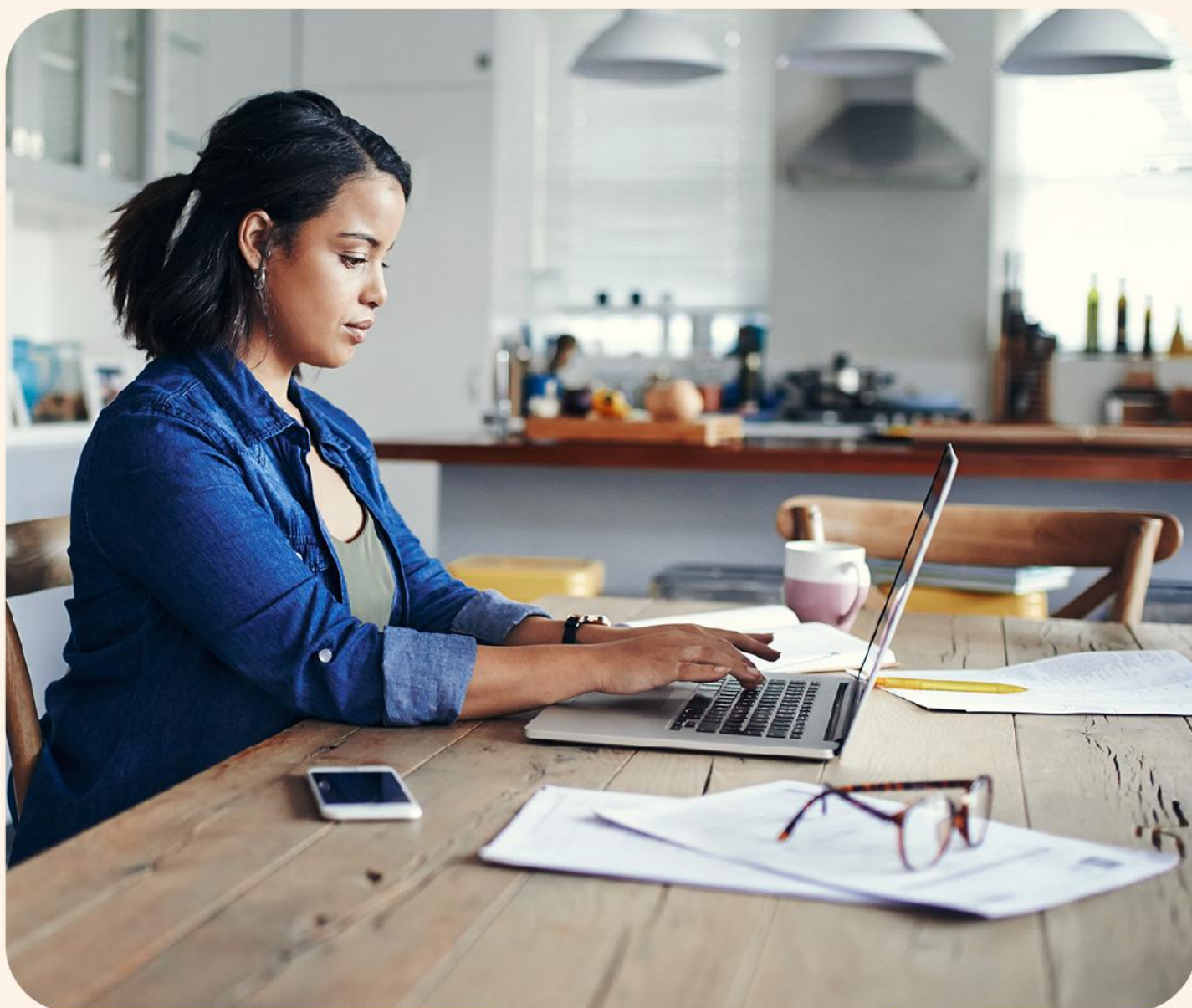


Manual Teamwork - Conectividade Avançada



Índice

1. Breve descrição do serviço	3
Principais funcionalidades do serviço.....	3
Alterações possíveis ao serviço.....	8
2. Preparativos para a instalação do serviço	9
Requisitos de instalação	9
Versões de SW homologadas para funcionamento	10
Versões mais recentes de software.....	10
2.1.1. Software para PCs.....	10
2.1.2. Software para Tablets e Smartphones.....	12
3. Instalação do serviço, configuração e utilização	13
3.1. Windows PC (IPSec e SSL).....	13
3.1.1. Windows PC (IPSec e SSL) - Instalação	14
3.1.2. Windows PC (IPSec e SSL) - Configuração	17
3.1.3. Windows PC (IPSec e SSL) - Utilização.....	22
3.2. MAC OS PC (IPSec e SSL).....	23
3.2.1. MAC OS PC (IPSec e SSL) - Instalação	24
3.2.2. MAC OS PC (IPSec e SSL) - Configuração.....	24
3.2.3. MAC OS PC (IPSec e SSL) - Utilização	25
3.3. LINUX PC (SSL).....	27
3.3.1. LINUX PC (SSL) - Instalação.....	27
3.3.2. LINUX PC (SSL) - Configuração.....	27
3.3.3. LINUX PC (SSL) - Configuração.....	28
3.4. Android Smartphone e Tablet (IPSec e SSL).....	29
3.4.1. Android Smartphone e Tablet (IPSec e SSL) - Instalação.....	29
3.4.2. Android Smartphone e Tablet (IPSec e SSL) - Configuração	31
3.4.3. Android Smartphone e Tablet (IPSec e SSL) - Utilização.....	33
3.5. iOS Smartphone e iOS Tablet (SSL).....	34
3.5.1. iOS Smartphones e iOS Tablet (SSL) - Instalação e configuração.....	35
3.5.2. iOS Smartphone e iOS Tablet (SSL) - Utilização.....	36
4. Apoio técnico	37

1. Breve descrição do serviço

O Teamwork é um serviço de acesso remoto e seguro à rede interna da empresa, a qualquer momento e em qualquer lugar. Permite a partir de múltiplas plataformas (PCs, Tablets ou Smartphones) com acesso à internet, efetuar o acesso remoto de forma segura a todos os recursos IP disponíveis na VPN IP do cliente, através de qualquer protocolo sem restrições de acesso. Esta VPN IP tem de estar suportada na rede empresarial MEO.

O licenciamento deste serviço é por conta. A cada conta são atribuídas credenciais de acesso únicas, que são válidas para os dois métodos alternativos de acesso IPsec e SSL - Tunnel Mode disponibilizados pelo serviço. Em simultâneo só pode ser usado um dos métodos por conta.

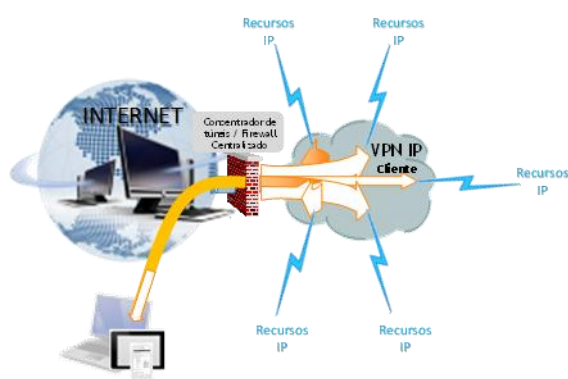
Em qualquer dos métodos de acesso, as comunicações são encriptadas a partir da plataforma utilizada até à VPN IP do cliente, de forma a garantir a confidencialidade dos dados transmitidos.

A instalação do software específico disponibilizado ao nível das plataformas de acesso, é feita pelo cliente de acordo com as instruções disponibilizadas no manual de utilizador. Caso o cliente tenha dificuldades na instalação, configuração e utilização do serviço, poderá entrar em contato com o serviço Pós-Venda. Realçamos que o apoio que o serviço Pós-Venda presta é sempre remoto via suporte telefónico.

Principais funcionalidades do serviço

As principais funcionalidades e características do serviço Teamwork são as que seguem.

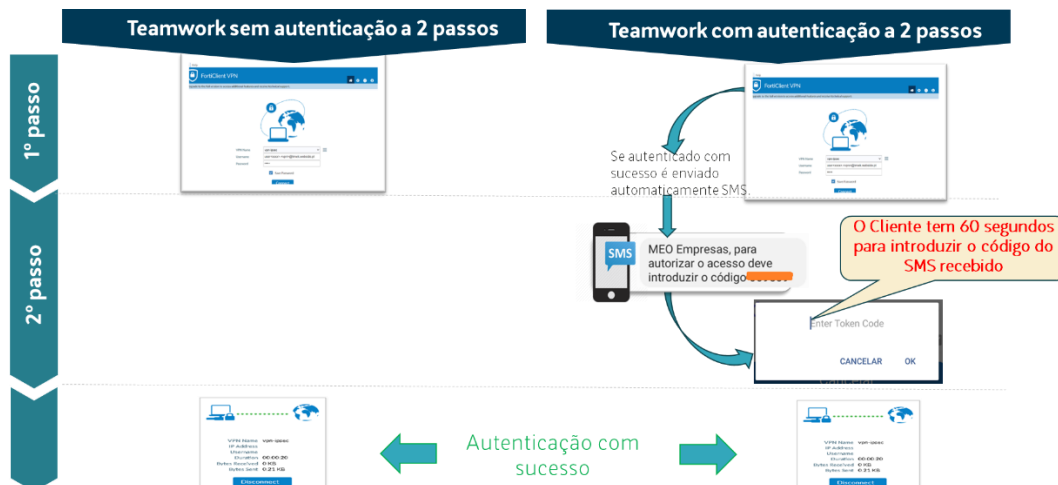
Acesso remoto - Permite a partir de múltiplas plataformas (PCs, Tablets ou Smartphones) com acesso à internet, o acesso remoto seguro a todos os recursos IP disponíveis na VPN IP do cliente, através de qualquer protocolo sem restrições de acesso.



O estabelecimento da comunicação/túnel é sempre iniciado pela plataforma acesso do cliente, ou seja, pelo software do Teamwork. Os PCs, Tablets ou Smartphones podem ter têm acesso à internet com endereço IP fixo ou IP dinâmico público, uma vez que o túnel (a encriptação) é sempre iniciado pelo terminal do utilizador e termina num concentrador de túneis centralizado localizado na infraestrutura MEO que liga à VPN IP do cliente.

Suporte de MFA (Multi Factor Authentication) com recurso a SMS - O Teamwork passou a incluir a possibilidade de ter autenticação MFA (Multi Factor Authentication) que assegure uma credenciação mais robusta com mecanismos de geração de tokens dinâmicos com validade temporal, em adição ao username e password. Neste contexto, o serviço Teamwork acrescenta ao username e password, um token transaccional recebido (código recebido por SMS com validade de 60 segundos).

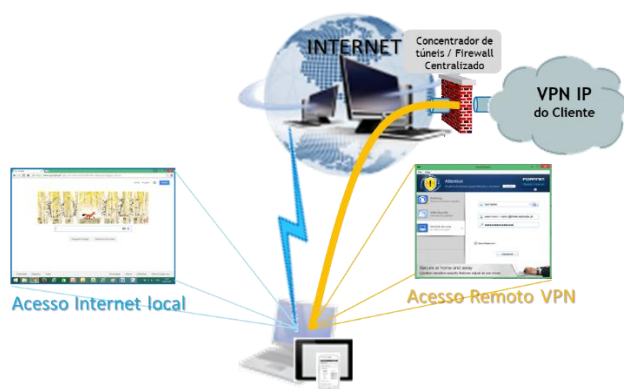
Por cada serviço Teamwork pode escolher se tem autenticação a 2 passos (com MFA) ou não.



