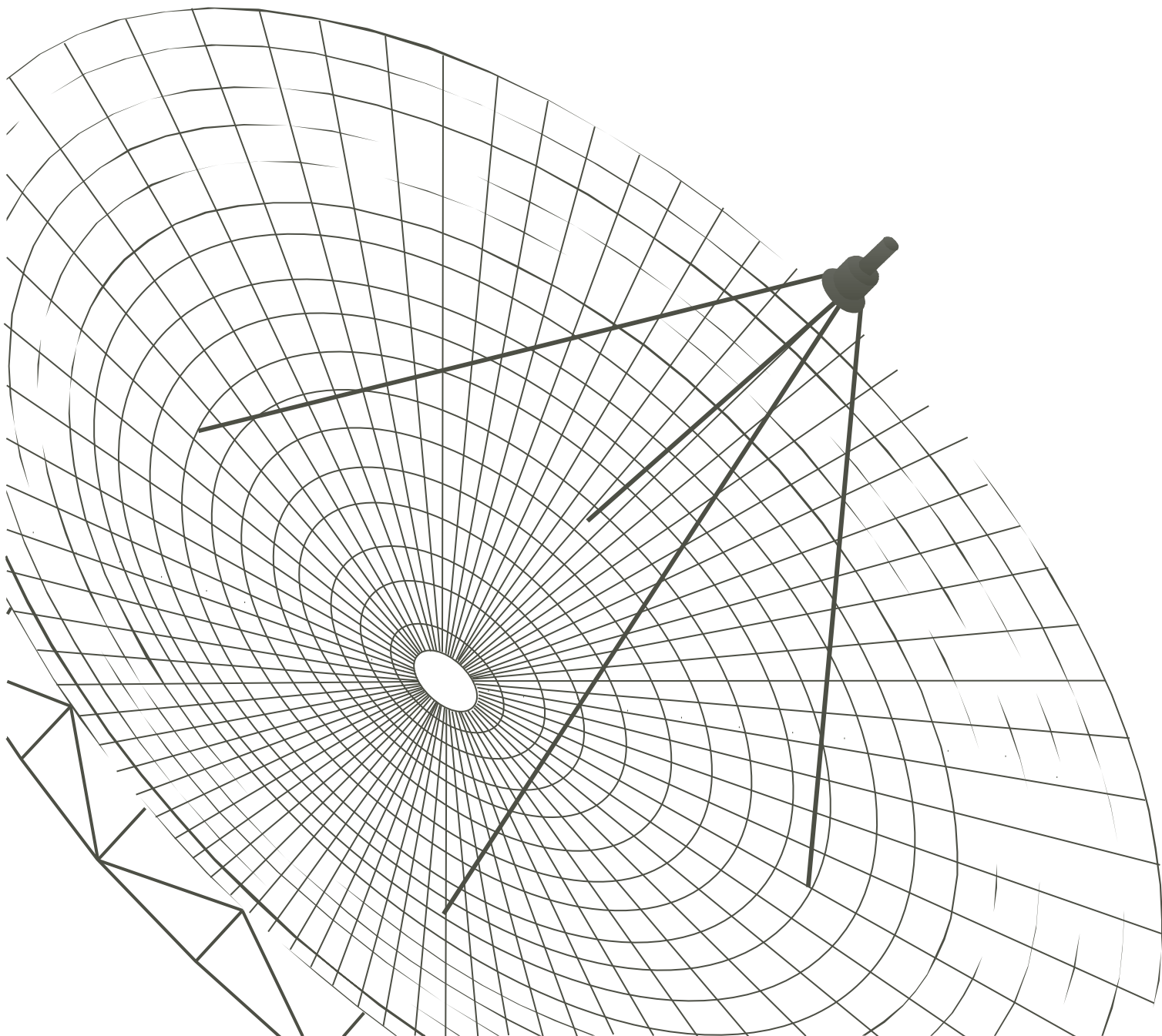


Les réseaux des EPLEFPA

Guide « Clients Mercure Ubuntu & Mac »



Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	1/14

Table des matières

Contexte de Mercure.....	2
Installation du client OpenVPN.....	3
Mac OsX.....	3
Ubuntu.....	4
Téléchargement de la configuration mercure.....	4
Générer le certificat utilisateur.....	5
Adaptation du script pour Mac OsX.....	6
Génération de la clef.....	6
Adaptation du fichier de configuration MAAPRAT.conf.....	7
Mac OsX.....	7
Ubuntu.....	7
Mise en place de la configuration.....	8
TunnelBlick sous Mac OsX.....	8
Ubuntu.....	9
Etablir la connexion VPN.....	9
Mac OsX.....	9
Ubuntu.....	11
S'authentifier grâce à son certificat.....	12
Post Scriptum.....	14
Dysfonctionnement DNS.....	14
Assistance.....	14

Contexte de Mercure

Le Ministère de l'Alimentation, de l'Agriculture, de la Pêche, de la Ruralité et de l'Aménagement du Territoire (MAAPRAT) a mis en place le service Mercure VPN (en remplacement de prisme3 et Cisco VPN) permettant l'accès aux ressources du réseau MAAPRAT depuis Internet.

L'accès aux ressources par Mercure VPN, nécessite d'installer le client Mercure VPN et de posséder un certificat numérique délivré par l'IGC du MAAPRAT installé sur le poste de utilisateur. Le client Mercure VPN permet de réaliser un Tunnel VPN (Virtual Private Network, ou réseau privé virtuel et chiffré) entre le client et le MAAPRAT. L'utilisateur est authentifié par son certificat numérique sur un portail d'accueil. Ce certificat lui permet d'accéder aux ressources et applications du MAAPRAT pour lesquelles une autorisation lui a été délivrée.

Mercure est opérationnel depuis le 01/07/2011.

Toute la documentation, ainsi que les logiciels d'installation de Mercure se trouvent sur le site du pôle de sécurité sur le réseau intranet du MAAPRAT : <http://securite.rmap.auzeville.agri/> sous les rubriques « Extranet » puis « MercureVPN ».

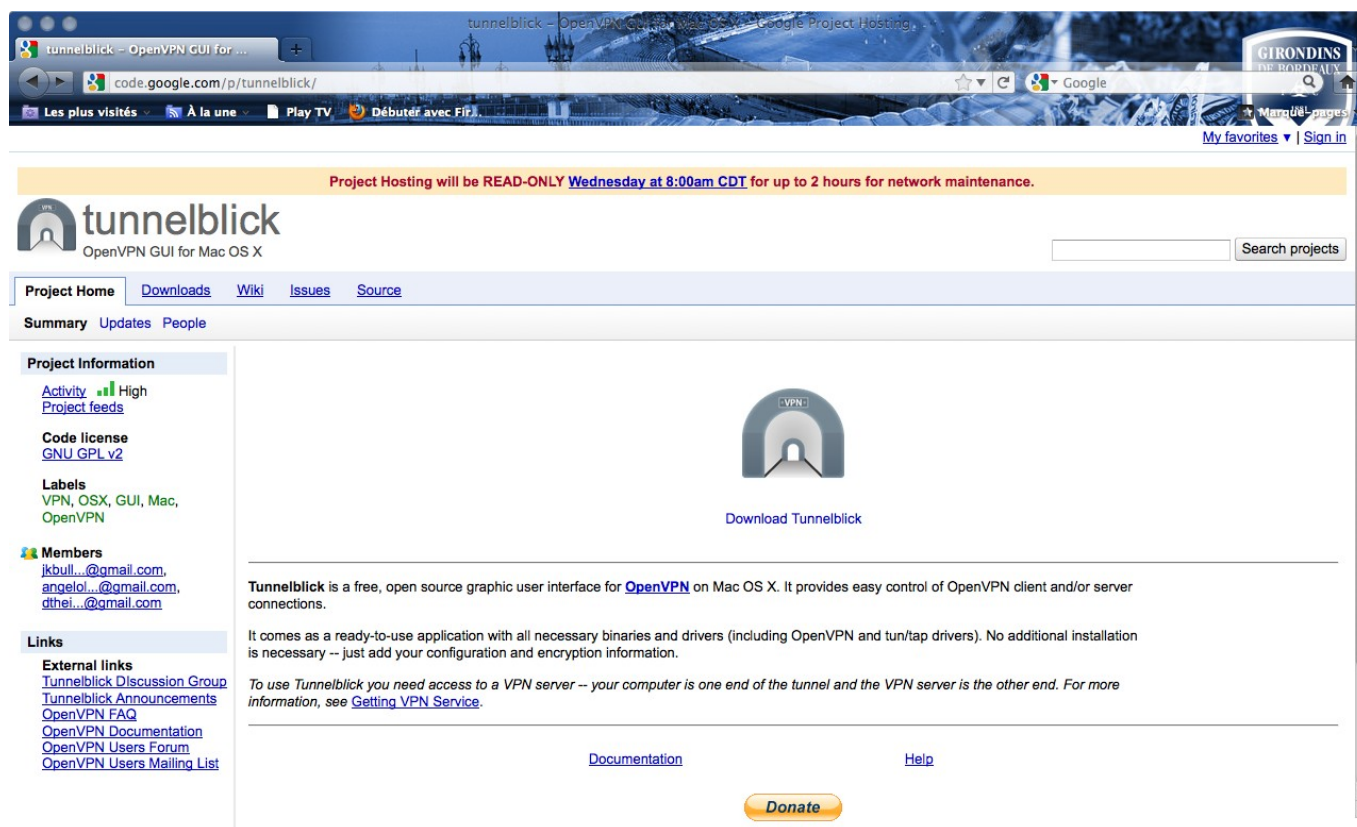
Toutefois, les services en charge de ce projet ne produisent et ne maintiennent que les versions pour les systèmes d'exploitations de la famille « Microsoft Windows ». Cependant l'équipement des établissements et des enseignants comporte un nombre important d'autres systèmes. Ce guide concerne les deux principaux : Mac OsX Léopard et supérieur ainsi que Ubuntu 11.04 et suivant.

