

FL MGuard

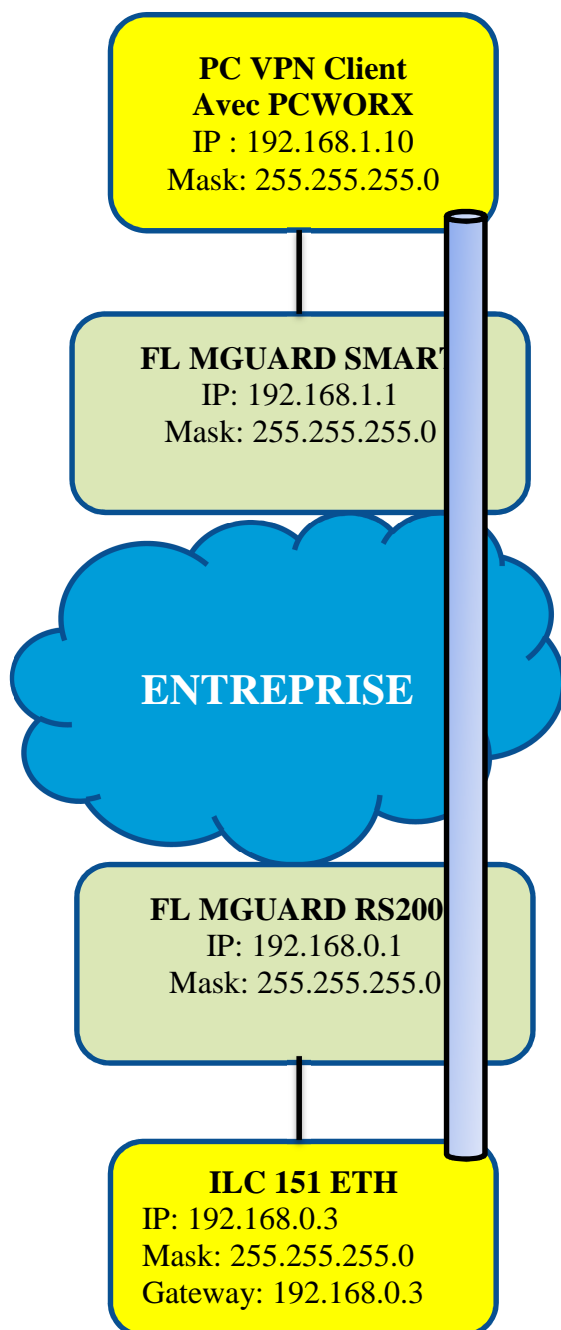


Liaison VPN IPsec PSK

But du manuel :	3
Annexes :	4
Annexe 1 : Versions Logicielles et matérielles utilisées pour ce manuel	4
Annexe 2 : Révision document	4
Architecture :	5
Configuration du MGUARD SMART2 VPN :	6
Configuration du MGUARD RS2000 VPN :	13
Mise en service de la communication :	15
MGUARD Secure Cloud :	16

But du manuel :

Ce guide vous permettra de mettre en œuvre une liaison VPN IPsec avec « Preshared Secret Key » entre un PC et un automate programmable de réseaux différents grâce à l'utilisation de deux routeurs avec pare feu intelligent de type FL MGuard.



Annexes :

Annexe 1 : Versions Logicielles et matérielles utilisées pour ce manuel

Matériels :

Fabricant	référence	Type	Version Hardware	Version Firmware
INNOMINATE	2700639	FL MGuard SMART2 VPN	00003000	7.4.1
INNOMINATE	2700642	FL MGuard RS2000 VPN	00003200	7.4.0
PHOENIX CONTACT	2700974	ILC151ETH	HW00	FW400

Logiciels :

Fabricant	lien	Type	Version
PHOENIX CONTACT		PCWORX	
SHREW	https://www.shrew.net/download/vpn	ShrewSoft VPN Client	V2.2.2
INNOMINATE	https://fr.cloud.mguard.com/	Secure Cloud	

Annexe 2 : Révision document

Version en cours : 1

Version	Date	Opérateur	Commentaires
1	27/05/2015	JF.FOUARD	Création

Architecture :

PC Client réseau local LAN1 :

Adresse IP : 192.168.1.10

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 192.168.1.1 (adresse locale du MGUARD1)

MGUARD1 réseau local LAN1 :

Adresse IP : 192.168.1.1

Masque de sous-réseau : 255.255.255.0

MGUARD1 réseau WAN :

Adresse IP : 10.1.80.100

Masque de sous-réseau : 255.255.255.0

Passerelle par défaut : 10.1.80.101 (adresse WAN du MGUARD2)

MGUARD2 réseau local LAN2 :

Adresse IP : 192.168.0.1

Masque de sous-réseau : 255.255.255.0

MGUARD2 réseau WAN :

Adresse IP : 10.1.80.101

Masque de sous-réseau : 255.255.255.0

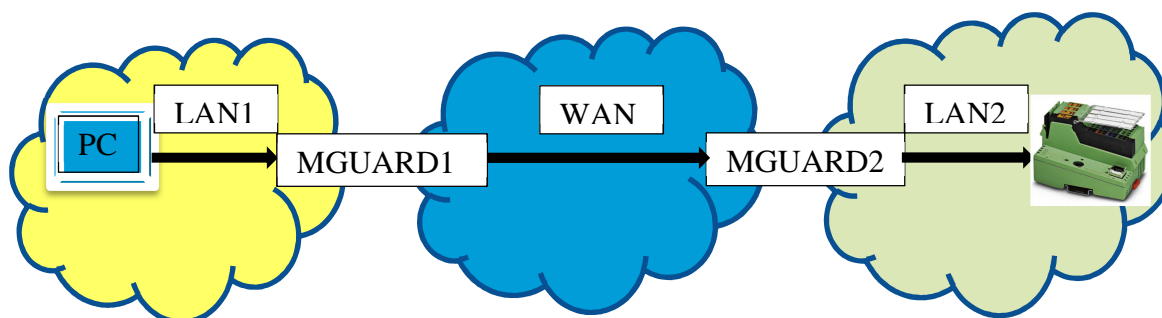
Passerelle par défaut : 10.1.80.100 (adresse WAN du MGUARD1)

ILC150ETH réseau local LAN2 :

Adresse IP : 192.168.0.3

Masque de sous-réseau : 255.255.255.0

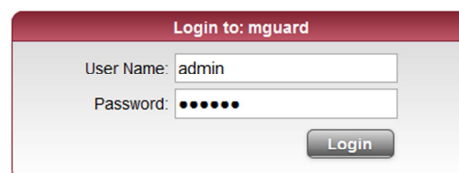
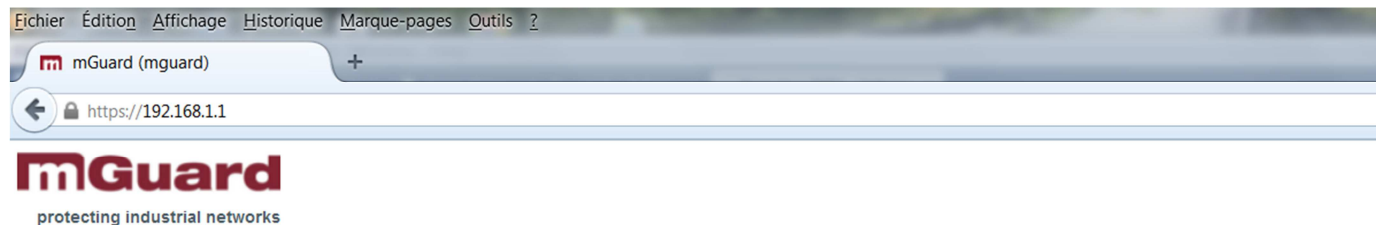
Passerelle par défaut : 192.168.0.1 (adresse locale du MGUARD2)



Configuration du MGUARD SMART2 VPN

Via n'importe quel explorateur Windows, se rendre sur l'adresse IP LAN du MGUARD : <https://192.168.1.1> ou WAN <https://1.1.1.1> puis entrer l'utilisateur « admin » et le mot de passe « mGuard ».

Tous ces paramètres sont les paramètres par défaut et modifiables.

A login form titled 'Login to: mguard'. It contains two input fields: 'User Name:' with the value 'admin' and 'Password:' with six dots. A 'Login' button is located at the bottom right of the form.

Si le MGUARD dispose déjà d'une adresse IP inconnue ou qu'il n'est plus accessible, utiliser la procédure de remise en configuration usine, deux séquences de 6 appuis à fréquence constante sur le bouton « Reset ».

Dans le menu « Network/Interfaces/Général » penser à changer le « Network Mode » en mode routeur car initialement paramétré en « Stealth ».

The screenshot shows the mGuard web interface with the following configuration details:

- Network Status:** External IP address: 10.1.80.100, Active Defaultroute: 10.1.80.101, Used DNS servers: DNS Root Servers.
- Network Mode:** Network Mode: Router, Router Mode: static.
- External Networks:** External IPs (untrusted port): IP: 10.1.80.100, Netmask: 255.255.255.0, Use VLAN: No, VLAN ID: 1. IP of default gateway: 10.1.80.101.
- Internal Networks:** Internal IPs (trusted port): IP: 192.168.1.1, Netmask: 255.255.255.0, Use VLAN: No, VLAN ID: 1.
- Secondary External Interface:** Network Mode: Off.

