LDAP Server Configuration Example

Introduction

The KVM Over the NET™ switch allows log in authentication and authorization through external programs. This chapter provides an example of how to configure Active Directory on Windows 2003 Server for a KVM Over the NET™ switch. Adapt the example to suit the requirements of your particular installation.

To allow authentication and authorization via LDAP or LDAPS, the Active Directory's LDAP *Schema* must be extended so that an extended attribute name for the KVM Over the NET™ switch – ***iKVM4140-userProfile* –** is added as an optional attribute to the *person* class.

You will have to complete the following procedures: 1) Install the Windows Server Support Tools; 2) Install the Active Directory Schema Snap-in; and 3) Extend and Update the Active Directory Schema.

Install the Windows 2003 Support Tools

To install the Windows 2003 Support Tools, do the following:

1. On your Windows Server CD, open the Support → Tools folder.
2. In the right panel of the dialog box that comes up, double click **SupTools.msi**.
3. Follow along with the Installation Wizard to complete the procedure.

Install the Active Directory Schema Snap-in

To install the Active Directory Schema Snap-in, do the following:

1. Open a Command Prompt.
2. Key in: `regsvr32 schmmgmt.dll` to register schmmgmt.dll on your Active Directory computer.
3. Open the *Start* menu; click **Run**; key in: `mmc /a`; click **OK**.
4. On the *File* menu of the screen that appears, click **Add/Remove Snap-in**; then click **Add**.
5. Under *Available Standalone Snap-ins*, double click **Active Directory Schema**; click **Close**; click **OK**.
6. On the screen you are in, open the *File* menu and click **Save**.
7. For *Save in*, specify the *C:\Windows\system32* directory.
8. For *File name*, key in **schmmgmt.msc**.
9. Click **Save** to complete the procedure.

Create a Start Menu Shortcut Entry

To create a shortcut entry on the Start Menu for the Active Directory Schema, do the following:

1. Right click Start; select: **Open all Users** → **Programs** → **Administrative Tools**.
2. On the *File* menu, select **New** → **Shortcut**
3. In the dialog box that comes up, browse to, or key in the path to schmmgmt.msc (C:\Windows\system32\schmmgmt.msc), then click **Next**.
4. In the dialog box that comes up, key in *Active Directory Schema* as the name for the shortcut, then click **Finish.**

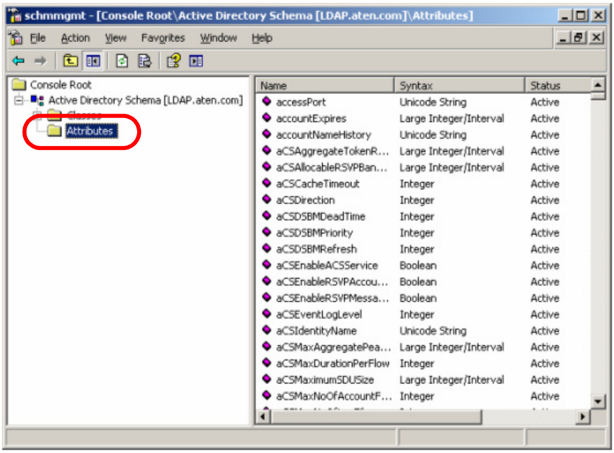
Extend and Update the Active Directory Schema

To extend and update the Active Directory Schema, you must do the following 3 procedures: 1) create a new attribute; 2) extend the object class with the new attribute; and 3) edit the active directory users with the extended schema.

Creating a New Attribute

To create a new attribute do the following:

1. From the Start menu, open Administrative Tools → Active Directory Schema.
2. In the left panel of the screen that comes up, right-click **Attributes**:



schmmgmt - [Console Root\Active Directory Schema [LDAP.aten.com]\Attributes]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Schema [LDAP.aten.com]
Classes
Attributes

Name	Syntax	Status
accessPort	Unicode String	Active
accountExpires	Large Integer/Interval	Active
accountNameHistory	Unicode String	Active
aCSAggregateTokenR...	Large Integer/Interval	Active
aCSAllocableRSVPBan...	Large Integer/Interval	Active
aCSCacheTimeout	Integer	Active
aCSDirection	Integer	Active
aCSDSBMDeadTime	Integer	Active
aCSDSBMPriority	Integer	Active
aCSDSBMRefresh	Integer	Active
aCSEnableACSService	Boolean	Active
aCSEnableRSVPAccou...	Boolean	Active
aCSEnableRSVPMessa...	Boolean	Active
aCSEventLogLevel	Integer	Active
aCSIdentityName	Unicode String	Active
aCSMaxAggregatePea...	Large Integer/Interval	Active
aCSMaxDurationPerFlow	Integer	Active
aCSMaximumSDUSize	Large Integer/Interval	Active
aCSMaxNoOfAccountF...	Integer	Active