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	2/14

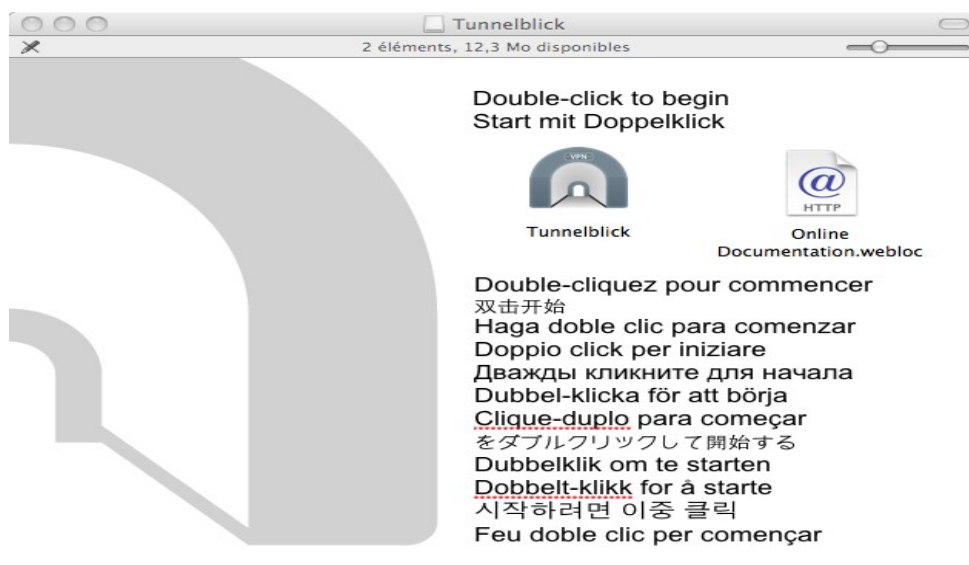
Installation du client OpenVPN

Mac OsX

Téléchargez le client TunnelBlick sur la forge de Google :



Procédez à l'installation du fichier en double cliquant sur le fichier .dmg :



Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	3/14

Ubuntu

Téléchargez et installez le client OpenVpn depuis la Logithèque Ubuntu.



