User administration via user certificates

TightGate-Pro supports certificate-based login without entering user name and password for the client operating systems Windows and Linux. Certificate-based login requires that the users already exist in TightGate-Pro. This can be done by manual creation of users or by importing users . importing users.

The user defaults, such as file transfer or audio transmission, are taken from the administrator's system-wide user defaults of the administrator ***config*** .

Generate and distribute certificates

This is required

- Only the client programs provided by m-privacy GmbH can be used. client programmes provided by can be used.
- A resolvable DNS name under which TightGate-Pro can be addressed from the internal network must be available.

This is how it works

Preparatory measures

- Logging in as administrator ***config***
- Enter the resolvable DNS name for the respective system under **settings > SSL name in the certificate**. The host name entered under **SSL name in the certificate** is stored in the respective certificate as Common Name (CN). If the host name in the SSL CN is changed, all client certificates must be regenerated and distributed to the clients (or at least the configuration files must be adapted on all clients). Before generating the client certificates and distributing them, it is strongly recommended to carefully check that the correct host name is entered.
- **Save** and **Apply**.

Generate certificates for existing users

- Log in as administrator ***maint***
- Go to **User Administration > Generate SSL Keys** to generate SSL certificates for individual groups or all users (Everyone group). After generating, you will be asked whether the keys should be exported immediately.

Distribute certificates to clients

- Open the file lock with the administrator's login data ***config***
- Change to the directory **certs**. There you will find a folder with the name of each created user with a number of certificates and configuration files. These files (not the folder itself) must be copied to **%APPDATA%\vnc** on the client computer from which TightGate-Pro is to be accessed.

Hinweis

If the folder **certs** cannot be displayed in the lock of ***config*** , please check the settings of the TightGate lock.

Revoke certificates

If certificates of individual users are to be revoked so that logon is no longer possible, this can be done with the following instructions. If a user is deleted, all certificates issued for that user are also revoked. It is therefore not necessary to revoke certificates before deleting a user.

This is how it works

- Log in as administrator ***maint***
- Select the menu item **User administration > Revoke certificate**
- Select the user IDs for which the certificates are to be revoked (selection is made by marking with the space bar)
- After confirming the selection, all certificates of the selected identifiers are revoked.

Achtung

Revoked certificates cannot be unblocked or reactivated. If necessary, new certificates must be generated and retrieved and distributed as specified above. In cluster systems, the revocation becomes effective after a waiting time of up to 10 minutes for logging in with the TightGate viewer and using the TightGate gateway. In the event of a certificate revocation, connections that have already been established remain in place until manual or automatic logout from the system. This applies equally to the TightGate viewer and the TightGate gateway.

Generate certificates in advance

As an alternative to generating certificates for existing user IDs, user certificates can also be generated in advance in any contingent. This allows users to log on to TightGate-Pro without a user account. This is generated automatically during the first login process, which reduces the administration effort.

Preparatory measures

- Log in as administrator ***config***
- Under **Settings > Authentication method**, set the menu item **User logon automatically > Cert** to **yes**
- **Save** and **Apply**

This is how it works

- Log in as administrator ***maint***

- Select the menu item **User administration > Bulk SSL key**
  A wizard starts which asks for a prefix and the number of certificates to be generated. The prefix forms the constant part of the later user name, supplemented by a sequential number. This starts with a selectable value and ends with the number of certificates to be generated. The generated certificates are automatically copied to the transfer directory of ***config*** and can be collected and distributed there.

Hinweise

- The automatically generated user names create an identical user ID (user account) at TightGate-Pro the first time a user logs in with the generated certificate. This cannot be changed later.
- No user ID (account) is created on TightGate-Pro as long as a certificate has only been generated but not yet used to log on to TightGate-Pro. The user administration of TightGate-Pro thus always contains only those identifiers that have actually already been used for logging in - regardless of the number of certificates generated in advance.

Remove/delete user

A user is removed by deleting him or her at TightGate-Pro in accordance with following these instructions.

Notes on deleting users with user certificates
The complete deletion of the user also recalls all user certificates (SSL certificates) with which the user has logged in. From now on, logging in with the certificates is no longer possible.