



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 <u>usxxxx.<VPN>@tmwk.webside.pt.</u> Se o seu username tem o formato <u>userxxxx.<VPN>@tmwk.webside.pt</u> 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 é necessário que essa rede de acesso à Internet não tenha restrições, nomeadamente que:

- Permita conectividade IP ao concentrador de túnel da PT;
- 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 Empresas a ativação 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 Empresas 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 antivírus que tiver instalado no seu PC.

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

No caso do antivírus 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 Empresas, 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 Empresas ao Cliente após a criação do primeiro acesso TeamWork;



• 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**.





General	VPN: Connec	tions				
VPN	Name	Gateway / Policy Server	VFN Type	Authentication	Status	
Connections Monitor My Certificates CA Certificates CPI	minhaVPN	1111	IPsec	Preshared Key	Down	
	Connec	* 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:

Open FortiClient Console FortiClient Help About FortiClient	
VPN 🕨	teste
Shutdown FortiClient	





FortiClient Console						
FORTIC	LIENT					a state
General	VPN: Connec	ctions				0
VPN	Name	Gateway / Policy Server	VPN Type	Authentication	Status	
Connections Monitor My Certificates CA Certificates CRL	minina//PN	1.1.1.1	IPsec	Pieshared Key	Up: (1736)	
	Discorr	ect				
	Dptions Start VPN bet Keep IPSec s	fore logging on to Windows service tunning forever unless manu	ally stopped			
	Beep when c	onnection error occurs	- 141	٦		Apply

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

Manual do Utilizador para Windows

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 aceso à Internet poderá não lhe permitir a utilização do TeamWork. Nesses casos, sugerimos que teste o funcionamento da sua conta TeamWork sobre um acesso direto, por exemplo um acesso dial-up ou 3G. Se o TeamWork funcionar corretamente a solução do problema poderá passar por retirar do router algumas restrições de protocolos ou ports ou desativar 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 Empresas Centro de Suporte a Clientes Empresariais;
- O acesso TeamWork não se desliga automaticamente por time-out em caso de inatividade 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 <u>internos</u> 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 <u>internamente</u> endereços públicos deverá informar o seu Gestor de Cliente a fim de o serviço TeamWork ser adequadamente configurado, <u>se tal for possível</u>;
- A mesma conta TeamWork não pode estar ativa <u>simultaneamente</u> em dois ou mais PCs.



Manual do Utilizador para Windows

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 <u>username</u> 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 2ªs vias de passwords, bem como a alterar/atribuir perfis de utilizador ou endereços IP. Esses serviços deverão ser solicitados ao seu Gestor de Cliente da PT Empresas.



5. Anexo 1 – Sequência de instalação



(Selecionar só a funcionalidade IPSec VPN)

Anexo 1 – Fig.6





Manual do Utilizador para Windows



Anexo 1 – Fig.7

Anexo 1 – Fig.8



Manual do Utilizador para Windows

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: usxxxx.<Nome_VDOM>@tmwk.webside.pt .

<VDOM> – 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.

xxxx – 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 efetuar a configuração.

FortiClient Wizard	
Welcome	
Welcome to the FortiClient Configuration Wizard.	
This wizard will help you configure FortiClient on this computer.	
Setup Type	1
C Basic Setup	
This option is recommended if you are using FortiClient at home.	
C Advanced Setup	
Choose this option to configure FortiClient on computers th are in office networks.	iat
	-

Anexo 2 – Fig. 1

Selecionar o Advanced Setup apenas se pretender aceder a partir de uma LAN.





Manual do Utilizador para Windows

Please	wait while F	ortiClient s	aves sett	ings and s	ipdates.		•
Applying u	pdates						
1							
			CRe	noceder	Update	21	Skip >

FortiClient Wizard	×
Configuration Complete	
The wizard has successfully configured FortiClient.	
	_





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".

