

CAPLIN

Caplin Trader 2.5

Permissioning Configuration XML Reference

March 2012

CONFIDENTIAL

Contents

1	Preface.....	1
1.1	What this document contains.....	1
	About Caplin document formats	1
1.2	Who should read this document.....	1
1.3	Related documents.....	2
1.4	Typographical conventions	3
1.5	Feedback.....	3
1.6	Acknowledgments.....	3
2	Getting started.....	4
2.1	Technical assumptions and restrictions.....	4
2.2	An example configuration file.....	4
2.3	Configuring TOBO permissioning namespaces.....	5
3	XML Reference information.....	7
3.1	Ordering and nesting of tags.....	7
3.2	XML tag descriptions.....	8
	<permissionDatasourceDefinitions>	8
	<permissionsource>	8
	<salesUserOnlyNamespace>	8
	<tobo>	9

1 Preface

1.1 What this document contains

This reference document describes the XML-based permissioning configuration used in Caplin Trader version 2.5.2 and later.

Note: To successfully deploy permissioning using the XML schema described in this document, you must also deploy one or more *compatible* Permissioning DataSources. For more information about this, see **Subscribing to Multiple Permissioning DataSources** in the document **Caplin Trader: How To Add Permissioning At The Client**.

About Caplin document formats

This document is supplied in three formats:

- ◆ Portable document format (*.PDF* file), which you can read on-line using a suitable PDF reader such as Adobe Reader®. This version of the document is formatted as a printable manual; you can print it from the PDF reader.
- ◆ Web pages (*.HTML* files), which you can read on-line using a web browser. To read the web version of the document, navigate to the *HTMLDoc* folder and open the file *index.html*.
- ◆ Microsoft HTML Help (*.CHM* file), which is an HTML format contained in a single file. To read a *.CHM* file just open it – no web browser is needed.

For the best reading experience

On the machine where your browser or PDF reader runs, install the following Microsoft Windows® fonts: Arial, Courier New, Times New Roman, Tahoma. You must have a suitable Microsoft license to use these fonts.

Restrictions on viewing *.CHM* files

You can only read *.CHM* files from Microsoft Windows.

Microsoft Windows security restrictions may prevent you from viewing the content of *.CHM* files that are located on network drives. To fix this either copy the file to a local hard drive on your PC (for example the Desktop), or ask your System Administrator to grant access to the file across the network. For more information see the Microsoft knowledge base article at <http://support.microsoft.com/kb/896054/>.

1.2 Who should read this document

This document is intended for System Administrators and Software Developers who need to configure permissioning in Caplin Trader.

1.3 Related documents

- ◆ **Caplin Xaqua: Permissioning Overview And Concepts**

Introduces permissioning concepts and terms, and shows the permissioning components of the Caplin Xaqua architecture.

- ◆ **Caplin Trader: How To Add Permissioning At The Client**

Describes how to add permissioning to Caplin Trader so that display components behave in accordance with the permissions of the logged in user.

- ◆ **Caplin Trader: API Reference**

The API reference documentation provided with Caplin Trader. The classes and interfaces of the `caplin.security.permissioning` package allow you to write JavaScript classes that extend the live permissioning capabilities of Caplin Trader.

- ◆ **Caplin Xaqua: How To Create A Permissioning DataSource**

Describes how to create a Permissioning DataSource adapter using the Permissioning DataSource API. A Permissioning DataSource adapter is required to integrate Caplin Xaqua with a Permissioning System.

- ◆ **Permissioning DataSource: API Reference**

The API reference documentation provided with the Permissioning DataSource SDK (Software Development Kit). The classes and interfaces presented by this API allow you to write a Java application that will integrate a Permissioning System with Caplin Xaqua.

1.4 Typographical conventions

The following typographical conventions are used to identify particular elements within the text.

Type	Uses
<i>/AFolder/Afile.txt</i>	File names, folders and directories
<div>Some code;</div>	Program output and code examples
value	XML tag and attribute names
XYZ Product Overview	Document name
◆	Information bullet point
■	Action bullet point – an action you should perform

Note: Important Notes are enclosed within a box like this.
Please pay particular attention to these points to ensure proper configuration and operation of the solution.

Tip: Useful information is enclosed within a box like this.
Use these points to find out where to get more help on a topic.

Information about the applicability of a section is enclosed in a box like this.
For example: “This section only applies to version 1.3 of the product.”

1.5 Feedback

Customer feedback can only improve the quality of our product documentation, and we would welcome any comments, criticisms or suggestions you may have regarding this document.

Visit our feedback web page at <https://support.caplin.com/documentfeedback/>.

