

TeamWork – Manual do Utilizador

FortiClient

**para Windows 2000, Windows XP,
Windows Vista e Windows 7**

(32 e 64 bits)

Nota Importante:

Este manual aplica-se apenas a usernames com o formato usxxxx.<VPN>@tmwk.webside.pt.

Se o seu username tem o formato userxxxx.<VPN>@tmwk.webside.pt deverá utilizar um dos manuais relativos ao Contivity VPN Client.

Índice

1. Introdução	4
2. Instalação e Configuração	5
3. Utilização	6
4. Apoio para instalação e configuração. Participação de avarias.	10
5. Anexo 1 – Sequência de instalação	11
6. Anexo 2 – Configuração do FortiClient Endpoint Security	13

1. Introdução

A sua conta TeamWork permite-lhe aceder à VPN nas seguintes condições:

- Utilizando um PC com sistema operativo Windows;
- Com segurança, através de um túnel IPSec;
- A partir de um acesso à Internet, utilizando qualquer ISP em qualquer país.

Nota Importante:

Para poder aceder a partir de um outro ISP que não a PT Prime é necessário que essa rede de acesso à Internet não tenha restrições, nomeadamente que:

- Permita conectividade IP ao concentrador de túnel da PT Prime;
- Não restrinja os seguintes ports / protocolos:
 - ICMP (Internet Control Message Protocol);
 - Port UDP 500 (IKE);
 - Port UDP 4500 (NAT Traversal);
 - IPSec – ESP (protocolo 50);
 - IPSec – AH (protocolo 51).

O Serviço TeamWork distingue duas entidades interessadas:

- O Cliente do Serviço TeamWork;
- O Utilizador do Serviço TeamWork.

O Cliente TeamWork poderá solicitar à PT Prime a activação das seguintes funcionalidades adicionais:

- Restrição do acesso dos Utilizadores TeamWork a alguns servidores e a alguns serviços da sua VPN;
- Restrição da possibilidade de os Utilizadores TeamWork acederem a endereços IP da gama pública.

2. Instalação e Configuração

O TeamWork utiliza o agente FortiClient Endpoint Security para estabelecer um túnel IPSec entre o seu PC e a sua VPN.

Para utilizar o serviço TeamWork deverá realizar previamente as seguintes tarefas:

- Instalar no seu PC o Software FortiClient, executando o ficheiro FortiClient_32.msi (Windows de 32 bits) ou FortiClient_64.msi (Windows de 64 bits). Poderá obter este SW a partir do site <http://www.ptempresas.pt>;
- No Anexo 1 é apresentada a sequência de ecrãs que deverão ocorrer durante a instalação;
- Configurar o FortiClient Endpoint Security de acordo com o Anexo 2.

A PT Prime fornecerá a seguinte informação relativa ao serviço TeamWork.

- **Username / Password** para cada Utilizador. O formato do username é o seguinte: usxxxx<Nome_VDOM>@tmwk.webside.pt;
- **Endereço IP do Remote Gateway**, específico de cada VPN. É o mesmo para todos os Utilizadores das contas de acesso a essa VPN;
- **Endereço IP atribuído ao terminal do Utilizador**. Este IP é fixo e, por defeito, pertencerá à gama 10.57.0.0/16. Se necessário, poderá ser definida outra gama de endereços. Para isso, deverá contactar com o seu Gestor de Cliente.

Nota Importante:

Antes de instalar o FortiClient deverá desinstalar o anti-vírus que tiver instalado no seu PC.

Depois de ter instalado o FortiClient (apenas a funcionalidade VPN) poderá instalar novamente o anti-vírus.

No caso do anti-vírus AVAST poderá ser necessário configurar o browser para utilizar um proxy (Host: localhost / Port: 12080), conforme descrito no Forum e na Knowledge Base :

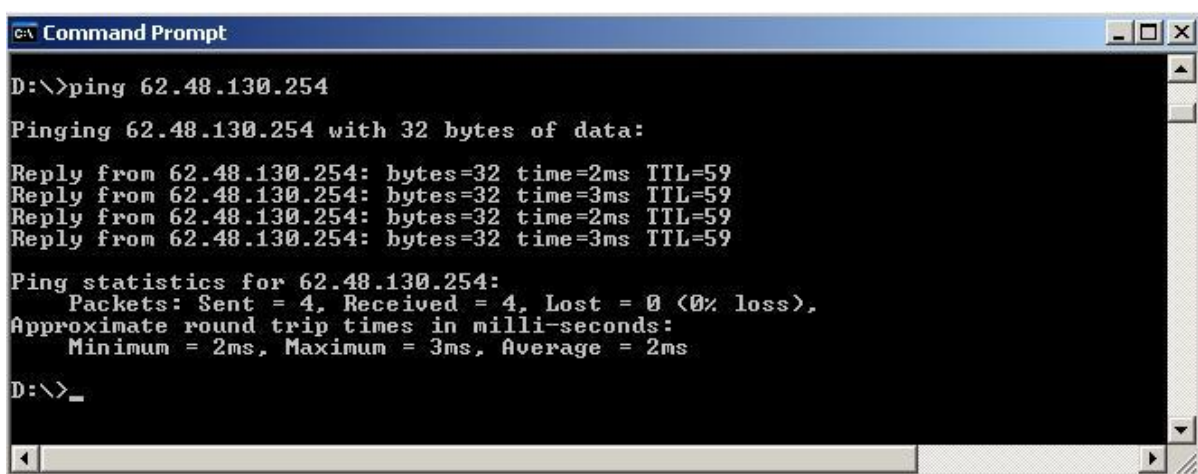
<http://forum.avast.com/index.php?topic=58544.0>

