL=<password as defined for user in MSAD>
- MSAD_BASE_CTX_DN=<cn=Users, dc=ny, dc=calypso, dc=com>
- MSAD_SEARCH_FILTER=sAMAccountName={0}

[NOTE: MSAD_BIND_CREDENTIAL can optionally be encrypted with key=MSAD_BIND_DN using Calypso Encryptor Launcher available with Calypso CLI]

▶ See Command Line Instructions for details.

Step 7 – Re-start Calypso. MSAD is now used for user authentication.

2.4.3 Synchronizing MS Active Directory

It is recommended to run the scheduled task SYNCLDAPUSER on a regular basis to synchronize the MS Active Directory with Calypso users. Calypso recommends every 300 seconds.

The SYNCLDAPUSER scheduled task:

- Reads the group names from the property file "client/resources/sync_ldap_group_mapping.properties".

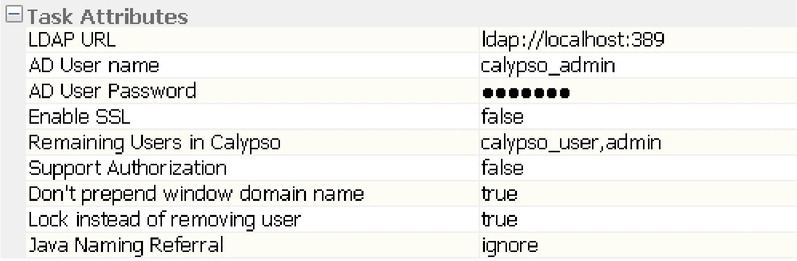
It should contain rows with <Calypso group name>=<MSAD group name>

If this file does not exist, the MSAD group name must exist in Calypso.

- Reads the users from the same list of Calypso function groups created in MS Active Directory. Note that the group can be nested and users in the outer group are considered as belonging to the inner groups.
- Updates the users and groups in the Calypso database.
- Removes users that do not belong to any Calypso group.

If necessary, the Administrator can immediately lock out a Calypso user using the "Lock" checkbox on the User Access tab of the Access Permissions window. Note that users locked via this method cannot be unlocked by the SYNCLDAPUSER scheduled task as it can only unlock users who have been locked by the SYNCLDAPUSER task.

Connection information for the Active Directory LDAP service is set up as scheduled task attributes.



⊟ Task Attributes

LDAP URL	ldap://localhost:389
AD User name	calypso_admin
AD User Password	●●●●●●●
Enable SSL	false
Remaining Users in Calypso	calypso_user,admin
Support Authorization	false
Don't prepend window domain name	true
Lock instead of removing user	true
Java Naming Referral	ignore

- LDAP URL – Host and port number of Active Directory LDAP URL.

Example: `ldap://msad_host:389`

- AD User name – Administrator's Active Directory user name.
- AD User Password – Administrator's Active Directory password.
- Enable SSL – Is the LDAP over SSL enabled? Configuration is required to enable SSL.

  ▶ Please refer to *Calypso Installation and Upgrade System Guide* for details on configuring SSL.
- Remaining Users in Calypso – Comma separated list of any Calypso users not defined in Active Directory to NOT be deleted. Typically these are user templates and not actual Calypso users.
- Support Authorization – When true, users added through SYNCLDAPUSER must have their changes authorized, if authentication is enabled in the Data Server.
- Don’t prepend window domain name – When set to true, the system does not prepend the window domain name when syncing MSAD users to calypso users. Refer to Step 9 of SYNCLDAPUSER Logic, below.
- Lock instead of removing user – When set to true, users who are no longer in MSAD are locked instead of being removed.
- Java Naming Referral – The value passed to the "java.naming.referral" property. Set to follow to automatically follow any referrals. Set to ignore to ignore referrals. Set to throw to throw a ReferralException for each referral. Default is follow. Ignore should be used when updating referral entries, and/or if you receive “javax.naming.PartialResultException”.

SYNCLDAPUSER Logic

The steps below describe how the SYNCLDAPUSER scheduled task fetches user/group information from Active Directory.

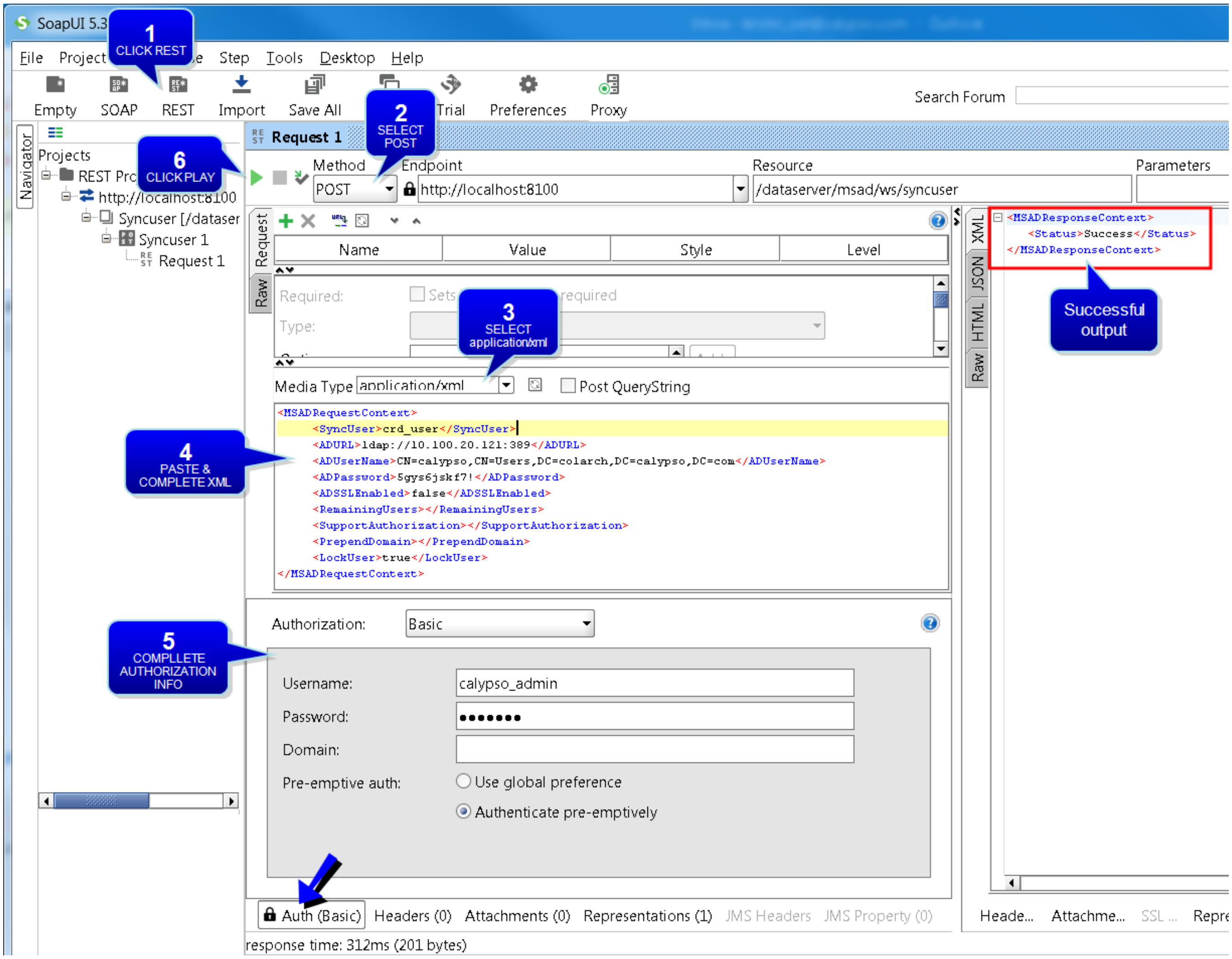
1. Collect a list of group names defined in "client/resources/sync_ldap_group_mapping.properties" or in the Calypso database if the file does not exist.
2. Use the LDAP URL to connect to Active Directory with baseDN as "" (i.e. connect to rootDSE).
3. Once connected to the rootDSE, get the values of two attributes, defaultNamingContext and schemaNamingContext.
4. With the schemaNamingContext attribute, construct groupSchemaDN by prefixing "CN=group," to the schemaNamingContext. All group objects defined in Active Directory will have their objectCategory attribute equal to groupSchemaDN.
5. Construct userSchemaDN by prefixing "CN=Person," to the schemaNamingContext. All user objects defined in Active Directory will have their objectCategory attribute equal to userSchemaDN.
6. Use the defaultNamingContext as the baseDN when fetching users or groups in Active Directory. Also, the sAMAccountName attribute on the user/group is used so make sure it is populated properly.
7. Fetch all Active Directory groups (objectCategory = groupSchemaDN as described in Step 4) with the name attribute in the group list collected in Step 1.
8. For each group fetched in Step 7, get its member attribute which contains a list of users/groups.
9. Fetch all users included in the member attribute of the groups from Step 7 or sub-group from Step 8.
   - **Don't prepend window domain name = FALSE:** The msDS-PrincipalName attribute is lower-cased and used as the username and displayName, and as the full_name in Calypso.
   - **Don't prepend window domain name = TRUE:** The sSAMAccout attribute is lower-cased and used as the username and displayName, and as the full_name in Calypso.

[NOTE: "msDS-PrincipalName" is a constructed property and not all LDAP browsers support constructed properties. This property contains a value in the form of "NetBIOS domain name"\"sAMAccountName"]

2.4.4 Synchronizing a Single User from MS Active Directory

Rather than running SYNCLDAPUSER to synchronize all users, you can sync a single user on demand using a web service which takes xml input. You can do this using a tool such as SoapUI or Postman. It is described here using SoapUI.

The web service API is: `public MSADResponseContext syncUser(MSADRequestContext)`


SoapUI 5.3
File Project ...e Step Tools Desktop Help
Empty SOAP REST Import Save All ... Trial Preferences Proxy
Search Forum
Navigator
Projects
REST Pro...
http://localhost:8100
Syncuser [/dataser...
Syncuser 1
Request 1
Request
Raw
Name Value Style Level
Required: Sets ... required
Type:
XML JSON HTML Raw
Auth (Basic) Headers (0) Attachments (0) Representations (1) JMS Headers JMS Property (0)
Heade... Attachme... SSL ... Repre...

1 CLICK REST

2 SELECT POST

3 SELECT application/xml

4 PASTE & COMPLETE XML

5 COMPLLETE AUTHORIZATION INFO

6 CLICK PLAY

Successful output

Method: POST
Endpoint: http://localhost:8100
Resource: /dataserver/msad/ws/syncuser
Parameters:

Media Type: application/xml
□ Post QueryString

```
<MSADRequestContext>
        <SyncUser>crd_user</SyncUser>
        <ADURL>ldap://10.100.20.121:389</ADURL>
        <ADUserName>CN=calypso,CN=Users,DC=colarch,DC=calypso,DC=com</ADUserName>
        <ADPassword>5gys6jskf7!</ADPassword>
        <ADSSLEnabled>false</ADSSLEnabled>
        <RemainingUsers></RemainingUsers>
        <SupportAuthorization></SupportAuthorization>
        <PrependDomain></PrependDomain>
        <LockUser>true</LockUser>
</MSADRequestContext>
```

Authorization: Basic

Username: calypso_admin
Password: •••••••
Domain:
Pre-emptive auth: ○ Use global preference
● Authenticate pre-emptively

```
<MSADResponseContext>
    <Status>Success</Status>
</MSADResponseContext>
```

response time: 312ms (201 bytes)

Step 1 – Click **REST**. You will be prompted to enter the web service URL.

Example: `http://localhost:8100/dataserver/msad/ws/syncuser` (where the port is the Data Server port)

Step 2 – Select POST as the method.

Step 3 – Select application/xml as the media type.

Step 4 – Paste the sample xml (given below), and complete the tags as needed. The conditional mandatory tags are only needed if they are not specified in the "calypsouser.properties" file.

- SyncUser – The user to be synchronized. Mandatory.
- ADURL – Host and port number of Active Directory LDAP URL. Conditional mandatory.

Example: `ldap://msad_host:389`

- ADUserName – Administrator's Active Directory user name. Conditional mandatory.
- ADPassword – Administrator's Active Directory password. Conditional mandatory.
- ADSSLEnabled – Is the LDAP over SSL enabled? Configuration is required to enable SSL.

  ▶ Please refer to *Calypso Installation and Upgrade System Guide* for details on configuring SSL.
- RemainingUsers – Comma separated list of any Calypso users not defined in Active Directory to NOT be deleted. Typically these are user templates and not actual Calypso users.
- SupportAuthorization – When true, users added through the web service must have their changes authorized, if authentication is enabled in the Data Server.
- PrependDomain – When set to true, the system prepends the window domain name when syncing MSAD users to calypso users.
  - **PrependDomain = TRUE:** The msDS-PrincipalName attribute is lower-cased and used as the username and displayName, and as the full_name in Calypso.
  - **PrependDomain = FALSE:** The sSAMAccout attribute is lower-cased and used as the username and displayName, and as the full_name in Calypso.

[NOTE: "msDS-PrincipalName" is a constructed property and not all LDAP browsers support constructed properties. This property contains a value in the form of "NetBIOS domain name"\"sAMAccountName"]

- LockUser – When set to true, users who are no longer in MSAD are locked instead of being removed.

Sample xml:

```
<MSADRequestContext>
<SyncUser></SyncUser>
<ADURL></ADURL>
<ADUserName></ADUserName>
<ADPassword></ADPassword>
<ADSSLEnabled></ADSSLEnabled>
<RemainingUsers></RemainingUsers>
<LockUser></LockUser>
<PrependDomain></PrependDomain>
<SupportAuthorization></SupportAuthorization>
</MSADRequestContext>
```

Step 5 – Select the Auth tab at the bottom. In the Authorization drop down, select Add New Authorization. You will be prompted to select the authorization type - Select Basic and click **OK**.

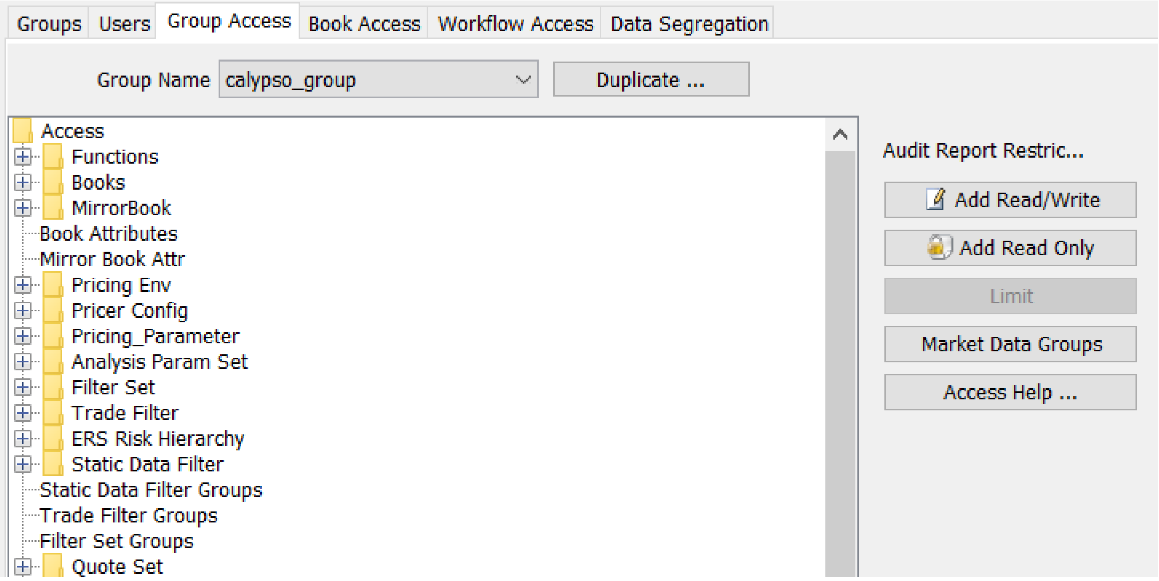
Step 6 – Click ▶. You should see a successful status in the xml output area on the right side.

2.5 Specifying Group Permissions

Select the Group Access panel to specify group permissions.

A group of users can be granted permission to execute certain applications and individual functions, and can be granted to access certain data. For example, a group can be granted read/write access on a given book, but if the group does not have the ModifyBook function, the users of the group will not be able to modify the book.

Under the Access label, the Application Name and Functions entities allow granting permission to run applications and execute individual functions. The other entities allow granting access to data.



Group Name: calypso_group

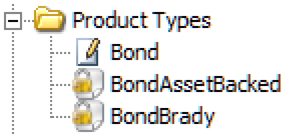
- Select a group from the Group Name field.
- You can click **Duplicate** to copy the permissions of another group. You will be prompted to select a group.
- Select an entity from the Access list.

  Once you have selected an entity, click **Add Read/Write** to add read/write permissions to certain data of that entity, and click **Add Read Only** to add read-only permissions to other data of that entity, as applicable.

  You will be prompted to select data from the selected entity. The entities are described below.

  Note that data that are not granted access will not appear in the environment of the user.

  Once you have selected entity data, you can double-click the entity to view the associated data as shown below.



  The lock icon identifies read-only data, and the pencil icon identifies read-write data.

- There is no local **Save** button, so it is recommended to click the general **Save** button before proceeding to another panel.
- Click **Access Help** for information on the access permission requirements of each application.
- Click **Function Help** for description of individual functions.
- Note that the **Limit** button only applies to quotes sets.

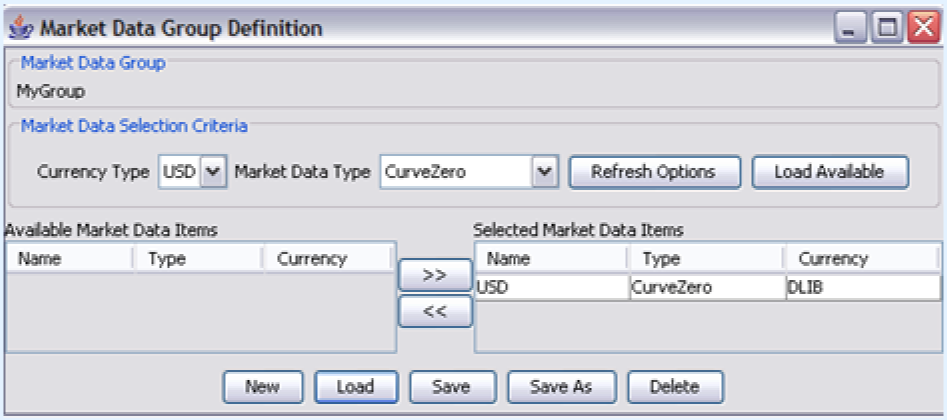
Entities	Description
Functions	Allows granting permission for executing individual application functions. You can select _ALL_ to grant permission for executing all functions. Functions can only be granted read/write permission since it is the function itself that dictates what it controls. You can click **Access Help** for details on these functions.
Books	Allows granting read/write and read-only access to books. You can select _ANY_ to grant access to any book. Note that Book access is also controlled by the Processing Org field in the User panel, and the Book Access panel. Books that have read/write permission can be used to enter trades, and their definition can be modified in the Book window. Books that have read-only permission cannot be used to enter trades (the trades that belong to these books can only be viewed), and their definition cannot be modified.
MirrorBook	Allows granting read/write and read-only access to books used as mirror books. You can select _ANY_ to grant access to any book. Note that Book access is also controlled by the Processing Org field in the Users panel, and the Book Access panel. Books that have read/write permission can be used to enter mirror trades, and their definition can be modified in the Book window. Books that have read-only permission cannot be used to enter mirror trades (the trades that belong to these books can only be viewed), and their definition cannot be modified.
Book Attributes	Allows granting read/write and read-only access to books based on book attributes. Books for which the book attributes have read/write permission can be displayed and modified. Books for which the book attributes have read-only permission cannot be displayed and modified. Example: If the book attribute ABC exists with possible value "yes" and "no" then in the access permissions if you set the Book Attributes = "ABC.yes", you give the ability to this group of users to have access to all the books which have the book attribute ABC set to "yes". If a book has no value or value = "no" for the book attribute ABC then it doesn't belong to the allowed group of books.
Mirror Book Attr	Allows granting read/write and read-only access to mirror book attributes. Mirror book attributes that have read/write permission can be displayed and modified. Mirror book attributes that have read-only permission cannot be displayed and modified.
Pricing Env	Allows granting read/write and read-only access to pricing environments. You can select _ALL_ to grant access to all pricing environments.

Entities	Description
	Pricing environments that have read/write permission can be used to price trades, and their definition can be modified in the Pricing Env window. Pricing environments that have read-only permission can be used to price trades, and their definition cannot be modified.
Pricer Config	Allows granting read/write and read-only access to pricer configurations. You can select _ALL_ to grant access to all pricer configurations. Pricer configurations that have read/write permission can be used in pricing environments, and their definition can be modified in the Pricer Configuration window. Pricer configurations that have read-only permission can be used in pricing environments, and their definition cannot be modified.
Pricing_Parameter	Allows granting read/write and read-only access to pricing parameter sets. You can select _ALL_ to grant access to all pricing parameter sets. Pricing parameter sets that have read/write permission can be used in pricing environments, and their definition can be modified in the Pricing Params window. Pricing parameter sets that have read-only permission can be used in pricing environments, and their definition cannot be modified.
Analysis Param Set	Allows granting read/write and read-only access to analysis parameter sets. You can select _ALL_ to grant access to all analysis parameter sets. Analysis parameter sets that have read/write permission can be used to run risk reports, and their definition can be modified in the Analysis Param Viewer window / Analysis Designer window. Analysis parameter sets that have read-only permission can be used to run risk reports, and their definition cannot be modified.
Filter Set	Allows granting read/write and read-only access to filter sets. You can select _ALL_ to grant access to all filter sets. Filter sets that have read/write permission can be used for loading trades, and their definition can be modified in the Filter Set window. Filter sets that have read-only permission can be used for loading trades, and their definition cannot be modified.
Trade Filter	Allows granting read/write and read-only access to trade filters. You can select _ALL_ to grant access to all trade filters. Trade filters that have read/write permission can be used for loading trades, and their definition can be modified in the Trade Filter window. Trade filters that have read-only permission can be used for loading trades, and their definition cannot be modified.
Static Data Filter	Allows granting read/write and read-only access to static data filters. You can select _ALL_ to grant access to all static data filters.

Entities	Description
	Static data filters that have read/write permission can be used for loading data, and their definition can be modified in the Static Data Filter window. Static data filters that have read-only permission can be used for loading data, and their definition cannot be modified.
Static Data Filter Groups	Allows granting read/write and read-only access to static data filter groups. You can select _ALL_ to grant access to all static data filter groups. Static data filter groups that have read/write permission allow the corresponding static data filters to be used from the windows belonging to the groups, and the definition of the corresponding static data filters can be modified. Static data filter groups that have read-only permission allow the corresponding static data filters to be used from the windows belonging to the groups, and the definition of the corresponding static data filters cannot be modified.
Trade Filter Groups	Allows granting read/write and read-only access to trade filter groups. You can select _ ALL_ to grant access to all trade filter groups. Trade filter groups that have read/write permission allow the corresponding trade filters to be used for loading trades, and the definition of the corresponding trade filters can be modified. Trade filter groups that have read-only permission allow the corresponding trade filters to be used for loading trades, and the definition of the corresponding trade filters cannot be modified.
Filter Set Groups	Allows granting read/write and read-only access to filter set groups. You can select _ ALL_ to grant access to all filter set groups. Filter set groups that have read/write permission allow the corresponding filter sets to be used for loading trades, and the definition of the corresponding filter sets can be modified. Filter set groups that have read-only permission allow the corresponding filter sets to be used for loading trades, and the definition of the corresponding filter sets cannot be modified.
Quote Set	Allows granting read/write and read-only access to quote sets. You can select _ALL_ to grant access to all quote sets. It is also possible to limit read/write access to subsets of quotes within a Quote Set. ▶ See Group Access Permission for Subsets of Quotes for details. Quote sets that have read/write permission can be used in pricing environments, and their definition can be modified in the Quote Set window. Quote sets that have read-only permission can be used in pricing environments, and their definition cannot be modified.
Risk Config	Allows granting read/write and read-only access to risk configurations. You can select _

Entities	Description
	ALL_ to grant access to all risk configurations. Risk configurations that have read/write permission can be used to run risk reports, and their definition can be modified in the Risk Analysis window. Risk configurations that have read-only permission can be used to run risk reports, and their definition cannot be modified.
Scheduled Task	Allows granting read/write and read-only access to scheduled tasks. You can select _ ALL_ to grant access to all scheduled tasks. Scheduled tasks that have read/write permission can be executed, and their definition can be modified in the Scheduled Tasks window. Scheduled tasks that have read-only permission can be executed, and their definition cannot be modified.
Book Hierarchy	Allows granting read/write and read-only access to book hierarchies. You can select _ ALL_ to grant access to all book hierarchies. Book hierarchies that have read/write permission can be used for loading trades, and their definition can be modified in the Book Hierarchy window. Book hierarchies that have read-only permission can be used for loading trades, and their definition cannot be modified.
Dispatcher Config	Allows granting read/write and read-only access to dispatcher configurations. You can select _ALL_ to grant access to all dispatcher configurations. Dispatcher configurations that have read/write permission can be used to run the dispatcher, and their definition can be modified in the Dispatcher Config window. Dispatcher configurations that have read-only permission can be used to run the dispatcher, and their definition cannot be modified.
Calculation Server Config	Allows granting read/write and read-only access to Calculation Server configurations (Configuration > System > Calculation Server). You can select _ALL_ to grant access to all Calculation Server configurations. Calculation Server configurations that have read/write permission can be used to run risk on demand, and their definition can be modified in the Calculation Server Config window. Calculation Server configurations that have read-only permission can be used to run risk on demand, and their definition cannot be modified.
Presentation Config	Allows granting read/write and read-only access to presentation server configurations (Configuration > System > Presentation Server). You can select _ALL_ to grant access to all presentation server configurations. Presentation server configurations that have read/write permission can be used to run presentation servers, and their definition can be modified in the Presentation Server Configuration window. Presentation server configurations that have read-only permission can be used to run

Entities	Description
	presentation servers, and their definition cannot be modified.
MktData Server Config	Allows granting read/write and read-only access to Market Data Server configurations. You can select _ALL_ to grant access to all Market Data Server configurations. Market Data Server configurations that have read/write permission can be used to run the Market Data Server, and their definition can be modified in the MktData Server Config window. Market Data Server configurations that have read-only permission can be used to run the Market Data Server, and their definition cannot be modified.
Risk OnDemand Config	Allows granting read/write and read-only access to calculation servers (Configuration > Reporting & Risk > Calculation Server). You can select _ALL_ to grant access to all calculation servers. Calculation servers that have read/write permission can be used to run risk reports, and their setup can be modified in the Calculation Server Setup window. Calculation servers that have read-only permission can be used to run risk reports, and their definition cannot be modified.
Risk Presenter Config	Allows granting read/write and read-only access to presentation servers (Configuration > Reporting & Risk > Presentation Server). You can select _ALL_ to grant access to all presentation servers. Presentation servers that have read/write permission can be used to run risk reports, and their setup can be modified in the Presentation Server Setup window. Presentation servers that have read-only permission can be used to run risk reports, and their definition cannot be modified.
Application Name	Allows granting permission for executing applications. You can select _ALL_ to grant permission for executing all applications, or add applications individually. Applications names are defined in the domain "applicationName".
Market Data Types	Allows granting read/write and read-only access to market data of specified types that do not belong to a pricer configuration, or to market data of specified types that belong to a pricer configuration if the environment property **DISABLE_MDI_PC_PERMISSION_INHERITANCE** is set to true. Otherwise, the market data types will follow the permissions of the pricer configuration. Market data of specified types that have read/write permission can be used in pricing, and their definition can be modified. Market data of specified types that have read-only permission can be used in pricing, and their definition cannot be modified.
Market Data Groups	Allows granting read/write and read-only access to market data of specified groups that do not belong to a pricer configuration, or to market data of specified groups that belong to a pricer configuration if the environment property **DISABLE_MDI_PC_PERMISSION_**

Entities	Description
	INHERITANCE is set to true. Otherwise, the market data groups will follow the permissions of the pricer configuration. Market data of specified groups that have read/write permission can be used in pricing, and their definition can be modified. Market data of specified groups that have read-only permission can be used in pricing, and their definition cannot be modified. Market data groups are created in the Groups panel by clicking on the **Market Data Groups** button.  Market Data Group Definition Market Data Group: MyGroup Market Data Selection Criteria: Currency Type USD, Market Data Type CurveZero Available Market Data Items: Name, Type, Currency Selected Market Data Items: Name USD, Type CurveZero, Currency DLIB Refresh Options Load Available >> << New Load Save Save As Delete » Select the market data you want to add to a group, and add them using the right arrow. Then click **Save**, you will be prompted to enter a group name.
Product Templates	Allows granting read/write and read-only access to product templates. You can select _ALL_ to grant access to all product templates. Product templates that have read/write permission can be used in trades, and their definition can be modified. Product templates that have read-only permission can be used in trades, and their definition cannot be modified.
Report Templates	Allows granting read/write and read-only access to report templates. You can select _ALL_ to grant access to all report templates. Report templates that have read/write permission can be used in reports, and their definition can be modified. Report templates that have read-only permission can be used in reports, and their definition cannot be modified. Note that private report templates do not appear here. They can only be used and modified by the user who created them.
Generic Comment Type	Allows granting read/write and read-only access to generic comment types. You can select _ALL_ to grant access to all generic comment types.

