



## ***Projet Mercure V2 et Demeter Document d'installation du client VPN***

# **Document d'installation du client VPN MERCURE V2 et DEMETER**

### **État**

État	Acteur/Structure	Date d'état
Rédigé par	Olivier PERDRIEL / BSIP	13/09/2019
Relu par		
Validé par		

### **Tableau d'historique des versions**

Version	Motif et nature de l'évolution	Acteurs	Date d'évolution
0.1	Rédaction initiale	E.FARS	27/04/2018
0.2	Test d'installation sur un poste Windows et complément	E.FARS	04/05/2018
1	Compléments	E.FARS	10/05/2018
1.2	Prise en charge de l'installation sous Linux	E.FARS	06/09/2018
1.3	Prise en compte des remarques des RMSI	E.FARS	07/01/2019
1.4	Adaptations à Windows 10 et prise en compte des premiers retours des DDI et des services déconcentrés	O. PERDRIEL	06/05/2019
1.5	Adaptations à MAC OS	O. PERDRIEL	13/09/2019
1.6	Prise en compte du VPN Demeter	O. PERDRIEL	13/11/2019

# Table des matières

<b>I. PRÉAMBULE.....</b>	<b>3</b>
<b>II. PRÉ-REQUIS ET RECOMMANDATIONS SUR LES POSTES WINDOWS.....</b>	<b>3</b>
<b>III. INSTALLATION DU CLIENT BIG-IP EDGE CLIENT POUR WINDOWS.....</b>	<b>3</b>
Installation interactive du client BIG-IP EDGE pour Windows.....	3
Installation silencieuse du client BIG-IP EDGE Client pour Windows.....	6
Vérification de la création des services Windows.....	7
Vérification de la création des interfaces réseau virtuelles.....	7
Accès VPN sous Windows.....	8
<b>IV. INSTALLATION DU CLIENT VPN BIGIP POUR LINUX.....</b>	<b>9</b>
<b>V. INSTALLATION DU CLIENT VPN BIGIP POUR MAC OS.....</b>	<b>10</b>
<b>VI. VPN SANS CLIENT : F5 HELPER APPS POUR INSPECTION ENDPOINT ET VPN.....</b>	<b>10</b>
Installation interactive des composants F5 Helper Apps sur Windows.....	11
Installation silencieuse des composants F5 Helper Apps sur Windows.....	13
Vérification de l'installation des services.....	13
<b>VII. PROBLÈMES CONNUS.....</b>	<b>14</b>

## I. Préambule

BIG-IP Edge Client est une application native spécifique à la plate-forme BIG-IP APM de F5 (Nouveau dispositif d'accès distant utilisé pour les VPNs du MAA) pour les systèmes d'exploitation de bureau. BIG-IP EDGE Client fournit l'accès aux réseaux privés virtuels (VPN) Mercure V2 et Demeter (dédié aux EPL d'enseignement agricole). Il permet aussi l'inspection des points de terminaison. Lors de la connexion VPN, il peut également démarrer des applications tierces configurées conformément à une stratégie d'accès aux systèmes d'information.

Le but du BIG-IP Edge Client de F5 est d'établir et de maintenir un tunnel VPN entre un poste de travail informatique et un serveur BIG-IP APM. Ce dernier peut jouer le rôle de filtrage pour les accès aux différents réseaux et ressources autorisées.

Ce document décrit l'installation manuelle et industrialisée du client BIG-IP EDGE pour les clients Windows, Linux et MAC OS.

Pour le VPN Demeter, seul le client Windows est supporté.

## II. Pré-requis et recommandations sur les postes Windows

- ◆ Avoir un certificat agent valide et issu de l'IGC du MAA stocké dans le magasin de certificat Windows : certmgr.msc → Personnel → certificats,
- ◆ L'option proxy doit être configurée dans les paramètres Internet de Windows. En effet, dans certains cas, les paramètres de proxy client (http://conf.proxy.national.agri/) sont nécessaires afin de valider la connexion au tunnel VPN. Pour le VPN Demeter cette option n'est pas nécessaire.
- ◆ Pour Windows 10 :
  - ✗ **Ne pas désinstaller le browser Windows EDGE (EDGEHTML) même si ce dernier n'est pas utilisé par les utilisateurs.**
- ◆ Disposer des droits d'accès à un compte administrateur local afin de pouvoir effectuer l'installation en réalisant une élévation de privilège,
- ◆ Version BIG-IP EDGE CLIENT à installer sur les postes Windows : version 7.1.7.1 publié par F5 le 17/08/2018. Pour l'AC du MAA et les DRAAF, la version 7.1.6 retenue pour le packaging de l'installation automatique via le paquet WAPT fourni par le BIP peut être maintenue car elle sera mise à jour automatiquement lors de la première connexion du poste de travail à la plate-forme BIG-IP APM.

**Il est recommandé de ne pas installer une version du client BIG-IP EDGE téléchargée directement du site internet de F5.** En effet, la plate-forme BIG-IP APM mise en place dans le Datacenter du MAA assemble les composants d'installation à partir de packages signés. Ainsi, après avoir sélectionné les options de configuration dans le profil de connectivité VPN, le package d'installation des clients est généré par la plate-forme BIGIP puis il est mis à la disposition des utilisateurs.

Les composants et les options APM retenus sont inclus dans un fichier de configuration, config.f5c du package BIG-IP Edge Client. Au cours de l'installation, le fichier de configuration config.f5c est appliqué sur les PC clients. Ceci minimise la configuration manuelle par l'utilisateur.

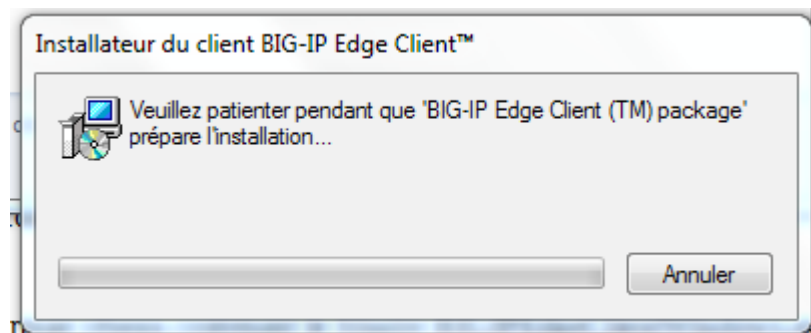
## III. Installation du client BIG-IP EDGE CLIENT pour Windows

### 1. INSTALLATION INTERACTIVE DU CLIENT BIG-IP EDGE POUR WINDOWS

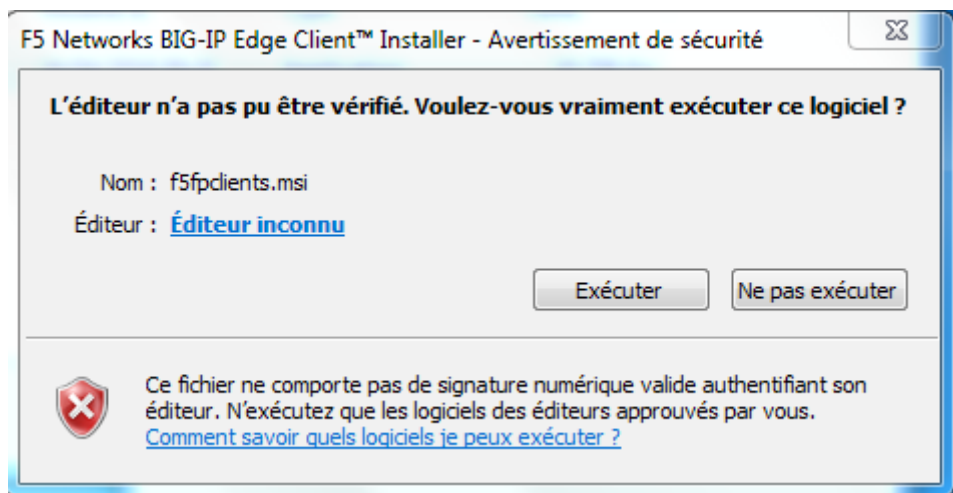
Le package d'installation du client BIG-IP EDGE a été généré par la plate-forme BIG-IP APM intégrée dans le Datacenter du MAA avant d'être mis à disposition des équipes d'assistance aux utilisateurs. Ce package est composé du fichier exécutable BIGIPEdgeClientWindows.exe à exécuter sur un poste Windows avec un compte ayant des privilèges administrateur ou permettant une élévation de privilèges.