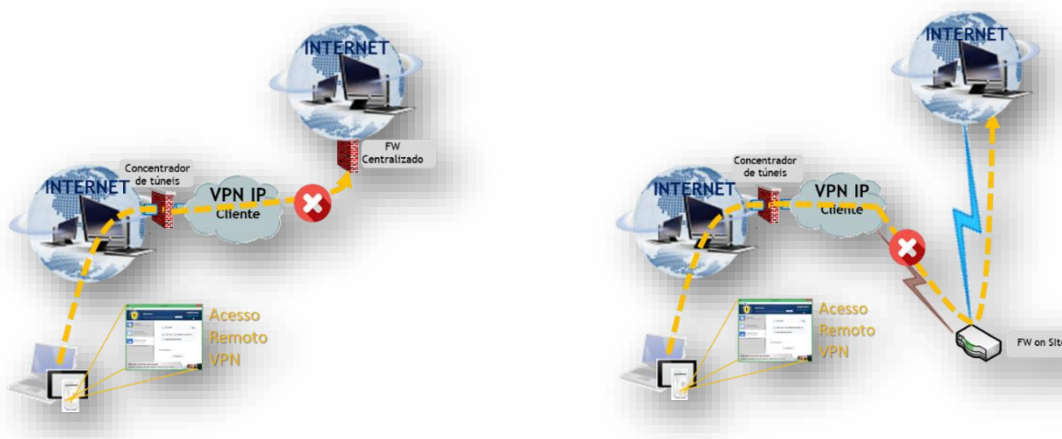
Na adesão ao serviço se não houver indicação explícita para ativar MFA (autenticação a 2 passos), a opção que é ativa por default é a modalidade sem autenticação a 2 passos. Após a ativação do serviço, eventuais migrações entre modalidades com e sem autenticação a 2 passos, requer que sejam aplicadas as condições comerciais em vigor.

A nova funcionalidade de autenticação a 2 passos é suportada no atual software de acesso remoto, não havendo necessidade de novas instalações ou atualizações para quem já tem o serviço. Esta nova funcionalidade é suportada no atual software de acesso remoto, não havendo necessidade de novas instalações ou atualizações para quem já tem o serviço.

Split tunneling - O serviço Teamwork, por default, permite em simultâneo aceder localmente à internet e aceder a recursos IP da VPN IP do cliente.



Caso pretenda que as contas configuradas na sua VPN IP, não possam aceder localmente à internet quando em simultâneo estão ligadas à VPN IP (ou seja, não haja split tunneling), é possível alterar as permissões de acesso para todas as contas (não para apenas para uma parte), através da contratação do opcional de split tunneling referido no ponto dos opcionais. Nota: não é suportado o acesso à internet a partir do serviço Teamwork, através da VPN IP do cliente (cursando o tráfego Internet pela VPN IP do cliente).



Diferentes métodos de acesso - São disponibilizados dois métodos alternativos de acesso IPSec ou SSL - Tunnel Mode, no entanto em simultâneo por cada conta só pode ser usado um dos métodos por conta. Na ativação do serviço Teamwork, o MEO Empresas efetua as parametrizações ao nível do concentrador de túneis para os dois métodos de acesso possíveis. Os dois métodos em causa são:

- O método IPSec: Requer a utilização de software específico para estabelecimento do túnel, fornecido no âmbito do serviço;
- O método SSL – Tunnel Mode: Requer a utilização de um SW específico para estabelecimento do túnel este último fornecido no âmbito do serviço.

Credenciais de acesso por conta - Estas credenciais de acesso são válidas para os dois métodos alternativos de acesso (IPSec ou SSL - Tunnel Mode) disponibilizados pelo serviço. O MEO Empresas, para poder criar o serviço, requer que seja identificado o email e número de telemóvel do utilizador da Empresa para efeitos de envio de credenciais de acesso.

Após a criação de cada conta por parte do MEO Empresas, recebe um email com um URL que identifica univocamente cada serviço. Este URL é protegido com um mecanismo contra bots (mecanismo hcapcha) e recolha de dados de validação adicional. O token (código), que será enviado por SMS, para o telemóvel registado no serviço, terá a validade de 90 segundos, e será solicitado no momento que antecede a consulta da password e outra informação técnica do serviço. Após validação do NIF e token (código), as credenciais de acesso só serão apresentadas uma vez, ficando inutilizado o respetivo URL e token (código). Por questões de segurança, poderá visualizar as credências de acesso apenas uma única vez. Caso o link não devolva a password pela primeira vez, significa que alguém já executou antes dele indevidamente este link uma vez, pelo que deverá entrar em contacto urgente com o MEO Empresas para solicitar alteração de password.

O licenciamento deste serviço é por utilizador, ou seja, a cada utilizador corresponde um serviço Teamwork. A cada serviço são atribuídas as credenciais de acesso únicas constituídas por:

- Endereço IP público do Remote Gateway - Endereço público específico por cada VPN do cliente do terminador de túneis centralizado. Este endereço é o mesmo para todos os serviços de acesso Teamwork à VPN IP de um cliente;
- Pre-shared key ¹ - Palavra usada no estabelecimento do túnel. Esta password é a mesma para todos os serviços de acesso Teamwork à VPN IP de um cliente;
- Username - O formato do username é o seguinte:
usxxx<Nome_VDOM>@tmwk.webside.pt. Cada serviço de acesso Teamwork tem um username diferente;
- Password - A password é alfanumérica com caracteres especiais (password forte). Cada serviço de acesso Teamwork tem uma password diferente. O cliente não pode escolher a password, esta é atribuída automaticamente pelo MEO Empresas;
- Os Usernames e Passwords são definidos pelo MEO Empresas e não podem ser alterados pelo cliente. Caso pretenda nova password pode solicitar novo envio junto do MEO Empresas sem custos adicionais;
- Endereços IP de WAN - Os endereços IPs privados fixos WAN atribuídos ao terminal do utilizador em função se está a usar uma ligação SSL ou uma ligação IPSec, ou seja:
 - Para ligação IPSec - Este IP WAN é fixo e, por defeito, pertencerá à gama 10.57.0.0/16;
 - Para ligação SSL - Este IP WAN é fixo e, por defeito, pertencerá à gama 10.58.0.0/16.

Estes endereços IPs ficam visíveis ao nível da VPN IP do cliente. Caso haja colisão de endereçamento com os endereços IPs presentes na VPN IP do cliente, é possível solicitar junto do MEO Empresas a alteração destes endereços de WAN.

Segurança e confidencialidade nas comunicações - Em qualquer dos métodos os dados são encriptados entre a plataforma de acesso (PC, Tablet ou Smartphone) usada pelo cliente e o concentrador de túneis centralizado localizado na infraestrutura MEO Empresas que liga à VPN IP do cliente, de forma a garantir a confidencialidade dos dados transmitidos.

Suporte de endereçamento - O serviço suporta endereçamento IPv4.

Suporte de múltiplas plataformas de acesso e sistemas operativos - Suporte para PCs, Tablets e Smartphones.

¹ A pré-Shared key não é aplicável ao método de acesso SSL.

		Método IPSec	Método SSL	
Tablet	iPad	✗	✓	Disponível em:  
	Android	✓	✓	
Smartphone	iPhone	✗	✓	Disponível em: https://www.meo.pt/empresas 
	Android	✓	✓	
PC	Windows	✓	✓	
	Mac	✓	✓	
		✗	✓	

Para mais detalhes consultar ponto 2.2 Versões de SW homologadas para funcionamento.

Disponibilização de software específico - Para PCs com sistemas operativos Windows, Linux e Mac OS x, o serviço Teamwork disponibiliza software específico FortiClient no site <https://www.meo.pt/empresas>, que é compatível com o concentrador de túneis do MEO Empresas. Nota: o cliente não deve ir ao site da Fortinet e fazer o download das versões disponibilizadas do FortiClient, pois podem ocorrer problemas de compatibilidade com as plataformas centralizadas que temos disponíveis para assegurar o serviço.

Para Tablets e Smartphones o software é disponibilizado na Google Play Store e na App Store.

O software pode estar instalado em mais que um equipamento, no entanto, só pode ser usado em simultâneo num dos equipamentos por serviço Teamwork.

Nota: o software específico para PCs Windows em versões anteriores podia incluir funcionalidades de segurança adicionais. Realçamos que o software disponibilizado visa apenas o estabelecimento do túnel IPSec ou SSL, no entanto, eventuais funcionalidades adicionais de segurança (Antivírus, Web Security,...) na opção complete de versões anteriores não estão abrangidas pelo serviço comercializado, não tem suporte garantido pelo MEO Empresas e não são garantidas em futuras atualizações de software.

Elevada disponibilidade - O concentrador de túneis localizado na infraestrutura MEO Empresas e a ligação à internet a partir da VPN IP são suportados numa arquitetura redundante o que aumenta a disponibilidade da solução.

Notificações automáticas para o contacto de segurança - Todos os pedidos de operações solicitados ao Order Entry (Backoffice MEO Empresas), quando concluídos geram automaticamente notificação adicional de PDS para o contacto de segurança do cliente. Esta funcionalidade permite um mecanismo adicional de controlo e gestão, permitindo por exemplo detetar atividades não coordenadas entre o utilizador do serviço e o contacto de segurança do cliente, facultando à Empresa total visibilidade sobre as alterações de configuração do serviço.

Possibilidade de alteração de password e preshared key - A password e a preshared key são sempre definidas pelo MEO Empresas. Eventuais necessidades de alteração, terão de ser endereçadas junto do Gestor MEO Empresas.

Revogação a sessão ativa (se existir) em pedidos de alteração - Todos os pedidos de alteração solicitados (alteração de password, alteração de preshared key ou atualizar IP, ativar/desativar MFA) forçam a revogação a sessão ativa (se existir). Esta medida corporiza uma medida de segurança adicional, garantindo que a configuração e início de sessão são feitos estritamente no cumprimento dos requisitos da Empresa.

Suporte técnico - Pode reportar avarias para o CSC - Centro de Suporte a Clientes 24 horas por dia 7 dias por semana. Dificuldades na instalação, configuração e utilização do serviço também poderão ser encaminhadas para esta linha de suporte, no entanto a resposta só é assegurada em horário útil (das 9h às 18h) dos dias úteis. Realçamos que o apoio que o CSC presta é sempre remoto via suporte telefónico.

Nota: alterações de password tem de ser solicitadas via Gestor MEO Empresas por questões de segurança.

Alterações possíveis ao serviço

Encontram-se disponíveis as seguintes alterações possíveis ao serviço:

Tipo de alteração	Descrição
Alteração para autenticação com MFA (a 2 passos)	Possibilidade de solicitar ao MEO Empresas a alteração, no entanto esta funcionalidade implica aplicação dos novos preços em vigor.
Alteração de password	Possibilidade de solicitar ao MEO Empresas a alteração da password. Este serviço não tem custo adicional para o cliente.
Alteração de preshare key	Possibilidade de solicitar ao MEO Empresas a alteração da preshared key. Esta alteração tem impacto em todas as contas que se ligam pelo método IPSec. Este serviço não tem custo adicional para o cliente.
Alteração dos endereços IPs de WAN	Possibilidade de atribuição de novos endereços IP WAN privados diferentes dos atribuídos da gama 10.57.0.0/16 (para método de acesso IPSec) e/ou da gama 10.58.0.0/16 (para método de acesso SSL). Esta atribuição pode ser motivada devido a duplicação (estas gamas de endereçamento já estarem a ser utilizadas para outro fim na rede do cliente), ou devido a necessidade de seguir determinado plano de endereçamento. Este serviço não tem custo adicional.
Aplicação de restrições de acesso	Permite alterar as permissões de acesso ao nível de: - Alterar/atribuir perfis de restrição de acesso por Teamwork, ou seja, implementar restrições de acesso para que um dado Teamwork só tenha acesso a determinadas redes IP e/ou a um endereço IP através de determinados protocolos; - Alterar o endereço IP LAN origem do Teamwork, quando o endereço IP LAN origem da rede local onde o utilizador do cliente está a utilizar o serviço Teamwork e o endereço IP destino da LAN do cliente (dos recursos que pretende aceder remotamente) são iguais. Este serviço tem um preço por pedido e pode envolver restrições de vários Teamwork no mesmo pedido.
Alteração de DNS	Permite alterar o DNS default do MEO Empresas para DNS privado da Empresa. Só é possível especificar 2 DNS privados por cliente e esta alteração é transversal a todos os Teamwork do cliente.
No Split Tunneling	Permite alterar as permissões de acesso para todas os Teamwork (não apenas para uma parte) de forma que não possam aceder localmente à internet quando em simultâneo estão ligadas à VPN IP, ou seja, que não haja Split Tunneling. Este serviço tem um preço por pedido envolve todos os Teamwork.