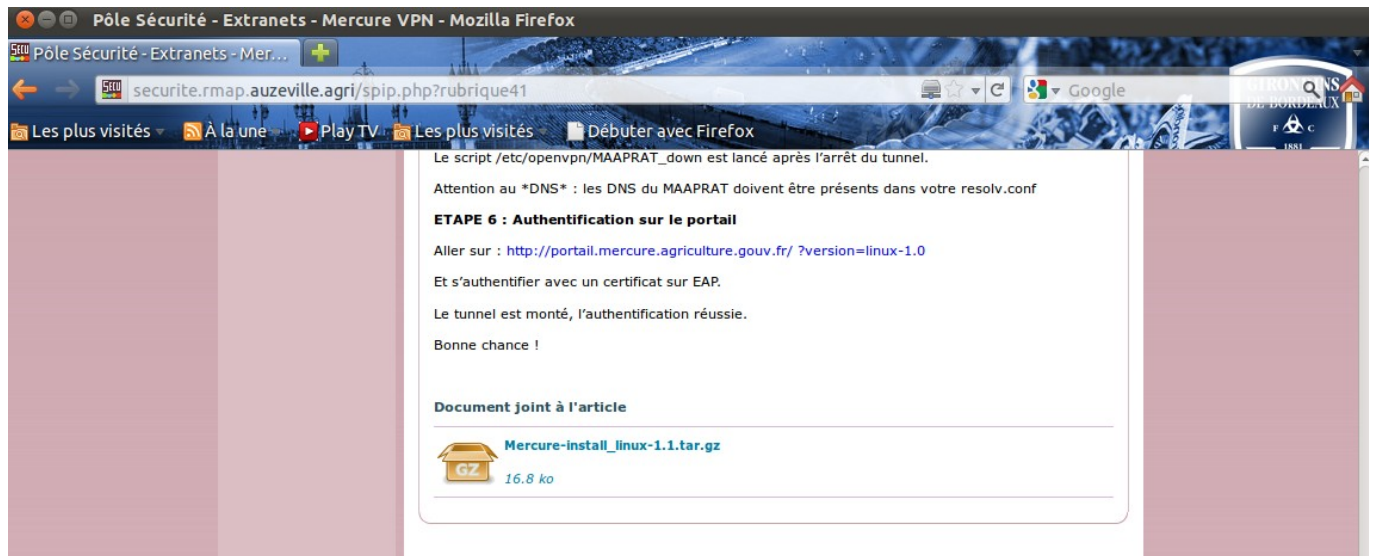
Téléchargement de la configuration mercure

Depuis un poste connecté au réseau du MAAPRAT, accédez au portail de sécurité du Ministère

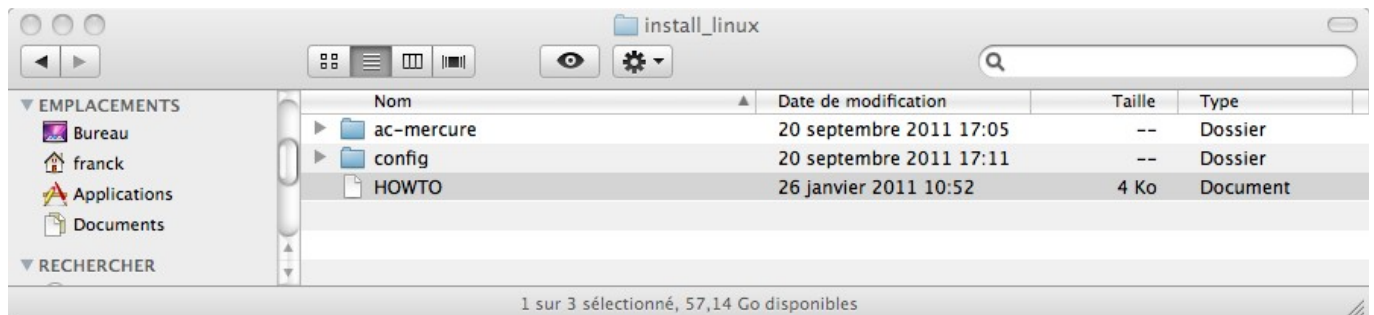


Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	4/14

Téléchargez l'archive compressée pour Linux en bas de la rubrique « Extranet/Mercure »