Pour lancer l'installation, effectuer un double clic sur le binaire « BIGIPEdgeClientWindows.exe ». Un installateur vous guidera pas à pas pour cette installation. Les captures suivantes illustrent les étapes d'une installation interactive.

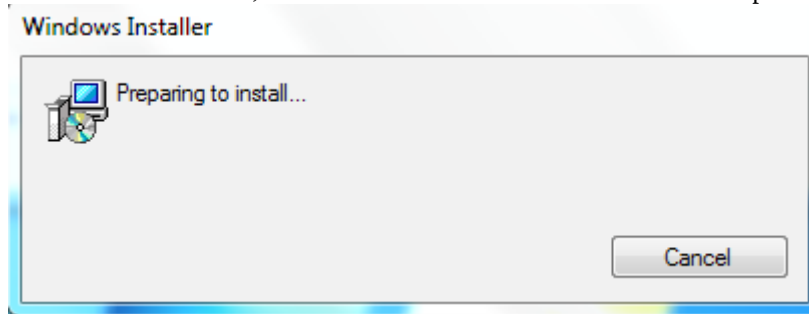
**Cliquer** deux fois sur l'exécutable « BIGIPEdgeClientWindows.exe » :



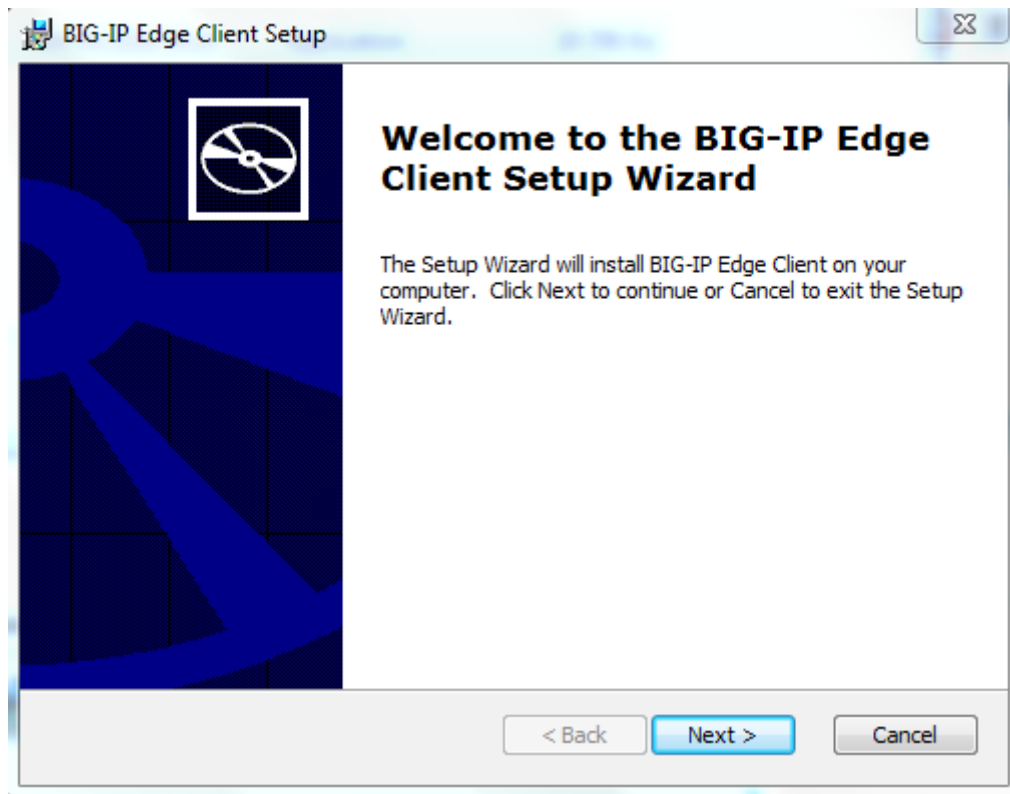
Si l'avertissement de sécurité suivant s'affiche, cliquer sur **Exécuter** pour continuer l'installation :



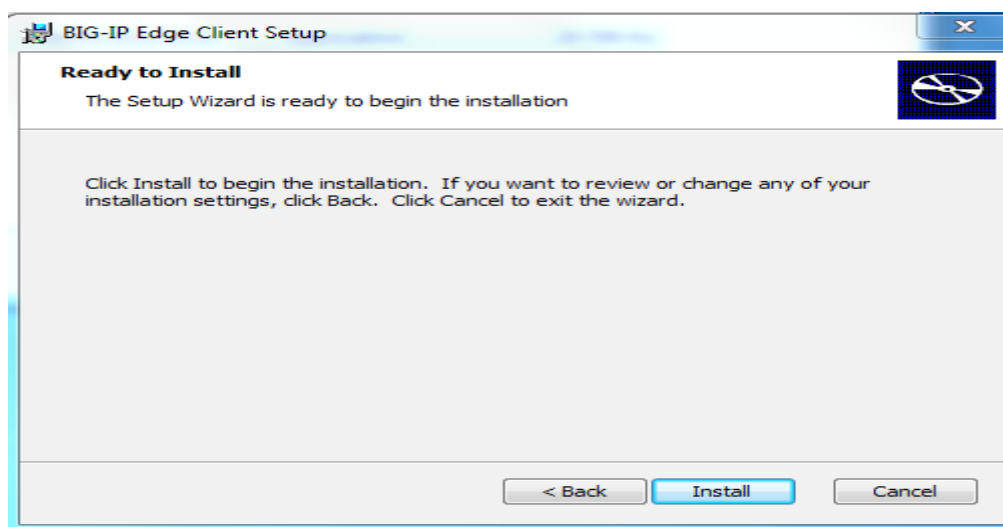
Après avoir cliqué sur le bouton Exécuter, l'installateur Windows se lance comme illustré par la capture suivante :



