

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.....	2
2.	Process Overview – MFA end user documentation.....	2
2.1	Prepare authenticator app.....	2
2.2	Enroll Partner Extranet Multi-factor authentication - Step-by-step instruction.....	2

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

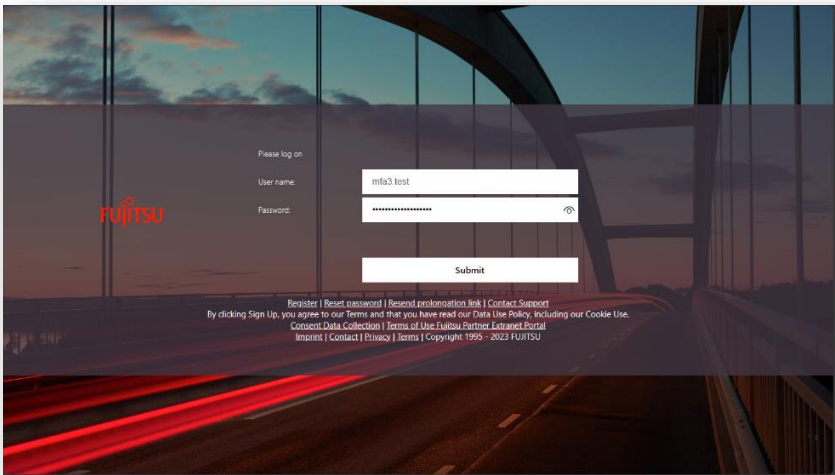
You require any authenticator App to enroll your MFA passcode later in step.
The following apps have been tested by Fujitsu:

	IOS	Android
Microsoft authenticator		
Google authenticator		
Citrix SSO		

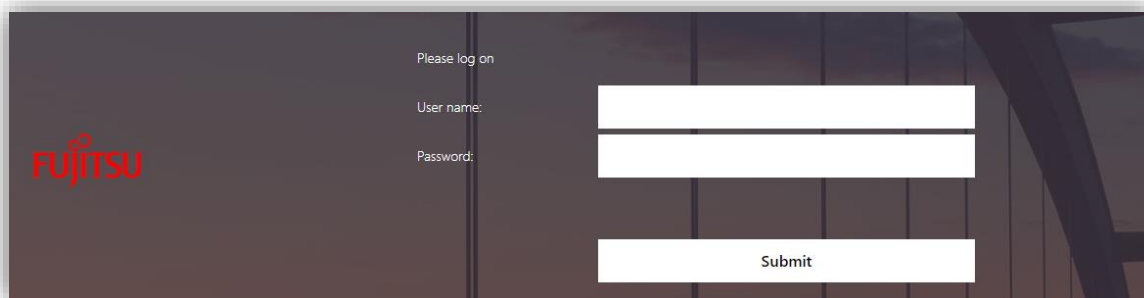
Other authenticator

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

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

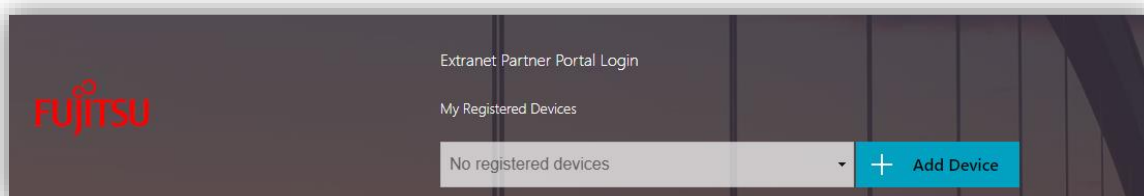


b) Login using your regular credentials (john.smith).



The screenshot shows the Fujitsu login page. On the left is the Fujitsu logo. On the right, there is a login form with the text "Please log on" above it. The form includes labels for "User name:" and "Password:" next to two white input fields. Below these fields is a white "Submit" button.

