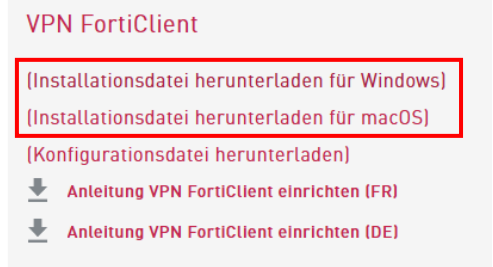
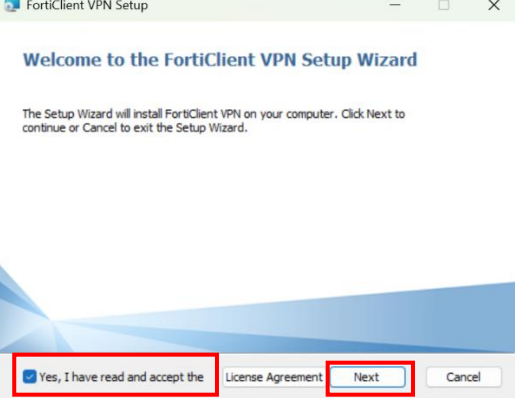
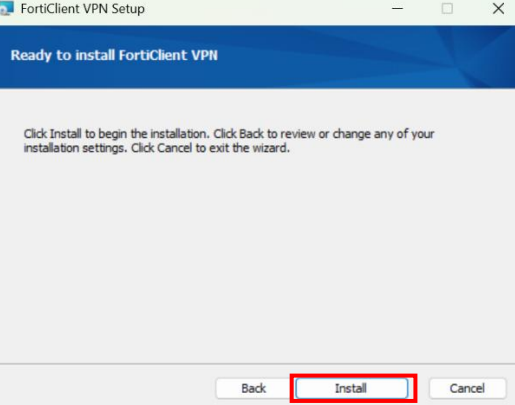
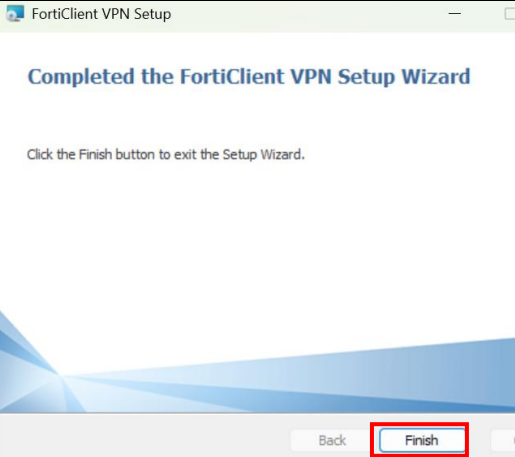


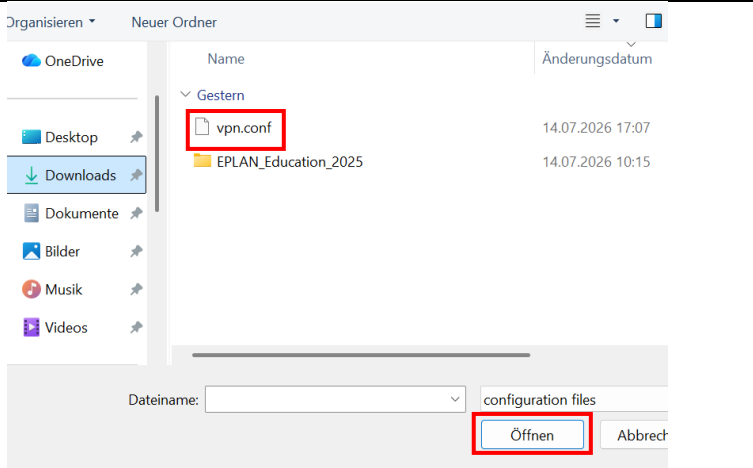
Table des matières

1.	Installation de FortiClient	2
1.1.	Instructions	2
2.	Configuration automatique	3
2.1.	Droits d'administrateur	3
2.2.	Instructions	3
3.	Configuration manuelle	5
3.1.	Cas d'utilisation	5
3.2.	Instructions	5