A red arrow points to the 'Apply' button at the bottom right of the configuration area.

Renseigner les adresses IP sur le modèle de l'architecture.

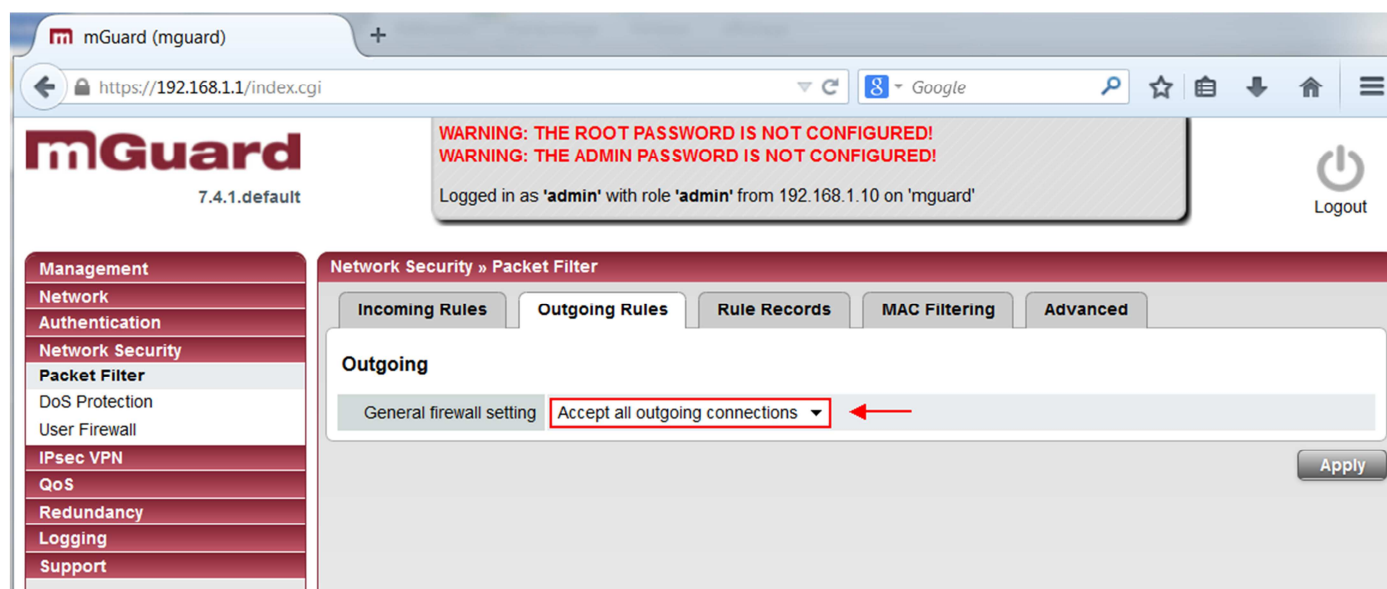
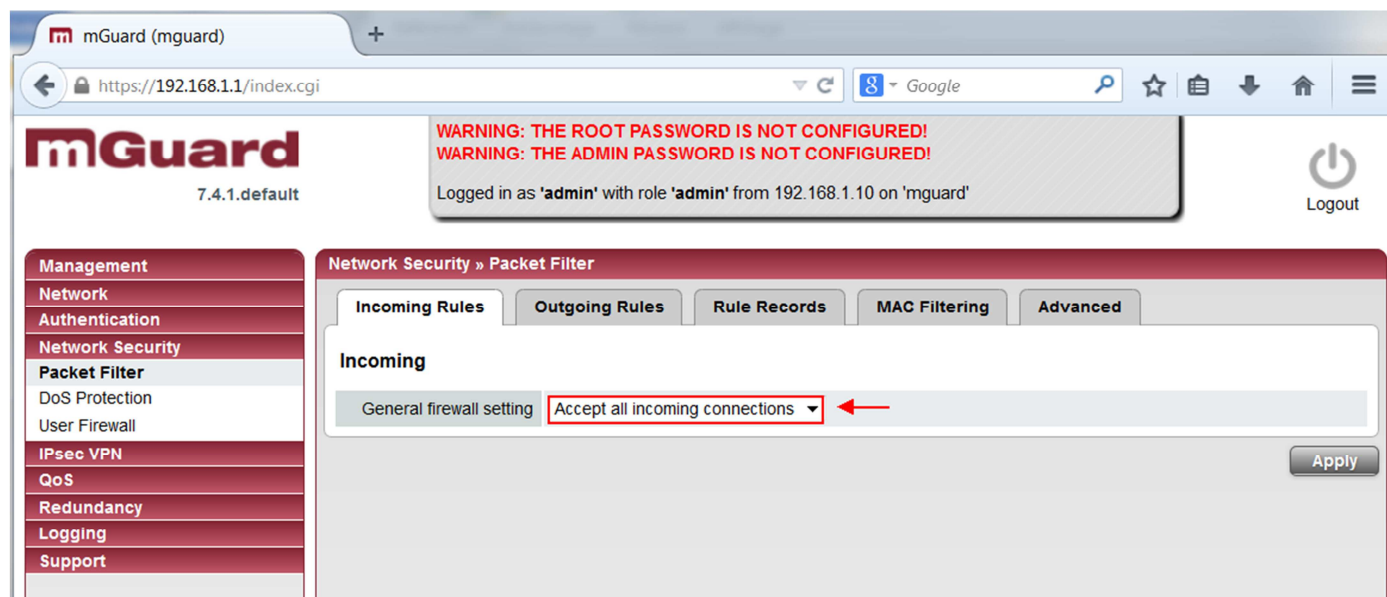
Nous rappelons qu'il est important de valider toute modification par le bouton « Apply » avant de changer de page sous peine de les perdre.

Dans les menus « Network/NAT/Masquerading » et « Network/NAT/IP and Port Forwarding » assurez-vous qu'aucun paramétrage ne soit effectif. En effet quand l'authentification par « Pre-Shared Secret Keys est utilisé il ne faut pas activer le « Network Adress Translation ».

The screenshot shows the mGuard web interface at the URL https://192.168.1.1/index.cgi. The page title is "mGuard 7.4.1.default". A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard'. The left sidebar contains a menu with items: Management, Network, Interfaces, NAT, DNS, DHCP, Proxy Settings, Authentication, Network Security, IPsec VPN, QoS, Redundancy, Logging, and Support. The main content area is titled "Network » NAT" and has two tabs: "Masquerading" and "IP and Port Forwarding". The "Masquerading" tab is active, showing "Network Address Translation/IP Masquerading". It features a table with columns: "Outgoing on Interface", "From IP", and "Comment". Below the table, there is explanatory text: "These rules let you specify which IP addresses (normally addresses within the private address space) are to be rewritten to the mGuard's IP address. Please note: These rules won't apply to the Stealth mode." Underneath, there is a section for "1:1 NAT" with a table with columns: "Local network", "External network", "Netmask", "Enable ARP", and "Comment". A note below this table states: "Please note: These rules only apply to the network mode 'Router' and if the router mode is set to 'static' or 'DHCP'." An "Apply" button is located at the bottom right of the configuration area.

The screenshot shows the mGuard web interface at the URL https://192.168.1.1/index.cgi. The page title is "mGuard 7.4.1.default". A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard'. The left sidebar contains a menu with items: Management, Network, Interfaces, NAT, DNS, DHCP, Proxy Settings, Authentication, Network Security, IPsec VPN, QoS, Redundancy, Logging, and Support. The main content area is titled "Network » NAT" and has two tabs: "Masquerading" and "IP and Port Forwarding". The "IP and Port Forwarding" tab is active, showing "IP and Port Forwarding". It features a table with columns: "N°", "Protocol", "From IP", "From Port", "Incoming on IP", "Incoming on Port", "Redirect to IP", "Redirect to Port", "Comment", and "Log". A log ID is displayed: "Log ID: fw-portforwarding-NP-00000000-0000-0000-0000-000000000000". Below the table, there is explanatory text: "These rules let you forward traffic targeted to the mGuard to another machine without modifying the source address. The column 'Incoming on IP' accepts the special value '%extern' as the mGuard's first external IP. Please note: These rules won't apply to the Stealth mode." An "Apply" button is located at the bottom right of the configuration area.

Dans les menus « Network security/Packet Filter/Incoming rules » et « Network security/Packet Filter/Outgoing rules » vérifiez que les règles de Firewall permettent tout trafic entrant et sortant.