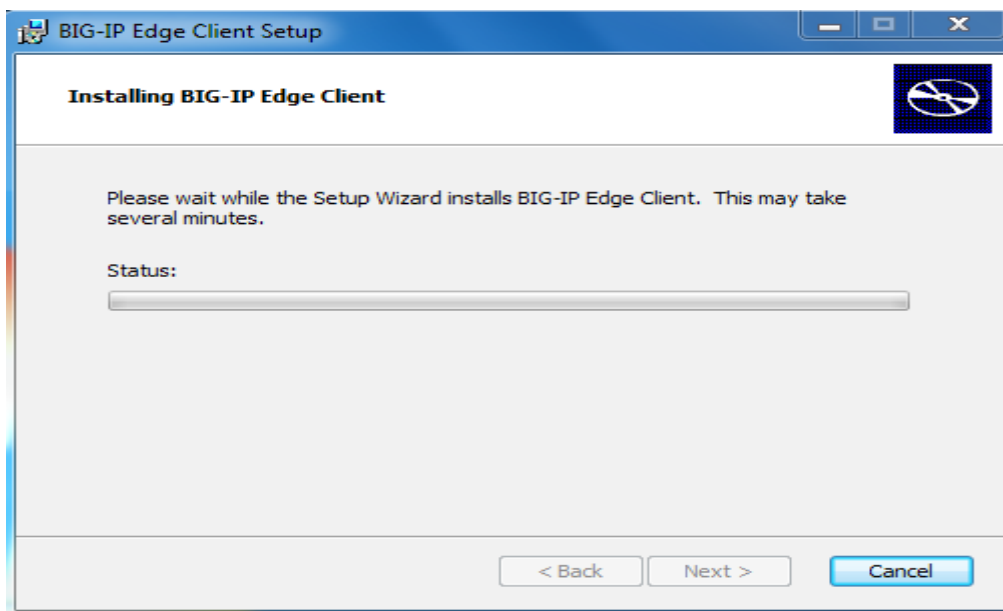
Dans la fenêtre de bienvenue, cliquez sur « Next » pour continuer l'installation :



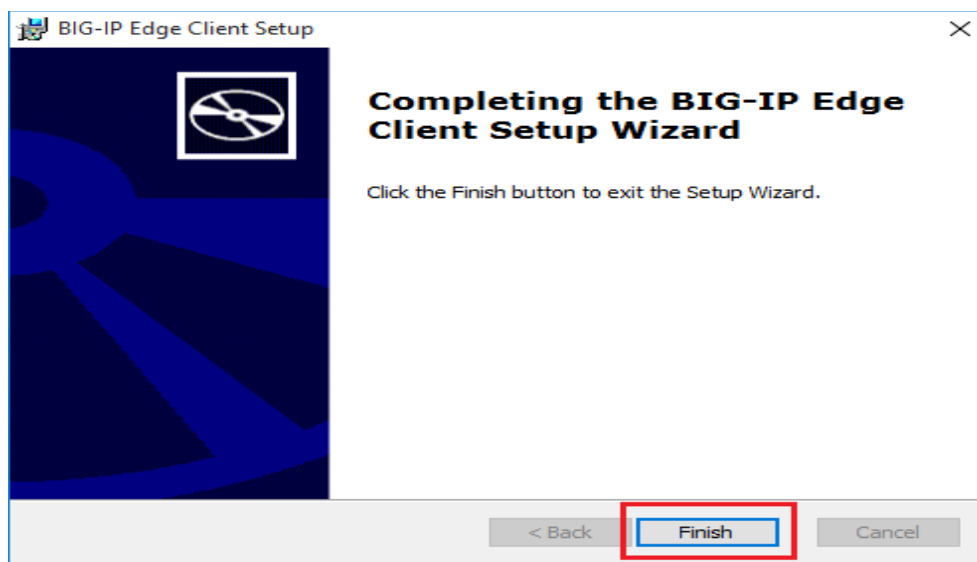
Pour démarrer l'installation du client EDGE, au menu suivant cliquez sur **Install** :



L'installation se lance et l'installateur vous invite à patienter comme illustré ci-après :



Pour finir l'installation, cliquez sur **Finish** :



NB : un redémarrage peut être nécessaire à la fin de l'installation.

## 2. INSTALLATION SILENCIEUSE DU CLIENT BIG-IP EDGE CLIENT POUR WINDOWS

L'installation industrialisée est basée sur l'utilitaire misexec.exe de Microsoft. Pour automatiser l'installation, il faut déposer un package sur un partage (share) réseau, par exemple sur l'instance NAS de l'AC « Bur-file-AC01-1.ad.national.agri ». Le package est composé du répertoire EDGE-Client-Windows qui contient notamment le fichier f5fpclients.msi qui sera lancé avec l'installateur msixec.exe.

Pour une installation silencieuse, à partir d'un poste de travail, cliquez sur démarrer puis exécutez la commande (à adapter en fonction du contexte) :

```
msiexec /i \\Bur-file-AC01-1.ad.national.agri\sources\F5\f5fpclients.msi /qn /quiet
```

L'installation du client EDGE démarre et ne demande aucune action à l'utilisateur. Pour rappel, cela nécessite une élévation de privilèges administrateur.

A la fin de l'installation, le poste redémarre automatiquement.

### 3. VÉRIFICATION DE LA CRÉATION DES SERVICES WINDOWS

Après installation du client BIG-IP EDGE et redémarrage du poste, on peut vérifier que l'installateur a bien créé **6 services pour Windows 7 et 4 services pour Windows 10**, un driver d'une carte réseau virtuelle appelé « APM Network Access », une entrée dans le menu démarrer appelée BIG-IP EDGE Client associée à l'icône suivante :



BIG-IP Edge Client

En ligne de commande, on peut vérifier la création et du démarrage des six (6) services Windows (**pour Windows 7**)

```
C:\Users\localadmin>net start ! findstr /i F5
F5 Networks Component Installer
F5 Networks Credentials Management Service
F5 Networks DNS Relay Proxy Service
F5 Networks Inspector Service
F5 Networks Machine Certificate Checker service
F5 Networks Traffic Control Service
```

Avec l'aide de la console MMC des services, on vérifie que les 6 services F5 sont en mode « démarrage automatique »(pour Windows 7) :

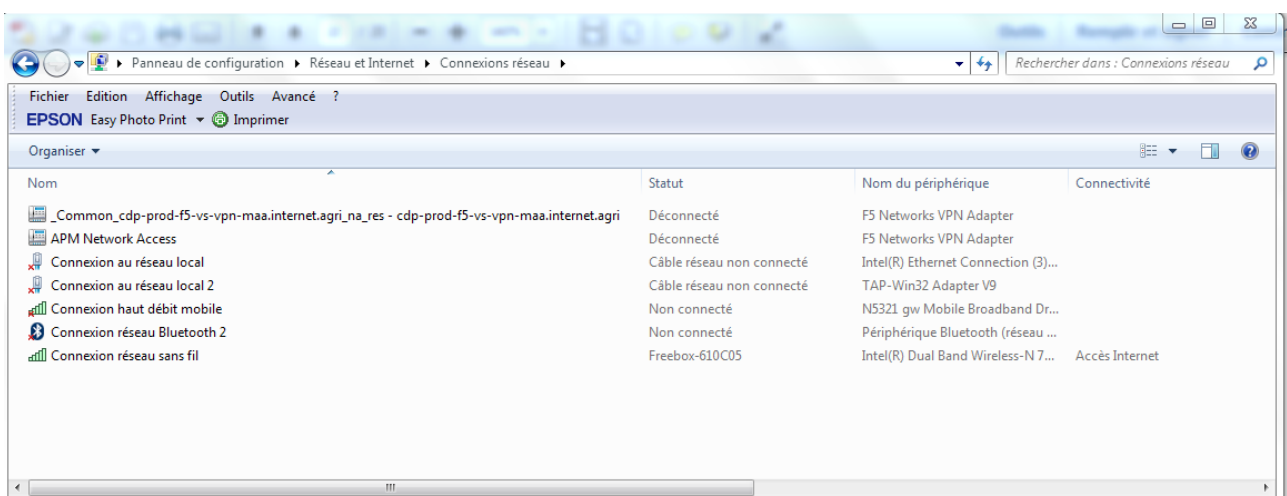
F5 Networks Component Installer	Installs and updates F5 client components on PCs without requiring administrative rights for user accounts.	Démarré	Automatique	Système local
F5 Networks Credentials Management Service	Manages Windows logon credentials for signing on to FirePass and BIG-IP Edge Gateway.	Démarré	Automatique	Système local
F5 Networks DNS Relay Proxy Service	Support name resolution without requiring administrative rights for user accounts.	Démarré	Automatique	Système local
F5 Networks Inspector Service	Supports endpoint security checks without requiring administrative rights for user accounts	Démarré	Automatique	Système local
F5 Networks Machine Certificate Checker service	Allows to check machine certificates	Démarré	Automatique	Système local
F5 Networks Traffic Control Service	Support traffic filtering without requiring administrative rights for user accounts.	Démarré	Automatique	Système local

