

Fujitsu VPN Guide





Table of Contents

1. Purpose 3

2. Pulse Secure – Authenticate using MFA 4

 a. Authenticate using Microsoft Authenticator App Notification 5

 b. Authenticate using Microsoft Authenticator Password Code: 5

 c. Authenticate using Text Password Code 6

 d. Authenticate using Phone Call..... 6

 e. Authenticate using Hard Token 6

3. Change Sign-in Method 8



1. Purpose

This VPN guide has been created to assist users with accessing corporate data using Pulse Secure and MFA (Azure Multi-Factor Authentication). If you are not set up for MFA, please contact Wireless Help using the email address of wirelesshelp@fujitsu.com. For questions related to VPN, contact your Fujitsu Help Desk.

MFA Support Email Address: wirelesshelp@fujitsu.com

Connect 0365 Community Site: <https://connect.americas.fujitsu.local/it/EN/0365/Pages/MFA.aspx>

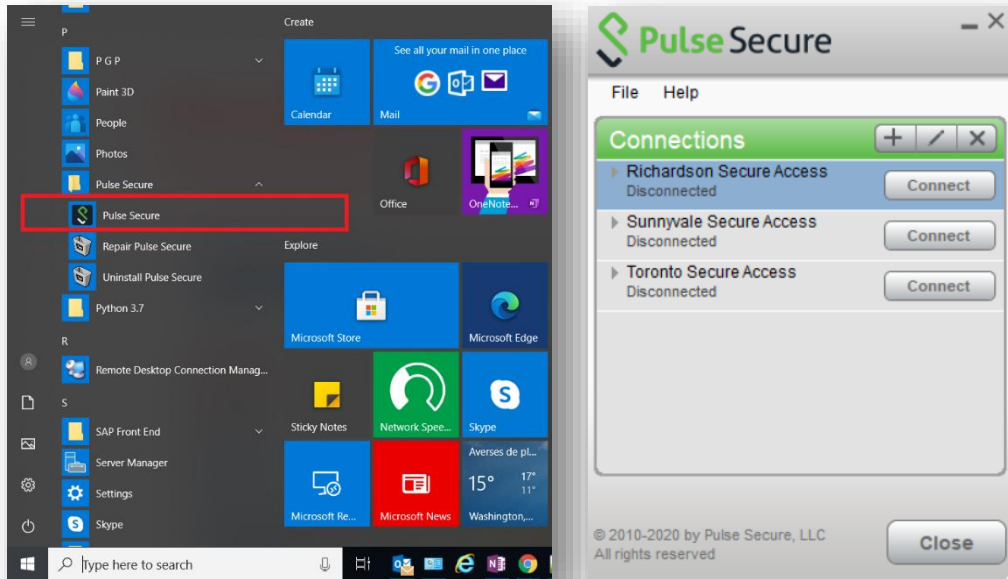
This guide is sectioned into multiple parts; please review and follow the sections that pertain to the step that you are trying to complete.

- **Pulse Secure – Authenticate using MFA (Azure Multi-Factor Authentication)**
 - Authenticate using Microsoft Authenticator App Notification
 - Authenticate using Microsoft Authenticator Password Code
 - Authenticate using Text Password Code
 - Authenticate using Phone Call
 - Authenticate using Deepnet Hard Token
- **Change Sign-in Method**