Dans le menu « IPsec VPN/Connections » créez une connexion VPN en sélectionnant la flèche encadrée puis appuyez sur la touche Edit pour faire apparaître les paramètres à renseigner.

mGuard (mguard) | https://192.168.1.1/index.cgi | WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED! | Logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard' | Logout

Management | Network | Authentication | Network Security | IPsec VPN | Global | **Connections** | L2TP over IPsec | IPsec Status | QoS | Redundancy | Logging | Support

IPsec VPN » Connections

Enabled	Name	Action
Yes	PSKVPN1	Edit

Apply

mGuard (mguard) | https://192.168.1.1/index.cgi | WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED! | Logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard' | Logout

Management | Network | Authentication | Network Security | IPsec VPN | Global | **Connections** | L2TP over IPsec | IPsec Status | QoS | Redundancy | Logging | Support

IPsec VPN » Connections » PSKVPN1

General | Authentication | Firewall | IKE Options

Options

A descriptive name for the connection: PSKVPN1

Enabled: Yes

Address of the remote site's VPN gateway (Either an IP address, a hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway.): 10.1.80.101

Interface to use for gateway setting %any: External

Connection startup: Initiate

Encapsulate the VPN traffic in TCP: No

Transport and Tunnel Settings

Enabled	Type	Local	Remote	Action
Yes	Tunnel	192.168.1.0/24	192.168.0.0/24	More...

Back | Apply

Dans l'onglet « Authentication » Sélectionner la méthode d'authentification par Pre-shared Secret Key.

The screenshot shows the mGuard web interface at the URL https://192.168.1.1/index.cgi. A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10. The left sidebar contains a navigation menu with categories: Management, Network, Authentication, Network Security, IPsec VPN, Global, Connections, QoS, Redundancy, Logging, and Support. The main content area is titled "IPsec VPN » Connections » PSKVPN1" and has tabs for General, Authentication, Firewall, and IKE Options. The "Authentication" tab is active, showing the "Authentication method" set to "Pre-Shared Secret (PSK)" and the "Pre-Shared Secret Key (PSK)" set to "motdepasse". Below this is the "VPN Identifier" section with "Local" and "Remote" fields, each with a text input and a description: "By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname")." "Back" and "Apply" buttons are at the bottom right.

Dans l'onglet « Firewall » autorisez toutes les connexions entrantes et sortantes.

The screenshot shows the mGuard web interface at the URL https://192.168.1.1/index.cgi. A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10. The left sidebar is the same as in the previous screenshot. The main content area is titled "IPsec VPN » Connections » PSKVPN1" and has tabs for General, Authentication, Firewall, and IKE Options. The "Firewall" tab is active, showing the "Incoming" and "Outgoing" sections. In the "Incoming" section, the "General firewall setting" is set to "Accept all incoming connections". In the "Outgoing" section, the "General firewall setting" is set to "Accept all outgoing connections". "Back" and "Apply" buttons are at the bottom right.

Dans l'onglet « IKE Options » préférez l'encryptage « 3DES ».

The screenshot shows the mGuard web interface. At the top, there is a warning banner: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". Below this, the user is logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard'. The interface is divided into a left sidebar with navigation menus (Management, Network, Authentication, Network Security, IPsec VPN, Connections, QoS, Redundancy, Logging, Support) and a main content area. The main content area is titled "IPsec VPN » Connections » PSKVPN1" and has tabs for "General", "Authentication", "Firewall", and "IKE Options". The "IKE Options" tab is active, showing the "ISAKMP SA (Key Exchange)" and "IPsec SA (Data Exchange)" sections. Both sections have an "Encryption" dropdown menu set to "3DES" and a "Hash" dropdown menu set to "All algorithms". Below these sections is the "Perfect Forward Secrecy (PFS)" section, which is set to "Yes". The "Lifetimes and Limits" section contains several fields: ISAKMP SA Lifetime (3600 seconds), IPsec SA Lifetime (28800 seconds), IPsec SA Traffic Limit (0 bytes), Re-key Margin for Lifetimes (540 seconds), Re-key Margin for the Traffic Limit (0 bytes), Re-key Fuzz (100 %), Keying tries (0), and Rekey (Yes). The "Dead Peer Detection" section contains two fields: Delay between requests for a sign of life (30 seconds) and Timeout for absent sign of life after which peer is assumed dead (120 seconds). At the bottom left, there is a copyright notice: "Copyright © 2001-2011 Innominate Security Technologies AG and others".

Configuration du MGUARD RS2000 VPN

Tous les paramètres sont identiques à l'exception des menus impliquant les adresses IP comme suit :

The screenshot shows the web interface for MGUARD RS2000 VPN. The browser address bar shows `https://192.168.0.1/index.cgi`. The page header includes the Phoenix Contact logo and the text "FL MGUARD 7.4.0.default". A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard'. The interface is divided into a left sidebar and a main content area.

Management

- Network
- Interfaces**
- NAT
- DNS
- DHCP
- Proxy Settings
- Authentication
- Network Security
- IPsec VPN
- Logging
- Support

Network » Interfaces

General | Ethernet | Console

Network Status

External IP address	10.1.80.101
Active Default route	10.1.80.100
Used DNS servers	DNS Root Servers

Network Mode

Network Mode	Router
Router Mode	static

External Networks

	IP	Netmask	Use VLAN	VLAN ID
External IPs (untrusted port)	10.1.80.101	255.255.255.0	No	1
Additional External Routes	Network	Gateway		
IP of default gateway	10.1.80.100			

Internal Networks

	IP	Netmask	Use VLAN	VLAN ID
Internal IPs (trusted port)	192.168.0.1	255.255.255.0	No	1
Additional Internal Routes	Network	Gateway		

Concernant le MGUARD en attente, spécifiquement en PSK, il faut absolument préciser l'adresse IP du site initiateur distant sans utiliser le sigle %any.

PHOENIX CONTACT
FL MGUARD 7.4.0.default

WARNING: THE ROOT PASSWORD IS NOT CONFIGURED!
WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!

Logged in as 'admin' with role 'admin' from 192.168.1.10 on 'mguard'

Apply Reset Logout

Management
Network
Authentication
Network Security
IPsec VPN
Global
Connections
L2TP over IPsec
IPsec Status
Logging
Support

IPsec VPN » Connections » PSKVPN1

General Authentication Firewall IKE Options

Options

A descriptive name for the connection: PSKVPN1

Enabled: Yes

Address of the remote site's VPN gateway (Either an IP address, a hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway.): 10.1.80.100

Interface to use for gateway setting %any: External

Connection startup: Wait

Encapsulate the VPN traffic in TCP: No

Transport and Tunnel Settings

Enabled	Type	Local	Remote	Action
Yes	Tunnel	192.168.0.0/24	192.168.1.0/24	More...

Back

Mise en service de la communication

Dans le cas où vous êtes connectés au réseau d'entreprise via des « Proxys » il vous faudra ajouter au moins une route car le système ne sait gérer qu'une passerelle.

Dans la fenêtre « Invite de commandes » utilisez la commande « route » comme suit :

C:\route add 192.168.0.0 mask 255.255.255.0 192.168.1.1 metric 3

Il faut alors enlever la passerelle d'adresse 192.168.1.1 dans l'IPV4 de la carte réseau afin de garder toutes les fonctionnalités d'accès à l'extérieur via le réseau d'entreprise.

Une fois la commande acceptée l'on peut observer les Statuts VPN depuis le menu « IPsec VPN/IPsec Status » des deux MGUARD :

The screenshot shows the mGuard (mguard) web interface. The browser address bar displays `https://192.168.1.1/index.cgi`. A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10. The left sidebar menu includes: Management, Network, Authentication, Network Security, IPsec VPN, Global, Connections, L2TP over IPsec, IPsec Status (selected), QoS, Redundancy, Logging, and Support. The main content area is titled "IPsec VPN » IPsec Status" and contains a table with the following data:

Connection Name	Connection	ISAKMP State	IPsec State
PSKVPN1 (MAI1332005173_1)	Gateway	10.1.80.100	10.1.80.101
	Traffic	192.168.1.0/24	192.168.0.0/24
	ID		
		STATE_MAIN_I4 (ISAKMP SA established)	STATE_QUICK_I2 (sent QI2, IPsec SA established)
		Algorithm: 3DES_CBC_192-MD5-MODP1536	Algorithm: 3DES_0-HMAC_MD5
		Lifetime: 2460s	Lifetime: 21778s

Buttons for "Edit", "Restart", and "Update" are visible below the table.