Entities	Description
	Generic comment types that have read/write permission can be viewed on objects and in reports, and they can be added to objects. Generic comment types that have read-only permission can be viewed on objects and in reports, and they cannot be added to objects.
Typed Legs	Allows granting read/write and read-only access to exotic typed legs. You can select _ ALL_ to grant access to all exotic typed legs. Exotic typed legs that have read/write permission can be used to capture trades, and their definition can be modified in the eXSP Type Creator window. Exotic typed legs that have read-only permission can be used to capture trades, and their definition cannot be modified.
HyperSurface Generators	Allows granting read/write and read-only access to hypersurface generators. You can select _ALL_ to grant access to all hypersurface generators. Hypersurface generators that have read/write permission can be used to generate hypersurfaces, and their definition can be modified. Hypersurface generators that have read-only permission can be used to generate hypersurfaces, and their definition cannot be modified.
Product Types	Allows granting read/write and read-only access to product types. You can select _ALL_ to grant access to all product types. Note that product types are also controlled by the Book Access panel. Product types that have read/write permission can be used to enter trades. Product types that have read-only permission cannot be used to enter trades (the trades on these product types can only be viewed).
Products StaticData	Allows granting read/write and read-only access to individual products based on a static data filter. The static data filter must only contain product criteria. You can select _ALL_ to grant access to all products. Products that have read/write permission can be modified. Products that have read-only permission cannot be modified (they can only be viewed).
Products Trading	Allows granting read/write and read-only access to individual products for trading based on a static data filter. The static data filter must only contain product criteria. You can select _ALL_ to grant access to all products. Note that you also need access to the corresponding product types. Also note that if a user belongs to multiple groups, and one of the groups uses Products Trading permissions, then the other groups the user belongs to must use Products Trading permissions as well. Products that have read/write permission can be used to enter trades. Products that have read-only permission cannot be used to enter trades (the trades on

Entities	Description
	these products can only be viewed).
Action Event Type	Allows granting access to performing trade lifecycle actions. You can select _ALL_ to grant access to all event types. Event types that have either read/write or read-only permissions are able to be performed by this group of users.
Benchmark Family	Allows granting read/write and read-only access to benchmark families. You can select _ALL_ to grant access to all benchmark families. Benchmark families that have read/write permission can be assigned to benchmarks. The benchmarks belonging to these families can be used, and their definition can be modified. Benchmark families that have read-only permission can be assigned to benchmarks. The benchmarks belonging to these families can be used, and their definition cannot be modified.
Funds	Allows granting read/write and read-only access to funds and mandates. You can select _ALL_ to grant access to all funds and mandates. Funds and mandates that have read/write permission can be associated with strategies, and their definition can be modified in the Fund or Mandate windows. Funds or mandates that have read-only permission cannot be associated with strategies, and their definition cannot be modified.
Strategy	Allows granting read/write and read-only access to strategies. You can select _ALL_ to grant access to all strategies. Strategies that have read/write permission can be used to enter trades, and their definition can be modified in the Strategy window. Strategies that have read-only permission cannot be used to enter trades (the trades that belong to these strategies can only be viewed), and their definition cannot be modified.
Custom Portfolios	Allows granting read/write and read-only access to custom portfolios. You can select _ALL_ to grant access to all custom portfolios. Custom portfolios that have read/write permission are displayed in the Portfolio Hierarchy window and in the PWS "Portfolios" drop down menu, and their definition can be modified in the Portfolio Hierarchy window. Custom portfolios that have read-only permission are displayed in the Portfolio Hierarchy window and in the PWS "Portfolios" drop down menu, and their definition cannot be modified.
Portfolio Hierarchies	Allows granting read/write and read-only access to portfolio hierarchies. You can select _ALL_ to grant access to all portfolio hierarchies. There is no distinction between read/write and read-only access for portfolio hierarchies.

Entities	Description
	Portfolio hierarchies that have read/write or read-only permission are displayed in the Portfolio Hierarchy window and in the PWS 'Portfolios' drop down menu.
Report Hierarchies	Allows granting read/write and read-only access to groups. You can select _ALL_ to grant access to all groups. Group Access permissions on specific Report Hierarchies must be added in the **Access Permissions > Group Access** window. When adding Read/Write or Read Only Access, existing reports and report groups must be selectable in the dedicated selection dialog.
Scenario Market Data	Allows granting read/write and read-only access to scenario market data sets. You can select _ALL_ to grant access to all market data sets. Market data sets that have read/write permission can be used to run scenarios, and their definition can be modified in the Scenario Editor window. Market data sets that have read-only permission can be used to run scenarios, and their definition cannot be modified.
Scenario Rule	Allows granting read/write and read-only access to scenario rules. You can select _ALL_ to grant access to all scenario rules. Scenario rules that have read/write permission can be used to run scenarios, and their definition can be modified in the Scenario Editor window. Scenario rules that have read-only permission can be used to run scenarios, and their definition cannot be modified.
Audit Report Restriction	Allows restricting access to audit report data. Audit report restrictions that have read/write permission are not restricted from viewing. Note that unless an audit report data type is expressly restricted by setting read-only permission on it, it will be viewable in audit reports. Audit report restrictions that have read-only permission restrict viewing audit report data of specified types. Selecting only _ALL_ will NOT restrict any data types - they must be selected individually. You also need to add the data types (audit classes) you wish to restrict to the *auditReportRestrictable* domain. ▶ See Data Auditing for details.
Feed Config	Allows granting read/write and read-only access to feed address mapping configurations. You can select _ALL_ to grant access to all feed address mapping configurations. Feed address mapping configurations that have read/write permission can be viewed, and their definition can be modified in the Feed Address window. Feed address mapping configurations that have read-only permission can be viewed, and their definition cannot be modified.
Hedge Accounting	Allows granting read/write and read-only access to hedge accounting standards. You

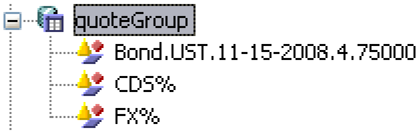
Entities	Description
Standard	can select _ALL_ to grant access to all hedge accounting standards. Hedge accounting standards that have read/write permission can be used in hedge strategy definition, and hedge strategies using them can be modified. Hedge accounting standards that have read-only permission cannot be used in hedge strategy definition, and hedge strategies using them cannot be modified (they can only be viewed).
Data Segregation Apps	For an implementation that includes eSelfService, the Data Segregation folder contains only a single entry for CalypsoBusinessServices. Data Segregation has no function for standard Calypso installations and will typically have no entries.
Rating Agencies	Allows granting read/write and read-only access to rating agencies. You can select _ ALL_ to grant access to all rating agencies. Rating agencies that have read/write permission can be used in legal entity credit ratings, and credit ratings for the corresponding agencies can be modified. Rating agencies that have read-only permission can be used in legal entity credit ratings, and credit ratings for the corresponding agencies cannot be modified.
Task Station Tabs	Allows granting read/write and read-only access to Task Station tabs. You can select _ ALL_ to grant access to all Task Station tabs. Task Station tabs that have read/write permission can be accessed, and their configuration can be modified in the Task Station Tabs panel. Task Station tabs that have read-only permission can be accessed, and their configuration cannot be modified.
Task Station Filters	Allows granting read/write and read-only access to Task Station enrichment filters. You can select _ALL_ to grant access to all Task Station enrichment filters. Task Station enrichment filters that have read/write permission can be used to filter tasks, and their definition can be modified in the Task Enrichment Filters panel. Task Station enrichment filters that have read-only permission cannot be used to filter tasks, and their definition cannot be modified.
Report Browser Configs	Allows granting read/write and read-only access to Report Browser configurations. You can select _ALL_ to grant access to all Report Browser configurations. Report Browser configurations that have read/write permission can be used to view reports, and their definition can be modified in the Report Browser. Report Browser configurations that have read-only permission can be used to view reports, and their definition cannot be modified.
OptimizationConfiguration	Allows granting read/write and read-only access to collateral optimization configurations. You can select _ANY_ to grant access to any optimization configuration. Optimization configurations that have read/write permission can be viewed, and their definition can be modified in the Collateral Optimization Configuration window.

Entities	Description
	Optimization configurations that have read-only permission can be viewed, and their definition cannot be modified.
TargetConfiguration	Allows granting read/write and read-only access to collateral target configurations. You can select _ANY_ to grant access to any target configuration. Target configurations that have read/write permission can be viewed, and their definition can be modified in the Target Configuration window. Target configurations that have read-only permission can be viewed, and their definition cannot be modified.

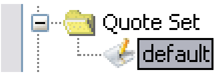
Group Access Permission for Subsets of Quotes

For quote sets, you can further define permissions on subsets of quotes. For example, a given user group could set FX quotes, while another user group could set bond quotes. Each group of quote is identified using a wild card mechanism. So FX quotes would be identified as FX% (all quotes starting with FX).

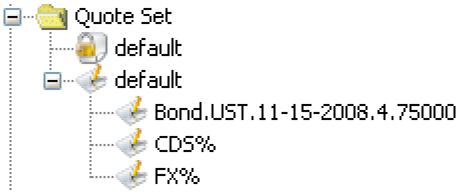
» You first need to define the groups of quotes, or individual quotes in the *quoteGroup* domain.



» Then, in the Group Access panel, select the Quote Set node, and click **Add Read/Write** or **Add Read Only** to define permissions on quote sets. You will be prompted to select quote sets.



» Finally, select the quote set and click **Limit**. You will be able to select quote groups as applicable.



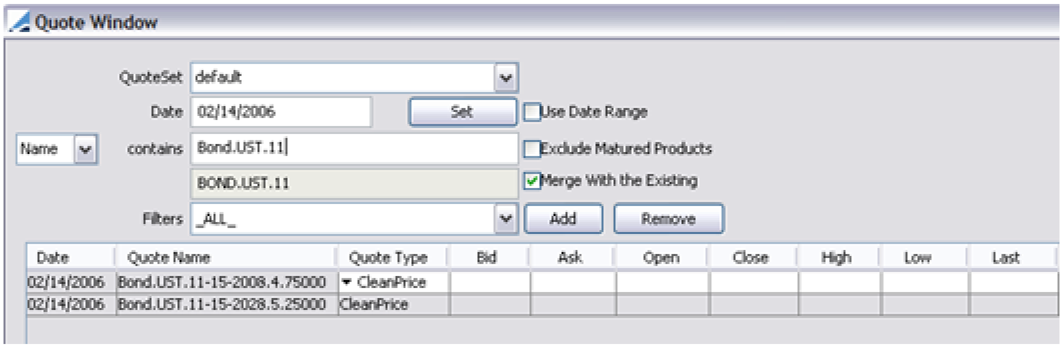
Sample Restrictions

Read or write permission is per quote set, i.e. you can have permission to write to a quote set or parts of it by specifying the wildcard.

- Read/write access on Quote Set A and FX% means you can save only FX quotes in Quote Set A.
- Read-only access on Quote Set B means you can only view quotes in Quote Set B. You cannot modify any quote.

- A typical case might be that a user can read all quotes in Quote Set C but can only modify a subset of them. So the setup would be read-only access on Quote Set C and read/write access on Quote Set C with limits on groups of quotes.

In the Quote window (**Calypso Navigator > Market Data > Market Quotes > Quotes**, menu action `marketdata.QuoteJFrame`) read/write rows are displayed with a white background, while read-only rows are grayed out and cannot be modified.


Quote Window

QuoteSet: default
Date: 02/14/2006
Name contains: Bond.UST.11
BOND.UST.11
Filters: _ALL_
☐ Use Date Range
☐ Exclude Matured Products
☑ Merge With the Existing

Date	Quote Name	Quote Type	Bid	Ask	Open	Close	High	Low	Last
02/14/2006	Bond.UST.11-15-2008.4.75000	CleanPrice							
02/14/2006	Bond.UST.11-15-2028.5.25000	CleanPrice							

Automatic Propagation of Access Permissions

When Static Data Filters, Trade Filters and Filter Sets are created, they are automatically granted read/write permissions for all the user groups to which the user who created them belongs under the Access entities: Static Data Filters, Trade Filters and Filter Sets.

If you want to use the following Access entities instead: Static Data Filter Groups, Trade Filer Groups and Filter Set Groups, you may disable that automatic propagation to individual filters by removing the corresponding entities from domain "propagateFilterAccessPermission":

- FilterSet
- StaticDataFilter
- TradeFilter

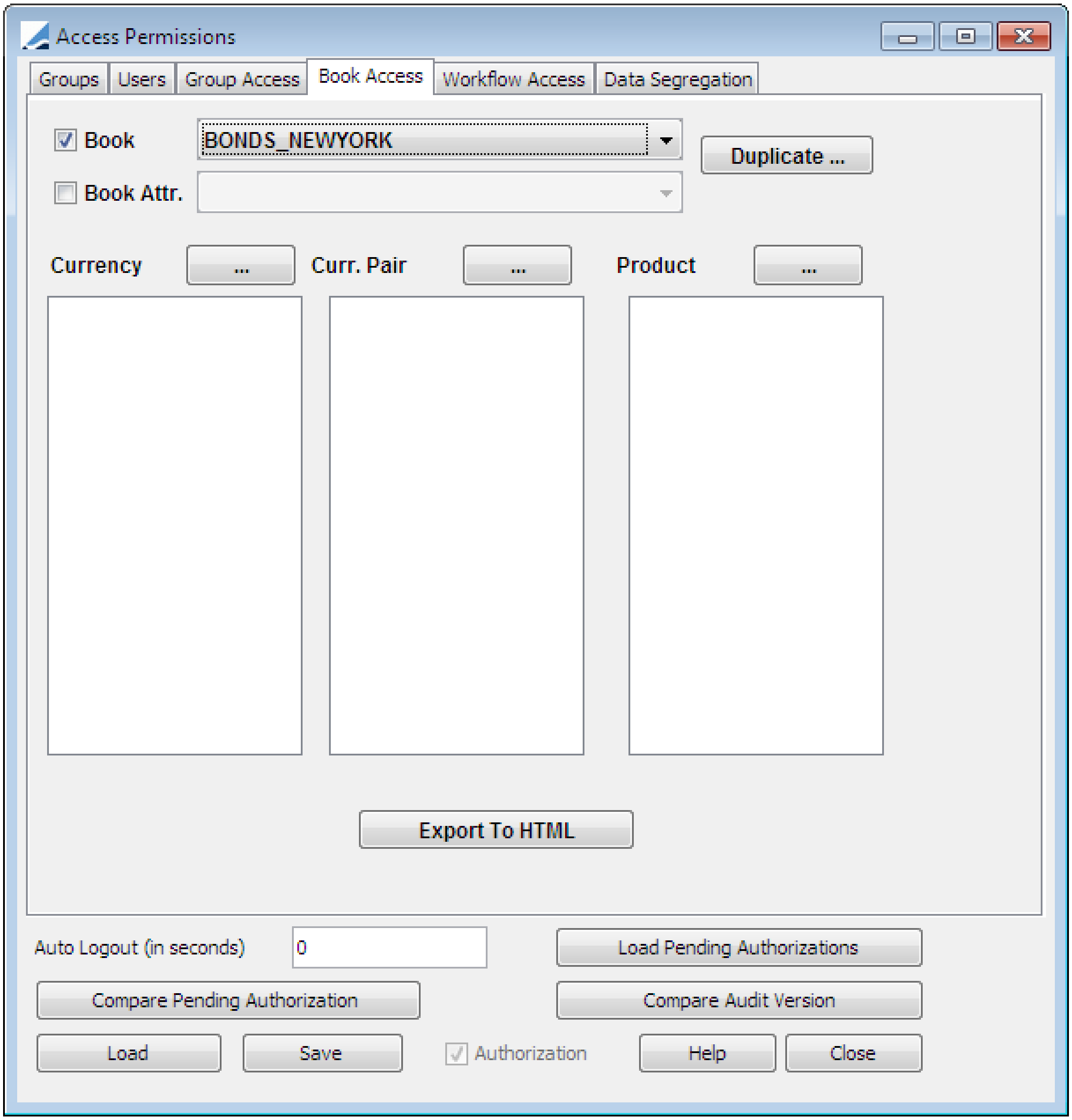
When books are created, they are automatically granted read/write permissions for all the user groups to which the user who created them belongs under the Access entity: Books unless:

- The user group has access to _ANY_ books (as access is already granted to all books)
- The user group does not have access to any book. *In this case, if you want the access permissions to be propagated for new books, you need to give the user group access to at least one book*.

2.6 Specifying Book Permissions

Select the Book Access panel to specify book permissions as applicable. For a given book, you can specify the currencies, currency pairs and products that can be traded in that book.

The book permissions apply regardless of the user. However, using the Group Access panel, you can specify the books that a group of users has access to.



☑ Book: BONDS_NEWYORK

□ Book Attr.:

Auto Logout (in seconds): 0

☑ Authorization

- Select a book from the Book field.
- You can click **Duplicate** to copy the permissions of another book. You will be prompted to select a book.
- Click the **...** button next to the Currency field to select the currencies that can be traded in the selected book.
- Click the **...** button next to the Curr. Pair field to select the currency pairs that can be traded in the selected book.
- Click the **...** button next to the Product field to select the products that can be traded in the selected book.

- There is no local save button, so it is recommended to click the general **Save** button before proceeding to another panel.

  Provided a group of users has read/write access to the selected book, the users will be restricted to enter trades in the specified currencies and currency pairs, and for the specified products.

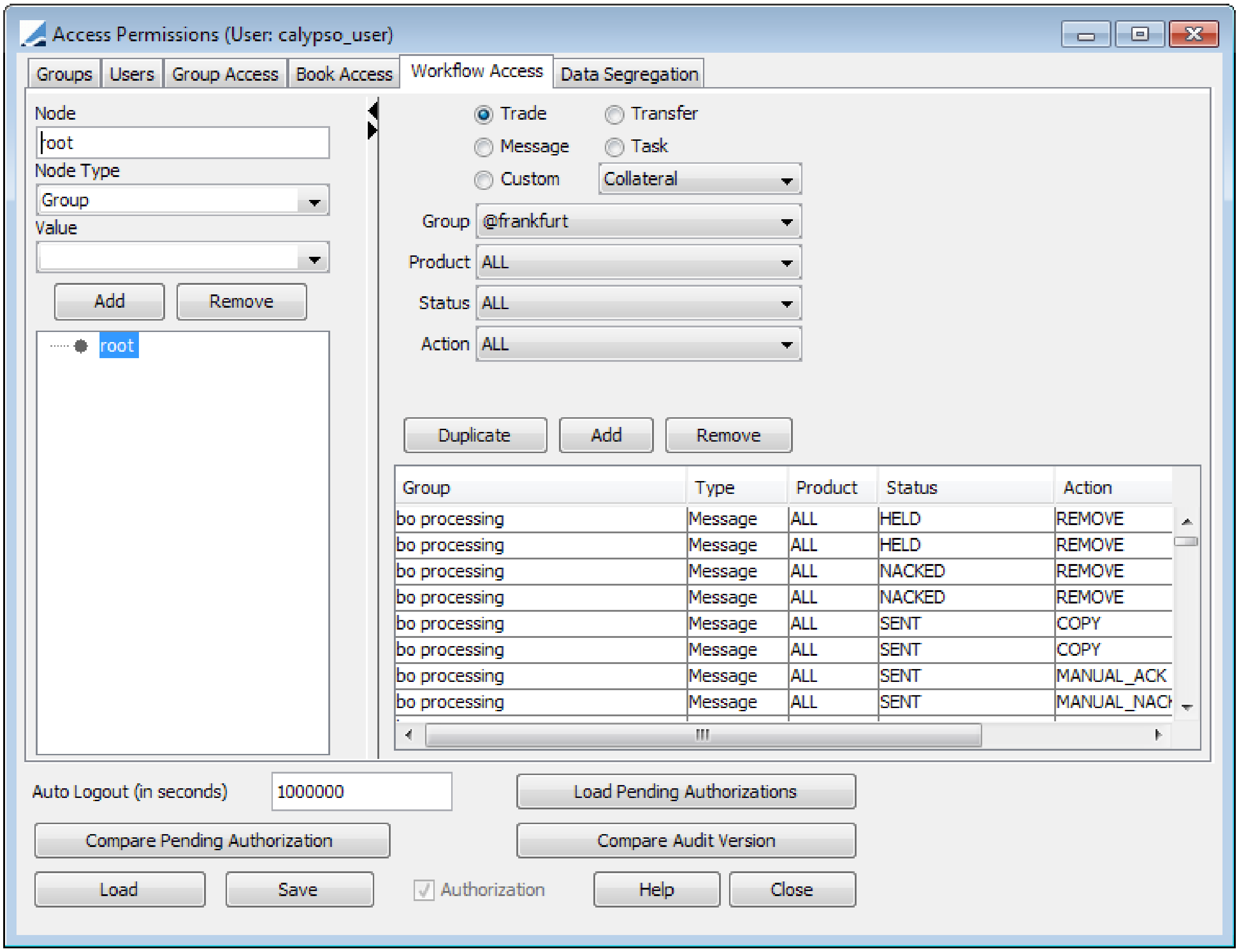
- Click **Export to HTML** to print the book permissions to an HTML file.

2.7 Specifying Workflow Permissions

Select the Workflow Access panel to specify what actions the users can apply to trades, transfers, messages and tasks, based on the products that are being processed, provided they are in the specified status.

For example, a given user can enter a trade in pending status, another user can verify the trade, and yet another user can process the payment.

Note that there must be a workflow transition corresponding to each status and action selected here. You can view workflow transitions using **Calypso Navigator > Configuration > Workflow > Workflow Graph** (menu action `refdata.WorkflowGraphJFrame`).



Node: root

Node Type: Group

Value:

root

● Trade ○ Transfer
○ Message ○ Task
○ Custom Collateral

Group: @frankfurt

Product: ALL

Status: ALL

Action: ALL

Group	Type	Product	Status	Action
bo processing	Message	ALL	HELD	REMOVE
bo processing	Message	ALL	HELD	REMOVE
bo processing	Message	ALL	NACKED	REMOVE
bo processing	Message	ALL	NACKED	REMOVE
bo processing	Message	ALL	SENT	COPY
bo processing	Message	ALL	SENT	COPY
bo processing	Message	ALL	SENT	MANUAL_ACK
bo processing	Message	ALL	SENT	MANUAL_NAC

Auto Logout (in seconds): 1000000

» Use the right-hand side area to add, remove, and duplicate restrictions on actions.

Select the entity for which you want to specify actions using the radio buttons: Trade, Transfer, Message or Task.

Select a group of users from the Group field, a status from the Status field, a product from the Product field, and an action from the Action field.

For a message, you can also select a message type.

You can select ALL for status, product, action, and message type, as applicable.

Then click **Add** to add the permission. The permission will appear in the table at the bottom of the window. You can click any column header to sort the table on the corresponding column.

There is no local save button, so it is recommended to click the general **Save** button before proceeding to another panel.

» Use the left-hand side area to browse the existing restrictions. If you click the root label, all restrictions will be displayed on the right-hand side. You can setup multiple hierarchies based on any of the following elements: Group, AccessType, Product, Status, Action, MessageType.

