Overview

In an "out of the box" installation of Active Data Calendar in a single web application virtual directory, the private calendar event display views are always initially accessed via a URL similar to the following:

http://www.mycalendar.com/default.aspx?type=xxx

In this case "xxx" is a configurable value set inside of *Configuration: Private Calendar* settings inside the administrative interface of the Calendar. Other than requiring that visitors enter the private calendar view by way of the URL specified above, the private calendar is open to anyone with browser access to the web application virtual directory.

This support tip sheet outlines the current recommended best practices for the installation and configuration of Active Data Calendar so as to facilitate securing of the private calendar views in order to prevent unauthorized visitors from accessing private calendar data.

Creating a Second Secured Instance of the Calendar

Active Data Calendar 3.7.x and above supports having the private calendar secured by splitting the application across two separate virtual directory instances. In this configuration, the private calendar and the public only calendar instances each have their own virtual directories which typically reside on physically separate application servers (Note: the use of distinct virtual directories on the same physical application server is also supported). Both virtual directories utilize the same calendar database.

In a typical setup with a separate private calendar virtual directory, the private calendar's virtual directory resides on an "intranet" application server which is protected from the outside internet via firewall and intrinsic network topology. Often these "intranet" application servers are setup to function within a single sign on (SSO) environment. With a minimal amount of customization, Active Data Calendar can also be configured to work within most single sign on (SSO) environments however this is outside of the scope of the "out of box" functionality and requires customized programming.

When the public/private calendar instances are split into two separate virtual directories, the private instance generally becomes the "master" instance, and the public only instance becomes the "slave". Please note that all calendar administration for both the public and private calendar should be done via the "master" instance.

In order to complete the setup of the separate instance for the private calendar as described above, the following steps need to be performed:

1. **A modified "public only" license key file needs to be created for the "slave" instance of the calendar; this instance will not display private events.

    a. NOTE: *Active Data Exchange must be contacted to provide this customized key.*

2. The calendar.properties file of the public only "slave' instance needs to be edited to have the line "IsSlaveCalendar=YES" (do not include the quote marks). This change will ensure that only the master instance of calendar will run various scheduled tasks like imports, event reminders etc.

3. The style sheets, custom headers/footers, and miscellaneous button images which can be administered in the configuration area of the calendar must be kept in sync between both instances of the calendar. This can be achieved in three ways:

    a. Internal file replication (recommended option) – A process internal to Active Data Calendar exists for replicating the noted file assets from the master instance to the slave instance. This process is enabled when both the master and slave instances' calendar.properties files contain the line "MasterFileRefreshEnabled=true"

    b. External file replication - A process external to Active Data Calendar is configured to physically copy the following files/directories from the master instance to the slave

instance whenever they change:

i. Calendar.css
ii. images directory
iii. custom_public_header.html
iv. custom_public_footer.html

c. Duplicate administration – Whenever a new public header/footer is uploaded, a public style configuration is changed, or a custom "Submit Events" image is uploaded in the master calendar administrative area, the same action should be repeated in the slave administration area.

i. **A drawback of this configuration is the requirement for an Active Data modified license key file for the public only instance. Active Data is examining the possibility for streamlining this process in future version.

Using an SSL Certificate with your Calendar Implementation

Often a client's security needs dictate that the private calendar data also be protected via the use of an SSL certificate. Active Data Calendar fully supports the use of an SSL certificate. The following considerations should be kept in mind when implementing Active Data Calendar with SSL:

- Performance considerations may be relevant. Requiring SSL encryption for web traffic does increase the server resource utilization slightly. This consideration may be relevant for extremely high volume calendar implementations.
- Care must be taken when constructing the header and footer of any SSL secured calendar instances to avoid "mixed content" HTML browser warning message issues which can arise when secured web pages contain absolute links to unsecured contents. Specifically, if SSL is required for access to the private calendar, then all image and javascript source URLs in the private header/footer must be absolute links to secured content (i.e. links that begin with https://)

Licensing Considerations

Clients who wish to split their calendar implementation into separate instances for the purpose of securing the private calendar will not incur additional licensing charges. This cost is considered paid through the licensing of the private module.

Support

Please contact Product Support at (610)-997-8100 or support@activedatax.com for further assistance.

190 Brodhead Road • Suite 300 • Bethlehem, PA 18017
Voice: 610.997.8100 • Fax: 610.866.7899 • info@activedataX.com • www.activedataX.com