LDAP Server Configuration Example

Introduction

KVM Over the NET™ switches allow log in authentication and authorization through external programs. This help file 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.

Note: The following configuration example uses the ATEN KN4140v. For the correct attribute settings and other information for your specific model, please see *LDAP Setting Values*, page 22.

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.**

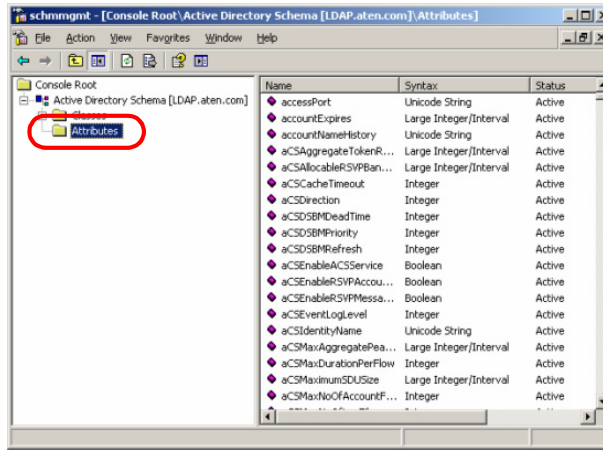
Extend and Update the Active Directory Schema

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**:

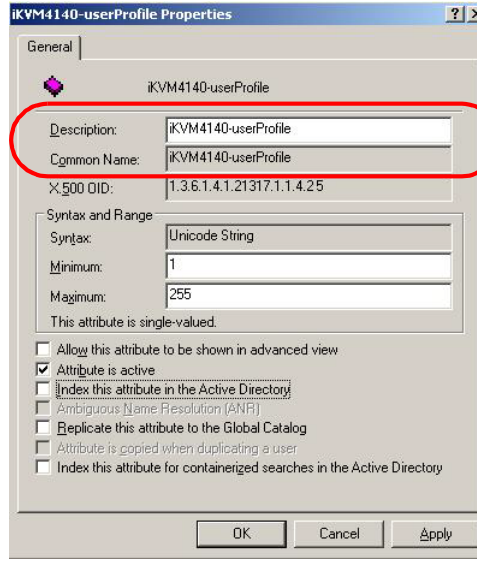


3. Select New → Attribute.
4. In the warning message that appears, click **Continue** to bring up the *Create New Attribute* dialog box.

(Continues on next page.)

5. Fill in the dialog box to match the entries for *Description* and *Common Name* shown below, enter the correct *X500 Object ID*, then click **OK** to complete the procedure.

Note: The Unique X500 Object ID uses periods, not commas. See *X500 Object ID Table*, page 5, for details



X500 Object ID Table

Model	OID
CN8000	.1.3.6.1.4.1.21317.1.3.1.6
CN8000A	.1.3.6.1.4.1.21317.1.3.1.100.31
CN8600	.1.3.6.1.4.1.21317.1.3.1.100.26
CN9600	.1.3.6.1.4.1.21317.1.3.1.100.50
CS1708i / CS1716i	.1.3.6.1.4.1.21317.1.3.1.100.39
CCVSR	.1.3.6.1.4.1.21317.1.2.2
IP8000	.1.3.6.1.4.1.21317.1.3.1.8
KE6900AiT / KE6940AiT	.1.3.6.1.4.1.21317.1.3.1.100.51
KH1508Ai / KH1516Ai	.1.3.6.1.4.1.21317.1.3.1.100.36
KL1508Ai / KL1516Ai	.1.3.6.1.4.1.21317.1.3.1.1
KL-1108VN / KL1116VN	.1.3.6.1.4.1.21317.1.3.1.100.34
KM0532 / KM0932 / KM0032	.1.3.6.1.4.1.21317.1.4.1.1
KN1000	.1.3.6.1.4.1.21317.1.3.1.9
KN1000A	.1.3.6.1.4.1.21317.1.3.1.100.32
KN1108v / KN1116v	.1.3.6.1.4.1.21317.1.3.1.11
KN1108VA / KN1116VA	.1.3.6.1.4.1.21317.1.3.1.100.33
KN1116VA-AC	.1.3.6.1.4.1.21317.1.3.1.100.38
KN4140v series[1]	.1.3.6.1.4.1.21317.1.3.1.3
KN series[2]	.1.3.6.1.4.1.21317.1.3.1.100.45
KN8132V / KN8164V	.1.3.6.1.4.1.21317.1.3.1.100.28
PN5xxx / PN7xxx	.1.3.6.1.4.1.21317.1.3.2.30
PM101DA	.1.3.6.1.4.1.21317.1.3.1.100.55
RCM101A	.1.3.6.1.4.1.21317.1.3.1.100.42
RCMDVI101	.1.3.6.1.4.1.21317.1.3.1.100.54
SN3101	.1.3.6.1.4.1.21317.1.3.3.2