2. Preparativos para a instalação do serviço

Requisitos de instalação

É necessário ter acesso à internet nas diferentes plataformas de acesso (PCs, Tablets e Smartphones) que vai usar para fazer o acesso remoto. Este acesso pode estar suportado numa das seguintes alternativas:

- Num acesso direto para internet disponível através de uma PEN/cartão colocado diretamente no equipamento com endereço IP WAN público fixo ou dinâmico;
- Num acesso à internet disponível através de uma rede local LAN (com ligação através de cabo Ethernet)/WirelessLAN (com ligação através de WiFi) com endereçamento IP local privado e saída para a internet através de gateway com endereço IP WAN público fixo ou dinâmico. Nesta situação, as políticas de segurança configuradas no equipamento gateway, têm de permitir a comunicação com o concentrador de túneis do MEO Empresas através do porto UDP 4500 no sentido da rede LAN do cliente para a internet.



Tem de ter uma VPN IP suportada na rede empresarial MEO.

As plataformas de acesso têm de cumprir os requisitos de sistema operativo e requisitos mínimos para instalação do software específico FortiClient. Para computadores com sistemas operativos Windows, Linux ou Mac OS, é disponibilizado software específico FortiClient compatível com a oferta, no site MEO Empresas. Para tablets e smartphones o software é disponibilizado na Play Store e na App Store, de acordo com o indicado no manual.

Por questões de segurança é fundamental atualizar regularmente o software FortiClient.

A instalação do software de suporte ao serviço Teamwork nas plataformas de acesso, é feita pelo cliente de acordo com as instruções disponibilizadas no manual de utilizador. Caso tenha dificuldades na instalação, configuração e utilização do serviço, poderá entrar em contato com o MEO Empresas para clarificar eventuais dúvidas que possam ocorrer. Realçamos que o apoio que o MEO Empresas presta é sempre remoto via suporte telefónico.

Versões de SW homologadas para funcionamento

Tipo de plataforma	Tipo de sistema operativo	Versão FortiClient	Método de acesso (Release de SW 7.0.9)	
			IPSec	SSL - Tunnel Mode
PC	Windows PC	7.0.7.0345	- Desktop - Desktop operating systems - Microsoft Windows 11 (64-bit) - Microsoft Windows 10 (32-bit and 64-bit) - Microsoft Windows 8.1 (32-bit and 64-bit) - Microsoft Windows 7 (32-bit and 64-bit) - FortiClient 7.0.7 does not support Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 8.	
	Mac OS PC	7.0.7.0245	- Desktop - Desktop operating systems - macOS Ventura (version 13) - macOS Monterey (version 12) - macOS Big Sur (version 11) - macOS Catalina (version 10.15)	
	Linux PC	7.0.7.0245	Não disponível	- Desktop - Desktop operating systems - Ubuntu 18.04 or newer - Debian 11 or newer - Red Hat 7.4 or newer - CentOS Stream 8, 7.4 or newer - Fedora 36 or newer with KDE or GNOME
Tablet	iOS (Ipad)	7.0.7.0070	Não disponível	iOS 9 a 16
	Android	7.0.6.0049	Não testado	Android 5 a 12
Smartphone	iOS (Iphone)	7.0.7.0070	Não disponível	iOS 9 a 16
	Android	7.0.6.0049	Não testado	Android 5 a 12

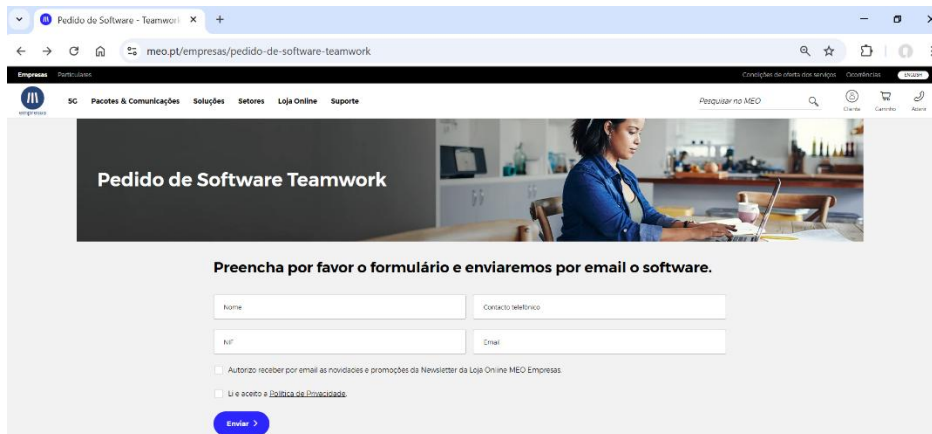
Versões mais recentes de software

Aquando da adesão ao serviço o MEO Empresas envia um email para o utilizador do serviço com link para o manual de Instalação, Configuração e Utilização do serviço e links para as versões de software para PCs. Para Tablets e Smartphones o software é disponibilizado na Google Play Store e na App Store.

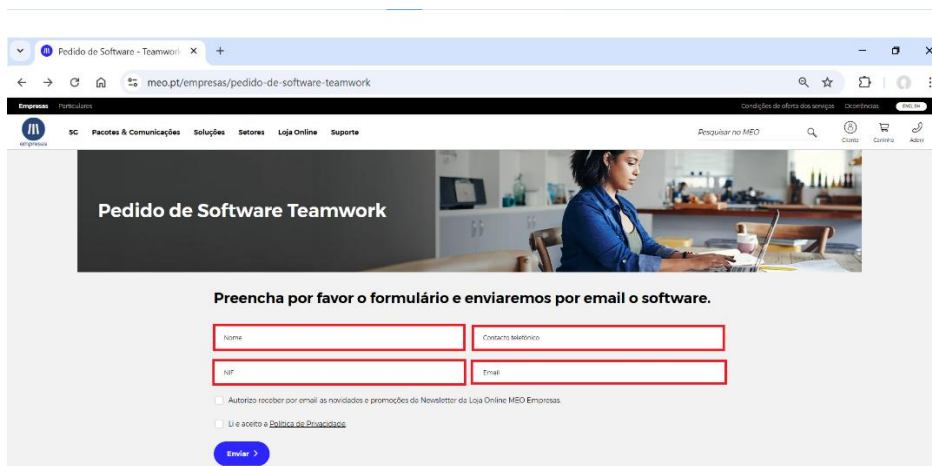
Caso não tenha presente estes emails, é também possível aceder às versões mais recentes de software, seguindo os passos enumerados de seguida.

2.1.1. Software para PCs

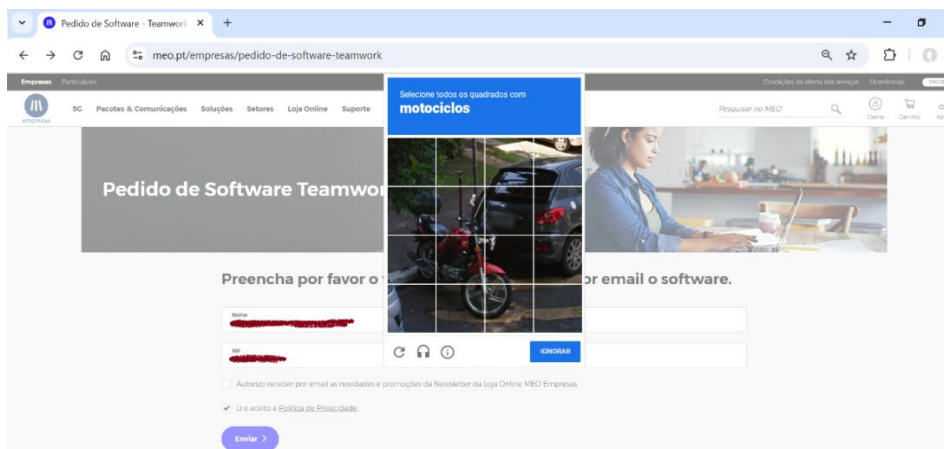
1º Passo - Aceder ao URL <https://www.meo.pt/empresas/pedido-de-software-teamwork>

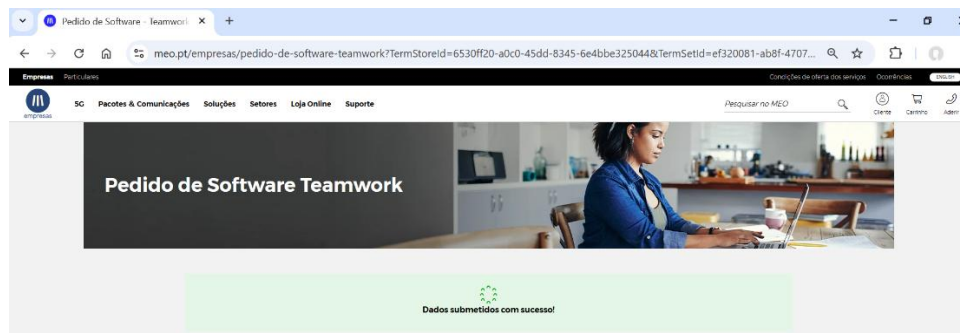


2º Passo - Preencher os dados no formulário:



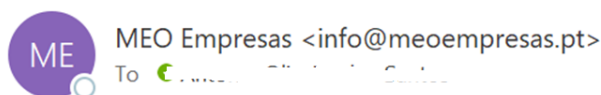
3º Passo - Submeter o pedido:





4º Passo - Receber o email com os links:

Pedido de Software Teamwork



Caro(a) cliente,
Bem-vindo ao serviço Teamwork.

Software de acesso remoto

Para utilizar o serviço Teamwork, tem de instalar o software de acesso remoto que depende do tipo de equipamento e sistema operativo.

Software de suporte ao serviço para PC:

- [Software FortiClient para Windows Windows PC 32bits \(IPSec e SSL\)](#)
- [Software FortiClient para Windows Windows PC 64bits \(IPSec e SSL\)](#)
- [Software FortiClient para MacOS PC \(IPSec e SSL\)](#)
- [Software FortiClient para Linux PC \(SSL\)](#)

Software de suporte ao serviço para Tablet e Smartphone disponível na Google Play Store ou na App Store.

Credenciais de acesso e manual

Após instalação do software bastará colocar as credenciais de acesso que lhe fornecemos para poder começar a utilizar este serviço. Para sua comodidade, criámos um [manual](#) de instalação, configuração e utilização do serviço, que pode utilizar para apoio passo a passo na configuração e utilização.

Ficamos ao seu dispor

Para mais informações, estamos sempre disponíveis através do seu gestor ou dos contactos abaixo.

Por questões de segurança (para evitar ataques de phishing), o MEO Empresas nunca envia emails ou outras notificações automáticas (sem ser a pedido de cliente), a informar que tem novas versões de software para instalar com links explícitos para atualização.

2.1.2. Software para Tablets e Smartphones

Para Tablets e Smartphones, o software específico é disponibilizado na Google Play Store (para equipamentos com android) e na App Store (para equipamentos iPad e iPhone da Apple com IOS).

3. Instalação do serviço, configuração e utilização

Nos pontos seguintes estão ilustrados os passos a considerar na instalação em função do tipo de equipamento e sistema operativo.