The screenshot shows the PHENIX CONTACT FL MGUARD 7.4.0.default web interface. The browser address bar displays `https://192.168.0.1/index.cgi`. A warning banner at the top states: "WARNING: THE ROOT PASSWORD IS NOT CONFIGURED! WARNING: THE ADMIN PASSWORD IS NOT CONFIGURED!". The user is logged in as 'admin' with role 'admin' from 192.168.1.10. The left sidebar menu includes: Management, Network, Authentication, Network Security, IPsec VPN, Global, Connections, L2TP over IPsec, IPsec Status (selected), Logging, and Support. The main content area is titled "IPsec VPN » IPsec Status" and contains a table with the following data:

Connection Name	Connection	ISAKMP State	IPsec State
PSKVPN1 (MAI0463838752_1)	Gateway	10.1.80.101	10.1.80.100
	Traffic	192.168.0.0/24	192.168.1.0/24
	ID		
		STATE_MAIN_R3 (sent MR3, ISAKMP SA established)	STATE_QUICK_R2 (IPsec SA established)
		Algorithm: 3DES_CBC_192-MD5-MODP1536	Algorithm: 3DES_0-HMAC_MD5
		Lifetime: 2922s	Lifetime: 22459s

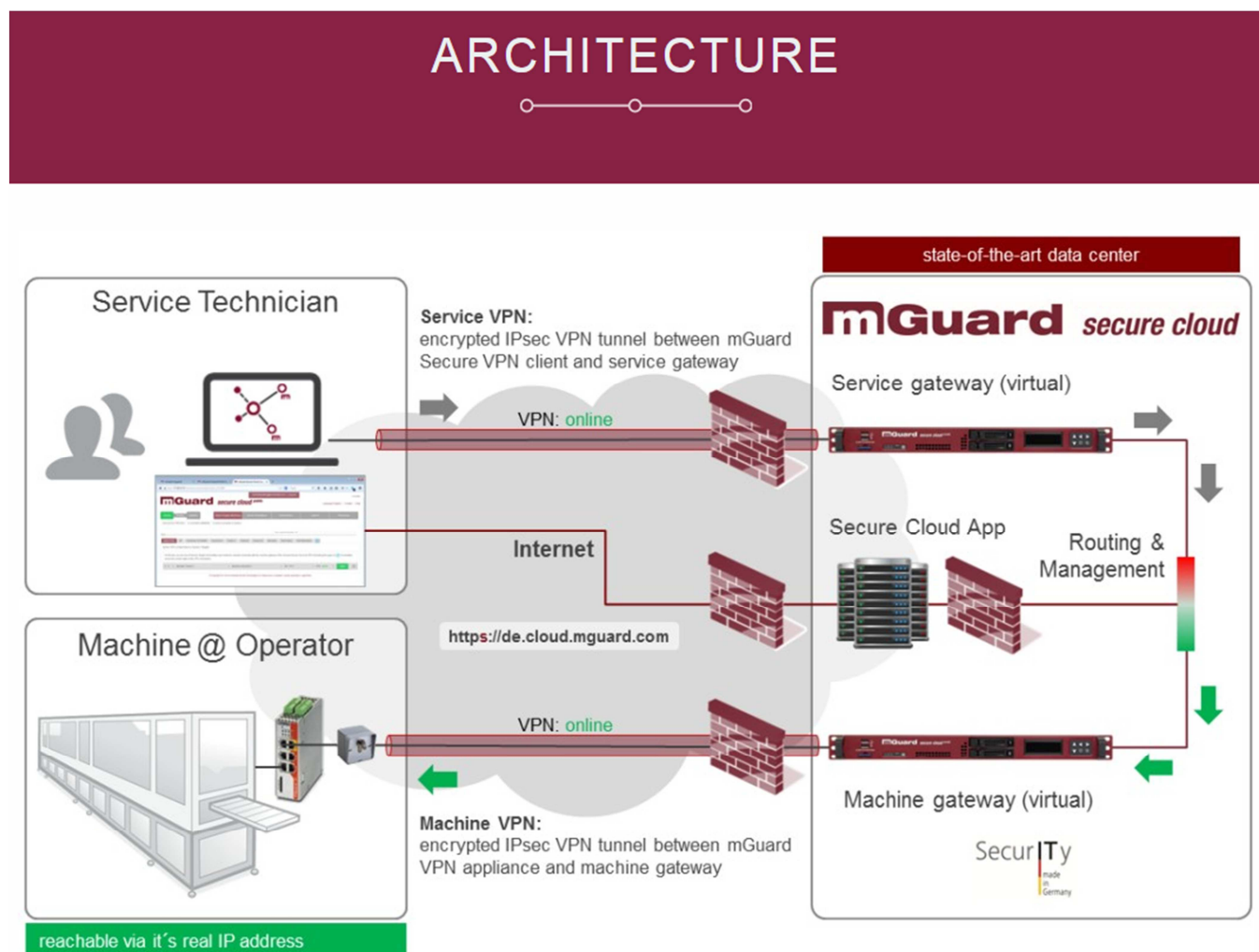
Buttons for "Edit", "Restart", and "Update" are visible below the table.

MGUARD Secure Cloud

Une autre solution consiste à utiliser en tant qu'assistance à la mise en service de la communication, le Cloud d'innominate.

C'est un portail qui permet de configurer une communication distante simplement avec un niveau de sécurité optimal.

L'architecture implique des connexions sortantes depuis la station de travail ainsi que des machines distantes, ce qui facilite la gestion des différentes politiques de sécurité. Le schéma ci-dessous illustre bien ce fait :

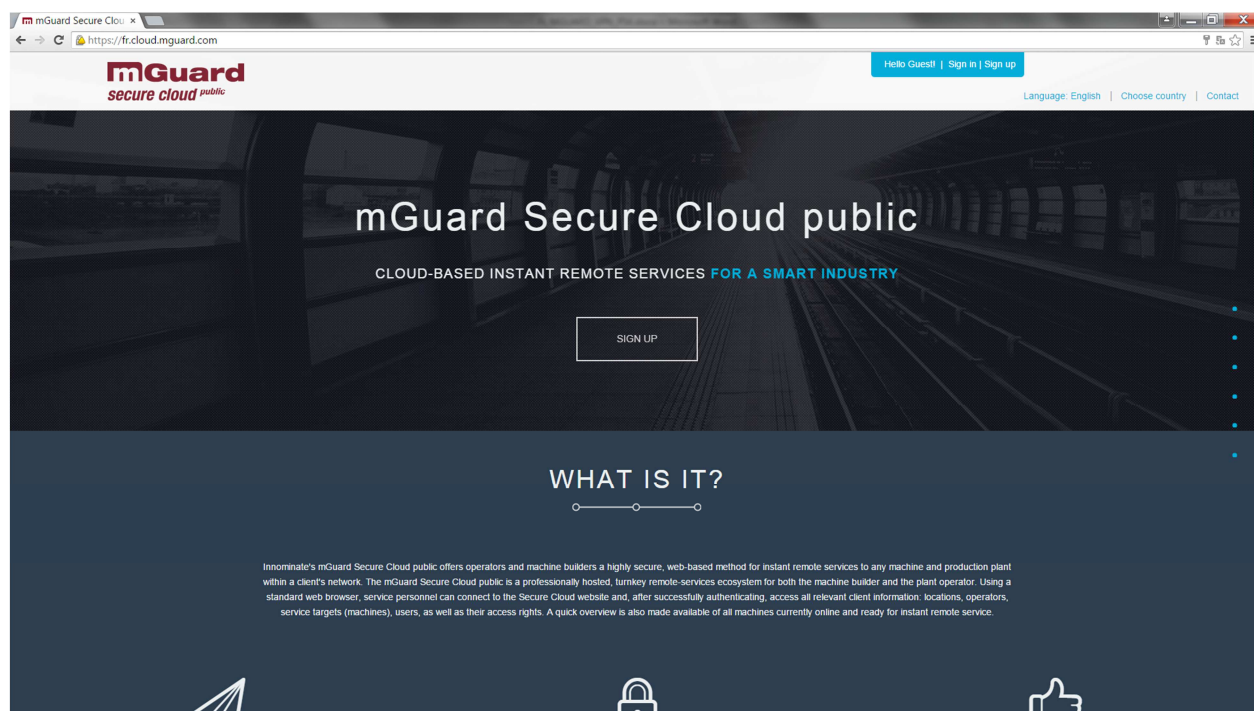


Le portail fournit aux tenants et aboutissants les fichiers de configuration des tunnels IPsec VPN avec certificats, ce qui évite toute programmation. Une fois les connexions sortantes validées il suffit depuis le portail d'assurer la jonction.

