VPN and Split VPN setup

Split VPN directs traffic outside the VPN tunnel, while still allowing users to access the ITU in-house systems and applications.

In ITU split tunnel setup, we directed all the common cloud-based applications outside the VPN tunnel, like the Outlook365 portfolio and most importantly applications like Teams and Zoom, which take up a lot of our bandwidth.

Now that most of us work from home using video conferencing apps, our VPN is peaking a lot during the day and users often experience scrambled voice and video. There is no technical need for these conferences to be streamed inside a VPN tunnel, so we now provide the option for people to choose to use the split VPN.

Another issue is the SMS authentication being slow and unresponsive. Therefore, we have incorporated the option to use the Microsoft Authenticator App as well.

Cases where you cannot use the split tunnel:

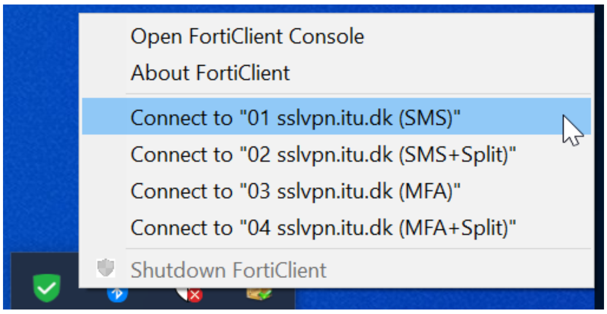
If you use a cloud-based application which only allows access from an ITU IP address, you must use one of our standard VPN tunnels.

How to use it?

Our VPN client will not change. At startup, the standard VPN with SMS authentication will be default.

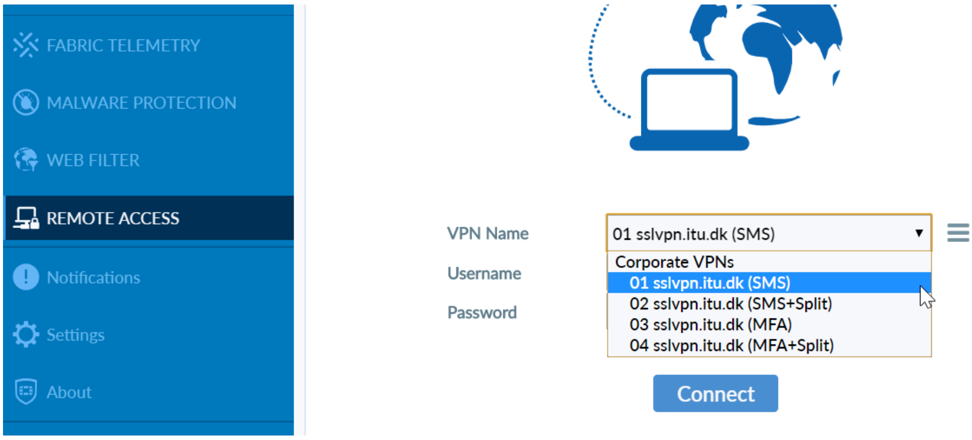
Your client will have a dropdown menu where you can choose SMS or MFA authentication as well as split tunneling with either form of authentication.

Quick connect:



Open FortiClient Console
About FortiClient
Connect to "01 sslvpn.itu.dk (SMS)"
Connect to "02 sslvpn.itu.dk (SMS+Split)"
Connect to "03 sslvpn.itu.dk (MFA)"
Connect to "04 sslvpn.itu.dk (MFA+Split)"
Shutdown FortiClient

Menu inside our FortiClient:



VPN Name: 01 sslvpn.itu.dk (SMS)

Username

Password

Corporate VPNs
- 01 sslvpn.itu.dk (SMS)
- 02 sslvpn.itu.dk (SMS+Split)
- 03 sslvpn.itu.dk (MFA)
- 04 sslvpn.itu.dk (MFA+Split)

Our VPN client is managed centrally and will be rolled out and updated automatically if you have an "ITU managed" computer with Windows or Mac OS.

If you use a different OS like Linux, you have to setup up your VPN manually, and the following gateway addresses must be used:

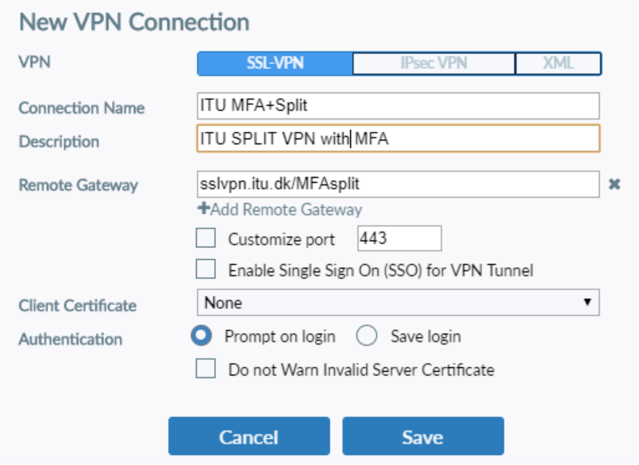
1a) Full VPN with SMS, **sslvpn.itu.dk**

1b) Split VPN with SMS, **sslvpn.itu.dk/split**

2a) Full VPN with Microsoft authenticator, **sslvpn.itu.dk/MFA**

2b) Split VPN with Microsoft authenticator, **sslvpn.itu.dk/MFAsplit**

It might look like this, depending on the client program:



VPN: SSL-VPN

Connection Name: ITU MFA+Split

Description: ITU SPLIT VPN with MFA

Remote Gateway: sslvpn.itu.dk/MFAsplit

□ Customize port 443

□ Enable Single Sign On (SSO) for VPN Tunnel

Client Certificate: None

Authentication: ● Prompt on login ○ Save login

□ Do not Warn Invalid Server Certificate

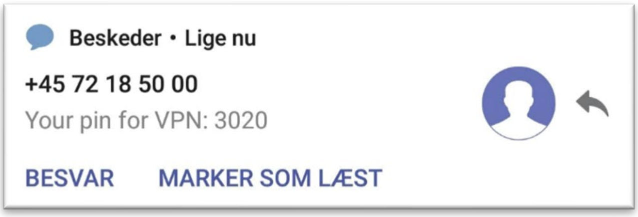
Authentication methods

Either method requires you to enter a valid ITU account username and password.

You should generally receive the prompt within a minute, however at peak hours it might take a bit longer, so please be patient.

Prompts will look like this:

SMS:



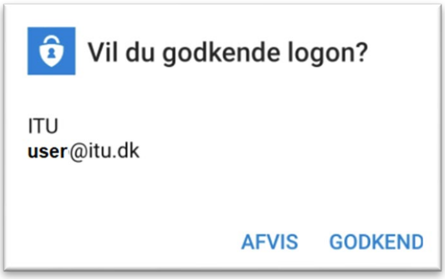
Beskeder • Lige nu

+45 72 18 50 00

Your pin for VPN: 3020

Enter the pin code into the “answer” box at your VPN client.

Microsoft Authenticator App:



Vil du godkende logon?

ITU
user@itu.dk

Simply press the “godkend”/“approve” button and the VPN client will establish the connection shortly afterwards.

Any questions or problems regarding the VPN setup and usage?

Contact our helpdesk during opening hours at 2C or at it@itu.dk