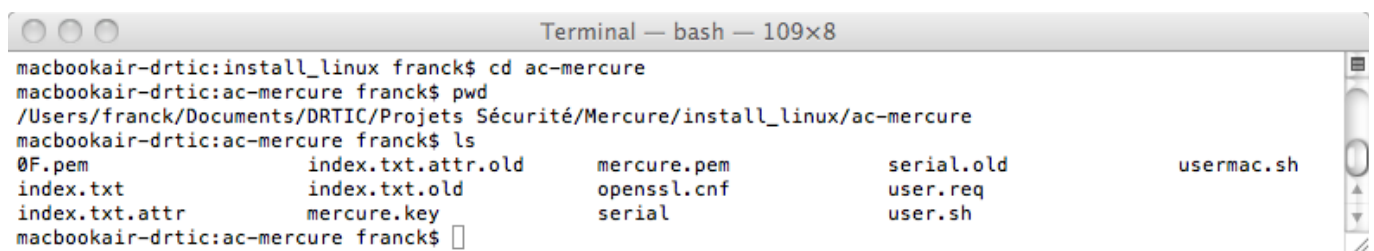


Enregistrez et décompressez ce fichier dans un répertoire personnel. Vous obtenez les répertoires :



Générer le certificat utilisateur

Pour les deux OS, ouvrez une console et placez vous dans votre dossier install_linux/ac-mercure.



Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	5/14

Adaptation du script pour Mac OsX

Le script user.sh fourni nécessite une modification de la commande date pour s'exécuter sous Mac OsX.

```

#!/bin/bash

if [ -z $1 ]; then
    echo "ERREUR"
    echo " le parametre mail est manquant"
    echo " USAGE : sudo ./user.sh jean.dupont@ministere.gouv.fr"
else
    echo "GÉNÉRATION du certificat de connexion..."

    openssl genrsa -out ../config/user.key 2048

    openssl req -subj "/C=FR/O=MAAPRAT/OU=Mercurie VPN/CN=$1" -new -key ../config/user.key -out user.req

    startdate=`date -v -1d +%y%m%d000000Z`

    openssl ca -batch -startdate $startdate -in user.req -out ../config/user.pem -config openssl.cnf

fi
    
```

Génération de la clef

Vérifiez que vous êtes dans le bon répertoire « install_linux/ac-mercure ».

Exécutez la commande suivante en spécifiant votre propre adresse mail agriculture.gouv.fr ou educagri.fr

sudo ./user.sh jean.dupont@ministere.gouv.fr

Votre certificat user.pem et votre clef user.key sont alors générés et copiés dans le répertoire ../config

Nom	Taille	Type	Date de modification
install_linux	3 éléments	dossier	mer. 26 janv. 2011 10:52:38 CET
config	8 éléments	dossier	mer. 28 sept. 2011 17:59:10 CEST
MAAPRAT.conf	565 octets	document texte brut	mer. 28 sept. 2011 17:59:10 CEST
user.pem	4,4 Kio	certificat X.509 codé DER/PEM/Netscape	jeu. 22 sept. 2011 09:30:14 CEST
user.key	1,6 Kio	document texte brut	jeu. 22 sept. 2011 09:30:14 CEST
update-resolv-conf	1,3 Kio	script shell	mer. 26 janv. 2011 10:27:04 CET
MAAPRAT_up.sh	353 octets	script shell	mer. 26 janv. 2011 10:27:04 CET
MAAPRAT_down.sh	7 octets	script shell	mer. 26 janv. 2011 10:27:04 CET
hmac.key	636 octets	document texte brut	mer. 26 janv. 2011 10:27:04 CET
ca.crt	12,6 Kio	certificat X.509 codé DER/PEM/Netscape	mer. 26 janv. 2011 10:27:04 CET
ac-mercure	12 éléments	dossier	jeu. 22 sept. 2011 09:30:14 CEST
HOWTO	2,6 Kio	différences entre fichiers	mer. 26 janv. 2011 10:52:38 CET

« install_linux » sélectionné (contenant 3 éléments), Espace libre : 9,2 Gio

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	6/14

Adaptation du fichier de configuration MAAPRAT.conf

Mac OsX

```

client

resolv-retry infinite
<connection>
remote vpn.mercure.agriculture.gouv.fr 443 udp
</connection>

<connection>
remote vpn.mercure.agriculture.gouv.fr 443 tcp
</connection>

dev tun
ca ca.crt
cert user.pem
key user.key

tls-auth hmac.key 1 # This file is secret

ns-cert-type server
comp-lzo
verb 2
    
```