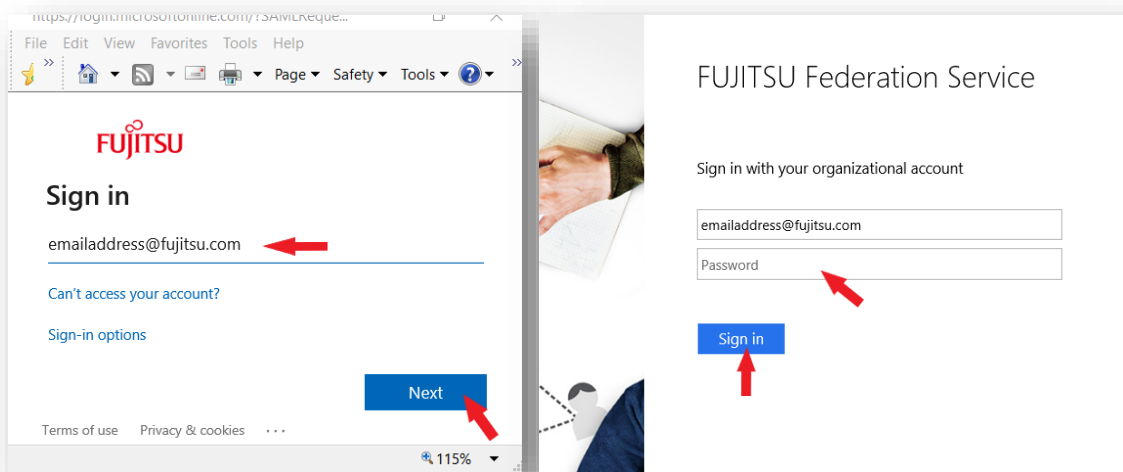


2. Pulse Secure – Authenticate using MFA

1. Please locate the Pulse Secure Client on your PC and click on your desired connection.



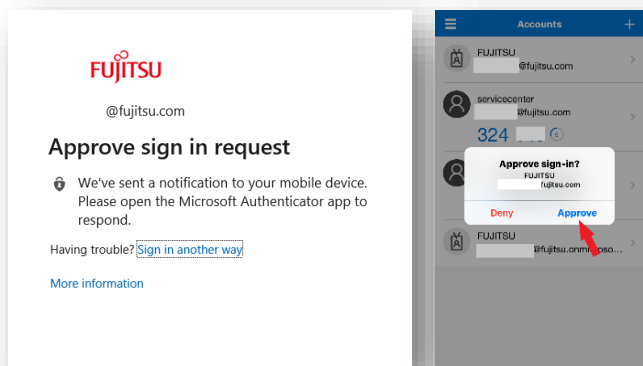
2. After clicking on the VPN connection, a web browser will open to the Microsoft Sign In Site. Please enter your Fujitsu Email Address or select your Fujitsu Email Address (already present). On the Fujitsu Federation Service Site enter your Fujitsu Password and click “Sign in”.



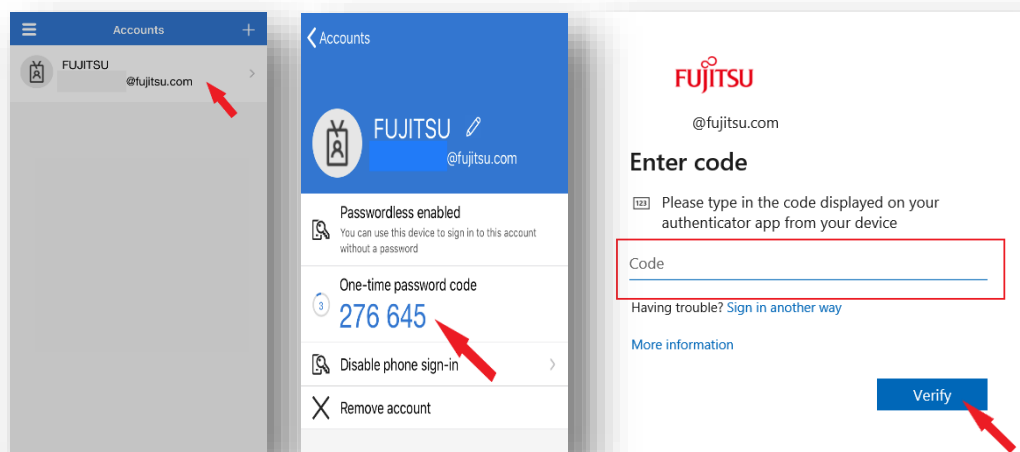


- Please review these sign-in options carefully and follow the directions that pertain to your default authentication method.

a. Authenticate using Microsoft Authenticator App Notification: Microsoft Sign In Site will display a message indicating that approval is required and a request will be sent to your Microsoft Authenticator App. Please locate your Microsoft Authenticator App on your smart phone and approve sign in.

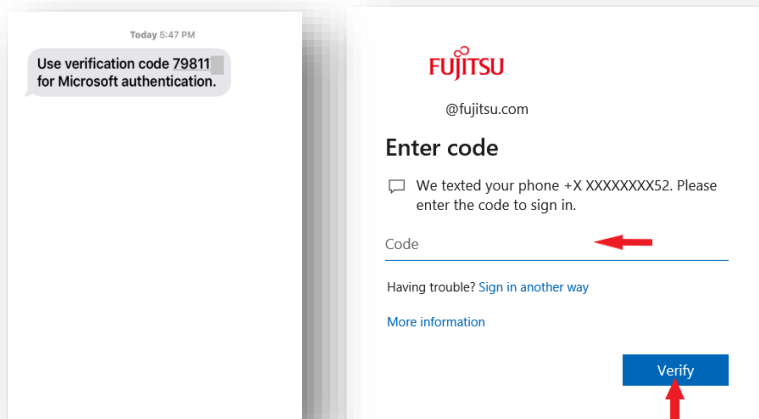


b. Authenticate using Microsoft Authenticator Password Code: The Microsoft Sign In Site will display a message indicating that it will need the code from your authenticator app. Please locate the Microsoft Authenticator App on your smart phone, then tap on your Fujitsu Account and enter the one-time password code into the Microsoft Sign In Site. Click on “Verify” after inputting the password code.

