HOW TO TROUBLESHOOT B07X-SERIES KVM SWITCHES FOR LDAP

Related Products	Article Number
KVM SWITCHES	**000001349**

Using LDAP/AD for authentication is fairly simple and uses the user's network credentials to access the KVM. There are three components involved: the Active Directory (AP), the Lightweight Directory Access Protocol (LDAP) server and the KVM authentication setup. Numerous configurations may be used. By following the directions in the owner's manual, clients should be able to configure LDAP with little to no issue. This document will address some commonly identified issues with the setup.

Basic

The Basic Mode Type is the easiest and least restrictive setup for LDAP authentication. The settings allow the Search Base to identify all active users in the AD and allow them to log into the KVM with their network credentials. This setting provides full access to the KVM (Administrator level access).

User

The User Mode Type allows access to be determined by an Access Rights Permission String, which determines access level (admin or user), KVM port accessibility, Virtual Media accessibility and Serial port accessibility. The Access Rights Permission String is applied to the user account on the AD. (Note: see information on Access Rights Permission String in this document.)

Group

The Group Mode Type allows access to be determined by an Access Rights Permission String, which determines access level (admin or user), KVM port accessibility, Virtual Media accessibility and Serial port accessibility. The Access Rights Permission String is applied to the group account on the AD. (Note: see information on Access Rights Permission String in this document.) Any active AD users placed in this group will have the rights assigned to the group.

User/Group Proximity

The proximity between a user and a KVM group in the AD should be no more than two levels apart. To eliminate the potential for this issue, it is advisable to place the group at the same level as the general body of users in the AD.

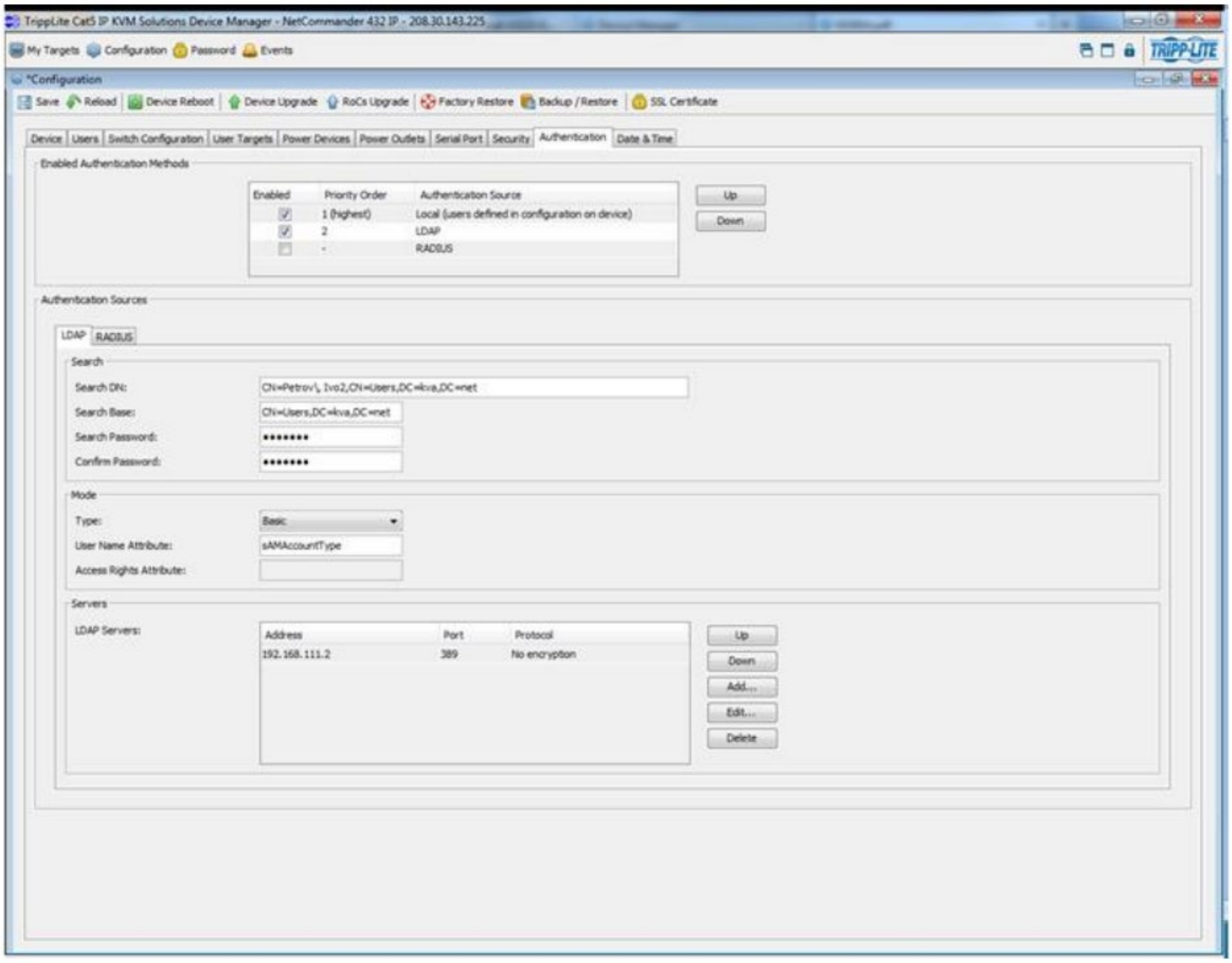
Access Rights Permission String

The Access Rights Permission String must be configured exactly as stated in the owner's manual. There should be no spaces between any characters in the string. The Access Rights Permission String must be placed in a string type attribute that is being repurposed for this function. The attribute should not be one that provides any manipulation of information from other fields. An example of a manipulated attribute would be *displayName*.

There have been some cases where a copied Access Rights Permission String has introduced corrupt characters. It may be beneficial to have the customer hand-key the permission string.

Non-Extended Schema

A Non-extended schema provides group level access from an AD Group but the permissions for the group are determined on the KVM. The B072 series of KVMs does not support non-extended schemas at this time.



TrippLite Cat5 IP KVM Solutions Device Manager - NetCommander 432 IP - 208.30.143.225

Enabled Authentication Methods

Enabled	Priority Order	Authentication Source
☑	1 (highest)	Local (users defined in configuration on device)
☑	2	LDAP
□	-	RADIUS

Authentication Sources

Search

Search DN: CN=Petrov\, Ivo2,CN=Users,DC=kva,DC=net

Search Base: CN=Users,DC=kva,DC=net

Search Password: •••••••

Confirm Password: •••••••

Mode

Type: Basic

User Name Attribute: sAMAccountType

Access Rights Attribute:

Servers

LDAP Servers:

Address	Port	Protocol
192.168.111.2	389	No encryption

Last Updated: Aug 23, 2021