Note: 1. 12 models: KN4140v, KN4132v, KN4116v, KN4124v, KN2140v, KN2132v, KN2116v, KN2124v, KN4116, KN4132, KN2116A, KN2132.

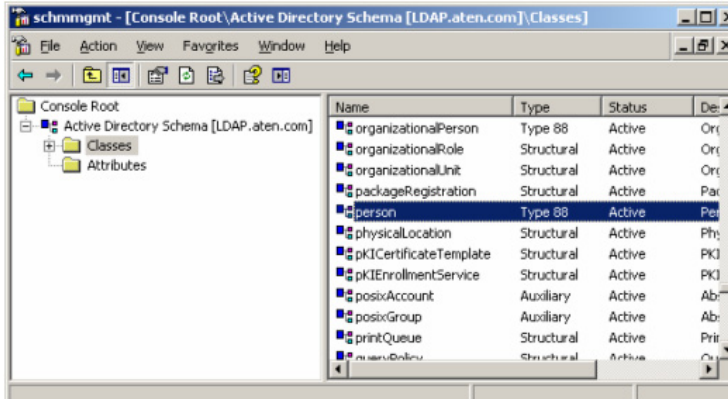
2. 10 models: KN1132V, KN2116VA, KN2124VA, KN2132VA, KN2140VA, KN4116VA, KN4124VA, KN4132VA, KN4140VA, KN4164V.

Extending the Object Class With the New Attribute

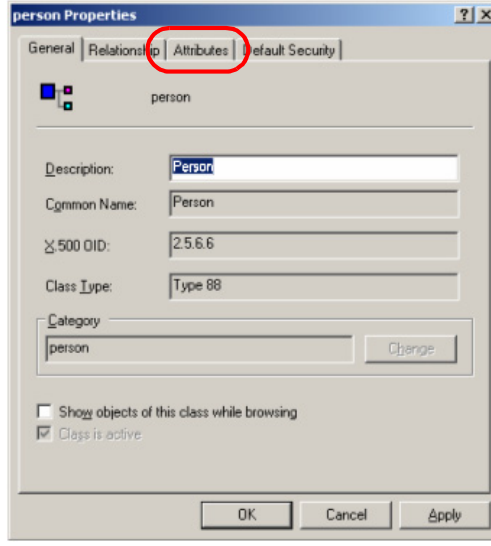
To extend the object class with the new attribute, do the following:

Note: The attribute name differs depending on the model that is used. Please see *LDAP Setting Values*, page 22.

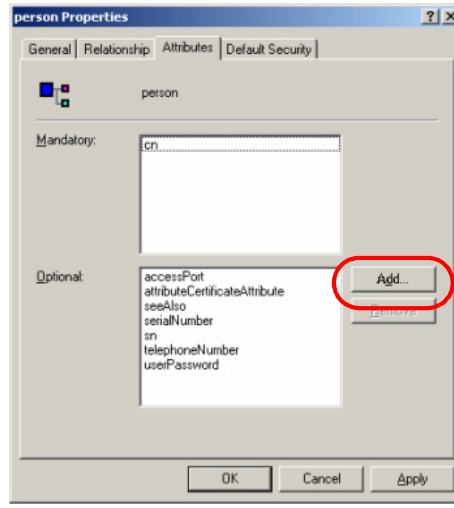
1. Open the Control Panel → Administrative Tools → Active Directory Schema.
2. In the left panel of the screen that comes up, select **Classes**.
3. In the right panel, right-click **person**:



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

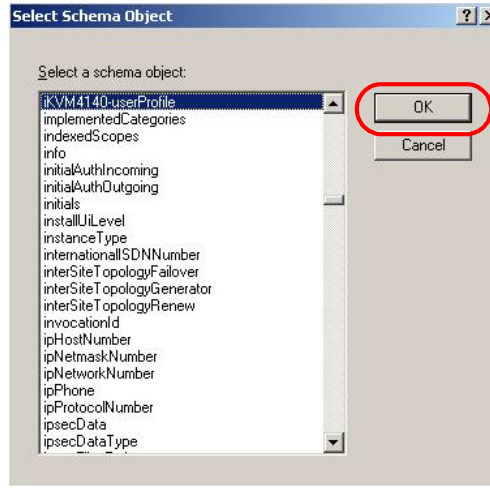


5. On the *Attributes* page, click **Add**:



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

Note: For the attribute settings for your specific model, please see *LDAP Setting Values*, page 22.



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

Editing Active Directory Users

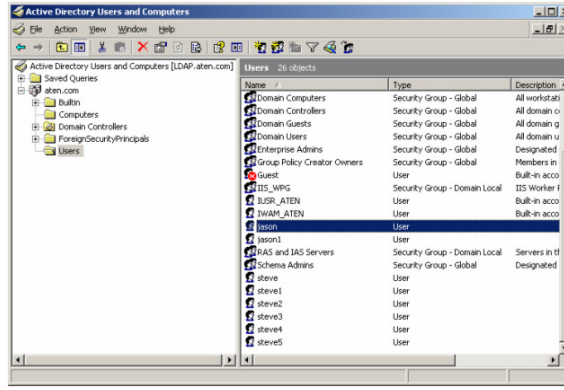
There are two kinds of Active Directory users – Type 1 (whose authentication and authorization parameter settings are supported on the LDAP server) and Type 2 (whose authentication takes place on the LDAP server, but authorization is via the KVM Over the NET™ switch's user database). See below for further details about Type 1 and page 13 for Type 2.

Type 1

For Type 1 users, both authentication and authorization parameter settings are supported on the LDAP server. To edit a Type 1 Active Directory user do the following:

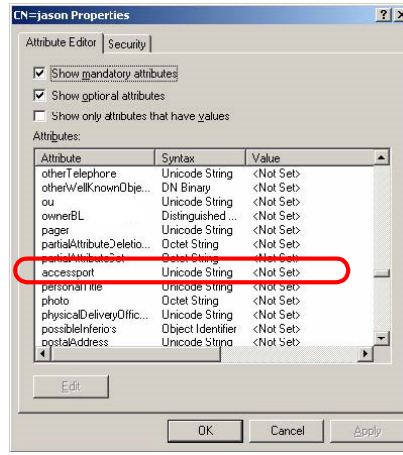
Note: The attribute name differs depending on the model that is used. Please see *LDAP Setting Values*, page 22.

1. Run **ADSI Edit**. (Installed as part of the *Support Tools*.)
2. Open **domain**, and navigate to the *cn=users dc=aten dc=com* node.
3. Locate the user you wish to edit. (Our example uses *jason*.)