#### Cas particulier du service DNS RELAY Proxy :

Le service de relais DNS est un service Windows facultatif qui permet aux exceptions de tunnel basées sur un nom d'hôte complet de fonctionner correctement. Le service de relais DNS facilite la gestion rapide des requêtes DNS et prend les décisions de gestion DNS pour le tunnel et le DNS local du client. Lorsque ce composant est manquant, les services VPN ou AppTunnel peuvent ne pas fonctionner correctement ou les requêtes DNS peuvent être retardées, ce qui entraîne une réponse lente aux demandes DNS. Pour que le trafic ne traverse pas le tunnel, ce service intercepte les requêtes DNS effectuées par le PC, écoute la réponse, puis ajoute des routes temporaires à la table de routage pour toutes les adresses renvoyées. Cependant, dans le cas du MAA, tout le trafic est dirigé dans le tunnel VPN (pas de split tunneling), donc ce cas ne s'applique pas.

### 4. VÉRIFICATION DE LA CRÉATION DES INTERFACES RÉSEAU VIRTUELLES

On ouvrant le panneau de configuration réseau, on peut vérifier qu'une interface réseau virtuelle dénommée « APM Network Access » de type accès distant et VPN est créée, comme illustré par la capture suivante :



L'APM utilise un mécanisme automatique pour attribuer des adresses IP aux utilisateurs VPN. Les adresses disponibles

sont sélectionnées et réservées dans un pool de location IPV4 ou IPV6 et restituées au pool après la fin de la session VPN d'un utilisateur.

## 5. ACCÈS VPN SOUS WINDOWS

L'interface utilisateur BIG-IP Edge Client pour Windows affiche les options de connexion illustrées dans la capture présentée ci-après.

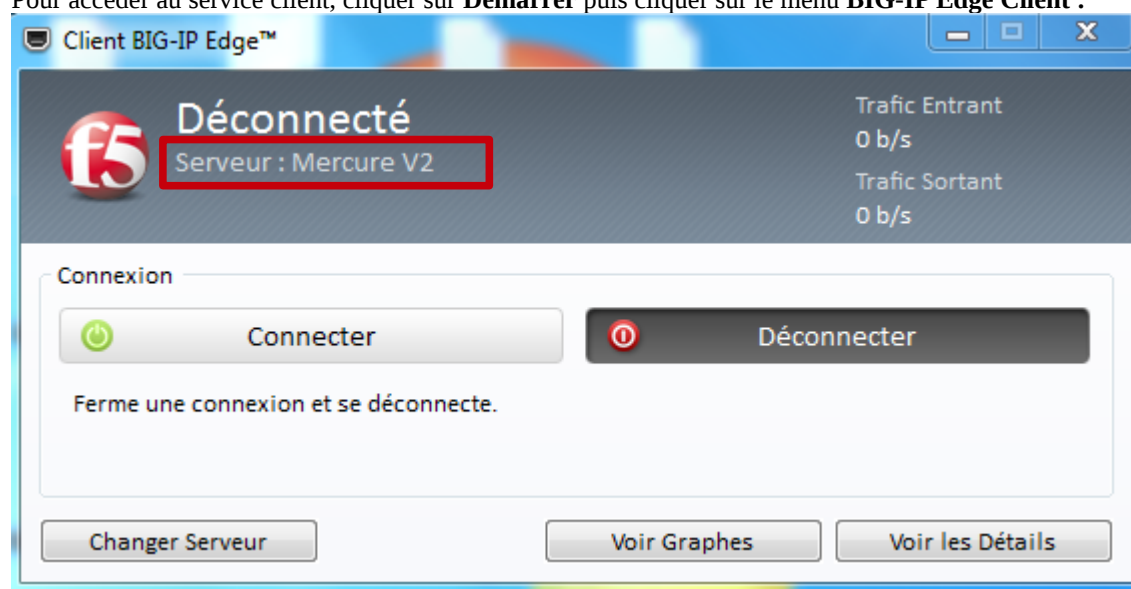
**Connecter** : démarre et maintient une connexion d'accès sécurisée à tout moment, quel que soit l'emplacement du réseau.

**Déconnecter** : arrête une connexion d'accès sécurisé active et empêche le client de se reconnecter jusqu'à ce qu'un utilisateur clique sur Connecter.

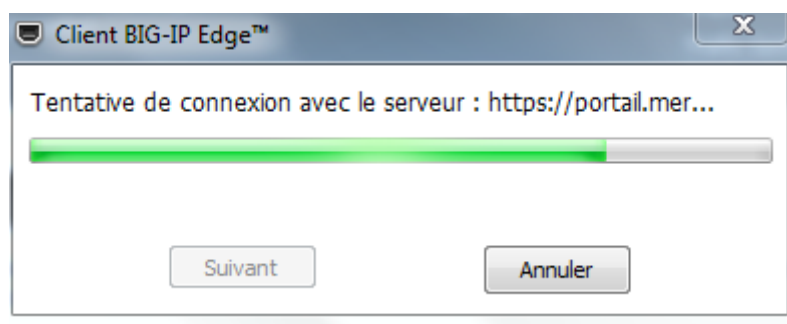
**Changer Serveur** : utilisé uniquement pour les utilisateurs des EPL de l'enseignement agricole qui accèdent au VPN MercureV2 et au VPN Demeter : permet de basculer entre ces 2 VPN. Des raccourcis Windows fournis dans le kit d'installation de Demeter permettent de simplifier ces bascules.

L'option **Auto-Connect** a été désactivée car elle nécessite de préciser tous les suffixes DNS dans les profils de connectivité pour déterminer quand l'ordinateur se trouve sur un réseau local défini. Lorsqu'elle est activée, cette option démarre une connexion d'accès sécurisée au besoin. Ainsi lorsque l'ordinateur n'est pas sur un réseau local défini, la connexion d'accès sécurisé démarre. A l'inverse, lorsque l'ordinateur est sur un réseau local, le client se déconnecte mais reste actif dans la barre d'état système.

Pour accéder au service client, cliquer sur **Démarrer** puis cliquer sur le menu **BIG-IP Edge Client** :



Le Client BIG-IP EDGE va établir une connexion SSL automatiquement avec le serveur virtuel VPN MercureV2 (<https://portail.mercurev2.agriculture.gouv.fr>) ou avec le serveur virtuel VPN Demeter (<https://portail.demeter.agriculture.gouv.fr>) :



En cas d'impossibilité de contacter le serveur virtuel VPN MercureV2 ou Demeter, le client BIG-IP EDGE affiche le message « Impossible de contacter le serveur. Changer de serveur ? ». Dans ce cas, il faut contacter le centre de services (par exemple en ouvrant un ticket IWS).