3.1. Windows PC (IPSec e SSL)

A versão do SW e documentação mais recente de suporte ao serviço Teamwork, para ambiente Windows PC (IPSec e SSL), compatível com a plataforma central de concentração de túneis é:

FortiClient - VERSION 7.0.7.0345

Para saber qual a versão que está a utilizar deve fazer:

Consulta na versão anterior	Consulta na versão mais recente
 Pressionar em . O resultado obtido vai depender da versão instalada. O resultado para a versão mais recente é:	 Pressionar em . O resultado obtido vai depender da versão instalada. O resultado para a versão mais recente é:

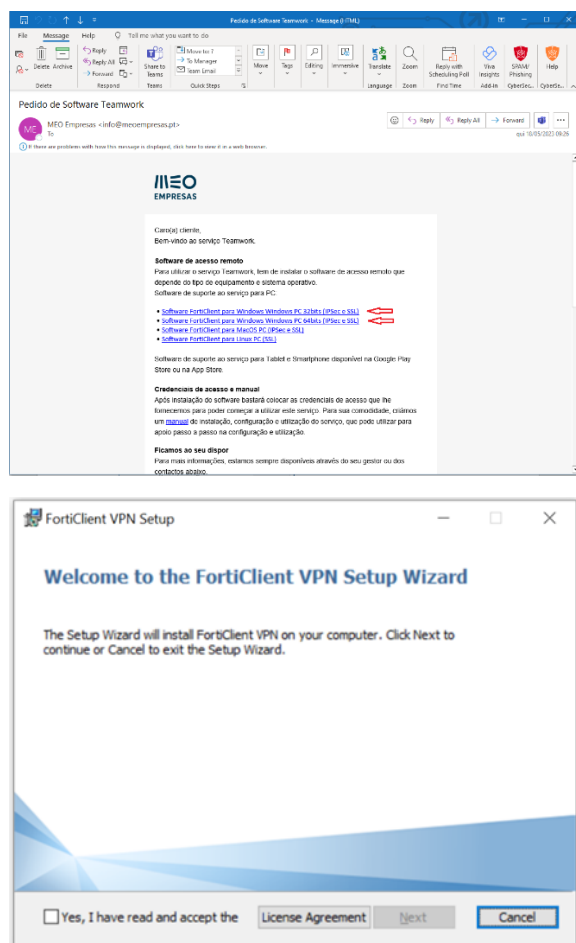
Os requisitos mínimos para instalação em ambiente Windows são:

Sistema operativos suportados	Requisitos mínimos do sistema
Desktop Desktop operating systems - Microsoft Windows 11 (64-bit) - Microsoft Windows 10 (32-bit and 64-bit) - Microsoft Windows 8.1 (32-bit and 64-bit) - Microsoft Windows 7 (32-bit and 64-bit) Note: FortiClient 7.0.7 does not support Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 8.	- Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient does not support ARM-based processors. - Compatible OS and minimum 512 MB RAM 600 MB free hard disk space - Native Microsoft TCP/IP communication protocol - Native Microsoft PPP dialer for dialup connections - Ethernet NIC for network connections - Wireless adapter for wireless network connections

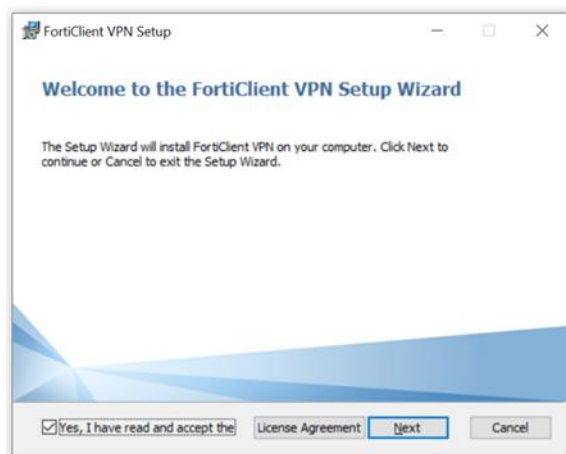
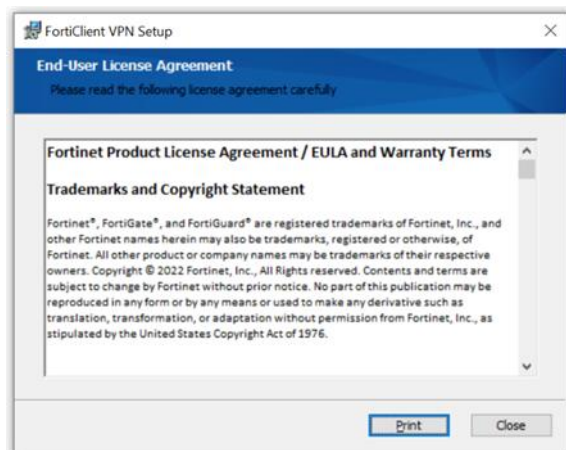
- Adobe Acrobat Reader for viewing documentation
- MSI installer 3.0 or later Adobe Acrobat Reader for viewing FortiClient documentation
- Windows Installer MSI installer 3.0 or later

3.1.1. Windows PC (IPSec e SSL) - Instalação

Escolher a versão para 32bits ou a versão para 64bits, em função do sistema operativo do PC:

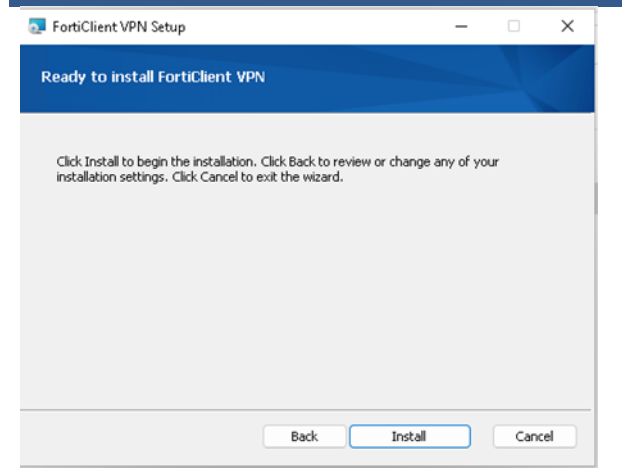
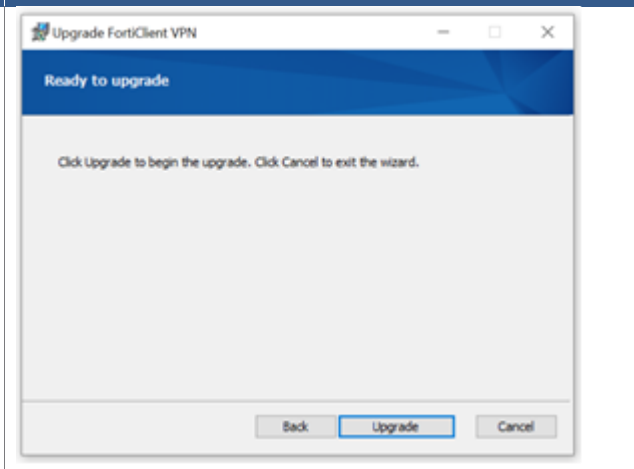


Pressionar em **License Agreement** e ler atentamente os termos da licença.



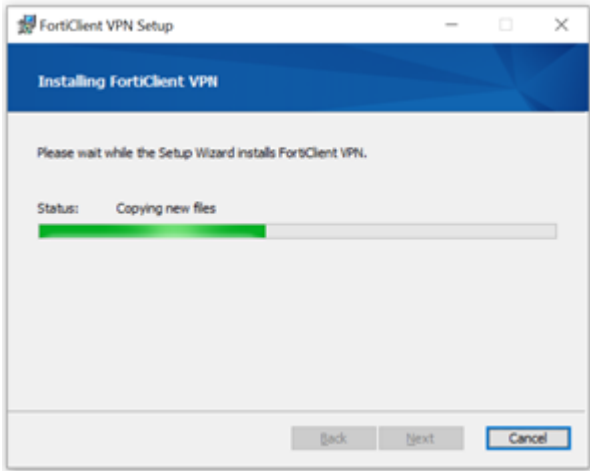
Concordar com os termos da licença pressionando em ☒ Yes, I have read and accept the

Para avançar pressionar em

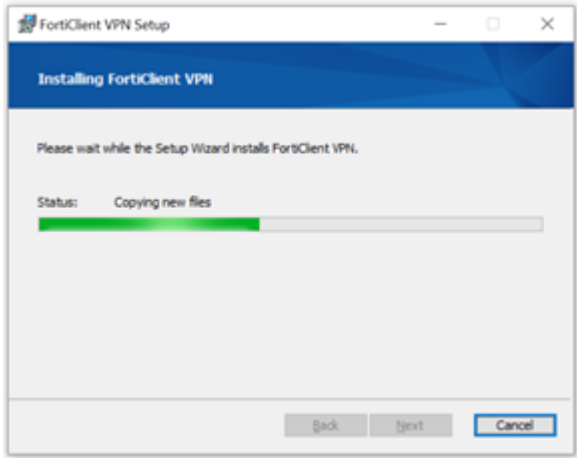
No caso de nova instalação	No caso de upgrade da versão instalada
	
Para avançar pressionar em Install	Para avançar pressionar em Upgrade



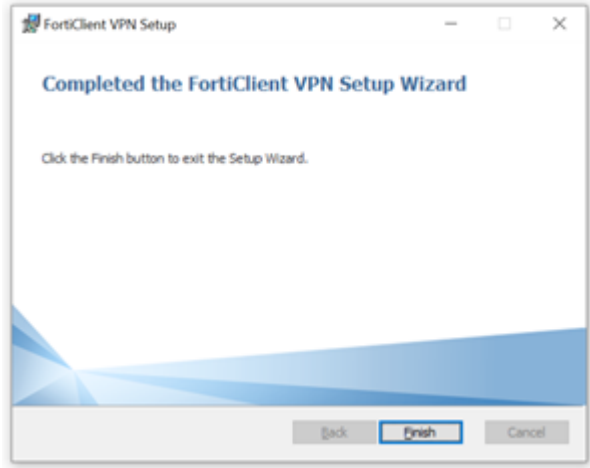
Instalação em andamento



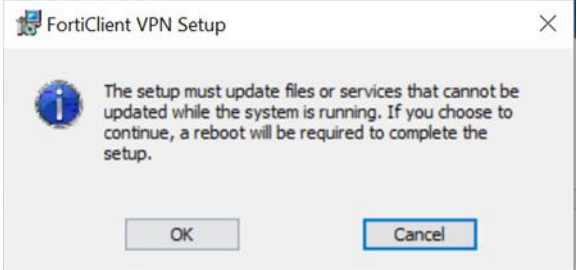
Instalação em andamento



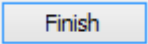
In



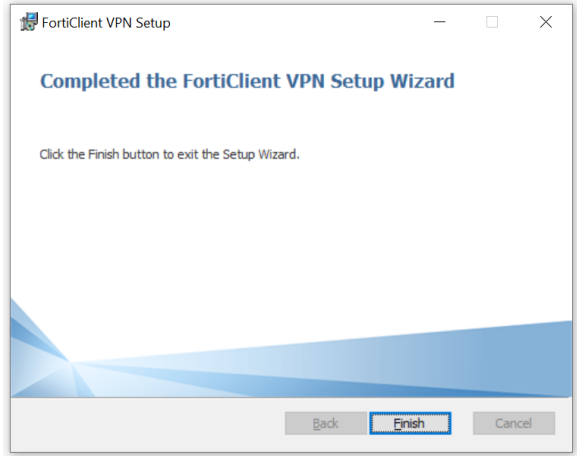
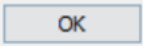
In



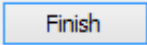
Para terminar a instalação pressionar em

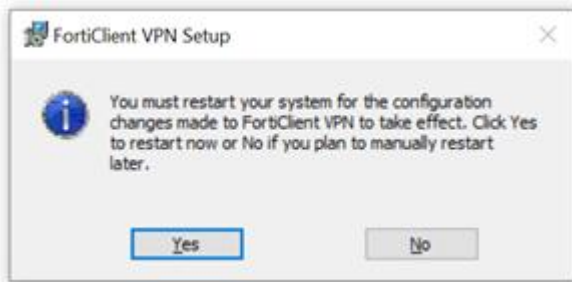


Para avançar pressionar em



Para terminar a instalação pressionar em



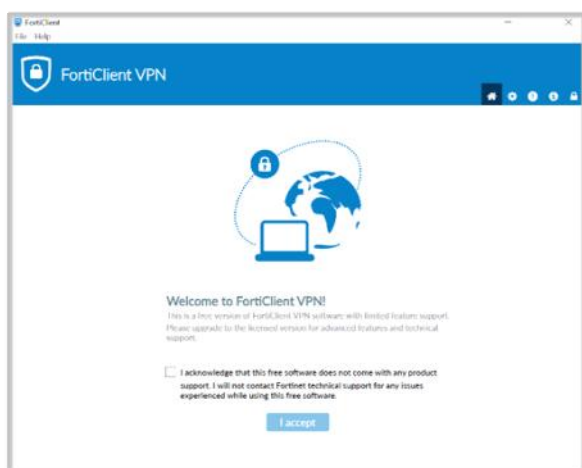


Para reinicializar o PC, pressionar em .

3.1.2. Windows PC (IPSec e SSL) - Configuração

Após a instalação é necessário proceder à configuração do software.

