Partner Extranet
Multi-factor authentication – MFA
Support Documentation

The implementation of Multi-factor authentication (MFA) by Fujitsu enhances security by requiring additional authentication factors, minimizing password theft, phishing attacks, and weak passwords, protecting corporate resources, complying with security standards, and ensuring the safeguarding of sensitive data.

Multi-factor authentication (MFA) is a security mechanism used to add an extra layer of protection to user accounts and systems. It requires users to provide two or more different forms of identification or evidence to verify their identity before they can access a system, application, or online service. This approach significantly enhances security compared to relying solely on a username and password for authentication.

Table of Contents

1. Introduction

From 12th November 2023, Fujitsu connected internet systems require mandatory Multi-factor authentication for each external login.

In addition we changed our password policy:

- minmum 12 characters
- password history is increased to 24
- Account logout time after 10 failed attempts is 30 minutes

Password policy

- At least 12 characters
- At least one symbol or numerical digit
- At least one uppercase and one lowercase character
- No part of your username
- No part of your first or last name
- password should be non-repeatable so cannot be any of the 24 previous used passwords.
- Fujitsu rules do not allow a password change within 24 hours of the last change.
- Account is locked for 30 minutes after 10 failed attempts.

2. Process Overview – MFA end user documentation

To enhance your account security, MFA (multi factor authentication) will be enrolled automatically once you sign in first time. In case you don't see your QR code please contact extranet@fujitsu.com and request an MFA reset.

2.1 Prepare authenticator app

You require any authenticator App to enroll your MFA passcode later in step.

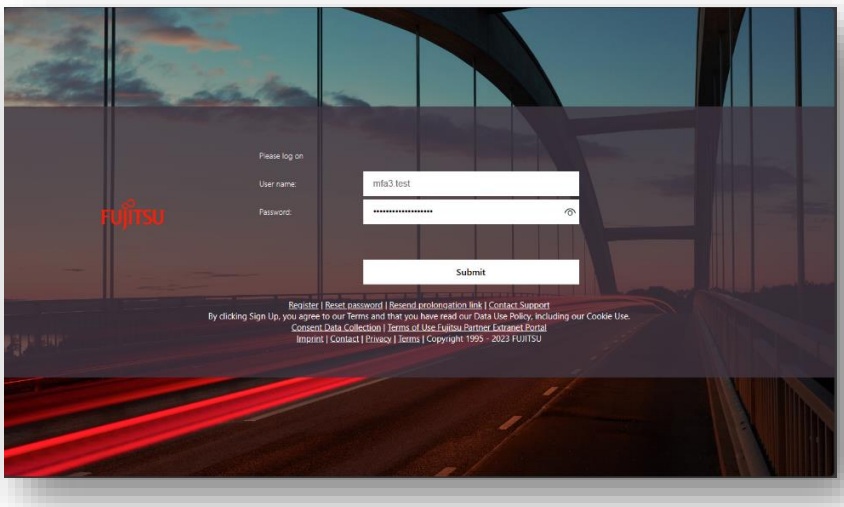
The following apps have been tested by Fujitsu:

	IOS	Android
Microsoft authenticator		
Google authenticator		
Citrix SSO		

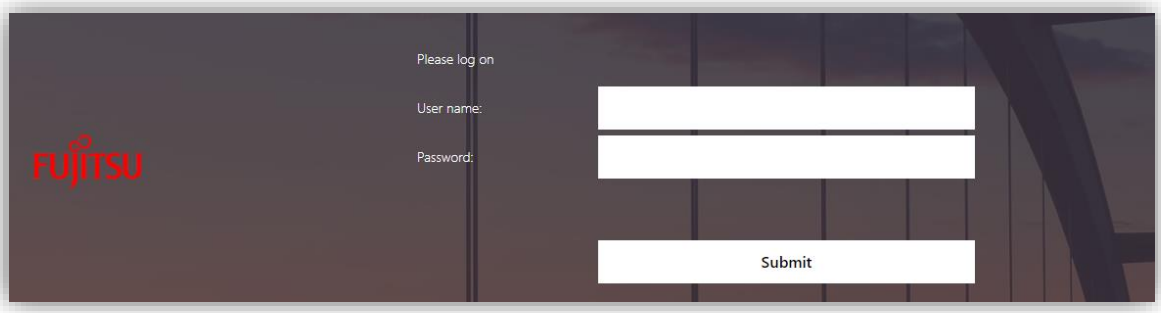
Alternative authenticator applications are described here:
https://docs.ts.fujitsu.com/dl.aspx?id=1bbad663-e8a2-4eae-92cb-77c405ae456c