## iv. Installation du client VPN BIGIP pour Linux (VPN MercureV2 uniquement)

Pour les utilisateurs utilisant un système d'exploitation Linux, le client VPN BIGIP est décliné en un composant CLI (ligne de commande) et un composant client Accès Network pour un accès via le navigateur.

**Le client Accès Network est à privilégier.**

Pour le composant client Accès Network, le nouveau dispositif prend en charge les principales fonctionnalités d'accès réseau, à l'exception de drive mappings et de certaines fonctionnalités de contrôle de la sécurité des terminaux clients.

Pour la ligne de commande pour Linux, le nouveau dispositif ne prend en charge que l'établissement de la connexion.

### ◆ Client Accès Network pour un accès via le navigateur (composant client Network Access) :

Pour les systèmes Linux, Mac OS X et Windows, le composant client Network Access est disponible en téléchargement automatique à partir de l'URL « <https://portail.mercurev2.agriculture.gouv.fr> ». **Afin d'accéder à cette URL, le certificat de l'agent issu de l'IGC du MAA doit être installé dans le navigateur.** Le composant client prend en charge l'accès Web distant sécurisé au réseau.

La première fois qu'un utilisateur distant démarre « Network Access », le client « Accès Network » télécharge un composant client. Ce composant client (au format deb ou rpm en fonction de la distribution Linux) est conçu pour s'auto-installer et se configurer automatiquement sur le poste de travail. Si le navigateur ne répond pas à certaines exigences, le nouveau dispositif d'accès VPN invite l'utilisateur à télécharger le composant client et à l'installer manuellement.

Pour pouvoir installer correctement les composants clients Network Access sur un système Linux, il faut :

- 1) utiliser Firefox pour installer le composant client. Le navigateur doit supporter l'installation de plugins
- 2) autoriser l'accès à l'adresse IP 127.0.0.1 sur le port 44444 si un pare-feu est activé sur le système Linux
- 3) que le système prenne en charge PPP. (c'est généralement le cas.). L'utilisateur doit avoir l'autorisation d'exécuter le démon PPP
- 4) que l'utilisateur distant dispose des droits équivalents à root ou soit en mesure de fournir le mot de passe du compte root pour installer correctement le client d'accès réseau.

**Lorsque le client « network Access » est fonctionnel, l'utilisateur lance le navigateur depuis lequel il a installé le client et il se rend sur l'URL « <https://portail.mercurev2.agriculture.gouv.fr> ». Il doit alors s'authentifier via son certificat issu de l'IGC du MAA. Suivant les cas, un second facteur d'authentification peut également lui être demandé.**

### ◆ Client en Ligne de commande (déconseillé) :

L'interface de ligne de commande est fournie par l'archive linux\_sslvpn.tgz : cette archive contient les binaires à décompresser et installer sur un poste Linux. Une fois décompressée, cette archive fournit le script « install.sh » d'installation des binaires F5 de l'interface ligne de commande qui permettra d'établir un tunnel SSL entre le poste client sous Linux et les boîtiers F5 afin d'accéder au VPN.

Pour installer l'interface « client ligne de commande » pour Linux, il faut :

1. Décompresser le fichier linux\_sslvpn.tgz dans votre répertoire local.
2. Extraire le fichier linux\_sslvpn.tar dans votre répertoire local.
3. Exécuter le script d'installation Install.sh sous le compte root.

Le texte suivant apparaît lorsque l'installation est terminée :

- f5fpc est installé dans /usr/local/bin
- Veuillez vérifier la commande f5fpc --help pour commencer
- Programme de désinstallation situé dans /usr/local/lib/F5Networks/uninstall\_F5.sh

Les utilisateurs Linux peuvent consulter l'URL suivante pour avoir plus d'information concernant les commandes de démarrage et d'arrêt du client VPN pour Linux :

[https://support.f5.com/kb/en-us/products/big-ip\\_apm/manuals/product/apm-client-configuration-12-0-0/5.html](https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-client-configuration-12-0-0/5.html)

## V. Installation du client VPN BIGIP pour MAC OS (VPN MercureV2 uniquement)

Pour les utilisateurs utilisant un système d'exploitation MAC OS, le client VPN BIGIP est décliné en un composant client Acces Network pour un accès via le navigateur.

Avec ce composant client Acces Network, le nouveau dispositif prend en charge les principales fonctionnalités d'accès réseau, à l'exception de drive mappings et de certaines fonctionnalités de contrôle de la sécurité des terminaux clients.

### ◆ Client Acces Network pour un accès via le navigateur (composant client Network Access) :

Pour les systèmes Linux, Mac OS X et Windows, le composant client Network Access est disponible en téléchargement automatique à partir de l'url « <https://portail.mercurev2.agriculture.gouv.fr> ». **Afin d'accéder à cette url, le certificat de l'agent issu de l'IGC du MAA doit être installé dans le navigateur.** Le composant client prend en charge l'accès Web distant sécurisé au réseau.

La première fois qu'un utilisateur distant démarre « Network Access », le client « Acces Network » télécharge un composant client. Ce composant client (au format pkg) est conçu pour s'auto-installer et se configurer automatiquement sur le poste de travail. Si le navigateur ne répond pas à certaines exigences, le nouveau dispositif d'accès VPN invite l'utilisateur à télécharger le composant client et à l'installer manuellement.

**Ce client pkg peut également être demandé auprès du centre de services ou du BIP pour les services dépendant de l'Administration Centrale du MAA.**

Pour pouvoir installer correctement les composants clients Network Access sur un système MAC OS, il faut :

- 1) utiliser Firefox pour installer le composant client. Le navigateur doit supporter l'installation de plugins
- 2) autoriser l'accès à l'adresse IP 127.0.0.1 sur le port 44444 si un pare-feu est activé sur le système
- 3) que l'utilisateur distant dispose des droits lui permettant d'installer correctement le client d'accès réseau (c'est généralement le cas).

**Lorsque le client « network Access » est fonctionnel, l'utilisateur lance le navigateur depuis lequel il a installé le client et il se rend sur l'url « <https://portail.mercurev2.agriculture.gouv.fr> ». Il doit alors s'authentifier via son certificat issu de l'IGC du MAA. Suivant les cas, un second facteur d'authentification peut également lui être demandé.**

## VI. VPN sans client : F5 Helper Apps pour inspection endpoint et VPN (VPN MercureV2 uniquement)

Le support des plugins NPAPI a été arrêté par les éditeurs de navigateurs. Les fonctionnalités qui étaient précédemment installées avec des plugins NPAPI sont maintenant gérées par ce qu'on appelle des "helper applications", qui sont installés sur la machine de l'utilisateur, et gérés par des "protocol handlers".

Techniquement, il faut installer une application pour l'accès VPN (Network Access) et une application pour le contrôle Endpoint. Ces clients peuvent être téléchargés depuis le BIG-IP APM et installés par GPO ou par une solution de télédéploiement.