<http://support.avast.com/index.php? m=knowledgebase& a=viewarticle&kbarticleid=22>

3. Utilização

Depois de o FortiClient Endpoint Security estar instalado e configurado no seu PC pode utilizar o serviço TeamWork da seguinte forma:

- Verificar se há conectividade desde o seu PC até ao concentrador de túneis IPsec da PT Prime, executando na linha de comando o ping para o Endereço IP do Remote Gateway da sua VPN. Este endereço, **único por VPN**, será comunicado pela PT Prime ao Cliente após a criação do primeiro acesso TeamWork;



```

C:\> Command Prompt
D:\>ping 62.48.130.254

Pinging 62.48.130.254 with 32 bytes of data:

Reply from 62.48.130.254: bytes=32 time=2ms TTL=59
Reply from 62.48.130.254: bytes=32 time=3ms TTL=59
Reply from 62.48.130.254: bytes=32 time=2ms TTL=59
Reply from 62.48.130.254: bytes=32 time=3ms TTL=59

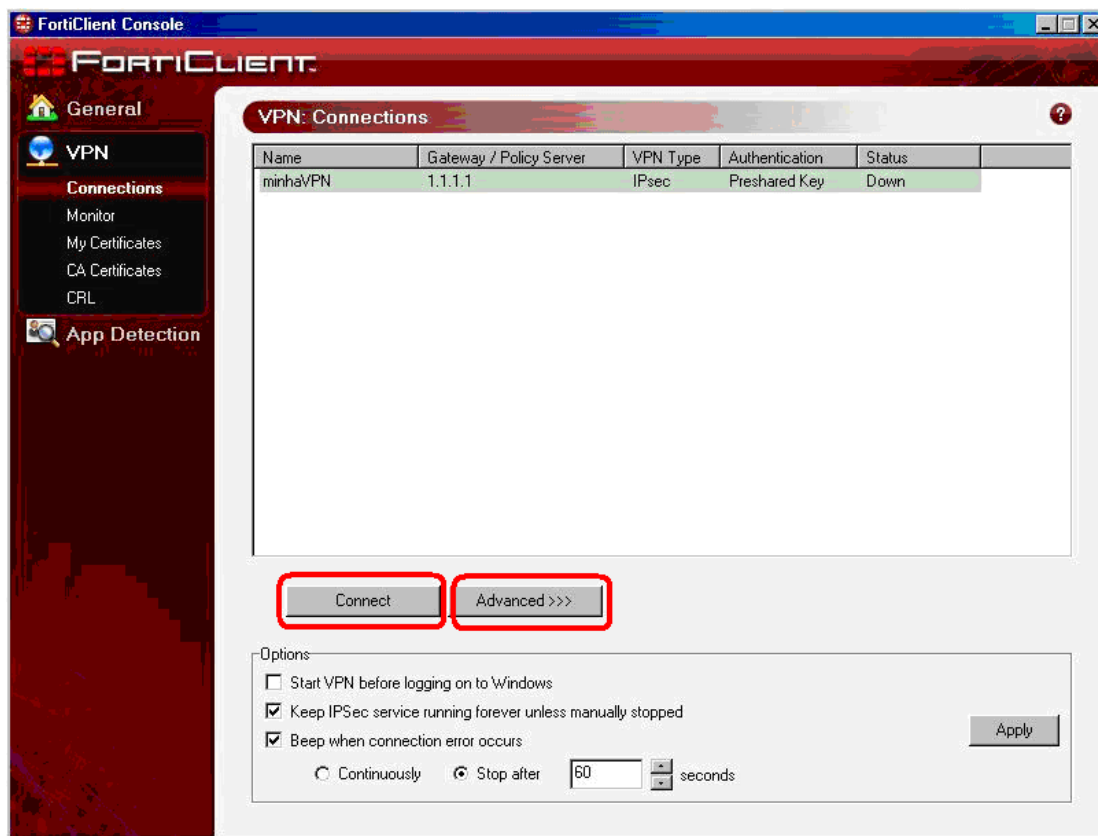
Ping statistics for 62.48.130.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

D:\>_
    
```

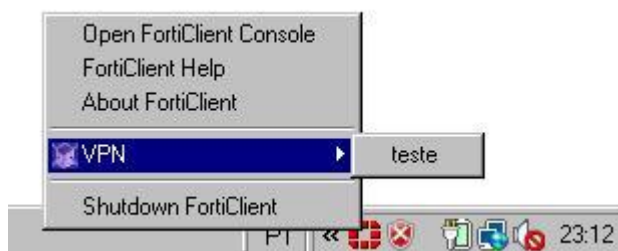
- Executar no seu PC o programa que estabelece o túnel IPsec até à VPN (FortiClient), clicando no seguinte ícone do Ambiente de Trabalho.