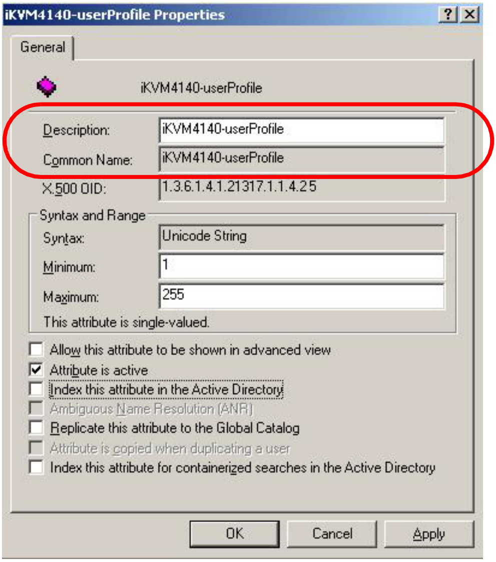
3. Select New → Attribute.
4. In the warning message that appears, click **Continue** to bring up the *Create New Attribute* dialog box.

(Continues on next page.)

(Continued from previous page.)

5. Fill in the dialog box to match the entries for *Description* and *Common Name* shown below, then click **OK** to complete the procedure.

Note: The Unique X500 Object ID uses periods, not commas.



iKVM4140-userProfile Properties

General

iKVM4140-userProfile

Description: iKVM4140-userProfile

Common Name: iKVM4140-userProfile

X.500 OID: 1.3.6.1.4.1.21317.1.1.4.25

Syntax and Range

Syntax: Unicode String

Minimum: 1

Maximum: 255

This attribute is single-valued.

☐ Allow this attribute to be shown in advanced view

☑ Attribute is active

☐ Index this attribute in the Active Directory

☐ Ambiguous Name Resolution (ANR)

☐ Replicate this attribute to the Global Catalog

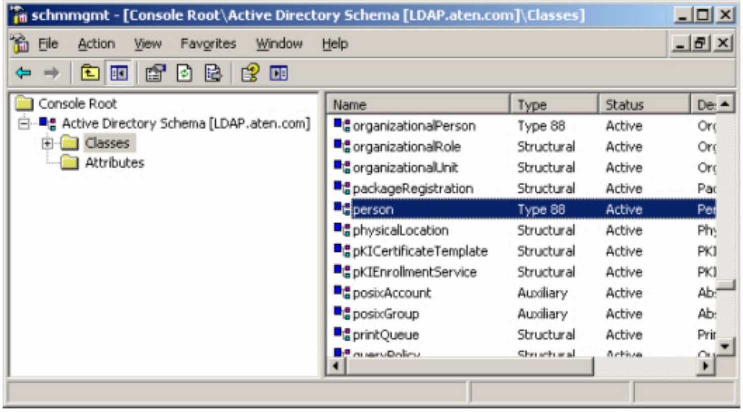
☐ Attribute is copied when duplicating a user

☐ Index this attribute for containerized searches in the Active Directory

Extending the Object Class With the New Attribute

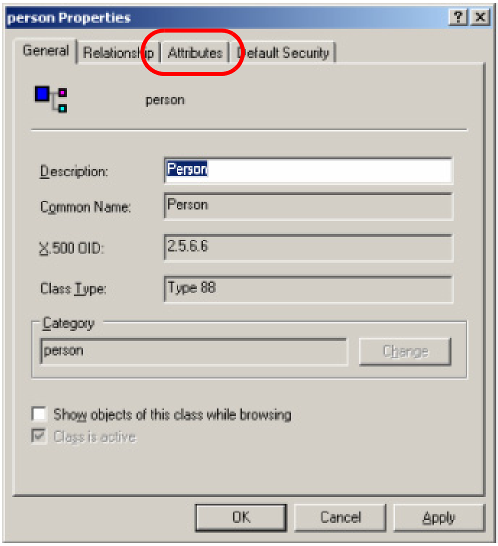
To extend the object class with the new attribute, do the following:

1. Open the Control Panel → Administrative Tools → Active Directory Schema.
2. In the left panel of the screen that comes up, select **Classes**.
3. In the right panel, right-click **person**:


schmmgmt - [Console Root\Active Directory Schema [LDAP.aten.com]\Classes]
File
Action
View
Favorites
Window
Help
Console Root
Active Directory Schema [LDAP.aten.com]
Classes
Attributes

Name	Type	Status	De:
organizationalPerson	Type 88	Active	Or(
organizationalRole	Structural	Active	Or(
organizationalUnit	Structural	Active	Or(
packageRegistration	Structural	Active	Pac
person	Type 88	Active	Per
physicalLocation	Structural	Active	Phy
pKICertificateTemplate	Structural	Active	PKI
pKIEnrollmentService	Structural	Active	PKI
posixAccount	Auxiliary	Active	Ab:
posixGroup	Auxiliary	Active	Ab:
printQueue	Structural	Active	Prir
queryPolicy	Structural	Active	Qu

4. Select **Properties**; the *person Properties* dialog box comes up with the *General* page displayed. Click the *Attributes* tab.



person

Description: Person

Common Name: Person

X.500 OID: 2.5.6.6

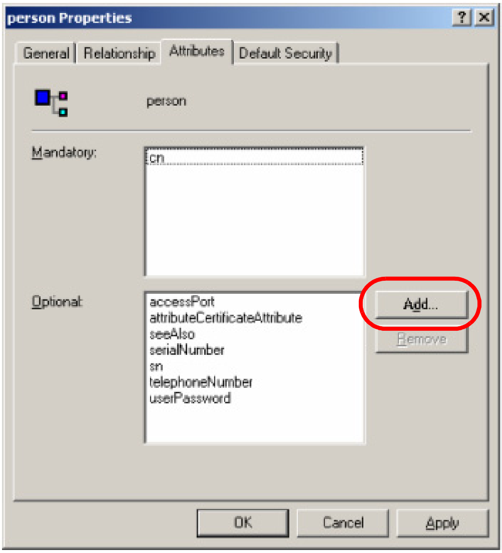
Class Type: Type 88

Category: person

□ Show objects of this class while browsing

☑ Class is active

5. On the *Attributes* page, click **Add**:



person Properties

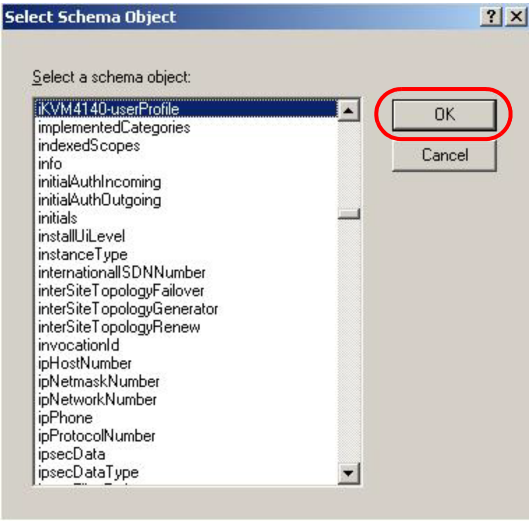
General | Relationship | Attributes | Default Security

person

Mandatory: cn

Optional: accessPort
attributeCertificateAttribute
seeAlso
serialNumber
sn
telephoneNumber
userPassword

6. In the list that comes up, select **iKVM4140-userProfile**, then click **OK** to complete the procedure.



Select Schema Object

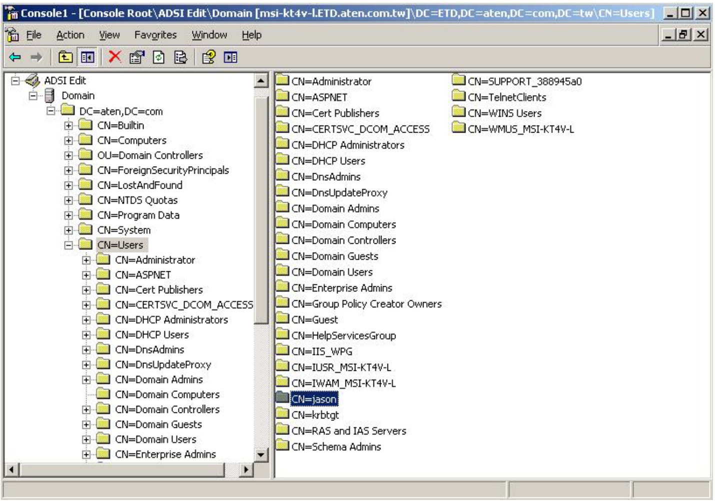
Select a schema object:

iKVM4140-userProfile
implementedCategories
indexedScopes
info
initialAuthIncoming
initialAuthOutgoing
initials
installUiLevel
instanceType
internationalISDNNumber
interSiteTopologyFailover
interSiteTopologyGenerator
interSiteTopologyRenew
invocationId
ipHostNumber
ipNetmaskNumber
ipNetworkNumber
ipPhone
ipProtocolNumber
ipsecData
ipsecDataType

Editing Active Directory Users

To edit Active Directory Users With the Extended Schema, do the following:

1. Run **ADSI Edit**. (Installed as part of the *Support Tools*.)
2. In the left panel, open **Domain**, and navigate to the *DC=aten,DC=com CN=Users* node.
3. In the right panel, locate the user you wish to edit. (Our example uses *jason*.)

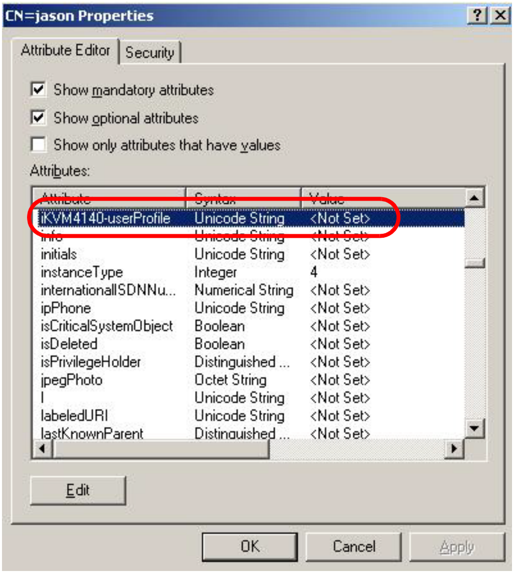


4. Right-click on the user's name and select **properties.**

(Continues on next page.)

(Continued from previous page.)

5. On the *Attribute Editor* page of the dialog box that appears, select **iKVM4140-userProfile** from the list.



CN=jason Properties

☑ Show mandatory attributes

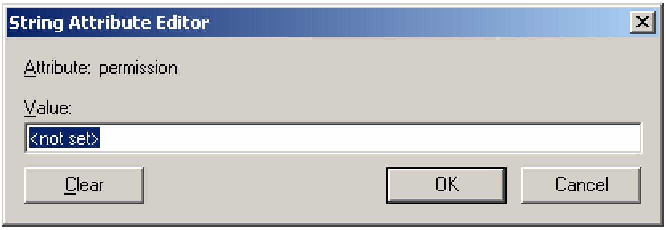
☑ Show optional attributes

□ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
iKVM4140-userProfile	Unicode String	<Not Set>
info	Unicode String	<Not Set>
initials	Unicode String	<Not Set>
instanceType	Integer	4
internationalISDNNu...	Numerical String	<Not Set>
ipPhone	Unicode String	<Not Set>
isCriticalSystemObject	Boolean	<Not Set>
isDeleted	Boolean	<Not Set>
isPrivilegeHolder	Distinguished ...	<Not Set>
jpegPhoto	Octet String	<Not Set>
l	Unicode String	<Not Set>
labeledURI	Unicode String	<Not Set>
lastKnownParent	Distinguished ...	<Not Set>

6. Click **Edit** to bring up the *String Attribute Editor*:



String Attribute Editor

Attribute: permission

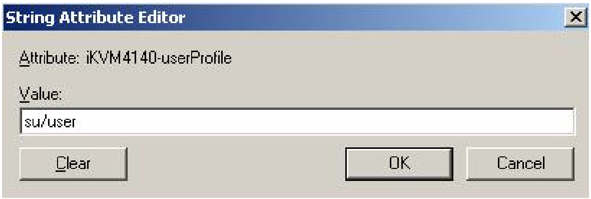
Value:

<not set>

(Continues on next page.)

(Continued from previous page.)

