

# Tecnologias de Comunicação sem Fio

## Mguard Secure Cloud

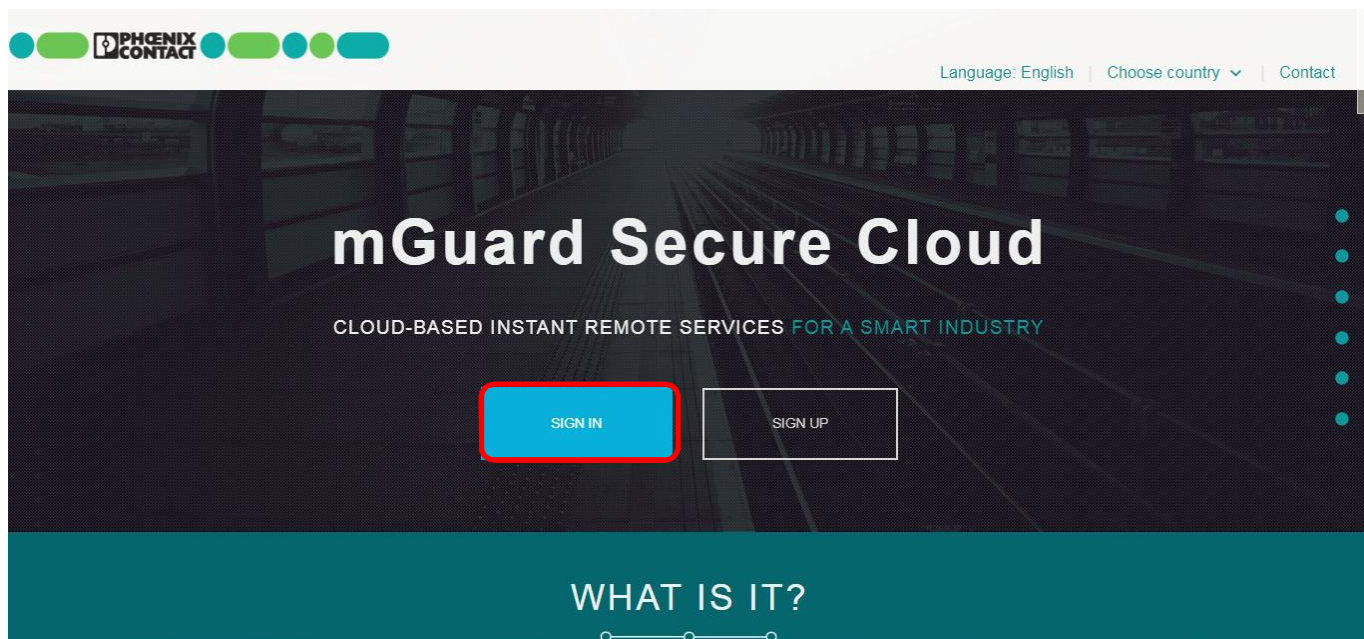


## TC Cloud LAN

# 1. Acessar o portal MGuard Secure Cloud

<https://us.cloud.mguard.com>

## a) Fazer login – SIGN IN



## b) Inserir dados do usuário para login

The image shows a 'SIGN IN' dialog box. It has three input fields: the first contains 'PHO91301US' (highlighted with a red box), the second contains 'phoenixcontactrs@gmail.com', and the third contains a masked password '\*\*\*\*\*'. Below the fields is a checkbox labeled 'Stay signed in'. At the bottom are 'Cancel' and 'OK' buttons (the 'OK' button is highlighted with a red box). A 'Password forgotten?' link is also present.

Conta: PHO91301US  
User: [phoenixcontactrs@gmail.com](mailto:phoenixcontactrs@gmail.com)  
Senha: Pxc@123456

## 2. Configurar o TC CLOUD a ser acessado remotamente

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

Service Targets (Machines)

Active VPNs

Active VPN connections to Service Targets

All Service Targets (facilities and machines) currently connected with the mGuard Secure Cloud via secure VPN.