Ubuntu

```

MAAPRAT.conf [Lecture seule] (/etc/openvpn) - gedit
Ouvrir Enregistrer Annuler
MAAPRAT.conf x
client

resolv-retry infinite
<connection>
remote vpn.mercure.agriculture.gouv.fr 443 udp
</connection>

<connection>
remote vpn.mercure.agriculture.gouv.fr 443 tcp
</connection>

dev tun
ca ca.crt
cert user.pem
key user.key

tls-auth hmac.key 1 # This file is secret

ns-cert-type server
comp-lzo
verb 3

script-security 4

up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf

#up '/bin/sh -x /etc/openvpn/MAAPRAT_up.sh'
#down '/bin/sh -x /etc/openvpn/MAAPRAT_down.sh'

log-append /tmp/openvpn-MAAPRAT.log
    
```

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	7/14

Mise en place de la configuration

TunnelBlick sous Mac OsX

Exécutez l'application tunnelBlick précédemment installée puis ajoutez une configuration en choisissant « j'ai des fichiers de configuration » :

Ajouter une configuration

Généralement, on installe de configurations en utilisant de fichiers que vous fournis votre administrateur réseau ou fournisseur d'accès VPN.

Les fichiers de configuration ont les extensions « .tblk », « .ovpn », ou « .conf ».

(Il peut être d'autres fichiers associés à la configuration, qui ont d'autres extensions ; ne les faites pas d'attention à ce temp.)

Avez-vous quelques fichiers de configuration ?

Annuler Je n'ai aucune fichier de configuration J'ai de fichiers de configuration

Choisissez ensuite « Configuration(s) OpenVPN » :

Quel type de configuration avez-vous ?

Il existe deux types de fichier de configuration :

- Configuration de VPN Tunnelblick VPN (ayant l'extensino « .tblk »)
- Configuration de VPN OpenVPN (ayant l'extension « .ovpn » ou « .conf »)

Quel type de fichier de configuration avez-vous ?

Revenir Configuration(s) OpenVPN Configuration(s) VPN Tunnelblick

Choisissez ensuite « Ouvrir dossier de configurations privées » :

Quel type de configuration voudriez-vous créer ?

- Avec un fichier de configuration, vous pouvez créer une configuration VPN Tunnelblick.
- Avec plusieurs fichiers de configuration, vous pouvez les placez (à côté de fichiers de certificat et de clé, si vous en avez) dans le dossier de configurations privées de Tunnelblick. Ceci est la mode traditionnelle selon laquelle les configurations OpenVPN ont été utilisées.

Remarque : Les configuration VPN Tunnelblick sont à préférer, parce qu'elles peuvent être partagées, peuvent être lancées quand l'ordinateur démarre, et sont sécurisées automatiquement.

Revenir Ouvrir dossier de configurations privées Créer configuration VPN Tunnelblick

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	8/14

Une fenêtre s'ouvre alors sur le dossier qui contient les configurations de Tunnelblick.
Vous devez alors y déposer les fichiers du répertoire install_linux/config suivants :

```
MAAPRAT.conf    # Fichier de configuration du Tunnel
ca.crt          # Certificat de l'AC Mercure
hmac.key        # Fichier secret pour établir la connection TLS
user.key        # Clef privée de l'utilisateur
user.pem        # Certificat de l'utilisateur
```

TunnelBlick est alors prêt à l'emploi.

Ubuntu

Copier l'ensemble des fichiers de configuration du répertoire install_linux/config dans le répertoire de configuration OpenVPN :

```
sudo cp ./config/* /etc/openvpn/
```

Dans le répertoire /etc/openvpn, il faut trouver les fichiers suivants :

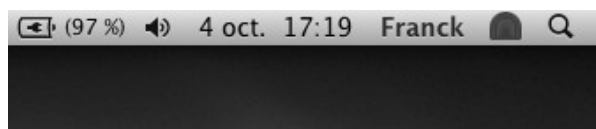
```
MAAPRAT.conf    # Fichier de configuration du Tunnel
ca.crt          # Certificat de l'AC Mercure
hmac.key        # Fichier secret pour établir la connection TLS
user.key        # Clef privée de l'utilisateur
user.pem        # Certificat de l'utilisateur
update-resolv-conf # Script de configuration du DNS
```

Le Vpn est alors prêt à l'emploi.