7. Key in the permission attribute values. For example:



Attribute: iKVM4140-userProfile

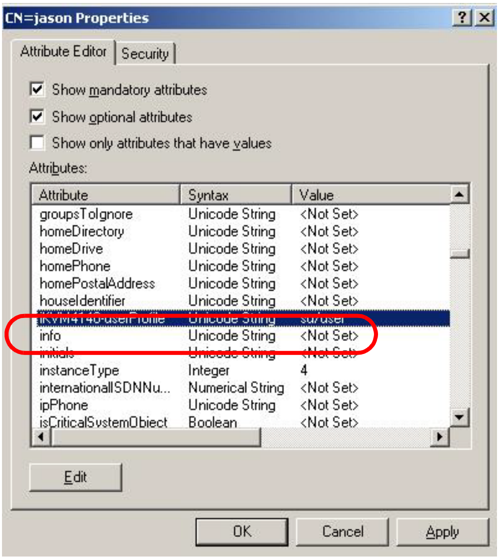
Value:

su/user

Note: 1. Where *user* represents the Username of a KVM Over the NET™ switch user whose permissions reflect the permissions you want Jason to have.

2. Refer to the Access Rights table in the User Manual of your KVM Over the NET™ switch model for further information about string attributes.

8. Click **OK**. When you return to the *Attribute Editor* page, the *iKVM4140-userProfile* entry now reflects the new permissions:



☑ Show mandatory attributes

☑ Show optional attributes

□ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
groupsToIgnore	Unicode String	<Not Set>
homeDirectory	Unicode String	<Not Set>
homeDrive	Unicode String	<Not Set>
homePhone	Unicode String	<Not Set>
homePostalAddress	Unicode String	<Not Set>
houseIdentifier	Unicode String	<Not Set>
iKVM4140-userProfile	Unicode String	su/user
info	Unicode String	<Not Set>
initials	Unicode String	<Not Set>
instanceType	Integer	4
internationalISDNNu...	Numerical String	<Not Set>
ipPhone	Unicode String	<Not Set>
isCriticalSystemObject	Boolean	<Not Set>

a) Click **Apply** to save the change and complete the procedure. Jason now has the same permissions as *user.*

b) Repeat the *Editing Active Directory Users* procedure for any other users you wish to add.

OpenLDAP

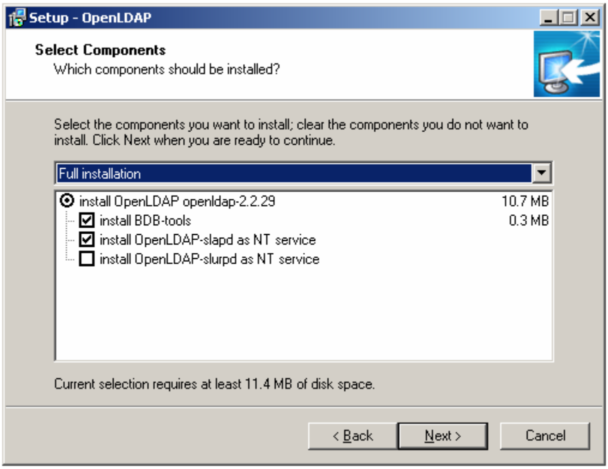
OpenLDAP is an Open source LDAP server designed for Unix platforms. A Windows version can be downloaded from:

```
http://download.bergmans.us/openldap/openldap-2.2.29/
openldap-2.2.29-db-4.3.29-openssl-0.9.8a-
win32_Setup.exe.
```

OpenLDAP Server Installation

After downloading the program, launch the installer, select your language, accept the license and choose the target installation directory. The default directory is: *c:\Program Files\OpenLDAP*.

When the *Select Components* dialog box appears, select *install BDB-tools* and *install OpenLDAP-slapd as NT service*, as shown in the diagram, below:



Select Components
Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

- ○ install OpenLDAP openldap-2.2.29 — 10.7 MB
  - ☑ install BDB-tools — 0.3 MB
  - ☑ install OpenLDAP-slapd as NT service
  - ☐ install OpenLDAP-slurpd as NT service

Current selection requires at least 11.4 MB of disk space.