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice

### a) Criar uma nova configuração de dispositivo ou editar uma já feita

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

Service Targets (Machines)

Active VPNs

PxC\_BR

		SN:	VPN:		
1	RS2000_3G		offline		
2	RS4000-4G		offline		
3	RS4000_TX		offline		

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice

### b) Escolher o modelo e o modo em que o dispositivo irá trabalhar

VPN Builder | Request VPN configuration (machine: TC CLOUD TX/TX)

1 VPN client (machine) 2 VPN connection 3 Mobile 4 Network 5 Internal network 6 Misc.

Choose a VPN client and mode

☐ mGuard Stealth mode

☐ mGuard Router mode

☐ mGuard Mobile (4G/3G)

☐ mGuard Ethernet plus 4G/3G

☒ TC CLOUD CLIENT LAN

☐ TC CLOUD CLIENT 4G

Back Next Request

### c) Configuração da rede LAN do TC CLOUD

VPN Builder | Request VPN configuration (machine: TC CLOUD TX/TX)

1 VPN client (machine) 2 VPN connection 3 Mobile 4 Network 5 Internal network 6 Misc.

DNS configuration (optional) ⓘ  
IP address of DNS server (optional): 8.8.8.8

Configure MTU size ⓘ  
MTU size: 1414

Configuration LAN IP address ⓘ  
☒ Static IP address ☐ Dynamic IP address (DHCP)  
LAN IP address: 192.168.1.1  
Netmask: 255.255.255.0

Internal network:  
e.g. 192.168.1.10  
e.g. 255.255.255.0  
Machine IP address: 192.168.1.XXX

WAN port LAN port

Default gateway: 192.168.1.254

Back Next Request

OPCIONAL - DNS do Google ou o IP do servidor de internet local

IP do porta LAN

IP do roteador de internet

### d) Inserir parâmetros da operadora de dados do chip a ser usado

VPN Builder | Request VPN configuration (machine: TC CLOUD TX/TX)

1 VPN client (machine) 2 VPN connection 3 Mobile 4 Network 5 Internal network 6 Misc.

Please enter the new admin password for the TC Cloud Client

Password: admin Repeat password: admin

Please enter the serial number of the VPN client (optional)

Serial Number:

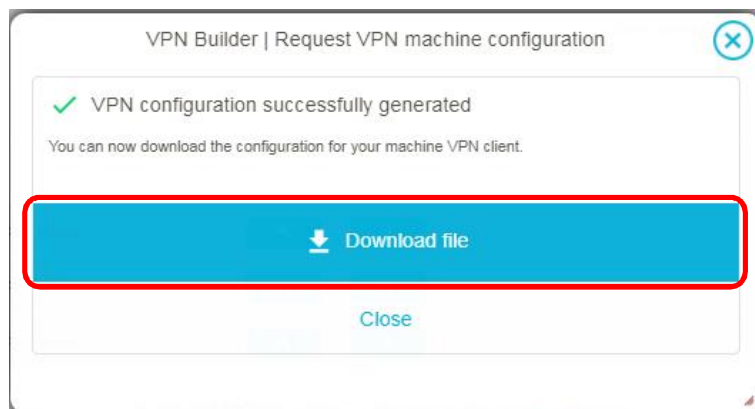
Shall the vpn connection be initiated via a key switch (Service-IO)?

Use key switch: No

Back Next Request

Caso já tenha acessado o browser e alterado manualmente a senha de acesso, basta inserir a nova senha

e) Download do arquivo de configuração realizada




f) Acesse o browser do TC CLOUD e faça upload da configuração feita.