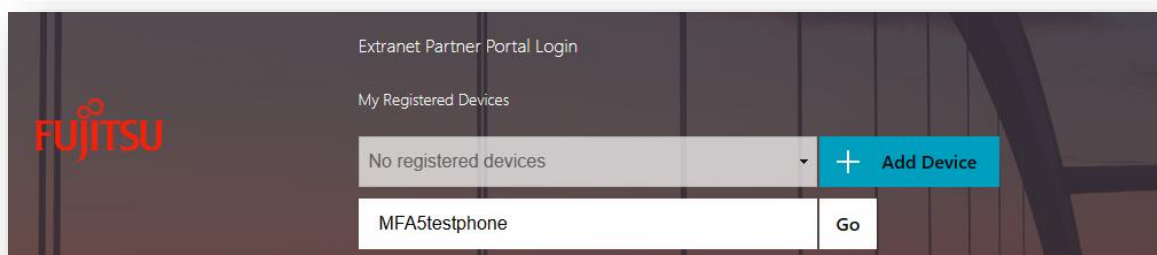
c) You can now enroll MFA - Click **Add Device**.



The screenshot shows the "Extranet Partner Portal Login" page. Under the heading "My Registered Devices", there is a dropdown menu that currently displays "No registered devices". To the right of this dropdown is a blue button with a white plus icon and the text "Add Device".

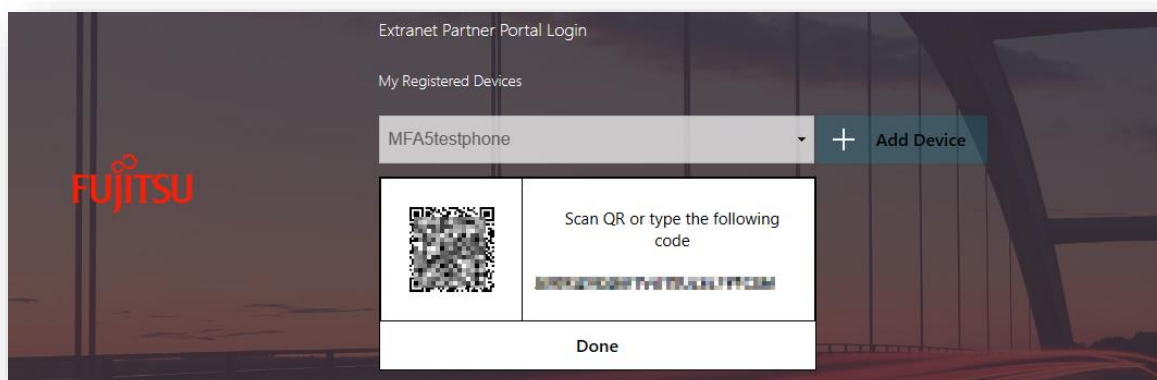
You can only enroll one device.

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



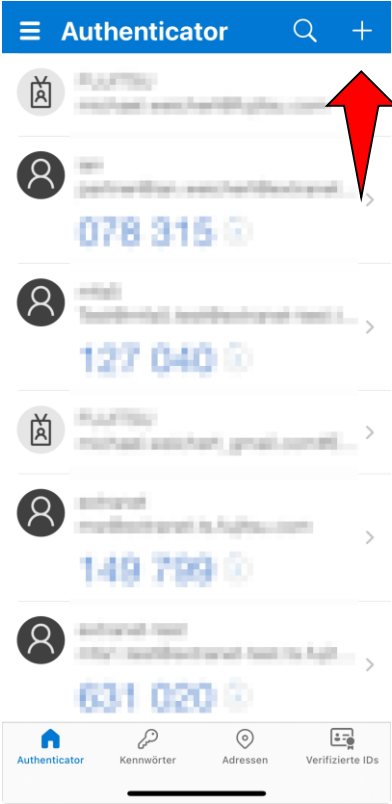
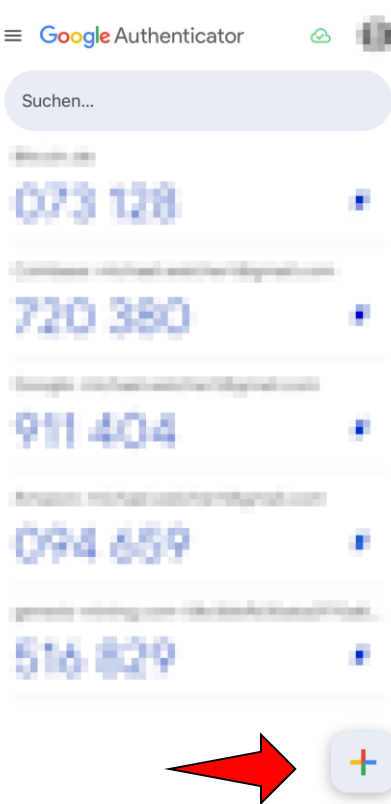

