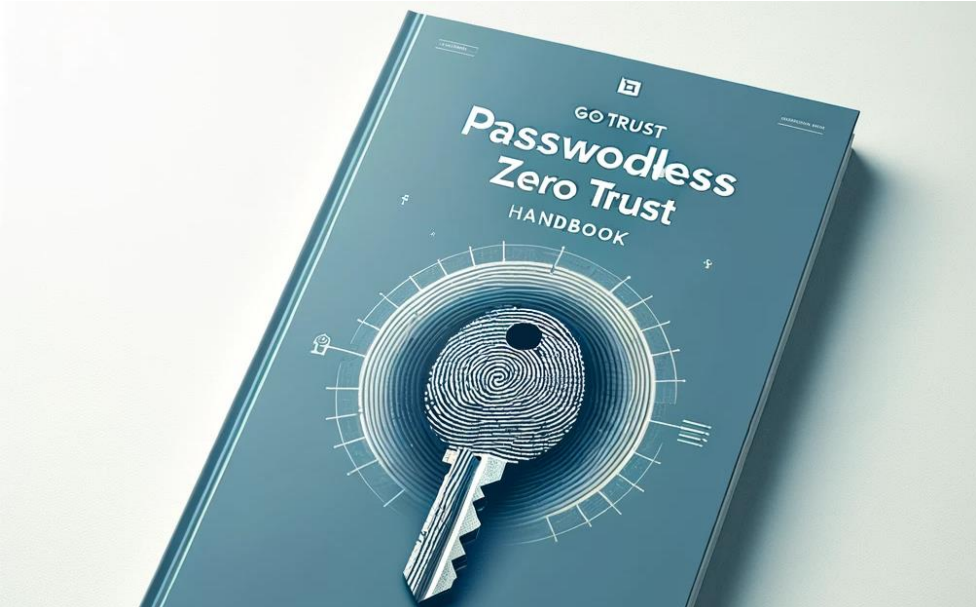
GoTrust
ID IS ME

GoTrust ID Passwordless ZTA Quick Installation Guide



Version 1.0

Table of Contents

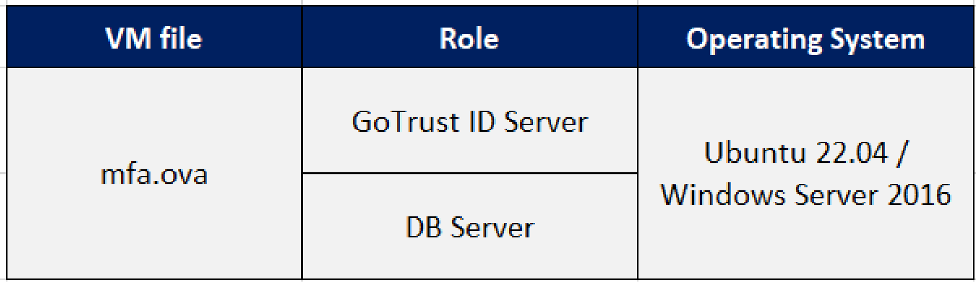
GoTrust ID Passwordless ZTA Solution | Quick Installation Guide

Part 1 : Server Environment

Environment Details

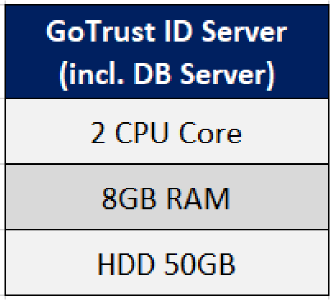
Deployment

- VM download link will be provided by GoTrust. Ubuntu is the default operating system environment we provide, please inform GoTrust if you need Windows Server instead of Ubuntu. Windows server license will be prepared by client.