### 3. Configurar a VPN para se conectar ao portal MGUARD SECURE

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

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


Active VPNs **All Service Workstations** 

Workstations

1	Iphone	No user	not connected	VPN: <b>offline</b>			
---	--------	---------	---------------	---------------------	---	---	---

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice

#### a) Criar uma nova configuração de VPN

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

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

Active VPNs **All Service Workstations** 

Add new service workstation

Eletrofair \*

Note

\* = Mandatory field


Cancel **OK**

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice






#### b) Editar parâmetros da nova VPN criada

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

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

Active VPNs **All Service Workstations** 

Workstations

1	Eletrofair	No user	not connected	VPN: <b>offline</b>			
2	Iphone	No user	not connected	VPN: <b>offline</b>			

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice

c) Editar parâmetros da nova VPN criada

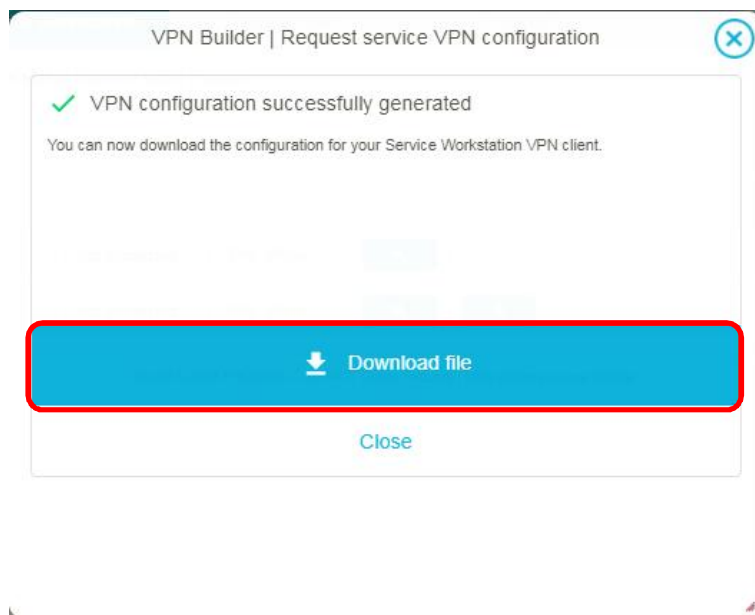
The screenshot shows the 'VPN client type' step in the 'VPN Builder | Request VPN configuration (service: Eletrofair)' interface. The progress bar at the top indicates three steps: '1 VPN client type' (highlighted with a red box), '2 VPN connection', and '3 Machine network'. The main content area is titled 'VPN client type' and contains a section 'Choose a VPN client type' with five radio button options. The second option, 'Shrew Soft VPN Client (free software client w/o vendor support)', is selected and highlighted with a red box. Below this, there is a section 'Please enter the client password:' with two input fields: 'Password: \*' and 'Repeat password: \*'. Both fields contain the text 'Pxc@123456' and are highlighted with a red box. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted with a red box), and 'Request'. A small note at the bottom left states: '\* = Mandatory field' and 'Passwords must be at least 8 characters long and should contain letters, numbers and special characters.'

d) Configurar na mesma faixa de IP em que a máquina remota configurada

e) Gerar o arquivo de configuração realizada

The screenshot shows the 'Machine network' step in the 'VPN Builder | Request VPN configuration (service: Eletrofair)' interface. The progress bar at the top indicates three steps: '1 VPN client type', '2 VPN connection', and '3 Machine network' (highlighted with a red box). The main content area is titled 'Machine network' and contains a text block explaining the purpose: 'Please enter 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.' Below this is a 'Hint' stating: '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'. There are two input fields: 'IP address of the network: \*' with the value '192.168.1.0' and 'Netmask: 255.255.255.0', both highlighted with a red box. To the right of these fields is a diagram showing a router with 'WAN port' and 'LAN port' labels. A box labeled 'Machine network: 192.168.1.0 255.255.255.0' is connected to the LAN port. Another box labeled 'Machine IP address: 192.168.1.XXX' is also shown. At the bottom right, there are three buttons: 'Back', 'Next', and 'Request' (highlighted with a red box). A small note at the bottom left states: '\* = Mandatory field'.

