Avoiding ACI Problems with Outlook Connector

Sun Java™ Enterprise System Technical Note

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–5193
August 2006

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la legislation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la legislation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement designés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

060808@15490

Avoiding ACI Problems with Outlook Connector

This technical note describes how to configure Access Control Instructions (ACIs) for Sun Java™ System Directory Server 5 2005Q4 to enable Sun Java System Connector for Microsoft Outlook 7 2005Q4 to perform corporate directory lookups.

The component products affected by this technical note are:

- Sun Java System Connector for Microsoft Outlook 7 2005Q4
- Sun Java System Directory Server 5 2005Q4

This technical note contain the following sections:

Technical Note Revision History

TABLE 1 Revision History

Date	Description of Changes
August 8, 2006	Re-issue of this technical note for Sun Java Enterprise System 2005Q4.

Avoiding ACI Problems with Outlook Connector

Sun Java System Connector for Microsoft Outlook provides the ability to browse a corporate directory for a particular user's email address, as well as for calendar information. The Outlook client browses the corporate directory by using its own internal LDAP browser. You define the configuration for the Microsoft LDAP browser in the Outlook Connector Deployment tool.

Once the Outlook Connector has been successfully deployed to end users, they will quickly find that the default setting of the Directory Server does not show all the necessary information needed for a corporate directory. Missing information includes postal address and telephone numbers. This information is filtered by the Access Control Instructions (ACIs) in the directory's Organization Tree. ACIs are instructions that grant or deny permissions to entries in the directory.

Authentication to Directory Server for corporate directory lookups is accomplished in two ways: *anonymous* or *authenticated*. Anonymous authentication enables any user to authenticate (LDAP BIND) to the directory without having to provide identification, that is, without having to use a Distinguished Name (DN) and password. By default, the Directory Server, when configured for Sun Java System Communications Services products, does not allow anonymous authentication. The default is for DN/password authentication, for obvious security reasons.

Should you want to allow anonymous access to the corporate Directory Server, create the following ACI (as the Directory Administrator):

```
# ldapmodify -D "cn=Directory manager"
dn: dc=red,dc=siroe,dc=com
changetype: modify
add: aci
aci: (targetattr != "userPassword") (version 3.0;acl "Anonymous access"; allow
(read,compare,search)(userdn = "ldap:///anyone");)
```

In the above rule, you would replace `dn: dc=red,dc=siroe,dc=com` with your own information. This ACI rule enables anyone to access users' LDAP attributes. The only attribute that is blocked is `userPassword`, by using the `targetattr != "userPassword"` rule.

Misused ACI Rules

In many environments, you do not want to grant anonymous access. You must pay attention to the potential security risks involved. For example, the following ACI rules cause a potential security problem by exposing user passwords.

```
aci:(target="ldap:///uid=*,ou=people,o=red.siroe.com,o=ugdata")(targetattr="*"
(version 3.0;acl"allowproxy-calmaster";allow(proxy)(user dn="ldap:///uid=uid=*,
ou=people,o=red.siroe.com,o=ugdata");)
```

The lesson here is to use the ACI `targetattr` rule with caution.

When you implement the above ACI, users' passwords are now visible. This is confirmed by running the following `ldapsearch` command:

```
# ldapsearch -b ou=people,o=red.siroe.com,o=ugdata -D "uid=jhawk,ou=people,o=red.siroe.com,o=ugdata"
-w demo "cn=naomi*" | moreuid=nhawkins,ou=People,o=red.siroe.com,o=ugdata uid=nhawkins
iplanet-am-modifiable-by=cn=Top-level Admin Role,o=ugdata
givenName=Naomi
mail=naomi.hawkins@red.siroe.com
mailUserStatus=active
sn=Hawkins
cn=Naomi Hawkins
icsStatus=Active
mailHost=par.red.siroe.com
inetUserStatus=Active
userPassword={SSHA}0qCnUCKtNK94ndKmEMlPp8i1Z/SKMAhapz3ZPA==
sunUCDefaultApplication=addressbook
sunUCTheme=uwc
<< remainder of output deleted >>
```

The highlighted text is the userPassword attribute that you do not want to expose.

Limiting Attributes Expected by the Outlook LDAP Browser

In addition to limiting security risks, you can use ACIs to limit the XML for Portal transmitted back to the Outlook Connector client.

The following ACI rule prevents delivery of the user password and also limits attributes expected by the Outlook LDAP Browser. You set the access rights in the Directory Server console:

```
aci:(targetattr = "initials || cn || mail || display-name || displayName || sn || co || o || givenName
|| objectClass || uid || mailnickname || title || company || physicalDeliveryOfficeName || telephoneNumber")
(targetfilter = (objectClass=icscalendaruser)) (version 3.0;acl "Allow Calendar users to read and search
other users - product=ics,class=admin,num=3,version=1";allow (read,search)(userdn = "ldap:///uid=*,
ou=People,o=red.siroe.com, o=ugdata");)
```

The targetattr indicates the list of attributes that can be returned. All other attributes are blocked. The targetfilter requires that the returned entries must have objectclass=icscalendaruser assigned.

The following ldapsearch command confirms two things: first, the userpassword attribute is no longer visible to end users; second, the returned LDAP attributes are limited to only the attributes expected by Outlook's LDAP Browser.

```
# ldapsearch -b ou=people,o=red.siroe.com,o=ugdata -D
"uid=jhawk,ou=people,o=red.siroe.com,o=ugdata" -w demo "cn=naomi*" | more
uid=nhawkins,ou=People,o=red.siroe.com,o=ugdata
uid=nhawkins
givenName=Naomi
```

```
mail=naomi.hawkins@red.siroe.com
sn=Hawkins
cn=Naomi Hawkins
objectClass=userpresenceprofile
objectClass=sunucpreferences
objectClass=iplanet-am-user-service
objectClass=iplanet-am-managed-person
objectClass=top
objectClass=icscalendaruser
objectClass=organizationalperson
objectClass=inetadmin
objectClass=person
objectClass=inetuser
objectClass=sunssoadapterperson
objectClass=inetlocalmailrecipient
objectClass=iplanetpreferences
objectClass=ipuser
objectClass=inetorgperson
objectClass=sunportaldesktopperson
objectClass=inetsubscriber
objectClass=inetmailuser
```

Further Reading

Refer to *Sun Java System Directory Server 5 2005Q1 Administration Guide* for more information.

Documentation, Support, and Training

The Sun web site provides information about the following additional resources:

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

Note – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com` and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 819-5193.