Trois formules sont disponibles permettant une prise en main progressive et adaptée aux différentes applications :

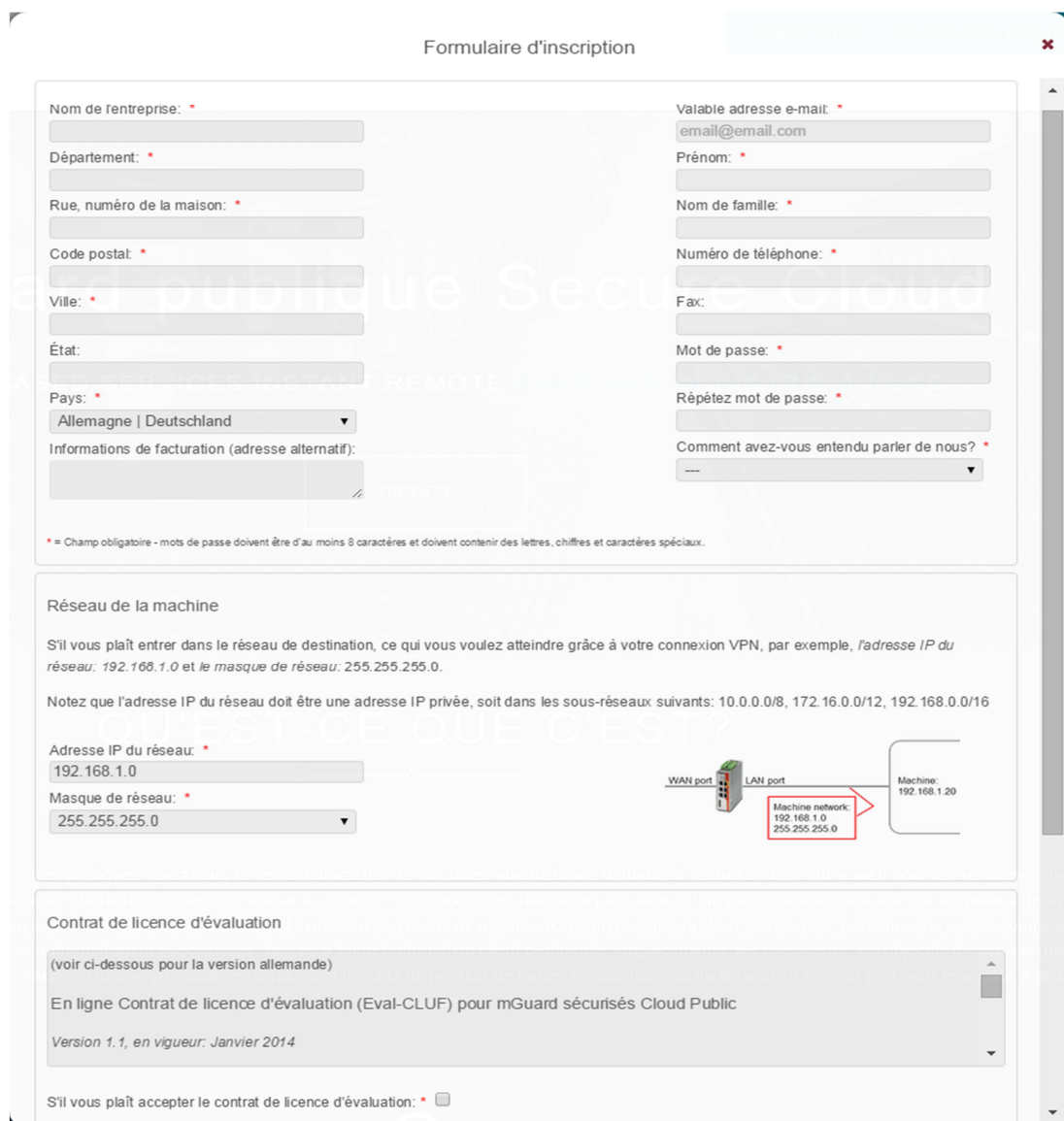
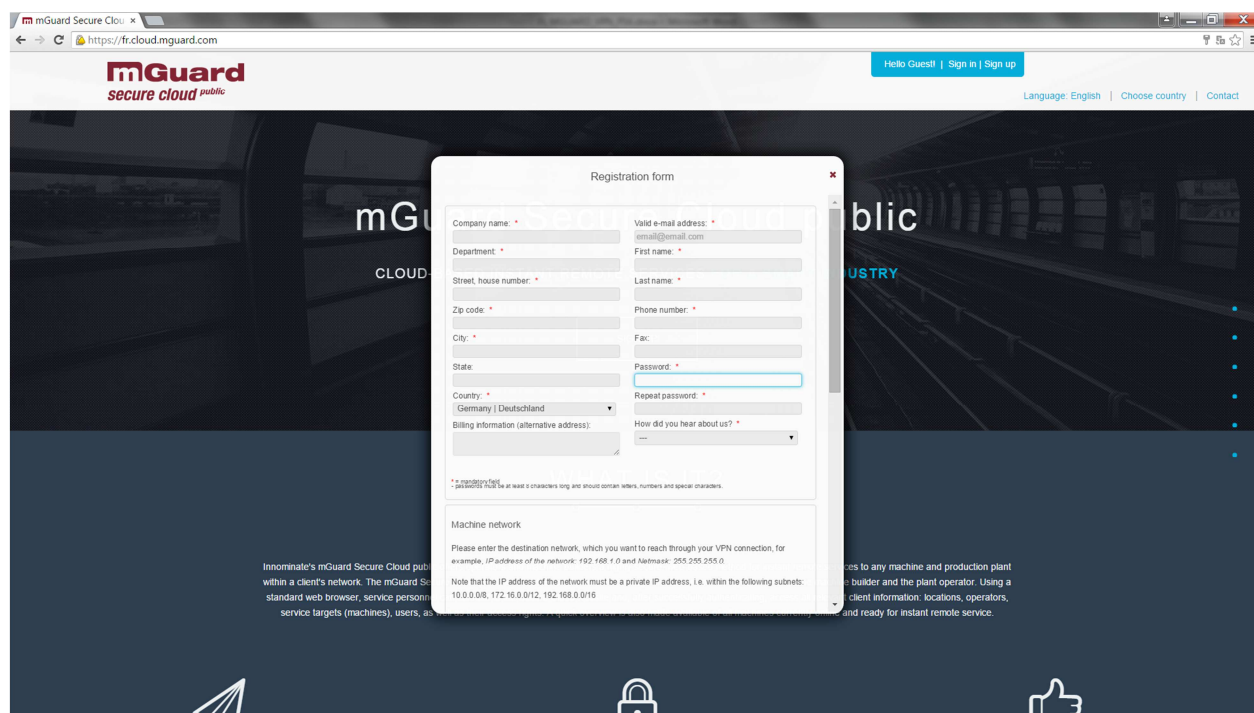
EDITIONS DISPONIBLES					
EVAL		BASE		PREMIUM	
30 jours gratuitement		gratuit		Payant	
SPÉCIFICATIONS:		SPÉCIFICATIONS:		SPÉCIFICATIONS:	
Nombre d'utilisateurs:	illimité	Nombre d'utilisateurs:	illimité	Nombre d'utilisateurs:	illimité
Nombre de machines:	1	Nombre de machines:	Illimité	Nombre de machines:	dépendante licence
Nombre de séances d'utilisateurs simultanés:	1	Nombre de séances d'utilisateurs simultanés:	1	Nombre de séances d'utilisateurs simultanés:	1
Bande passante par connexion de service garanti:	Non	Bande passante par connexion de service garanti:	Non	Bande passante garantie par raccordement au service:	
Garantie de disponibilité:	Non	Garantie de disponibilité:	Non	Disponibilité garantie:	98% ¹ Mbit / s
Volume de transfert par raccordement au service: 1 Go / mois		Volume de transfert par raccordement au service: 1 Go / mois		Volume de transfert par raccordement au service:	illimité
Niveau Hébergement:	Mission critique	Niveau Hébergement:	Faible	Niveau Hébergement:	Mission critique
Service de clients VPN:	mGuards, logiciel IPsec	Service de clients VPN:	mGuards, logiciel IPsec	Service de clients VPN:	mGuards, logiciel IPsec
Clients VPN machine:	mGuards	Clients VPN machine:	mGuards	Clients VPN machine:	mGuards
Hotline:	téléphone, e-mail	Hotline:	e-mail	Hotline:	téléphone, e-mail
CARACTÉRISTIQUES		CARACTÉRISTIQUES		CARACTÉRISTIQUES	
Modèle d'autorisation:	Enhanced	Modèle d'autorisation:	standard	Modèle d'autorisation:	Enhanced
Reporting:	Oui	Reporting:	Oui	Reporting:	Oui
Signaler filtrage:	Oui	Signaler filtrage:	Non	Signaler filtrage:	Oui
Rapport exportation:	Oui (CSV, XLS, PDF)	Exporter le rapport:	Non	Rapport exportation:	Oui (CSV, XLS, PDF)

Ce portail est accessible en renseignant suivant la zone géographique dans votre navigateur internet l'adresse suivante (cas de la France) : <https://fr.cloud.mguard.com/>
 Nous recommandons l'utilisation de Firefox (V17.0 ou plus), Google Chrome (V28.0 ou plus), Apple Safari (V5.1.7 ou plus) voire Internet Explorer 10 minimum.