VM file	Role	Operating System
mfa.ova	GoTrust ID Server	Ubuntu 22.04 / Windows Server 2016
	DB Server	

Minimum System Requirement

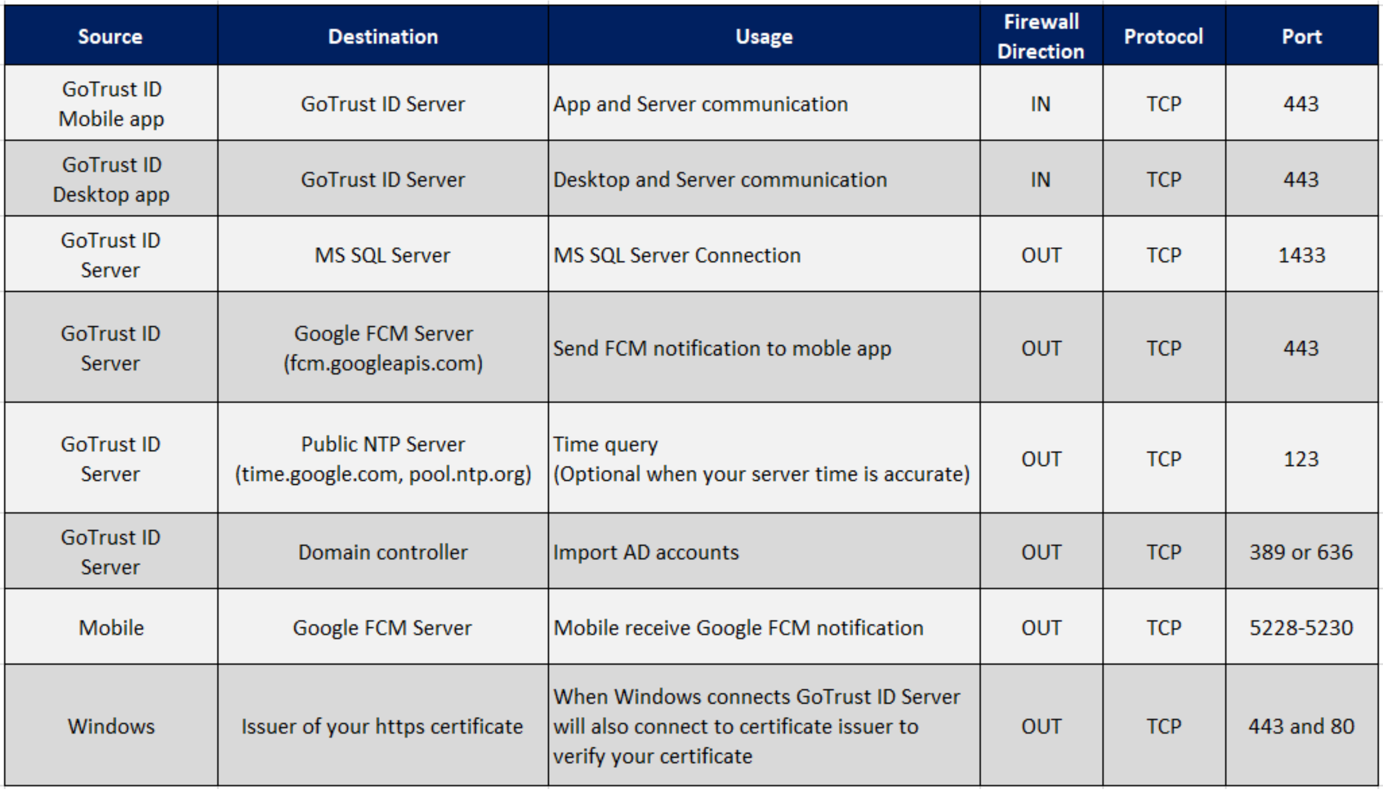


GoTrust ID Server (incl. DB Server)
2 CPU Core
8GB RAM
HDD 50GB

HTTPS SSL Certificate

- Please prepare Public URL and its IP for GoTrust ID Server.
- Please prepare Https certificate in .pfx format which will be installed in the GoTrust ID Tomcat server.
- GoTrust ID Server will use https 443, please make sure the ports have been set up according to the table below.

