

SAMSUNG

SAMSUNG MFA **USER GUIDE**

SAMSUNG MFA USER GUIDE

01

User Registration

SAMSUNG MFA USER GUIDE

WEB

1 Samsung Electronics Multi-factor Authentication Portal

Welcome to the Samsung Multi-factor Authentication Portal.
To access Samsung's major systems, You must complete
registration for using multi-factor authentication.

Please press the 'Start' button to proceed with registration.

2

Getting started

© SAMSUNG

Samsung's multi-factor authentication is a two-step security feature that protects your account in addition to your username and password. We provide additional authentication using the mobile app, SMS or EMAIL.

- 1** When you log in to the system that uses MFA for the first time, the 2-step verification registration screen is displayed.
- Click the 'Getting started' button to go to the app connection page

WEB

STEP 1
Please select an authentication method.

[Authentication Method 1] Mobile App

Please install the mobile app first. Run the installed app and click on the arrow to move on to the app registration step. After registering APP, one e-mail must be registered.

Can't find the app?
Please enter your mobile number to receive the URL via SMS.
UNITED STATES [Get installation URL](#)

QR Scan
1. Scan code on the left with QR code scanner
2. Install automatically by moving to the store

Android
Search and install 'SEC.MFA' from Google Play

iOS
Search and install 'SEC.MFA' from the App Store

[MFA Guide for Users in China](#)

[Authentication Method 2] SMS, EMAIL

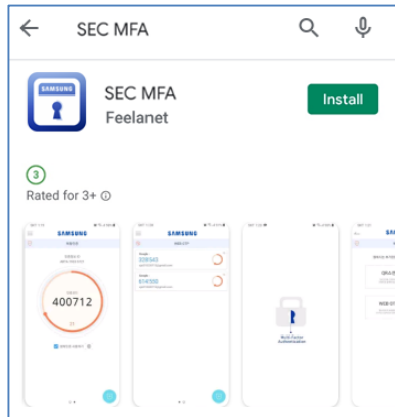
If mobile app is not available or cannot be installed, you can authenticate with SMS or EMAIL.
We recommend using App Push / App OTP / Public Personal e-mail as it may be difficult to receive SMS depending on the local carrier situation.

[Register SMS or EMAIL](#)

- 1 "Using the app"
When registering through the app, click on the arrow in [Authentication Method 1] to go to the mobile app connection page.
- 2 "Using SMS or EMAIL"
When using SMS or e-mail without registering through the app, click the "Register SMS or EMAIL" button in [Authentication Method 2] to go to user information registration page.

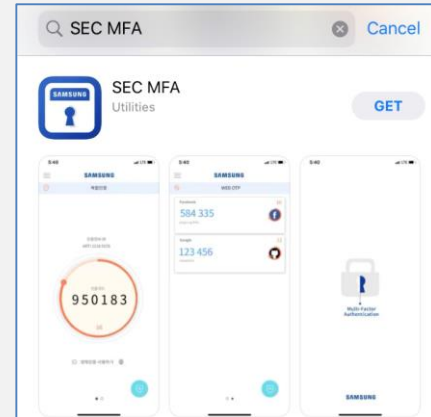
Android

- 1 Launch Google Play
- 2 Search and install 'SEC MFA'



IOS

- 1 Launch App Store
- 2 Search and install 'SEC MFA'



QR Scan

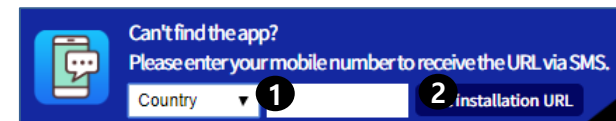
- 1 Scan the code below with QR code scanner
- 2 Go to the installation page and install 'SEA MFC'



Install SEC MFA app on your device

SMS

- 1 Enter your country code and mobile number to receive the installation URL.
- 2 Click the 'Get Installation URL' button.
- 3 Install app by accessing the URL.



SMS

SEC MFA Android APP
Google Play
*Url - <https://bit.ly/SRE4AbkQ> -

SEC MFA Android APP
Download .apk file directly
*Url - <https://bit.ly/2PDR1VW> -

WEB



STEP 2
Please register the APP.