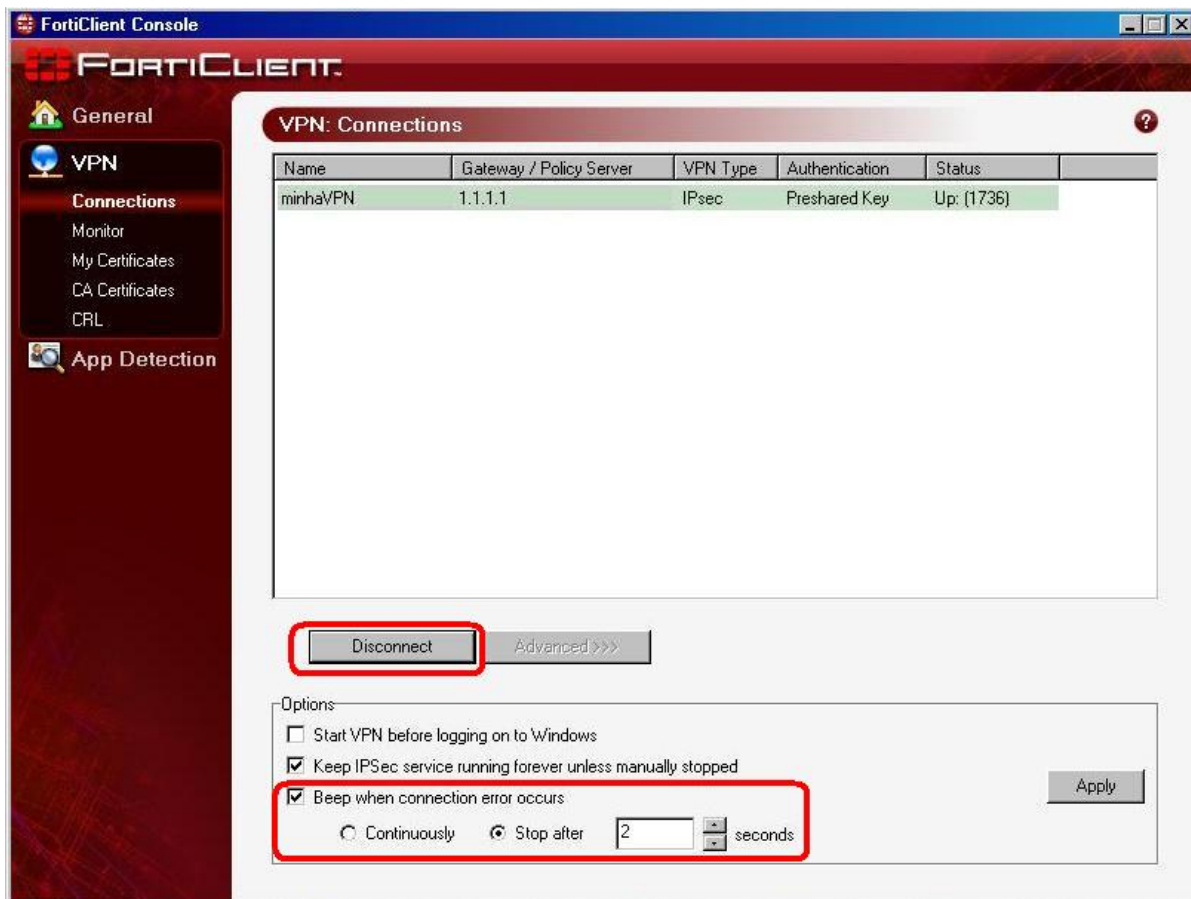
Surgirá depois a Consola FortiClient, onde deverá clicar em **Connect**, para iniciar a ligação à sua VPN. Para alterar a configuração da ligação deverá clicar em **Advanced**.



Poderá seguir no ecrã do seu PC o desenrolar do processo de login, findo o qual surgirá na Área de Notificação da Barra de Tarefas (canto inferior direito) o seguinte ícone:



A Consola do Fortinet passará a indicar o estado de ligação à VPN:



Passará então a poder desligar a ligação à VPN através do botão **Disconnect**.

Nota: Para sua comodidade poderá reduzir a duração do sinal sonoro de erro na ligação que, por defeito, é de 60 segundos.

Pode verificar qual o endereço IP atribuído ao seu PC através do comando **ipconfig /all**.

Para tal, poderá utilizar o botão Start do Windows (canto inferior esquerdo do ecrã):

Run... > cmd > ipconfig /all

```
C:\>ipconfig /all

Ethernet adapter Local Area Connection 5:

    Connection-specific DNS Suffix  . :
    Description . . . . . : Fortinet virtual adapter
    Physical Address. . . . . : 00-09-0F-FE-00-01
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.57.0.4
    Subnet Mask . . . . . : 255.255.255.255
```

Depois de estar ligado à VPN pode comunicar com todos os endereços IP da VPN que não tenham acesso condicionado.

