

## Accès spécifiques VPN SoftEther

### Accès pour certains étudiants de l'ICOM sur certaines machines installées dans les salles de cours du bâtiment I

#### Plateforme Windows

#### Pré requis

Pour accéder aux machines des salles de cours du bâtiment I :

- vous devez être référencé et autorisé (les demandes d'accès se font en contactant la hotline de la DSI)
- vous devez avoir installé et configuré le client VPN SoftEther sur votre poste
- vous devez disposer d'un logiciel de prise en main à distance adapté à la situation (en général VNC pour vous connecter à un Mac, Microsoft Remote Desktop pour vous connecter à un PC Windows).

Le principe de connexion est le suivant :

Une fois connecté au VPN SoftEther, un portail web d'authentification s'affiche automatiquement. Une fois authentifié sur ce portail, la connexion via le logiciel de prise à distance est possible tant que la session web du portail est active ou réduite.

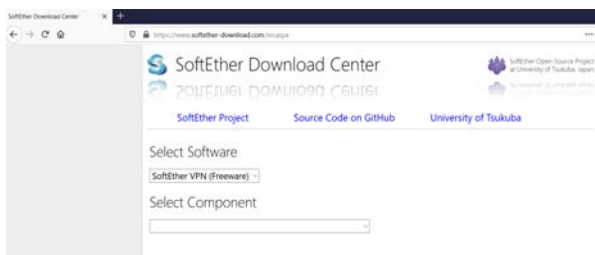
L'infrastructure VPN Open source SoftEther constituée d'un serveur principal et d'un serveur secondaire nécessite l'installation d'un programme SoftEther sur votre poste pour assurer une session VPN sécurisée, requêtes DNS comprises.

Le paramétrage ci-dessous est validé pour tous les systèmes Windows 10 (32 bits et 64 bits), les copies d'écran du présent document ont été réalisées depuis un windows 10 version 1903.

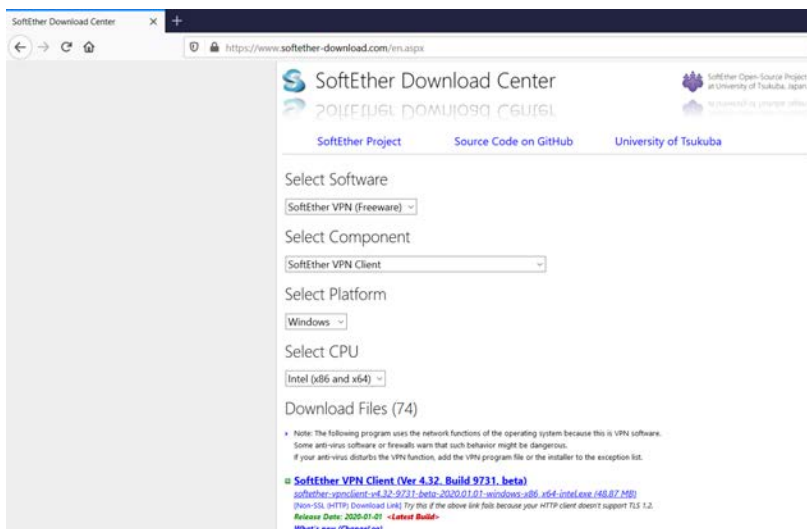
Une fois connecté en VPN, tous les flux réseau de l'ordinateur connecté sont dirigés sur le serveur VPN de l'Université et par conséquent, les règles de filtrage réseau de l'université s'appliquent sur l'ordinateur tant qu'il est connecté en VPN.

#### I – Téléchargement du client SoftEther

Le client SoftEther étant régulièrement remis à jour, il convient lors de l'installation d'utiliser la version la plus récente téléchargée sur le site <https://www.softether-download.com/en.aspx>



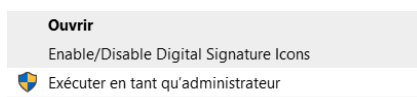
Sélectionnez les choix suivants pour faire apparaître la dernière version du client Windows SoftEther. Actuellement c'est la version SoftEther VPN Client (Ver 4.32, Build 9731, beta) qu'il faut télécharger en cliquant dessus.