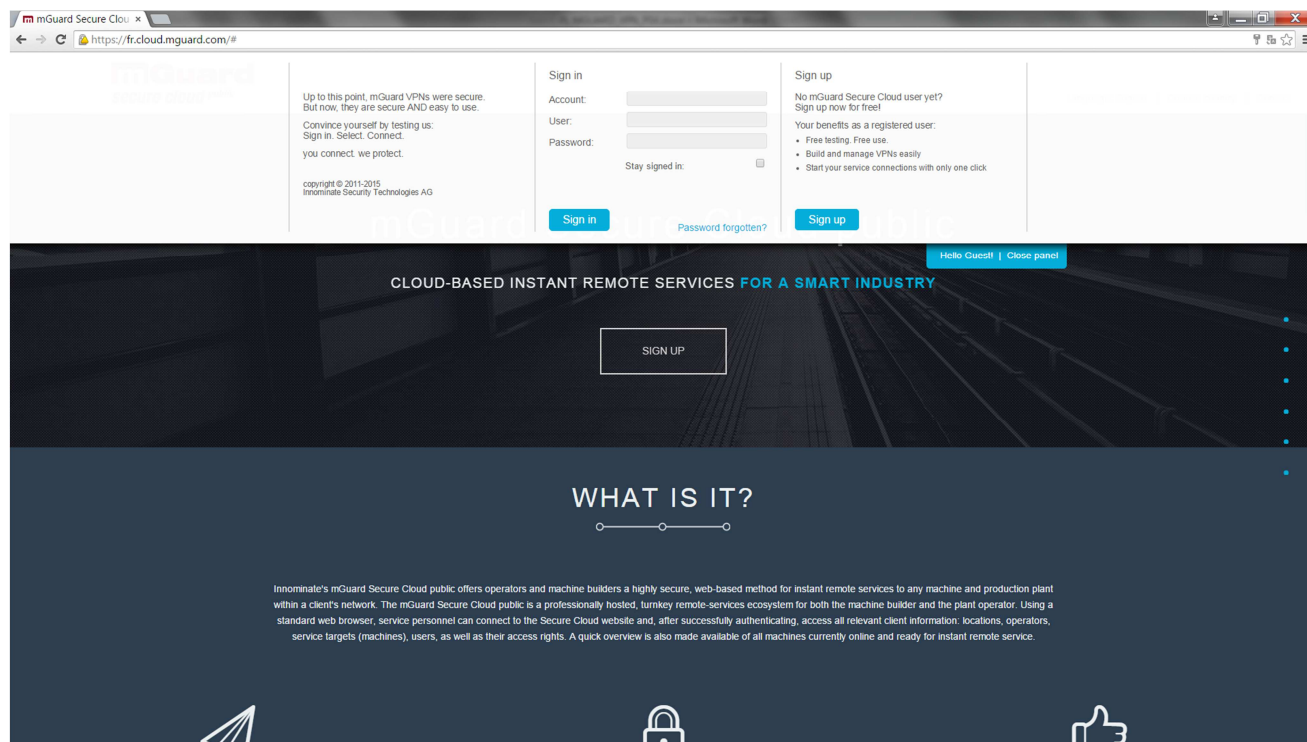
MGUARD Secure Cloud
FL MGUARD_VPN_PSK
Version : 1

Dans un premier temps et afin de bénéficier de l'offre gratuite valable pendant 30 jours il est nécessaire de remplir un formulaire en cliquant sur la zone « SIGNER » :



Une fois ce formulaire renseigné vous devrez confirmer par réponse à un mail reçu les clauses du contrat afin de transformer la formule « EVAL » en une formule « BASE » ou « PREMIUM ».

Enfin pour vous connecter à votre compte il vous faudra renseigner les paramètres « Compte », « Utilisateur » et « mot de passe » fournis dans le mail de confirmation.

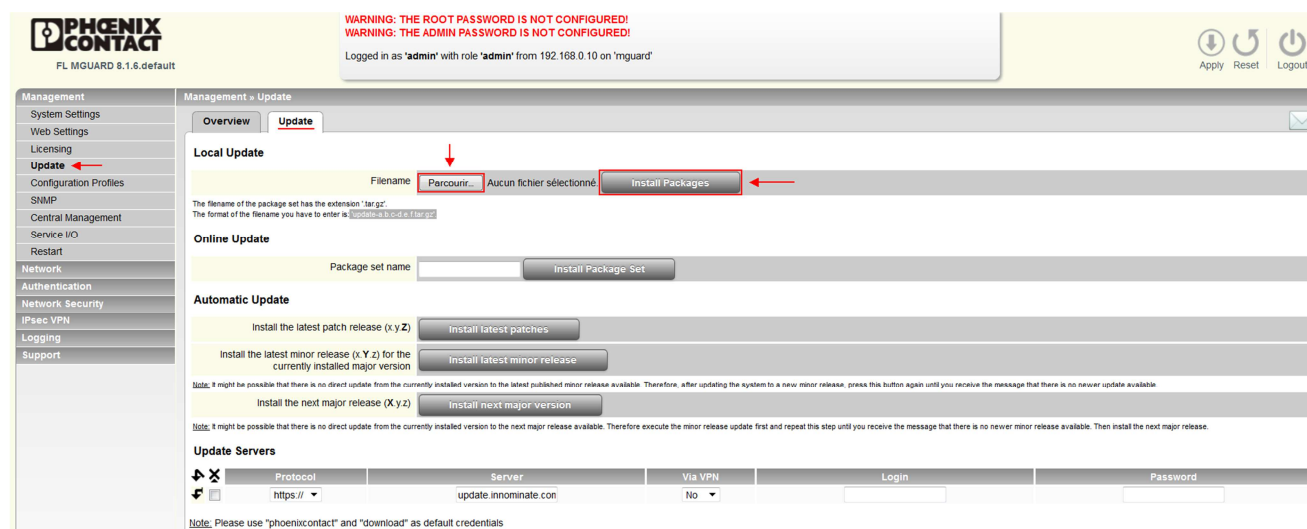


Notez que tous les équipements mGuard connectés au portail doivent impérativement avoir la version Firmware 7.5 minimum.

La Mise à jour du Firmware est téléchargeable sur notre site

<https://www.phoenixcontact.com/online/portal/fr> dans l'onglet « Téléchargements » du produit concerné. C'est un fichier compressé de type « update-a.b.c-d.e.f.tar.gz ».

Dans le mGuard aller dans le menu « Management/Update » comme suit :

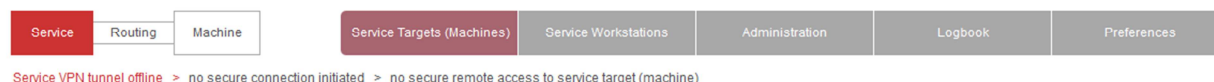


Dans « Local Update » appuyer sur « Parcourir » et sélectionner le fichier « update-a.b.c-d.e.f.tar.gz » puis « Install Packages ».

A la première connexion au portail vous obtenez :

mGuard *secure cloud public*

Account: PHO77401FR | User: jfouard@phoenixcontact.fr | Role: admin



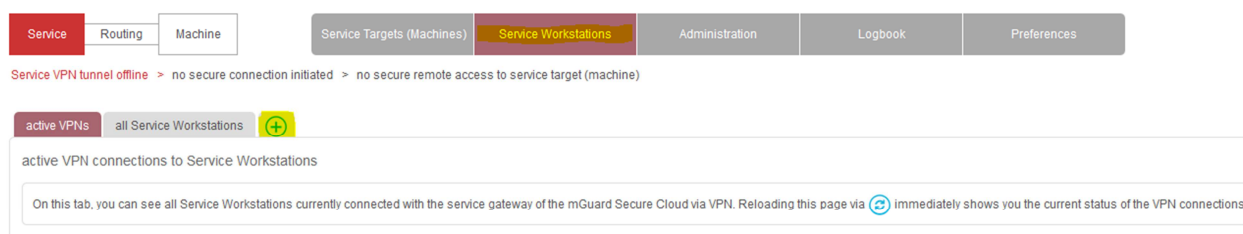
Les services principaux sont présentés en deux parties :

- Station de travail
- Machines

Il est préférable de commencer par la station de travail comme suit :

mGuard *secure cloud public*

Account: PHO77401FR | User: jfouard@phoenixcontact.fr | Role: admin

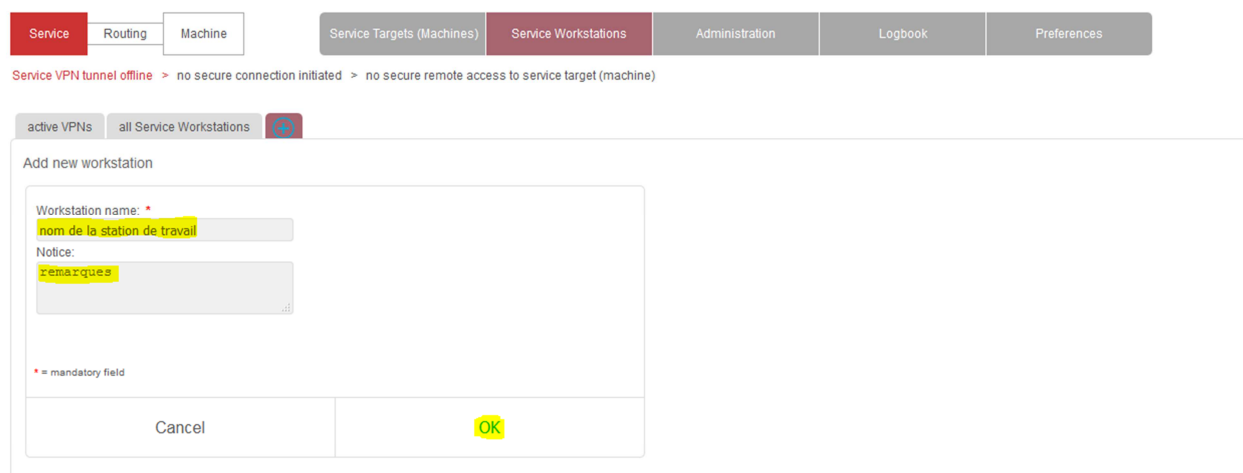


© Copyright 2011-2015 Innominate Security Technologies AG | Data privacy | Evaluation License Agreement | Legal Notice