User account
mfa.sec2@samsung.com

Authentication ID
Please enter the 12-digit alphabetic and numeric characters that appear in the mobile APP without spaces.

1

Verification code
Please enter the 6-digit verification code shown on the mobile APP in 90 seconds.
If you time out, please enter the new verification code.


2

3


In order to log in in case of phone change or loss,
user registration is completed only by registering at least one email in the next step.

- 1** Check the 12-digit authentication ID from the installed app.
Enter the ID in the Credential ID field.
- 2** Enter the verification code displayed on the app.
(Verification code changes every 30 seconds.)
- 3** Click the 'Next' button to go to app user information registration page.

WEB

1  **STEP 3**
Please check your user information.

- It is recommend using **App Push / App OTP / Public Personal e-mail** as it may be difficult to receive SMS depending on the local carrier situation.
- In order to log in in case of phone change or loss, **user must register at least one email.**
- You can register up to 2.




SMS information (1) +Add SMS

82-01026126441

KOREA(▼) 01026126441 Certification request

401170 Certification

Verified.



EMAIL Information (1) +Add EMAIL

mfa.sec2@samsung.com

mfa.sec2 @ samsung.con Input direct ▼

Certification request

401170 Certification

Verified.

2 Confirm

- 1** SMS number / public email address to receive temporary code You must register.
Once your SMS number or email address has
- 2** been added, click the 'Confirm' button to complete the registration

[How to add SMS number]

Enter your mobile number >

Click the 'Request Authentication' button >

Enter the verification code received with the entered mobile number in the field >

Click the 'Certification' button.

[How to add email address]

Enter your e-mail address >

Click the 'Certification request' button >

Enter the verification code received with the entered e-mail address in the field >

Click the 'Certification' button.

- SMS may not be received depending on the local carrier situation, so it is recommended to register **the push app / app OTP / public personal email**.
- Register your public personal e-mail so that you can log in even if APP or SMS authentication is not available due to lost mobile phone.

02

Multi-Factor Authentication Login

SAMSUNG MFA USER GUIDE

WEB

2

ID verification

Login request has been sent to the mobile devices.
(Mobile: ARTI05438399)
Please approve the request on your device to complete the login.

CORPAD

ID : mfa.sec2@samsung.com

3

MOBILE



Registration Approval

Approval is required to complete
the multi-factor authentication.
Do you want to accept user registration?

4



Approved



Cancel

- 1 First, login to the work system you want to access.
- 2 The ID Confirmation page for secondary authentication is displayed.
- 3 Check push notifications for the app on your registered mobile device.
- 4 Launch the app and touch the 'Approve' button. (Approval notification is valid for 90 seconds.)
- 5 Once the approval is completed, you will be able to log in to the work system.

WEB

2

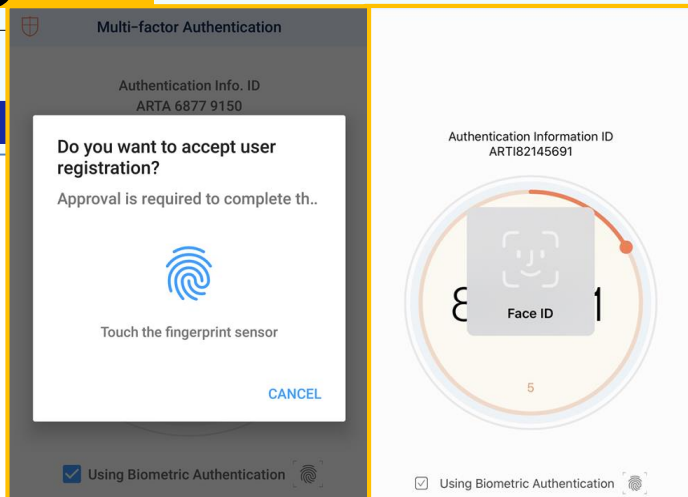
ID verification

Login request has been sent to the mobile devices.
(Mobile: ARTI05438399)
Please approve the request on your device to complete the login.