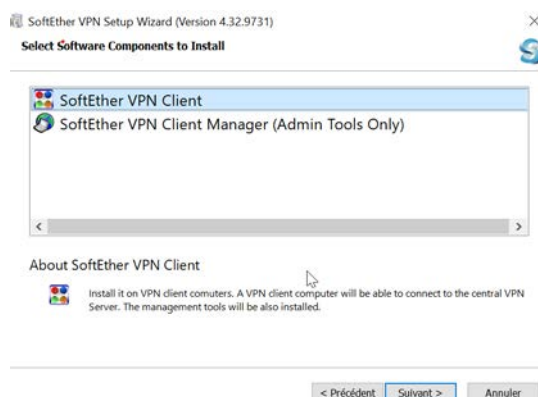
## II – Installation du client SoftEther

Une fois l'installation du client SoftEther téléchargé sur votre PC :

- Faites un clic droit sur le nom du programme et sélectionner Exécuter en tant qu'administrateur

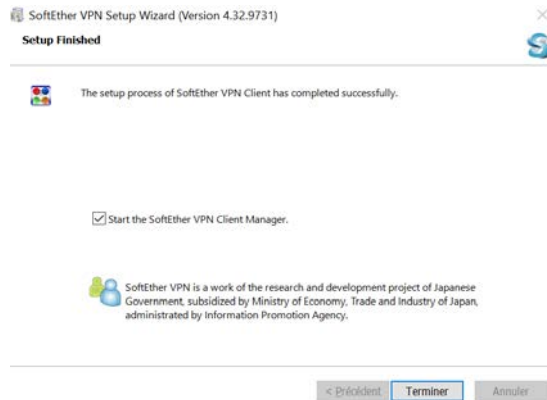


Si votre session Windows ne possède pas les droits Administrateurs, une bannière vous invitera à saisir l'identifiant et le mot de passe d'une session ayant des droits Administrateurs.





- Sélectionnez **SoftEther VPN Client**

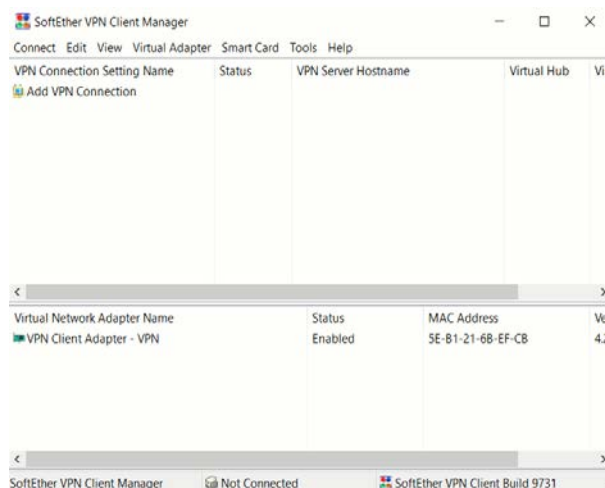
- Cliquez sur le bouton **Suivant** jusqu'à faire afficher la fenêtre suivante :



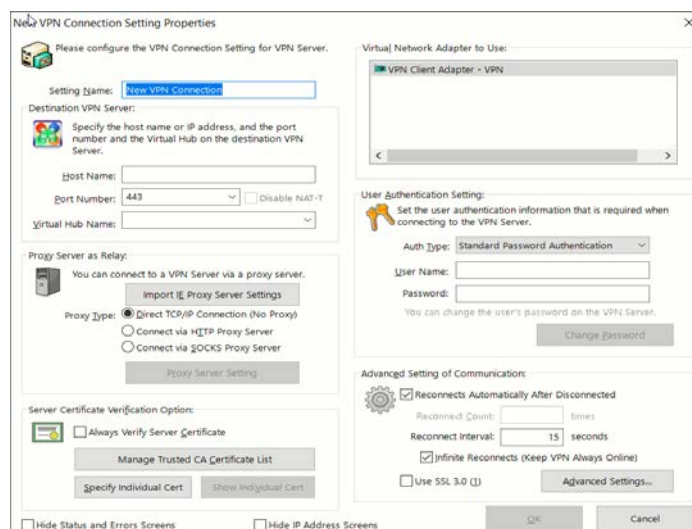
- Cliquez sur le bouton **Terminer**

### III – Paramétrage de la session VPN sur le serveur Principal

- Cliquez sur l'icône **SoftEther VPN Client Manager** qui se trouve sur le bureau  pour lancer le gestionnaire VPN, ou faites un double clic sur l'icône SofEther  situé en bas à droite du bureau.