General	VPN: Conne	ctions								
VPN	Name	Gatew	vay / Po	ácy S	lerve	í.	V	PN Ty	pe	Auth
Connections Monitor My Certificates CA Certificates	New Conne Con	ation nection Name	minha	/PN						J.
CRL App Detection	C	vrn type	C Auto	omati nual I 	c IPs Psec I	ec		_	_	כ
	Rer	note Gateway	1.1.1.1							
	Re	mote Network	0	*:	0	141	0		0	-
		1	0	÷.	0	(6)	0		0	1
	Authentic	cation Method	Presha	red K	ley				*	L
	E F	Preshared Key		•						

Anexo 2 – Fig. 6

- 1. Selecione a opção Manual IPSec
- Inscreva o IP do Remote Gateway.
- Inscreva a Preshared Key: ipsec
- 4. Clique "Advanced"

	۱
\mathbf{O}	
DT	I
	I

IKE	Main mode; E 3DES-MD5: 3 Key life: 2880	DH Group: 5 3DES-SHA1:AES128-MD9 30s;Nat-T:ON,Frequenc	5: AES128-SHA1: y 5s; DPD: ON;
PSec	3DES-MD5: 3 DH Group: 5 Keylife: Secor	DES-SHA1; AES128-MD nds : 1800s ; Replay Dete	5; AES128-SHA1; ction: ON; PFS: ON;
	-		
	Legacy	Default	Config
dvance Z Acc	Legacy d	Default	Config Config
ivance Z Acc Z eX	Legacy ed quire virtual IP a ended Authentic	ddress cation	Config Config.
dvance V Acc V ext emote	Legacy ed une vitual IP a ended Authentic Network	ddress cation	Config
dvance ▼ Acc ▼ ei0 emote IP ad	Legacy ad aute vitual IP a ended Authentic Network dress	ddiess cation Subnet Mask	Config Config Config Add
dvance Acc emote IP ad 0.0.0	Legacy ed puise vistual IP a ended Authentio Network dress 0	ddress cation Submet Mask 0.0.0	Config

Anexo 2 – Fig. 7

- 1. Selecione a opção Acquire Virtual IP Address
- Selecione a opção Extended
 Authentication e clique o respetivo botão
 Config

E	stended Authentic	ation (XAuth)
PSe	C Prompt to login	
	Pem	it 3 🗷 altempts
(Automatic login	
dvar	User Name:	k nomevdom@tmwk.webside.pt
₹ ¢	Password	
7 e	Confirm Password	
	1. Contract (1. Contract)	

Anexo 2 – Fig. 8

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





Manual do Utilizador para Windows

ang.	Main mode: DH 3DES-MD5: 3D Key life: 28800:	Group: 5 ES-SHA1: AES128-M s: Nat-T: ON, Freque	D5: AES128-SHA ncy 5a: DPD: ON	ML L
PSec	3DES MD5; 3D DH Group: 5 Keylife: Second	ES-SHA1; AES128 M s : 1900s ; Replay De	D5; AES128 SHA Rection: ON; PFS	1; ON;
	Legacy	Default	Config	
dvance	d nine side al IP add			Confin
F 64	ended Authentica	tion	-	Config
Remote	Newbik			
Remote IP ad	dess	Subnet Mask		Add
IP ad	hess 10 6 0 0	Subnet Mask 255.0.0 255.240.0.0	-	Add.

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

and the second se										
General	VPN: Connections									
VPN	Name	Gateway / Policy Server		iver	VPN Type Authen					
Connections										
Monitor										
My Certificates										
CRI										
	New	Connection								
App Detection	Connection Name minhaVPN									
	VPN Type C Automatic IPsec									
	Manual IPsec ■									
		1	C SSLVPN							
		Remote Gateway	11.1.1							
		Remote Network	0	. 0	. 0		0			
		Remote Network	0	. 0	. 0	2	0			
		Remote Network / [0 0 Preshar	. 0 . 0	, 0 , 0	2	0			
	^	Remote Network / [uthentication Method]	0 0 Preshar	, 0 , 0 ed Key	. 0	*	0			

Anexo 2 – Fig. 10

1. Clique no botão OK





Manual do Utilizador para Windows

	VPN: Connec	tions				0
VPN Connections Monitor My Certificates DA Detificates CPL App Detection	Name mental/PN	Goleway / Polcy Server 1.1.1.1	Pase:	Authentication Patchared Key	Stetue Down	
	Larre	et Advanced >>>				

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

 Para iniciar a ligação selecione a VPN e clique.