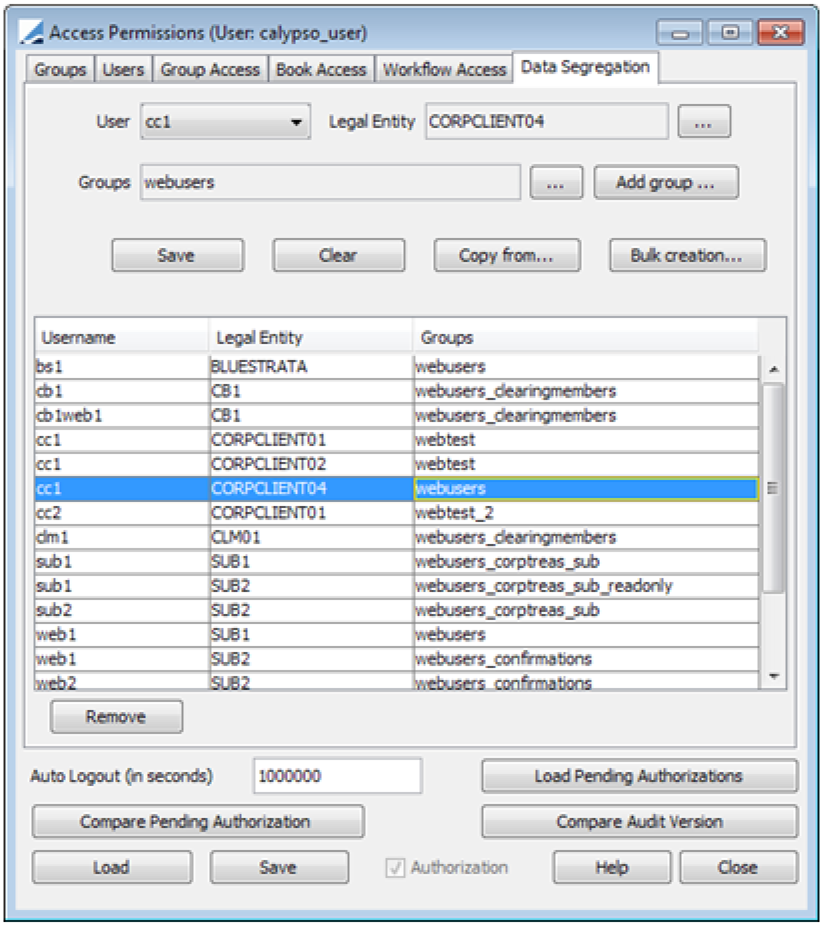
Select a node, then select a node type and click **Add** to add a new level.

When you select a node, the corresponding restrictions will be displayed in the right-hand side.

2.8 Data Segregation

Use the Data Segregation tab on the Access Permissions window to associate eSelfService users with the proper Legal Entity and Groups. The Data Segregation tab has no function for standard Calypso installations.

[NOTE: Only Groups having permissions set on the Data Segregation Apps node of the Group Access tab are available for selection]



User: cc1

Legal Entity: CORPCLIENT04

Groups: webusers

Username	Legal Entity	Groups
bs1	BLUESTRATA	webusers
cb1	CB1	webusers_clearingmembers
cb1web1	CB1	webusers_clearingmembers
cc1	CORPCLIENT01	webtest
cc1	CORPCLIENT02	webtest
cc1	CORPCLIENT04	webusers
cc2	CORPCLIENT01	webtest_2
clm1	CLM01	webusers_clearingmembers
sub1	SUB1	webusers_corptreas_sub
sub1	SUB2	webusers_corptreas_sub_readonly
sub2	SUB2	webusers_corptreas_sub
web1	SUB1	webusers
web1	SUB2	webusers_confirmations
web2	SUB2	webusers_confirmations

Auto Logout (in seconds): 1000000

- Select a User, Legal Entity, and Group.
- Click **Save** (below the Groups field) to create the association.

  Note that if the Authorization mode is enabled, an authorized user must approve your entry.

To associate a particular user or group with multiple Legal Entities, do so one record at a time by repeating Steps 1 and 2 as necessary.

Click **Save** on the bottom of the Access Permissions window to store the associations in the database.

Note that if the Authorization mode is enabled, an authorized user must approve your entry.

▶ Refer to the *Calypso eSelfService Installation and Configuration Guide* for further information on configuring eSelfService.

3. User Permission and Activity Reports

The following reports detailing user permissions and activity are available:

- ActiveUser
- LastLogin
- UserAccessPermission
- UserAudit
- WorkflowAccess

Access to these reports is through a modified Calypso Navigator Reports menu. Use the following procedure to add reports to Navigator:

» Launch the Main Entry Customizer (**Calypso Navigator > Utilities > Main Entry Customizer**).

» Select the appropriate user from the drop-down selector and click **Load**.

» Expand the Reports item (click ⊞).

» Click Reports once to highlight it. Then, for each report item add an entry:

Name – The report name

Action – `reporting.ReportWindow$ReportName#TemplateName`

Where *ReportName* is the report name, and *TemplateName* is the template name (optional).

» Click **Insert**.

» After adding the desired reports, click **Save** to store your changes in the database.

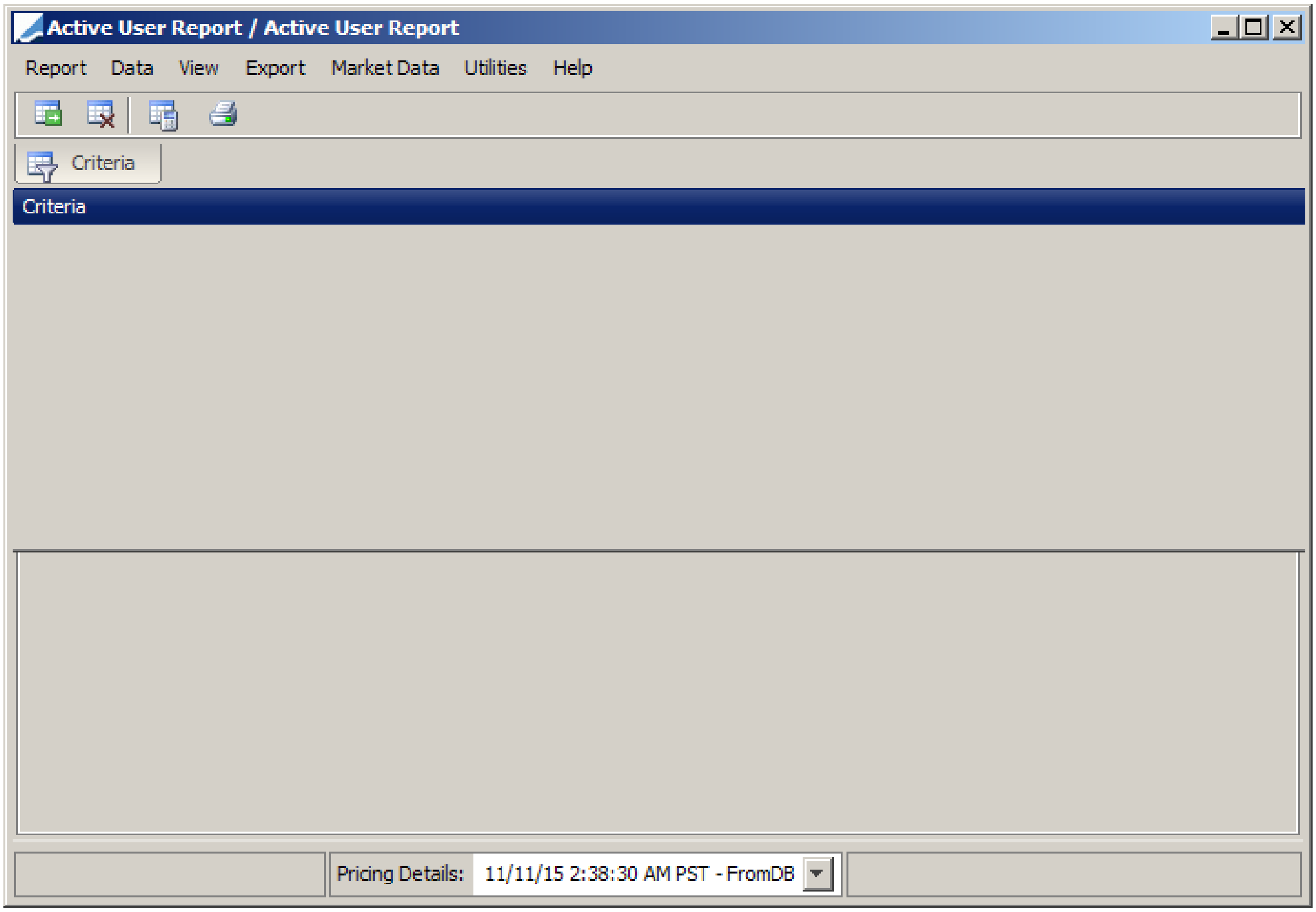
» Click **Close** to exit the Main Entry Customizer.

Restart Calypso Navigator to access the reports from the Reports menu.

3.1 Active User

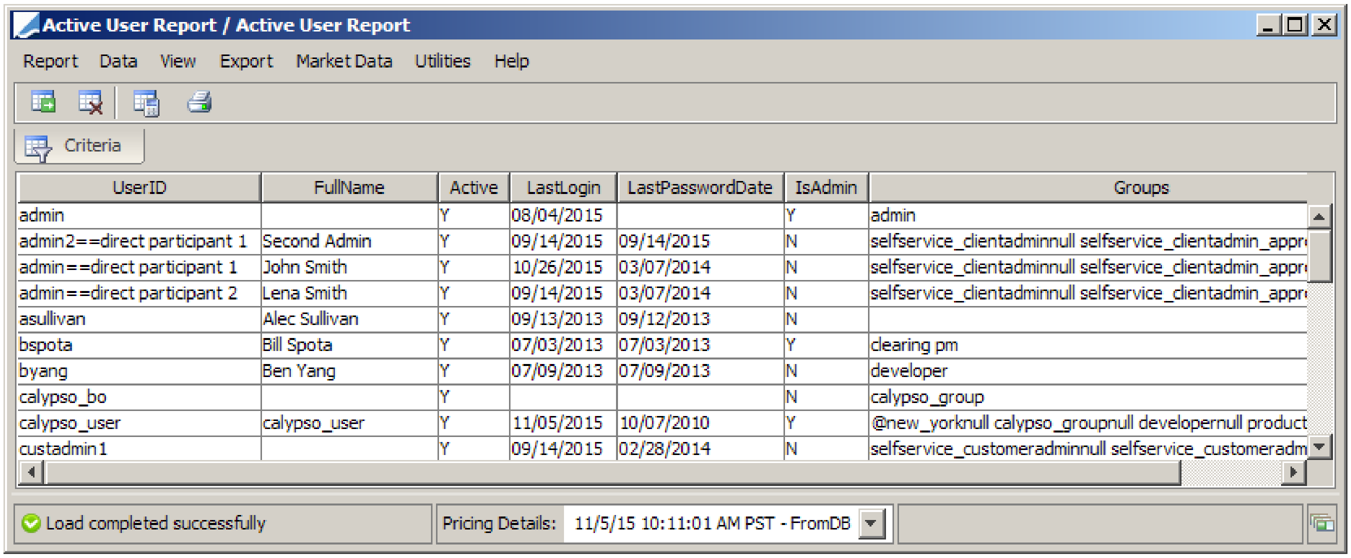
The Active User Report provides the following details for active users:

- User ID – The user's Calypso User ID.
- Full Name – The user's full name.
- Active – Is the user active (i.e., not locked or disabled)?
- Last Login – Date of the last user login.
- Last Password Date – Date of the last password change.
- Is Admin – Does the user have Admin privileges?
- Groups – A list of group memberships.



Pricing Details: 11/11/15 2:38:30 AM PST - FromDB

Active User Report



UserID	FullName	Active	LastLogin	LastPasswordDate	IsAdmin	Groups
admin		Y	08/04/2015		Y	admin
admin2==direct participant 1	Second Admin	Y	09/14/2015	09/14/2015	N	selfservice_clientadminnull selfservice_clientadmin_appr
admin==direct participant 1	John Smith	Y	10/26/2015	03/07/2014	N	selfservice_clientadminnull selfservice_clientadmin_appr
admin==direct participant 2	Lena Smith	Y	09/14/2015	03/07/2014	N	selfservice_clientadminnull selfservice_clientadmin_appr
asullivan	Alec Sullivan	Y	09/13/2013	09/12/2013	N	
bspota	Bill Spota	Y	07/03/2013	07/03/2013	Y	clearing pm
byang	Ben Yang	Y	07/09/2013	07/09/2013	N	developer
calypso_bo		Y			N	calypso_group
calypso_user	calypso_user	Y	11/05/2015	10/07/2010	Y	@new_yorknull calypso_groupnull developernull product
custadmin1		Y	09/14/2015	02/28/2014	N	selfservice_customeradminnull selfservice_customeradm

Load completed successfully

Pricing Details: 11/5/15 10:11:01 AM PST - FromDB

Active User Report, with Data

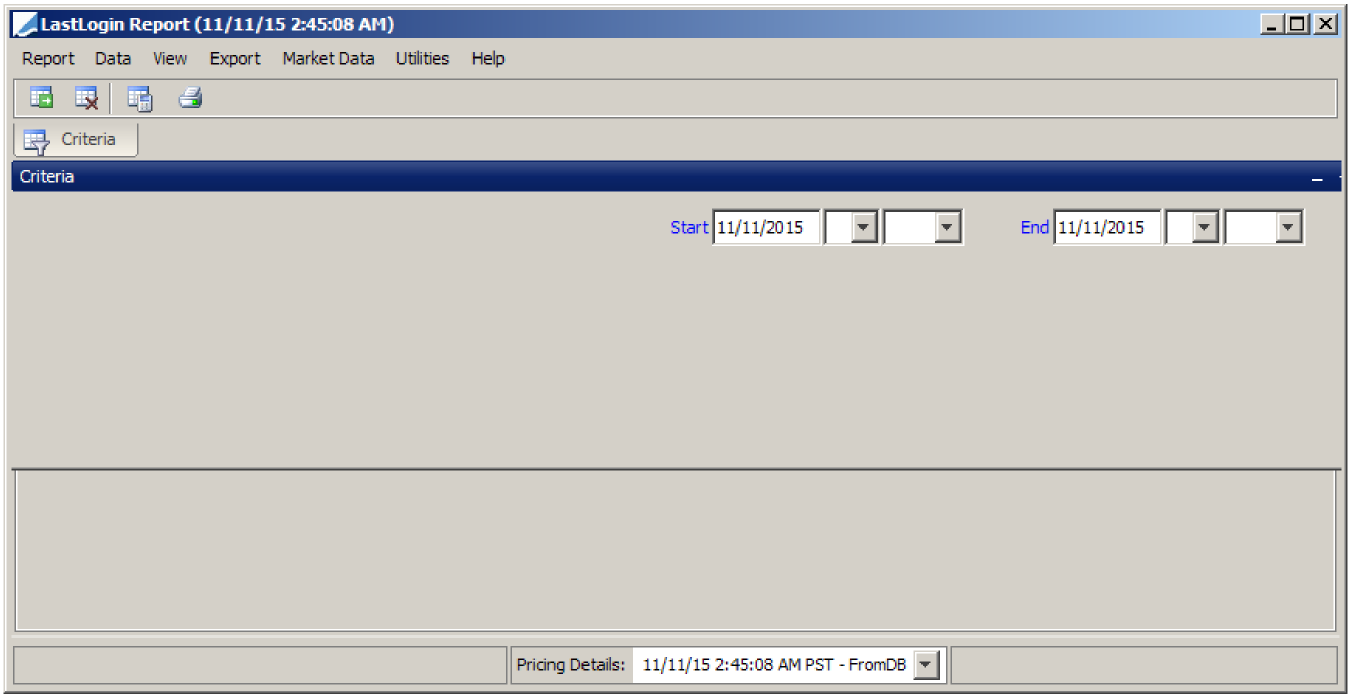
3.2 Last Login

Login/Logout user provides activity for a selected period.

The Last Login report allows the user to set a reporting range using date selectors, a forward/backward selector, and a tenor selector. Combinations of dates, a plus or minus to indicate direction, and the tenors, provide a data range for the system to select records.

Reports the following details for user logins/logouts:

- Login/Logout – Which action occurred.
- User ID – The user's Calypso User ID.
- User Name – The User's full name.
- Login Date – The date of the action.
- Success – Was the action successful or not?



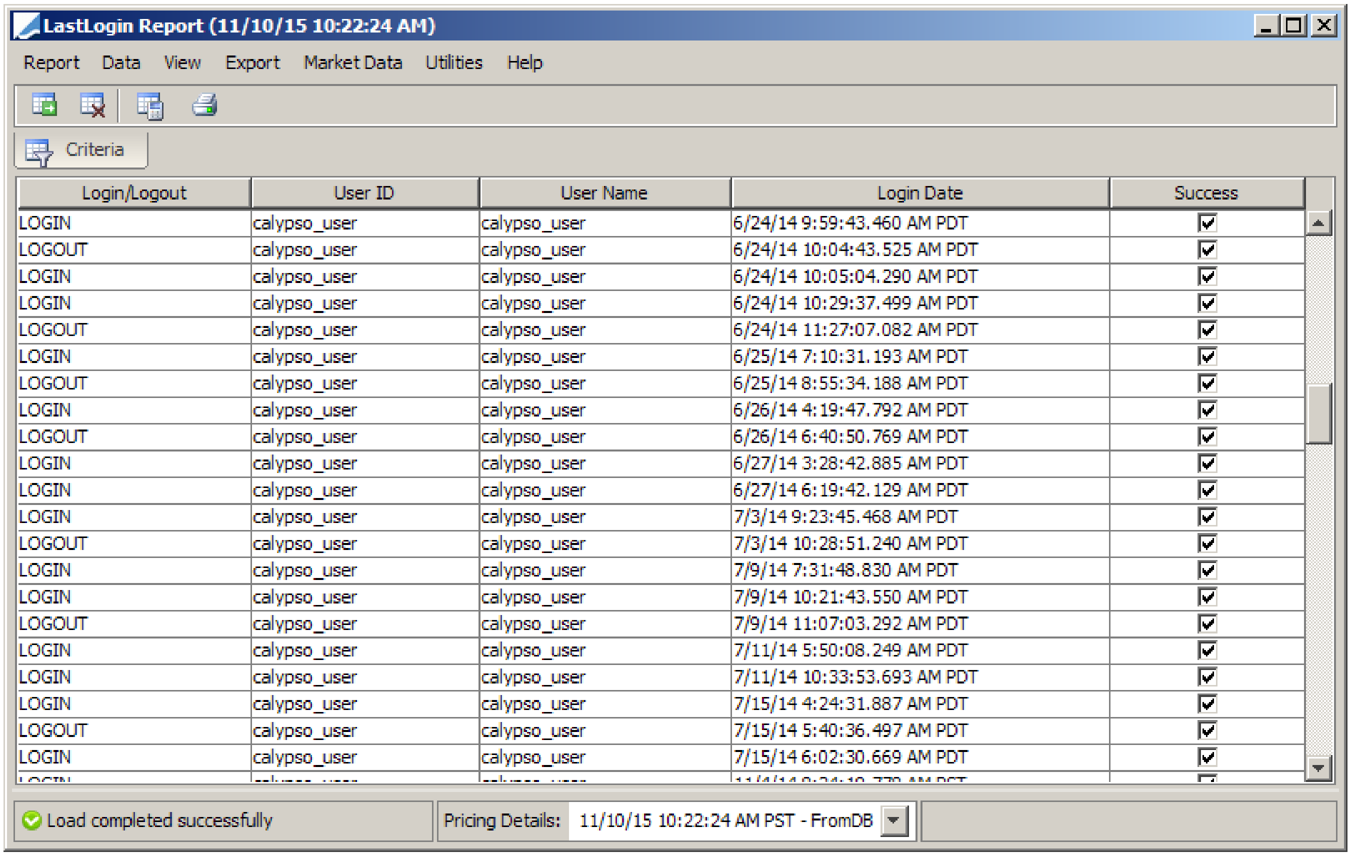
LastLogin Report (11/11/15 2:45:08 AM)

Start 11/11/2015

End 11/11/2015

Pricing Details: 11/11/15 2:45:08 AM PST - FromDB

Last Login Report



Login/Logout	User ID	User Name	Login Date	Success
LOGIN	calypso_user	calypso_user	6/24/14 9:59:43.460 AM PDT	☑
LOGOUT	calypso_user	calypso_user	6/24/14 10:04:43.525 AM PDT	☑
LOGIN	calypso_user	calypso_user	6/24/14 10:05:04.290 AM PDT	☑
LOGIN	calypso_user	calypso_user	6/24/14 10:29:37.499 AM PDT	☑
LOGOUT	calypso_user	calypso_user	6/24/14 11:27:07.082 AM PDT	☑
LOGIN	calypso_user	calypso_user	6/25/14 7:10:31.193 AM PDT	☑
LOGOUT	calypso_user	calypso_user	6/25/14 8:55:34.188 AM PDT	☑
LOGIN	calypso_user	calypso_user	6/26/14 4:19:47.792 AM PDT	☑
LOGOUT	calypso_user	calypso_user	6/26/14 6:40:50.769 AM PDT	☑
LOGIN	calypso_user	calypso_user	6/27/14 3:28:42.885 AM PDT	☑
LOGIN	calypso_user	calypso_user	6/27/14 6:19:42.129 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/3/14 9:23:45.468 AM PDT	☑
LOGOUT	calypso_user	calypso_user	7/3/14 10:28:51.240 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/9/14 7:31:48.830 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/9/14 10:21:43.550 AM PDT	☑
LOGOUT	calypso_user	calypso_user	7/9/14 11:07:03.292 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/11/14 5:50:08.249 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/11/14 10:33:53.693 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/15/14 4:24:31.887 AM PDT	☑
LOGOUT	calypso_user	calypso_user	7/15/14 5:40:36.497 AM PDT	☑
LOGIN	calypso_user	calypso_user	7/15/14 6:02:30.669 AM PDT	☑

Load completed successfully

Pricing Details: 11/10/15 10:22:24 AM PST - FromDB

Last Login Report, with Data

3.3 User Access Permission

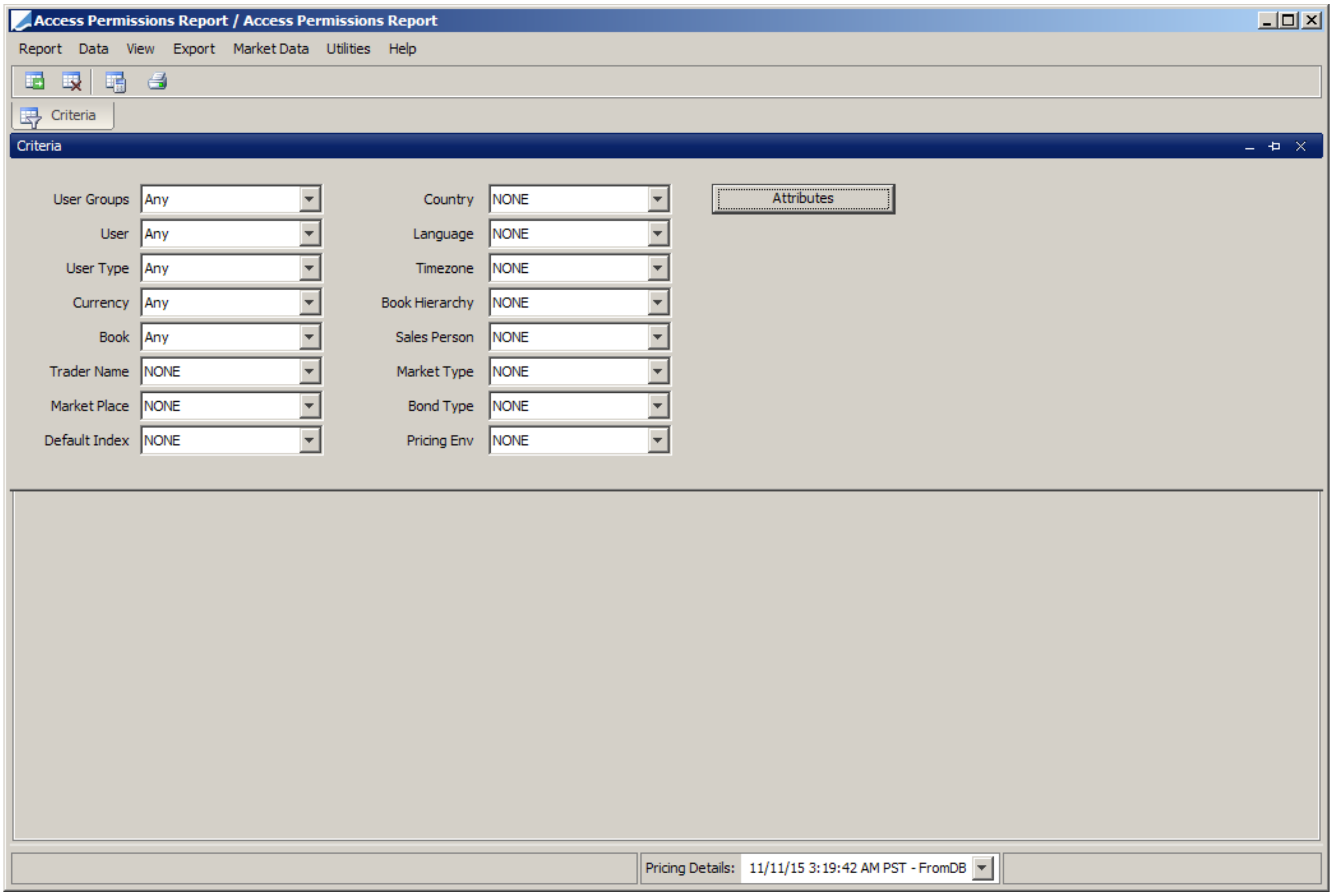
The User Access Permission report details the user's permissions to access Calypso objects. The following User details are provided:

- User (Calypso User ID)
- User Groups (Group memberships)
- Function
- Book
- Pricing Env
- Filter Set
- Trade Filter
- Static Data Filter
- Quote Set
- Risk Config

- Scheduled Task
- Book Hierarchy
- Pricer Config
- Pricer Parameter
- Dispatcher config
- Analysis Param Set
- Application Name (Applications accessible to the user)
- Curve Types
- Product Templates
- Report Templates
- Product Types
- BookBundle
- Calculation Server config
- Products StaticData
- Products Trading
- Risk OnDemand Config
- MarketData Groups
- Fund
- Strategy
- Risk Presenter Config
- Scenario Market Data
- Scenario Rule
- Presentation config
- Mirror Book
- Typed Legs
- MktData server config
- Audit Report Restriction
- Book Attribute
- Feed Config
- Static Data Filter Groups
- Mirror Book Attribute
- Tenant Impersonate Access
- Dashboard Monitoring Configs

- Hedge Accounting Standard

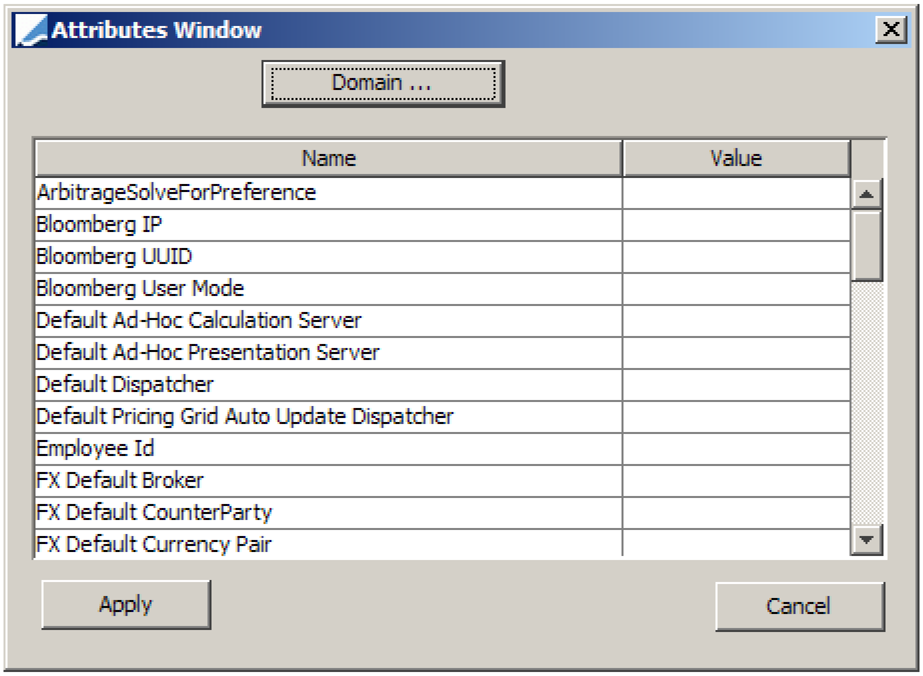
Users can filter the records by selecting various criteria and User Attributes. Note that User Attributes are set on the User Defaults window by clicking **Attributes**.