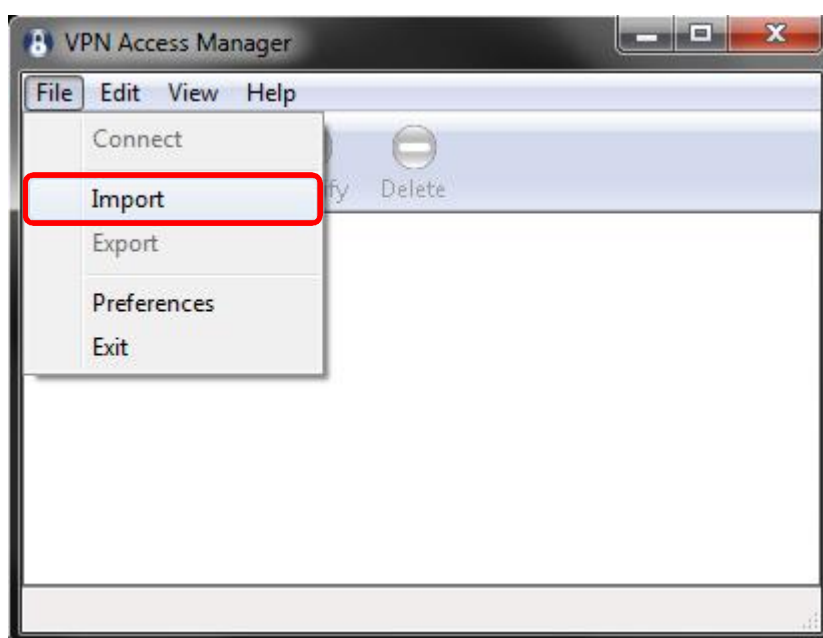
f) Download do arquivo de configuração de VPN realizada