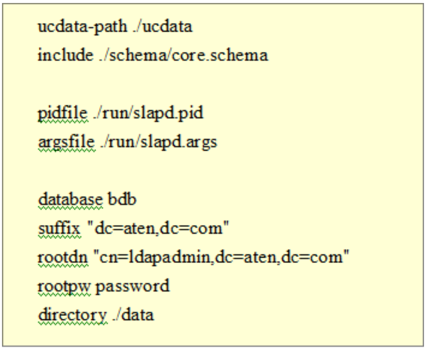
OpenLDAP Server Configuration

The main OpenLDAP configuration file, *slapd.conf*, is found in the /OpenLdap directory. It has to be customized before launching the server. This section provides a quick summary of the modifications to the configuration file in order for it to be used with the KVM Over the NET™ switch, for a complete explanation of OpenLDAP, refer to the official OpenLDAP documentation.

The modifications to the configuration file will do the following:

- Specify the Unicode data directory. The default is *./ucdata*.
- Choose the required LDAP schemas. The core schema is mandatory.
- Configure the path for the OpenLDAP *pid* and *args* start up files. The first contains the server pid, the second includes command line arguments.
- Choose the database type. The default is *bdb* (Berkeley DB).
- Specify the server suffix. All entries in the directory will have this suffix, which represents the root of the directory tree. For example, with suffix *dc=aten,dc=com*, the fully qualified name of all entries in the database will end with dc=aten,dc=com.
- Define the name of the administrator entry for the server (*rootdn*), along with its password (*rootpw*). This is the server's super user. The rootdn name must match the suffix defined above. (Since all entry names must end with the defined suffix, and the rootdn is an entry.)

An example configuration file is provided in the figure, below:



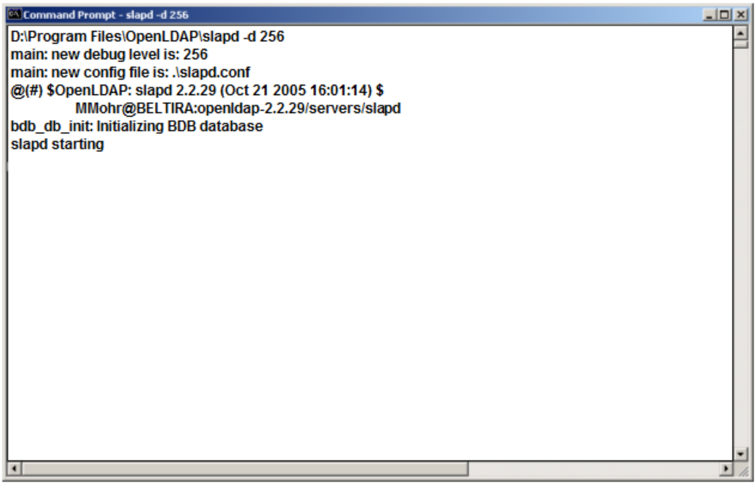
```
ucdata-path ./ucdata
include ./schema/core.schema

pidfile ./run/slapd.pid
argsfile ./run/slapd.args

database bdb
suffix "dc=aten,dc=com"
rootdn "cn=ldapadmin,dc=aten,dc=com"
rootpw password
directory ./data
```

Starting the OpenLDAP Server

To start the OpenLDAP Server, run **slapd** (the OpenLDAP Server executable file) from the command line. slapd supports a number of command line options, the most important option is the **d** switch that triggers debug information. For example, a command of:

```
slapd -d 256
```

would start OpenLDAP with a debug level of 256, as shown in the following screenshot:



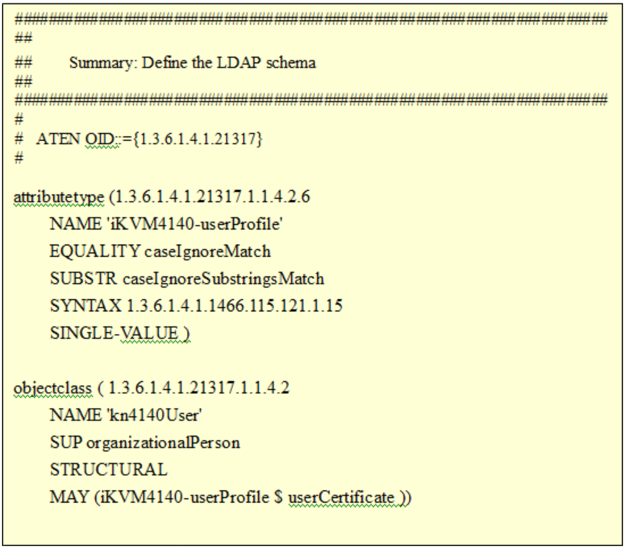
```
D:\Program Files\OpenLDAP\slapd -d 256
main: new debug level is: 256
main: new config file is: .\slapd.conf
@(#) $OpenLDAP: slapd 2.2.29 (Oct 21 2005 16:01:14) $
            MMohr@BELTIRA:openldap-2.2.29/servers/slapd
bdb_db_init: Initializing BDB database
slapd starting
```

Note: For details about slapd options and their meanings, refer to the OpenLDAP documentation.

