Sun Java System Calendar Server

System Administrator's Guide

Release 6.3

July 2015

Sun Java System Calendar Server System Administrator's Guide, Release 6.3

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Chapter 1. Calendar Server 6.3 Documentation Errata

Oracle Communications Sun Calendar Server (Calendar Server 6.3) Documentation Errata

This information describes documentation errata for Calendar Server 6.3.

Topics:

service.dwp.maxpostsize Parameter Should Be Documented

In the Calendar Server 6.3 Administration Guide, the `service.dwp.maxpostsize` parameter was not documented. Here is the omitted content:

Parameter	Description
`service.dwp.maxpostsize`	Maximum DWP post content length. Syntax: unsigned integer. Default: 5242880

When you set or change the value of this parameter, you need to restart Calendar Server for the new value or change to take effect.

filter Example Description

The filter example in the fetchcomponents_by_range.wcap documentation in the Sun Java System Calendar Server 6.3 WCAP Developer's Guide is incorrect. The correct description is as follows:

```
@   filter=ATTENDEE=jdoe@sesta.com
```

In addition, the `emailorcalid` parameter appears twice in the fetchcomponents_by_range Parameters table.

storeevents.wcap icsClass Description

The descriptions for `PRIVATE` and `CONFIDENTIAL` in the `icsClass` parameter in the Sun Java System Calendar Server 6.3 WCAP Developer's Guide are incorrect. The correct descriptions are as follows:

PRIVATE	Others can see nothing. (Set transparent = 1 to make it invisible to freebusy queries)
CONFIDENTIAL	Others can see time and date only.

Availability of cs5migrate Utility to Upgrade Databases From Calendar Server 5.1.1 to Calendar Server 6.2

The `cs5migrate` utility, which upgrades Calendar Server 5.1.1 databases to Calendar Server 6.2, is available starting with patch 116577-42. Older Release Notes for Calendar Server 6, for example, the Release Notes for Communications Suite 6.2, do not reflect that the `cs5migrate` utility is not included with the base distribution but must be obtained by this patch.

icsAllowedServiceAccess Attribute

The following information on the `icsAllowedServiceAccess` attribute was omitted from the Sun Java Communications Suite 5 Schema Reference.

icsAllowedServiceAccess

Origin	Calendar Server 6.0
Syntax	cis, single-valued
Object Classes	`icsCalendarDomain`, `icsCalendarUser`
OID	2.16.840.1.113730.3.1.726

Definition

This attribute is used only if the `icsStatus` attribute is not set, or in other words, if `icsStatus` is set, this attribute is ignored. Use this attribute to disallow calendar services to a user. As a default all users are allowed access with `http`. Any other setting, or absence of the attribute entirely, results in the user having access to `http` services (user is enabled).

Syntax

```
icsAllowedServiceAccess:[+ | -][<service>]:[<client_hostname>]
```

where

[+ | -]	Grants or denies a service
service	Specifies the service, such as `http`
client_hostname	Specifies a specific client hostname or `all`, to globally grant or deny service to all clients

Examples

- To grant HTTP access to all calendar clients:

```
icsAllowedServiceAccess:+http:all
```

- To not allow HTTP access from the host `host1.example.com`:

  ```
  icsAllowedServiceAccess:-http:host1.example.com
  ```

- To not allow HTTP from all client hosts:

  ```
  icsAllowedServiceAccess:-http:all
  ```

- To allow HTTP access for all client hosts:

  ```
  icsAllowedServiceAccess:+http:all
  ```

- To not allow any access for all client hosts:

  ```
  icsAllowedServiceAccess:-all:all
  ```

Chapter 2. Calendar Server 6.3 Passwords Removed From Configuration Files

Passwords Removed From Configuration Files

Topic:

- Changing Calendar Server Administrator Passwords

Changing Calendar Server Administrator Passwords

In the past, the Calendar Server configuration file had some passwords in clear text. Though there are read permission restrictions on `ics.conf`, someone can see the passwords when the administrator is editing the configuration file. In Calendar Server 6.3, the passwords have been moved to another file and obfuscated by using base 64 encoding. This encoding prevents others from seeing the passwords accidentally. However, since no encryption is used, the file must still be read protected in order to keep passwords secure and prevent them from falling into the wrong hands.

