KVM over IP Matrix
Access Control Overview

MR

KVM over IP – Access Control

- Showcased for the first time at NAB 2026!

- Apantac introduced a new branch of FW in April 2026 supporting Access Control, A7.5.3.2AC
- It has the same capabilities as the regular FW but with additional support for Access Control
- When using a KVM over IP matrix with the Access Control, operators need to provide valid credentials before accessing Tx modules from a console

Access Control implementation

- Access Control can work in two ways:
  - Use the Access Control utility to configure User Accounts, Resources (Tx transmitter modules) and Permissions. The configuration is stored in, and the management is carried from, in addition to their usual role, by two designated Tx. One is the Master Tx and a second is the Slave Tx. In case one of the two is down or disconnected from the network, operation is seamlessly taken over by the second. In this mode, Access Control can work without any external server
  - Have the KVM matrix connecting to either an OpenLDAP or an Active Directory Server, over the LDAP (Lightweight Directory Access Protocol) IP protocol or its encrypted version, LDAPS. In this case the AC configuration is stored in the external server

Access Control Concepts

- In its simplest implementation, User Accounts and Resources (Transmitters/Tx = Computers) are defined:
  - User Accounts This is a list of Usernames & Passwords
  - Resources This is a list of tables, one for each Tx including the Access Permission Rights for each defined User
- There are five permission levels or modes defined as: (Highest to lowest priority)
  - Exclusive When an Exclusive User is accessing a Tx, no other user can connect to that Tx. An Exclusive User kicks out any other non-Exclusive User of the same Tx. The timeout function does not apply when an Exclusive User is accessing the Tx

Access Control Concepts – Cont.

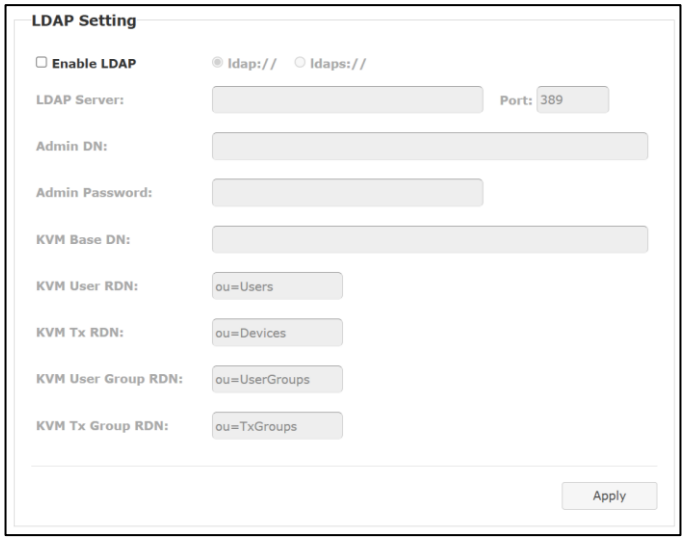
- Occupy If a Tx is accessed by a User with an Occupy permission, all other permitted users (except Exclusive) can connect to the same Tx but only in View Only mode until the predefined Tx timeout expires. The timeout value is Tx specific and configured via its web page. If a Tx is accessed by a Control User, another Occupy User can connect to the same Tx, and the Control User permission will switch to Occupy
- Control If a Tx is accessed by a Control User, the Tx is under Keyboard/Mouse Sharing Mode that provides concurrent control of this Tx for all Control Users
- View Only A user with a View Only permission will see the video but has no Keyboard and Mouse control of the Tx
- Disabled The Tx is not visible/accessible to the User. (It does not show up in the console Tx selection drop down menu)

Access Control Concepts – Cont.

- However, if there are numerous Tx modules and Users, the configuration might become long and tedious, specifically in facilities with free lance users that need to be added or removed frequently… To address this concern, two extra concepts are defined:
  - User Groups Individual users can be gathered into User Groups. A User Group has its own name and password, and the Tx Access menu / configuration allows assigning a "User Group permission" to any Tx or Tx Group
  - Tx Groups Tx modules can be gathered into groups, and the Tx Access menu / configuration allows assigning at once each User or User Group the same permission for all the Tx Group members

Access Control - Configuration

- A new "LDAP Setting" section has been added to the Tx and Rx Functions web page



