Benutzerverwaltung per Benutzerzertifikaten

TightGate-Pro unterstützt die zertifikatsbasierte Anmeldung ohne Eingabe von Benutzername und Passwort für die Klienten-Betriebssysteme Windows und Linux. Die zertifikatsbasierte Anmeldung setzt voraus, dass die Benutzer bereits im TightGate-Pro existieren. Dies kann durch das manuelle Anlegen von Benutzern erfolgen oder durch den Import von Benutzern.

Die Benutzervorgaben, wie z. B. der Dateitransfer oder die Audioübertragung werden dabei aus den systemweiten Benutzervorgaben des Administrators ***config*** verwendet.

Zertifikate erzeugen und verteilen

Das wird benötigt

- Es können nur die seitens der m-privacy GmbH bereitgestellten Klientenprogramme verwendet werden.
- Ein auflösbarer DNS-Name, unter dem TightGate-Pro aus dem internen Netz angesprochen werden kann, muss vorhanden sein.

So geht's

Vorbereitende Maßnahmen

- Anmeldung als Administrator ***config***
- Eintragung des auflösbaren DNS-Namens für das betreffende System unter **Einstellungen > SSL-Name im Zertifikat**. Der unter **SSL-Name im Zertifikat** eingetragene Hostname wird im jeweiligen Zertifikat als Common Name (CN) hinterlegt. Wird der Hostname in der SSL CN geändert, so sind alle Klientenzertifikate neu zu generieren und an die Klienten zu verteilen (oder zumindest auf allen Klienten die Konfigurationsdateien anzupassen). Vor der Erstellung der Klientenzertifikate und deren Verteilung empfiehlt es sich unbedingt, sorgfältig auf Eintragung des richtigen Hostnamens zu achten.
- **Speichern** und **Anwenden** durchführen.

Zertifikate für bestehende Benutzer erzeugen

- Anmeldung als Administrator ***maint***
- Unter **Benutzerverwaltung > Erzeuge SSL-Schlüssel** für einzelne Gruppen oder alle Benutzer (Gruppe Everyone) SSL-Zertifikate erzeugen. Nach dem Erzeugen wird gefragt, ob die Schlüssel gleich exportiert werden sollen.

Zertifikate auf Klienten verteilen

- Öffnen der Dateischleuse mit den Anmeldedaten des Administrators ***config***
- Wechsel in das Verzeichnis **certs**. Dort befindet sich jeweils ein Ordner mit dem Namen eines jeden angelegten Benutzers mit einer Reihe von Zertifikaten und Konfigurationsdateien. Diese Dateien (nicht der Ordner an sich) sind nach **%APPDATA%\vnc** auf dem Klientenrechner zu kopieren, von dem aus auf TightGate-Pro zugegriffen werden soll.

Hinweis

Falls der Ordner **certs** in der Schleuse von ***config*** nicht angezeigt werden kann, prüfen Sie bitte die Einstellungen der TightGate-Schleuse.

Zertifikate widerrufen

Sollen Zertifikate einzelner Benutzer widerrufen werde, damit eine Anmeldung nicht mehr möglich ist, so ist dies mit nachfolgender Anleitung möglich. Sofern ein Benutzer gelöscht wird, werden ebenfalls alle für ihn herausgegebenen Zertifikate gesperrt. Es ist also nicht notwendig Zertifikate vor dem Löschen eines Benutzers zu widerrufen.

So geht's

- Anmeldung als Administrator ***maint***
- Auswahl des Menüpunkts **Benutzerverwaltung > Rückruf Zertifikat**
- Auswahl der Benutzerkennungen, für welche die Zertifikate gesperrt werden sollen (Auswahl erfolgt durch Markieren mit der Leertaste)
- Nach der Bestätigung der Auswahl werden alle Zertifikate der ausgewählten Kennungen widerrufen.

Achtung

Widerrufene Zertifikate können nicht entsperrt oder reaktiviert werden. Nötigenfalls sind neue Zertifikate zu erzeugen und wie oben angegeben abzurufen und zu verteilen. In Clustersystemen wird die Sperre nach einer Wartezeit bis zu 10 Minuten für die Anmeldung mit dem TightGate-Viewer und die Nutzung der TightGate-Schleuse wirksam. Bereits aufgebaute Verbindungen bleiben im Fall einer Zertifikatssperre bis zur manuellen oder automatischen Abmeldung vom System bestehen. Dies betrifft den TightGate-Viewer und die TightGate-Schleuse gleichermaßen.

Zertifikate auf Vorrat erzeugen

Alternativ zur Zertifikatserzeugung für bereits vorhandene Benutzerkennungen, können Benutzerzertifikate auch in beliebigen Kontingenten im Voraus erzeugt werden. Benutzer können sich damit auch ohne Benutzeraccount an TightGate-Pro anmelden. Dieser wird im Zuge des ersten Anmeldevorgangs automatisch generiert, was den Administrationsaufwand vermindert.

Vorbereitende Maßnahmen

- Anmeldung als Administrator ***config***
- Unter **Einstellungen > Authentisierungsmethode** den Menüpunkt **Benutzerverz. automatisch > Cert** auf **ja** setzen
- **Speichern** und **Anwenden**

So geht's

- Anmeldung als Administrator ***maint***
- Auswahl des Menüpunkts **Benutzerverwaltung > Massen-SSL-Schlüssel**
  Es startet ein Assistent, der ein Präfix und die Anzahl zu erzeugender Zertifikate abfragt. Der Präfix bildet den konstanten Teil des späteren Benutzernamens, ergänzt um eine laufende Nummer. Diese beginnt bei einem wählbaren Wert und endet bei der Anzahl der zu erzeugenden Zertifikate. Die erzeugten Zertifikate werden automatisch in das Transfer-Verzeichnis von ***config*** kopiert und können dort abgeholt und verteilt werden.

Hinweise

- Die automatisch generierten Benutzernamen legen bei der ersten Anmeldung mit dem erzeugten Zertifikat eine gleichlautende Benutzerkennung (Benutzerkonto, Account) auf TightGate-Pro an. Diese kann nachträglich nicht verändert werden.
- Es wird keine Benutzerkennung (Account) auf TightGate-Pro erzeugt, solange ein Zertifikat nur generiert, jedoch noch nicht zur Anmeldung an TightGate-Pro verwendet wurde. Die Benutzerverwaltung von TightGate-Pro enthält damit stets nur solche Kennungen, die tatsächlich bereits zur Anmeldung verwendet wurden - unabhängig von der Zahl der im Voraus erzeugten Zertifikate.

Benutzer entfernen/löschen

Entfernt wird ein Benutzer, indem er auf TightGate-Pro nach dieser Anleitung gelöscht wird.

Hinweise zum Löschen bei einer Benutzerverwaltung mittels Benutzerzertifikaten
Die komplette Löschung des Benutzers ruft auch alle Benutzerzertifikate (SSL-Zertifikate), mit denen sich der Benutzer angemeldet hat zurück. Eine Anmeldung mit den Zertifikaten ist fortan nicht mehr möglich.