User Groups	Any	Country	NONE
User	Any	Language	NONE
User Type	Any	Timezone	NONE
Currency	Any	Book Hierarchy	NONE
Book	Any	Sales Person	NONE
Trader Name	NONE	Market Type	NONE
Market Place	NONE	Bond Type	NONE
Default Index	NONE	Pricing Env	NONE

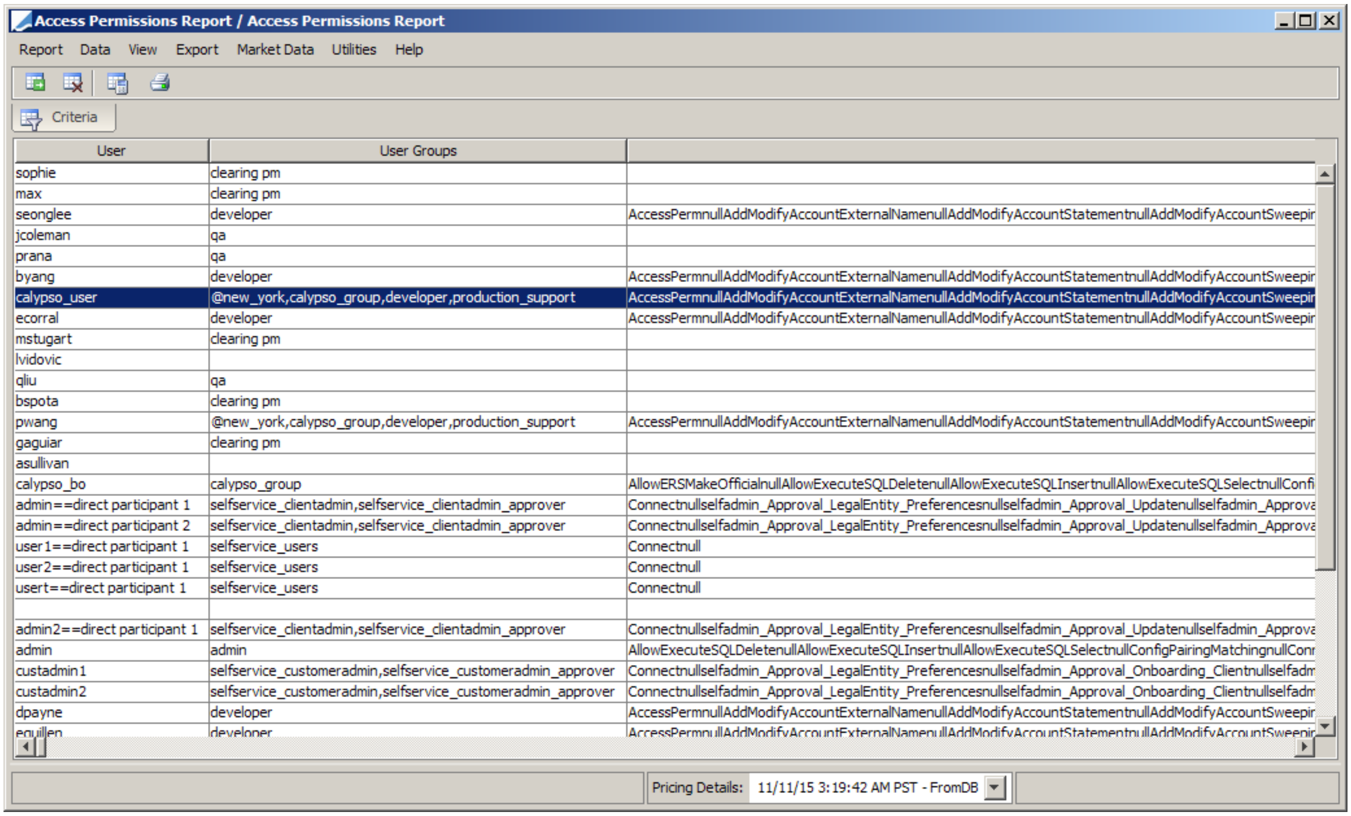
Pricing Details: 11/11/15 3:19:42 AM PST - FromDB

User Access Permissions Report



Name	Value
ArbitrageSolveForPreference	
Bloomberg IP	
Bloomberg UUID	
Bloomberg User Mode	
Default Ad-Hoc Calculation Server	
Default Ad-Hoc Presentation Server	
Default Dispatcher	
Default Pricing Grid Auto Update Dispatcher	
Employee Id	
FX Default Broker	
FX Default CounterParty	
FX Default Currency Pair	

User Attributes (for User Access Permissions Report)



User	User Groups	
sophie	clearing pm	
max	clearing pm	
seonglee	developer	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir
jcoleman	qa	
prana	qa	
byang	developer	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir
calypso_user	@new_york,calypso_group,developer,production_support	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir
ecorral	developer	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir
mstugart	clearing pm	
lvidovic		
qliu	qa	
bspota	clearing pm	
pwang	@new_york,calypso_group,developer,production_support	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir
gaguiar	clearing pm	
asullivan		
calypso_bo	calypso_group	AllowERSMakeOfficialnullAllowExecuteSQLDeletenullAllowExecuteSQLInsertnullAllowExecuteSQLSelectnullConfi
admin==direct participant 1	selfservice_clientadmin,selfservice_clientadmin_approver	Connectnullselfadmin_Approval_LegalEntity_Preferencesnullselfadmin_Approval_Updatenullselfadmin_Approva
admin==direct participant 2	selfservice_clientadmin,selfservice_clientadmin_approver	Connectnullselfadmin_Approval_LegalEntity_Preferencesnullselfadmin_Approval_Updatenullselfadmin_Approva
user1==direct participant 1	selfservice_users	Connectnull
user2==direct participant 1	selfservice_users	Connectnull
usert==direct participant 1	selfservice_users	Connectnull
admin2==direct participant 1	selfservice_clientadmin,selfservice_clientadmin_approver	Connectnullselfadmin_Approval_LegalEntity_Preferencesnullselfadmin_Approval_Updatenullselfadmin_Approva
admin	admin	AllowExecuteSQLDeletenullAllowExecuteSQLInsertnullAllowExecuteSQLSelectnullConfigPairingMatchingnullConr
custadmin1	selfservice_customeradmin,selfservice_customeradmin_approver	Connectnullselfadmin_Approval_LegalEntity_Preferencesnullselfadmin_Approval_Onboarding_Clientnullselfadm
custadmin2	selfservice_customeradmin,selfservice_customeradmin_approver	Connectnullselfadmin_Approval_LegalEntity_Preferencesnullselfadmin_Approval_Onboarding_Clientnullselfadm
dpayne	developer	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir
equillen	developer	AccessPermnullAddModifyAccountExternalNamenullAddModifyAccountStatementnullAddModifyAccountSweepir

Pricing Details: 11/11/15 3:19:42 AM PST - FromDB

User Access Permissions Report, with Data

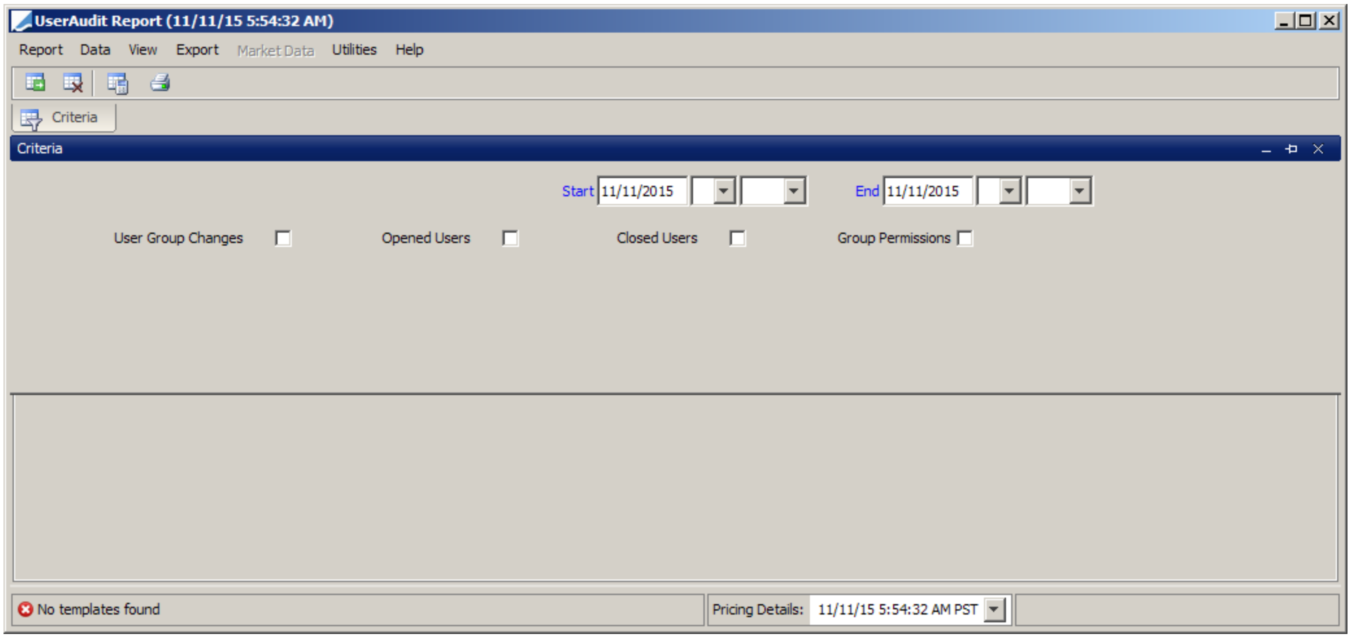
3.4 User Audit

The User Audit report provides a list of users with changes to the following items that have occurred within a given period:

- User Group
- Opened Users (i.e., new users)
- Closed Users (locked/disabled accounts)
- Group Permission changes
-

The following data is provided:

- User/Group ID – The name of the modified User or Group.
- User Name – The name of the Calypso User who made the modification.
- Action – The type of action performed. Closed, Opened, or Updated.
- Old Value – Contains the value before modification. For new Users and group and update changes to non-audited values, this column is empty.



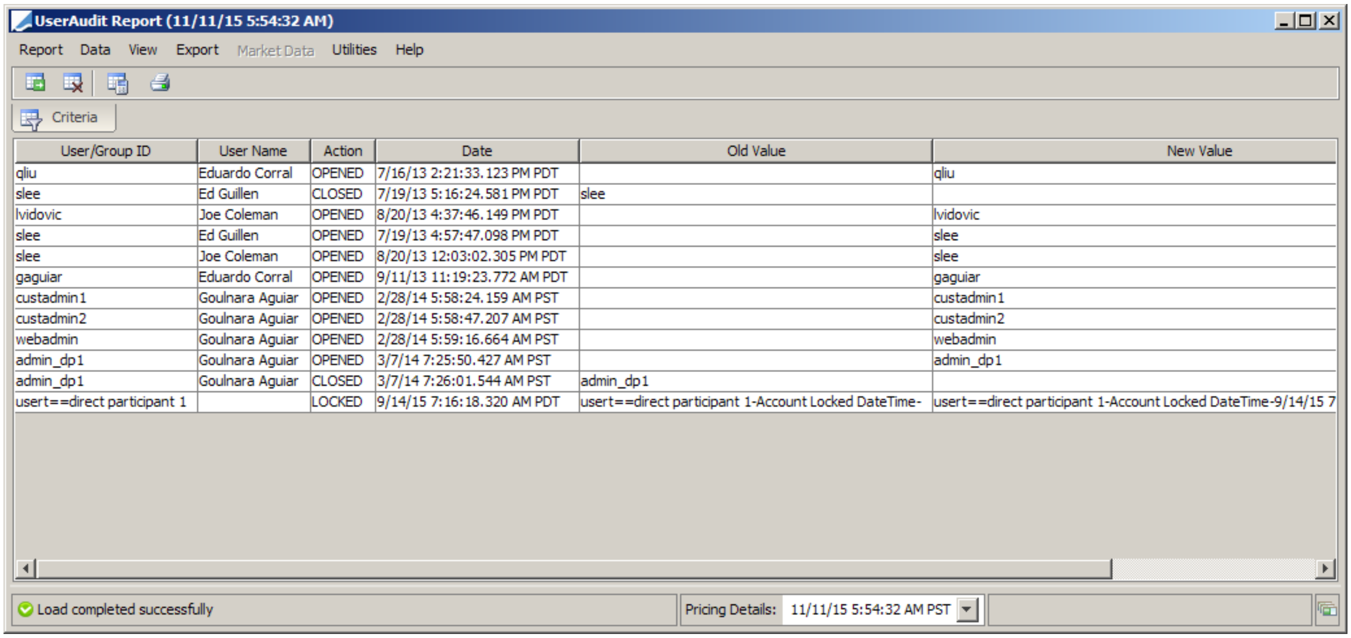
Start 11/11/2015 End 11/11/2015

User Group Changes □ Opened Users □ Closed Users □ Group Permissions □

No templates found

Pricing Details: 11/11/15 5:54:32 AM PST

User Audit Report



User/Group ID	User Name	Action	Date	Old Value	New Value
qliu	Eduardo Corral	OPENED	7/16/13 2:21:33.123 PM PDT		qliu
slee	Ed Guillen	CLOSED	7/19/13 5:16:24.581 PM PDT	slee	
lvidovic	Joe Coleman	OPENED	8/20/13 4:37:46.149 PM PDT		lvidovic
slee	Ed Guillen	OPENED	7/19/13 4:57:47.098 PM PDT		slee
slee	Joe Coleman	OPENED	8/20/13 12:03:02.305 PM PDT		slee
gaguiar	Eduardo Corral	OPENED	9/11/13 11:19:23.772 AM PDT		gaguiar
custadmin1	Goulnara Aguiar	OPENED	2/28/14 5:58:24.159 AM PST		custadmin1
custadmin2	Goulnara Aguiar	OPENED	2/28/14 5:58:47.207 AM PST		custadmin2
webadmin	Goulnara Aguiar	OPENED	2/28/14 5:59:16.664 AM PST		webadmin
admin_dp1	Goulnara Aguiar	OPENED	3/7/14 7:25:50.427 AM PST		admin_dp1
admin_dp1	Goulnara Aguiar	CLOSED	3/7/14 7:26:01.544 AM PST	admin_dp1	
usert==direct participant 1		LOCKED	9/14/15 7:16:18.320 AM PDT	usert==direct participant 1-Account Locked DateTime-	usert==direct participant 1-Account Locked DateTime-9/14/15 7

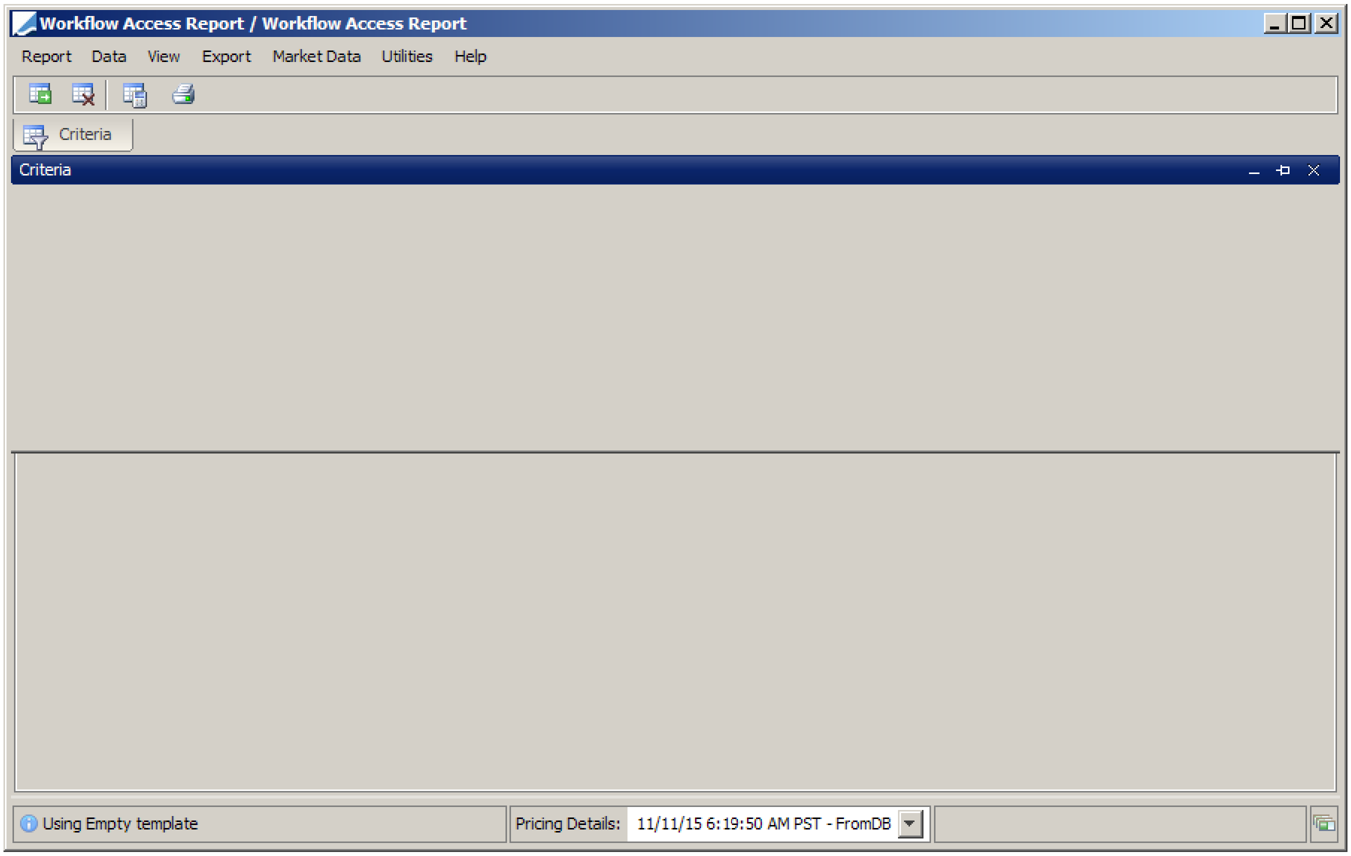
Load completed successfully

Pricing Details: 11/11/15 5:54:32 AM PST

User Audit Report – Opened and Closed Users, shown

3.5 Workflow Access

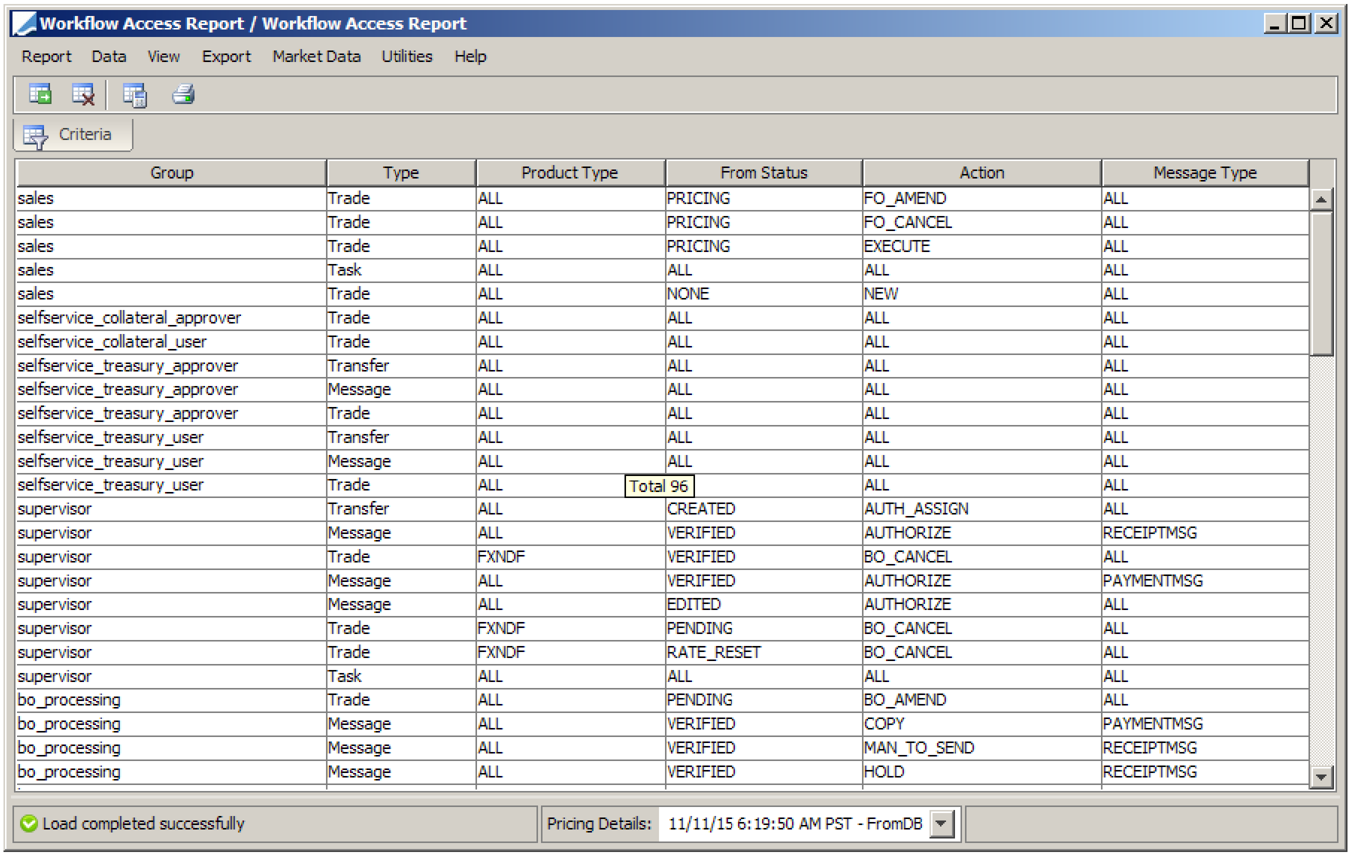
The Workflow Access report provides a listing of Workflow Access permissions by Group, and their characteristics. This report has no selection criteria:



Using Empty template

Pricing Details: 11/11/15 6:19:50 AM PST - FromDB

Workflow Access Report



Group	Type	Product Type	From Status	Action	Message Type
sales	Trade	ALL	PRICING	FO_AMEND	ALL
sales	Trade	ALL	PRICING	FO_CANCEL	ALL
sales	Trade	ALL	PRICING	EXECUTE	ALL
sales	Task	ALL	ALL	ALL	ALL
sales	Trade	ALL	NONE	NEW	ALL
selfservice_collateral_approver	Trade	ALL	ALL	ALL	ALL
selfservice_collateral_user	Trade	ALL	ALL	ALL	ALL
selfservice_treasury_approver	Transfer	ALL	ALL	ALL	ALL
selfservice_treasury_approver	Message	ALL	ALL	ALL	ALL
selfservice_treasury_approver	Trade	ALL	ALL	ALL	ALL
selfservice_treasury_user	Transfer	ALL	ALL	ALL	ALL
selfservice_treasury_user	Message	ALL	ALL	ALL	ALL
selfservice_treasury_user	Trade	ALL		ALL	ALL
supervisor	Transfer	ALL	CREATED	AUTH_ASSIGN	ALL
supervisor	Message	ALL	VERIFIED	AUTHORIZE	RECEIPTMSG
supervisor	Trade	FXNDF	VERIFIED	BO_CANCEL	ALL
supervisor	Message	ALL	VERIFIED	AUTHORIZE	PAYMENTMSG
supervisor	Message	ALL	EDITED	AUTHORIZE	ALL
supervisor	Trade	FXNDF	PENDING	BO_CANCEL	ALL
supervisor	Trade	FXNDF	RATE_RESET	BO_CANCEL	ALL
supervisor	Task	ALL	ALL	ALL	ALL
bo_processing	Trade	ALL	PENDING	BO_AMEND	ALL
bo_processing	Message	ALL	VERIFIED	COPY	PAYMENTMSG
bo_processing	Message	ALL	VERIFIED	MAN_TO_SEND	RECEIPTMSG
bo_processing	Message	ALL	VERIFIED	HOLD	RECEIPTMSG

Total 96

Load completed successfully

Pricing Details: 11/11/15 6:19:50 AM PST - FromDB

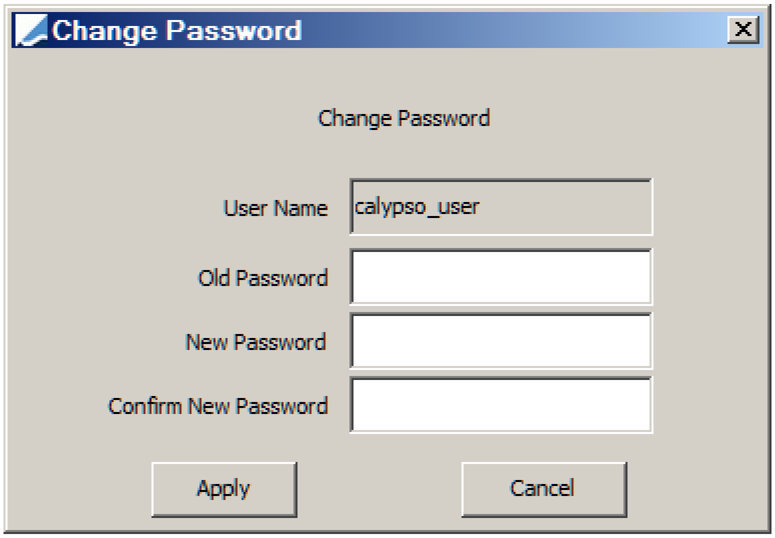
Workflow Access Report, with data

4. Change Password

If your implementation makes use of Active Directory, the user and password management functions are controlled via Active Directory.