Notas Importantes:

- Se estiver ligado a uma LAN, a configuração do router de acceso à Internet poderá não lhe permitir a utilização do TeamWork. Nesses casos, sugerimos que teste o funcionamento da sua conta TeamWork sobre um acesso directo, por exemplo um acesso dial-up ou 3G. Se o TeamWork funcionar correctamente a solução do problema poderá passar por retirar do router algumas restrições de protocolos ou ports ou desactivar a funcionalidade IPSEC ALG (IPSec Transparent). Para o fazer, terá de ter privilégios de administração do router;
- Em caso de dúvida ou persistência do problema deverá contactar a PT Prime – Centro de Suporte a Clientes Empresariais;
- O acesso TeamWork não se desliga automaticamente por time-out em caso de inactividade prolongada durante a sessão;
- Por vezes as interrupções curtas no acesso à Internet podem terminar o túnel IPSec de forma abrupta. Nesses casos a sessão só poderá ser reiniciada após uma espera de 180 segundos;
- O TeamWork está vocacionado para permitir o acesso a VPNs com endereços IP internos da gama privada (10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16). No caso de a sua VPN utilizar internamente endereços públicos deverá informar o seu Gestor de Cliente a fim de o serviço TeamWork ser adequadamente configurado, se tal for possível;
- A mesma conta TeamWork não pode estar activa simultaneamente em dois ou mais PCs.

4. Apoio para instalação e configuração. Participação de avarias.

Poderá participar avarias ou solicitar apoio para a instalação e configuração do serviço TeamWork telefonando para o CSC – Centro de Suporte a Clientes Empresariais. O CSC registará e encaminhará a situação para um departamento técnico, o qual dará continuidade ao processo, contactando-o telefonicamente mais tarde.

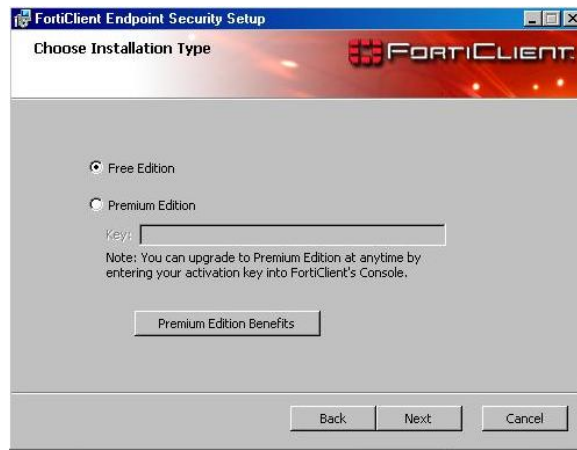
Ao entrar em contacto com o Centro de Suporte a Clientes Empresariais deverá estar preparado para comunicar o username da sua conta TeamWork, descrever o problema e indicar o número telefónico para onde a equipa técnica de suporte o deverá contactar.

Por razões de segurança, o Centro de Suporte a Clientes Empresariais não está autorizado a alterar ou emitir 2^{as} vias de passwords, bem como a alterar/atribuir perfis de utilizador ou endereços IP. Esses serviços deverão ser solicitados ao seu Gestor de Cliente na PT Prime.