CORPAD

ID : mfa.sec2@samsung.com

5 MOBILE



- 1 Check 'Use Biometric Authentication' on the registered mobile device.
- 2 First, login to the work system you want to access.
- 3 The ID Confirmation page for secondary authentication is displayed.
- 4 Check push notifications for the app on your registered mobile device.
- 5 Launch the app to proceed with biometric authentication.
(Android – Fingerprint Authentication / iPhone – Face ID)
- 6 Once the approval is completed, you will be able to log in to the work system.

WEB

The screenshot displays the MFA login process on a web interface. It is divided into two main sections: 'Select user authentication method' and 'Certification number input'.

Select user authentication method: This section prompts the user to 'Please select the method you would like to verify from below.' It features four options: 'PUSH authentication' (with a smartphone icon), 'OTP authentication' (with a lock icon), 'EMAIL authentication' (with an envelope icon), and 'SMS authentication' (with a smartphone and message icon). A black circle with the number '4' is positioned over the 'OTP authentication' button.

Certification number input: This section prompts the user to 'Please enter the OTP code displayed in the Multi-Factor Authentication app within the valid time.' It includes a sample OTP: '(OTP : ART105438399)' and a note: 'If you do, you will need to re-enter your newly issued verification code.' Below this, the user's ID is shown as 'ID : mfa.sec2@samsung.com'. A row of six input fields is provided for the OTP code, with a black circle and the number '6' over the first field. A 'MOBILE' label is placed above the input fields. A black circle with the number '7' is positioned over the 'Code Verification' button. At the bottom, there is a 'Can't use OTP?' link and an 'Authenticate in another way' button.

MOBILE App Screenshot: An inset shows the 'Multi-factor Authentication' app interface. It displays 'Authentication Info. ID ARTA 3578 6444' and a 'Verification Code' of '999749'. A black circle with the number '5' is over the code, and a '10' timer is at the bottom.

- 1 First, login to the work system you want to access.
- 2 The ID Confirmation page for secondary authentication is displayed.
- 3 Click the 'Authenticate in another way' button.
- 4 Click the 'OTP Authentication' button.
- 5 Launch the app.
- 6 Enter the OTP code displayed on the app screen in the code field.
- 7 Click the 'code verification' button to log in to the work system.

WEB

The screenshot displays the MFA login process on a web interface. It is divided into two main sections. The top section, titled "Select user authentication method", prompts the user to choose a verification method from four options: PUSH, OTP, EMAIL, and SMS. The "EMAIL authentication" option is highlighted with a blue circle and a black number 4. The bottom section, titled "Certification number input", informs the user that an authentication request has been sent to their email (EMAIL: rukas20**@gmail.com) and asks them to enter a 6-digit verification code. The user's ID is shown as mfa.sec2@samsung.com. A row of six input boxes is provided for the code, with the first box highlighted by a black number 6. Below the input boxes is a "Code Verification" button, also highlighted with a black number 7. A circular timer in the bottom right corner shows 04:55. At the bottom of the interface, there are three buttons: "Resend", "Authenticate in another way", and "MFA User Portal".

Select user authentication method

Please select the method you would like to verify from below.

PUSH authentication

OTP authentication

EMAIL authentication

SMS authentication

© SAMSUNG

Certification number input

Authentication request has been sent by email.
(EMAIL : rukas20**@gmail.com)

Please enter your 6-digit verification code sent to your email within the time limit.

ID : mfa.sec2@samsung.com

6

7 Code Verification

04:55

Didn't receive an authentication request?

Resend Authenticate in another way MFA User Portal


5 **【SEC MFA】** Use this One Time Password to validate your log in:[780534]


- 1 First, login to the work system you want to access.
- 2 The ID Confirmation page for secondary authentication is displayed.
- 3 Click the 'Authenticate in another way' button.
- 4 Click the 'E-mail Authentication' button.
- 5 Check the verification e-mail sent to the registered e-mail address.
- 6 Enter the verification code shown in the e-mail in the code field.
- 7 Click the 'code verification' button to log in to the work system.