2.2 Enroll Partner Extranet Multi-factor authentication - Step-by-step instruction

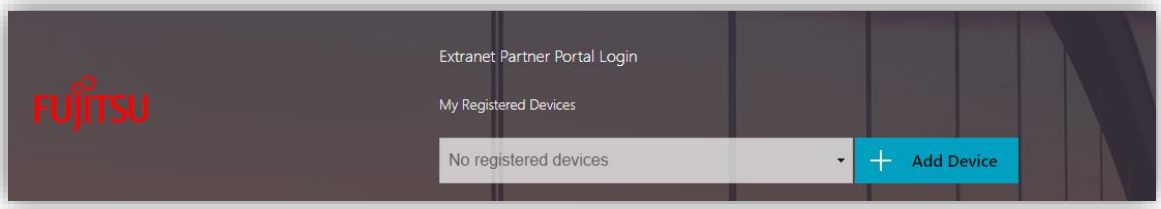
a) Enter URL https://extranet.ts.fujitsu.com



b) Login using your regular credentials (john.smith).

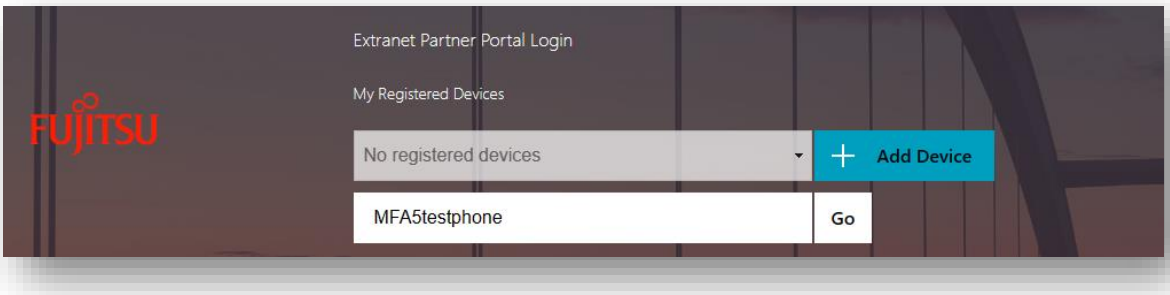


c) You can now enroll MFA - Click **Add Device**.

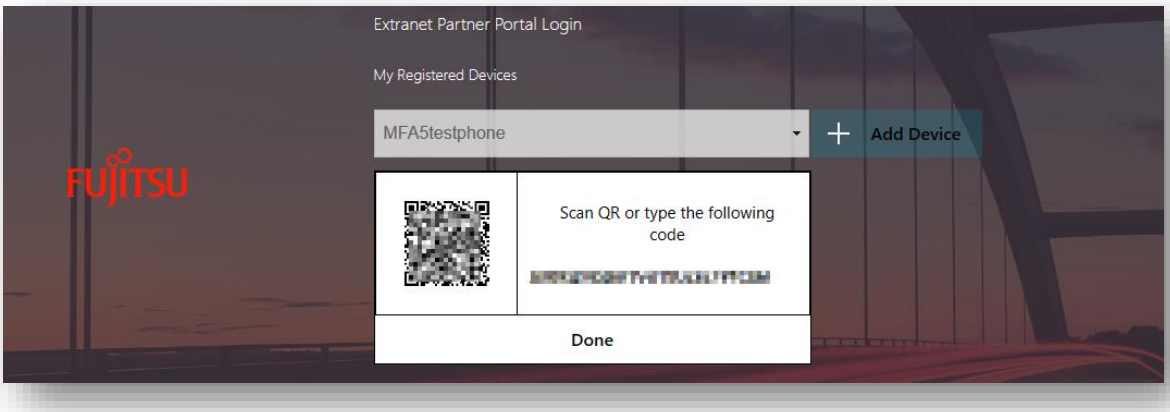


You can only enroll one device.