4. Abrir o software Shrew Soft VPN

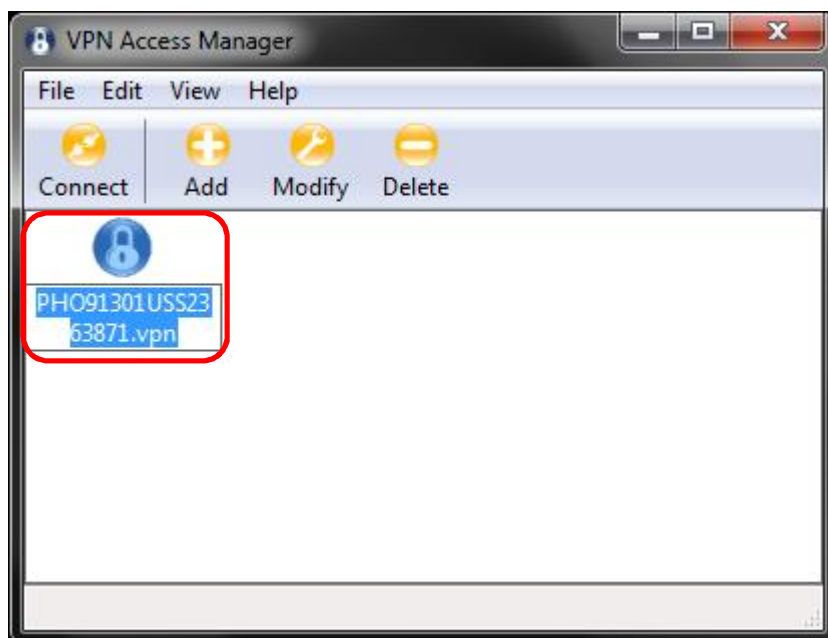


a) Importar a configuração ao discador VPN Shrew Soft VPN

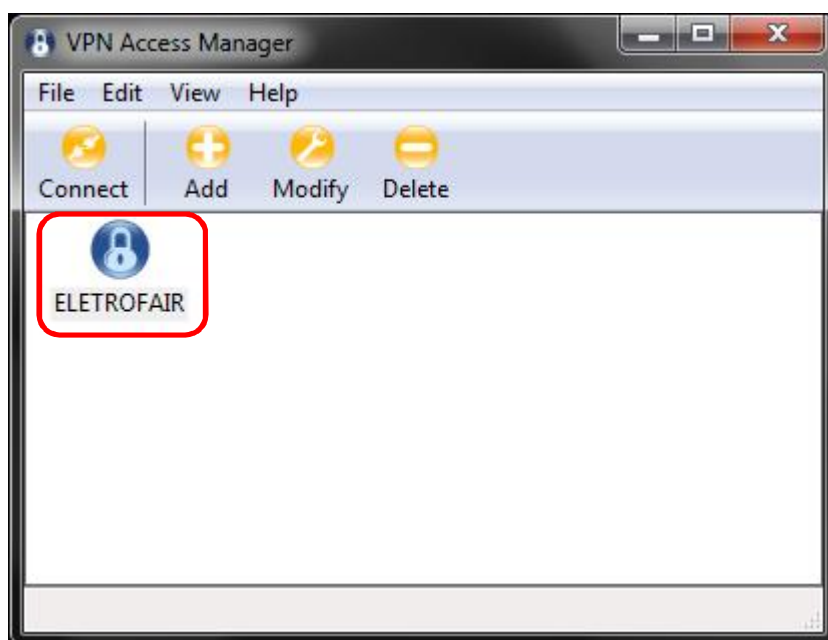




b) Buscar e importar o arquivo de configuração de VPN feito no portal

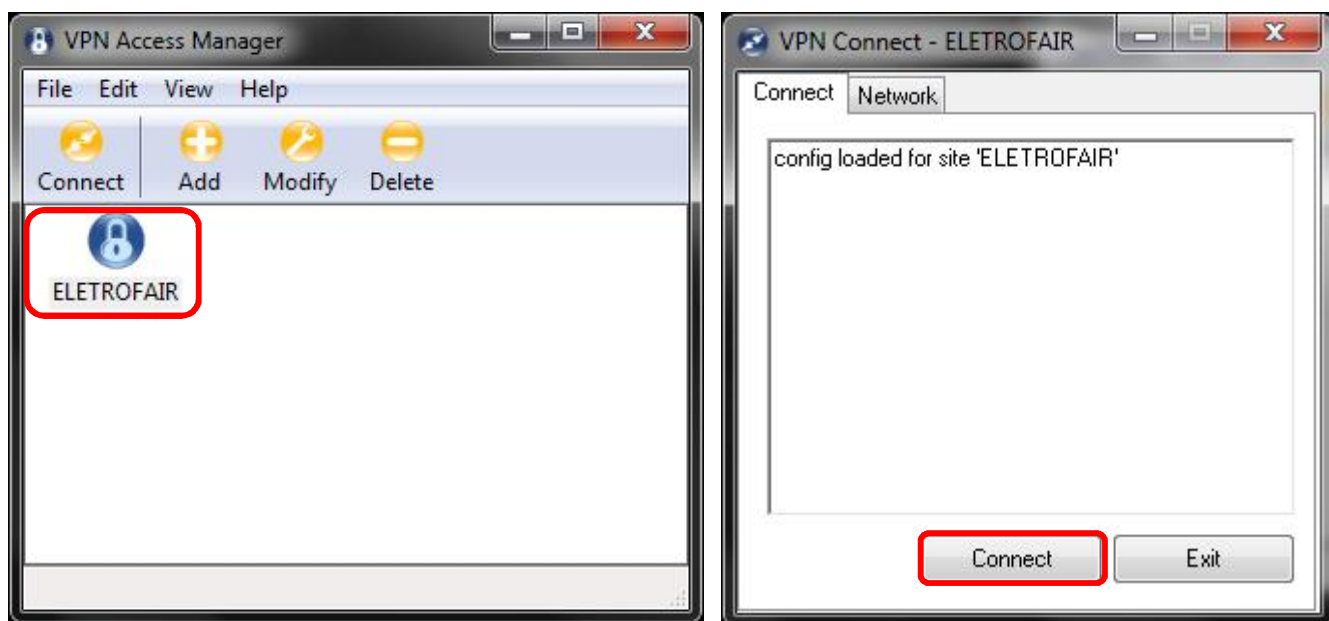


c) Renomei a configuração de VPN de acordo sua preferência

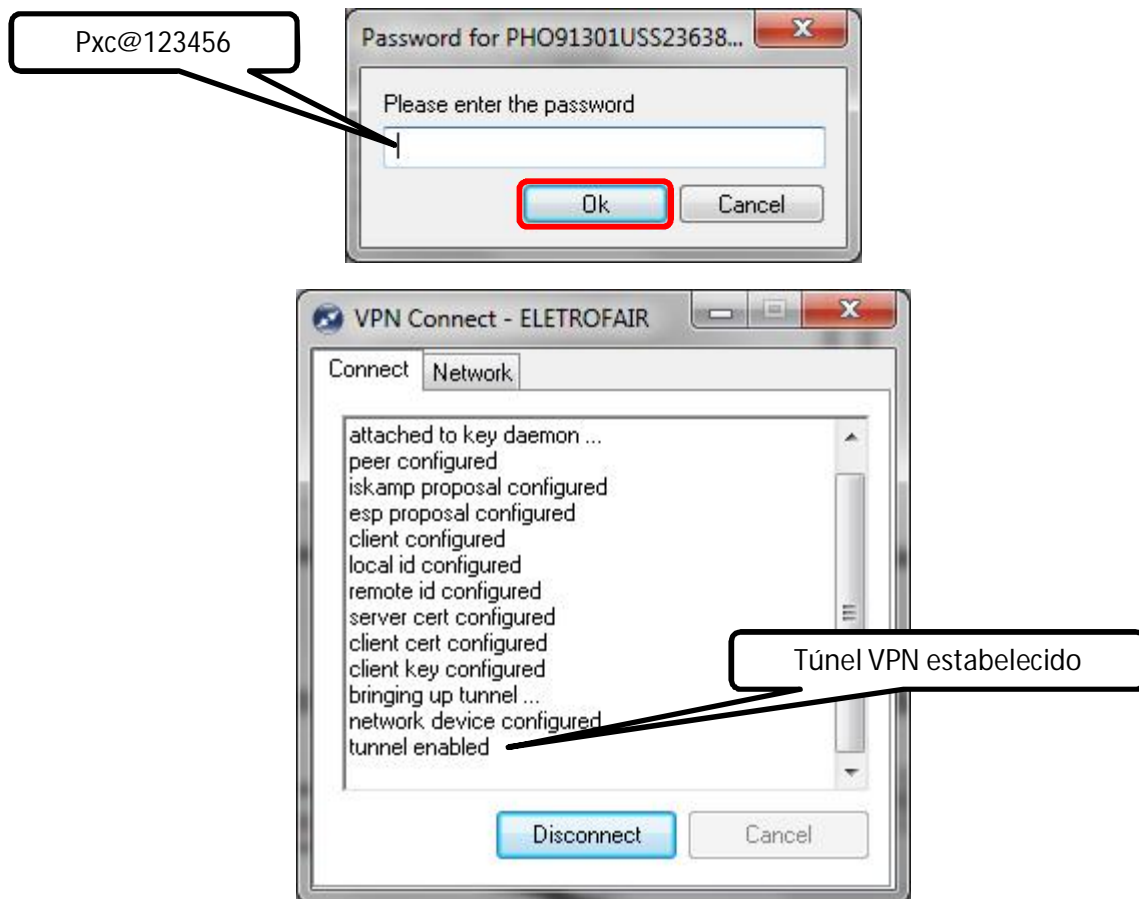


## 5. Conexão VPN com o portal MGUARD SECURE CLOUD

a) Duplo clique na conexão configurada ELETROFAIR em seguida Connect



b) Entre com a mesma senha configurada e em seguida OK



## c) Conexão VPN ao porta MGuard SECURE estabelecida com sucesso









Service VPN tunnel online > No secure connection initiated > No secure remote access to service target (machine)

