STANDARD OPERATING PROCEDURE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**Connecting to the TRE VPN with 2-FA**
Effective Date:	**14 Feb 2019**
Reference Number:	**SOP-03-22**
Version Number:	**1.1**
Owner:	**Information Security Manager,**
Review Date:	**04 Feb 2021**

Table of Contents

1. Purpose

This document provides guidance to Trustworthy Research Environment (TRE) users for setting up new connections to the TRE Virtual Private Network (VPN) and its associated 2-Factor Authentication (2-FA) service.

The TRE VPN provides a secure tunnel that further protects connections between user end-points (workstations/laptops) and the TRE. The VPN also improves accessibility by enabling TRE users to connect to the VPN from different physical locations.

The 2-FA service provides each TRE user with a unique token. As this token is required to connect to the VPN, it makes unauthorised access to the TRE extremely unlikely.

Please check the Scope section of this document, as VPN and 2-FA is only applicable to certain users and not required if you are University of Manchester staff or students on the University of Manchester wired campus network.

As the VPN is a layer on top of the standard TRE connection, it does not affect the way standard connections are made. SOP-03-16 describes how a TRE user establishes a standard connection to the TRE.

This document assumes the details of the standard TRE connection have already been sent to the TRE user. Email messages from the TRE Service Team are sent from the following accounts:

tre-support@manchester.ac.uk & helpdesk@zendto.manchester.ac.uk

2. Scope

Connection to the TRE using the VPN/2-FA service is mandatory for the following types of TRE users:

- TRE users who are not University of Manchester staff or students, and connected to the TRE from their local institution's network
- TRE users who are University of Manchester staff or students who are connected to the University of Manchester wireless network, or any other network off-campus

TRE users who are University of Manchester staff or students and connected to the University of Manchester 'wired' network using an Ethernet network cable are not required to use the TRE VPN and 2-FA services. However, if a laptop is the primary device for connecting to the TRE, the VPN/2-FA connection can still be used on campus.

3. Procedure

Access to the TRE VPN requires a 2-FA step to be completed as part of the login process, therefore this document describes the setup of 2-FA first.

As described in section 1, document SOP-03-16 must also be followed to setup the 'standard' connection to the TRE using secure remote desktop tools. As it is not possible to test the standard connection to the TRE without first connecting to the VPN, it should be attempted afterwards, although the exact order in which software tools are installed and configured is not important.

3.1. 2-FA

The TRE 2-FA service uses an RSA Securid system that distributes digital tokens to users. University of Manchester staff and students have the choice of obtaining these tokens via a physical key-fob device or via a mobile phone app. Non-University of Manchester staff and students can only use the mobile phone app. This document only describes the use of the mobile phone app.

The RSA Securid app can be obtained directly from the Apple App Store (for iPhones) or Google Play (for Android phones). There are also version for many other operating systems, but this document only describes the procedure for Android devices.

Please refer to RSA's instructions for installing and configuring their Securid app for your device:

Two-factor Authentication: RSA SECURID® Software Tokens

After clicking the link to your device from the above web page you are taken to the device specific support page. Navigate down this page and select the link to the Quick Start Guide, and from the page that follows, open the embedded PDF document.

The following steps must be followed:

a) Install the Securid app on your device
b) Obtain your Device ID and email this along with your mobile phone number (including country code) to tre-support@manchester.ac.uk
c) The TRE Service Team will send a text message to your mobile phone containing a passphrase needed to decrypt downloads of VPN and 2-FA software
d) The TRE Service Team will then email you a link to download your RSA Securid Token (this involves receiving a QR Code. Follow the instructions provided within the corresponding email message).
e) Import the Token into your Securid app (by scanning the QR Code)
f) Once imported, the Securid app should then display the Tokencode, which is an 8-digit number that is used for authenticating you access to the TRE VPN service

Note: the 8-digit Tokencode refreshes every 60 seconds and is unique each time

3.2. VPN

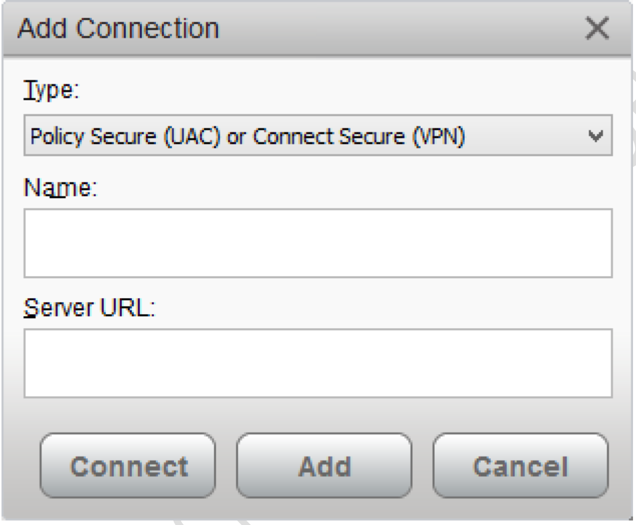
The VPN adds a security layer on top of the standard connection from the TRE user's workstation/laptop and the TRE (usually SSH or RDP). This requires a VPN software client to be installed on that same device.