Abrir a consola da aplicação:



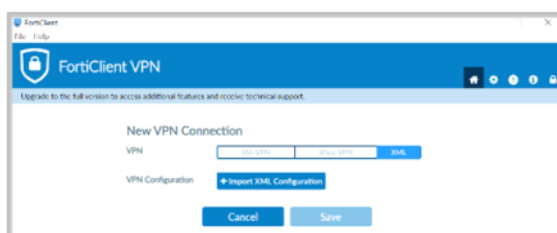
Ler as condições da licença:



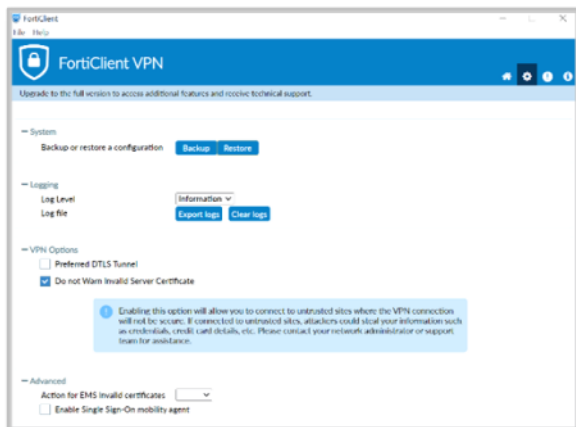
Para concordar com os termos da licença pressionar em .



Para personalizar a configuração do software, pressionar em: [Configure VPN](#). No entanto, para facilitar a instalação, o MEO Empresas disponibiliza o ficheiro de configuração standard sem as credenciais de acesso ([Faça download do ficheiro aqui](#)) evitando desta forma estar a fazer as parametrizações dos detalhes dos dois ecrãs seguintes.

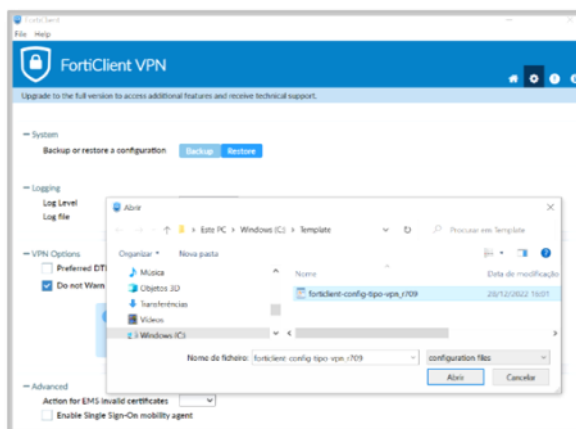


Para carregar o ficheiro de configuração standard tem de pressionar em  permitir acesso à edição dos parâmetros, seguido de .

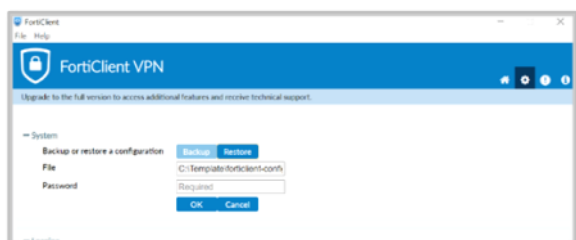


Para abrir o ecrã de importação do ficheiro, pressionar em System -> **Restore**.

Selecionar o ficheiro.

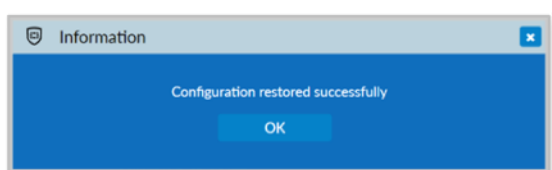


Pressionar em -> abrir.



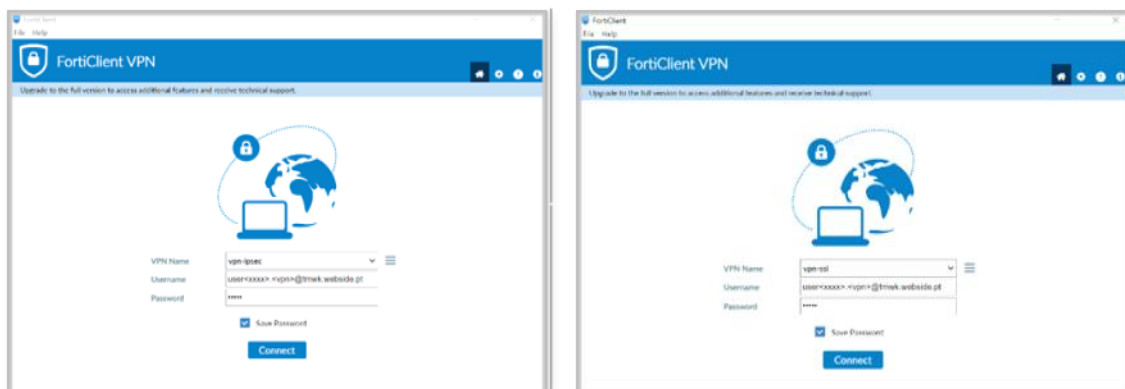
Password = TempConfR709

Proceder ao restore pressionar em **OK**.



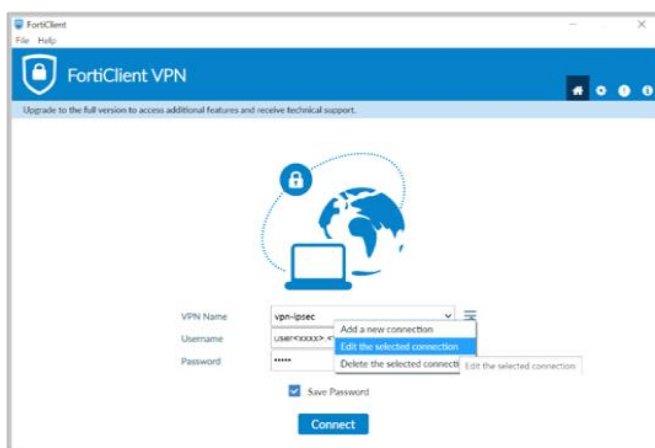
Para terminar o carregamento do ficheiro de configuração pressionar em **OK**.

O resultado do ficheiro de configuração standard carregado é o seguinte:

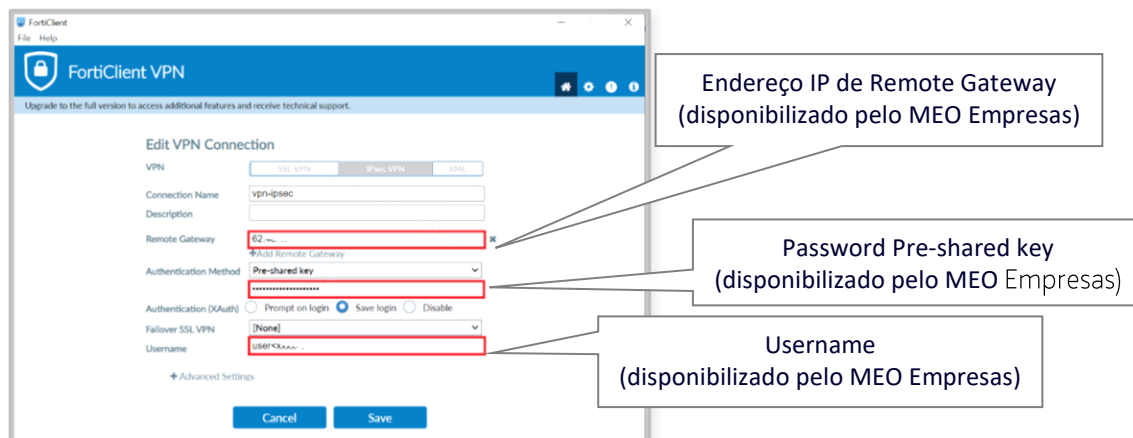


Para visualizar as restantes configurações standard que foram carregadas nas outras janelas, seguir os seguintes passos:

Para o método IPsec



Configurar o endereço IP do Remote Gateway, password pre-shared key e username.



Manter parâmetros dos Advanced Settings, ao nível de:

Advanced Settings

VPN Settings

IKE ☒ Version 1 ☐ Version 2

Mode ☐ Main ☒ Aggressive

Options ☒ Mode Config ☐ Manually Set ☐ DHCP over IPsec

Phase 1

IKE Proposal

Encryption Authentication

Encryption Authentication

DH Group ☐ 1 ☐ 2 ☒ 5 ☐ 14 ☐ 15

☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20

Key Life sec

Local ID

☒ Dead Peer Detection

☒ NAT Traversal

☐ Enable Local LAN

Phase 2

IKE Proposal

Encryption Authentication

Encryption Authentication

Key Life ☒ 43200 Seconds

☐ 5120 KBytes

☒ Enable Replay Detection

☒ Enable Perfect Forward Secrecy (PFS)

DH Group

Para o método SSL

FortiClient

File Help

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.



VPN Name

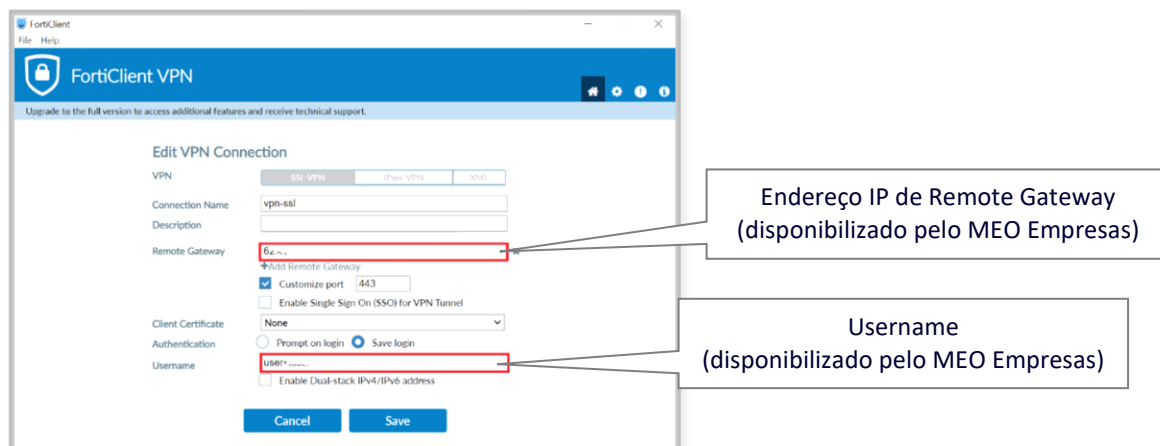
Username

Password

☒ Save Password

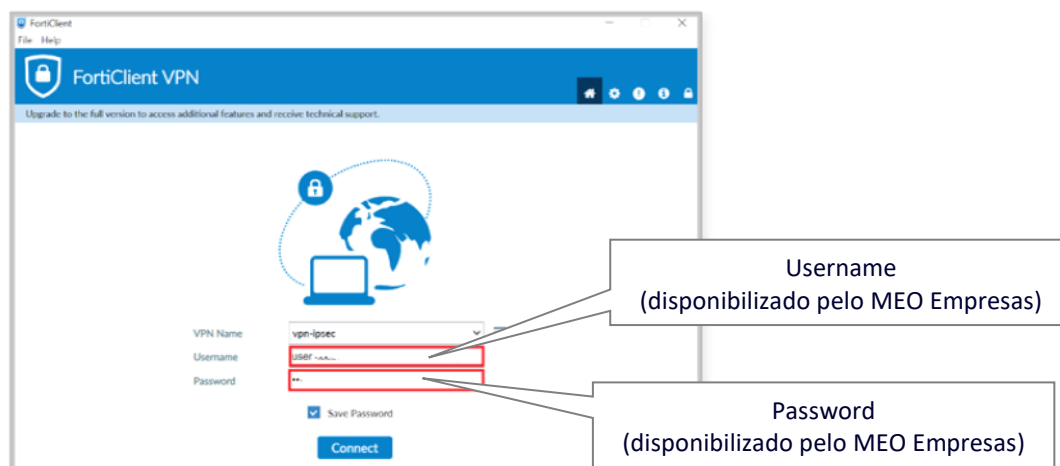
Add a new connection
Edit the selected connection
Delete the selected connection

Configurar o endereço IP do Remote Gateway e username.