WEB


Select user authentication method

Please select the method you would like to verify from below.


PUSH
authentication


OTP
authentication


EMAIL
authentication


SMS
authentication

© SAMSUNG

Certification number input

Authentication request has been sent by your mobile.
(SMS: 82-*****3606)

Please enter your 6-digit verification code sent to your mobile within the time limit.

ID : mfa.sec2@samsung.com

6

-

-

-

-

Code Verification

03:28

Didn't receive an authentication request?

7

Re...

Authenticate in another way

MFA User Portal

5 SMS

[Web발신]
【SEC MFA】 Use this One Time Password
to validate your log in:[701175]

- 1 First, login to the work system you want to access.
- 2 The ID Confirmation page for secondary authentication is displayed.
- 3 Click the 'Authenticate in another way' button.
- 4 Click the 'SMS Authentication' button.
- 5 Check the verification text sent to the registered number.
- 6 Enter the verification code shown in the text into the code field.
- 7 Click the 'code verification' button to log in to the work system.

WEB

ID : mfa.sec2@samsung.com

1 1 1 1 1 1


1

❌ Verification code do not match
If it doesn't match 5 times, your account will be locked for 5 minutes, limiting your logon. (Number of attempts: 1 / 5)

Code Verification

2

Account lockout notification



3 Account mfa.sec2@samsung.com is temporarily locked
until Today at 10:34 AM due to authentication failure.

* If it is not due to your own authentication failure, please report it to the Security Department.

- 1 If you enter the wrong authentication code, a lock guide will be displayed.
- 2 If the authentication code is incorrect 5 times in a row, MFA authentication is locked for security.
- 3 The authentication lock is held for 5 minutes and is automatically unlocked after 5 minutes.
- 4 If authentication is successful, the account failure count is reset.

03

Authentication Method

SAMSUNG MFA USER GUIDE

WEB

1 System with MFA

ID :

PW :

2

3 ID verification

Login request has been sent to the mobile devices.
(Mobile: ART109712100)
Please approve the request on your device to complete the login.

CORPAD

ID : mfa.sec2@samsung.com

4

Welcome to Samsung's Multi-factor Authentication site.
Please select the type of multi-factor authentication method you want to use.
(If you click ★, it will be registered as a preferred option for convenience.)

 PUSH 1 registration(s)	 OTP authentication 1 registration(s)	 SMS authentication 1 registration(s)	 EMAIL 1 registration(s)	 Temporary code You can receive a temporary OTP code via registered SMS or EMAIL.
-------------------------------	---	---	--------------------------------	---

Authentication Information List

- 1 First login to the system you want to access.
- 2 Click the 'MFA User Portal' button on the composite authentication standby screen.
- 3 The User Portal Secondary Authentication page is displayed in a separate browser window.
- 4 When authentication is completed using the previously registered method, the user portal home is displayed.

❖ If you are using a separate Client authentication other than WEB, please enter the User Portal URL in your browser to access it User portal .

User portal URL : <https://mfa.secsso.net>

WEB

2 ID verification

Login request has been sent to the mobile devices.
(Mobile: ARTI09712100)
Please approve the request on your device to complete the login.

CORPAD

ID : mfa.sec2@sams

Select user authentication method

Please select the method you would like to verify from below.



PUSH



OTP



EMAIL



SMS

Didn't receive a authentication request?

Resend

Authenticate in another way

Welcome to Samsung's Multi-factor Authentication site.

Please select the type of multi-factor authentication method you want to use.
(If you click ★, it will be registered as a preferred option for convenience.)



PUSH

1 registration(s)



OTP authentication

1 registration(s)



SMS authentication

1 registration(s)



EMAIL

1 registration(s)



Temporary code

You can receive a temporary OTP code via registered SMS or EMAIL.

4

Authentication Information List

Please input search keyword.