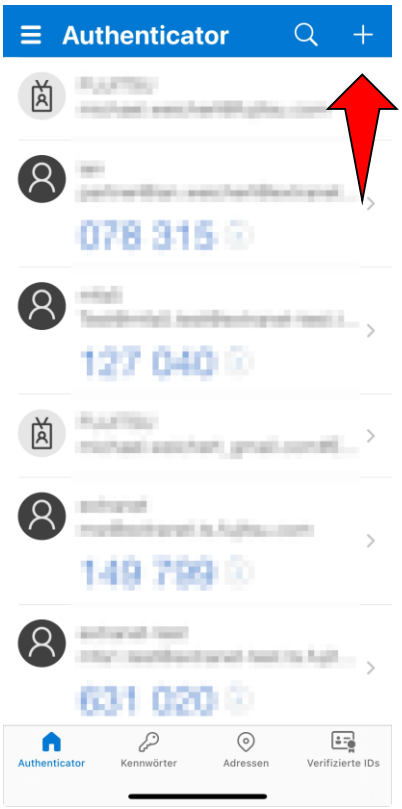
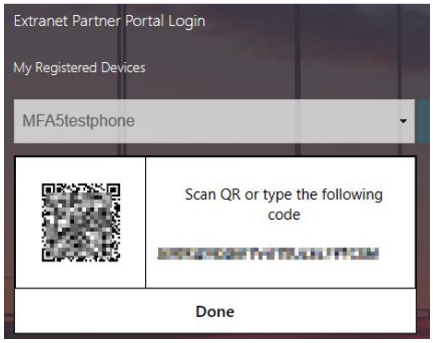
d) Enter a device name and click **Go**.

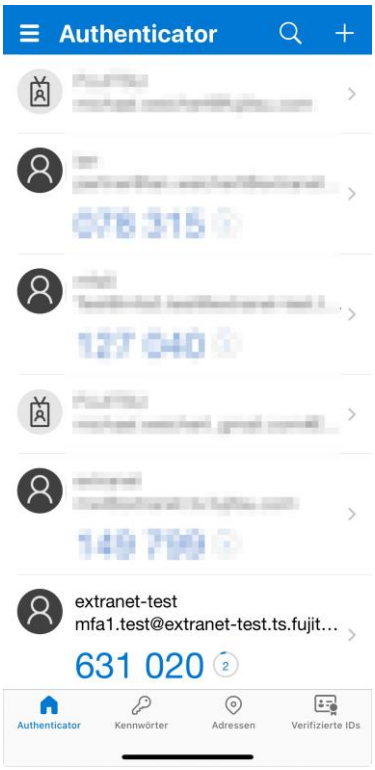
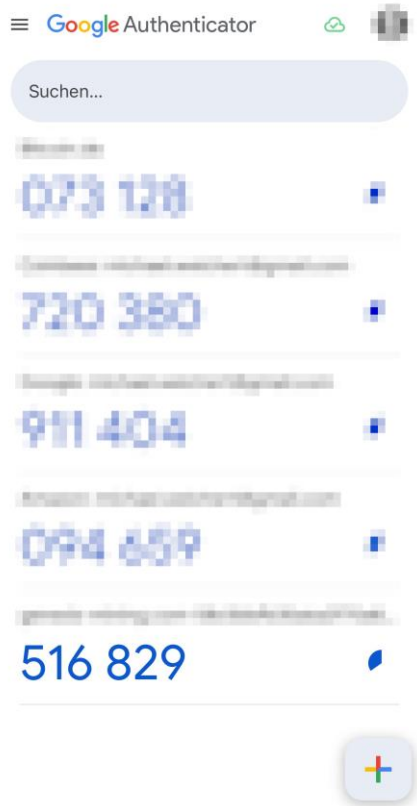
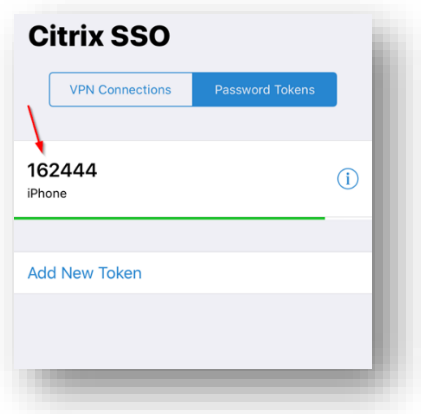


e) Scan code with your favorite authenticator app and click done



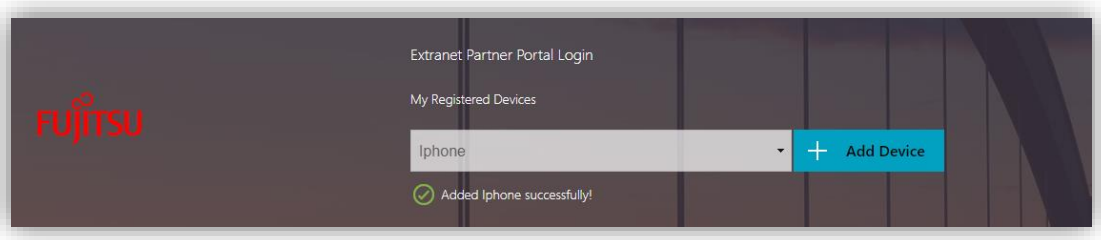
f) Authenticator Application specific enrollment instruction