3.1.3. Windows PC (IPSec e SSL) - Utilização

Para o método IPSec

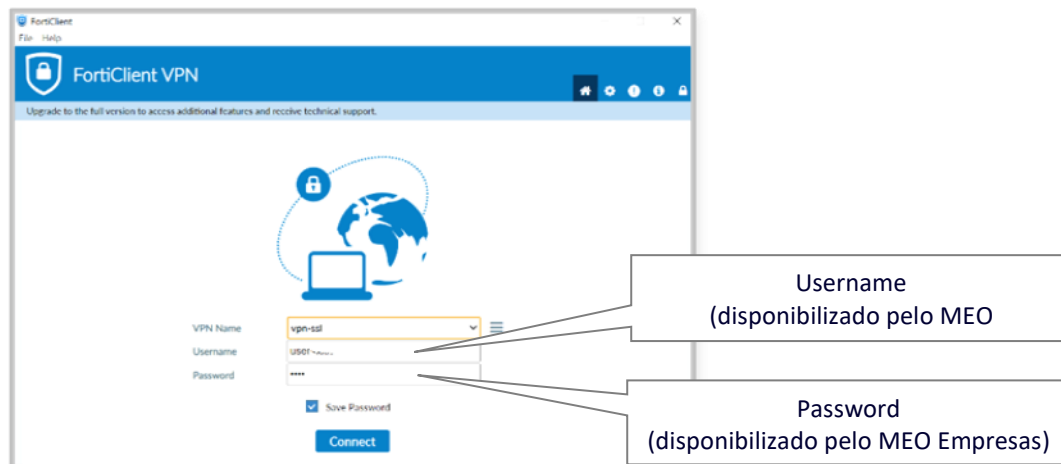


Digitar username e password e pressionar em .

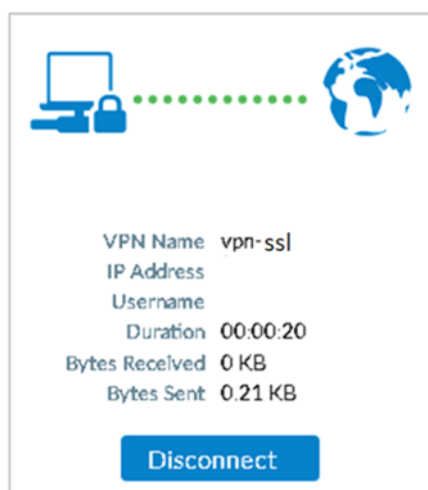


Para desligar pressionar em **Disconnect**.

Para o método SSL



Digitar username e password e pressionar em **Connect**.



Para desligar pressionar em **Disconnect**.

3.2. MAC OS PC (IPSec e SSL)

A versão do SW e documentação mais recente de suporte ao serviço Teamwork, para ambiente MAC OS PC (IPSec e SSL), compatível com a plataforma central de concentração de túneis é:

FortiClient – VERSION 7.0.7.0245

Os requisitos mínimos para instalação em ambiente MAC OS são:

Sistema operativos suportados	Requisitos mínimos do sistema
Desktop Desktop operating systems macOS Ventura (version 13)	- Apple Mac computer with Intel processor or M1 or M2 chip 256 MB of RAM

- macOS Monterey (version 12)
- macOS Big Sur (version 11)
- macOS Catalina (version 10.15)

- 20 MB of hard disk drive (HDD) space
- TCP/IP communication protocol
- Ethernet NIC for network connections
- Wireless adapter for wireless network connections

3.2.1. MAC OS PC (IPSec e SSL) - Instalação

Os passos para a instalação são:

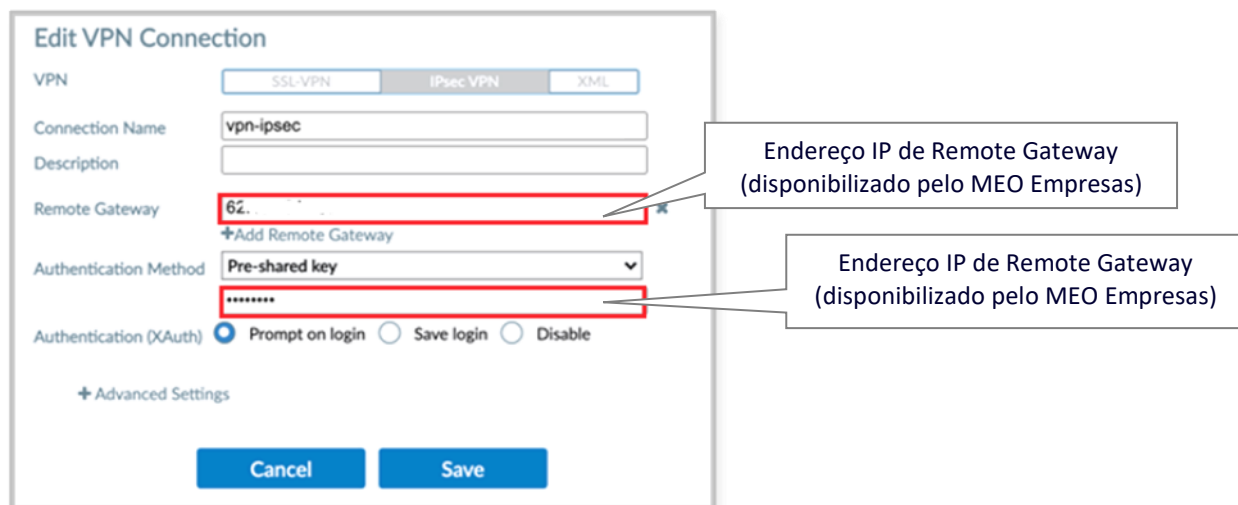
- Pressionar no ficheiro de instalação FortiClient_7.0.7.xx_macosx .dmg. É mostrada a caixa de diálogo The FortiClient for macOS;
- Pressionar em Install. É mostrada a mensagem Welcome to the FortiClient Installer;
- (Optional) Verificar os detalhes no canto superior direito e fechar em OK;
- Pressionar Continue;
- Ler o Software License Agreement e clicar em Continue. É apresentada a opção de Agree;
- Se concordar com os termos do licenciamento clicar em Agree para prosseguir com a instalação;
- Pode ser necessário introduzir a password de Sistema para continuar;
- Depois de concluída a instalação clicar em Close para sair do processo de instalação.

3.2.2. MAC OS PC (IPSec e SSL) - Configuração

Após a instalação é necessário proceder à configuração do software.

Para o método IPSec

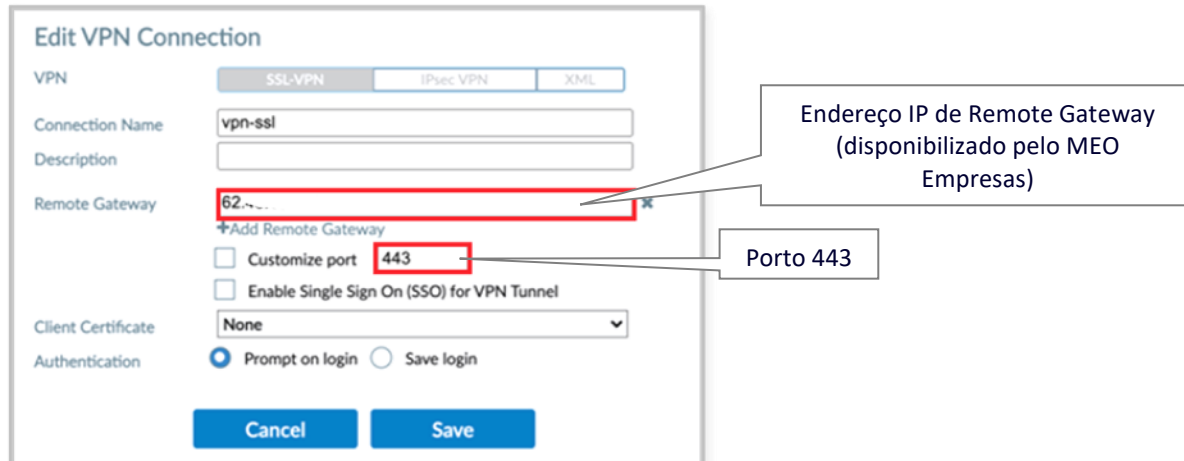
Abrir a consola da aplicação e configurar uma ligação com o nome vpn-ipsec e configurar o endereço IP do Remote Gateway, a Pre-shared key e o username.



Para guardar os dados seleccionar .

Para o método SSL

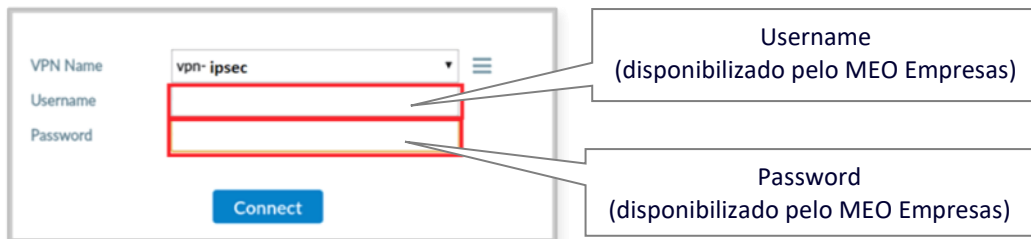
Abrir a consola da aplicação e configurar uma ligação com o nome vpn-ssl e configurar o endereço IP do Remote Gateway, o porto 443 e o Username.



Para guardar os dados seleccionar .

3.2.3. MAC OS PC (IPSec e SSL) - Utilização

Para o método IPSec



VPN Name: vpn-ipsec

Username:

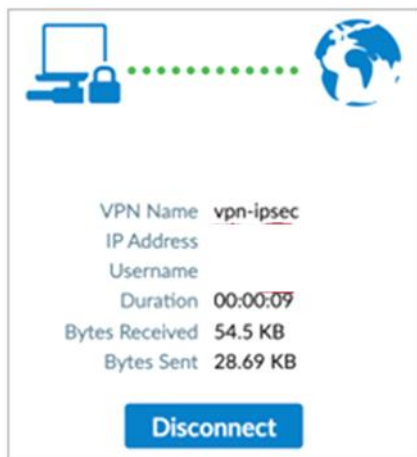
Password:

Connect

Username (disponibilizado pelo MEO Empresas)

Password (disponibilizado pelo MEO Empresas)

Digitar usermane e password e pressionar em **Connect**.



VPN Name: vpn-ipsec

IP Address:

Username:

Duration: 00:00:09

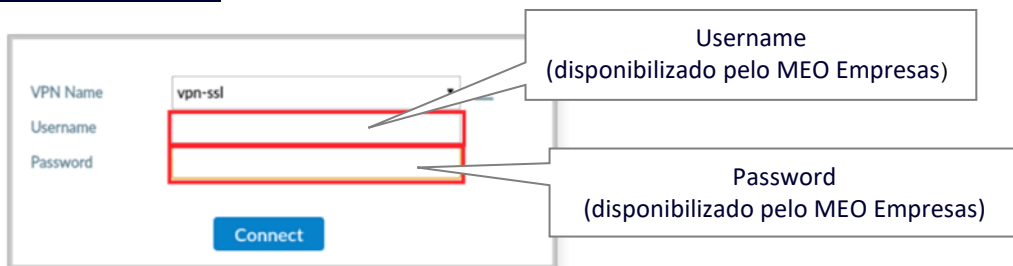
Bytes Received: 54.5 KB

Bytes Sent: 28.69 KB

Disconnect

Para desligar pressionar em **Disconnect**.

Para o método SSL



VPN Name: vpn-ssl

Username:

Password:

Connect

Username (disponibilizado pelo MEO Empresas)

Password (disponibilizado pelo MEO Empresas)

Digitar usermane e password e pressionar em **Connect**.



VPN Name: vpn-ssl

IP Address:

Username:

Duration: 00:00:04

Bytes Received: 0.34 KB

Bytes Sent: 0.82 KB

Disconnect

Para desligar pressionar em **Disconnect**.