Keyword

Search

5

	AuthType	Method info.	Created
<input type="checkbox"/>	APP	arti67127800	2020-04-23
<input type="checkbox"/>	SMS	82-01026126441	2020-04-16
<input type="checkbox"/>	Email	mfa.sec2@stage.samsung.co	2020-04-16


6


Add APP Add SMS Add Email Delete


- 1 Connect to the user portal.
- 2 The secondary authentication screen is displayed.
- 3 If the authentication method is Push authentication or OTP, click Authentication as another method to change the authentication method. (Email, SMS, etc.)
- 4 Click the "Authentication Information List" button on the user portal home.
- 5 Select and delete the existing registered APP information.
- 6 Add APP.
(Refer to Adding APP page)


WEB


3 Welcome to Samsung's Multi-factor Authentication site.
Please select the type of multi-factor authentication method you want to use.
(If you click ★, it will be registered as a preferred option for convenience.)


PUSH
1 registration(s)


OTP authentication
1 registration(s)


SMS authentication
1 registration(s)


EMAIL
1 registration(s)


Temporary code
You can receive a temporary OTP code via registered SMS or EMAIL.

4 Authentication Information List

Keyword

Please input search keyword.

Search

5

	AuthType	Method Info.	Created
<input type="checkbox"/>	APP	arti67127800	2020-04-23
<input type="checkbox"/>	SMS	82-01026126441	2020-04-16
<input type="checkbox"/>	Email	mfa.sec2@stage.samsung.com	2020-04-16

6 Add APP Add SMS Add Email Delete

- 1 Log in to the User. Portal.
- 2 The authentication page for secondary authentication is displayed.
- 3 When authentication is complete, the User Portal Home is displayed.
- 4 Click the 'Authentication Information List' button.
- 5 The registered mobile number, e-mail address, and app registration status are displayed.
- 6 You can add or delete authentication methods from the authentication information list.
(Public Personal email registration is recommended to issue temporary authentication code)

WEB

Keyword

Please input search keyword.

<input type="checkbox"/>	AuthType	Method Info.	Created
<input type="checkbox"/>	APP	arti67127800	2020-04-23
<input type="checkbox"/>	SMS	82-01026126441	2020-04-16
<input type="checkbox"/>	Email	mfa.sec2@stage.samsung.com	2020-04-16

Add APP

Authentication ID
Enter the 12-digit alphabetic and numeric characters that appear in the mobile APP without spaces.

Verification code
Please enter the 6-digit verification code shown on the mobile APP in 90 seconds.
If you time out, please enter the new verification code.

[Wondering how to install the app?](#)

- 1 Log in to the User Portal.
- 2 Click the Authentication Information List' button.
- 3 Click the 'Add APP' button.
- 4 Run the app you want to add and check the verification code.
- 5 Enter your verification ID and verification code in the fields.
- 6 Click the 'confirm' button.
- 7 The added app information can be checked from the list.

WEB

Keyword

Please input search keyword.

<input type="checkbox"/>	AuthType	Method Info.	Created
<input type="checkbox"/>	APP	arti67127800	2020-04-23
<input type="checkbox"/>	SMS	82-01026126441	2020-04-16
<input type="checkbox"/>	Email	mfa.sec2@stage.samsung.com	2020-04-16

Add SMS

UNITED S

- 1 Log in to the User Portal.
- 2 Click the Authentication Information List' button.
- 3 Click the 'Add SMS' button.
- 4 Enter the number you want to add.
- 5 Click the 'Certification request' button.
- 6 Check the verification code from the authentication text sent to the registered number.
- 7 Enter the verification code in the field.
- 8 Click the "Certification" button.
- 9 The added number can be checked from the list.

WEB

The screenshot displays the 'WEB' interface for adding an email. At the top, there is a search bar with the placeholder text 'Please input search keyword.' and a green 'Search' button. Below this is a table titled 'Authentication Information List' with columns: 'AuthType', 'Method Info.', and 'Created'. The table contains three rows: 'APP' (method: arti67127800, created: 2020-04-23), 'SMS' (method: 82-01026126441, created: 2020-04-16), and 'Email' (method: mfa.sec2@stage.samsung.com, created: 2020-04-16). Below the table are buttons for 'Add APP', 'Add SMS', 'Add Email' (circled with a black circle and the number 3), and 'Delete'.