- Cliquez sur **Add VPN Connection** pour ouvrir la fenêtre de paramétrage



- Saisissez les informations suivantes :

Dans « Setting Name » : **VPN Lyon 2 – Serveur Principal**

Dans « Host Name » : **vpn-lyon2-p.univ-lyon2.fr**

Dans « Virtual Hub Name » : **ETU**

- Cliquez sur « Standard Password Authentication » pour choisir dans la liste déroulante **RADIUS or NT Domain Authentication**

- Saisissez les informations suivantes :

Dans « User Name » : votre identifiant/login Lyon 2 (par ex **ddupont**)

Dans « Password » : le **mot de passe** de votre identifiant Lyon 2

- Cliquez sur la case « **Infinite Reconnects (Keep VPN Online)** » pour activer le champ « **Reconnect Count** » et saisissez **10** dans ce champ.

- Cliquez sur le bouton **OK** pour finir la saisie

New VPN Connection Setting Properties

Please configure the VPN Connection Setting for VPN Server.

Setting Name: **VPN Lyon 2 – Serveur Principal**

Destination VPN Server:

Specify the host name or IP address, and the port number and the Virtual Hub on the destination VPN Server.

Host Name: **vpn-lyon2-p.univ-lyon2.fr**

Port Number: 443 ☐ Disable NAT-T

Virtual Hub Name: **ETU**

Proxy Server as Relay:

You can connect to a VPN Server via a proxy server.

Import IE Proxy Server Settings

Proxy Type: ☒ Direct TCP/IP Connection (No Proxy)  
☐ Connect via HTTP Proxy Server  
☐ Connect via SOCKS Proxy Server

Proxy Server Setting

Server Certificate Verification Option:

☐ Always Verify Server Certificate

Manage Trusted CA Certificate List

Specify Individual Cert Show Individual Cert

Virtual Network Adapter to Use:

VPN Client Adapter - VPN

User Authentication Setting:

Set the user authentication information that is required when connecting to the VPN Server.

Auth Type: **RADIUS or NT Domain Authentication**

User Name: **ddupont**

Password: **.....**

Advanced Setting of Communication:

☒ Reconnects Automatically After Disconnected

Reconnect Count: **10** times

Reconnect Interval: 15 seconds

☒ **Infinite Reconnects (Keep VPN Always Online)**

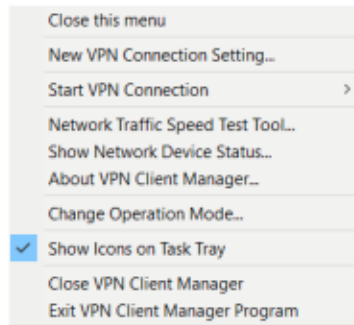
☐ Use SSL 3.0 (1) Advanced Settings...

☐ Hide Status and Errors Screens ☐ Hide IP Address Screens

OK Cancel

## IV – Lancement de la session VPN sur le serveur Principal

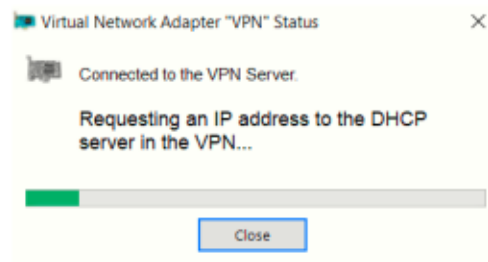
Faire un clic droit sur l'icône SofEther  situé en bas à droite du bureau



Sélectionner **Start VPN Connection** pour sélectionner la session VPN suivante

VPN Lyon 2 – Serveur Principal - vpn-lyon2-p.univ-lyon2.fr (Direct TCP/IP Connection) [ETU]

Cette fenêtre s’affiche brièvement



Une fois la connexion VPN active, la fenêtre indiquant le n° IP s’affiche brièvement

