Setting up TightGate-Pro (Active Directory)

After the preparation of the Active Directory server for user authentication with TightGate-Pro has been completed and the generated keytab file as well as the CA for LDAPS communication have been copied to the transfer directory of the user ***config*** on TightGate-Pro, the final configuration on TightGate-Pro can be started.

This is how it works

- Log in as administrator ***config*** and change to the menu **System preferences.**
- Select the menu item **user config. automatically for** and there select **Krb**.
- Select the menu item **Authentication method** and there **Select AD**. After the selection, further menu items appear below the menu item.
- Configure the other menu items using the following table. Please note that the example values refer to our example . example.

Menu item	Example value	Comment
Kerberos Realms*	SSO.M-PRIVACY.HOM:sso.m-privacy.hom:192.168.4.208:192.168.4.208	Specification of the REALMS,the DNS domain, the Kerberos Admin Server as well as the responsible KDCs in the form: REALM:DNS Domain:Admin Server:KDC1:KDC2... .
Kerberos Hostname*	TGPro (for single system) internet.intern.netz (for cluster system)	DNS name of the Kerberos server (usually, but not necessarily, the name of a single system or the cluster). Specific to the infrastructure at the place of use. **Attention:** If this parameter is entered incorrectly, no login is possible. A dedicated error message will not be displayed.
Import Kerberos Host Keytab*	TGPro.keytab	Selection of the keytab file stored in the transfer directory of ***config*** . The keytab file can be deleted from the transfer directory after **saving** and **applying** the settings.

Menu item	Example value	Comment
Transfer MIME type groups*	2	Defines the number and content of the groups of MIME types that may be transferred via the file lock of TightGate-Pro under AD control. A maximum of 99 groups can be created and populated with any number of MIME types. Users can be assigned to each of these groups in the Active Directory (AD). If a user is not in a transfer group, he or she cannot transfer files via the file lock. The transfer permissions of the groups are cumulative. **Attention:** The group **tgtransfer** is always required - a user must belong to it on the AD to be authorised to transfer files at all.
AD group-based login*	Yes	Determines whether the tg* groups are read from the AD. If No, only checks whether the user exists and is authenticated.

Menu item	Example value	Comment
Search for additional AD servers automatically*	No	If this menu item is activated, the system searches in the background for SRV entries of the Kerberos domains at the entered DNS servers. The responsible LDAP servers can be found in the SRV entries. Without this setting, only the servers named in the REALM are used. If this menu item is activated, a menu item for excluding certain AD/LDAP servers appears below.
Excluded LDAP servers*	–	This menu item only appears if the value **Yes** was selected under the menu item **Search for additional AD servers automatically**. Here, individual servers (DCs or GCs) can be explicitly excluded from use.
LDAP protocol	LDAP+LDAPS	Defines the protocol to be used for the connection to the Active Directory server.
—-		

Menu item	Example value	Comment
Import LDAPS-Custom-CA	–	Here the necessary certificate for the encrypted LDAP variant (LDAPS) for standard communication with Active Directory is imported. For this communication to work, the CA must be imported from the AD server in TightGate-Pro. The required CA should already be in the administrator's transfer directory ***config*** . Then it can be imported via this menu item. **Note:** The custom CA must be in Base64 encoding and can be deleted from the transfer directory after the import. Make sure that the file name of the CA does not contain any of the following characters, otherwise the CA cannot be imported: "()§'`°&;
Remove LDAPS-Custom-CA	–	Remove an already stored Custom-CA for the LDAPS communication.

After the settings have been made, they must be saved via the menu option **Save**. Subsequently, the menu option **Apply** causes the activation of the saved settings.

Checking the settings

The correctness of the settings when using an Active Directory can be checked as an administrator ***config*** via the menu item **Check network**. The following tests should be confirmed by the system with OK so that the prerequisites for cooperation with TightGate-Pro are given:

Test name	Result
Kerberos realm [Names of the REALM]	
KDC 1 with TCP:	OK
KDC1 IP DNS reverse:	OK

Test name	Result
KDC1 DNS forward:	OK
KDC1 DNS = IP:	OK
KDC 1 LDAP with TCP:	OK
Keytab Principal with SSL CN:	OK
TGT request (with keytab):	OK
AD GCs and DCs (with ports):	OK
GC ldap Port Check:	OK
GC ldaps Port Check:	OK
DC ldap Port Check:	OK
DC ldaps Port Check:	OK
AD server 1:	
Forward DNS:	OK
Reverse DNS:	OK
GSSAPI support (ldap):	OK
GSSAPI support (ldaps):	OK
–	
if necessary, further AD servers …	

Hinweis

If LDAPS is used, the tests for LDAP are displayed with **Failed** if necessary. This does not affect the functioning of TightGate-Pro, provided the connections with LDAPS are configured correctly.