Below the table is a modal window titled 'Add EMAIL'. It contains the following fields and buttons:

- Field 4: Email address input field.
- Field 5: 'Input direct' dropdown menu.
- Field 6: 'Certification request' button.
- Field 7: 'Certification number input' field.
- Field 8: 'Certification' button.
- 'Close' button at the bottom right.

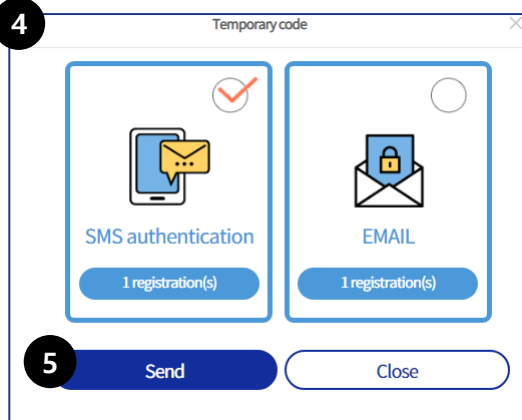
- 1 Access the User Portal.
- 2 Click the Authentication Information List' button.
- 3 Click the 'Add Email' button.
- 4 Enter the e-mail address you want to add.
- 5 Click the 'Certification request' button.
- 6 Check the verification code from the e-mail sent to the registered e-mail address.
- 7 Enter the verification code in the field.
- 8 Click the "Certification" button.
- 9 The added e-mail can be checked from the list.

04

Temporary Code Issuance

SAMSUNG MFA USER GUIDE

WEB



- 1 Log in to the User Portal.
- 2 Click the 'Temporary Code' button.
- 3 Mobile number or e-mail address that can be issued with a temporary code is displayed.
- 4 Select your mobile number or email address to receive the verification code.
- 5 Click the 'Send' button to send the temporary code.
- 6 Enter the sent code into your work system to get authenticated.

05

WEB OTP Management

SAMSUNG MFA USER GUIDE

MOBILE



3

Multi-factor Authentication

Please select your preferred verification method.

QR scan

Scan the QR code and you will be automatically registered.

WEB OTP

Register by entering OTP code through website and SNS.

QR Scan

QR scan

Position the QR code in the center of the screen to focus on the QR code.

Registration key

WEB OTP service registration

Service name (★)

Account

Registration Key (★)

Adding service(s)

Samsung multi-factor authentication app allows you to add OTP service of public websites.

(Facebook, GitHub, twitter etc.)

[Add OTP Service by QR Scan]

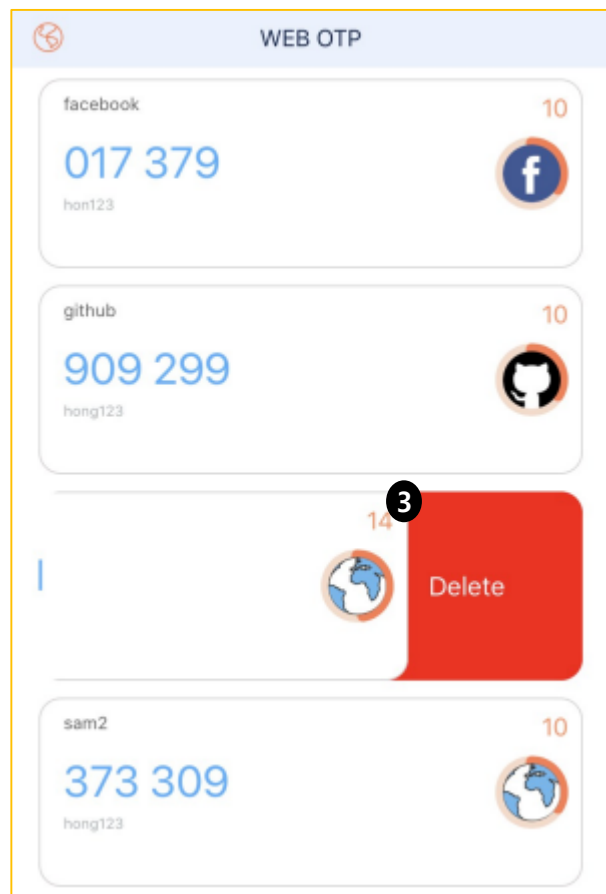
- 1 Launch Samsung Multi-factor Authentication app.
- 2 Touch the '+' button on the bottom right.
- 3 Touch the 'QR Scan' button.
- 4 Scan the QR code of the OTP service to add.