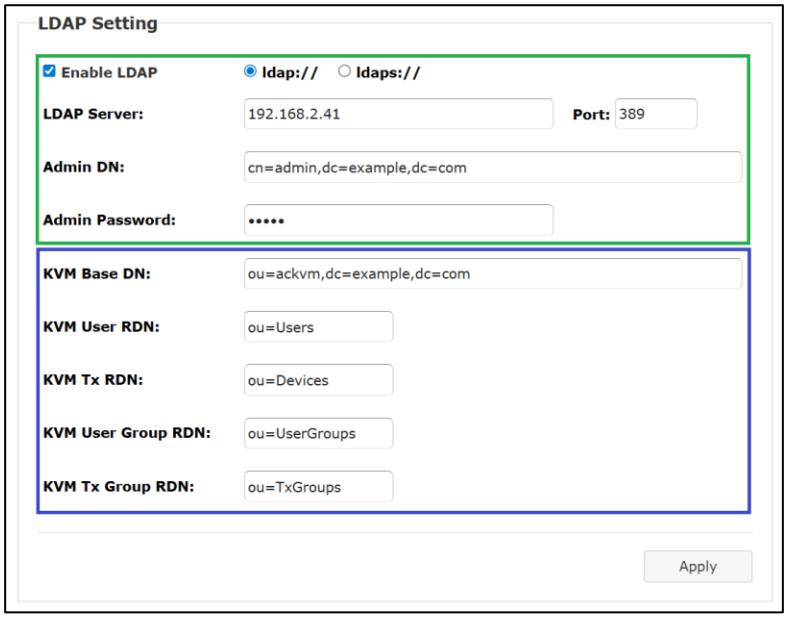
- When "Enable LDAP" is not checked (For all modules), the Apantac Access Control Application is used for configuring Access Control. Refer to the Application manual for the configuration details

Access Control – Config. – Cont.

- When "Enable LDAP" is checked (for all modules), the Access Control management is handled by the OpenLDAP or Microsoft Active Directory Server
- Make sure the AC Server connects to the KVM matrix IP network
- With OpenLDAP, import the supplied ackvm-schema.ldif file and configure Users Credentials, Resources (Tx) Permissions, etc. A sample ackvm-data.ldif file is provided, but you will need to enter your own data using your favorite OpenLDAP Management Tool
- With Microsoft Active Directory, import the supplied ackvm-schema-attribute.ad-ldif and the ackvm-schema-objectclass.ad-ldif files and configure Users Credentials, Resources (Tx) Permissions, etc. An ackvm-data.ad-ldif file is provided as an example but you will need to enter your own data using your favorite Active Directory Management Tool

Access Control – Config. – Cont.

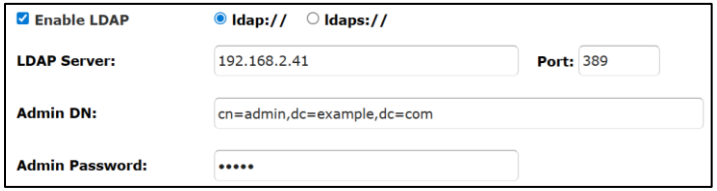
- Configure LDAP settings of each module



- Green rectangle: LDAP server parameters (Used each time the KVM matrix modules connects to the LDAP server)
- Blue rectangle contains KVM matrix Access Control entries

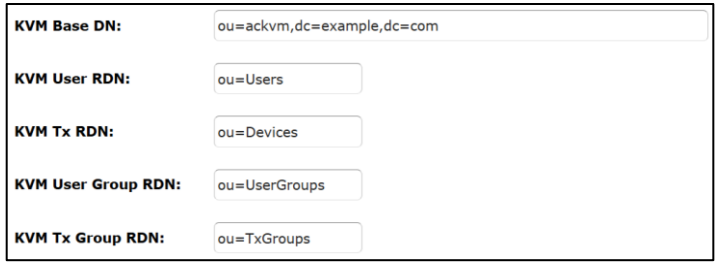
Access Control – Config. – Cont.

- More specifically…



  - Connection. **ldap://** Uses standard LDAP (unencrypted). Default port: 389
  - Connection. **ldaps://** Uses LDAP over SSL/TLS (encrypted). Default port: 636
  - **LDAP Server**. IP address or hostname of the LDAP directory server. This is where the KVM modules send authentication requests
  - **Admin DN**. The Distinguished Name (DN) of the LDAP administrator account used by the KVM system to query the directory
    cn=admin → common name of the admin user
    dc=example,dc=com → domain components
  - **Admin Password**. Password for the Admin DN account. Used by the KVM matrix to:
    bind/login to LDAP
    search users/groups/devices
    validate credentials

Access Control – Config. – Cont.