Customizing the OpenLDAP Schema

The schema that slapd uses may be extended to support additional syntaxes, matching rules, attribute types, and object classes.

In the case of the KVM Over the NET™ switch, the *User* class and the *permission* attribute are extended to define a new schema. The extended schema file used to authenticate and authorize users logging in to the KVM Over the NET™ switch is shown in the figure, below:

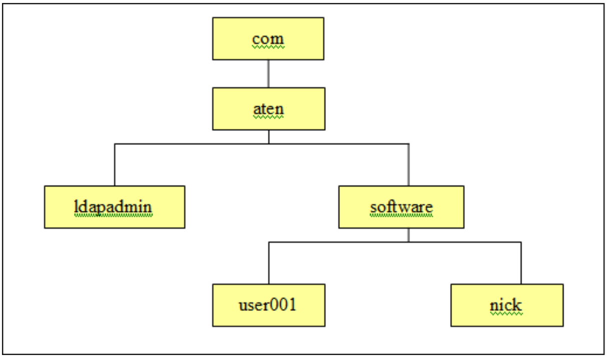


```
######################################################################
##
##      Summary: Define the LDAP schema
##
######################################################################
#
#  ATEN OID::={1.3.6.1.4.1.21317}
#

attributetype (1.3.6.1.4.1.21317.1.1.4.2.6
      NAME 'iKVM4140-userProfile'
      EQUALITY caseIgnoreMatch
      SUBSTR caseIgnoreSubstringsMatch
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
      SINGLE-VALUE )

objectclass ( 1.3.6.1.4.1.21317.1.1.4.2
      NAME 'kn4140User'
      SUP organizationalPerson
      STRUCTURAL
      MAY (iKVM4140-userProfile $ userCertificate ))
```

LDAP DIT Design and LDIF File

LDAP Data Structure

An LDAP Directory stores information in a tree structure known as the Directory Information Tree (DIT). The nodes in the tree are directory entries, and each entry contains information in attribute-value form. An example of the LDAP directory tree for the KVM Over the NET™ switch is shown in the figure, below:

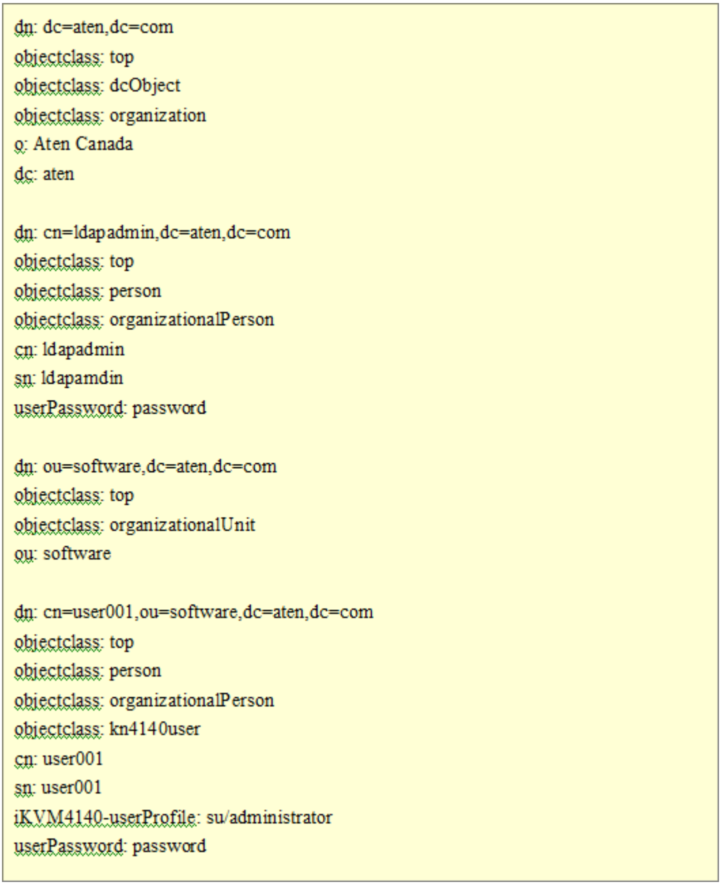


(Continues on next page.)