Etablir la connexion VPN

Mac OsX

TunnelBlick est représenté par une icône grisée en forme de tunnel dans la barre supérieure



Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	9/14

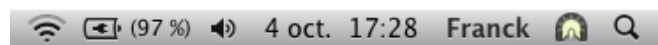
Cliquez sur ce tunnel et choisissez « connecter MAAPRAT »



l'icône clignote et des fenêtres d'état se succèdent jusqu'à :



l'icône se fige sur un tunnel ouvert et vous êtes connecté :



Vous devez alors vous authentifier sur le **portail mercure depuis Firefox**.

La déconnexion s'effectue en cliquant sur l'icône du tunnel ouvert et choix « deconnecter MAAPRAT »

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	10/14

Ubuntu

Il est possible d'établir le tunnel VPN à l'aide de commandes depuis une console :

```

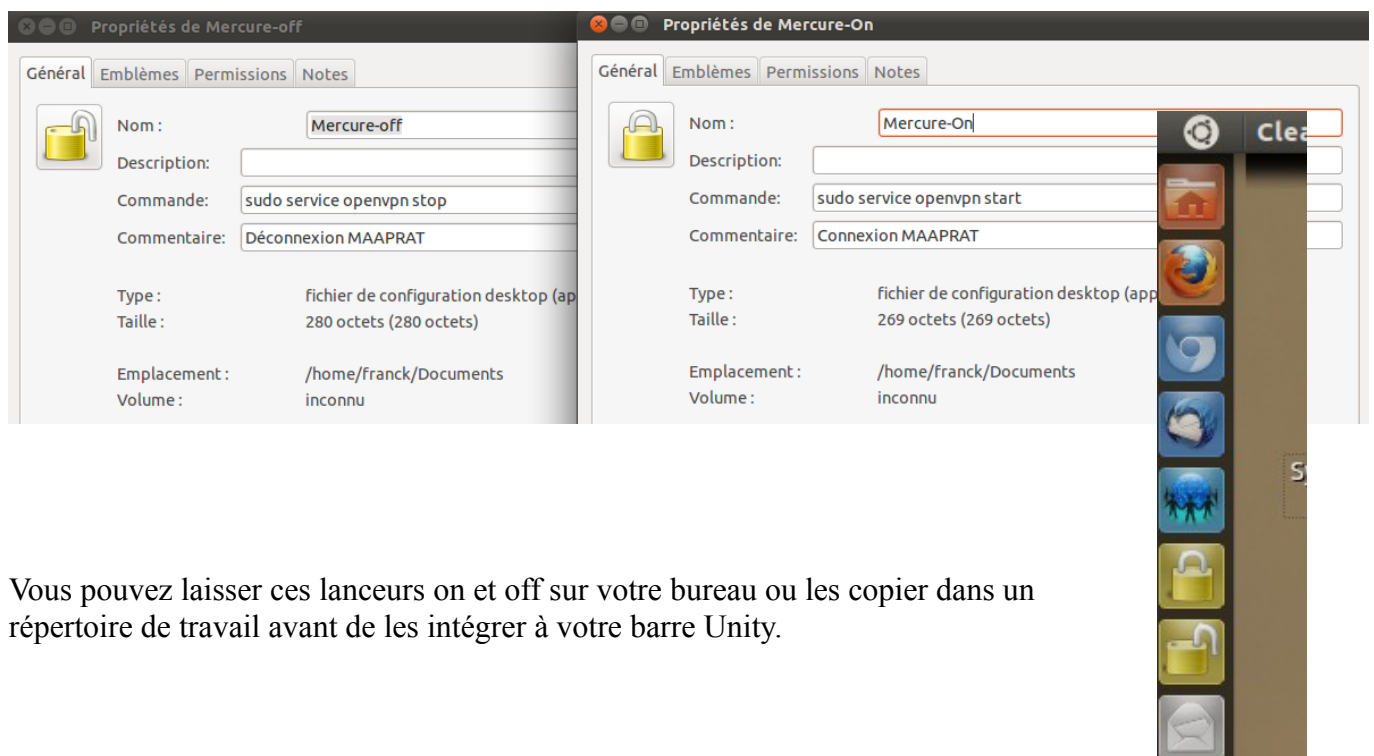
franck@ubuntu: ~
franck@ubuntu:~$ sudo service openvpn start
[sudo] password for franck:
* Starting virtual private network daemon(s)...
*   Autostarting VPN 'MAAPRAT'
franck@ubuntu:~$
    
```