5. Anexo 1 – Sequência de instalação



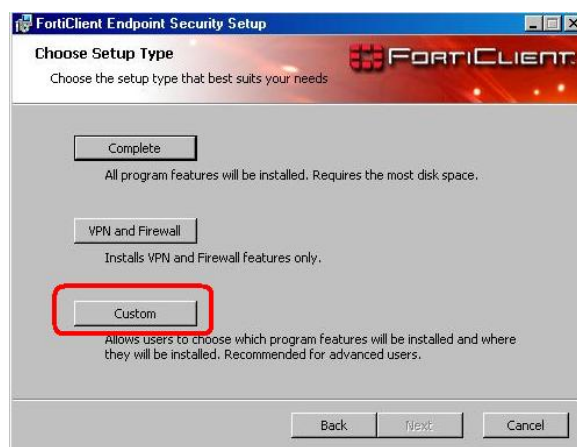
Anexo 1 – Fig. 1



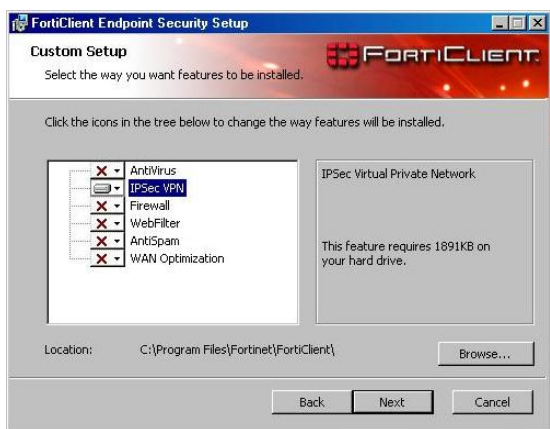
Anexo 1 – Fig. 2



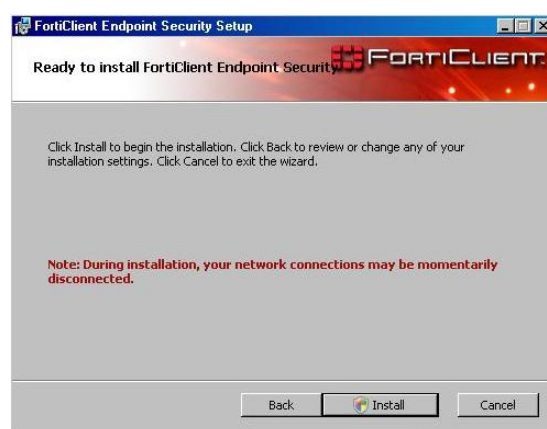
Anexo 1 – Fig. 3



Anexo 1 – Fig.4

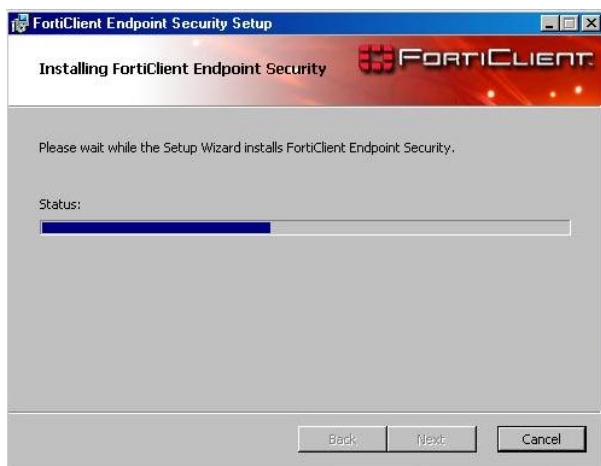


Anexo 1 – Fig. 5

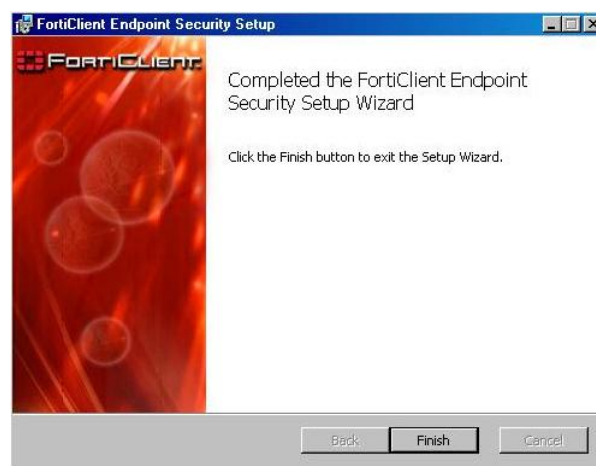


Anexo 1 – Fig.6

(Seleccionar só a funcionalidade IPSec VPN)



Anexo 1 – Fig. 7



Anexo 1 – Fig. 8

6. Anexo 2 – Configuração do FortiClient Endpoint Security

Antes de utilizar o FortiClient Endpoint Security tem de o configurar, definindo nomeadamente:

User Name

O formato do Username é o seguinte: usxxx.<Nome_VDOM>@tmwk.webside.pt .

<VDM> – nome do VDOM da VPN, à qual a conta TeamWork permite o acesso. O VDOM é a entidade na VPN que faz a interligação segura à Internet.

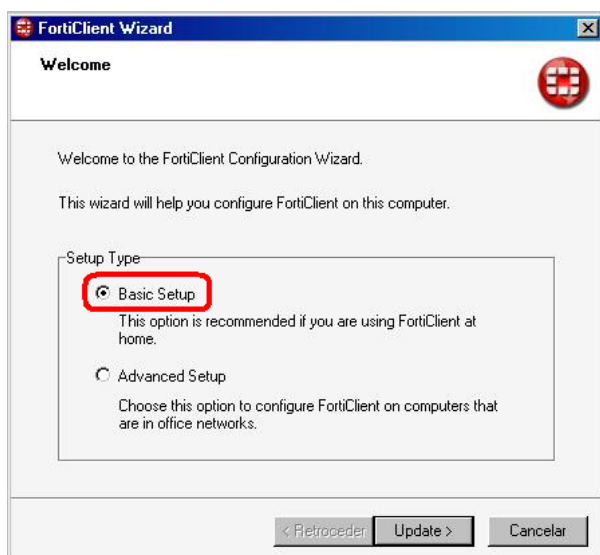
xxx – Sequência numérica entre 0001 e 9999

Password

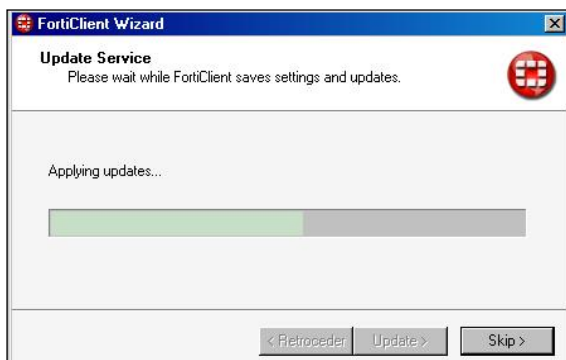
1. **Preshared Key:** É sempre **ipsec**)
2. **Remote Gateway:** Endereço IP do Remote Gateway, específico de cada VPN.