(Continued from previous page.)

DIT Creation

The LDAP Data Interchange Format (LDIF) is used to represent LDAP entries in a simple text format (refer to RFC 2849). The figure below illustrates an LDIF file that creates the DIT for the KN4140 directory tree. The name of the file is *init.ldif* and you create it in the /OpenLDAP directory, as follows:

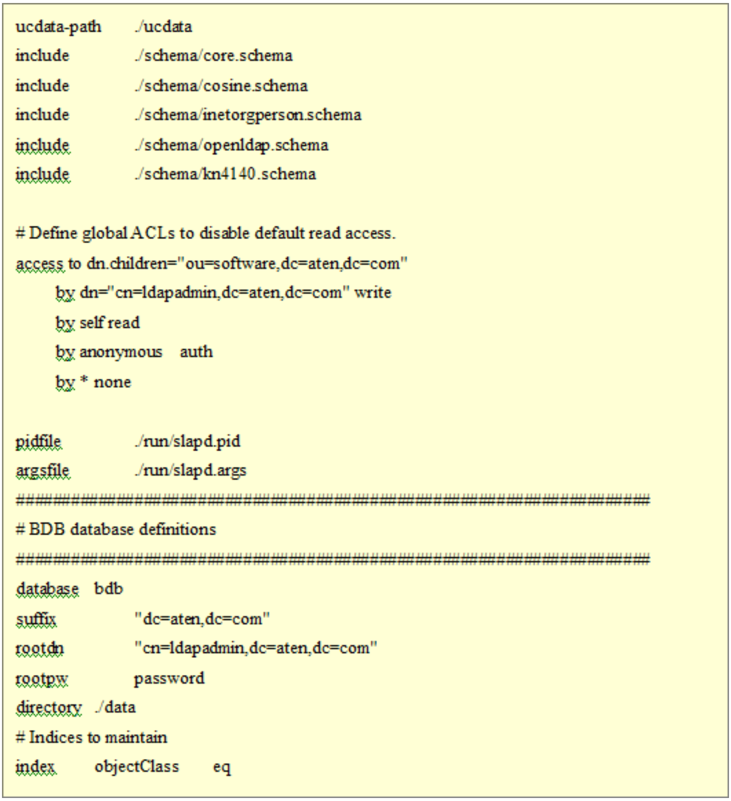


```
dn: dc=aten,dc=com
objectclass: top
objectclass: dcObject
objectclass: organization
o: Aten Canada
dc: aten

dn: cn=ldapadmin,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: ldapadmin
sn: ldapamdin
userPassword: password

dn: ou=software,dc=aten,dc=com
objectclass: top
objectclass: organizationalUnit
ou: software

dn: cn=user001,ou=software,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: kn4140user
cn: user001
sn: user001
iKVM4140-userProfile: su/administrator
userPassword: password
```

Using the New Schema

To use the new schema, do the following:

1. Save the new schema file (e.g., kn4140.schema) in the /OpenLDAP/schema/ directory.
2. Add the new schema to the *slapd.conf* file (in the /OpenLDAP directory), as shown in the figure, below:



```
ucdata-path     ./ucdata
include         ./schema/core.schema
include         ./schema/cosine.schema
include         ./schema/inetorgperson.schema
include         ./schema/openldap.schema
include         ./schema/kn4140.schema

# Define global ACLs to disable default read access.
access to dn.children="ou=software,dc=aten,dc=com"
        by dn="cn=ldapadmin,dc=aten,dc=com" write
        by self read
        by anonymous    auth
        by * none

pidfile         ./run/slapd.pid
argsfile        ./run/slapd.args
#######################################################################
# BDB database definitions
#######################################################################
database   bdb
suffix          "dc=aten,dc=com"
rootdn          "cn=ldapadmin,dc=aten,dc=com"
rootpw          password
directory  ./data
# Indices to maintain
index      objectClass      eq
```

3. Restart the LDAP server.
4. Write the LDIF file and create the database entries in init.ldif with the *ldapadd* command, as shown in the following example:

```
ldapadd -f init.ldif -x -D "cn=ldapadmin,dc=aten,dc=com"
-w password
```