▶ To work with users when using MS Active Directory for authentication, see Specifying Users Using MS Active Directory for further information.

Choose **Calypso Navigator > Configuration > User Access Control > Change Password** (menu action `util.ChangePasswordDialog`) to change your password after logging in. The Change Password window will appear as shown below.



User Name: calypso_user

The name of the user currently connected will be displayed in the User Name field. The user currently connected can change only his or her own password.

- Enter the old password in the Old Password field, enter the new password in the New Password field, and retype the new password in the Confirm New Password field.

  The passwords can be validated using Calypso's built-in routine or with a client-written extension.

- Then click **Apply**.

  By default, passwords are validated according to the settings on the Users tab of the Access Permissions window. Clients have the option of implementing an External Authentication System or entirely replacing the Calypso password system with Microsoft Active Directory.

Password Expiration

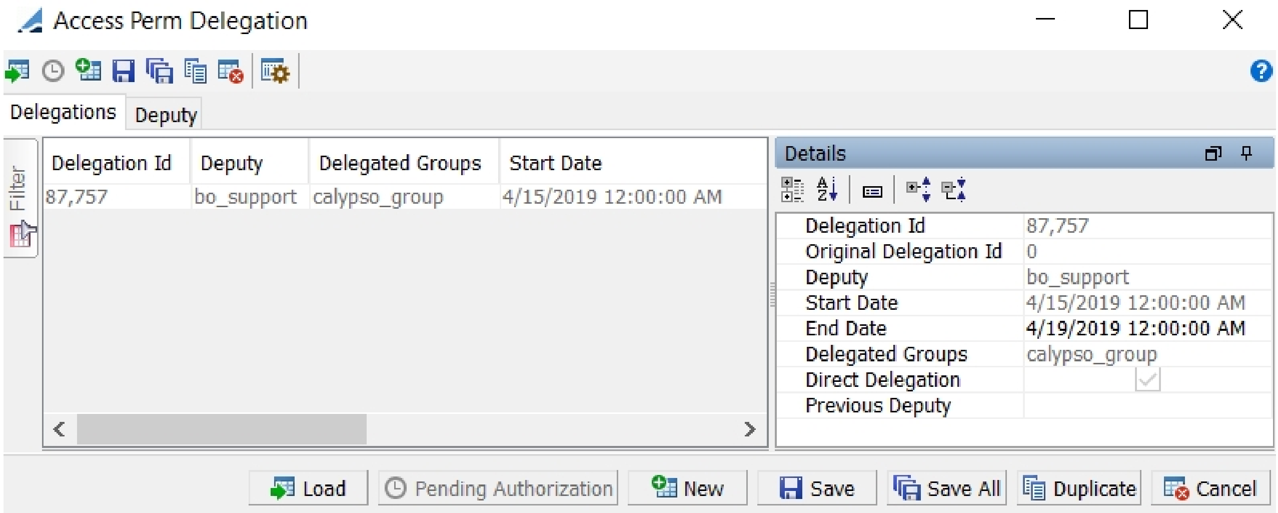
A password will expire after the time specified in the Users panel of the Access Permissions window (Threshold Days field). It will never expire if the Threshold Days field is set to 0.

5. Access Permissions Delegation

A user can delegate his or her access permissions to another user for a temporary period as needed.

[NOTE: This is not currently supported for actions performed in Market Risk, ERS Limits, and Limits & Compliance]

From the Calypso Navigator, choose **Configuration > User Access Control > Delegation Window** to define delegation configurations (menu action `refdata.accessperm.AccessPermDelegationWindow`).



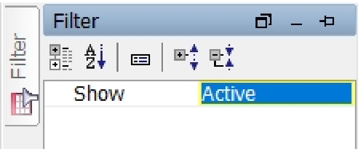
Delegation Id	Deputy	Delegated Groups	Start Date
87,757	bo_support	calypso_group	4/15/2019 12:00:00 AM

Delegation Id	87,757
Original Delegation Id	0
Deputy	bo_support
Start Date	4/15/2019 12:00:00 AM
End Date	4/19/2019 12:00:00 AM
Delegated Groups	calypso_group
Direct Delegation	✓
Previous Deputy	

Access Perm Delegation window

- All existing configurations for the user currently logged in are loaded by default.

  You can filter the list of configurations using the Filter tab, as needed.

Show	Active

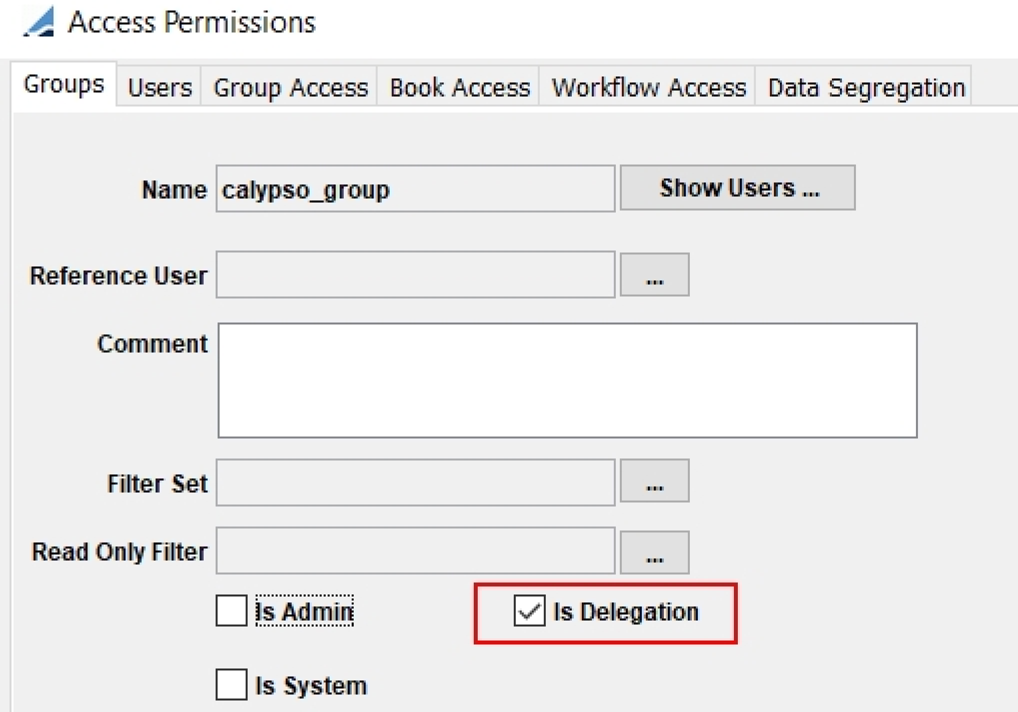
- You can click to configure the column display.
- You can create delegation configurations in the Delegations panel, and the deputy user can re-delegate configurations in the Deputy panel.

5.1 Before you Begin

Delegated Group

You need to check "Is Delegation" for the groups to be delegated.

Example: A user from the group "calypso_group" wants to delegate his or her access permissions.



Name: calypso_group

Reference User:

Comment:

Filter Set:

Read Only Filter:

□ Is Admin

☑ Is Delegation

□ Is System

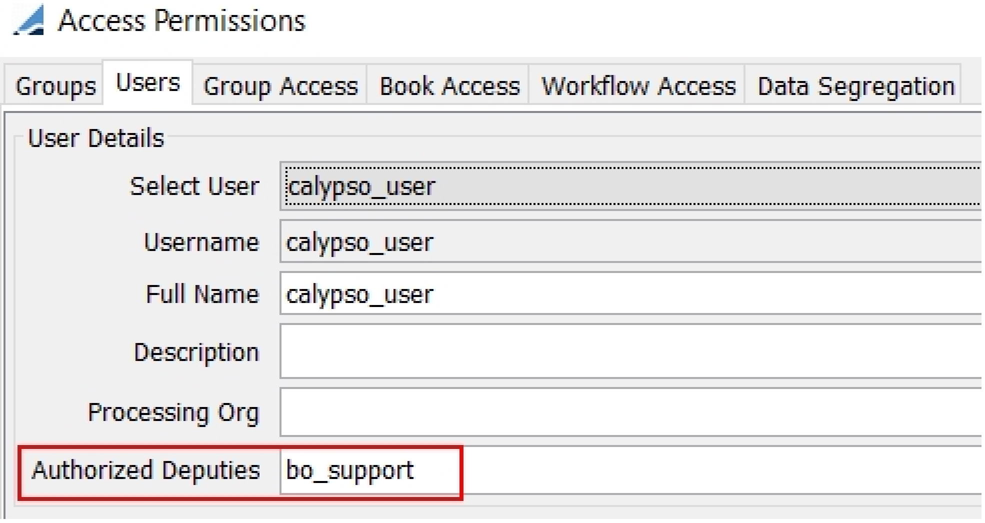
[NOTE: A delegated group *cannot* be a system group, and *should not* be an admin group]

Deputies

You need to associate the delegating user with a number of deputies to whom the user can delegate his or her access permissions.

The deputy must have access to the delegated group (group defined with "Is Delegation" checked), and must have access to the Applications required to perform the actions of the delegated group (Navigator for example).

Example: calypso_user wants to delegate his or her access permissions to bo_support.



Select User: calypso_user

Username: calypso_user

Full Name: calypso_user

Description:

Processing Org:

Authorized Deputies: bo_support

ⓘ **[NOTE: Processing Organization restrictions are not superseded by the delegation function. A deputy is limited to its Processing Organizations]**

5.2 Creating Delegation Configurations

You need to be logged in as the delegating user.

Select the Delegations panel.

- Click ⊞ to create a new configuration, and enter the fields described below in the Details panel.
- Click 💾 to save your changes.

Fields Details

Fields	Description
Id	ID given by the system upon saving.
Original Delegation Id	Original delegation in case of re-delegation. See Deputy Panel for details.
Deputy	Select the user to whom the access permissions are delegated (user associated as authorized deputy).
Start Date	Select the start date of the delegation.
End Date	Select the end date of the delegation.
Delegated Groups	Select the groups that are delegated (groups defined with "Is Delegation" checked).
Direct Delegation	Checked by the system upon saving a new delegation. It appears clear if the delegation has been re-delegated.

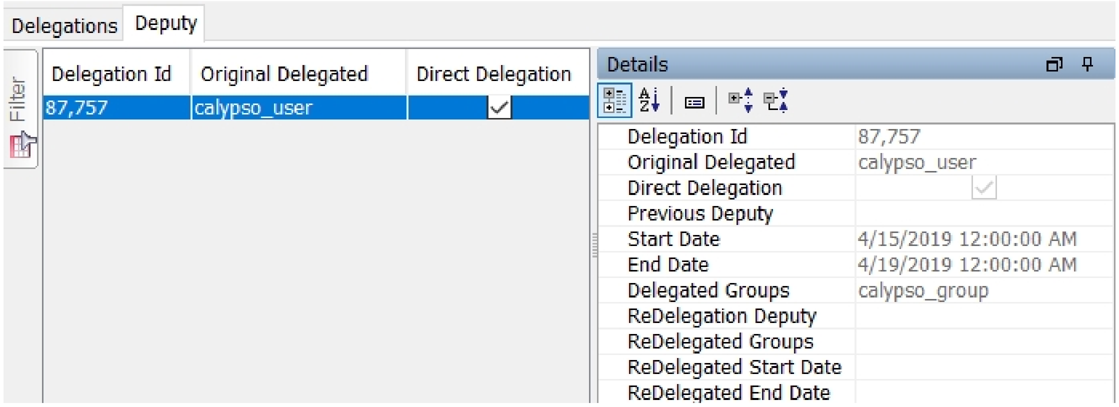
Fields	Description
Previous Deputy	Previous deputy in case of re-delegation.

You can also cancel a delegation or change the end date of a delegation.

5.3 Deputy Panel

You need to be logged in as the deputy user.

Select the Deputy panel. It shows the delegations you are associated with.



Delegation Id	Original Delegated	Direct Delegation
87,757	calypso_user	✓

Delegation Id	87,757
Original Delegated	calypso_user
Direct Delegation	✓
Previous Deputy	
Start Date	4/15/2019 12:00:00 AM
End Date	4/19/2019 12:00:00 AM
Delegated Groups	calypso_group
ReDelegation Deputy	
ReDelegated Groups	
ReDelegated Start Date	
ReDelegated End Date	

- You can re-delegate a delegation by entering the fields described below in the Details panel.
- Then click 💾 to save your changes.

Fields	Description
ReDelegation Deputy	Select the user to whom the delegation is re-delegated (user associated as authorized deputy).
ReDelegated Groups	Select the groups that are delegated (groups defined with "Is Delegation" checked).
ReDelegated Start Date	Select the start date of the re-delegation.
ReDelegated End Date	Select the end date of the re-delegation.

You can also cancel a re-delegation or change the end date of a re-delegation.

6. Data Authorization

Calypso provides the ability to run the system in Authorization mode. In Authorization mode, any change to static data must be authorized by an authorization user. An authorization user is a user who has permission to authorize modifications and who is different from the user who actually made the modifications.

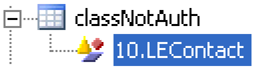
▶ Please refer to the *Calypso Installation Guide* for details on enabling Authorization mode.

The Authorization mode only applies to classes specified in the *classAuthMode* domain. You can remove a given class from that domain as applicable using **Calypso Navigator > Configuration > System > Domain Values** (menu action `refdata.DomainValueWindow`) to disable the Authorization mode for that class.

▶ See Authorizable Objects for a list of all objects that support authorization.

You can also disable a given class for a given processing organization only using the domain *classNotAuth*. You can add values to that domain in the form "<ProcessingOrg ID>.<class name>" to disable authorization of the given class for the given processing organization.

Example: "10.LEContact" – All changes to the legal entity contacts of processing org # 10 will not need authorization.



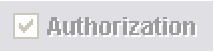
classNotAuth
10.LEContact

▶ For information on making your own custom classes authorizable, refer to the *Calypso Developer's Guide*.

Data Modification

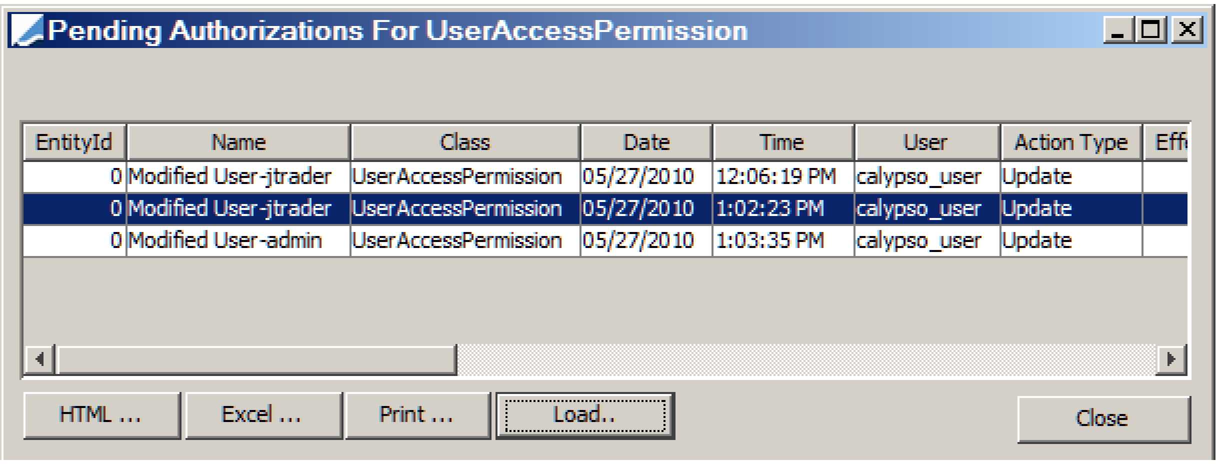
When new static data is entered or static data is modified, it is not be visible to any user (including the user who made the modification) until the data is actually authorized.

In most windows, an Authorization checkbox will appear checked and grayed-out as shown below to indicate that the Authorization mode is enabled.



A **Show Auth** button or **Show Pending** button will also be available to allow viewing any pending authorization.

When you click **Show Auth** or **Show Pending**, a pending authorizations window will appear as in the example below.



Pending Authorizations For UserAccessPermission

EntityId	Name	Class	Date	Time	User	Action Type	Eff
0	Modified User-jtrader	UserAccessPermission	05/27/2010	12:06:19 PM	calypso_user	Update	
0	Modified User-jtrader	UserAccessPermission	05/27/2010	1:02:23 PM	calypso_user	Update	
0	Modified User-admin	UserAccessPermission	05/27/2010	1:03:35 PM	calypso_user	Update	

It displays all data that have been modified and require authorization before they can be actually saved.

» Click **Close** when you are done.

Data Authorization

The actual authorization of data can be done using the Data Authorization window or using the Authorization task by an authorization user. See below for details.

A user can accept self-modifications provided the SameUserAuthorization function is granted to the group of the user or the user is an Admin user (a user from a "Is Admin" group).

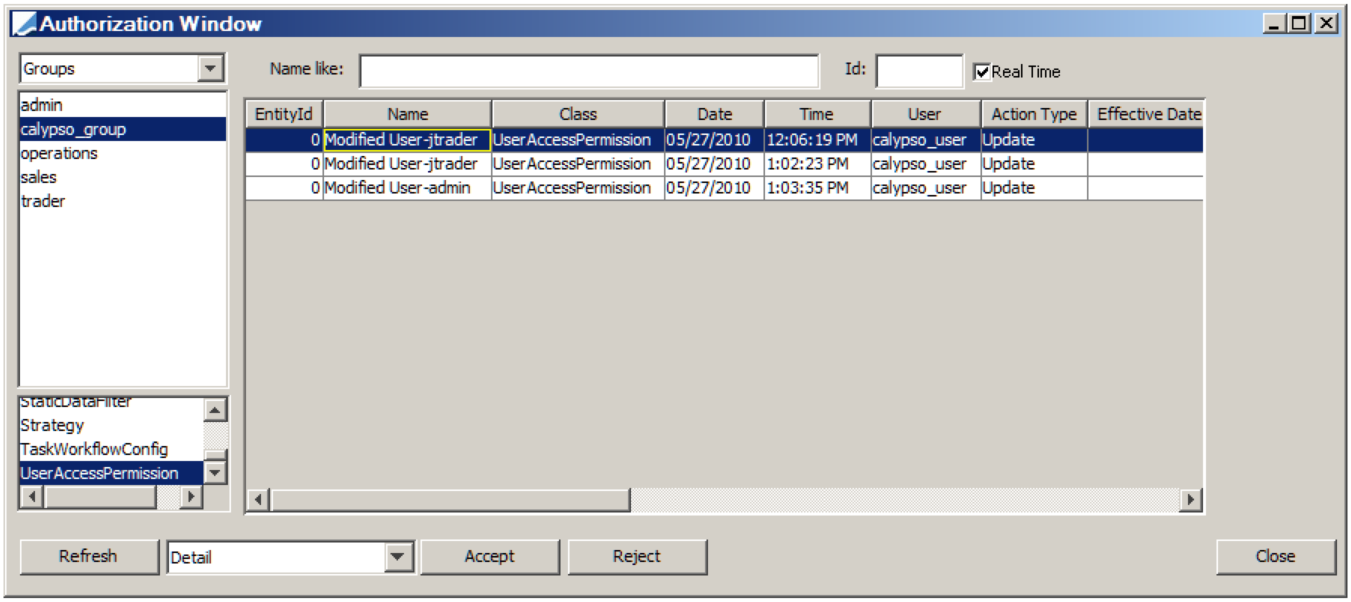
A user can reject self-modifications provided the SameUserRejection is granted to the group of the user or the user is an Admin user.

Trade Authorization

▶ For information on using the Authorization mode for trades, please refer to Calypso Workflow documentation - Trade Workflow Manual Authorization.

6.1 Using the Data Authorization Window

To authorize new and modified data, choose **Calypso Navigator > Processing > Data Authorization** (menu action `refdata.AuthorizationWindow`). The Data Authorization window will appear as shown below.



EntityId	Name	Class	Date	Time	User	Action Type	Effective Date
0	Modified User-jtrader	UserAccessPermission	05/27/2010	12:06:19 PM	calypso_user	Update	
0	Modified User-jtrader	UserAccessPermission	05/27/2010	1:02:23 PM	calypso_user	Update	
0	Modified User-admin	UserAccessPermission	05/27/2010	1:03:35 PM	calypso_user	Update	

» Select Users or Groups from the field in the upper-left corner. Then select a user or a group from the list as applicable, to filter the pending authorizations for that user or group. Select a class from the list at the lower-left corner as applicable, to filter the pending authorizations for that class.

You can also specify one or more characters in the "Name like" field to filter entity names that start with these characters. Or you can enter an object id in the Id field to load an individual object.

Then click **Refresh** to load the pending authorizations for the specified criteria.

- Select Detail or Version from the field next to the **Refresh** button to display the pending authorizations per version, or to show the individual modifications. There will only be a difference when multiple changes have been made to a given entity version.
- The Real Time checkbox is checked by default to remove authorized data or rejected data in real-time from the Data Authorization window. This prevents conflicts when multiple users are authorizing data at the same time.
- You can double-click a row to view the details of an object.
- Enumerated Fields - Use the tables in Enumerated Field Keys to determine the human readable values.

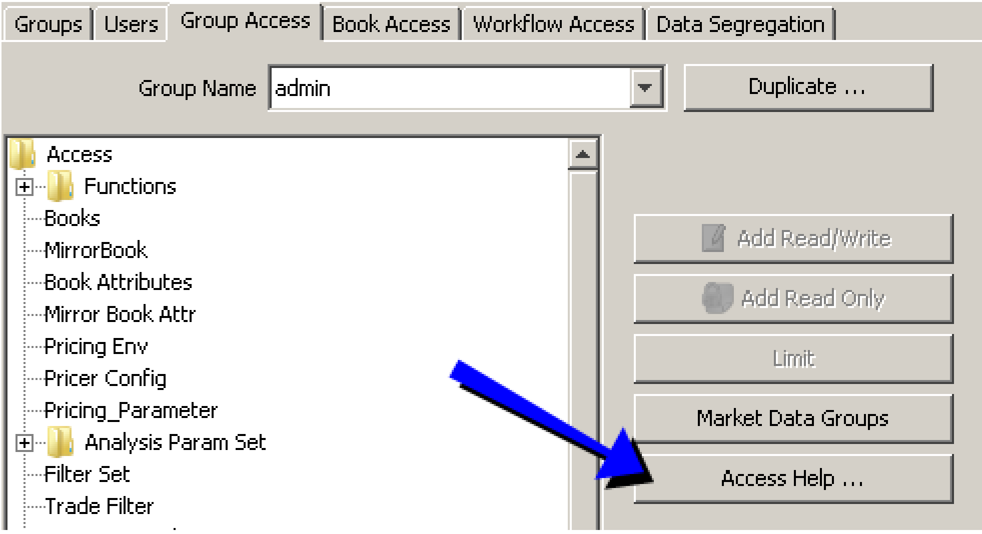
  ▶ See Enumerated Field Keys for details.
- Select a row or multiple rows and click **Accept** to authorize the modification. You can also click **Reject** to reject the modification.

  Note that if the Access Permissions mode is enabled, you will be able to modify individual changes only if your group is granted the ApplyIndividualAuth function. Otherwise you will only be able to authorize versions.
- You can right-click a row and select **Configure Columns** to customize the columns if desired.

Access Permissions

Data authorization using the Data Authorization window is controlled by a number of functions: You need "Authorization" functions for all the objects you wish to authorize: AuthorizeAccount, AuthorizeBook, AuthorizeCountry, AuthorizeHoliday, etc.

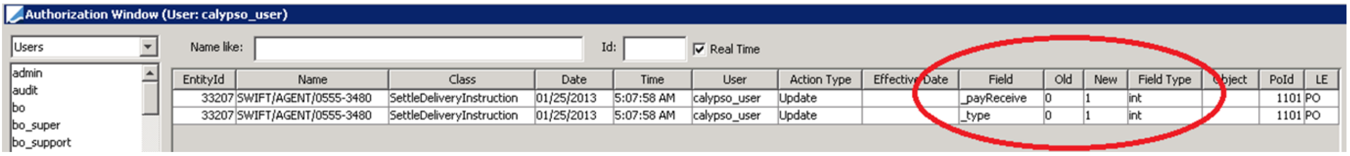
These functions are described under **Calypso Navigator > Configuration > User Access Control > Access Permissions**, Group Access panel > **Access Help** button.



Group Name admin

Enumerated Field Keys

Certain fields are represented by enumerations rather than words. The example below shows the SDI table:



EntityId	Name	Class	Date	Time	User	Action Type	Effective Date	Field	Old	New	Field Type	Object	PoId	LE
33207	SWIFT/AGENT/0555-3480	SettleDeliveryInstruction	01/25/2013	5:07:58 AM	calypso_user	Update		_payReceive	0	1	int		1101	PO
33207	SWIFT/AGENT/0555-3480	SettleDeliveryInstruction	01/25/2013	5:07:58 AM	calypso_user	Update		_type	0	1	int		1101	PO

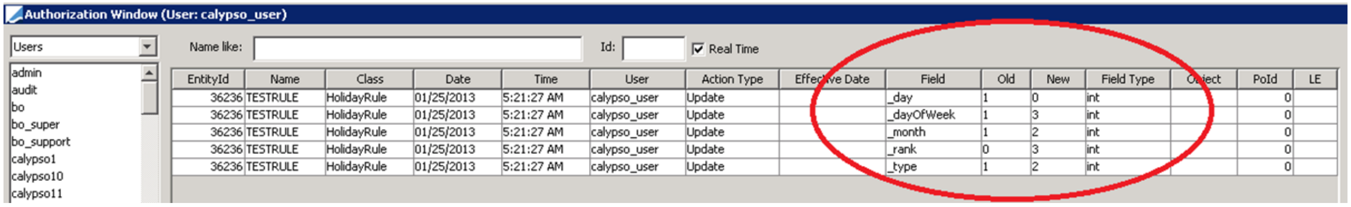
The following table provides keys for the "_payReceive" column in an SDI record:

_type Value	Meaning & Description
0	BOTH - SDI is for pay and receive.
1	PAY - SDI is for the pay direction.
2	RECEIVE - SDI is for the receive direction.