Sélectionner l'onglet marqué d'un « + » pour ajouter une nouvelle station de travail :

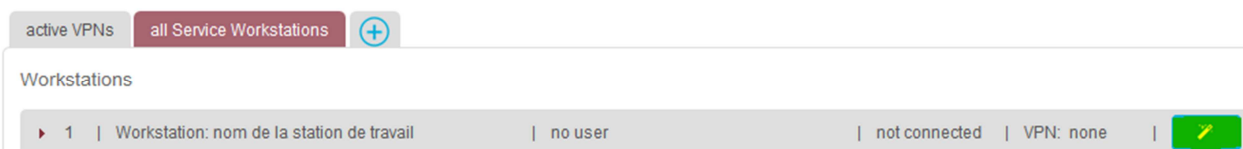
mGuard *secure cloud public*

Account: PHO77401FR | User: jfouard@phoenixcontact.fr | Role: admin



© Copyright 2011-2015 Innominate Security Technologies AG | Data privacy | Evaluation License Agreement | Legal Notice

Après avoir renseigné le nom et d'éventuelles remarques et validé, vous ajoutez à la liste existante une nouvelle station que vous pourrez paramétrer par l'appui sur l'icône stylet :



Vous obtenez alors la feuille de renseignement présentant les trois types de clients VPN possibles :

The screenshot shows the 'VPN-Builder | Request VPN configuration (service: nom de la station de travail)' window. It has three tabs: '1 VPN client type', '2 VPN connection', and '3 Machine network'. The 'VPN client type' tab is active. The form contains the following elements:

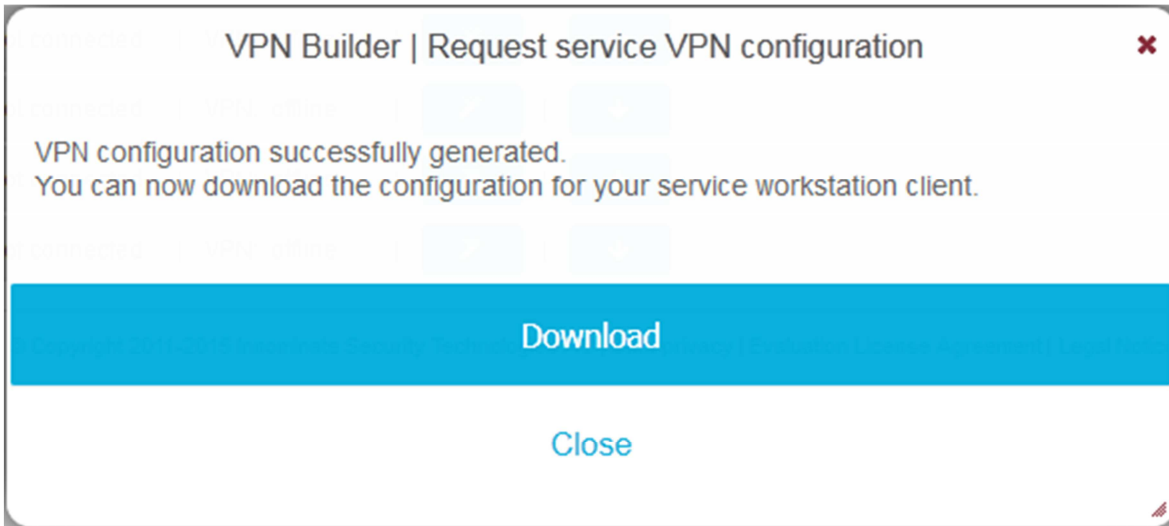
- VPN client type**
- Text: "What kind of VPN client are you going to use for this service workstation? Your workstation can be securely connected to the mGuard Secure Cloud public via *mGuard VPN appliances* like mGuard smart® or mGuard delta®. You may also use a certified software IPsec VPN client like the *mGuard Secure VPN Client*."
- Choose a VPN client type**
- Three radio button options:
 - mGuard Secure VPN Client (commercial software client with vendor support)
 - Shrew Soft VPN Client (free open source software client)
 - mGuard VPN appliance (hardware)
- Please enter the client password:**
- Two password input fields with 'Show' buttons:
 - Password: *
 - Repeat password: *
- Footnote: "* = mandatory field - passwords must be at least 8 characters long and should contain letters, numbers and special characters."
- Navigation buttons: 'Back', 'Next', and 'Request'.

Après avoir obligatoirement renseigné le mot de passe si le choix s'est porté par exemple sur un client VPN logiciel :

The screenshot shows the 'VPN-Builder | Request VPN configuration (service: nom de la station de travail)' window. The 'Machine network' tab is active. The form contains the following elements:

- Machine network**
- Text: "Here you can configure the destination network, which you want to reach through your VPN connection, for example, *IP address of the network: 192.168.1.0 and Netmask: 255.255.255.0*." Note that the IP address of the network must be a private IP address, i.e. within the following subnets: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16"
- Input fields for network configuration:
 - IP address of the network: * (value: 192.168.0.0)
 - Netmask: (value: 255.255.255.0)
- Diagram: A router icon with 'WAN port' and 'LAN port' labels. A red box highlights the 'Machine network: 192.168.1.0 255.255.255.0' configuration, with an arrow pointing to a 'Machine: 192.168.1.20' box.
- Navigation buttons: 'Back', 'Next', and 'Request'.

L'appui sur la touche « Request » permet de télécharger le fichier de configuration pour le VPN client Shrewsoft dans notre exemple.

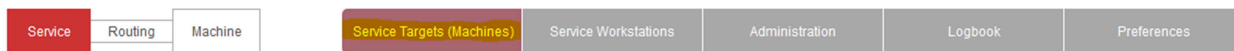


Vous obtenez un fichier de type *.vpn exploitable via le logiciel VPN client Shrewsoft en renseignant le mot de passe choisi.

Vous pouvez maintenant passer à l'étape suivante en sélectionnant la cible « Machines » :

mGuard *secure cloud public*

Account: PHO77401FR | User: jfouard@phoenixcontact.fr | Role: admin



Service VPN tunnel offline > no secure connection initiated > no secure remote access to service target (machine)

Sélectionner l'onglet marqué d'un « + » pour ajouter une nouvelle Machine, opération qui se fait en deux temps, « Lieu » et « Machine » :

Add new operator/location

Operator/location name: *	Contact person:
<input type="text" value="lieu"/>	<input type="text"/>
Street, house number:	Phone number:
<input type="text"/>	<input type="text"/>
Zip code:	Fax:
<input type="text"/>	<input type="text"/>
City:	e-mail address:
<input type="text"/>	<input type="text"/>
Country:	Notice:
<input type="text"/>	<input type="text"/>

* = mandatory field

Cancel OK

Add new machine ✕

<p>Machine name: * <input type="text" value="Machine"/></p> <p>Type: <input type="text"/></p> <p>Serial number: <input type="text"/></p> <p>Build year: <input type="text"/></p> <p>Manufacturer: <input type="text"/></p> <p>Supplier: <input type="text"/></p> <p>Manufacturing number: <input type="text"/></p> <p>Delivery day: <input type="text"/></p>	<p>Location: <input type="text"/></p> <p>Positioning data (Lat,Long): <input type="text"/></p> <p>Inventory number: <input type="text"/></p> <p>Cost center: <input type="text"/></p> <p>Activation: <input type="text"/></p> <p>Software: <input type="text"/></p> <p>Notice: <input type="text"/></p>
--	--

* = mandatory field

Cancel
OK

Vous ajoutez à la liste existante une nouvelle machine que vous pourrez paramétrer par l'appui sur l'icône stylet :

VPN-Builder | Request VPN configuration (machine: Machine) ✕

1 mGuard mode
2 VPN connection
3 3G
4 External network
5 Internal network
6 Misc.

mGuard operation mode

The mGuard can operate in different modes:

- if the machine is designed to fit into the existing network the *Stealth* mode (which behaves transparently to the network) should be used.
- if the end customer network and the machine network are different, the *Router* mode should be used to connect both networks.
- if the machine is connected via a mobile connection 3G should be used.
- choose *Ethernet plus 3G* if a mobile connection is used as a fallback for an ethernet connection .

Choose a mode

Stealth
 Router
 3G
 Ethernet plus 3G

Back
Next
Request

Différentes étapes permettent de renseigner les caractéristiques principales de fonctionnement du mGuard afin de télécharger son fichier de configuration.

VPN-Builder | Request VPN configuration (machine: Machine)

1 mGuard mode 2 **VPN connection** 3 3G 4 External network 5 Internal network 6 Misc.

VPN connection mode (UDP/TCP configuration)

An mGuard VPN appliance can use different ports to establish a connection to a destination device. When using *standard IPsec ports*, the UDP ports 4500 and 500 must be opened for outbound IPsec traffic (also through firewalls, proxies, etc.).