Active VPNs

All Service Workstations

Workstations

1	Eletrofair	phoenixcontactrs@gmail.com	not connected	VPN: online			
2	Iphone	No user	not connected	VPN: offline			

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice


## 6. Roteamento de VPN até o dispositivo TC CLOUD remoto



Service VPN tunnel online > No secure connection initiated > No secure remote access to service target (machine)

Show operator/locations: All | 0-9 | A-B | C-D | E-F | G-H | I-J | K-L | M-N | O-P | Q-R | S-T | U-V | W-X | Y-Z



Active VPN connections to Service Targets	
All Service Targets (facilities and machines) currently connected with the mGuard Secure Cloud via secure VPN.	
1	PxC_BR   RS2000_3G   SN:   VPN: online 

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice


## a) Conexão VPN entre usuário e MGuard remoto estabelecida com sucesso



Service VPN tunnel online > Secure connection initiated > PxC\_BR / RS2000\_3G

Show operator/locations: All | 0-9 | A-B | C-D | E-F | G-H | I-J | K-L | M-N | O-P | Q-R | S-T | U-V | W-X | Y-Z

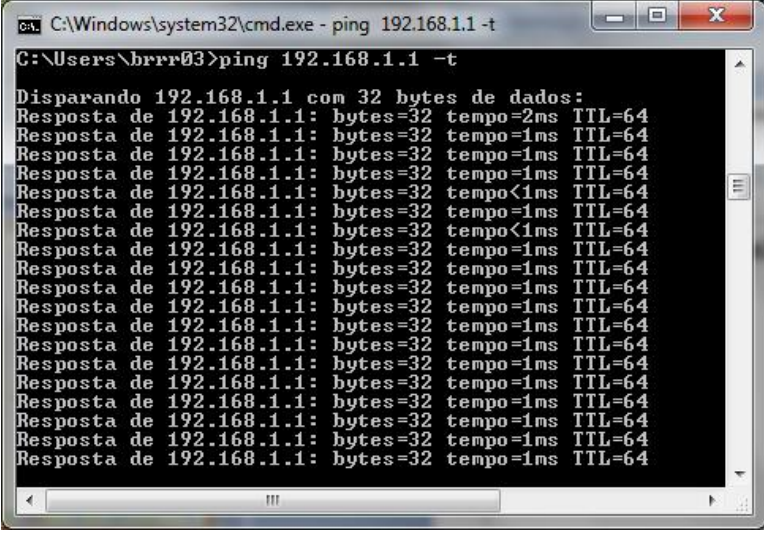


Active VPN connections to Service Targets	
All Service Targets (facilities and machines) currently connected with the mGuard Secure Cloud via secure VPN.	
1	PxC_BR   RS2000_3G   SN:   VPN: online 