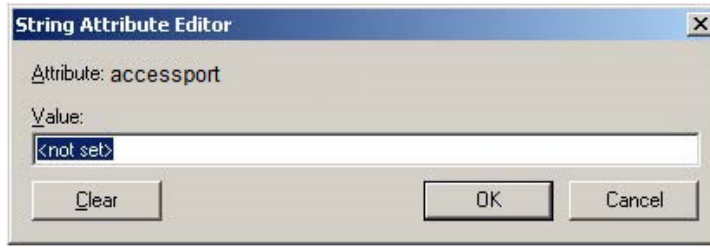


4. Right-click on the user's name and select **properties.**

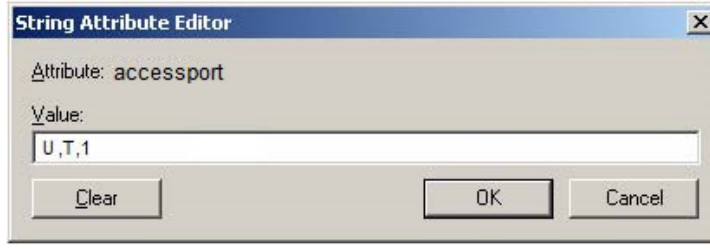
5. On the *Attribute Editor* page of the dialog box that appears, select **accessPort** from the list.



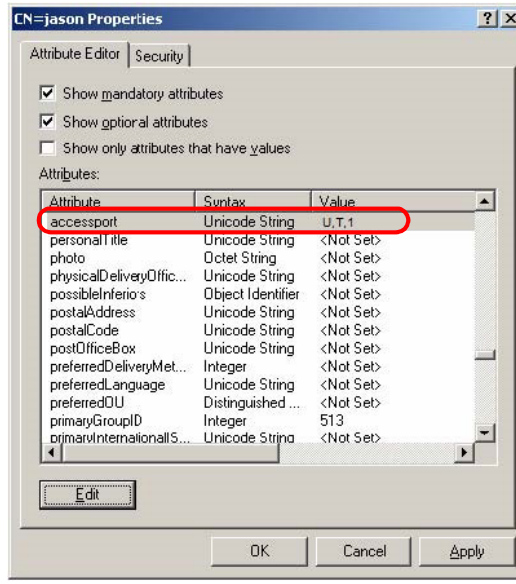
6. Click **Edit** to bring up the *String Attribute Editor*:



7. Key in the desired KVM Over the NET™ switch permission attribute values (see *The Permission Attribute Value*, page 11 for details). For example:



8. Click **OK**. When you return to the *Attribute Editor* page, the *accessPort* entry now reflects the new accessPort:



a) Click **Apply** to save the change and complete the procedure.

b) Repeat the *Click Apply to save the change and complete the procedure. Jason now has the same permissions as user.* procedure for any other Type 1 users you wish to add.

The Permission Attribute Value

The attribute value for *permission* is made up of two parts: 1) the IP address of the KVM Over the NET™ switch a user will access; and 2) a string that indicates the access rights the user has on the KVM Over the NET™ switch at that IP address. For example:

```
192.168.0.80&c,w,j;192.168.0.188&v,l
```

The makeup of the permission entry is as follows:

- An ampersand (&) connects the KVM Over the NET™ switch's IP with the access rights string.
- The access rights string is made up of various combinations of the following characters: c w j p l v s. The characters can be entered in upper or lower case. The meanings of the characters is provided in the *Permission String Characters* table, below.
- The characters in the access rights string are separated by a comma (,). There are no spaces before or after the comma.
- If a user has access rights to more than one KVM Over the NET™ switch, each permission segment is separated by a semicolon (;). There are no spaces before or after the semicolon.

Permission String Characters

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java applet.
P	Allows the user to Power On/Off, Reset devices via an attached PN0108.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.
S	Allows the user to use the Virtual Media function – Read Only.
M	Allows the user to use the Virtual Media function – Read/Write.
T	Allows the user to access the system via Telnet.
H	Allows the user to access the system via SSH.
A	Allows the user to access the system via Telnet and SSH.

Note: Different models support different permission settings. Please see *LDAP Setting Values*, page 22, for details.