You can administer one or more of the administrator passwords used to authenticate administrators in Calendar Server by using the `cspassword` utility. This utility, found in the *`cal-svr-base`*`/sbin` directory, can be used for adding, modifying, deleting, and listing passwords. The exit code for the program is 0 on success and non-zero on failure.

This sections covers following topics:

- Modifying Calendar Server Administrator Passwords
- Listing Calendar Server Administrator Passwords

Modifying Calendar Server Administrator Passwords

To add a new password, issue the following command:

```
cspassword -p "password parameter" add
```

To modify an existing password, issue the following command:

```
cspassword -p "password parameter" modify
```

Where *password parameter* is one of the following parameters or any other password option:

- `local.authldapbindcred`
- `local.enduseradmincred`
- `local.lookupldapbindcred`
- `service.siteadmin.cred`

The utility asks you to enter and then confirm the new password. You enter the password in plain text, but only asterisks ★ are displayed on the screen. Password values can be any "non-null" string. The utility uses base64 to encode the password before storing it in the parameter you specify.

An example of the command-line dialog follows:

```
cspassword -p "service.siteadmin.cred" modify
Enter new password: ********
Confirm new password: ********
```

To delete a password, issue the following command:

```
cspassword -p "password parameter" delete
```

Listing the cspassword Utility Options

The `cspassword` utility can be used to list passwords and their values. For this, issue the following command:

```
cspassword list
```

To list only a particular password, issue the command:

```
cspassword -p "password parameter" list
```

For example:

```
cspassword -p "service.siteadmin.cred" list
service.siteadmin.cred="ZecretZ"
```

Note
The utility also supports the required standard utility options `-V`, and `-help`.

Chapter 3. Configuring Calendar Server Software for High Availability (Failover Service)

Configuring Calendar Server Software for High Availability (Failover Service)

For information about configuring HA for the Communications Suite 6 release of Calendar Server, see the following chapter in the Communications Suite 5 release of the *Calendar Server 6.3 Administration Guide*: **Configuring Calendar Server Software for High Availability (Failover Service)**.

The remainder of this page contains the following topics:

- New Installation Paths in Communications Suite 6 Calendar Server
- New Supported Versions of High-Availability Software in Communications Suite 6 Calendar Server
- Installing Calendar Server Sun Cluster HA Agent in Oracle Solaris Zones
- Deployment Example: Configuring Calendar Server 6.3 on Oracle Solaris Cluster 3.2 Software with ZFS

New Installation Paths in Communications Suite 6 Calendar Server

In the Communications Suite 5 *Calendar Server 6.3 Administration Guide*, wherever you see references to the Communications Suite 5 *cal-svr-base* path:

```
/opt/SUNWics5/cal
```

use the Communications Suite 6 *cal-svr-base* path instead:

```
/opt/sun/comms/calendar
```

New Supported Versions of High-Availability Software in Communications Suite 6 Calendar Server

Wherever the Communications Suite 5 *Calendar Server 6.3 Administration Guide* refers to Sun Cluster 3.0 and 3.1, note that the Communications Suite 6 release of Calendar Server 6.3 is also supported on Sun Cluster 3.2.

For the latest supported versions and platforms, see High Availability Support.

Installing Calendar Server Sun Cluster HA Agent in Oracle Solaris Zones

Take the following steps to install the Calendar Server Oracle Solaris Cluster HA agent in non-global zones:

1. Run the Communications Suite command in the global zone only:

```
# commpkg install
```

This command installs the Oracle Solaris Cluster HA Agent package on global zone and all non-global zones.

2. Run the Sun Cluster HA Agent pre-configuration command in the global zone only:

```
# <cs_scha_base>/bin/init-config
```

Deployment Example: Configuring Calendar Server 6.3 on Oracle Solaris Cluster 3.2 Software with ZFS

The following deployment example gives you high-level steps for Deploying Calendar Server on Oracle Solaris Cluster 3.2 with ZFS.

Chapter 4. Enabling Anonymous Calendar Access in Calendar Express

Enabling Anonymous Calendar Access in Calendar Express

Overview

Calendar Express provides a feature for sharing calendars anonymously, without requiring login.