Ces applications requièrent les privilèges suivants pour être installées :

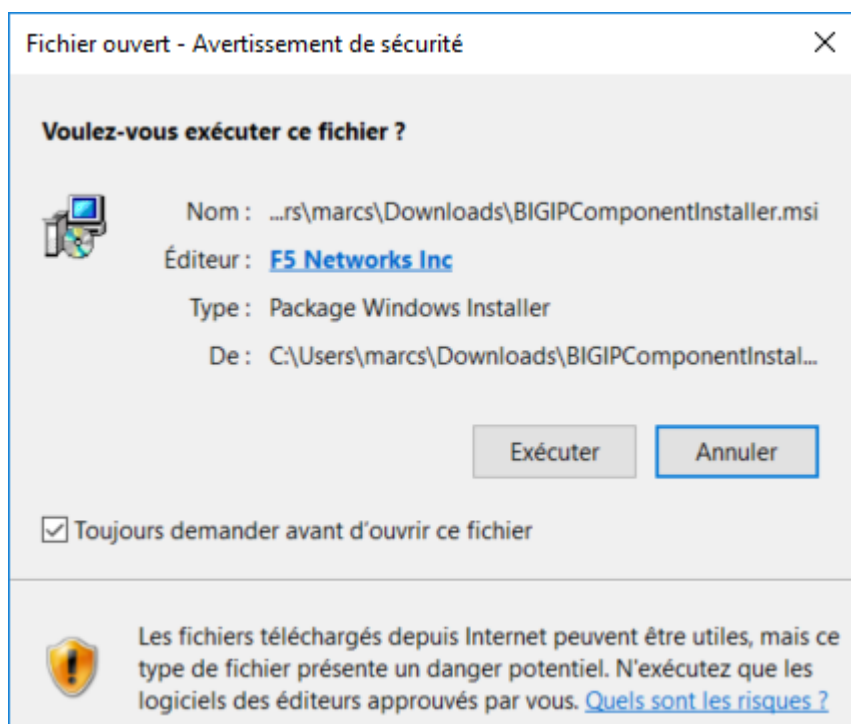
Application	Windows	MacOS	Linux
EPS Helper App	Utilisateur standard	Standard	Root
VPN Helper App	Admin	Admin	root

Cette solution fonctionne pour les navigateurs Google Chrome, Firefox et Microsoft Edge en versions 32-bit et 64-bit. Internet Explorer et Safari ne supportent pas ce mode de connexion car ils utilisent encore les plugins NPAPI.

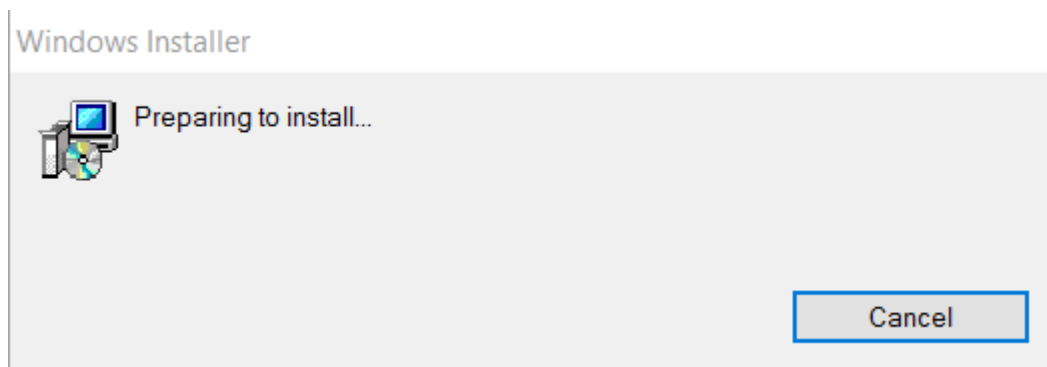
## 1. INSTALLATION INTERACTIVE DES COMPOSANTS F5 HELPER APPS SUR WINDOWS

La première étape consiste à télécharger les composants F5 Helper pour Windows. Ces composants sont téléchargeables depuis l'interface d'administration web F5.

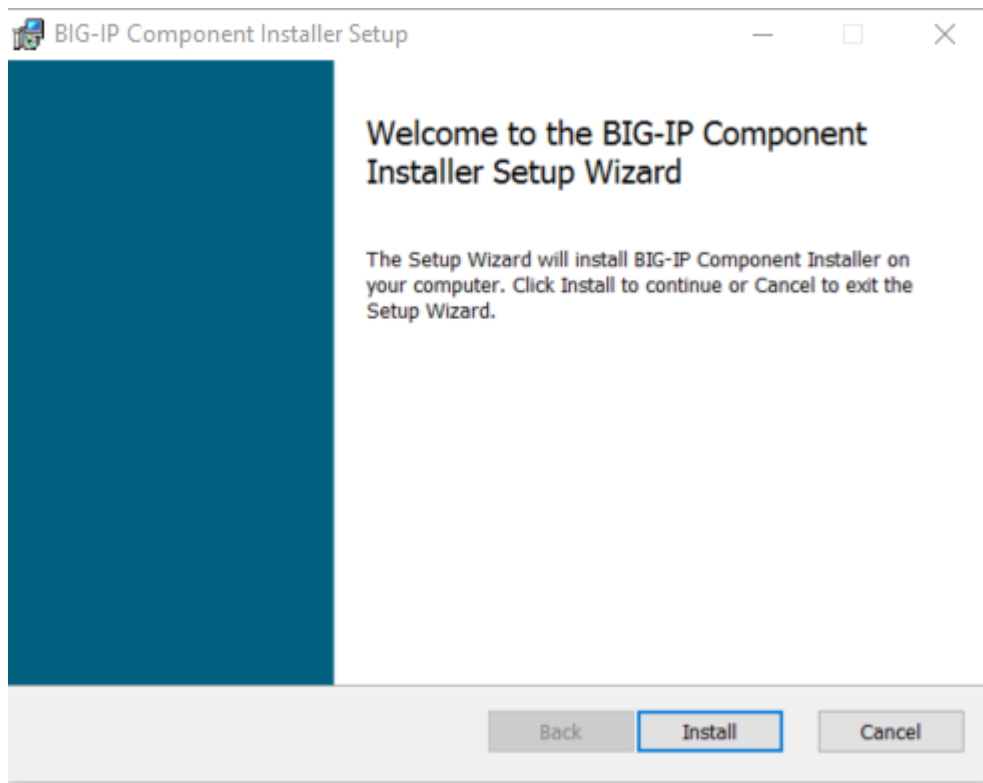
Ensuite, double-cliquer sur le binaire **BIGIPComponentInstaller.msi** pour lancer l'installation. Cet utilitaire nécessite une élévation de privilèges administrateur pour être installé.