© 2011-2016 PHOENIX CONTACT Cyber Security | Data privacy | Legal Notice

## 7. Teste de conexão de com os dispositivos remotos - Ping

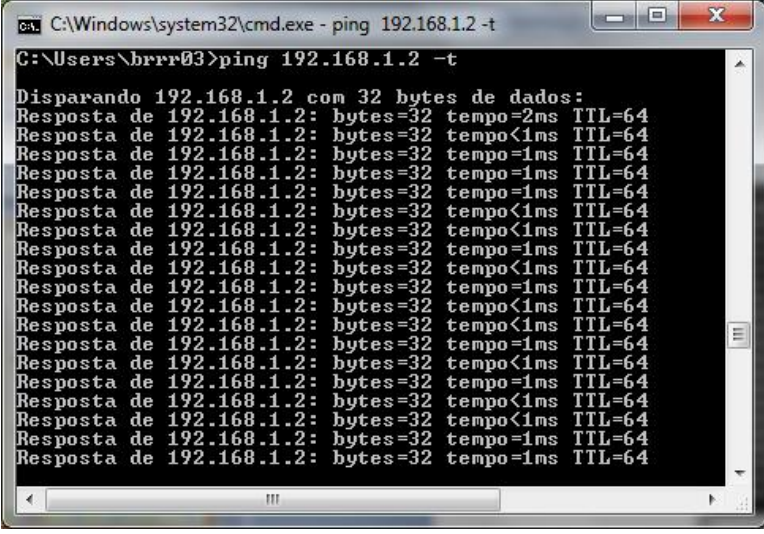
a) Ping (192.168.1.1) no porta LAN do TC CLOUD remoto.



```
C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t
C:\Users\brrr03>ping 192.168.1.1 -t

Disparando 192.168.1.1 com 32 bytes de dados:
Resposta de 192.168.1.1: bytes=32 tempo=2ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.1: bytes=32 tempo=1ms TTL=64
```

b) Ping (192.168.1.2) no CLP remoto conectado na porta LAN do TC CLOUD.

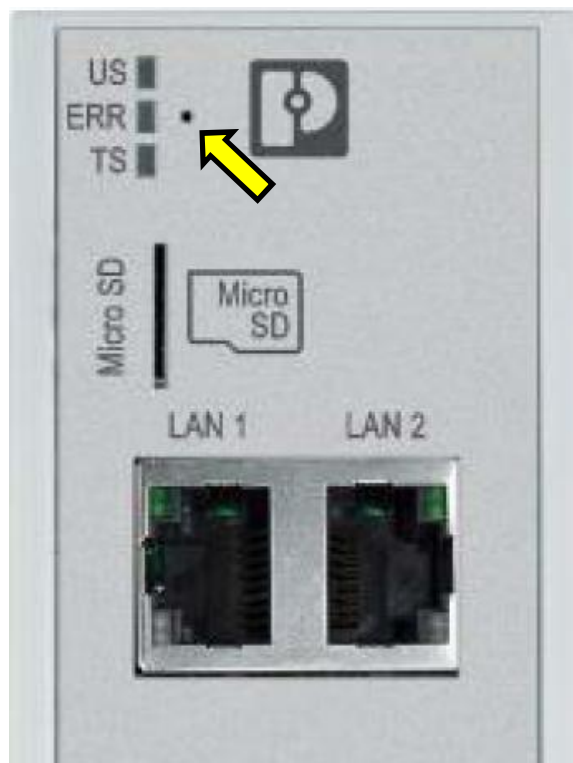


```
C:\Windows\system32\cmd.exe - ping 192.168.1.2 -t
C:\Users\brrr03>ping 192.168.1.2 -t

Disparando 192.168.1.2 com 32 bytes de dados:
Resposta de 192.168.1.2: bytes=32 tempo=2ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
Resposta de 192.168.1.2: bytes=32 tempo=1ms TTL=64
```

## 8. Procedimento de RESET de IP default de fábrica

1. Precione o botão de reset por 6 segundos;
2. Mantendo pressionado o reset, desconecte o cabo LAN;
3. Ainda mantendo pressionado, reconecte o cabo LAN;
4. Aguarde por mais 6 segundos até que os LEDs das portas LAN acendam;
5. O IP padrão restaurado é [192.168.0.1](#)



Obrigado!