3.3. LINUX PC (SSL)

A versão do SW e documentação mais recente de suporte ao serviço Teamwork, para ambiente LINUX PC (SSL), compatível com a plataforma central de concentração de túneis é:

FortiClient - VERSION 7.0.7.0246

Os requisitos mínimos para instalação em ambiente LINUX são:

Sistema operativos suportados	Requisitos mínimos do sistema
Desktop Desktop operating systems • Ubuntu 18.04 or newer • Debian 11 or newer • Red Hat 7.4 or newer • CentOS Stream 8, 7.4 or newer • Fedora 36 or newer	• Linux-compatible computer with Intel processor or equivalent • Compatible OS and minimum 512 MB RAM • 600 MB free hard disk space • TCP/IP communication protocol • Ethernet NIC for network connections • Wireless adapter for wireless network connections

3.3.1. LINUX PC (SSL) - Instalação

Os passos para a instalação são:

- Fazer download do ficheiro para o Linux PC. Instalar com o instalador de pacotes do SO;
- Executar o ficheiro -> forticlient:



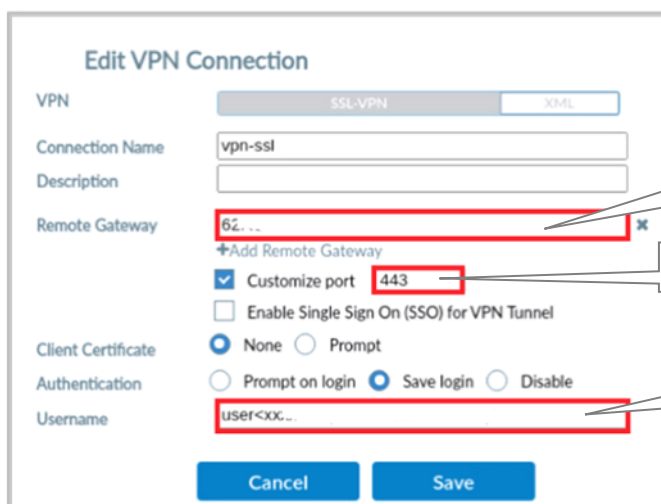
Para avançar fazer .

3.3.2. LINUX PC (SSL) - Configuração

Após a instalação é necessário proceder à configuração do software.

Abrir a consola da aplicação e configurar uma ligação com o nome vpn-ssl e configurar o endereço IP do Remote gateway e o username.

[Configure VPN](#)



Edit VPN Connection

VPN: SSL-VPN XML

Connection Name:

Description:

Remote Gateway:

+Add Remote Gateway

☒ Customize port:

☐ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: ☒ None ☐ Prompt

Authentication: ☐ Prompt on login ☒ Save login ☐ Disable

Username:

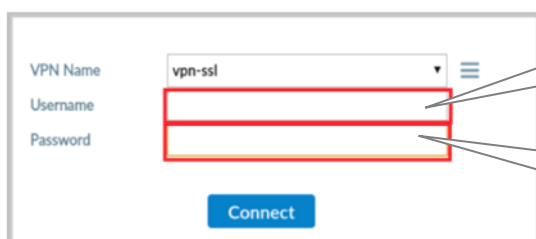
Endereço IP de Remote Gateway
(disponibilizado pelo MEO Empresas)

Porto 443

Username
(disponibilizado pelo MEO Empresas)

Para guardar os dados seleccionar .

3.3.3. LINUX PC (SSL) - Configuração



VPN Name:

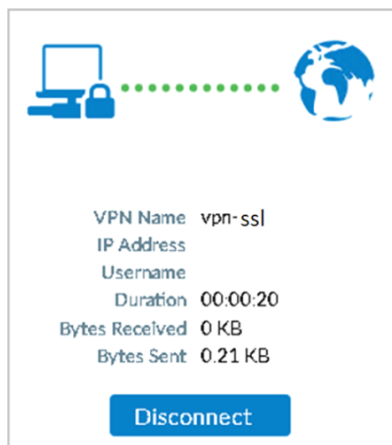
Username:

Password:

Username
(disponibilizado pelo MEO Empresas)

Password
(disponibilizado pelo MEO Empresas)

Digitar username e password e pressionar em .



VPN Name: vpn-ssl

IP Address:

Username:

Duration: 00:00:20

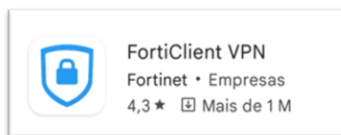
Bytes Received: 0 KB

Bytes Sent: 0.21 KB

Para desligar pressionar em .

3.4. Android Smartphone e Tablet (IPSec e SSL)

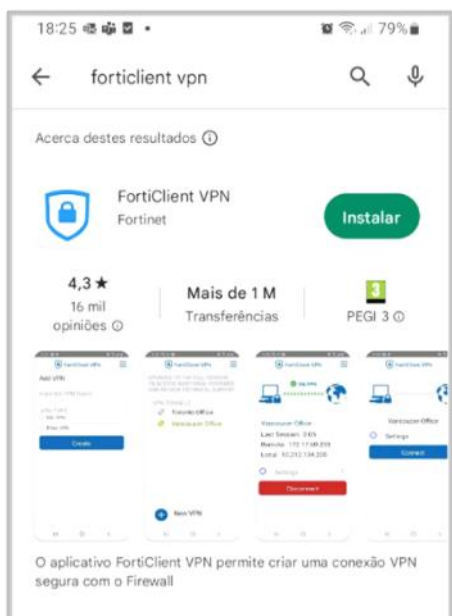
Para estes equipamentos terá de instalar a partir da Google Play Store a aplicação da Fortinet denominada por FortiClient VPN.



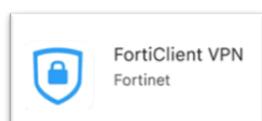
Tipo de plataforma	Tipo de sistema operativo	Versão FortiClient	Método de acesso (Release de SW 7.0.9)	
			IPSec	SSL
Tablet	Android	7.0.6.0049	Não testado	Android 5 a 12
Smartphone	Android	7.0.6.0049	Não testado	Android 5 a 12

A versão testada pelo MEO Empresas está enumerada no quadro acima, no entanto, a versão atualmente disponibilizada na Google Play Store é mais recente.

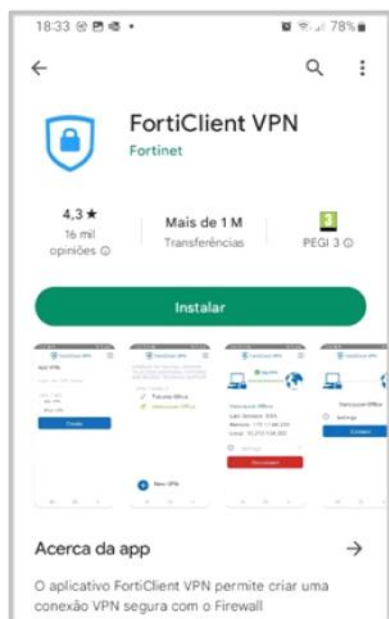
3.4.1. Android Smartphone e Tablet (IPSec e SSL) - Instalação



Pressionar em:



Ver os detalhes da aplicação, para ter certeza da aplicação a instalar.

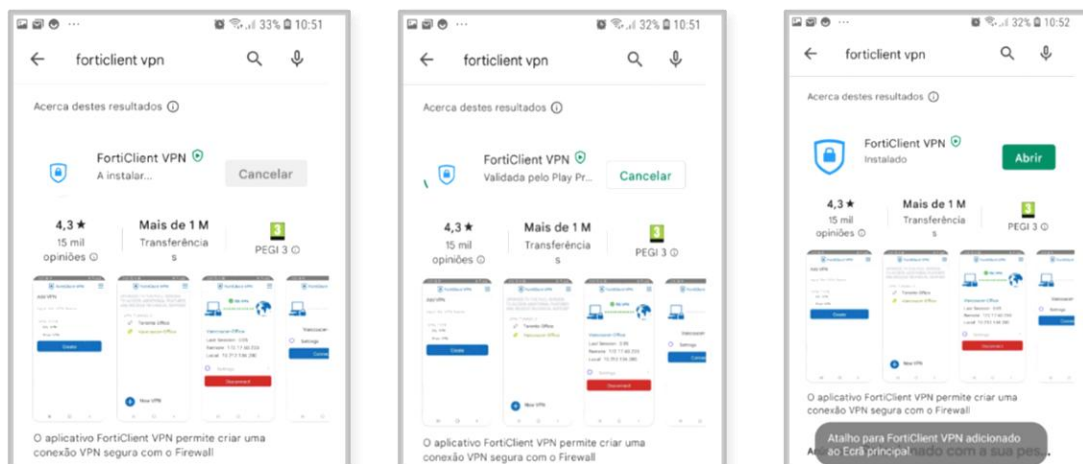


Pressionar em Acerca da app e visualizar a informação.

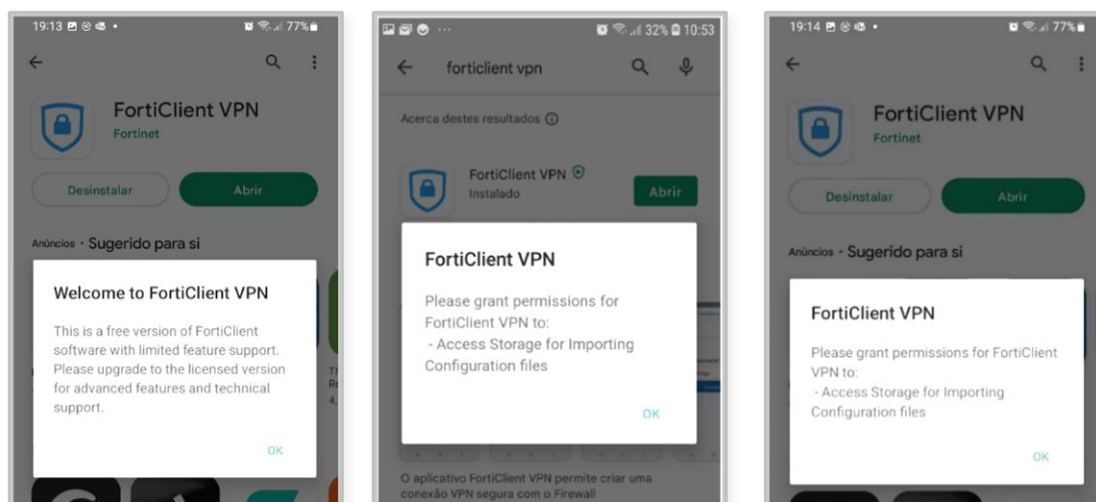


Fazer back, ou seja pressionar em ←.

Para avançar pressionar em Instalar.



Para avançar pressionar em Abrir.



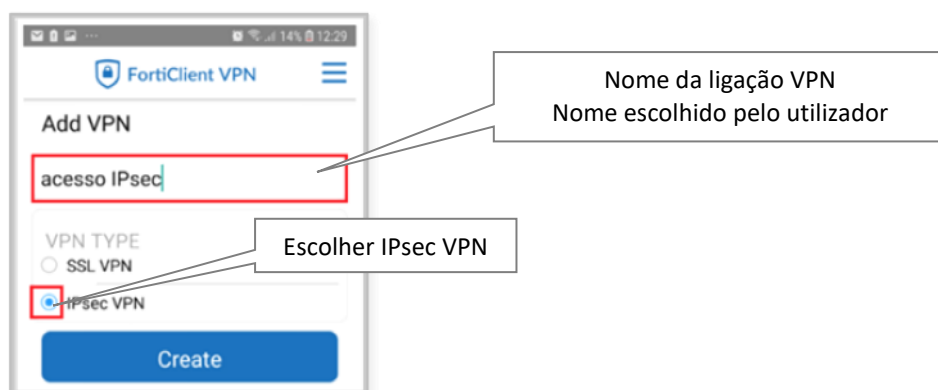
Para avançar pressionar em OK; OK; OK.



3.4.2. Android Smartphone e Tablet (IPSec e SSL) - Configuração

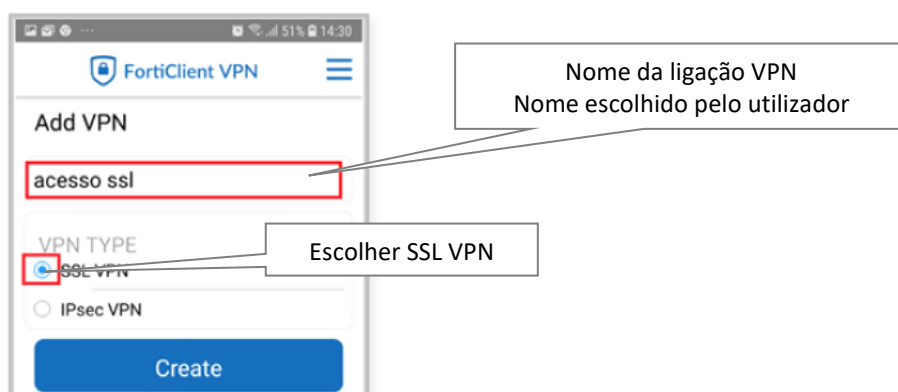
Após a instalação é necessário proceder à configuração do software.