This feature has two parts:

- Access controls that will service the request of an a calendar's anonymous URL.
- Display of an anonymous URL in the Calendar Express GUI, to make the URL discoverable to the anonymous user.

In this context, the client-server distinction is made at a content-sharing level. The client is the browser and the HTML pages used by the browser. The server is the access provided to calendar content.

Server-Side Access Control

The Calendar Express server will accept certain types of requests as anonymous when a URL has no `id=` field. Normally, `id=` field contains the session ID, and is visible in the URL of normal sessions when a user successfully logs in.

This anonymous feature is enabled by default in Calendar Express, and is configurable in `ics.conf`. The server configuration is described in Configuring Anonymous Access for Calendar Server Users in the *Sun Java System Calendar Server 6.3 Administration Guide*.

> **Note**
> Configuration in `ics.conf` controls only the access controls for URL requests. Displaying calendar's anonymous access URL, described below, cannot be disabled even when anonymous access is disabled in `ics.conf`.

Displaying a Calendar's Anonymous Access URL

Navigation

"Calendar" (top level) tab > "Properties" column, "Edit" link.

Steps

- Click on "Calendar" tab.
- Click on "Edit" (in "Properties" column) for a calendar.

In the "Calendar Address" section, displayed text:

"You can give others access to this calendar by giving them the link here. They can then use it in their browsers to view this calendar, provided that access control is set to give them access."

The text of the link is the path of the URL:

"/command.shtml?view=overview&calid=CALID&tzid=Atlantic/South_Georgia&security=1"

Here is the HTML code of the link:

```
<a
href="/command.shtml?view=overview&calid=CALID&tzid=Atlantic/South_Georgia&
target="_blank">
<font size="2" face="PrimaSans BT, Verdana,
sans-serif">/command.shtml?view=overview&calid=CALID&tzid=Atlantic/South_Ge
```

- In the example "CALID" was inserted to replace the actual calid from the URL.
- The timezone in this example is: "Atlantic/South_Georgia"
- The user can send this URL to anyone: other users, as well as people with no user access to the calendar server.

Configuration

This UI feature cannot be disabled or enabled in the server configuration file `ics.conf`. Even if the actual server-side access is disabled in `ics.conf` as described above, the display of the anonymous URL will appear in the user's GUI.

The only time the calendar properties do not display the anonymous URL is if the Properties column provides a View link. This link's state (Edit or View) is controlled by the calendar's permissions.

Anonymous URL Format

The anonymous URL format is similar to the regular Calendar Express URL format. It will contain `calid=` and possibly `tzid=`. The distinguishing characteristic is that URL has no session `id=`.

Timezone `tzid=` in Displayed URL

The display will attempt to insert a timezone with `tzid=` when possible.

If the calendar has no `tzid` set, then the value of the user's `icstimezone:` attribute is used. If the user has no attribute, then no `tzid` is provided. You can check the `timezone` field by issuing the command:

```
cscal list -v
```

> **Note**
> Since calendars have no timezone set by default, the most common `tzid=` in the URL will be the user's timezone.

Anonymous Access From a User's Perspective

When you use an anonymous URL, you will see several differences including:

1. Welcome banner in upper right will say "Welcome anonymous".
2. "Login" link will remain available.
3. Only the "View" tab will be available.

4. The "Color Scheme" will be the default (blue/grey).

Timezone Displayed

The anonymous URL displays a timezone based on the following criteria:

1. The `tzid` in the URL.
2. The Calendar Express default timezone:

/opt/SUNWics5/cal/html/en/default_user_prefs.xml

```
<!-- Default TimeZone -->
<userpref name="icsTimeZone" default_value="America/New_York" />
```

The timezone specified by the calendar owner's `icsTimezone` attribute and the calendar's timezone itself are ignored. However, they often appear in the URL's `tzid` field provided by the display GUI, and take effect via the URL.

Configuration

This feature is enabled by default.

The anonymous URL handler is controlled by:

`service.http.allowanonymouslogin`

When disabled, anonymous URLs will return to the login page (since the session id was rejected).

Issues and Patches

- Anonymous access did not work in Calendar Express with Calendar Server 6.3 until patch -26. This may have affected patch versions as early as -17. When this problem occurred, a valid anonymous URL will always receive the login page.