Cada conta deverá ter um nome, a ser atribuído livremente pelo utilizador.

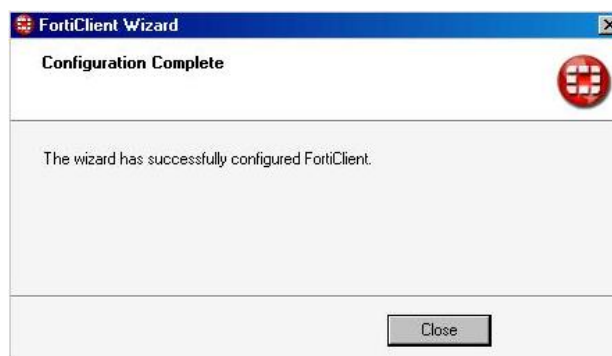
Nas figuras seguintes indica-se onde deve efectuar a configuração.



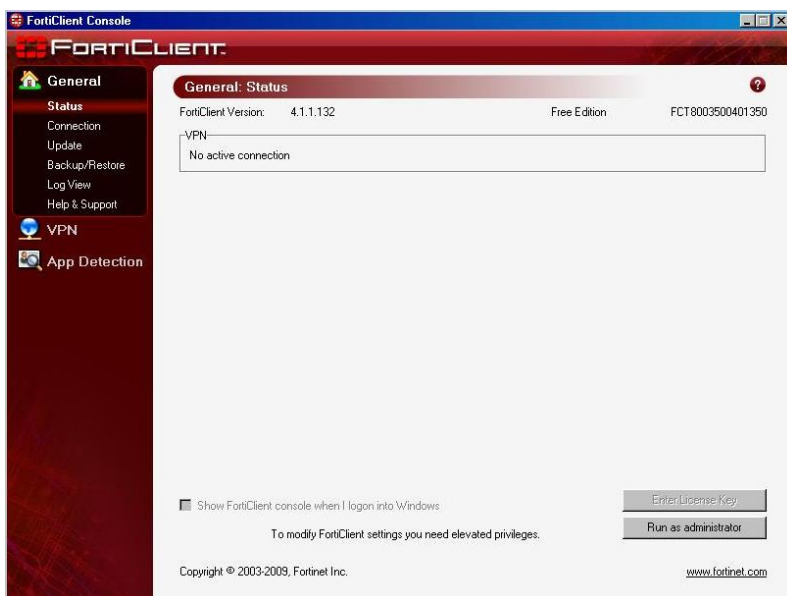
Anexo 2 – Fig. 1
Seleccionar o Advanced Setup apenas se pretender aceder a partir de uma LAN.