[Add OTP service with OTP registration key]

- 1 Launch Samsung Multi-factor Authentication app
- 2 Touch the '+' button on the bottom right.
- 3 Touch the 'WEB OTP' button.
- 4 Enter the service name / account / registration key.
- 5 Touch the 'Add Service' button.

※QR code of user registration page and user portal is QR code for APP installation.

MOBILE



Samsung multi-factor authentication app allows you to add OTP service of general websites.

[Confirm OTP code to use]

- 1 Launch Samsung Multi-factor Authentication app.
- 2 Swipe the screen to go to the WEB OTP list.
- 3 You can check the service name, account and OTP code in the WEB OTP list.

[Delete WEB OTP]

- 1 Launch Samsung Multi-factor Authentication app.
- 2 Swipe the screen to go to the WEB OTP list.
- 3 Drag the WEB OTP service item to be deleted to the left.

06 FAQ

SAMSUNG MFA USER GUIDE

Q I lost my phone. How can I use multi-factor authentication?

A Depending on the system where the multi-factor authentication is applied, in case of general web / mobile system that is not a VPN connection client, authentication can be performed using a different authentication method. Click the "Authenticate by other method" button on the multi-factor authentication screen and change the authentication method by SMS or E-mail. On the multi-factor authentication screen, click the "Authenticate in another way" button and change the authentication method by SMS or email. Considering this situation, it is necessary to register SMS and public email in advance.

Q Do I have to register for SMS or e-mail authentication?

A Although not required, you will not be able to get push authentication if your phone is lost or not available. In this case, you can be issued a verification code via SMS or public e-mail through the "Authenticate in another way" function. Therefore, for this situation, SMS and public e-mail must be registered in advance.

Q What should I do if I change my phone?

A If you have registered additional authentication methods such as Email, you must register a new APP using the following procedure.

1. Log on to a service that requires Multi-Factor Authentication (MFA), such as RBS.
2. On the Multi-Factor Authentication standby screen, click the '[MFA User Portal](#)' button.
3. A separate browser window appears and accesses the 'MFA User Portal'.
4. Since APP PUSH is sent to the phone you have previously, you need to change the authentication method by clicking the '[Authenticate in a another way](#)' button.
5. Select E-mail to receive the passcode and complete Multi-Factor Authentication.
6. Click the '[Authentication Information List](#)' button at the bottom of the screen.
7. Select '[APP](#)' registered from the list and '[Delete](#)'.
8. Click the '[Add APP](#)' button to register the app.
9. If you click on '[Wondering how to install the app?](#)', You will be guided how to install the APP.

If additional authentication methods are not registered,
You cannot log on to the MFA User Portal, so follow the steps below.

1. Send a multi-factor authentication reset request email to mfa.sec@samsung.com through your **Knox email**. (Working hours 9:00 AM~6:00PM KST)
2. If you do not have a Knox email, please apply through **Samsung Electronics' employees**.
3. When you receive a reply to the reset completion email, you can register a new Multi-Factor Authentication.

Let's register public personal e-mail in advance so that you can log on even if the phone is changed or lost.

Q How do I register an public personal email?**A** In order to register additional Emails, access to the MFA user portal is required.

1. Log on to a service that requires Multi-Factor Authentication (MFA), such as RBS.
2. On the multi-factor authentication standby screen, click the '[MFA User Portal](#)' button.
3. A separate browser window appears and a second authentication screen for accessing the MFA user portal is displayed.
4. Complete the authentication using the existing authentication method.
5. When accessing the User Portal, click the '[Authentication Information List](#)' button at the bottom of the screen.
6. Click the '[Add Email](#)' button.
7. Enter the public personal email address to be added and click the '[Certification Request](#)' button.
8. Check the verification code sent to the entered email address.
9. Enter the authentication code and click the '[Certification](#)' button.
10. If there are two or more existing registered emails (however, it may be changed by security policy), select the emails that will not be used for authentication and 'delete'.

