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 and the CA for LDAPS communication have been copied to the user's transfer directory ***config*** on TightGate-Pro, the final configuration on TightGate-Pro can be started.

This is how it works

- Login as administrator ***config*** and switch to the menu **System defaults.**
- Select the menu item **Automatically set user preferences for** and there **Yes** Select Yes.
- Select the menu item **Authentication method** and there **AD** there. After selection, further menu items appear below the menu item.
- The other menu items are configured using the following table.

Menu item	Description	Example value
Kerberos Realms*	Specification of the REALMS, the DNS domain, the Kerberos Admin Server and the responsible KDCs in the form: REALM:DNS domain:Admin server:KDC1:KDC2... **Note:** The admin server and the KDCs can be entered as an IP address or as a name (FQDN).	AD.DOMAIN.LOCAL:ad.domain.local:192.168.5.100:192.168.5.100
Import Kerberos Host Keytab*	Selection of the Kerberos host keytab in the transfer directory of ***config*** transfer directory. **Note:** The keytab file can be deleted after **saving** and **applying** the settings from the transfer directory.	mp.keytab

Menu item	Description	Example value
Transfer MIME type groups*	Defines the number and content of groups of MIME types that may be transferred AD-controlled via the file transfer from TightGate-Pro. A maximum of 99 groups can be created and populated with any 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, they cannot transfer files via the file transfer. The transfer authorisations of the groups are cumulative.	2
TG group-based login*	Defines whether the tg* groups are read from the AD. If **No** only checks whether the user exists and is authenticated. Only if for this menu item **Yes** is selected for this menu item, the following menu items become available.	Yes

Menu item	Description	Example value
Automatically search for additional AD servers*	If this menu item is activated, the system searches in the background for SRV entries for the Kerberos domains in the DNS servers entered. The relevant 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.	No
Excluded LDAP servers*	Individual servers (DCs or GCs) can be explicitly excluded from use here.	-
LDAP protocol*	Definition of the protocol to be used for the connection to the Active Directory server. **Note:** In principle, communication between TightGate-Pro and the AD server should only take place using a functioning protocol (LDAP or LDAPS). The LDAPS protocol should preferably be used. Both protocols can be activated for test purposes.	LDAPS

Menu item	Description	Example value
Import LDAPS Custom CA*	This menu item only appears if LDAPS or LDAP+LDAPS has been selected for the LDAP protocol. The certificate required for encrypted LDAPS communication is imported here. The required CA must already be in the administrator's transfer directory ***config*** transfer directory, then it can be imported via this menu item. **Note:** The custom CA must be available in Base64 encoding and can be deleted from the transfer directory after import. Make sure that the file name of the CA does not contain any of the special characters "()§'`°&;, otherwise the import will fail.	-
Remove LDAPS Custom CA*	Remove an already stored Custom CA for LDAPS communication. This menu item only appears if an LDAPS custom CA has been imported to TightGate-Pro.	-

Menu item	Description	Example value
Read clear name when logging in from AD*	If this menu item is set to **Yes** the associated clear name is retrieved from the AD server and saved in TightGate-Pro each time a user ID logs in. As administrator ***maint*** these are then stored under the **user administration** are then displayed. If the value is set to **No** another query is displayed asking whether all clear names previously saved in TightGate-Pro should be deleted. If this is confirmed, all clear names are deleted and from then on no more clear names are retrieved from the AD server when users log in.	Yes

Once the settings have been made, they can be saved via the menu item **Save** menu item and saved via the **Apply** menu item.

Checking the settings

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

Test name	If the test is passed	In case of errors	Troubleshooting
Kerberos realm [Names of the AD server]			
KDC 1 with TCP:	OK	Failed!	The TightGate-Pro cannot reach the KDC via TCP port 88. The most common reason for this is that a firewall between TightGate-Pro and the KDC prevents this.

Test name	If the test is passed	In case of errors	Troubleshooting
KDC1 IP DNS reverse:	OK	Failed!	It is necessary to check whether one of the administrator ***config*** under the menu item **Network > Nameserver** or **Network > Local domain name servers** the IP address and the name of the AD server can be resolved forwards and backwards.
KDC1 DNS forward:	OK	Warning!	
KDC1 DNS = IP:	OK		
Keytab Principal with SSL CN:	OK	Failed!	If this test fails, the domain/REALM details do not match. Check that the domain and the REALM match in the following places: 1) Domain name in the **keytab file** 2) Under the menu item **Basic settings > DNS name in the certificate** 3) Under the menu item **System defaults > Kerberos realms**
TGT request (with keytab):	OK	Failed!	If this test fails, the test for the **Keytab Principal with SSL CN** but **OK** is OK, this is because the keytab file was not created with administrative rights. It must be ensured that the keytab file was created with an identifier **Default security group Administrator** is created.
AD GCs and DCs (with ports):			
GC ldap Port Check:	OK	Failed!	The TightGate-Pro cannot reach the GC server (Global Catalog) via TCP port 3268. Common causes for this are: 1) A firewall between TightGate-Pro and the GC prevents this. 2) The GC server does not support the LDAP protocol. It must be ensured that the firewall allows the connection and that the GC server supports the LDAP protocol.
GC ldaps Port Check:	OK	Failed!	The TightGate-Pro cannot reach the GC server (Global Catalog) via TCP port 3269. Common causes for this are: 1) A firewall between TightGate-Pro and the GC prevents this. 2) The GC server does not support the LDAPS protocol. It must be ensured that the firewall allows the connection and that the GC server supports the LDAPS protocol.
DC ldap Port Check:	OK	Failed!	The TightGate-Pro cannot reach the DC server (AD server) via TCP port 389. Common causes for this are: 1) A firewall between TightGate-Pro and the DC prevents this. 2) The AD server does not support the LDAP protocol. It must be ensured that the firewall allows the connection and that the AD server supports the LDAP protocol. **Note:** In principle, communication between TightGate-Pro and the AD server should only be authorised with a functioning protocol (LDAP or LDAPS). The LDAPS protocol should preferably be used.

Test name	If the test is passed	In case of errors	Troubleshooting
DC ldaps Port Check:	OK	Failed!	The TightGate-Pro cannot reach the DC server (AD server) via TCP port 639. Common causes for this are: 1) A firewall between TightGate-Pro and the DC prevents this. 2) The AD server does not support the LDAPS protocol. It must be ensured that the firewall allows the connection and that the AD server supports the LDAPS protocol. **Note:** In principle, communication between TightGate-Pro and the AD server should only be authorised with a functioning protocol (LDAP or LDAPS). The LDAPS protocol should preferably be used.
AD server 1:			
Forward DNS:	OK		
Reverse DNS:	OK		
GSSAPI support (ldap):	OK		
GSSAPI support (ldaps):	OK		
LDAPS certificate:	OK	Failed!	Cheks whether the LDAPS certificate is still valid. A warning is issued if the certificate is due to expire within 60 days. If the test fails, the certificate has already expired or is invalid.
–			
additional AD servers if necessary ...			