LDAP integration in the Netop Portal (EN)

Article Number: 468 | Last Updated: Mon, Jan 15, 2018 7:22 AM

With the integration of Lightweight Directory Access Protocol (LDAP), the Netop Portal provides yet another way of integration into the company´s central user directory. This enables administrators to manage users and users' permissions from only one place â€“ the company's user directory. For security reasons, we use the LDAPS over the Internet to have an encrypted channel between the Netop Portal and the DCs. No passwords are stored in the Netop Portal and they will be checked on every login over an encrypted channel. This article provides details on how to set up an LDAPS over the Internet and how to configure it in the Portal. **Prerequisites**: You have an Active Directory Domain Controller. Please note that LDAPS can be configured for other types of Directories as well. Please check the manual for your LDAP Directory for ways to activate LDAPS. Ensure that a validÂ certificate (X.509 certificate) is installed in the Domain Controller. Please note that the Portal does not work with self-signed certificates. **Setting up the LDAPS over the Internet** To use LDAPS over the Internet without a VPN tunnel without exposing the Domain Controller to the Internet, you should use a Read Only Domain Controller (RODC). Using RODC allows you to add an extra layer of security to the DC as it restricts the ability of hackers to compromise corporate users (they don't have access to user passwords and they cannot push any updates to the Global Catalogue (GC). Introduced by Microsoft in Windows 2008, a RODC contains a replica of the Domain Controller data, except for user passwords (it does not store any passwords). The RODC handles the communication between the DC and the Internet. To set up the LDAPS-over-the-Internet, follow these

steps: Install an Read-only domain controllers (RODCs) in a perimeter network (DMZ) with a public IP address. For detailed information on how to plan and deploy RODCs in perimeter networks, see the Microsoft documentation. Ensure that a validÂ certificate (X.509 certificate) is installed on the RODC. Restrict access to a port of your choice and do a port forwarding on your firewall to redirect the non-standard port to port 636 (whereas 636 is the standard port for LDAP SSL encrypted connections). **Netop Portal Configuration** To properly configure the LDAP server profile when adding an LDAP authentication method in the Portal (from **Account>Authentication > Add LDAP**), besides enabling the LDAP authentication method, configure the parameters for the LDAP server:

Parameter	Description
Domain identifier	Â
LDAP Type	The authentication type, in this scenario is LDAP
Hostname	The FQDN used by the LDAP server.
Port	The TCP port used by the LDAP server.

Once you've finished the LDAP server configuration, click Save LDAP authentication method and that's it. Now the users in your Active Directory can start using the Netop Portal

References

You Don't Need A VPN Part II - LDAP Integrations, User Data Imports, & the Internet solution

>

Posted - Mon, Dec 4, 2017 2:16 PM.
Online URL: http://kb.netop.com/article/ldap-integration-in-the-netop-portal-en-468.html