-If you want to change the email, you can delete the existing email after registering a new email.

-The added email can be checked in the authentication information list.

Q I only registered Email and SMS, how do I use the APP?

A In order to register an additional APP, access to the user portal is required.

1. Log on to a service that requires Multi-Factor Authentication (MFA), such as RBS.
2. On the multi-factor authentication standby screen, click the '[MFA User Portal](#)' button.
3. A separate browser window appears and a second authentication screen for accessing the MFA user portal is displayed.
4. Complete the authentication using the existing authentication method.
5. When accessing the User Portal, click the '[Authentication Information List](#)' button at the bottom of the screen.
6. Click the '[Add APP](#)' button.
 - If the maximum number of registrations is exceeded, delete the existing registered APP from the list and register a new APP.
7. Enter the [12-digit authentication information ID](#) and [6-digit authentication code](#) of the installed APP and click the 'Confirm' button.
 - The added APP can be checked in the authentication information list and can be changed to the preferred authentication method on the user portal home screen.

Q How do I access the user portal?

A To add, change or delete the registered authentication information, you need to access the user portal. The user portal access method is as follows.

When the connected system authenticates through the composite authentication page

1. First log in to the system you want to access.
2. Click the 'MFA User Portal' button on the composite authentication standby screen.
3. The User Portal Secondary Authentication page is displayed in a separate browser window.
4. When authentication is completed using the previously registered method, the user portal home is displayed.

When the connected system authenticates through a separate authentication client

1. Connect by entering <https://mfa.secsso.net> in an Internet browser.
2. The User Portal Secondary Authentication page is displayed.
3. When authentication is completed using the previously registered method, the user portal home is displayed.

After accessing the user portal, you can add or delete authentication methods from 'Authentication Information List'

Q

Push does not work after deleting and reinstalling the app.

A

In order to proceed with authentication process with a new app, the app must to be registered first. After installing the app on your new phone, you can access the user portal and register via 'Authentication Information List' -> Delete previously registered APP information -> 'Add App'

Q If I delete the app, will the general website OTP information registered on WEB OTP be safely removed?

A Yes. When you delete the app, the private key used to issue WEB OTP is safely removed. **Caution!)** If you delete the app, WEB OTP's private key is also removed and cannot be recovered.

Q I want to change my phone. How can I move WEB OTP?

A A WEB OTP is generated using a 'private key', which is like a password. This information cannot be moved between phones. You must turn off OTP authentication for each registered service, install the app and register again.

Q How do I authenticate if I register both an app, SMS and e-mail?

A Unless otherwise specified, the priority of authentication method is push authentication> e-mail authentication> SMS authentication. If you register both the app, mobile number and e-mail, push authentication is the default authentication method .If you have registered only mobile number and e-mail, then SMS authentication will be the default authentication method. You can change the 'preferred' authentication method by accessing the user portal.

Q I am using multiple IDs due to the nature of my work. Do I have to use a different smartphone for each ID?

A App can be associated with multiple IDs. (N number of accounts for each device)
The first time you use multi-factor authentication with a specific ID, you will be registered. At this time, you can register by using the 'authentication information ID ' and ' authentication code' from the already installed app. It can be used to authenticate multiple IDs with a single device.

Q Due to the nature of work, we are using multiple devices. Can an ID be registered on multiple device?

A A single ID can be connected to multiple devices. (However, it may be limited to 1 ID 1 device by security policy.) Install the 'Samsung Multi-factor Authentication' app on the other device. After accessing the user portal, click the "Authentication List" and click on the "Add App" button to register the app. Push authentication requests are sent simultaneously to all devices enlisted in the ID.

Can I register multiple SMS or e-mails?

Q You can register multiple SMS or e-mail addresses. Verification codes will be sent to all registered phone numbers when requesting SMS verification and to all registered email addresses when requesting email verification. (However, it may be restricted to 1 ID 1 phone number / EMAIL by security policy.)

A