The following table provides keys for the "_type" column in an SDI record:

_type Value	Meaning & Description
0	BOTH - Payment is cash and security.
1	CASH - Payment is cash.
2	SECURITY - Payment is in securities.

The example below shows the Holiday Rules table:



EntityId	Name	Class	Date	Time	User	Action Type	Effective Date	Field	Old	New	Field Type	Object	PoId	LE
36236	TESTRULE	HolidayRule	01/25/2013	5:21:27 AM	calypso_user	Update		_day	1	0	int		0	
36236	TESTRULE	HolidayRule	01/25/2013	5:21:27 AM	calypso_user	Update		_dayOfWeek	1	3	int		0	
36236	TESTRULE	HolidayRule	01/25/2013	5:21:27 AM	calypso_user	Update		_month	1	2	int		0	
36236	TESTRULE	HolidayRule	01/25/2013	5:21:27 AM	calypso_user	Update		_rank	0	3	int		0	
36236	TESTRULE	HolidayRule	01/25/2013	5:21:27 AM	calypso_user	Update		_type	1	2	int		0	

The following tables provide keys for "_dayofweek", "_month", "_rank", and "_type":

"_dayofweek" Column:

_dayofweek Value	Weekday
1	NONE
2	Monday
3	Tuesday

_dayofweek Value	Weekday
4	Wednesday
5	Thursday
6	Friday
7	Saturday
8	Sunday

"_month" Column:

_month Value	Month
1	January
2	February
3	March
4	April
5	May
6	June
7	July
8	August
9	September
10	October
11	November
12	December

"_rank" Column:

_rank Value	Rank
0	NONE
1	FIRST
2	SECOND
3	THIRD
4	FOURTH
5	LAST

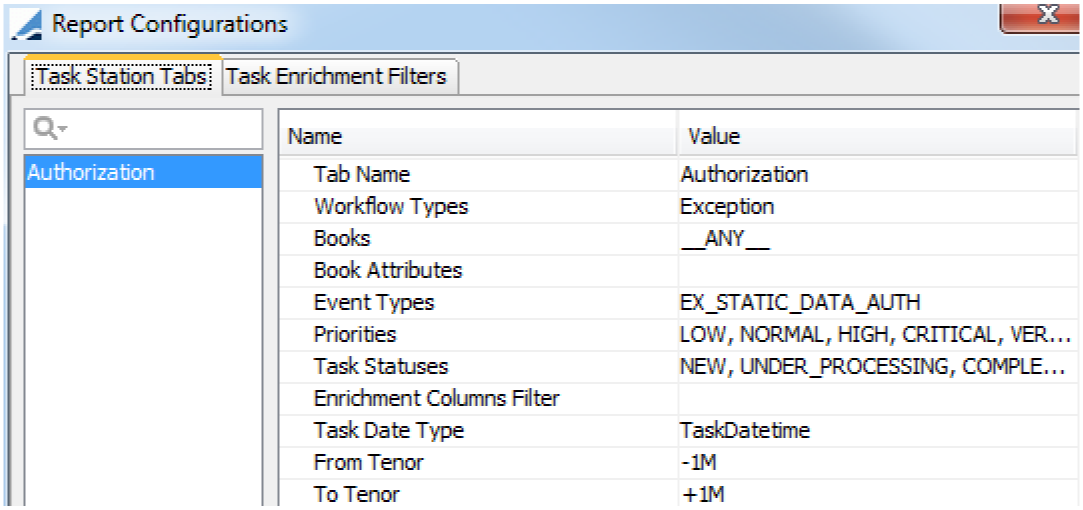
"_type" Column:

_type Value	Meaning & Description
0	FIXED - This holiday occurs on the same date each year.
1	FLOAT - The calendar date of this holiday varies from year to year.
2	EASTER - Easter.

6.2 Using the Authorization Task

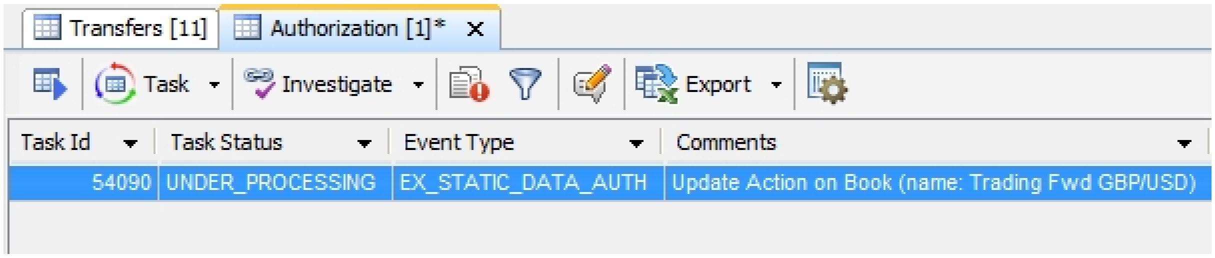
In order to use the Authorization task, you need to set the environment property **AUTHORIZATION_TASK=true**.

You will be able to display authorization exceptions in the Task Station and accept or reject the modification.



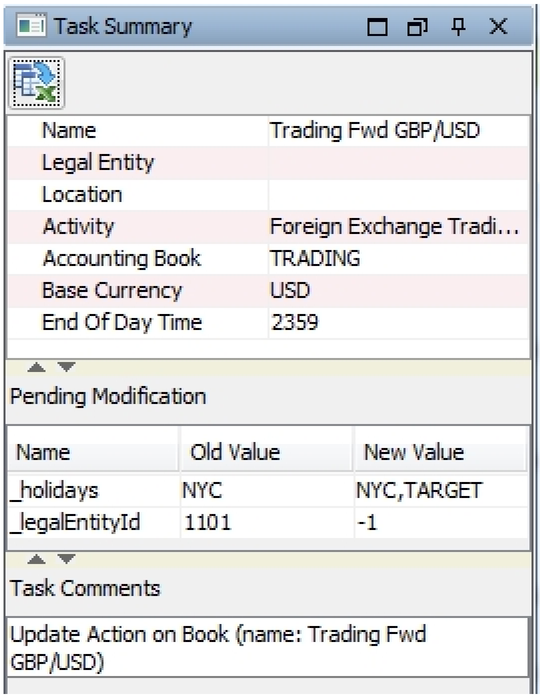
Name	Value
Tab Name	Authorization
Workflow Types	Exception
Books	__ANY__
Book Attributes	
Event Types	EX_STATIC_DATA_AUTH
Priorities	LOW, NORMAL, HIGH, CRITICAL, VER...
Task Statuses	NEW, UNDER_PROCESSING, COMPLE...
Enrichment Columns Filter	
Task Date Type	TaskDatetime
From Tenor	-1M
To Tenor	+1M

Note that only modifications that have been made after the environment property AUTHORIZATION_TASK is set to true will appear.



Task Id	Task Status	Event Type	Comments
54090	UNDER_PROCESSING	EX_STATIC_DATA_AUTH	Update Action on Book (name: Trading Fwd GBP/USD)

- Right-click a row, process it, and choose **Workflow > Accept** or **Workflow > Reject** from the popup menu to authorize or reject the modification. You can view details on the Task Summary panel.



Name	Trading Fwd GBP/USD
Legal Entity	
Location	
Activity	Foreign Exchange Tradi...
Accounting Book	TRADING
Base Currency	USD
End Of Day Time	2359

Pending Modification

Name	Old Value	New Value
_holidays	NYC	NYC,TARGET
_legalEntityId	1101	-1

Task Comments

Update Action on Book (name: Trading Fwd GBP/USD)

- You can also choose **Workflow > Show Modifs** to bring up the Data Authorization window, and **Workflow > Show Object** to bring up the corresponding data configuration window.

The default exception is EX_STATIC_DATA_AUTH but you can define specific authorization tasks for each type of modified data.

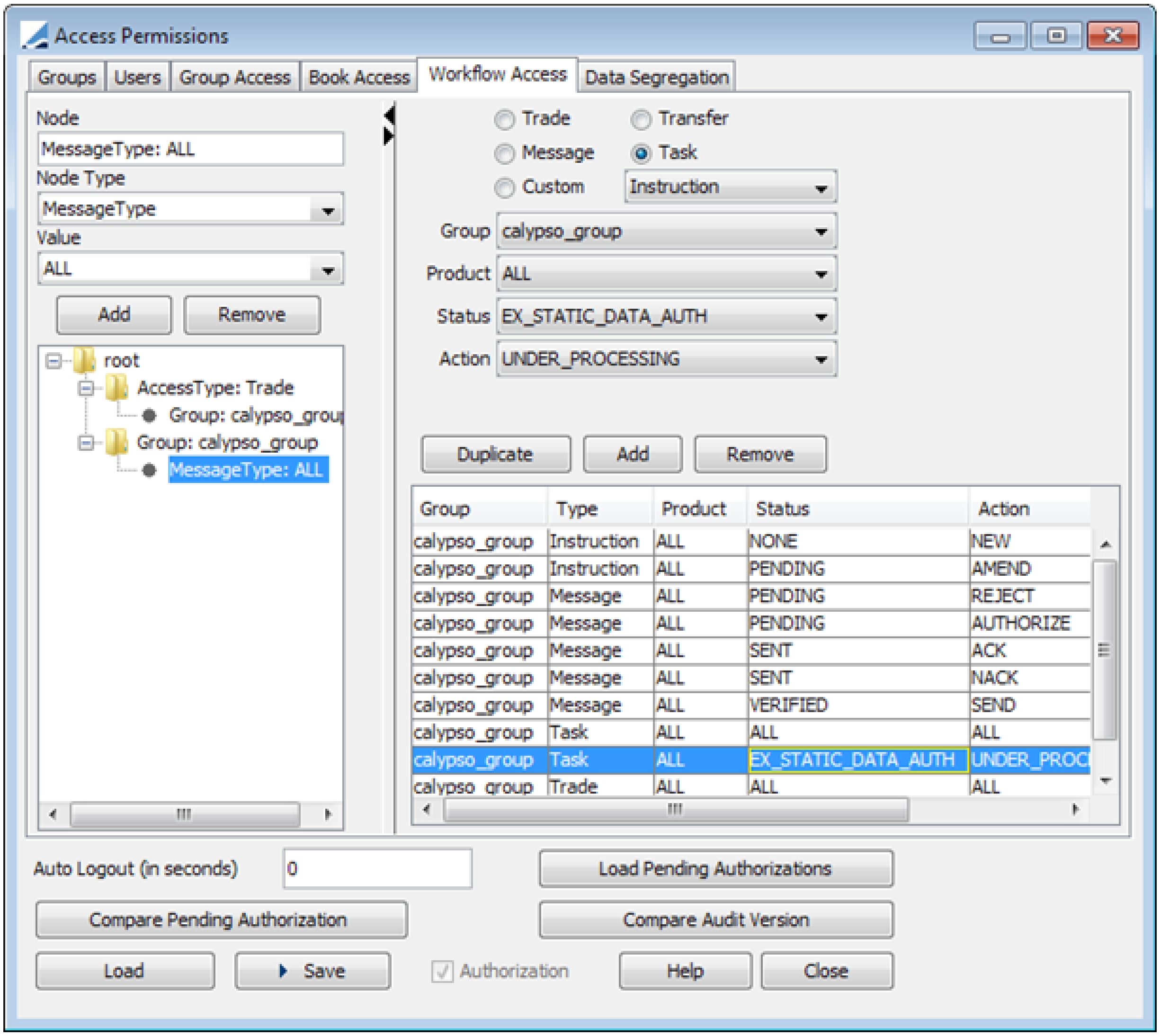
Example: Add MANUALPOSTING_AUTH to the *exceptionType* domain, and EX_MANUALPOSTING_AUTH to the *eventType* domain to have a specific authorization task for manual postings.

The following objects can be authorized using the Authorization Task mechanism: Account, CollateralConfig, LEContact, LegalEntity, LegalEntityAttribute, SettleDeliveryInstruction, HaircutRule, Legal Agreements, Margin Contracts, QuoteValue, StaticDataFilter, AccountSweepingConfig, AdviceConfig, Bond, BondAssetBacked, BondFRN, BondMMDiscount, Holiday, LegalEntityRelation.

You will create the exception type and event type as "<object name from classAuthMode in uppercase>_AUTH" and "EX_<object name from classAuthMode in uppercase>_AUTH" respectively.

Access Permissions

You need access to the UNDER_PROCESSING action for tasks in status EX_STATIC_DATA_AUTH (or other customized status), for authorizing modifications using the Authorization task.



Node: MessageType: ALL

Node Type: MessageType

Value: ALL

○ Trade ○ Transfer
○ Message ● Task
○ Custom Instruction

Group: calypso_group

Product: ALL

Status: EX_STATIC_DATA_AUTH

Action: UNDER_PROCESSING

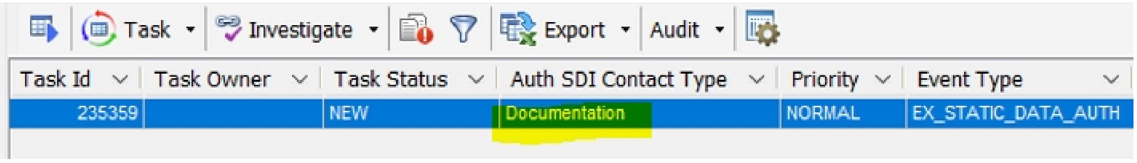
Group	Type	Product	Status	Action
calypso_group	Instruction	ALL	NONE	NEW
calypso_group	Instruction	ALL	PENDING	AMEND
calypso_group	Message	ALL	PENDING	REJECT
calypso_group	Message	ALL	PENDING	AUTHORIZE
calypso_group	Message	ALL	SENT	ACK
calypso_group	Message	ALL	SENT	NACK
calypso_group	Message	ALL	VERIFIED	SEND
calypso_group	Task	ALL	ALL	ALL
calypso_group	Task	ALL	EX_STATIC_DATA_AUTH	UNDER_PROC
calypso_group	Trade	ALL	ALL	ALL

Auto Logout (in seconds): 0

☑ Authorization

Authorizing SDIs by Contact Type

You can define a Task Enrichment field for the SDI contact type and filter EX_STATIC_DATA_AUTH tasks by SDI contact type.



Task Id	Task Owner	Task Status	Auth SDI Contact Type	Priority	Event Type
235359		NEW	Documentation	NORMAL	EX_STATIC_DATA_AUTH

Task Enrichment Field:

Field Display Name = Auth SDI Contact Type

Field Db Name = auth_sdi_contact_type

Workflow Type = CrossWorkflows

Data Source Class = com.calypso.bo.task

Custom Class = com.calypso.taskenrichment.data.enrichment.DefaultTaskEnrichmentCustom

Data Source Getter Info = getSDIContactType.

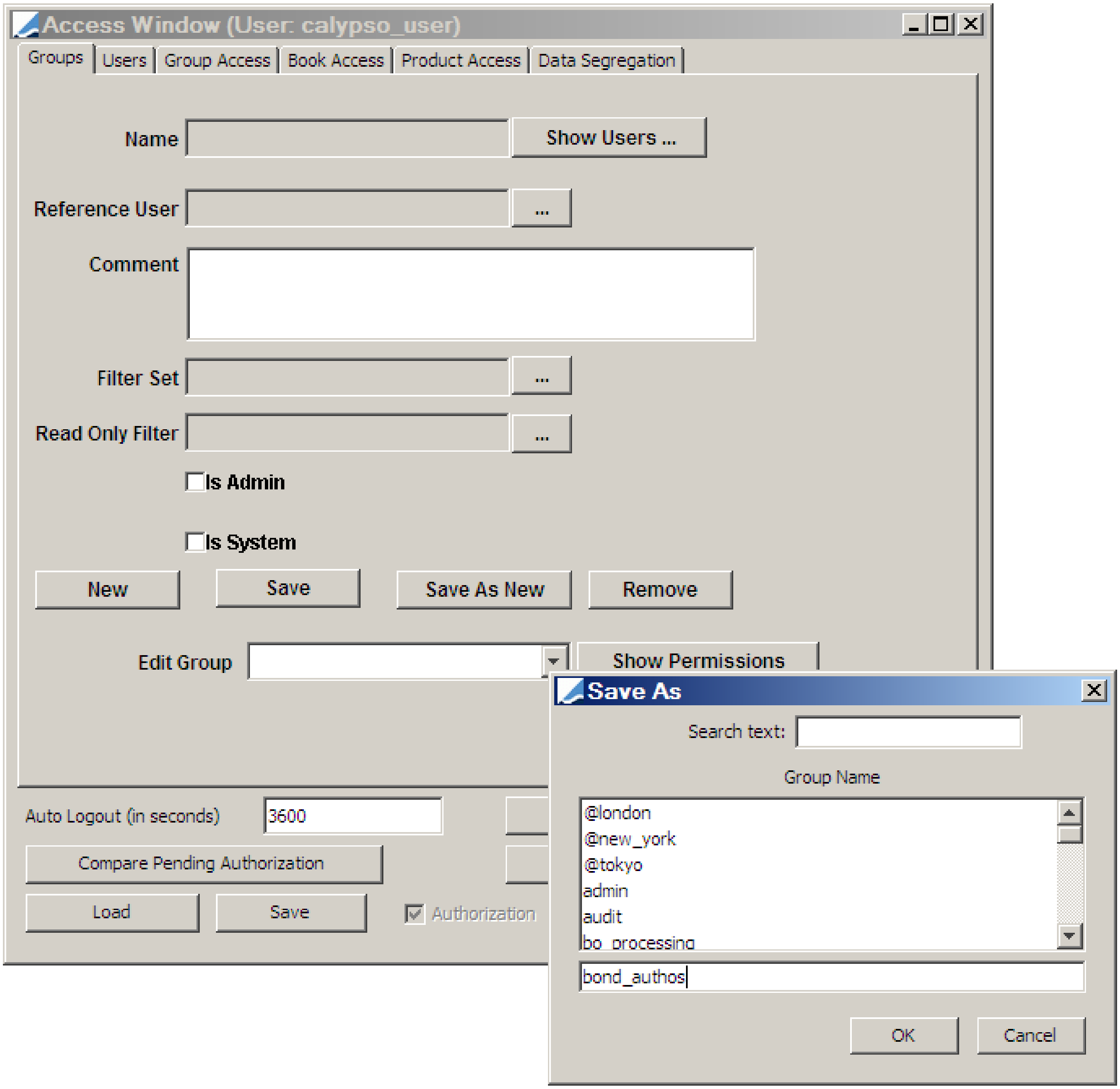
▶ Please refer to Calypso Task Station documentation for complete details on defining enrichment fields.

6.3 Creating an Authorization User

When the administrator has enabled Authorization mode, changes to certain data must be authorized by a special user, known as the Authorization User. Depending on the size of your implementation and volumes, there may be one or several such users.

On the Access Permissions window, use the Group tab to create a group that will have Access Permission for the data that the user will authorize. Our example shows the process for creating a group for "Bonds" Authorization Users. Permissions are applied to a group and the user is then assigned to the group.

To begin, click **New**, then click **Save As New**. Enter the desired group name in the Save As dialog, then click **OK**.



□ Is Admin

□ Is System

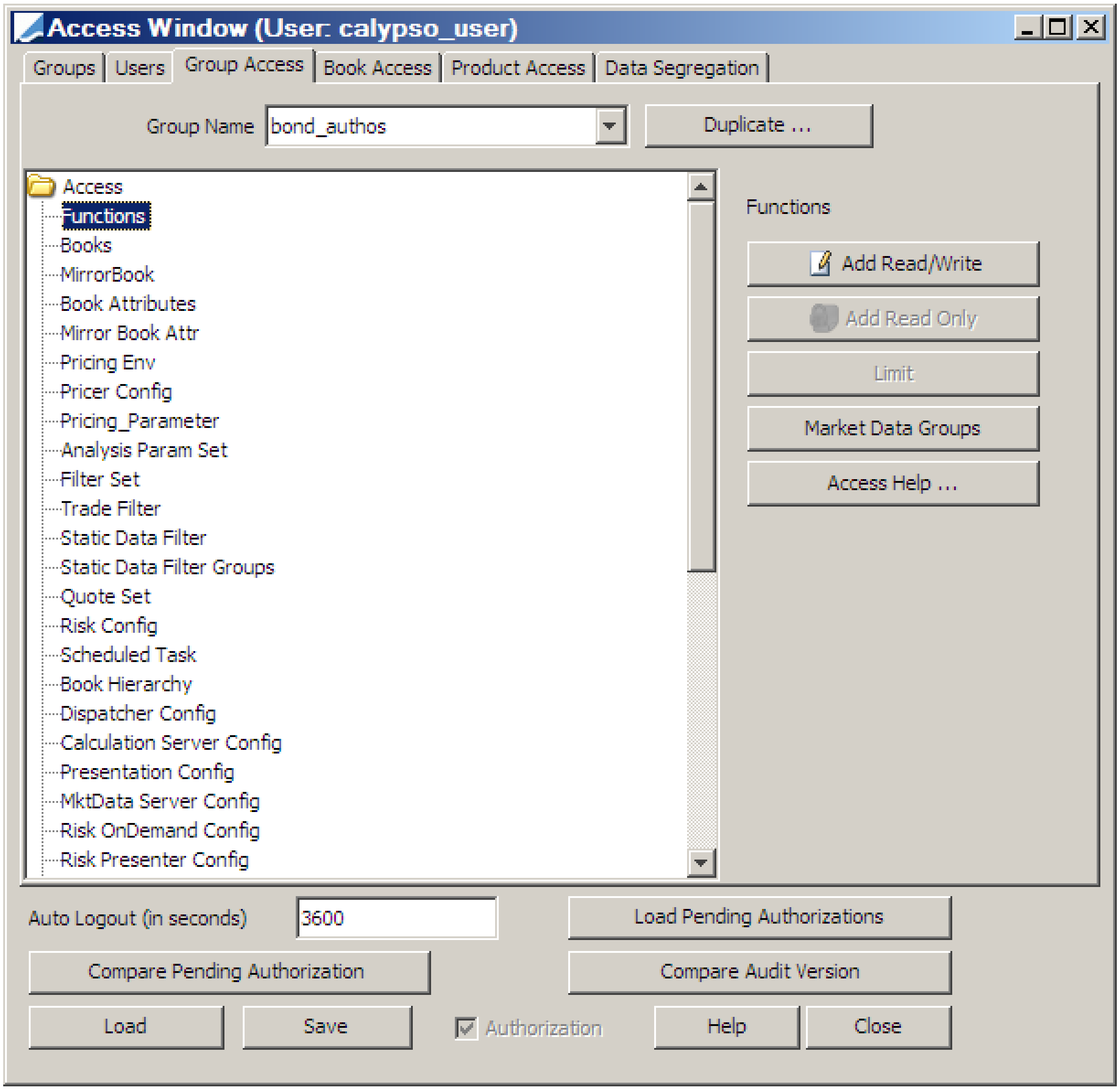
Auto Logout (in seconds) 3600

☑ Authorization

Group Name:
@london
@new_york
@tokyo
admin
audit
bo_processing

bond_authos

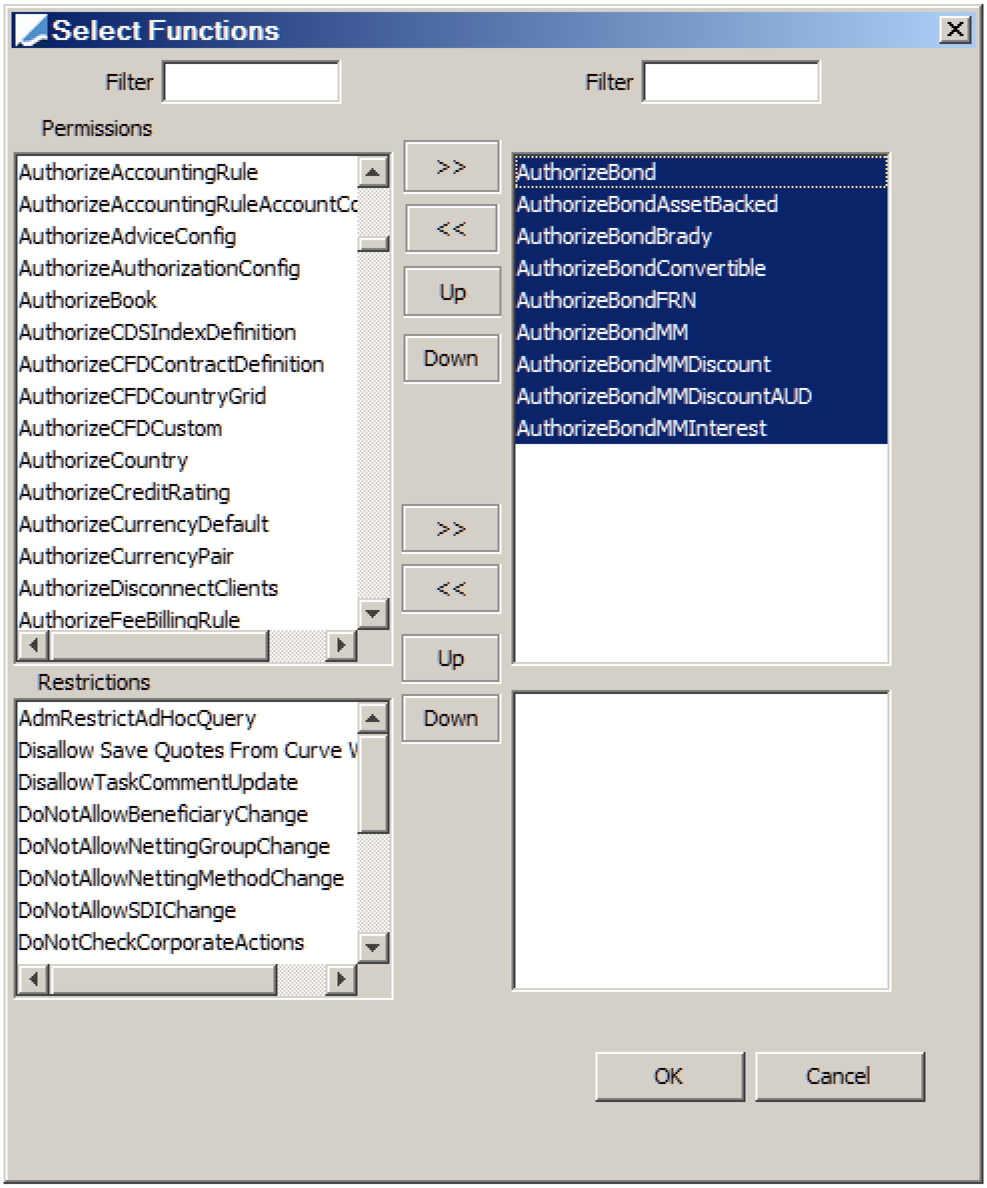
1. From the Group Access tab, select Functions on the Access list, then click **Add Read/Write**.