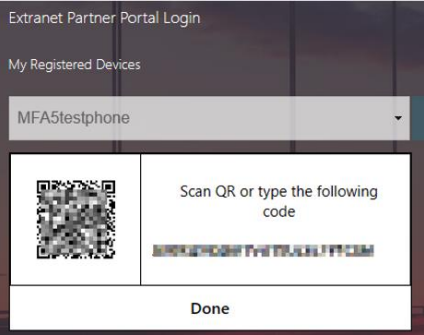
This screenshot shows the device enrollment form. The "My Registered Devices" dropdown now displays "MFA5testphone". To its right is the same "Add Device" button. Below the dropdown is a white input field containing the text "MFA5testphone". To the right of this field is a white "Go" button.

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

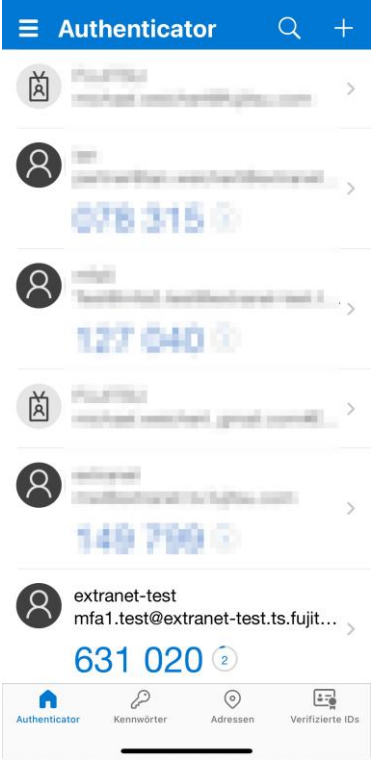


The screenshot shows the final step of device enrollment. The "My Registered Devices" dropdown still shows "MFA5testphone". A modal window is displayed in the center of the screen. On the left side of the modal is a QR code. On the right side, it says "Scan QR or type the following code" above a long, colorful alphanumeric code. At the bottom of the modal is a white "Done" button.

f) Authenticator Application specific enrollment instruction


Microsoft authenticator	Google	Citrix
<p>click on right top (+) icon</p> 	<p>click on right bottom (+) icon</p> 	<p>click on "Tokens", then on right bottom (+) icon</p> 
	<p>Scan QR code or type in Key</p> 	

OTP password is shown in app



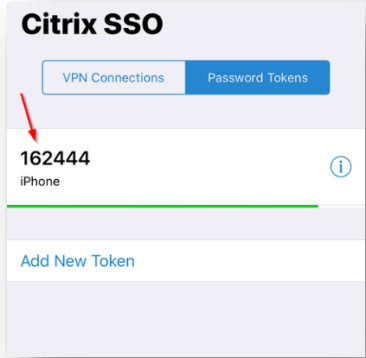
The screenshot shows the Authenticator app interface. At the top is a blue header with a menu icon, the word 'Authenticator', a search icon, and a plus icon. Below the header is a list of accounts, each with a profile icon, a name, an email address, and a large blue OTP code. The accounts listed are: 'P...@...', '...', '...', 'P...@...', '...', and 'extranet-test mfa1.test@extranet-test.ts.fujit...'. The bottom of the screen has a navigation bar with four icons: a house (Authenticator), a key (Kennwörter), a location pin (Adressen), and a document with a checkmark (Verifizierte IDs).

OTP password is shown in app



The screenshot shows the Google Authenticator app interface. At the top is a header with a menu icon, the Google logo, the word 'Authenticator', a green cloud icon, and a profile icon. Below the header is a search bar labeled 'Suchen...'. Below the search bar is a list of accounts, each with a name, a large blue OTP code, and a blue square icon. The accounts listed are: '...', '...', '...', '...', '...', and '...'. The bottom of the screen has a large blue plus icon.