Para o método IPsec

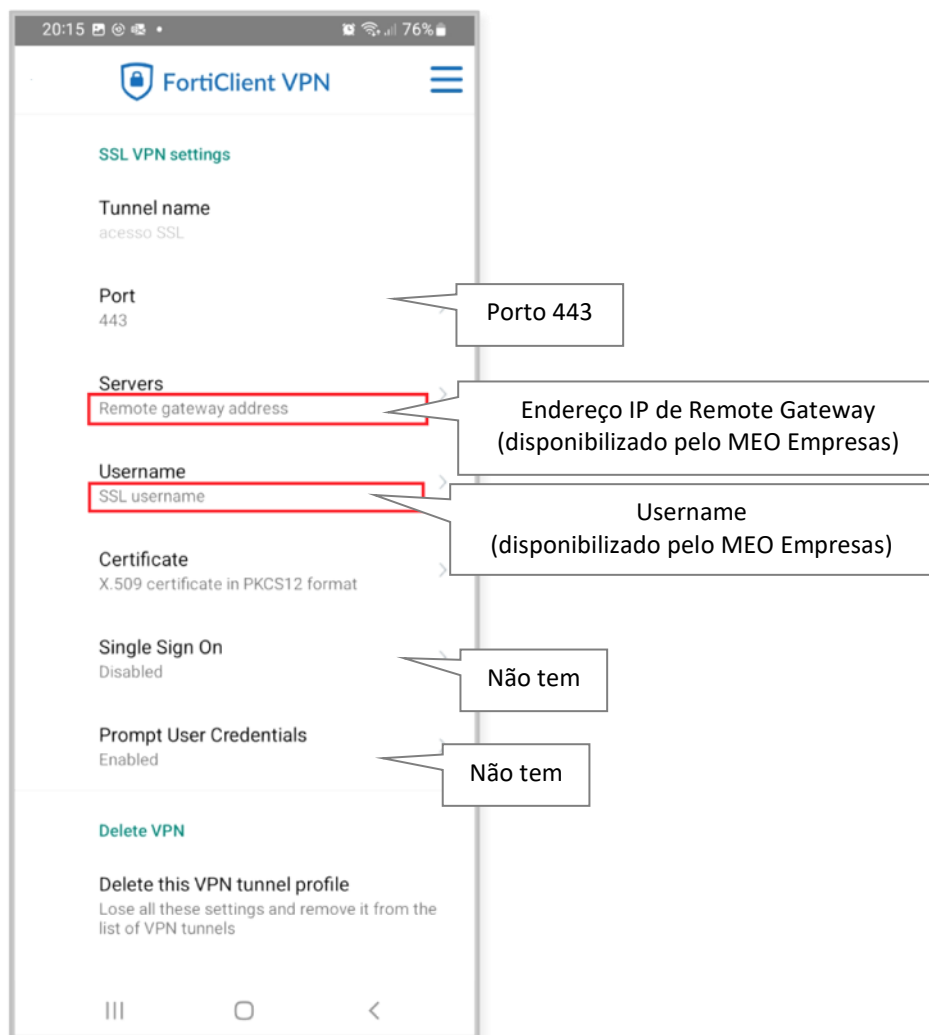


Apesar de possível acesso através de IPsec com Android, não testamos e por isso não detalhamos as configurações necessárias.

Para o método SSL



Para avançar pressionar em Create.

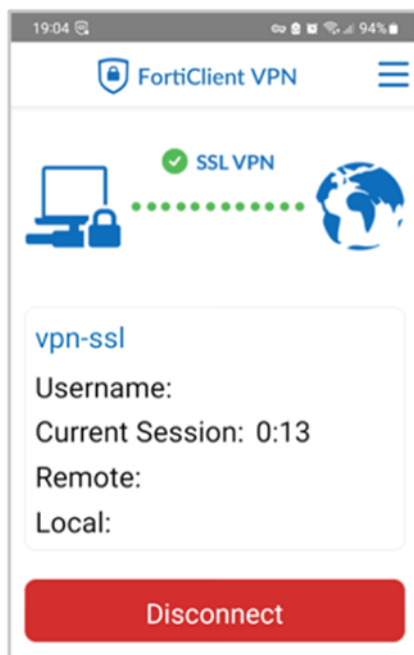
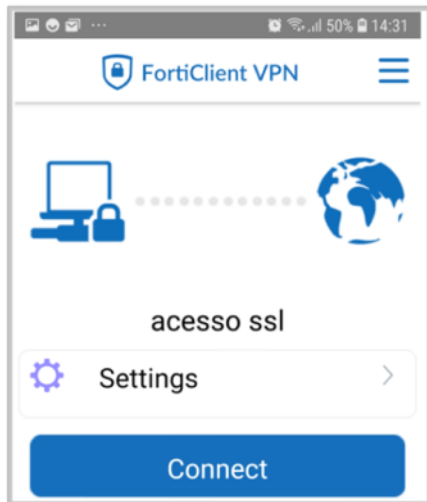


3.4.3. Android Smartphone e Tablet (IPSec e SSL) - Utilização

Para o método IPSec

Apesar de possível acesso através de IPSec com Android, não testamos e por isso não detalhamos as configurações necessárias.

Para o método SSL



3.5. iOS Smartphone e iOS Tablet (SSL)

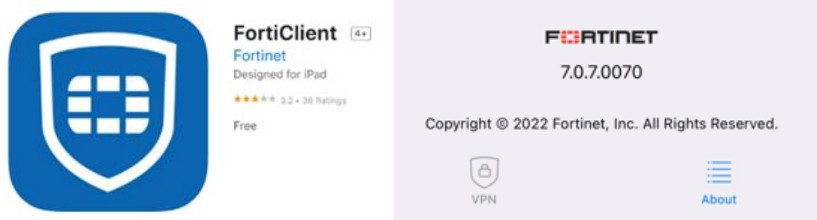
Para estes equipamentos terá de instalar a partir da App Store a aplicação da Fortinet denominada por FortiClient VPN.



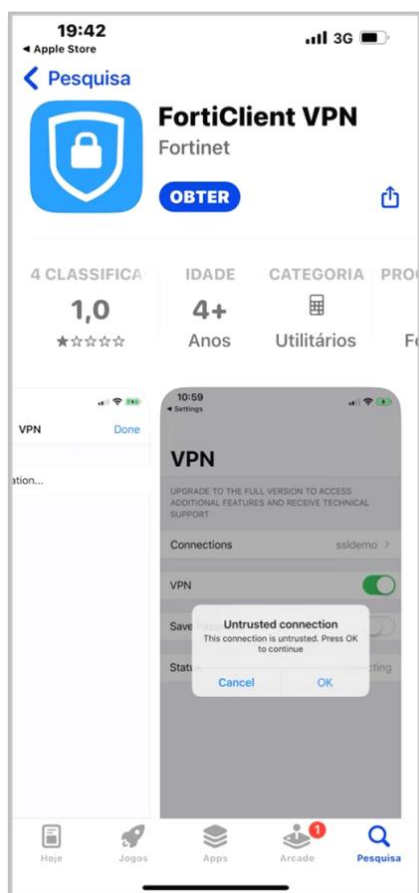
Tipo de plataforma	Tipo de sistema operativo	Versão FortiClient	Método de acesso (Release de SW 7.0.9)	
			IPSec	SSL
Tablet	iOS (Ipad)	7.0.7.0070	Não disponível	iOS 9 a 16
Smartphone	iOS (Iphone)	7.0.7.0070	Não disponível	iOS 9 a 16

A versão testada pelo MEO Empresas está enumerada no quadro acima, no entanto, a versão atualmente disponibilizada na App Store é mais recente.

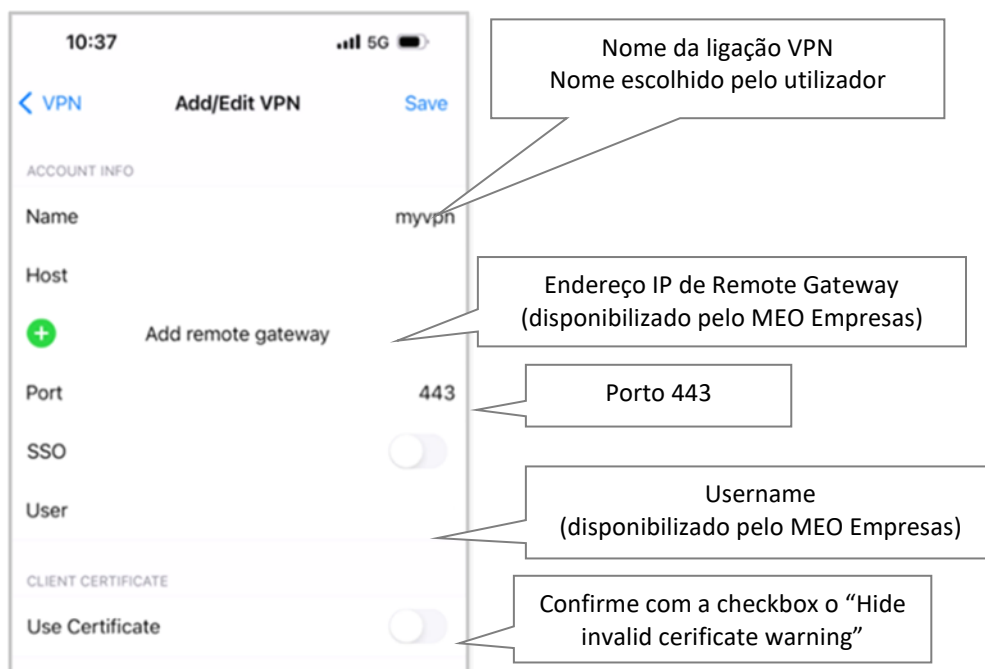
3.5.1. iOS Smartphones e iOS Tablet (SSL) - Instalação e configuração



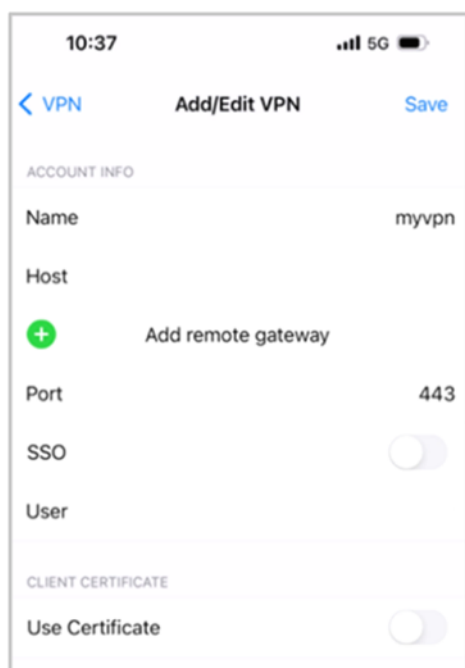
Selecionar no icon FortClient para avançar com a instalação.



Após a instalação é necessário proceder à configuração do software.



3.5.2. iOS Smartphone e iOS Tablet (SSL) - Utilização



4. Apoio técnico

A instalação do serviço é assegurada pelo cliente de acordo com as instruções do Manual de Configuração e Utilização. Caso tenha dificuldades na instalação, configuração e utilização do serviço, poderá entrar em contato com o MEO Empresas através dos contactos de Apoio técnico disponibilizados em: <https://www.meo.pt/empresas/contactos>

O CSC - Centro de Suporte a Clientes Empresariais registará e encaminhará a situação para um departamento técnico, o qual dará continuidade ao processo, contactando-o posteriormente por telefone (das 9h às 18h em dias úteis).

Ao entrar em contato com o CSC, deverá ter o username da sua conta Teamwork, descrever o problema e indicar o número de telefone para a equipa técnica de suporte o contatar.

Reforçamos que, por razões de segurança, o CSC não está autorizado a: alterar passwords, a restringir permissões de acesso a recursos IP da VPN, a alterar os endereços IP WAN, a alterar DNS, nem a alterar as permissões de split tunneling. Esses serviços deverão ser solicitados ao seu Gestor MEO Empresas.