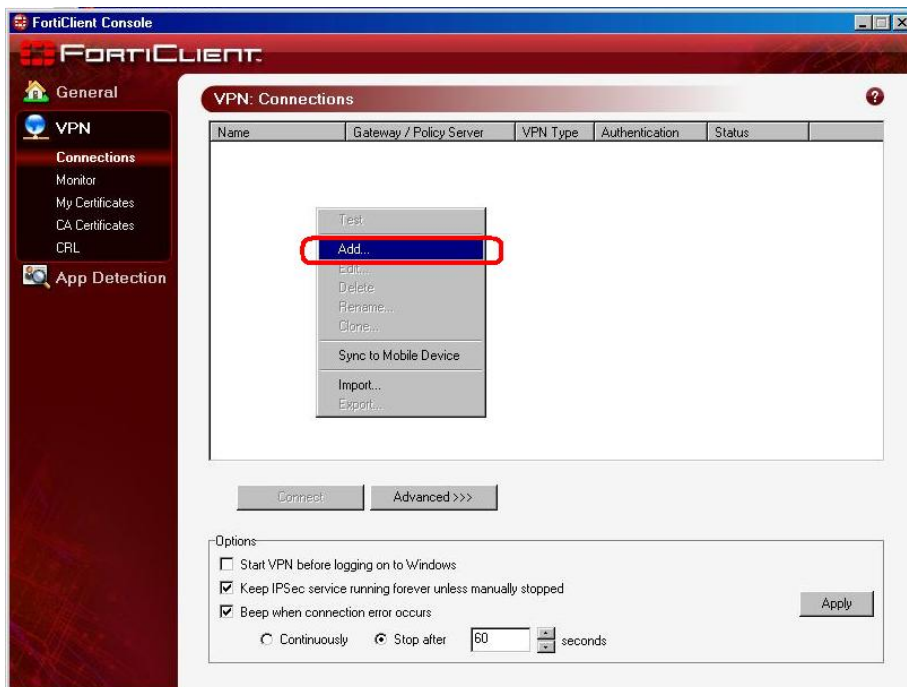
Anexo 2 – Fig. 2



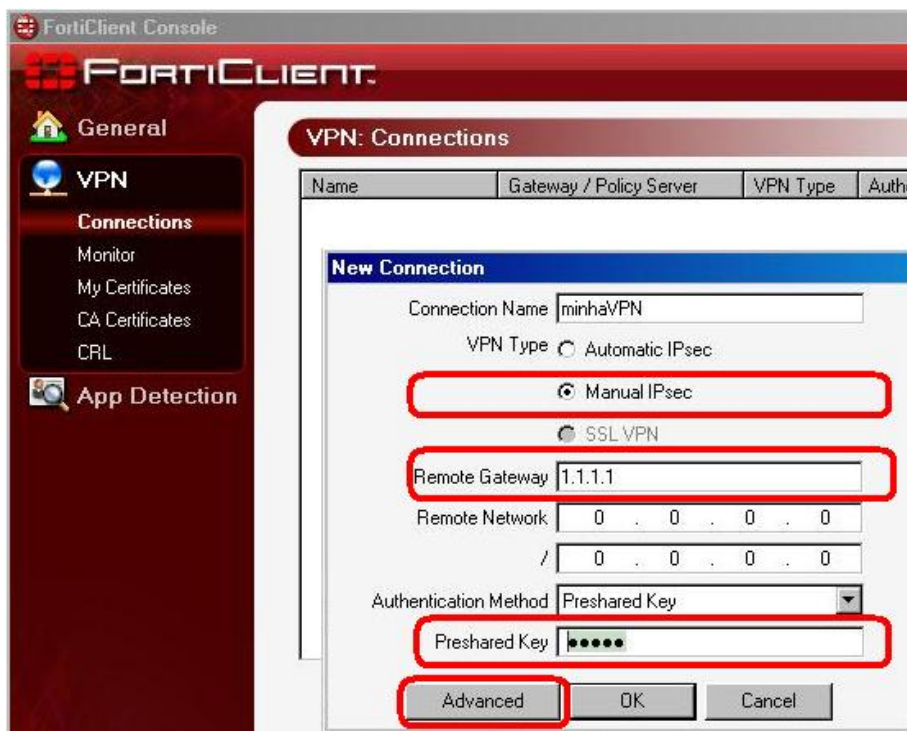
Anexo 2 – Fig. 3



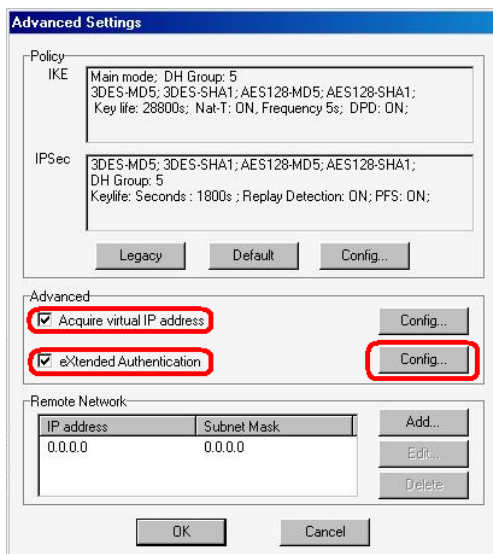
Anexo 2 – Fig. 4
Consola FortiClient.



Anexo 2 – Fig. 5
Para configurar o acesso a uma VPN coloque o cursor na área de trabalho indicada e clique no botão direito do rato. Escolha a opção “Add”.

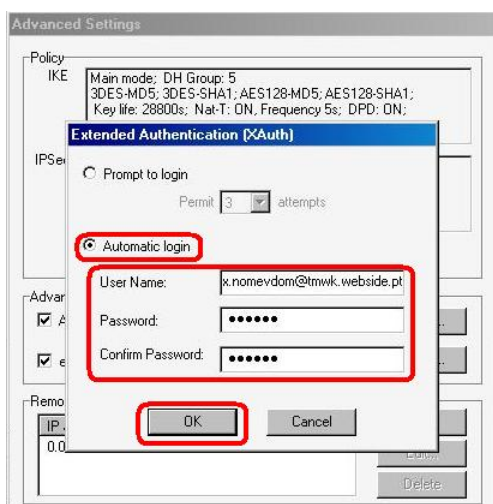


Anexo 2 – Fig. 6
1. Selecciona a opção **Manual IPsec**
2. Inscreva o IP do Remote Gateway.
3. Inscreva a Preshared Key: **ipsec**
4. Clique “Advanced”



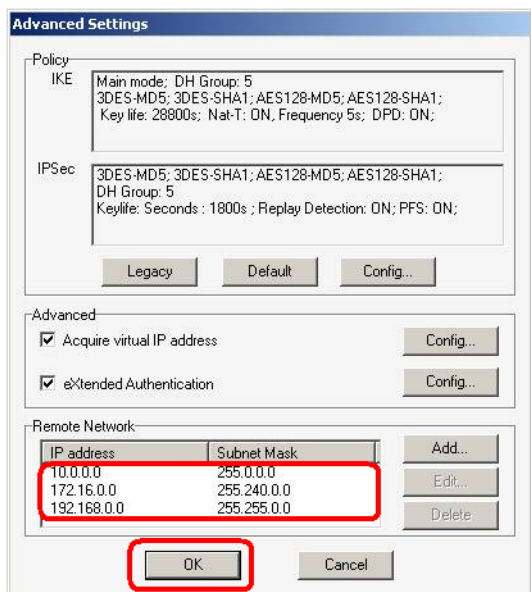
Anexo 2 – Fig. 7

1. Selecione a opção **Acquire Virtual IP Address**
2. Selecione a opção **Extended Authentication** e clique o respectivo botão Config