1.6 Acknowledgments

Adobe® Reader is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

2 Getting started

2.1 Technical assumptions and restrictions

XML

The XML markup defined in this document conforms to XML version 1.0 and the XML schema version defined at <http://www.w3.org/2001/XMLSchema>.

2.2 An example configuration file

The Permissioning configuration XML for Caplin Trader defines the Permissioning DataSources that the Caplin Trader client must subscribe to in order to receive permissioning data. This is shown in the following example, which specifies one master and two slave Permissioning DataSources:

Example Permissioning configuration XML in Caplin Trader:

```
<?xml version="1.0"?>
<permissionDataSourceDefinitions
  xmlns="http://schema.caplin.com/Security/permissions">
  <permissionsource name="MASTER" role="Master"/>
  <permissionsource name="SLAVE1" />
  <permissionsource name="SLAVE2" />
</permissionDataSourceDefinitions>
```

The name of the master must always be "MASTER", and its role must be set to "master". The name of a slave must match the name of the Permissioning DataSource that provides the permissioning data (note that if the role attribute of the <permissionsource> tag is not specified it defaults to "Slave").

In this example Caplin Trader subscribes to permissioning data from the following containers:

/PERMISSIONS/MASTER/CONTAINER/<username>

/PERMISSIONS/SLAVE1/CONTAINER/<username>

/PERMISSIONS/SLAVE2/CONTAINER/<username>

where <username> is the logged in user.

Tip: Each permissioning container is mapped to a Permissioning DataSource in the Liberator configuration. See **Configuring Liberator to connect to multiple Permissioning DataSources** in the document **Caplin Xaqua: Installing Permissioning Components** for further information.

The location of the XML configuration file is specified by setting the application property **CAPLIN.PERMISSION.CONFIG.URL** in the file *Application.jsp*.

Example configuration file specification

```
caplin.core.ApplicationProperties.setProperty(  
    "CAPLIN.PERMISSION.CONFIG.URL",  
    "conf/permissionDataSourceDefinitions.xml");
```

Note: If the permissioning configuration XML file is not defined (or is invalid), Caplin Trader will subscribe to the permissioning container called `/PERMISSIONS/CONTAINER/<username>`. This allows legacy client applications that do not subscribe to multiple Permissioning DataSources to continue working without modification if the Caplin Trader library is upgraded.

If the permissioning configuration XML file is invalid, permissioning error messages will be logged to the console log. End users will be able to log in to Caplin Trader but will not be able to view or trade instruments.

Tip: For more information about how to set up permissioning in Caplin Trader, see **Caplin Trader: How To Add Permissioning At The Client**.

2.3 Configuring TOBO permissioning namespaces

When a logged in user is 'trading on behalf of' (TOBO) another user, the permissions that are sent to and cached by the permissioning library depend on the permissioning mode the Permissioning Auth Module is configured to run in.

If the permissioning mode is **SalesUser**, only permissions for the logged in user are sent to the permissioning library. In this mode the library methods that return product permissions always return permissions for the logged in user.

If the permissioning mode is **SalesIntersectCustomerUser**, permissions for both the logged in user and the user they are trading on behalf of are sent to and cached by the permissioning library. In this mode the permissions returned by the permissioning library are the logical AND of the logged in user and the user they are trading on behalf of.

This allows the application to modify the user interface according to returned permissions, such as to enable or disable trade tiles or tickets when the logged in user is trading on behalf of another user. However, there are situations when only the permissions of the logged in user are wanted.

An example is when the logged in user is trading on behalf of user 'A' and the application wants to get permissions that list the other users the logged in user can trade on behalf of, perhaps to populate an on-screen widget. Because user 'A' will not be permitted to trade on behalf of any other user, the library must only return permissions for the logged in user, even when the permissioning mode is **SalesIntersectCustomerUser**.

The `<tobo>` tag and child `<salesUserOnlyNamespace>` tags allow you to define permissioning namespaces in which permissions returned by the permissioning library are always for the logged in user. The following example XML configuration sets up two such namespaces.

```
...  
<tobo>  
    <salesUserOnlyNamespace>ToboUserList</salesUserOnlyNamespace>  
    <salesUserOnlyNamespace>ToboUserSwitch</salesUserOnlyNamespace>  
</tobo>  
...
```

In this example, `ToboUserList` could be a namespace containing the list of users the logged in user can trade on behalf of, and `ToboUserSwitch` a namespace containing a permission that can be switched to allow or deny the logged in user to trade on behalf of any other user.

For further information about these XML tags, see the [XML Reference information](#) .

For further information about adding permissioning to a Caplin Trader client application, refer to the document **Caplin Trader: How To Add Permissioning At The Client**.

For further information about permissioning concepts and terms, including the terms that relate to TOBO, refer to the document **Caplin Xaqua: Permissioning Overview And Concepts**.