When choosing *secure HTTP port TCP 443*, IPsec traffic will be encapsulated and carried firewall friendly via standard TCP port 443 (TCP encapsulation). An interconnected proxy server can also be used.

Connect through

the standard IPsec ports of UDP 500 and 4500

the secure HTTP port TCP 443 (this also supports going through a network proxy)

Proxy configuration (optional)

Does your company network use a proxy? If you don't know if a proxy is used, your IT department should be able to help.

Proxy IP address:

Proxy port:

Proxy login (if necessary):

Proxy password (if necessary):

Back Next Request

La connexion VPN offre le choix d'utiliser les ports standards IPsec (500 et 4500) ou des ports sécurisés notamment en présence de serveurs proxys. Dans ce cas il sera nécessaire de renseigner au minimum l'adresse IP ainsi que le port du proxy.

VPN-Builder | Request VPN configuration (machine: Machine)

1 mGuard mode 2 VPN connection 3 3G 4 **External network** 5 Internal network 6 Misc.

External network

DNS configuration (optional)

Enter the DNS Server Address used by the mGuard.

IP address of DNS server (optional):

Configuration external IP address

Select the external IP address mode of the machine side mGuard VPN appliance:

- choosing *static IP address* means that the mGuard VPN appliance requires a fixed IP address in the customer LAN.
- choosing *Dynamic IP address (DHCP)* means the mGuard VPN appliance is assigned an IP address via DHCP (not available in stealth mode).

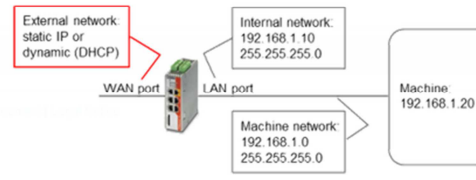
Static IP address

Dynamic IP address (DHCP)

Netmask:

Default gateway:

mGuard IP address (WAN port):



Back Next Request

VPN-Builder | Request VPN configuration (machine: Machine)

1 mGuard mode 2 VPN connection 3 3G 4 External network 5 Internal network 6 Misc.

Internal network

The mGuard IP address (LAN port) together with the Netmask of internal network is the reserved IP of the mGuard VPN appliance in your machine network.

Note that the IP address of the network must be a private IP address, i.e. within the following subnets: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16

mGuard IP address (LAN port): *
192.168.0.10

Netmask of internal network: *
255.255.255.0

External network: static IP or dynamic (DHCP)

Internal network: 192.168.1.10
255.255.255.0

Machine network: 192.168.1.0
255.255.255.0

Machine: 192.168.1.20

Back Next Request

Une fois les paramètres du réseau externe comme du réseau interne renseignés, il est demandé de préciser l'extension du fichier de configuration pour cibler soit directement le mGuard soit une carte SD enfichable ultérieurement dans le routeur :

VPN-Builder | Request VPN configuration (machine: Machine)

1 mGuard mode 2 VPN connection 3 3G 4 External network 5 Internal network 6 Misc.

Misc.

Choose the format of the VPN configuration for your machine connection:

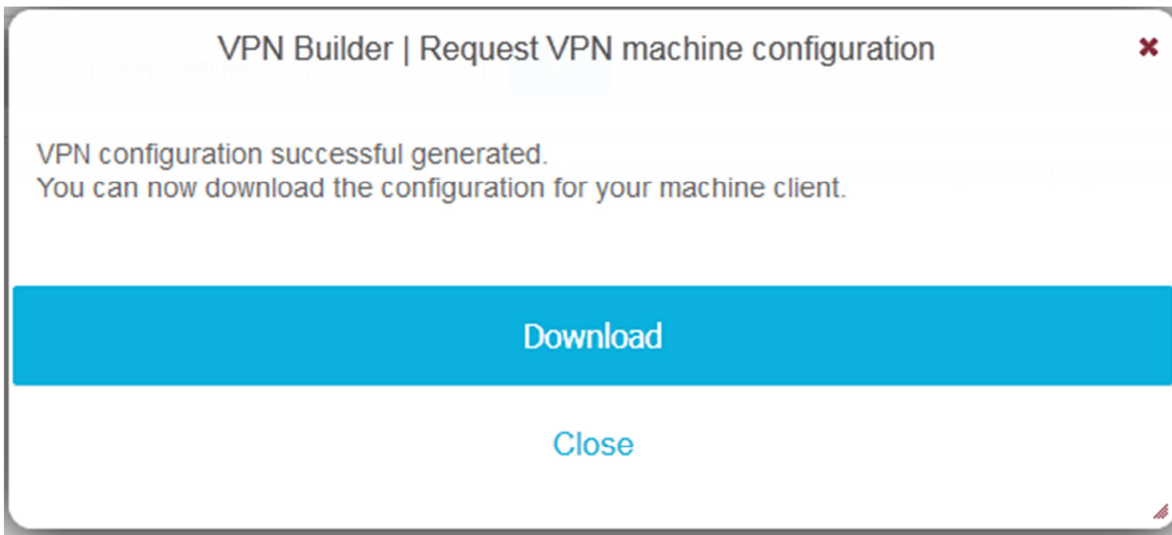
- type atv to upload the configuration via the mGuard web interface
- type ecs to activate the configuration via external configuration memory (e.g. SD card, USB stick)

Format of the mGuard configuration file:
.atv

Please enter the serial number of the mGuard VPN appliance to configure (optional):
mGuard serial number:

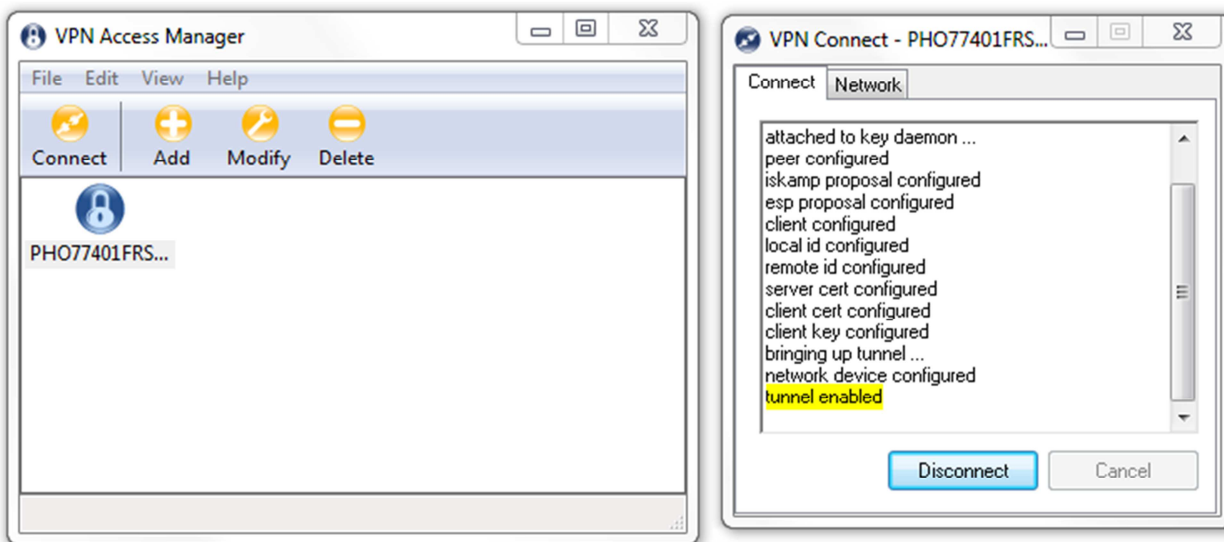
Shall the vpn connection be initiated via a key switch (Service-ID)?
Use key switch: no

Back Next Request



Vous obtenez un fichier de type *.atv téléchargeable directement dans le mGuard ou de type *.ecs téléchargeable dans une carte SD qui sera ensuite enfichée dans le mGuard.

Vous pouvez maintenant passer à l'étape suivante en activant le tunnel VPN depuis le logiciel Shrewsoft avec le fichier téléchargé :



Quand le tunnel VPN entre la station de travail et le cloud vous obtenez :



Appuyer alors sur la touche « Start » pour finaliser la connexion entre la station de travail et la machine sélectionnées.

Vous obtenez alors le visuel « Service/Router/Machine » totalement vert qui confirme la réunion des deux connexions sortantes :


mGuard *secure cloud public*

Account: PHO77401FR | User: jfouard@phoenixcontact.fr | Role: admin

Service Routing Machine Service Targets (Machines) Service Workstations Administration Logbook Preferences

Service VPN tunnel online > secure connection initiated > Maquette Phoenix Emérainville / mGuard

active VPN connections to Service Targets

On this tab, you can see all Service Targets like facilities and machines currently connected with the mGuard Secure Cloud public via secure VPN. Reloading this page via  immediately shows the current status of the VPN connections.

▼ 1 | Operator: Maquette Phoenix Emérainville | Machine: mGuard | SN: | VPN: **online** | Stop

Vous pouvez alors à tout moment décider de gérer comme bon vous semble la liaison VPN.