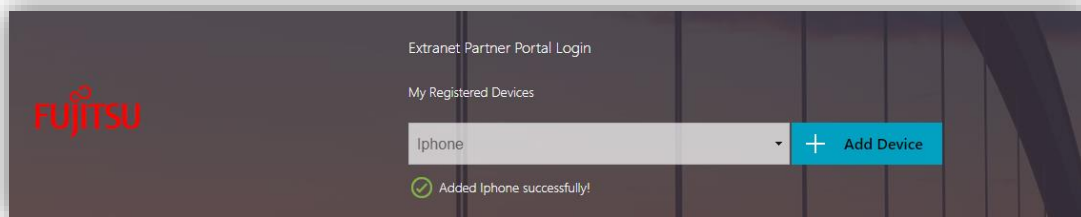
Citrix SSO app shows the passcode on the main Password Tokens view.



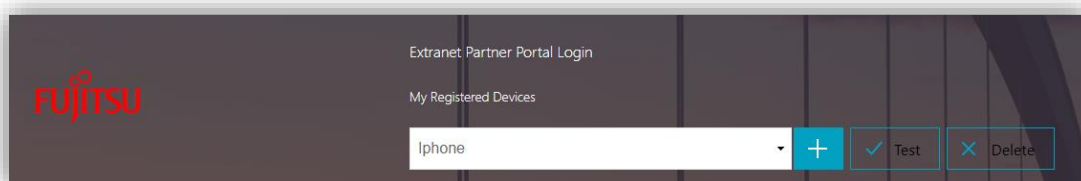
The screenshot shows the Citrix SSO app interface. At the top is a header with the word 'Citrix SSO'. Below the header are two tabs: 'VPN Connections' and 'Password Tokens'. Below the tabs is a list of tokens, each with a large blue passcode, a small blue circle with an 'i' icon, and a blue link labeled 'Add New Token'. The token listed is '162444 iPhone'.

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

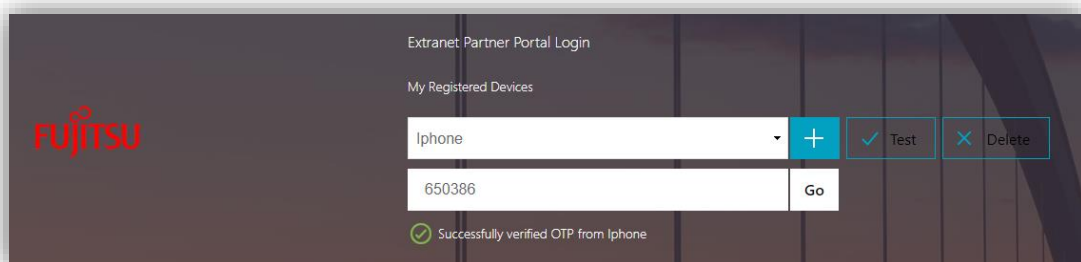
- g) Optional Step: Test your one time password code
After adding your device, you will not see a **Test** button.
To display the Test button, simply refresh your browser page.



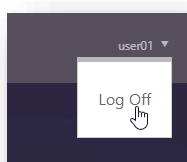
- h) Click **Test**.



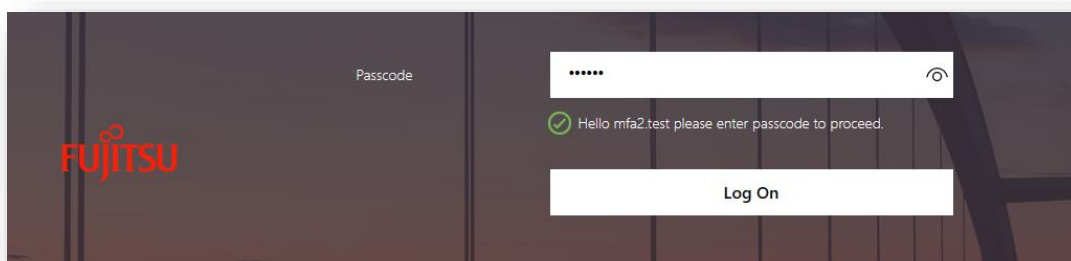
- i) Enter the passcode shown in your Authenticator and click **Go**.



- 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