- **KVM Base DN** (**D**istinguished **N**ame). The starting point in LDAP where the KVM-related objects are stored. Here:
  ou=ackvm → **o**rganizational **u**nit containing KVM objects under the domain example.com
- **RDN** = **R**elative **D**istinguished **N**ame. These define sub containers under the Base DN
- **KVM User RDN**. LDAP container where user accounts are stored
- **KVM Tx RDN**. Container for Transmitter/Tx devices entries
- **KVM User Group RDN**. Container holding LDAP groups of users
- **KVM Tx Group RDN**. Container for Transmitter/Tx groups

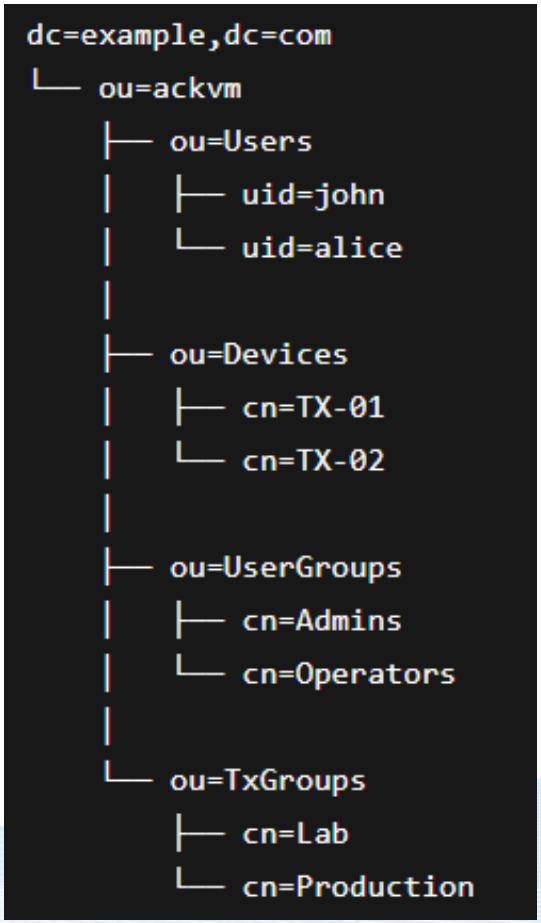
A document getting into the details of Access Control configuration is in preparation

Access Control – Config. – Cont.

- Here is an example how the LDAP structure will roughly look like

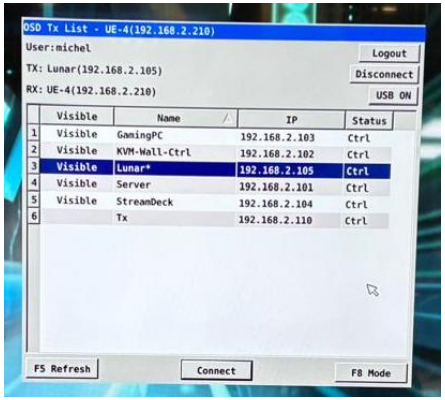
- Decoding the LDAP jargon… ☺

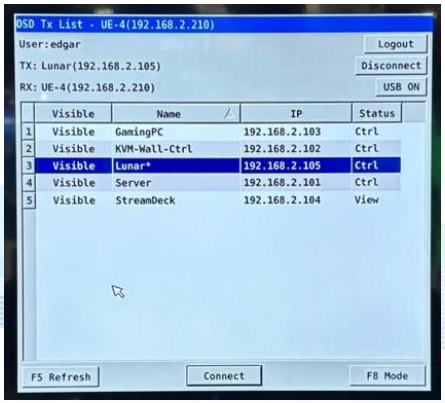
dc	Domain Component
ou	Organizational Unit
uid	User ID/Login
cn	Common Name



Access Control – User Interface

- With Access Control, operators need to enter valid credentials to be able accessing to the Tx selection drop down menu





- User: The current user. Press "Logout" to return to the Login page
- Status Column: The user permission for each Tx / Computer (Computers with "Disabled" permission for this user do not show up in the list)
- Visible Column: "Visible" Tx means the attached computer is up and running. Otherwise, the column is blank

Access Control – User Interface

- If the LDAP Server is down or not accessible, or if both the Master and Slave Tx are unavailable when using the Access Control utility, the current access permission granted when users last logged in are still valid
- However, if a user logs out, he won't be able accessing resources again until the Access Control Server or the Master / Slave Tx are back online
- Until normal operation is restored, the KVM Connection Manager utility can still be used as a back up tool to assign computers to consoles