et de le stopper par :

```

franck@ubuntu:~$
franck@ubuntu:~$ sudo service openvpn stop
* Stopping virtual private network daemon(s)...
*   Stopping VPN 'MAAPRAT'
franck@ubuntu:~$
    
```

Vous pouvez également créer deux lanceurs de type « Application dans un terminal » (sur le bureau click droit/nouveau lanceur) :



Vous pouvez laisser ces lanceurs on et off sur votre bureau ou les copier dans un répertoire de travail avant de les intégrer à votre barre Unity.

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	11/14

S'authentifier grâce à son certificat

Pour accéder au réseau du MAAPRAT le tunnel VPN ne suffit pas, il faut s'authentifier sur le portail mercure avec son certificat Agricoll depuis le navigateur Firefox qui le contient :

MAAPRAT - Portail Mercure VPN

MINISTÈRE DE L'ALIMENTATION, DE L'AGRICULTURE, DE LA PÊCHE, DE LA RURALITÉ ET DE L'AMÉNAGEMENT DU TERRITOIRE

Portail Mercure VPN

Bienvenue sur le portail Mercure VPN

L'accès à ce service doit se faire dans le respect de la Politique de Sécurité des Systèmes d'Information du MAAPRAT et du Cadre Commun SSI.

Il est par ailleurs rappelé les articles de loi suivants :

Art. 323-1 : Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Art. 323-2 : Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Art. 323-3 : Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

[S'authentifier avec mon certificat](#)

MAAPRAT - Mercure VPN SG/SM/SDSI v0.1-5

Cliquez sur « s'authentifier avec mon certificat » puis sélectionner le bon certificat :

Ce site vous demande de vous identifier avec un certificat de sécurité :
 identification.agriculture.gouv.fr:443
 Organisation : « service-public gouv agriculture »
 Émis sous : « service-public gouv agriculture »

Choisir un certificat à présenter comme identification :
 Franck DANIEL's service-public gouv agriculture ID [35:DA]

Détails du certificat sélectionné :

Émis pour :
 E=franck.daniel@agriculture.gouv.fr,UID=franck.daniel,serialNumber=80677,CN=Franck DANIEL,OU=0002 110070018,O=service-public gouv agriculture,C=FR
 Numéro de série: 35:DA
 Valide de 05/02/11 17:19:00 pour 05/03/12 17:16:12
 Sujets: Signature
 Usage de la clé de certificat: Signature,Non-répudiation

Se souvenir de cette décision

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	12/14

Vous arrivez alors sur le portail d'authentification du MAAPRAT.
Cliquez sur « Présenter mon certificat » :

Victoire :

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	13/14

Post Scriptum

Dysfonctionnement DNS

Des dysfonctionnements dans la résolution des noms (DNS) peuvent se produire si votre configuration de base comporte déjà plusieurs DNS.

La solution consiste à ne laisser qu'un DNS par défaut sur un poste utilisant Mercure.

Assistance

Ce guide est réalisé à l'aide des configurations que j'ai mises en œuvre sur mes deux postes de travail sous ubuntu 11.04 et Mac OsX Snow Léopard. Elles sont opérationnelles.

Ce document est réalisé pour vous aider en vous évitant de trop chercher.

Vous comprendrez aisément que je ne suis pas en mesure d'assurer l'assistance technique.

BON COURAGE

Date	Référence	Version	Etat du document	Nom document	Page
04/10/11	F. Daniel	1.0	Document final	Guide mercure Mac Ubuntu.odt	14/14