Sun Java™ Enterprise System Technical Note: Avoiding ACI Problems with Outlook Connector

2005Q1

Part Number 819-2315-10

The *Sun Java Enterprise System 2005Q1 Technical Note: Avoiding ACI Problems with Outlook Connector* describes how to configure Access Control Instructions (ACIs) for Sun Java™ System Directory Server 5 2005Q1 to enable Sun Java™ System Connector for Microsoft Outlook 7 2005Q1 to perform corporate directory lookups.

The component products affected by this technical note are:

- Sun Java System Connector for Microsoft Outlook 7 2005Q1
- Sun Java System Directory Server 5 2005Q1

This technical note contain the following sections:

Technical Note Revision History

Table 1 Revision History

Date	Description of Changes
April 5, 2005	Initial release of this technical note.

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=sirore,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 the following documentation for more information.

- *Sun Java System Directory Server 5 2005Q1 Administration Reference*:

  http://docs.sun.com/source/817-7613

Known Issues and Limitations

See the Java Enterprise System Release Notes Collection at the following URL to find out about known problems:

http://docs.sun.com/app/docs/coll/entsysrn_05q1

How to Report Problems and Provide Feedback

If you have problems with Sun Java Enterprise System, contact Sun customer support using one of the following mechanisms:

- Sun Software Support services online at
  http://www.sun.com/service/sunone/software

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.
- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

- Description of the problem, including the situation where the problem occurs and its impact on your operation
- Machine type, operating system version, and product version, including any patches and other software that might be affecting the problem
- Detailed steps on the methods you have used to reproduce the problem
- Any error logs or core dumps

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 document title and part number. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title of this book is *Sun Java Enterprise System 2005Q1 Technical Note: Avoiding ACI Problems with Outlook Connector*, and the part number is 819-2315-10.

Additional Sun Resources

Useful Sun Java System information can be found at the following Internet locations:

- Sun Java System Documentation
  http://docs.sun.com/prod/java.sys
- Sun Java System Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun Java System Software Products and Service
  http://www.sun.com/software
- Sun Java System Software Support Services
  http://www.sun.com/service/sunone/software
- Sun Java System Support and Knowledge Base
  http://www.sun.com/service/support/software
- Sun Support and Training Services
  http://training.sun.com
- Sun Java System Consulting and Professional Services
  http://www.sun.com/service/sunps/sunone
- Sun Java System Developer Information
  http://developers.sun.com
- Sun Developer Support Services
  http://www.sun.com/developers/support

- Sun Java System Software Training
  http://www.sun.com/software/training
- Sun Software Data Sheets
  http://wwws.sun.com/software