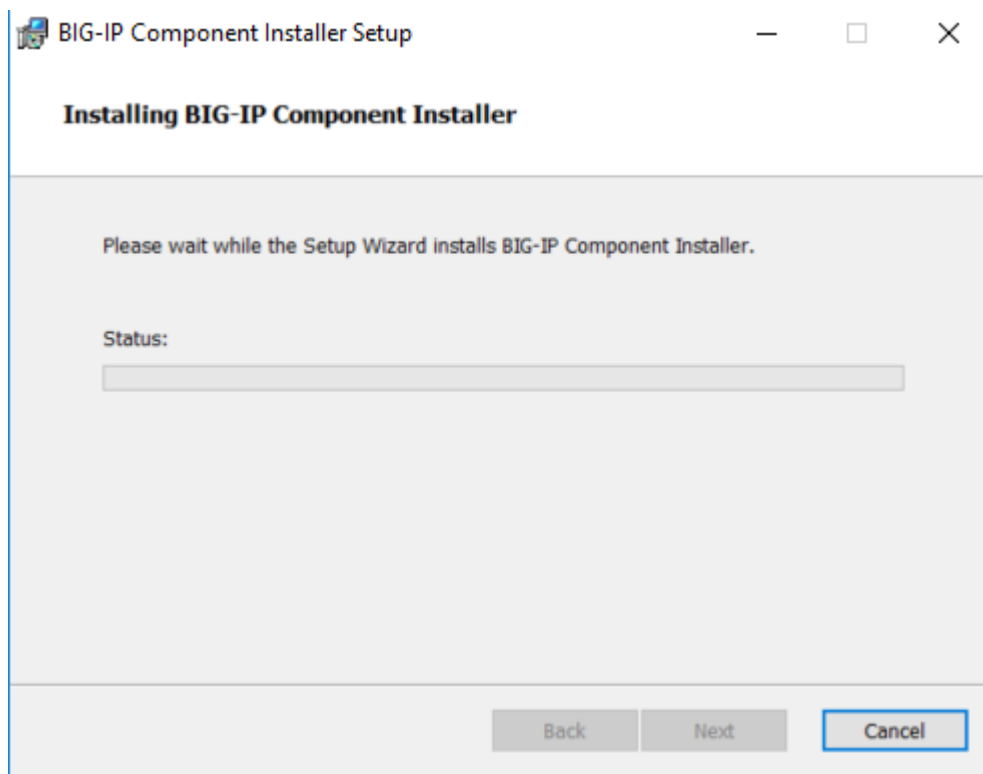
Cliquer sur "Exécuter". L'installateur se lance.



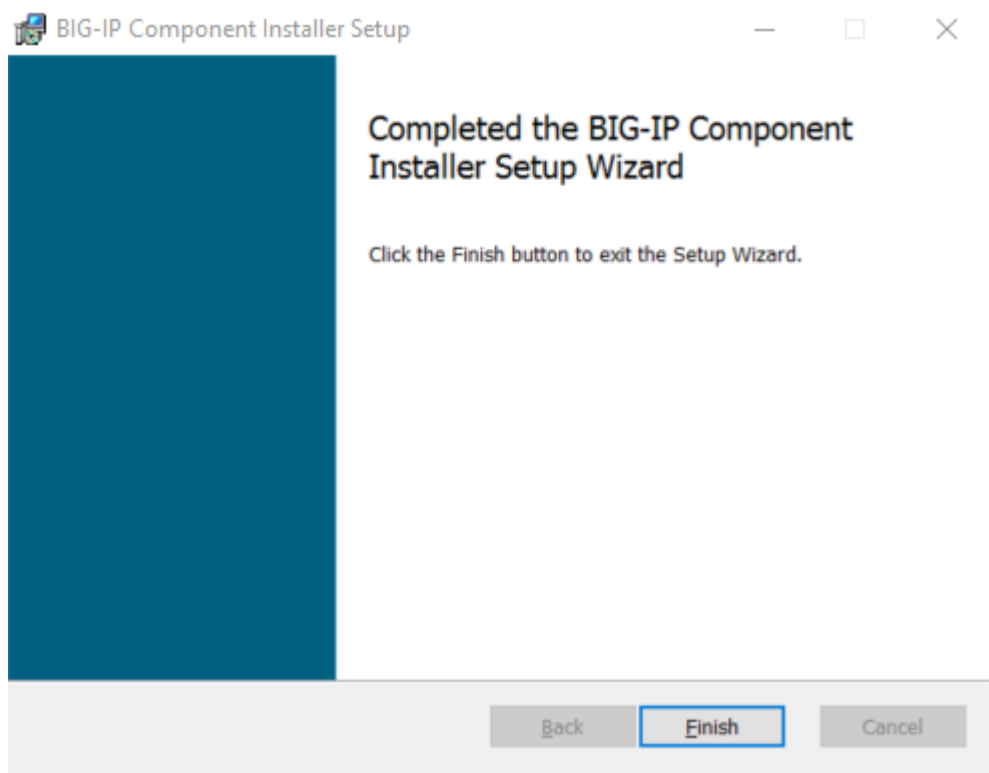
L'interface interactive d'installation propose d'installer les composants, cliquer sur "Install".



L'installation se lance. Patienter jusqu'à la fin de l'installation.



Une fois l'installation terminée, cliquer sur "Finish".



## 2. INSTALLATION SILENCIEUSE DES COMPOSANTS F5 HELPER APPS SUR WINDOWS

L'installation industrialisée est basée sur l'utilitaire « misexec.exe » de Microsoft. Pour automatiser l'installation en administration centrale, un package a été mis à disposition sur le serveur NAS de l'AC : « Bur-file-AC01-1.ad.national.agri ».



Pour les structures n'accédant pas à ce partage il est possible de se rapprocher du Bureau de l'Informatique de Proximité (BIP) du MAA afin d'obtenir une copie de ce package.

A partir d'un poste de travail, cliquer sur démarrer puis exécuter la commande :  
`msiexec /i BIGIPComponentInstaller.msi /qn /quiet`

L'installation des composants F5 Helper Apps démarre et ne demande aucune action à l'utilisateur. Pour rappel, elle nécessite une élévation de privilèges d'administrateur.

## 3. VÉRIFICATION DE L'INSTALLATION DES SERVICES

Premièrement, vérifier dans le panneau de configuration que les composants ont bien été installés (Windows 7).

	BIG-IP Component Installer F5 Networks	7,99 Mo 25/05/2018
	BIG-IP Edge Client Components (All Users) F5 Networks, Inc.	25/05/2018

Ensuite, vérifier l'installation des services Windows en ouvrant une invite de commande (cmd) et en lançant la commande suivante :

```
c:\>net start | findstr /i F5
F5 Networks Component Installer
c:\>
```

Par rapport à l'installation du client BIG-IP Edge Client, seul un service est installé. En effet, c'est celui qui permettra d'installer les autres composants nécessaires lors de l'établissement du tunnel VPN via un navigateur.

On retrouve également le même service installé visible depuis l'utilitaire Microsoft « services.msc » :



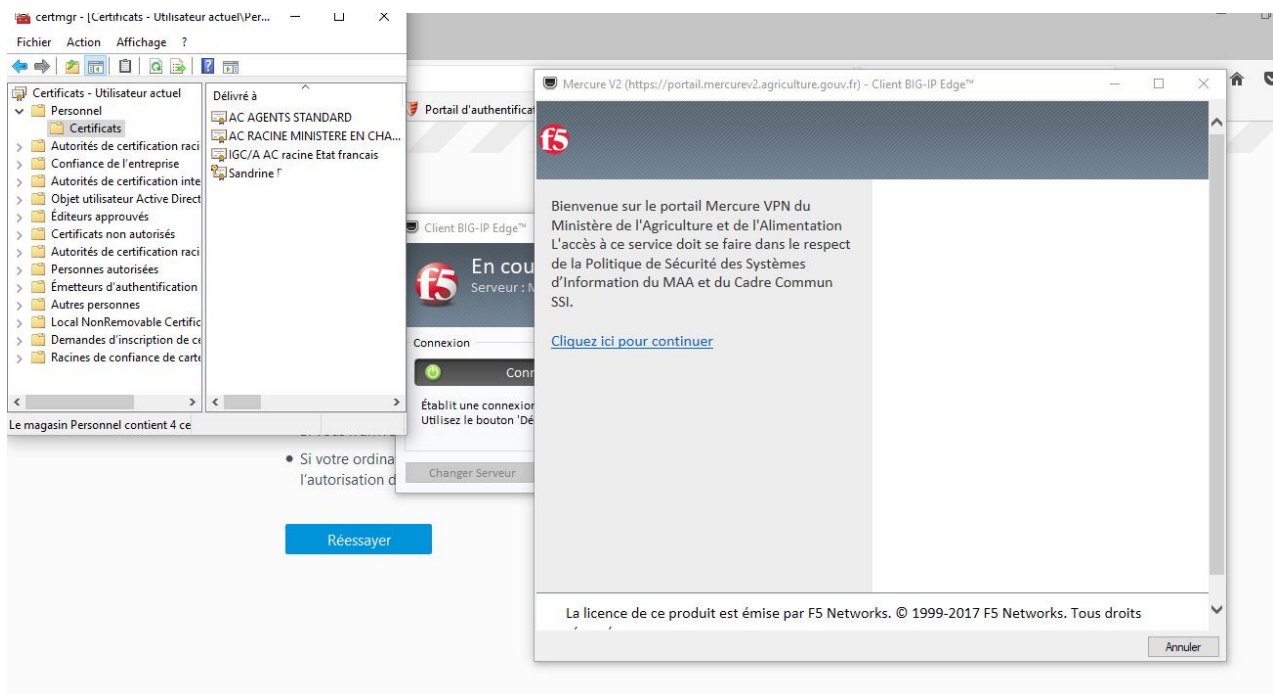
Vérifier que le service est bien en démarrage automatique.