Group Name: bond_authos

Auto Logout (in seconds): 3600

2. In the Select Function window, choose the desired authorizations, then click **OK**:



Permissions:

- AuthorizeAccountingRule
- AuthorizeAccountingRuleAccountCc
- AuthorizeAdviceConfig
- AuthorizeAuthorizationConfig
- AuthorizeBook
- AuthorizeCDSIndexDefinition
- AuthorizeCFDContractDefinition
- AuthorizeCFDCountryGrid
- AuthorizeCFDCustom
- AuthorizeCountry
- AuthorizeCreditRating
- AuthorizeCurrencyDefault
- AuthorizeCurrencyPair
- AuthorizeDisconnectClients
- AuthorizeFeeBillingRule

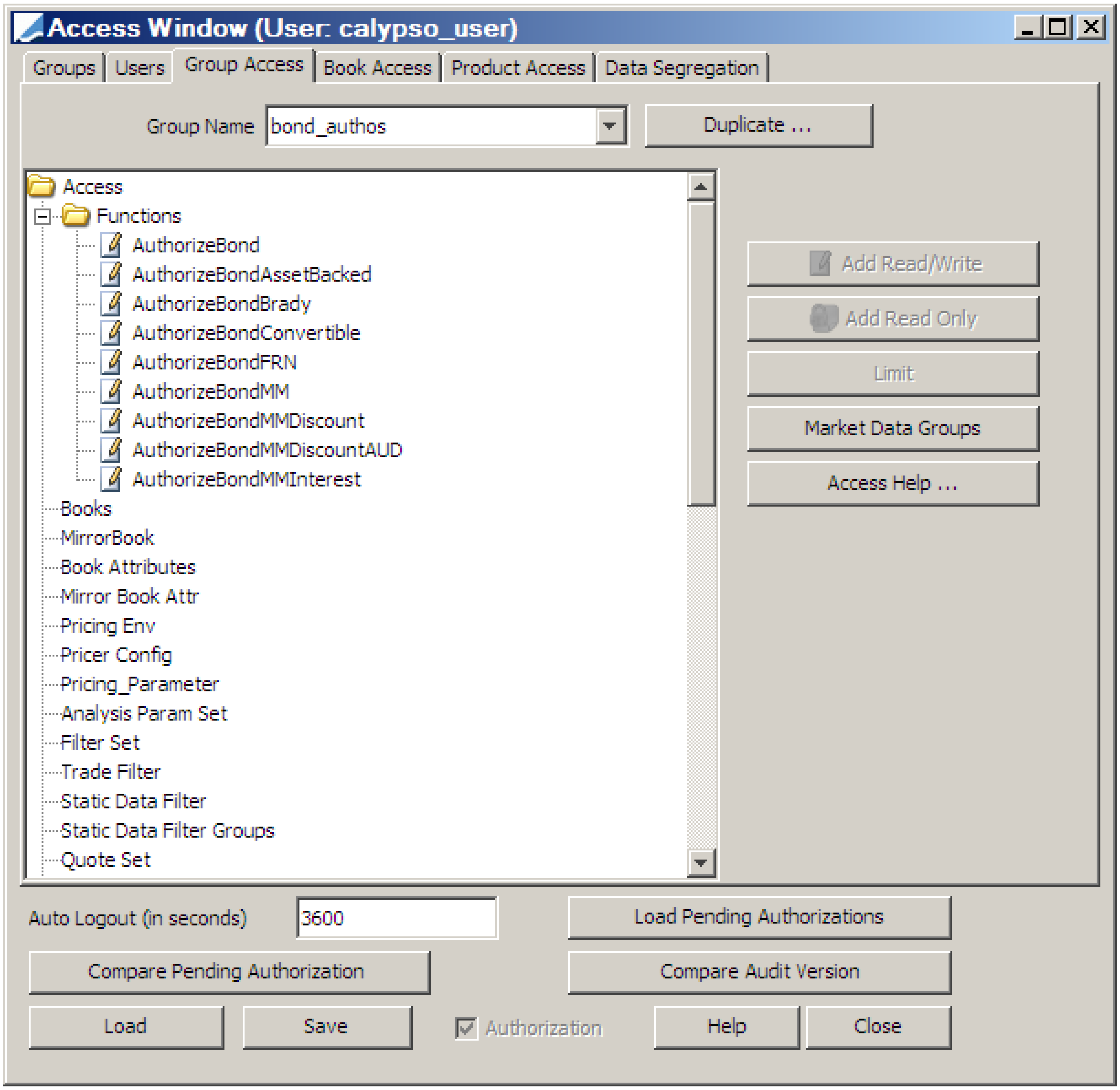
Selected:

- AuthorizeBond
- AuthorizeBondAssetBacked
- AuthorizeBondBrady
- AuthorizeBondConvertible
- AuthorizeBondFRN
- AuthorizeBondMM
- AuthorizeBondMMDiscount
- AuthorizeBondMMDiscountAUD
- AuthorizeBondMMInterest

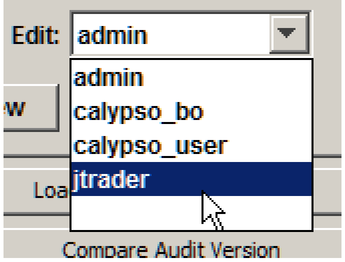
Restrictions:

- AdmRestrictAdHocQuery
- Disallow Save Quotes From Curve V
- DisallowTaskCommentUpdate
- DoNotAllowBeneficiaryChange
- DoNotAllowNettingGroupChange
- DoNotAllowNettingMethodChange
- DoNotAllowSDIChange
- DoNotCheckCorporateActions

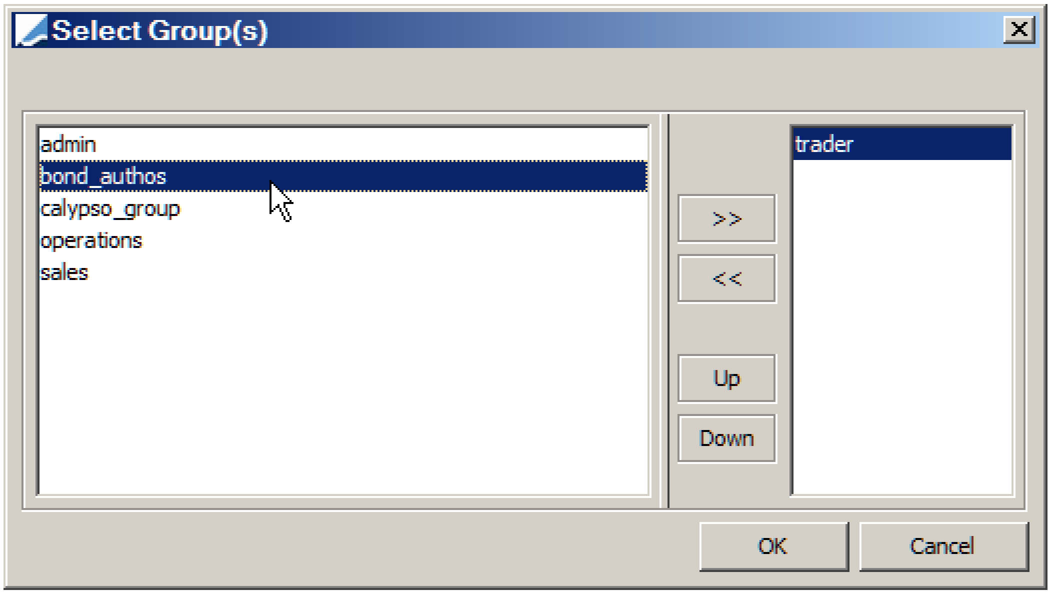
3. On the Access Permissions window, click **Save** to save the changes to the group:



4. On the Users tab, choose the desired user:

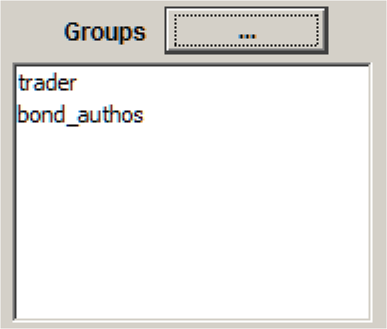


5. Click **...** to open the Select Groups window:



6. Double-click the group having the authorization permissions, then click **OK**.

In our example, the user *jtrader* now is now a member of the *bond_authos* group. Members of the *bond_authos* group are Authorization Users who can accept or reject changes to bond data.

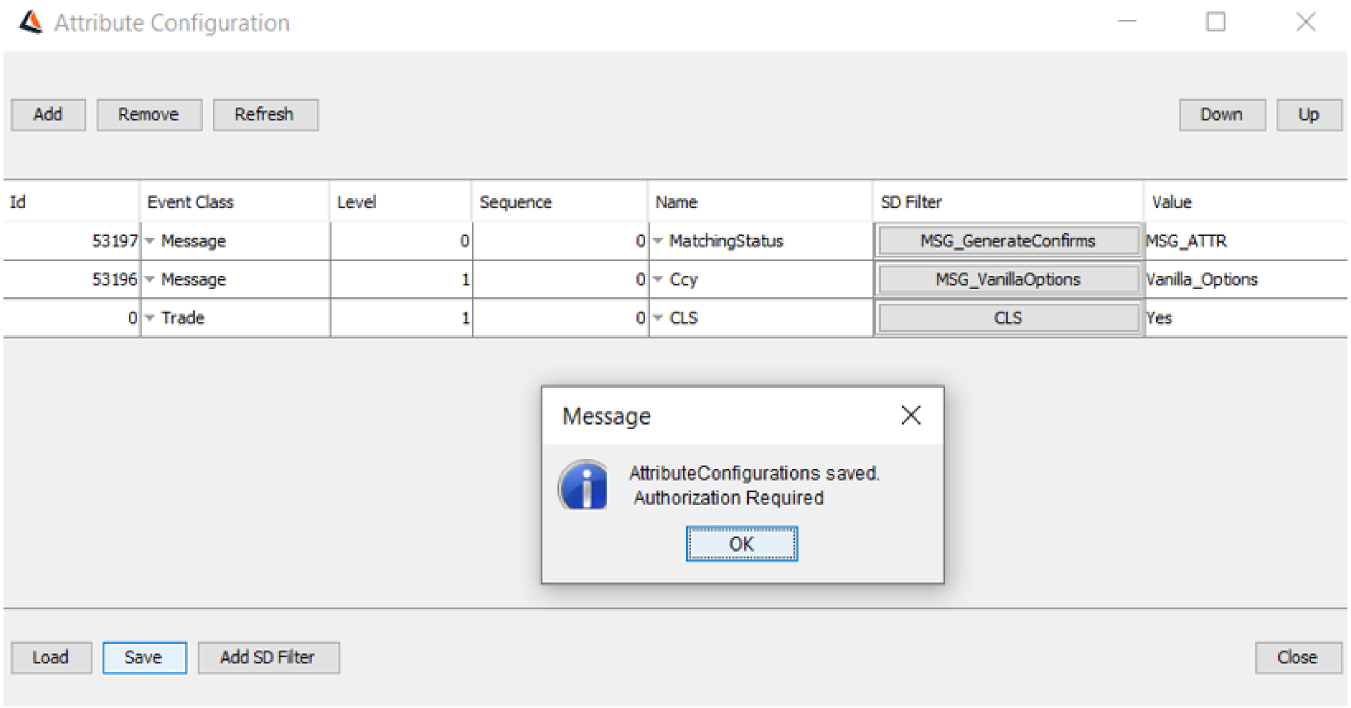


6.4 Data Authorization for Attribute Configuration Window

In order to use Data Authorization for Attribute Configuration Window, you need to set the environment property DATA_AUTHORIZATION_ENABLED=true and AUTHORIZATION_TASK=true.

You will be able to create, modify and remove any entry from the Attribute Configuration Window. For data authorization, it will undergo four-eye check functionality once the authorization mode is enabled. You will receive a request to accept or reject the modifications in Authorization Window.

You can view the recorded entries in Authorization Audit Window.



Id	Event Class	Level	Sequence	Name	SD Filter	Value
53197	Message	0	0	MatchingStatus	MSG_GenerateConfirms	MSG_ATTR
53196	Message	1	0	Ccy	MSG_VanillaOptions	Vanilla_Options
0	Trade	1	0	CLS	CLS	Yes

AttributeConfigurations saved.
Authorization Required

7. Authorizable Objects

The table below describes the objects that can be authorized when the Authorization mode is enabled.

Note that some of these objects are not part of the *classAuthMode* domain by default and must be added in order to make them authorizable.

▶ See Data Authorization for details on using Authorization mode.

Objects	Description
Account	Account definition. **Navigator > Configuration > Accounting > Accounts**
AccountInterestConfigRange	This is part of Account Interest Config and is not itself an authorizable object. Modifications will require AccountInterestConfig authorization.
AccountSweepingConfig	Account sweeping configuration. **Navigator > Configuration > Accounting > Sweeping**
AccountingBook	Accounting book. **Navigator > Configuration > Accounting > Books**
AccountingBookRuleLink	Accounting rule book link. **Navigator > Configuration > Accounting > Accounting Rules** > Book Link panel
AccountingEventConfig	Accounting event configuration. **Navigator > Configuration > Accounting > Accounting Events**
AccountInterestConfig	Account interest configuration. **Navigator > Configuration > Accounting > Interests**
AccountingRule	Accounting rule definition. **Navigator > Configuration > Accounting > Accounting Rules** > Definition panel
AccountingRuleAccountConfig	Accounting rule configuration. **Navigator > Configuration > Accounting > Accounting Rules** > Configuration panel
AdviceConfig	Message configuration. **Navigator > Configuration > Messages & Matching > Message Set-up**
AuditFilter	Audit filter definition.

Objects	Description
	Navigator > Configuration > Filters > Audit Filter
Benchmark	Benchmark definition for Asset Management. **Navigator > Configuration > Asset Management > Benchmark**
BillingGrid	Billing grid definition. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Fee Set Up** > Billing Grid panel
Book	Trading book definition. **Navigator > Configuration > Books & Bundles > Trading Book**
BookValCcy	Book valuation currency configuration. **Navigator > Configuration > Books & Bundles > Book Valuation Currency**
CASwiftEventCodeAttributes	Corporate action SWIFT code mapping. **Navigator > Trade Lifecycle > Corporate Action > CA Swift Event Code**
CDSIndexDefinition	CDS index definition. **Navigator > Configuration > Credit Derivatives > CDS Index Definition**
CFDContractDefinition	Contract for difference contract definition. **Navigator > Configuration > Equity > CDF Contracts**
CFDCountryGrid	Contract for difference country grid definition. **Navigator > Configuration > Equity > CDF Country Grid**
CLSPayInSchedule	Continuous Linked Settlement pay-in schedule definition. **Process > Create Schedule** or **Process > Edit Schedule** from the CLS Pay-In Schedule Report window. The CLS Pay-In Schedule Report window is not available from Navigator by default. ▶ Please refer to the *Calypso CLS Integration Guide* for details on adding the CLS Pay-In Schedule Report window.
ClearingService	Clearing service configuration for Collateral Cover Distribution. **Util > Clearing Service Configuration** from the Clearing Member Configuration window. The Clearing Member Configuration window is not available from Navigator by default. ▶ Please refer to Calypso Collateral documentation for details on

Objects	Description
	adding the Clearing Member Configuration window.
ClientOnboardingData	Client data in the Onboarding Manager for Clearing Member module. Not available from Navigator by default. ▶ Please refer to the *Calypso Clearing Member Installation and Setup Guide* for details on adding the Onboarding Manager.
CollateralConfig	Margin call contract and clearing member contract definitions. Margin Call Contract: **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call** Clearing Member Contract: Not available from Navigator by default. ▶ Please refer to Calypso Collateral documentation for details on adding the Clearing Member Configuration window.
CollateralContext	Collateral context configuration. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call**, then **Util > Collateral Context**
CollateralExposureContext	Collateral exposure context configuration. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call**, then **Util > Collateral Exposure Context**
CommodityReset	Commodity reset definition. **Navigator > Configuration > Commodities > Commodity Reset**
ConcentrationRule	Collateral concentration rule configuration. Not available from Navigator by default. ▶ Please refer to Calypso Collateral documentation for details on adding the Concentration Rule Configuration window.
ContextPosition	Context position configuration. **Navigator > Configuration > Liquidity > Liquidity Position > Context Position Setup Manager**
ContextPositionBucketConfig	Context position bucketing configuration. **Navigator > Configuration > Liquidity > Liquidity Position > Context Position Setup Manager** > Bucketing Configurations area
ContextPositionBucketScope	Context position bucketing scope. **Navigator > Configuration > Liquidity > Liquidity Position > Context Position Setup Manager** > Bucketing Scope area
ContextPositionFilter	Context position filter definition.

Objects	Description
	Navigator > Configuration > Liquidity > Liquidity Position > Context Position Setup Manager > **Context Position Filters** button The Context Position Filter window is not available from Navigator by default. ▶ Please refer to Calypso Liquidity documentation for details on adding the Context Position Filter window.
Country	Country definition. **Navigator > Configuration > Definitions > Countries**
CreditRating	Credit ratings for legal entities. **Navigator > Market Data > Credit Curves > Credit Ratings**
CurrencyDefault	Currency definition. **Navigator > Configuration > Definitions > Currency Defaults** > Currency Default panel
CurrencyPair	Currency pair definition. **Navigator > Configuration > Definitions > Currency Defaults** > Currency Pairs panel
ETLJob	ETL job for collateral reconciliation. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call**, then **Util > Reconciliation Configuration**
EligibilityExclusionConfiguration	This is part of Clearing Member Contract configuration and is not itself an authorizable object. Modifications will require CollateralConfig authorization.
EligibilityRule	Eligibility rule definition for repo trade acceptable collateral. **Navigator > Configuration > Legal Data > Eligibility Rules**
FXReset	FX rate definition. **Navigator > Configuration > Foreign Exchange > FX Rate Definitions**
FXResetPair	FX reset pair configuration. **Navigator > Configuration > Foreign Exchange > FX Reset Pairs**
FeeBillingRule	Fee billing rule definition. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Fee Billing Rule**
FeeConfig	Fee configuration for the FeeConfig calculator. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Fee**

Objects	Description
	Set Up > Fee Config panel
FeeGrid	Fee grid definition. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Fee Set Up** > Fee Grid panel
Fund	Fund and mandate definitions for Asset Management. **Navigator > Configuration > Asset Management > Fund** or **Navigator > Configuration > Asset Management > Mandate**
FutureContract	Future contract definition. **Navigator > Configuration > Listed Derivatives > Future Contracts**
FutureOptionContract	Future option contract definition. **Navigator > Configuration > Listed Derivatives > Future Option Contracts**
GlobalRatingConfiguration	Global rating configuration for Collateral module. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call**, then **Util > Global Rating Configuration**
HREnrichmentMapping	Hedge enrichment mapping for Hedge Accounting. **Navigator > Configuration > Accounting > Hedge Enrichment Mapping**
HaircutRule	Haircut rule definition. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Haircut Rule**
HeadroomCheckCollateral	Headroom Check collateral amounts. ▶ Refer to Calypso Headroom Check documentation for details.
HeadroomCheckLimit	Headroom Check limits. ▶ Refer to Calypso Headroom Check documentation for details.
HedgeAccountingScheme	Hedge accounting scheme definition. **Navigator > Configuration > Accounting > Hedge Accounting Scheme**
HedgeDefinition	Hedge definition for Hedge Accounting. **Navigator > Configuration > Accounting > Hedge Definition**
HedgePricerMeasureMapping	Hedge pricer measure mapping for Hedge Accounting. **Navigator > Configuration > Accounting > Hedge Pricer Measure Mapping**

Objects	Description
HedgeRelationship	Hedge relationship for Hedge Accounting. **Navigator > Trade Lifecycle > Hedge > Hedge Relationship Details**
HedgeRelationshipConfiguration	Hedge relationship configuration for Hedge Accounting. **Navigator > Trade Lifecycle > Hedge > Hedge Relationship Details**
HedgeRelationshipDefinition	Hedge relationship definition for Hedge Accounting. **Navigator > Trade Lifecycle > Hedge > Hedge Relationship Details**
Holiday	"Holiday" makes both holiday calendars and holiday rules authorizable. See HolidayCode and HolidayRule below.
HolidayCode	Holiday calendar definition. "Holiday" must be added for holiday calendars to be authorizable. Modifications will require both Holiday and HolidayCode authorization. **Navigator > Configuration > Definitions > Holiday Calendars** > Codes label
HolidayRule	Holiday rule definition. "Holiday" must be added for holiday rules to be authorizable. Modifications will require HolidayRule authorization. **Navigator > Configuration > Definitions > Holiday Calendars** > Rules label
IntradayConfiguration	Intraday policy configuration for commodity derivatives trading. **Navigator > Configuration > Commodities > Intraday Configuration**
KickOffCutOffConfig	Workflow kickoff cutoff configuration. **Navigator > Configuration > Workflow > Kick-Off/Cut-Off**
LEContact	Legal entity contact details. **Navigator > Configuration > Legal Data > Contact Personnel**
LERegistration	Legal entity registration details. **Navigator > Configuration > Legal Data > Registration Details**
LEUserAccessRelation	Legal entity and group associations for eSelfService users. **Navigator > Configuration > User Access Control > Access Permissions** > Data Segregation panel
LegalAgreement	Legal agreement definition. **Navigator > Configuration > Legal Data > Agreements**
LegalEntity	Legal entity definition. **Navigator > Configuration > Legal Data > Entities**

Objects	Description
LegalEntityAttribute	Legal entity attribute details. **Navigator > Configuration > Legal Data > Attributes**
LegalEntityRelation	Legal entity relation details. **Navigator > Configuration > Legal Data > Relation**
LegalEntityTolerance	Payment amount tolerance when matching imported payment messages for a given legal entity. **Navigator > Configuration > Legal Data > Tolerance**
LiabilityGroupContext	Liability group configuration for Collateral Cover Distribution. **Util > Liability Group Configuration** from the Clearing Member Configuration window. The Clearing Member Configuration window is not available from Navigator by default. ▶ Please refer to Calypso Collateral documentation for details on adding the Clearing Member Configuration window.
LiqLimitBase	Liquidity limit definition. **Navigator > Configuration > Liquidity > Limit Configuration Manager**
LiqLimitCcyBucket	Liquidity 'Currency & Bucket' limit definition. **Navigator > Configuration > Liquidity > Limit Configuration Manager**
LiqLimitCcyClassificationLevel	Liquidity 'Currency & Classification Level' limit definition. **Navigator > Configuration > Liquidity > Limit Configuration Manager**
LiqLimitCcyClassificationLevelBucket	Liquidity 'Currency, Classification Level & Bucket' limit definition. **Navigator > Configuration > Liquidity > Limit Configuration Manager**
LiquidationConfig	Liquidation configuration. **Navigator > Configuration > Books & Bundles > Liquidation** > ✏ from Liquidation Config column
MCCBagTol	Market Conformity bagatelle tolerance configuration. Market Conformity Configuration window > Bagatelle Tolerances panel The Market Conformity Configuration window is not available from Navigator by default.

Objects	Description
	▶ Please refer to Calypso Market Conformity documentation for details on adding the Market Conformity Configuration window.
MCCIntradayParamConfig	Market Conformity intraday market data configuration. Market Conformity Configuration window > Intraday Market Data Settings panel The Market Conformity Configuration window is not available from Navigator by default. ▶ Please refer to Calypso Market Conformity documentation for details on adding the Market Conformity Configuration window.
MCCNPVTol	Market Conformity market tolerance configuration. Market Conformity Configuration window > Market Tolerances panel The Market Conformity Configuration window is not available from Navigator by default. ▶ Please refer to Calypso Market Conformity documentation for details on adding the Market Conformity Configuration window.
MCCProductConfig	Market Conformity product configuration. Market Conformity Configuration window > Products panel The Market Conformity Configuration window is not available from Navigator by default. ▶ Please refer to Calypso Market Conformity documentation for details on adding the Market Conformity Configuration window.
MCCTimeTol	Market Conformity time tolerance configuration. Market Conformity Configuration window > Time Tolerances panel The Market Conformity Configuration window is not available from Navigator by default. ▶ Please refer to Calypso Market Conformity documentation for details on adding the Market Conformity Configuration window.
ManualPosting	Manual posting details. **Navigator > Processing > Manual Posting**
ManualSDI	Manual settlement instruction definition. **Navigator > Configuration > Settlements > Manual SDI**
MarginCallConfig	Not used. See CollateralConfig.
MarginCallCreditRatingConfiguration	Margin call credit rating configuration for Collateral module.

Objects	Description
	Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call, then **Util > Global Rating Configuration**, then **Util > Margin Call Rating**
MasterConfirmation	Master confirmation definition. **Navigator > Configuration > Messages & Matching > Master Confirmations**
MatchingAlias	Matching alias definition. **Navigator > Configuration > Messages & Matching > Matching Alias**
MessageGroup	Message group definition. **Navigator > Configuration > Messages & Matching > Message Group**
MessageRule	Message rule definition. **Navigator > Configuration > Messages & Matching > Message Rule**
NettingMethod	Netting method configuration. **Navigator > Configuration > Settlements > Netting Method**
OptimizationConfiguration	Collateral optimization configuration. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call**, then **Util > Optimization Configuration**
PaymentSetup	Valid payment configurations. **Navigator > Configuration > Workflow > Valid Payment Setup**
PLMark	PL marks created by the scheduled task EOD_CAPLMARKING. **Navigator > Position & Risk > P&L Mark > P&L Mark Report**
PeriodDistribution	Period distribution configuration for commodities intraday policies. **Navigator > Configuration > Commodities > Period Distribution**
PortfolioSwapContract	Portfolio swap contract definition. **Navigator > Configuration > Equity > Portfolio Swap Contract**
PricerConfig	Pricer configurations. **Navigator > Market Data > Pricing Environment > Pricer Configuration**
Product	Objects that extend the Product class are authorizable. You need to add a class (i.e. Equity or BondMMDiscount) to the *classAuthMode* domain to make it authorizable.