- Normal sessions that were idle beyond the login session timeout would become anonymous sessions before patch -30. End users may not notice this because the anonymous access is very similar to the normal user session. See the user experience description above for details.

Customers who wish to use the full functionality of this feature should upgrade to the most recent Calendar Server patch.

Limitations of This Document

- This document does not discuss the effect of the ACE on anonymous access.
- This document does not discuss all the `ics.conf` parameters that configure this feature.

Documentation

download.oracle.com

To Configure HTTP Services (cshttpd) for Calendar Server Version 6.3 - Chapter 4.6

`service.http.allowanonymouslogin`

If "yes", allow anonymous (no authentication) access. This is a special type of login that is allowed only specified, restricted access (usually read only access to public calendars). The default is "yes".

Chapter 5. Using Service Management Framework with Calendar Server

Using Service Management Framework (SMF) with Sun Java System Calendar Server 6

SMF was added in Oracle Solaris 10 as a replacement to the `/etc/init.d` scripts for starting, stopping, and restarting services. SMF dramatically decreases boot time as it is aware of dependencies between services, and starts services in parallel where possible.

You must disable the legacy start-up and shut-down scripts prior to enabling the Calendar Server SMF functionality. This can be achieved by removing the following sym-link files.

```
/etc/rc2.d/K11sunwics5
/etc/rc3.d/S94sunwics5
```

Calendar Server provides two SMF service definition files.

```
cal-svr-base/lib/watcher.xml
cal-svr-base/lib/restofcalendar.xml
```

The SMF service definitions can be imported by using the `svccfg` command.

```
svccfg import cal-svr-base/lib/watcher.xml
svccfg import cal-svr-base/lib/restofcalendar.xml
```

The following example shows how to check initial Calendar Server status, enable SMF, then verify status. You must stop the Calendar Server prior to using the `svcadm enable` command.

```
# svcs calendar_server
STATE          STIME    FMRI
disabled        9:33:15 svc:/network/calendar_server:default

# svcs cswatcher
STATE          STIME    FMRI
disabled        9:33:58 svc:/network/cswatcher:default

# svcadm enable cswatcher
# svcadm enable calendar_server

# svcs cswatcher
STATE          STIME    FMRI
online          9:34:55 svc:/network/cswatcher:default

# svcs calendar_server
STATE          STIME    FMRI
online          9:35:02 svc:/network/calendar_server:default
```

For more information on SMF, see Managing Services (Overview), in the *Solaris System Administration Guide*. This chapter provides an overview of SMF, including SMF concepts, administrative and programming interfaces, components, and run levels provided.

For more information on running `svcs` commands to start and stop Calendar Server as the calendar user (`inetuser`), refer to the following steps:

- Remove the default init script

```
rm /etc/rc3.d/S94sunwics5
rm /etc/rc2.d/K11sunwics5
```

- Modify *calendar_base*/config/restofcalendar.xml and change <`cal.RootPath`> to the value of *calendar_base* e.g. `/opt/sun/comms/calendar/SUNWics5/cal/`
- Add to *calendar_base*/config/restofcalendar.xml (just above the `<stability value='Unstable' />` statement)

```
<property_group name='general' type='framework'>
                <!-- to start/stop/enable/disable calendar service
-->
                <propval name='action_authorization' type='astring'
                        value='solaris.smf.manage.calendar_server'
/>
                <propval name='value_authorization' type='astring'
                        value='solaris.smf.manage.calendar_server'
/>
        </property_group>
```

- Modify *calendar_base*/config/watcher.xml and change <`cal.RootPath`> to the value of *calendar_base* e.g. `/opt/sun/comms/calendar/SUNWics5/cal/`
- Add to *calendar_base*/config/watcher.xml (just above the `<stability value='Unstable' />` statement)

```
<property_group name='general' type='framework'>
                <!-- to start/stop/enable/disable calendar service
-->
                <propval name='action_authorization' type='astring'
                        value='solaris.smf.manage.cswatcher' />
                <propval name='value_authorization' type='astring'
                        value='solaris.smf.manage.cswatcher' />
        </property_group>
```

- Validate the script files:

```
svccfg validate watcher.xml
svccfg validate restofcalendar.xml
```