Anexo 2 – Fig. 8

1. Selecione a opção **Automatic login**
2. Inscreva o **Username** e a **Password** da sua conta TeamWork
3. Clique no botão **OK**

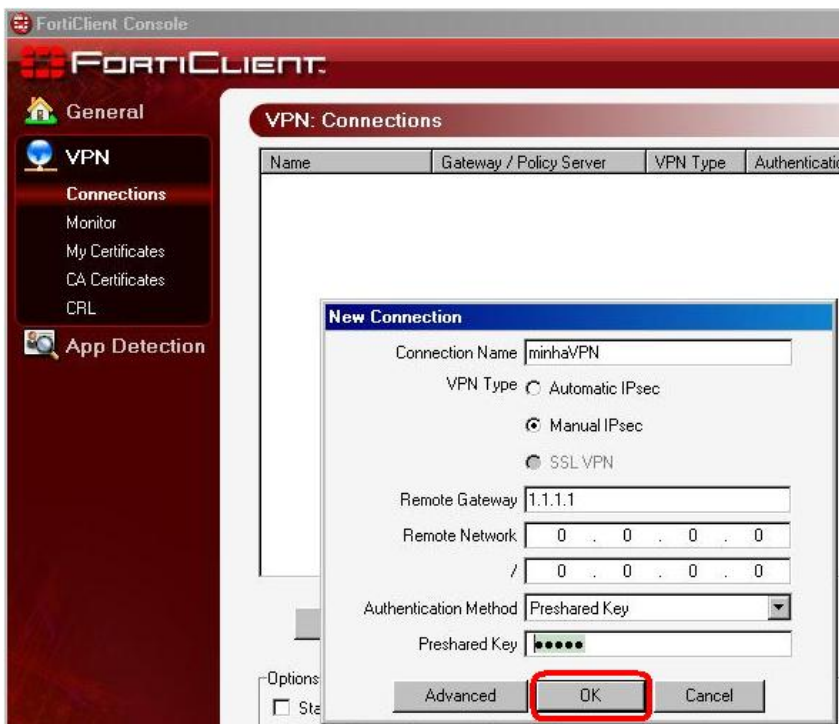


Anexo 2 – Fig. 9

1. Adicione os seguintes Remote Network:

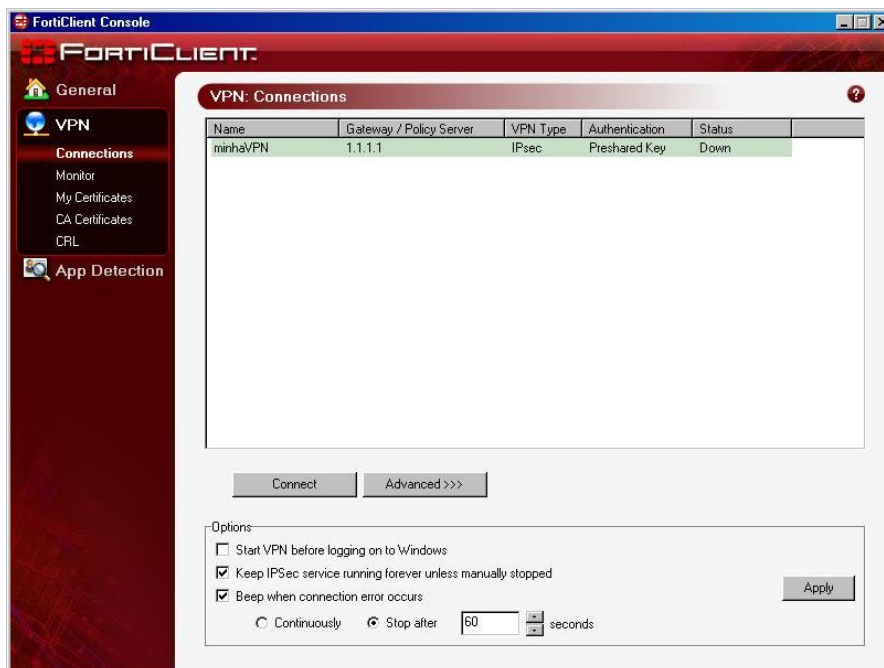
IP Address	Subnet Mask
10.0.0.0	255.0.0.0
172.16.0.0	255.240.0.0
192.168.0.0	255.255.0.0

2. Clique no botão OK



Anexo 2 – Fig. 10

1. Clique no botão OK



Anexo 2 – Fig. 11
A VPN está pronta a ser acedida.

1. Para iniciar a ligação seleccione a VPN e clique em **Connect**