Permission Examples

Access rights examples are given in the table, below:

User	String	Meaning
User1	10.0.0.166&w,v	1. User has *Windows Client* and *View Only* rights on a KVM Over the NET™ switch with an IP address of 10.0.0.166. 2. User has no rights on any other KVM Over the NET™ switch units administered by the LDAP server.
User2	10.0.0.164&p,s;10.0.0.166&j,c	1. User has *PON* and *Virtual Media* rights on a KVM Over the NET™ switch with an IP address of 10.0.0.164. 2. User has *Java Applet* and *Administrator* rights on a KVM Over the NET™ switch with an IP address of 10.0.0.166. 3. User has no rights on any other KVM Over the NET™ switch units administered by the LDAP server.
User3	v,l;10.0.0.164&p,j	1. User has *View Only* and *Log Information* rights on all KVM Over the NET™ switch units administered by the LDAP server, except for the one with an IP address of 10.0.0.164. 2. User has *PON* and *Java Applet* rights on a KVM Over the NET™ switch with an IP address of 10.0.0.164.
User4		User has no access rights to any KVM Over the NET™ switch units administered by the LDAP server.
User5	v,w	User has *View Only* and *Windows Client* rights on all KVM Over the NET™ switch units administered by the LDAP server.
User6	v;10.0.0.166&;10.0.0.164&c,j	1. User has *View Only* rights on all KVM Over the NET™ switch units administered by the LDAP server, except for the ones with IP addresses of 10.0.0.166 and 10.0.0.164. 2. User has no access rights on the KVM Over the NET™ switch with an IP address of 10.0.0.166. 3. User has *Administrator* and *Java Applet* rights on the KVM Over the NET™ switch with an IP address of 10.0.0.164.

Type 2

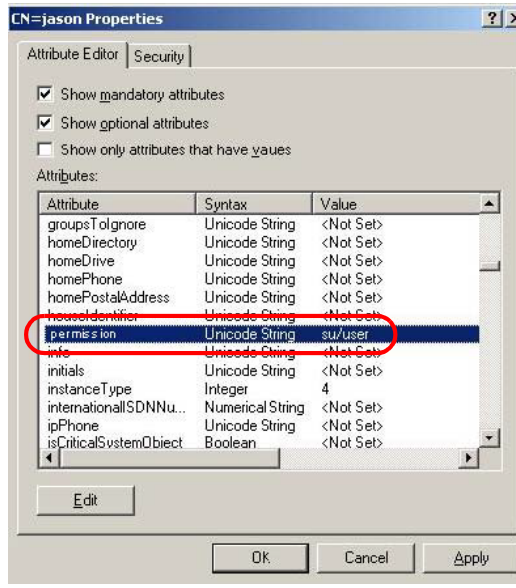
For Type 2 users, authentication takes place on the LDAP server, but authorization is via the KVM Over the NET™ switch's user database. To edit a Type 2 user, do the following:

Note: The attribute name differs depending on the model that is used. Please see *LDAP Setting Values*, page 22.

1. Follow Steps 1 – 6 of Editing a Type 1 user (beginning on page 8)
2. In the String Attribute Editor, key in the values shown in the screenshot, below:

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

3. Click **OK**. When you return to the *Attribute Editor* page, the *permission* entry now reflects the new permissions:



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

d) Repeat the *Click Apply to save the change and complete the procedure. Jason now has the same permissions as user.* procedure for any other users you wish to add.