- Stop the calendar server instance

```
cd _calendar_base_/sbin
./stop-cal
```

- Import the svcs files

```
svccfg import watcher.xml
svccfg import restofcalendar.xml
```

- Add the following to `/etc/security/auth_attr`

```
solaris.smf.manage.calendar_server:::Start and Stop Calendar
Server::
solaris.smf.manage.cswatcher:::Start and Stop Calendar Server
Watcher process::
```

- Run the following command as the root user (where icsuser in the following command is the calendar user)

```
usermod -A
"solaris.smf.manage.calendar_server,solaris.smf.manage.cswatcher"
icsuser
```

- As the calendar user (icsuser)

```
/usr/sbin/svcadm enable cswatcher
/usr/sbin/svcadm enable calendar_server
```

Chapter 6. Setting Up and Managing Oracle Communications Sun Calendar Server Security

Setting Up and Managing Oracle Communications Sun Calendar Server Security

> **As of Communications Suite 7, Oracle Communications Sun Calendar Server (formerly Sun Java System Calendar Server 6.3) has been deprecated.**
> For more information on deprecated and removed features of Sun Calendar Server, See Deprecated and Removed Features for Calendar Server 6.3.

This information provides an overview about security for the Oracle Communications Sun Calendar Server (formerly known as Sun Java System Calendar Server 6) product. It also provides links to security topics that provide more indepth information for configuring and administering Oracle Communications Sun Calendar Server security.

Topics:

- Overview of Oracle Communications Sun Calendar Server
- Secure Installation and Configuration
- Security Features

Overview of Oracle Communications Sun Calendar Server

For an overview of the product, see Introduction to Calendar Server Software. For information on general security principals, such as security methods, common security threats, and analyzing your security needs, see Designing for Security. For an overview of operating system security, see Oracle Solaris Security for System Administrators.

Secure Installation and Configuration

Topics in this section:

- Installation Overview
- Installing Infrastructure Components
- Installing Oracle Communications Sun Calendar Server Components
- Post Installation Configuration

Installation Overview

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

Understanding Your Environment

To better understand your security needs, ask yourself the following questions:

1. Which resources am I protecting?

In a Sun Calendar Server production environment, consider which of the following resources you want to protect and what level of security you must provide:

- Sun Calendar Server front- and back-end hosts
- Dependent resources, such as Directory Server
- Access Manager (optional, for Single Sign-on)

2. From whom am I protecting the resources?
   In general, resources must be protected from everyone on the Internet. But should the Sun Calendar Server deployment be protected from employees on the intranet in your enterprise? Should the system administrators have access to all resources? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well trusted system administrators. On the other hand, perhaps it would be best to allow no system administrators access to the data or resources.
3. What will happen if the protections on strategic resources fail?
   In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use Sun Calendar Server. Understanding the security ramifications of each resource help you protect it properly.

Deployment Topologies

You can deploy Sun Calendar Server on a single host or on multiple hosts, splitting up the components into multiple front ends and multiple back ends. For more information, see the following information:

- Developing a Calendar Server Architecture
- Developing a Communications Suite Logical Architecture.

The general architectural recommendation is to use the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture. For more information on addressing network infrastructure concerns, see Determining Your Communications Suite Network Infrastructure Needs.

Installing Infrastructure Components

Access Manager is an optional component for Single Sign-on. For information on how to install and configure Access Manager, see Installation Scenario - Access Manager. See the Sun Java System Access Manager 7.1 Postinstallation Guide for information on how to set up security for Access Manager.

Installing Oracle Communications Sun Calendar Server Components

See Installation Scenario - Oracle Communications Calendar Server Back End and Installation Scenario - Oracle Communications Calendar Server Front End.

The installation prompts for authentication credentials for the following:

- Directory Server manager (bind DN and password)
- Sun Calendar Server administrator

If you are installing Oracle Communications Sun Calendar Server for the first time, the configuration program encodes the passwords you create during the configuration process, and stores them in a separate password configuration file. If you are upgrading your existing Sun Calendar Server software to the Sun Calendar Server 6.3 version, the configuration program encodes the existing passwords found in the `ics.conf` file, and moves them to the password configuration file. For more information, see Automatic Base 64 Encoding of Passwords for Calendar Server 6.3.