3 XML Reference information

This is the XML reference information for the Element Renderer.

3.1 Ordering and nesting of tags

Each top level tag is shown below, together with the child tags that it can contain.

Tip: Advanced users may wish to consult the XML Schema in *permissionDatasourceDefinitions.rnc* for definitive information about the ordering and nesting of tags. This file is supplied with the permissioning software for Caplin Trader.

For a description of each tag and its attributes, see [XML tag descriptions](#) .

<permissionDatasourceDefinitions>

This is the outermost tag.

```
<permissionDatasourceDefinitions>
  <permissionsource> (zero or more)
  <tobo> (zero or one)
</permissionDatasourceDefinitions>
```

<tobo>

```
<tobo>
  <salesUserOnlyNamespace></salesUserOnlyNamespace> (one or more)
</tobo>
```

<salesUserOnlyNamespace>

```
<salesUserOnlyNamespace>
  text
</salesUserOnlyNamespace>
```

3.2 XML tag descriptions

This section describes the XML tags that you can use to configure permissioning in Caplin Trader.

For each tag, the attributes you can use are listed and described in a table. The "Req?" column indicates whether the attribute is always required ("Y") or is optional ("N"). If you do not supply an optional attribute then the default value is applied.

<permissionDataSourceDefinitions>

```
<permissionDataSourceDefinitions>
```

The outermost tag of the Permissioning DataSource XML definitions, containing one or more optional <permissionsource> tags, and an optional <tobo> tag.

Attributes: This tag has no attributes.

<permissionsource>

```
<permissionsource>
```

Specifies a single Permissioning DataSource that determines the name of a permissioning data container that is requested from Liberator. If this tag is omitted, the Caplin Trader application uses a single Permissioning DataSource whose name is "MASTER" and whose role is "Master" (the container name is therefore "/PERMISSIONS/MASTER/CONTAINER/<username>"). Only one instance of a <permissionsource> whose 'role' attribute is set to "Master" can be defined.

Attributes:

Name	Type	Default	Req?	Description
name	string	(none)	Y	The name of the Permissioning DataSource. This name is used in the request for the permissioning data container. This attribute must be set to "MASTER" if the 'role' attribute is set to "Master".
role	string	Slave	N	The role of the Permissioning DataSource. Valid values are "Master" or "Slave".

<salesUserOnlyNamespace>

```
<salesUserOnlyNamespace>
```

A child of the <tobo> tag, this tag specifies a permissioning namespace.

When the Caplin Trader application requests permissions that reside in this namespace, the returned permissions are for the logged in user only, even if that user is trading on behalf of another user and the mode of the Permissioning Auth Module is 'SalesIntersectCustomerUser'.

Attributes: This tag has no attributes.

<tobo>

<tobo>

An optional list of permissioning namespaces, each defined by a child <salesUserOnlyNamespace> tag.

When the Caplin Trader application requests permissions that reside in any of these namespaces, the returned permissions are for the logged in user only, even if that user is trading on behalf of another user and the mode of the Permissioning Auth Module is 'SalesIntersectCustomerUser'.

For all other permissioning namespaces, when the mode is 'SalesIntersectCustomerUser', the returned permissions are the logical AND of the logged in user and the user they are trading on behalf of. The "TradeOnBehalfOf" and "ToboEnabled" namespaces are added to this list by default.

For further information about using this tag, see "Configuring TOBO permissioning namespaces" in this document. For a description of the "TradeOnBehalfOf" and "ToboEnabled" namespaces, refer to the document "Caplin Xaqua: Permissioning Overview And Concepts".

Attributes: This tag has no attributes.

Contact Us

Caplin Systems Ltd
Cutlers Court
115 Houndsditch
London EC3A 7BR
Telephone: +44 20 7826 9600
www.caplin.com

The information contained in this publication is subject to UK, US and international copyright laws and treaties and all rights are reserved. No part of this publication may be reproduced or transmitted in any form or by any means without the written authorization of an Officer of Caplin Systems Limited.

Various Caplin technologies described in this document are the subject of patent applications. All trademarks, company names, logos and service marks/names ("Marks") displayed in this publication are the property of Caplin or other third parties and may be registered trademarks. You are not permitted to use any Mark without the prior written consent of Caplin or the owner of that Mark.

This publication is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, warranties of merchantability, fitness for a particular purpose, or non-infringement.

This publication could include technical inaccuracies or typographical errors and is subject to change without notice. Changes are periodically added to the information herein; these changes will be incorporated in new editions of this publication.

Caplin Systems Limited may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time.

This publication may contain links to third-party web sites; Caplin Systems Limited is not responsible for the content of such sites.