Note: As described in section 1, the VPN allows users to connect to the TRE from different physical locations. This is best achieved using a laptop, and setting it up as the primary TRE user end-point. It is, in theory, possible for an individual TRE user to connect to the TRE using multiple devices, but this *would require copies of their SSH private key to be transferred to each end-point device which is not recommended; hence the reason a laptop is recommended for TRE users who wish to connect from multiple locations.*

The TRE Service team will send an email to the TRE user containing a link to download the VPN client software. Different clients are available for Windows, MacOS and Linux.

This software client must be installed on the device that will connect to the TRE.

After installing the VPN client, it is necessary to add a new VPN connection. Open the VPN client and click on the '+' icon:



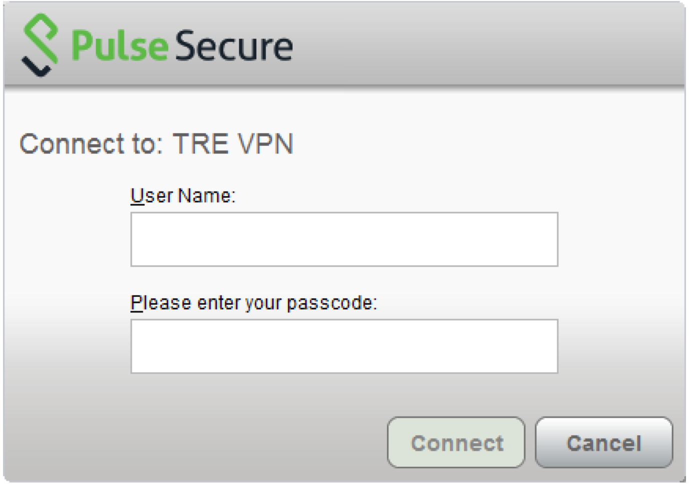
Add Connection

Type: Policy Secure (UAC) or Connect Secure (VPN)

Choose a phrase to type into the 'Name' field, for example, 'TRE VPN' (you can choose anything). The URL of the VPN server will be sent to the TRE user via email. This must be typed into the 'Server URL' field.

The connection details will be stored in the client, so they won't need to be typed in again.

To connect to the TRE VPN service, click the 'Connect' icon and the following screen will appear:

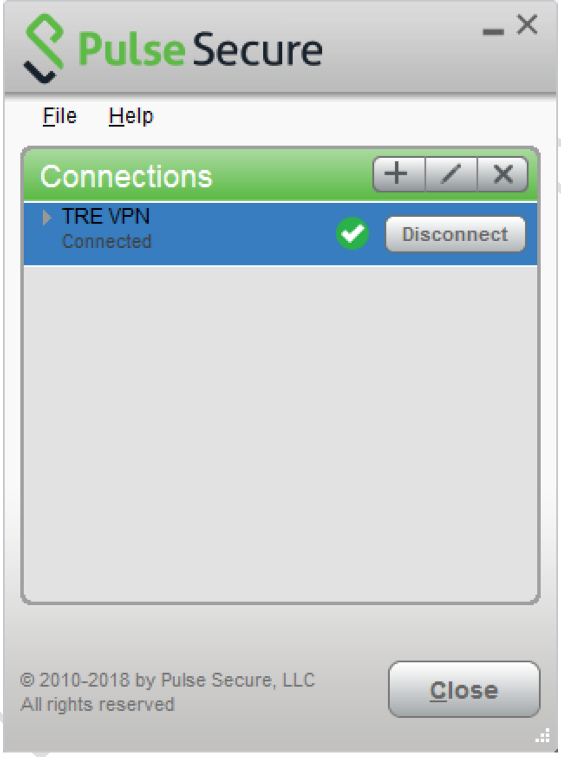


Connect to: TRE VPN

The ‘User Name’ is the same as the username you have been allocated for your standard connection to the TRE and will have been sent in an email.

When logging in for the first time, the ‘passcode’ is the 8-digit Tokencode that is generated by the RSA Securid 2-FA service (see section 3.1 for more details). Immediately after clicking ‘Connect’, the Pulse Secure client will ask for a 4-digit PIN to by chosen and typed into the pop-up box (make sure you store this number as it will be need for each subsequent connection to the VPN).

After successfully connecting to the TRE VPN, the status will be displayed as follows:



Note: Subsequent connections to the VPN will require a different passcode format (there is a comma between the two numbers, with no space characters):

```
[4-digit PIN],[8-digit RSA Tokencode]
```

For example, if you typed in ‘1234’ when prompted to create a PIN during the first connection to the VPN, and your RSA Securid app displays a Tokencode of ‘6000 7777’, then the VPN client passcode will be:

```
1234,60007777
```

4. Cross-referenced ISMS Documents

Number	Type	Title

SOP-03-16	ISMS\SOP\TRE Operations - SOP	Connecting to the TRE with X2Go

5. Appendices

None