1. Installation de FortiClient

1.1. Guide

Télécharger le fichier d'installation de FortiClient (fichier d'installation macOS)	
Lancer le fichier d'installation	
Cliquer sur « Yes, I have read... » Cliquer sur « Next »	
Cliquez sur « Install »	
Cliquez sur « Finish ». FortiClient est ainsi installé. Pour la configuration, passez au chapitre 2 ou 3	

Sélectionner « XML » Sélectionnez ensuite « Importer la configuration XML ».	
Rechercher et ouvrir le fichier « vpn.conf »	
Récupérer le mot de passe à importer à partir du fichier texte : Identifiants	
Une fois l'importation terminée, des droits d'administrateur sont nécessaires pour valider la configuration.	
Une fois la confirmation effectuée, la connexion « HFTM » s'affiche. Cliquez ensuite sur « Se connecter »	

3. Configuration manuelle

3.1. Cas d'utilisation

La configuration manuelle est effectuée si des connexions existantes **doivent être conservées** ou en cas **d'absence de droits d'administrateur**

3.2. Instructions

[illegible]

Effectuez les réglages de base suivants : - Nom de la connexion : HFTM - Passerelle distante : vc.hftm.ch - Méthode d'authentification : Clé - Clé issue des identifiants d'accès - Paramètres d'authentification unique : Activer - Ajuster le port : 9443	Neue VPN Verbindung VPN: SSL-VPN IPsec-VPN XML Verbindungsname: HFTM Beschreibung: Verbindung zur hftm Remote Gateway: vc.hftm.ch Authentifizierungsmethode: Schlüssel Failover SSL VPN: [Keines] Single Sign On Settings: ☒ Aktiviere Single Sign On (SSO) für den VPN Tunnel Port anpassen: 9443 ☐ Verwende externen Browser als User-Agent für SAML
Ouvrir les paramètres avancés Paramètres VPN : - IKE : version 2	Experteneinstellungen VPN Einstellungen IKE ☐ Version 1 ☒ Version 2 Address Assignment: ☒ Modus Konfiguration ☐ Manuell setzen ☐ DHCP über IPsec Encapsulation: ☒ IKE UDP Port ☐ IPsec over TCP ☐ Auto (UDP fallback TCP) 500
Paramètres de la phase 1 : - Proposition IKE : comme sur l'image - Groupe DH : 20, 21	Phase 1 IKE Vorschlag: Verschlüsselung: AES128 Authentifizierung: SHA256 Verschlüsselung: AES256 Authentifizierung: SHA256 DH Gruppe: ☐ 1 ☐ 2 ☐ 5 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☒ 20 ☒ 21 Schlüssel: 86400 Sek Gültigkeitsdauer: Optional Lokale ID: ☒ Dead Peer Erkennung ☒ NAT Traversal ☐ Aktiviere Local LAN
Paramètres de la phase 2 : - Proposition IKE : comme sur l'image - Groupe DH : 21	Phase 2 IKE Vorschlag: Verschlüsselung: AES128 Authentifizierung: SHA256 Verschlüsselung: AES256 Authentifizierung: SHA256 Schlüssel: ☒ 43200 Sekunden ☐ 5120 KBytes Gültigkeitsdauer: ☒ Replay Erkennung aktivieren ☒ Perfect Forward Secrecy (PFS) aktivieren DH Gruppe: 21
Pour finir, cliquez sur « Enregistrer »	Abbrechen Sichern

Cliquez ensuite sur « Se connecter » et connectez-vous avec vos identifiants Office.

La connexion au réseau hftm s'établit alors.