OpenLDAP

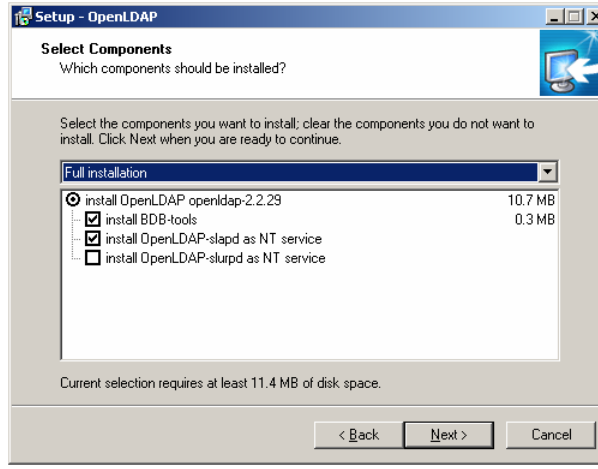
OpenLDAP is an Open source LDAP server designed for Unix platforms. A Windows version can be downloaded from:

```
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:



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.)

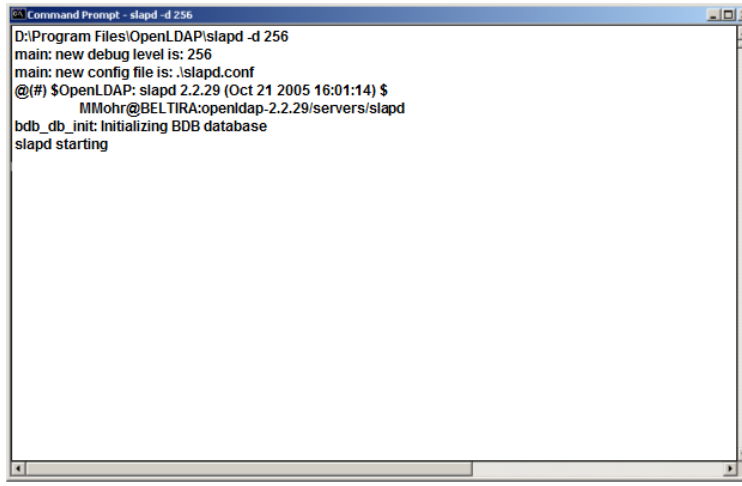
An example configuration file is provided in the figure, below:

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:



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:

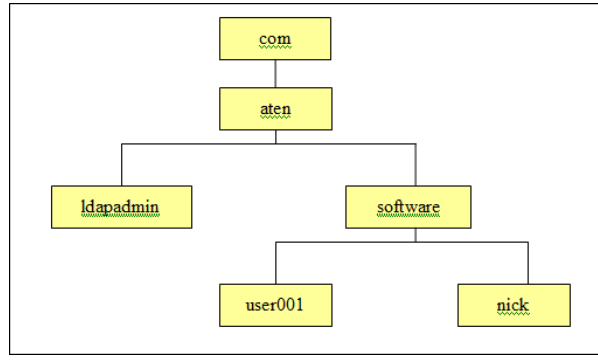
```
#######################################################################
##
##       Summary: Define the LDAP schema
##
#######################################################################
#
#   ATEN OID::={1.3.6.1.4.1.21317}
#

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 ))
```

Note: For the correct attribute type and object class for your specific model, please see *LDAP Setting Values*, page 22.

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:



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
```

Appendix

LDAP Setting Values

The following table shows the attribute name and permission settings for all ATEN and ALTUSEN models that allow authentication and authorization via LDAP or LDAPS.

Model	Attribute Name (Win LDAP) / Attributetype (OPenLDAP)	Objectclass (OpenLDAP)	Permission Settings
CN8000	permission	CN8000User	All
CS1708i / CS1716i	CS1716i-accessRight	CSUser	C, W, J, L
CCVSR	iVlog-userProfile	VSRUser	All
IP8000	permission	IP8000User	C, W, J, L, S, M
KH1508Ai / KH1516Ai	KH15xxAi-accessRight	KHUser	C, W, J, L
KL1508Ai / KL1516Ai	KL15xxAi-accessRight	KLUser	
KM0932 / KM0952 / KM0032	iKVM0932-userProfile	KMUser	C, L, P
KN1000	KN1000-accessRight	KNUser	All
KN1108v / KN1116v	KN1116-userProfile		
KN4140v *	iKVM4140-userProfile		
PN7212 / PN7320	PNxxxx-userProfile	PN7xxxUSer	N/A (SU mode only)
PN5212 / PN5320		PN5xxxUser	
SN3101	accessPort	SN3xxxUser	

Note: 12 models: KN4140v, KN4132v, KN4116v, KN4124v, KN2140v, KN2132v, KN2116v, KN2124v, KN4116, KN4132, KN2116A, KN2132.