<table>
<tr><th>Microsoft authenticator</th><th>Google</th><th>Citrix</th></tr>
<tr>
<td>click on right top (+) icon
 
</td>
<td>click on right bottom (+) icon
 
</td>
<td>click on “Tokens”, then on right bottom (+) icon
 
</td>
</tr>
<tr>
<td></td>
<td>Scan QR code or type in Key
 
</td>
<td></td>
</tr>
</table>

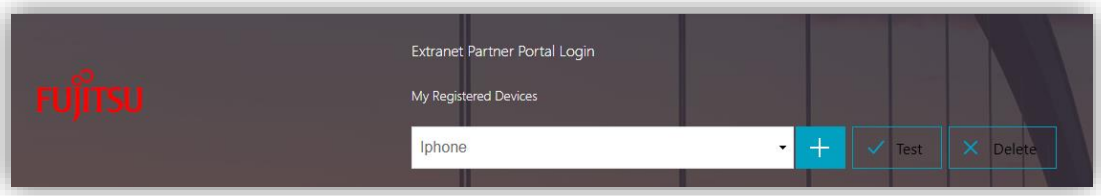
OTP password is shown in app	OTP password is shown in app	Citrix SSO app shows the passcode on the main Password Tokens view.
		

The OTP code is changing every Minute. You can't use expired codes.

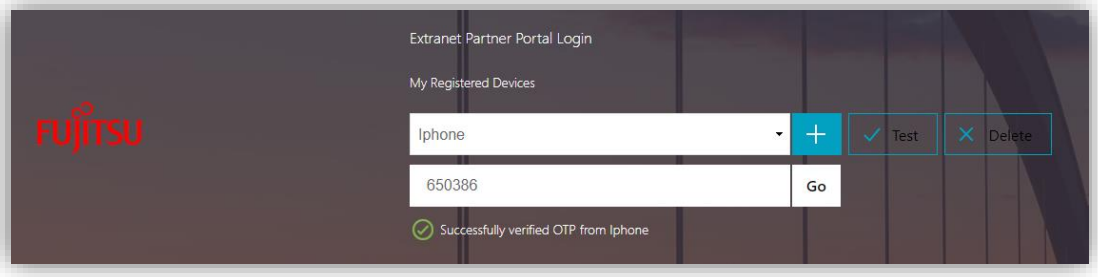
g) Optional Step: Test your one time password code
After adding your device, you will not see a **Test** button.
To display the Test button, simply refresh your browser page.



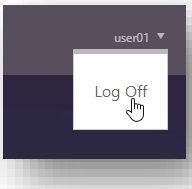
h) Click **Test**.



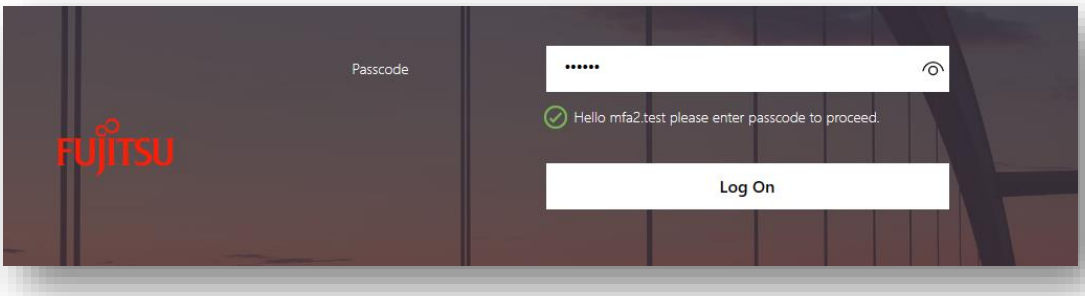
i) Enter the passcode shown in your Authenticator and click **Go**.



j) After successful verification, on the top right, click your name and **Log Off**.



k) Open https://extranet.ts.fujitsu.com and sign in with your credentials.



You will now ask to enter your second factor passcode from your authenticator app