Post Installation Configuration

As part of the post-installation phase, you can enable SSL. Oracle Communications Sun Calendar Server supports the SSL protocol to encrypt data between calendar client end users and Sun Calendar Server.

To support SSL, Sun Calendar Server uses SSL libraries from Netscape Security Services (NSS) `certutil` tool, which are also used by Messaging Server. You can configure Sun Calendar Server to encrypt only the Sun Calendar Server login and password or an entire calendar session. The SSL (HTTPS) on the server can be enabled independent of certificate authentication. When SSL is enabled, all the communication is secure, not just the authentication. For more information, see Configuring SSL.

Security Features

This section outlines the specific security mechanisms offered by Oracle Communications Sun Calendar Server.

Topics:

- About System Security in Oracle Communications Sun Calendar Server
- The Security Model
- Configuring and Using Authentication
- Configuring and Using Access Control
- Disabling Anonymous Access to User Calendars

About System Security in Oracle Communications Sun Calendar Server

Sun Calendar Server provides a number of security levels to protect users against eavesdropping, unsanctioned usage, or external attack. The basic level of security is through authentication. Sun Calendar Server uses LDAP authentication by default, but also supports the use of an authentication plugin for cases where an alternate means of authentication is desired. Integration with Access Manager enables Sun Calendar Server to take advantage of its single sign-on capability.

The Security Model

Security requirements arise from the need to protect data: first, from accidental loss and corruption, and second, from deliberate unauthorized attempts to access or alter that data. Secondary concerns include protecting against undue delays in accessing or using data, or even against interference to the point of denial of service. The global costs of such security breaches run up to billions of dollars annually, and the cost to individual companies can be severe, sometimes catastrophic.

The critical security features that provide these protections are:

- Authentication
- Access Control

Authentication is the way in which an entity (a user, an application, or a component) determines that another entity is who it claims to be. An entity uses security *credentials* to authenticate itself. The credentials might be a user name and password, a digital certificate, or something else. Usually, servers or applications require clients to authenticate themselves. Additionally, clients might require servers to authenticate themselves. When authentication is bidirectional, it is called *mutual authentication*.

Sun Calendar Server supports the following authentication types:

- LDAP
- Client Certificates

Access Control, also known as authorization, is the means by which users are granted permission to access data or perform operations. After a user is authenticated, the user's level of authorization determines what operations the owner can perform.

Sun Calendar Server uses Access Control Lists (ACLs) to determine access control for calendars and scheduling. For more information, see Access Control for Calendar Server Version 6.3.

Configuring and Using Authentication

For information on Oracle Communications Sun Calendar Server and LDAP authentication, see End User Administration in Calendar Server Version 6.3.

For information on client certificates, see How to Configure Oracle Communications Sun Calendar Server Client Authentication. This information discusses how to configure Oracle Communications Sun Calendar Server to use client certificates with CRLs with SSL/TLS. Instead of presenting a password, the client presents the user's certificate when it establishes an SSL session with the server.

Configuring and Using Access Control

For information on configuring access control for calendars and scheduling, see Calendar Access Control .

Disabling Anonymous Access to User Calendars

By default, Sun Calendar Server enables anonymous access to user calendars. That is, the default calendar access is free busy/schedule (also known as "invite permissions"), which enables users to anonymously access other users' calendars. (Only event time information is displayed, the actual event shows as "busy.") The configuration parameter that controls the access control permissions is `calstore.calendar.default.acl`. When you install Sun Calendar Server, the default value for this parameter is:

```
"@@o^a^r^g;
@@o^c^wdeic^g;
@^a^fs^g;
@^c^^g;
@^p^r^g"
```

The line `@^a^fs^g` means that all users are granted free busy/schedule permissions.

To disable free busy/schedule permissions, and thus disable anonymous calendar access:

1. Edit the `ics.conf` file.

   ```
   cd /etc/opt/sun/comms/calendar/SUNWics5/config
   cp ics.conf ics.conf.orig
   vi ics.conf
   ```

2. Change the default value of the `calstore.calendar.default.acl` parameter to remove freebusy and schedule rights.
   Change `@^a^fs^g` to `@^a^fs^d`.
3. Save your change and quit the file.

For more information, see the topic on access controls in *Calendar Server 6.3 Administration Guide*.