## VII. Problèmes connus

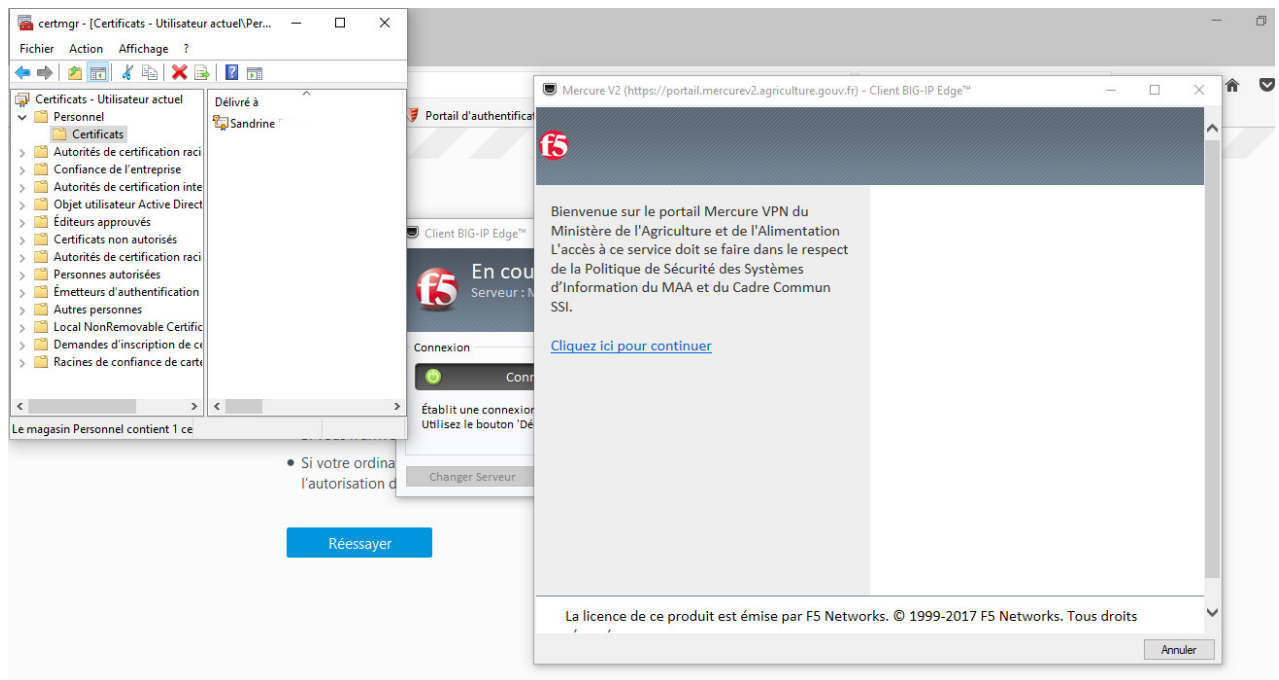
- lors de la connexion au VPN , si le navigateur ou le client Edge rebouclent en permanence sur la page d'accueil du VPN, il s'agit la plupart du temps d'un problème d'accès au certificat fourni à l'utilisateur via l'IGC du MAA. Dans ce cas supprimer le certificat du magasin du navigateur (ou du magasin Windows dans le cas de l'utilisation du client EdgeBigIP sur cette plateforme) et le réimporter à l'issue. Certaines stratégies de durcissement de la configuration du poste de travail peuvent également empêcher les navigateurs d'accéder à ce certificat.

- lors de la connexion au VPN , si le navigateur ou le client Edge rebouclent en permanence sur la page d'accueil du VPN **et la solution proposée ci-dessus n'a pas fonctionné :**

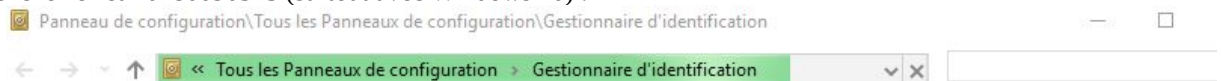
**si on constate la présence de certificats d'AC dans le conteneur « Personnel - Certificats » du magasin de certificats Windows :**



**tenter de supprimer ces certificats et re-tester la connexion à l'issue :**



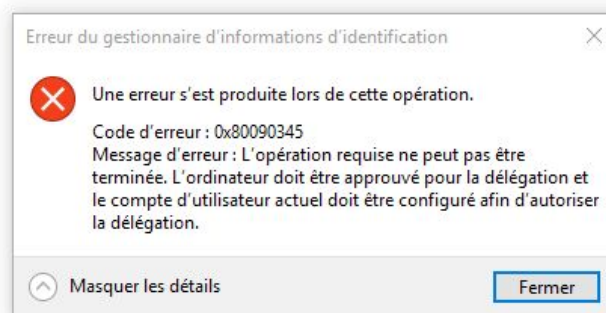
- lors de la connexion au VPN, si le navigateur ou le client Edge rebouclent en permanence sur la page d'accueil du VPN **et que** l'ouverture du gestionnaire d'identification (Panneau de configuration puis Gestionnaire d'identification) déclenche l'erreur 0x80090345 (surtout avec Windows 10) :



Page d'accueil du panneau de configuration

### Gérer vos informations d'identification

Affichez et supprimez vos informations d'ouverture de session enregistrées pour les sites Web, les applications connectées et les réseaux.



dans ce cas, ouvrir la base de registre à l'emplacement suivant :

"HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb" puis dans df9d8cd0-1501-11d1-8c7a-00c04fc297eb, créer la valeur DWORD 32bit nommée ProtectionPolicy. A l'issue double cliquer sur ProtectionPolicy et mettre la valeur 1

Effectuer la même opération à l'emplacement suivant :

"HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb"

A l'issue supprimer le certificat utilisateur du magasin Windows et le réimporter.

- impossibilité d'installer le client EdgeBigIP sur certains postes Windows : dans ce cas l'opération suivante peut être tentée :

sur certains postes de travail le souci provient de la clé de registre suivante qu'il convient donc de supprimer avant toute installation du client "BIG-IP Edge Client" :

"\\HKEY\_LOCAL\_MACHINE\SOFTWARE\Classes\Installer\Products\BC9384D64B820704C87A16C29AC23A0D\ProductName" = "BIG-IP Edge Client (7.1.7.1)"

Fin de document