

Calendar server access control requirements

When used with an external LDAP directory server, Steltor's calendar server both writes information to and accesses information from the directory server. If you are familiar with your LDAP directory server's access control information, you may wish to configure it to restrict the read and write permissions extended to calendar users and administrators, but you must ensure that certain permissions remain at a minimum to avoid calendar client and server errors.

Your directory server may or may not support access control restrictions at the necessary level of granularity. Consult your directory server documentation for details on configuring access control information. Also, please note that some terms used in this document may be slightly different depending on your directory server.

Read requirements

All search operations on the directory server are performed using either an anonymous profile or a profile specified by the `unison.ini [LDAP] binddn` and `bindpwd` parameters. If your directory server allows anonymous binding but you feel that the default read permissions are too loose, or if you wish to configure a bind DN with restricted rights for the calendar server to use, make sure that the calendar server has permission to access the following information:

Target Directory Information Tree (DIT):

- `calendar basedn`

Target attributes:

- `objectclass`
- `objectclasses`
- `member` and/or `uniquemember`

- all calendar attributes (identified by the ctCal prefix)
- c
- cn
- employeeNumber
- generationQualifier
- sn
- givenName
- postalAddress
- telephoneNumber
- facsimileTelephoneNumber
- o
- ou
- mobile
- title
- mail
- initials
- uid

For example, using Netscape Directory Server, a restricted anonymous access control profile might look like the following:

```
aci: (target="ldap:///BASEDN")(targetattr="objectclass || member ||
uniqueMember || c || cn || employeeNumber || generationQualifier ||
sn || givenName || postalAddress || telephoneNumber ||
facsimileTelephoneNumber || o || ou || mobile || title || mail ||
initials || uid || ctCal*" )(version 3.0; acl "Calendar User Read
Access"; allow (read,search) userdn = "ldap:///BINDDN"; )
```

This is the recommended limit for restricting access. If you wish to restrict the access rights even further, you may reduce read access to the following at an absolute minimum:

Target attributes:

- objectclass
- objectclasses
- all calendar attributes (identified by the ctCal prefix)
- commonName
- sn
- givenName
- initials
- generationQualifier
- uid

- mail

If you use this configuration, please ensure that you set the `unison.ini [DAS] dir_adminupdcalonly` parameter to `TRUE` to disable all modification to non-calendar attributes stored in the directory server. Note also that although the calendar server will not generate error messages, some loss of functionality will occur using this access right profile. Specifically, without access to the 'member' and 'uniquemember' attributes, LDAP groups will no longer be supported. In addition, without access to a given attribute, calendar users will not be able to perform searches using that attribute.

Write requirements

Both calendar users and administrators have the ability to modify records in the directory server. To perform a write operation, users and administrators bind to the directory server as themselves. The level of access they have depends upon the restrictions you set for their access control profiles on your directory server.

User access control requirements

Calendar users are created by adding an object class (`ctCalUser`) and a number of calendar attributes (identified by the "ctcal" prefix) to existing users. They bind to the directory server as themselves, using the self entry modification access control profile (`ldap:///self`), which on most directory servers grants full access to modify all attributes. This includes both calendar-specific attributes and other user attributes such as e-mail address and mobile phone number.

If you wish to restrict write access for your calendar users, modify the self entry modification access control profile, but ensure that the access control information for your users contains the following permissions at a minimum:

Target Directory Information Tree (DIT):

- calendar basedn

Target filter:

- An entry with the `ctCalUser` object class attribute

Target attributes:

- `ctcaldisplayprefs`

- `ctcalrefreshprefs`
- `ctcaloperatingprefs`
- `ctcalnotifmechanism`
- `ctcaldefaultreminder`
- `ctcaldefaultnotereminder`
- `ctcaldefaulttaskreminder`
- `ctcallanguageid`
- `ctcaltimezone`
- `ctcalsmstimerange`
- `ctcalmobiletelephonetype`
- `ctcalpublishedtype`
- `ctcalpreferredsmsctelephonenumber`

For example, on Netscape Directory Server, a calendar user access control profile with only calendar permissions might look like the following:

```
aci:(target="ldap:///BASEDN")(targetfilter="objectclass=ctcaluser")
(targetattr="ctcaldisplayprefs || ctcalrefreshprefs ||
ctcaloperatingprefs || ctcalnotifmechanism || ctcaldefaultreminder
|| ctcaldefaultnotereminder || ctcaldefaulttaskreminder ||
ctcallanguageid || ctcaltimezone || ctcalmobiletelephonetype ||
ctcalpublishedtype || ctcalsmstimerange ||
ctcalpreferredsmsctelephonenumber")(version 3.0; acl "Calendar User
Self ACI"; allow (read,write,compare) userdn="ldap:///self";)
```

If you need greater security, this configuration is recommended. However, bear in mind that users will be unable to modify their e-mail addresses and mobile phone numbers through their calendar clients. If you choose to restrict user modification to calendar attributes, you should also set the `unison.ini` parameter `[DAS] dir_updcaldonly` to `FALSE`. This will ensure that users do not encounter security errors if they attempt to modify other read-only information through their calendar clients. For more information, consult Reference Appendix B of your calendar server's Reference Manual.

If you desire a more secure access control profile than the default, without limiting the functionality of your calendar clients, consider specifying the `mail` and `mobile` attributes in addition to all `ctcal` attributes. For example (again, assuming Netscape Directory Server):

```
aci:(target="ldap:///BASEDN")(targetfilter="objectclass=ctcaluser")
(targetattr="ctcaldisplayprefs|| ctcalrefreshprefs ||
ctcaloperatingprefs || ctcalnotifmechanism || ctcaldefaultreminder
|| ctcaldefaultnotereminder || ctcaldefaulttaskreminder ||
```

```
ctcallanguageid || ctcaltimezone || ctcalmobiletelephonenumber ||
ctcalpublishedtype || ctcalmsttimerange ||
ctcalpreferredsmsctelephonenumber || mail || mobile")(version 3.0;
acl "Calendar User Self ACI"; allow (read,write,compare)
userdn="ldap:///self";)
```

Administrator access control requirements

Calendar administrators are added to the directory server as members of the group specified by the `unison.ini` parameter `[LDAP] admingroup`. When you install the calendar server, a default access control profile is created for members of this group which allows access to all LDAP attributes.

Always ensure that the group specified by the `[LDAP] admingroup` parameter has the following permissions at a minimum:

Target Directory Information Tree (DIT):

- calendar basedn

Target filter:

- all calendar users (any entry with the `ctCalUser` object class)

Target attributes:

- objectclass
- all calendar attributes (`ctcal*`)

If you modify the administrator group's access control information to restrict directory server permissions, SYSOPs may encounter security errors by using the calendar server administration tools to modify attributes to which they have been denied access. Set the `unison.ini` `[DAS] dir_updcalonly` parameter to `TRUE` to have the calendar server block the SYSOP from attempting to modify non-calendar attributes and avoid these security errors.

For example, on Netscape Directory Server, a calendar administrator access control profile with only calendar permissions might look like the following:

```
aci:(target="ldap:///BASEDN")(targetfilter="objectclass=ctcaluser")
(targetattr="objectclass || ctCal*")(version 3.0; acl "Calendar
Administratortor ACI"; allow (read,write,compare) groupdn =
"ldap:///ADMINGROUPDN, BASEDN";)
```

```
aci:(target="ldap:///BASEDN")(targetfilter="objectclass=
```

```
ctcalresource") (targetattr="*)(version 3.0; acl "Calendar
Administrators ACI"; allow (read,write,compare) groupdn =
"ldap:///ADMINGROUPDN, BASEDN";)
```