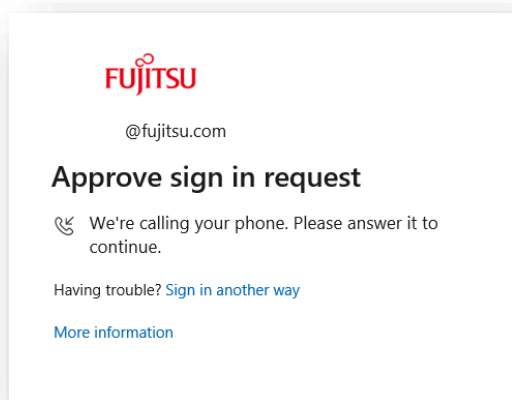




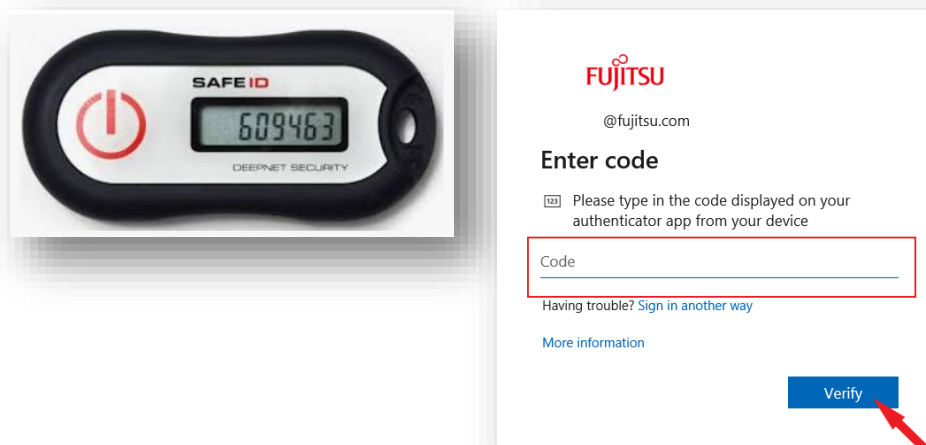
c. Authenticate using Text Password Code: The Microsoft Sign In Site will display a message indicating that a verification code has been texted to your smart phone. Please locate the verification code and input it into the Microsoft Sign In Site.



d. Authenticate using Phone Call: Microsoft will call your cell phone to verify your account. Please answer the phone call and follow the instructions. After completing the instructions the verification will be complete.

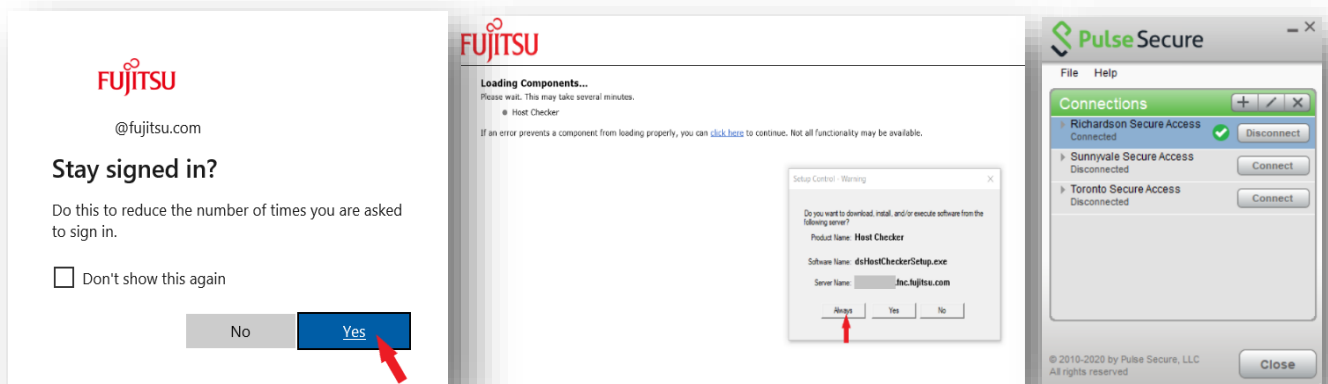


e. Authenticate using Deepnet Hard Token: The Microsoft Sign In Site will display a message indicating that it will need the code from your authenticator app. Please locate your Deepnet Hard Token and input the password code. Click on "Verify" after inputting the password code.





4. On the Microsoft Sign In Site click on “Yes” to stay signed in. Once the Host Checker Site loads and the Setup Control appears, please click on “Always”. After successful validation Pulse Secure will show the “Connected” status.



3. Change Sign-in Method

1. While using your work PC in the office or on VPN, use Chrome or IE (Do not use Firefox.) Go to <https://aka.ms/mfasetup> and sign-in with your Fujitsu email address and password. On your device that is already setup for MFA, you will receive a notification (phone call, text message or prompted by Microsoft Authenticator). Please input the PIN or accept the prompt from Microsoft Authenticator to gain access to the site.





2. On the Additional Security Verification Site, choose your default verification option and save. You will need to verify your new verification option before it becomes the default.

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
[View video to know how to secure your account](#)

what's your preferred option?

We'll use this verification option by default.

Notify me through app  

Call my authentication phone

Text code to my authentication phone

Call my office phone


Notify me through app


Use verification code from app or token

☐ Alternate authentication phone

☒ Authenticator app or Token

Set up Authenticator app

Authenticator app -  Delete

Save  cancel

Your phone number will only be used for account security. Standard telephone and SMS charges will apply.