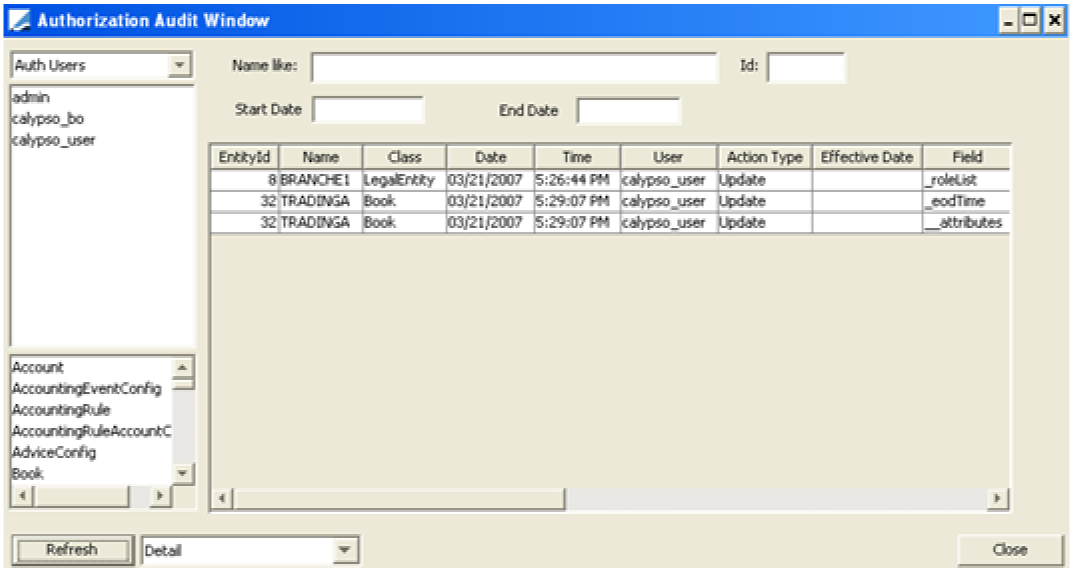
Objects	Description
QuoteValue	Saved market quote values. **Navigator > Market Data > Market Quotes > Quotes**
RateIndexDefaults	Rate index definition. **Navigator > Configuration > Interest Rates > Rate Index Definitions**
ReferenceEntityBasket	Reference entity basket definition. **Navigator > Configuration > Credit Derivatives > Reference Entity Basket**
ReferenceEntityTranche	(Reference entity basket) tranche definition. **Navigator > Configuration > Credit Derivatives > Reference Entity Basket** > Tranches panel > **Add** button
SDIRelationShip	SDI relationship configuration between a beneficiary and an intermediary. **Navigator > Configuration > Settlements > Delivery Instructions**, then **Utilities > SDI RelationShip**
SelfAdminClient	Changes made in eSelfService by client administrators. ▶ Refer to Calypso eSelfService documentation for details.
SelfAdminUser	Changes made in eSelfService by end users. ▶ Refer to Calypso eSelfService documentation for details.
SettleDeliveryInstruction	Settlement and delivery instruction definition. **Navigator > Configuration > Settlements > Delivery Instructions**
SettlementMessageSending	Settlement message sending configuration.
SettlementMethod	The possible settlement methods and the info in order for a settlement method to be used. Only valid in case the SDISelector is set to SDISelectorAlternate.
SftrConfigurationField	SFTR (Securities Financing Transaction Regulation) Configuration Table fields. **Navigator > Deal Management > Sec Finance Trade Report > Securities Financing Transaction Regulation > SFTR Configuration Table**
StatementConfig	Security lending billing statement configuration. **Navigator > Configuration > Messages & Matching > Statement Config**
StaticDataFilter	Static data filter definition.

Objects	Description
	Navigator > Configuration > Filters > Static Data Filter
SubstitutionFacade	This is part of Margin Call Contract configuration and is not itself an authorizable object. Modifications will require CollateralConfig authorization.
SwiftMessageMappingConfiguration	SWIFT message mapping configuration. Used for Triparty Repo MT527 messages. **Navigator > Configuration > Messages & Matching > Swift Message Mapping Config**
TargetConfiguration	Collateral optimization target configuration. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Margin Call**, then **Util > Optimization Configuration**, then **Util > Target Configuration**
TaskWorkflowConfig	Workflow transition configuration. **Navigator > Configuration > Workflow > Workflow**
Trade	Trade authorization requires additional setup. ▶ Please refer to Calypso Workflow documentation for details.
TriangulationCcyRuleSet	Triangulation currency rule definition. **Navigator > Configuration > Definitions > Triangulation Ccy Rule Set Manager**
UserAccessPermission	User access permission configuration. **Navigator > Configuration > User Access Control > Access Permissions**
WithholdingTaxAttribute	Withholding tax attribute definition. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Withholding Tax Attribute**
WithholdingTaxConfig	Withholding tax configuration. **Navigator > Configuration > Fees, Haircuts, & Margin Calls > Withholding Tax Config**
WrongWayRiskGroup	Wrong way risk group definition. The Wrong Way Risk Group window is not available from Navigator by default. ▶ Please refer to Calypso Haircut Rules documentation for details on adding the Wrong Way Risk Group window.

8. Data Authorization Audit

The Data Authorization Audit window allows viewing the history of authorizations provided the STORE_PENDING_MODIF_HISTORY environment property is true.

Choose **Calypso Navigator > Reports > Audit > Data Authorization Audit** (menu action `refdata.AuthorizationAuditWindow`) to view the history of authorizations. The Data Authorization Audit window will appear as shown below.



EntityId	Name	Class	Date	Time	User	Action Type	Effective Date	Field
8	BRANCHE1	LegalEntity	03/21/2007	5:26:44 PM	calypso_user	Update		_roleList
32	TRADINGA	Book	03/21/2007	5:29:07 PM	calypso_user	Update		_eodTime
32	TRADINGA	Book	03/21/2007	5:29:07 PM	calypso_user	Update		__attributes

» Select Users or Groups from the field in the upper-left corner. Then select a user or a group from the list as applicable, to filter the authorizations for that user or group. Select a class from the list at the lower-left corner as applicable, to filter the authorizations for that class.

You can also specify one or more characters in the "Name like" field to filter entity names that start with these characters.

Then click **Refresh** to load the authorizations for the specified criteria.

Note that only authorizations that have been made after the environment property STORE_PENDING_MODIF_HISTORY is set to true will appear. Or you can enter an object id in the Id field to load an individual object.

» Select Detail or Version from the field next to the **Refresh** button to display the authorizations per version, or to show the individual modifications. There will only be a difference when multiple changes have been made to a given entity version.

» Click **Close** when you are done.

9. Data Auditing

The system runs in Audit mode: any change to any data is stored to the database, and versioning is applied to the modified data so that users can compare different versions of data. In particular, it allows reconstructing trades as they existed at a particular point in time.

The version number of data is only incremented if the data has actually been modified. If you save a data multiple times without making any change, the version number will remain the same.

Changes to trade data are saved individually for each version, and changes to other types of data are saved by version.

Audit Mode

The Audit mode only applies to classes specified in the *classAuditMode* domain. You can remove a given class from that domain as applicable using **Calypso Navigator > Configuration > System > Domain Values** (menu action `refdata.DomainValueWindow`) to disable the Audit mode for that class.

Restricted Audit Views

You can also restrict a particular group from viewing audit data:

- » Add one or more audit classes (see the *classAuditMode* domain) to restrict to the *auditReportRestrictable* domain using **Calypso Navigator > Configuration > System > Domain Values** (menu action `refdata.DomainValueWindow`).
- » On the Group Access tab of the Access Window, select the group to have the viewing restriction.
- » Select "Audit Report Restriction" under the Access label.
- » Click **Add Read Only**.
- » From the dialog, select the audit classes that the chosen group may not view. Use the arrow buttons to move items between panes.
- » Click **OK** to accept the selection or click **Cancel** to discard your changes.
- » Click **Save** on the Access Window.

Audit Quote Schemes

Note that different audit schemes can be set up for Quotes. In the domain *classAuditMode*, you can choose between the following values:

- QuoteValue: Default behavior – Audit is only triggered when a CLOSE quote is modified.
- QuoteValue and QuoteValue_InsertDelete – Audit is triggered when a CLOSE quote is added, modified, or removed.
- QuoteValue and QuoteValue_AllInstances – Audit is triggered when any quote is modified (unless QUOTE_AUDIT_CLOSE_B is true, in which case only CLOSE quotes are audited).

- QuoteValue, QuoteValue_InsertDelete, and QuoteValue_InsertDelete – Audit is triggered when any quote is added, modified, or removed (unless QUOTE_AUDIT_CLOSE_B is true, in which case only CLOSE quotes are audited).

▶ Refer to the *Calypso Developer's Guide* for information on making a class auditable.

Note that to disable the Audit mode for the whole system, you just need to clear the Audit checkbox in any of the above-mentioned applications.

9.1 Trade Audit Report

The Trade Audit Report displays trades based on the user permissions. A user can only view those trades for which he has permission. This requires no additional configuration.

To audit new and modified data, choose **Calypso Navigator > Reports > Audit > Trade Audit** (menu action `reporting.ReportWindow$TradeAudit`).

» Begin by choosing search criteria. You can specify the Trade ID, choose a Trade Filter, Bundle, User Group, or enter a Start/End Date range, as well as choose specific Trade Actions to exclude from the report.

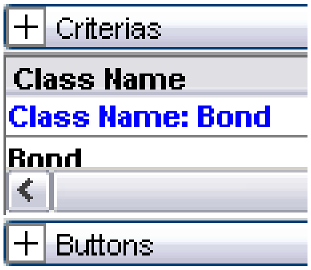
» Then click ➡ to load the audit data corresponding to the selected criteria.

You can double-click a row to view the corresponding version of the object.

Example: You have 7 versions of a Trade in Audit, and version 5 has three modifications. When you double-click one of the version 5 changes, the system will undo all of version 6 changes and all of version 7 changes, and will only undo the selected change in version 5.

» Click 🖨 to print the report results.

» Click ⊟ to collapse the Criteria or Buttons areas as shown below.

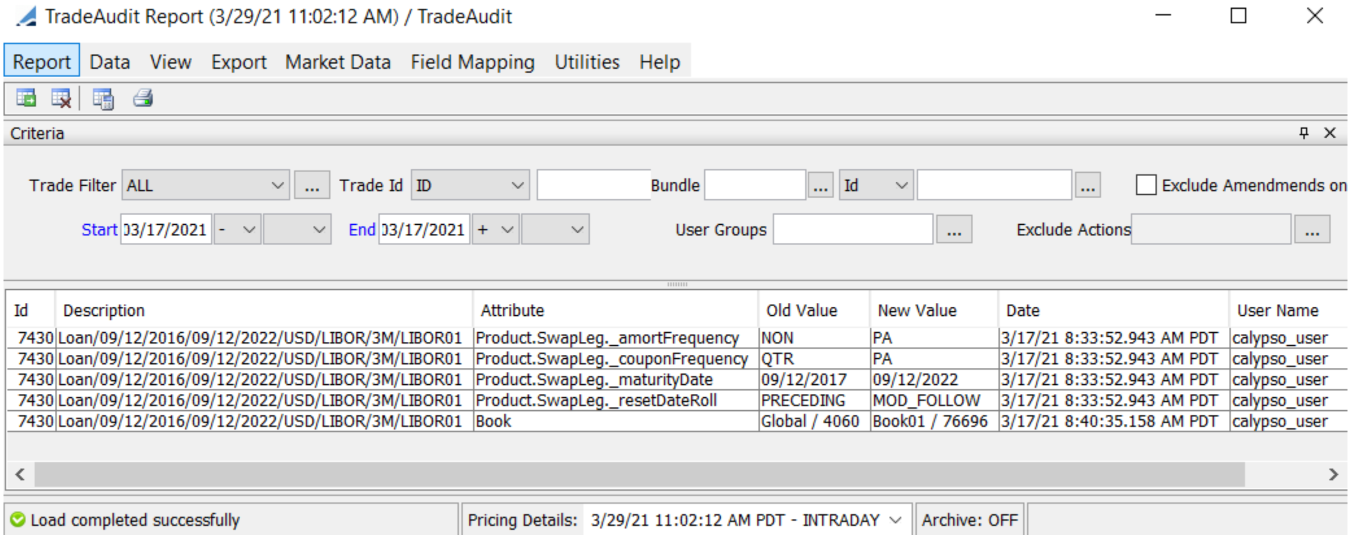


Or click ⊞ to expand the Criteria or Buttons areas.

» Choose **Help > Menu Item** for details on the menus.

To view a report of Today's audit entries when using the Scheduled Task report, define a template having the following tenors:

- Start Date Tenor: -0D
- End Date Tenor: +0D



Trade Filter ALL | Trade Id ID | Bundle | Id | □ Exclude Amendmends on

Start 03/17/2021 - | End 03/17/2021 + | User Groups | Exclude Actions

Id	Description	Attribute	Old Value	New Value	Date	User Name
7430	Loan/09/12/2016/09/12/2022/USD/LIBOR/3M/LIBOR01	Product.SwapLeg._amortFrequency	NON	PA	3/17/21 8:33:52.943 AM PDT	calypso_user
7430	Loan/09/12/2016/09/12/2022/USD/LIBOR/3M/LIBOR01	Product.SwapLeg._couponFrequency	QTR	PA	3/17/21 8:33:52.943 AM PDT	calypso_user
7430	Loan/09/12/2016/09/12/2022/USD/LIBOR/3M/LIBOR01	Product.SwapLeg._maturityDate	09/12/2017	09/12/2022	3/17/21 8:33:52.943 AM PDT	calypso_user
7430	Loan/09/12/2016/09/12/2022/USD/LIBOR/3M/LIBOR01	Product.SwapLeg._resetDateRoll	PRECEDING	MOD_FOLLOW	3/17/21 8:33:52.943 AM PDT	calypso_user
7430	Loan/09/12/2016/09/12/2022/USD/LIBOR/3M/LIBOR01	Book	Global / 4060	Book01 / 76696	3/17/21 8:40:35.158 AM PDT	calypso_user

Load completed successfully | Pricing Details: 3/29/21 11:02:12 AM PDT - INTRADAY | Archive: OFF

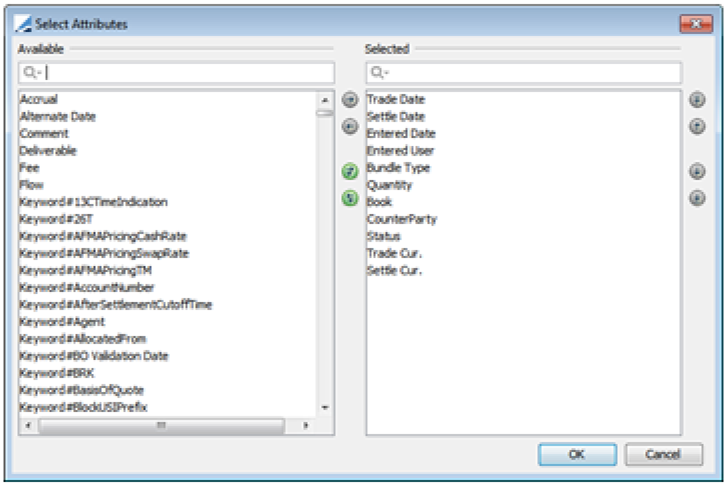
Trade Audit Report

Adding Attributes

[NOTE: To show all results, do not select any mapping attribute. If some mapping attributes are selected, only the results for those attributes are shown]

» Choose **Field Mapping > Configure Attributes** to access the Select Attributes Chooser.

Use the arrow buttons to move fields between the "Available" and "Selected" pane. The fields in the "Selected" pane appear as columns in your Trade Audit Report:



Available

Accrual
Alternate Date
Comment
Deliverable
Fee
Flow
Keyword#13CTimeIndication
Keyword#26T
Keyword#AFMAPricingCashRate
Keyword#AFMAPricingSwapRate
Keyword#AFMAPricingTM
Keyword#AccountNumber
Keyword#AfterSettlementCutoffTime
Keyword#Agent
Keyword#AllocatedFrom
Keyword#BO Validation Date
Keyword#BRK
Keyword#BasisOfQuote
Keyword#BlockUSIPrefix

Selected

Trade Date
Settle Date
Entered Date
Entered User
Bundle Type
Quantity
Book
CounterParty
Status
Trade Cur.
Settle Cur.

Click **OK** when you are done selecting fields.

» You can use the Audit Mappings Window to map the internal Calypso column name to a user-friendly version for use in the report. Select **Field Mappings > View Mappings** to open the Audit Mappings Window. Note that you can add field mappings specific to a Product Family/Product Type by defining a mapping using a Product Name and Product Type.

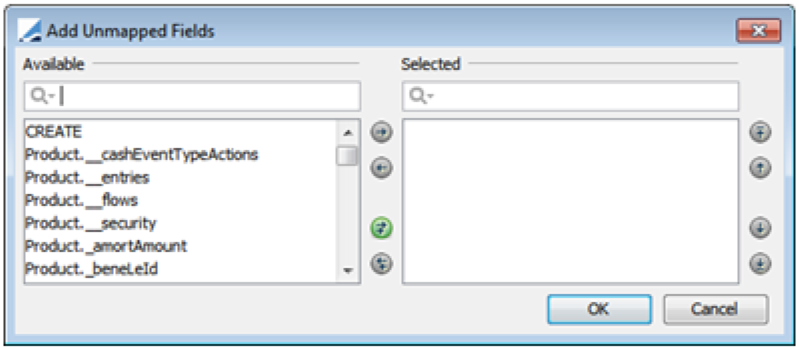
To add a new Mapping, enter the Display Name for use in the Report, add the Audit Field Name, and optionally, enter a Product Family and Product Type if this mapping is for a specific Product Family/Type. Click **Add** to add the new row to the table. Click **Save** to save the new entry.

You can also remove an existing row by selecting it and then clicking **Remove**.

Click **Close** to exit the window.

Adding Unmapped Fields

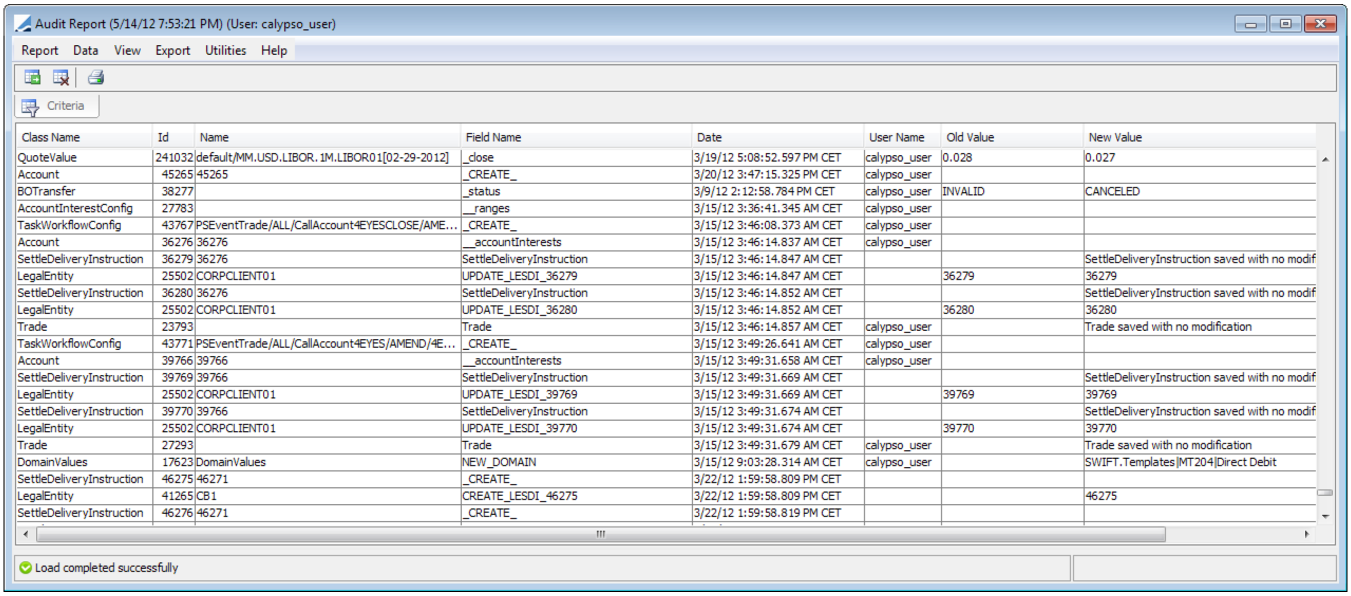
You can select **Field Mappings > Add Unmapped Fields** to add an unmapped field to the report. From the Unmapped Fields window:



Select a field from the "Available" pane and then use the arrow buttons to move the field to the "Selected" pane. Click **OK** to save and close the window.

9.2 Audit Report

To audit new and modified data, choose **Calypso Navigator > Reports > Audit > Audit Report** (menu action `reporting.ReportWindow$Audit`).



Class Name	Id	Name	Field Name	Date	User Name	Old Value	New Value
QuoteValue	241032	default/MM.USD.LIBOR.1M.LIBOR01[02-29-2012]	_close	3/19/12 5:08:52.597 PM CET	calypso_user	0.028	0.027
Account	45265	45265	_CREATE_	3/20/12 3:47:15.325 PM CET	calypso_user		
BOTransfer	38277		_status	3/9/12 2:12:58.784 PM CET	calypso_user	INVALID	CANCELED
AccountInterestConfig	27783		__ranges	3/15/12 3:36:41.345 AM CET	calypso_user		
TaskWorkflowConfig	43767	PSEventTrade/ALL/CallAccount4EYESCLOSE/AME...	_CREATE_	3/15/12 3:46:08.373 AM CET	calypso_user		
Account	36276	36276	__accountInterests	3/15/12 3:46:14.837 AM CET	calypso_user		
SettleDeliveryInstruction	36279	36276	SettleDeliveryInstruction	3/15/12 3:46:14.847 AM CET			SettleDeliveryInstruction saved with no modif
LegalEntity	25502	CORPCLIENT01	UPDATE_LESDI_36279	3/15/12 3:46:14.847 AM CET		36279	36279
SettleDeliveryInstruction	36280	36276	SettleDeliveryInstruction	3/15/12 3:46:14.852 AM CET			SettleDeliveryInstruction saved with no modif
LegalEntity	25502	CORPCLIENT01	UPDATE_LESDI_36280	3/15/12 3:46:14.852 AM CET		36280	36280
Trade	23793		Trade	3/15/12 3:46:14.857 AM CET	calypso_user		Trade saved with no modification
TaskWorkflowConfig	43771	PSEventTrade/ALL/CallAccount4EYES/AMEND/4E...	_CREATE_	3/15/12 3:49:26.641 AM CET	calypso_user		
Account	39766	39766	__accountInterests	3/15/12 3:49:31.658 AM CET	calypso_user		
SettleDeliveryInstruction	39769	39766	SettleDeliveryInstruction	3/15/12 3:49:31.669 AM CET			SettleDeliveryInstruction saved with no modif
LegalEntity	25502	CORPCLIENT01	UPDATE_LESDI_39769	3/15/12 3:49:31.669 AM CET		39769	39769
SettleDeliveryInstruction	39770	39766	SettleDeliveryInstruction	3/15/12 3:49:31.674 AM CET			SettleDeliveryInstruction saved with no modif
LegalEntity	25502	CORPCLIENT01	UPDATE_LESDI_39770	3/15/12 3:49:31.674 AM CET		39770	39770
Trade	27293		Trade	3/15/12 3:49:31.679 AM CET	calypso_user		Trade saved with no modification
DomainValues	17623	DomainValues	NEW_DOMAIN	3/15/12 9:03:28.314 AM CET	calypso_user		SWIFT.Templates|MT204|Direct Debit
SettleDeliveryInstruction	46275	46271	_CREATE_	3/22/12 1:59:58.809 PM CET			
LegalEntity	41265	CB1	CREATE_LESDI_46275	3/22/12 1:59:58.809 PM CET			46275
SettleDeliveryInstruction	46276	46271	_CREATE_	3/22/12 1:59:58.819 PM CET			

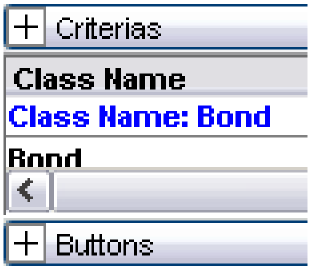
Load completed successfully

[NOTE: The columns of this picture have been configured. Sort columns, subheadings and subtotals have to be explicitly specified - See Help > Menu Item for details]

- Select the type of audit data you wish to load from the Type field, or ALL. You can also specify an entity id as applicable (for example, trade id, legal entity id, etc). Select a user name from the User Name field, and enter start and end dates as applicable.
- Then click to load the audit data corresponding to the selected criteria.

  You can double-click a row to view the corresponding version of the object.

  For example, you have 7 versions of a Trade in Audit, and version 5 has three modifications. When you double-click one of the version 5 changes, the system will undo all of version 6 changes and all of version 7 changes, and will only undo the selected change in version 5.
- Click to print the report results.
- Click ⊟ to collapse the Criteria or Buttons areas as shown below.



  Or click ⊞ to expand the Criteria or Buttons areas.
- Choose **Help > Menu Item** for details on the menus.

NOTE: To view a report of Today's audit entries when using the Scheduled Task report, define a template having the following tenors:

- Start Date Tenor: -0D
- End Date Tenor: +0D

9.3 Limiting BOAudit Report Results

In a high-volume implementation, the number of records returned by the BOAudit Report can cause the system to appear frozen. To limit the number of records that are returned to a user or group, follow the procedure below:

▶ See "Max.BOAudit" under Creating and Editing Users to verify that the Max.BOAudit setting is available. If not, create the entry as explained in that section.

» On the Access Window's Users tab, select a user.

» Click **Permission Attributes**.

» In the dialog, double-click in the Value column next to "Max.BOAudit" and then enter the maximum number of BOAudit records to return.

» Click **Close**.

» To save the setting for a single user, click **Save** on the Users tab.

If after saving to a specific user, you wish to apply that setting to an entire group, click **Apply to Group**, then select the group(s). Click **OK** to apply the "Max.BOAudit" value to the entire group or **Cancel** to abandon the group change.