GoTrust ID Server Port List



Source	Destination	Usage	Firewall Direction	Protocol	Port
GoTrust ID Mobile app	GoTrust ID Server	App and Server communication	IN	TCP	443
GoTrust ID Desktop app	GoTrust ID Server	Desktop and Server communication	IN	TCP	443
GoTrust ID Server	MS SQL Server	MS SQL Server Connection	OUT	TCP	1433
GoTrust ID Server	Google FCM Server (fcm.googleapis.com)	Send FCM notification to moble app	OUT	TCP	443
GoTrust ID Server	Public NTP Server (time.google.com, pool.ntp.org)	Time query (Optional when your server time is accurate)	OUT	TCP	123
GoTrust ID Server	Domain controller	Import AD accounts	OUT	TCP	389 or 636
Mobile	Google FCM Server	Mobile receive Google FCM notification	OUT	TCP	5228-5230
Windows	Issuer of your https certificate	When Windows connects GoTrust ID Server will also connect to certificate issuer to verify your certificate	OUT	TCP	443 and 80

Correct Time is essential to GoTrust ID Server and User Mobile Phone

- Please make sure GoTrust ID server time and user mobile phone time are correct and synchronized.

GoTrust ID Server License

- GoTrust ID Server License file will be provided by GoTrust.

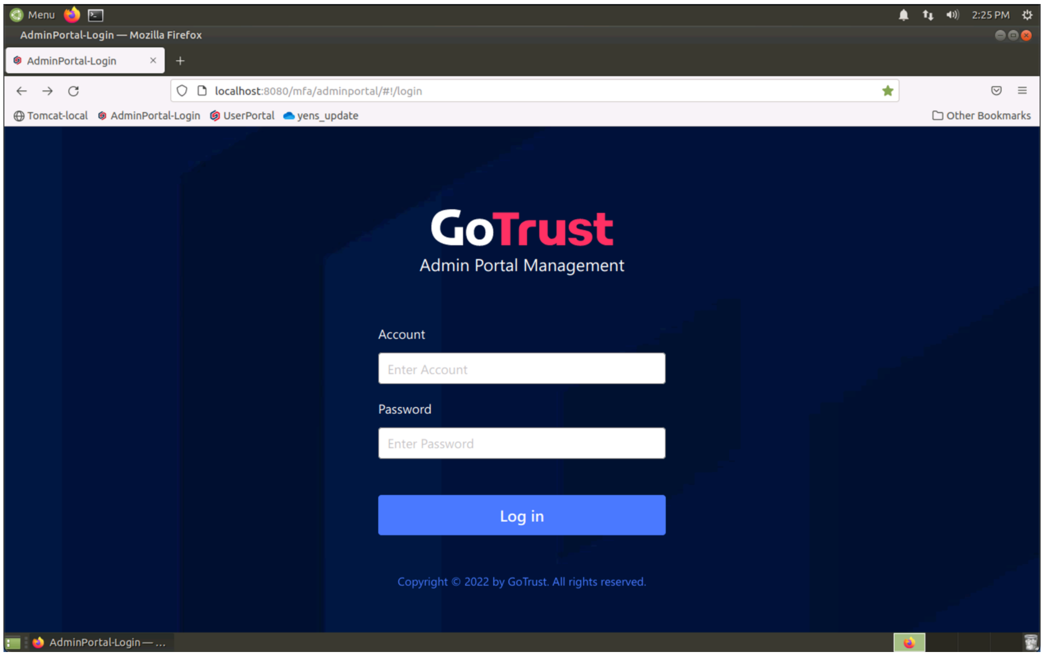
Part 2 : AdminPortal Quick Start

AdminPortal Quick Introduction

Connect to AdminPortal

- Account and Password will be provided by GoTrust.
- Default access is from localhost at http://localhost:8080/mfa/adminportal

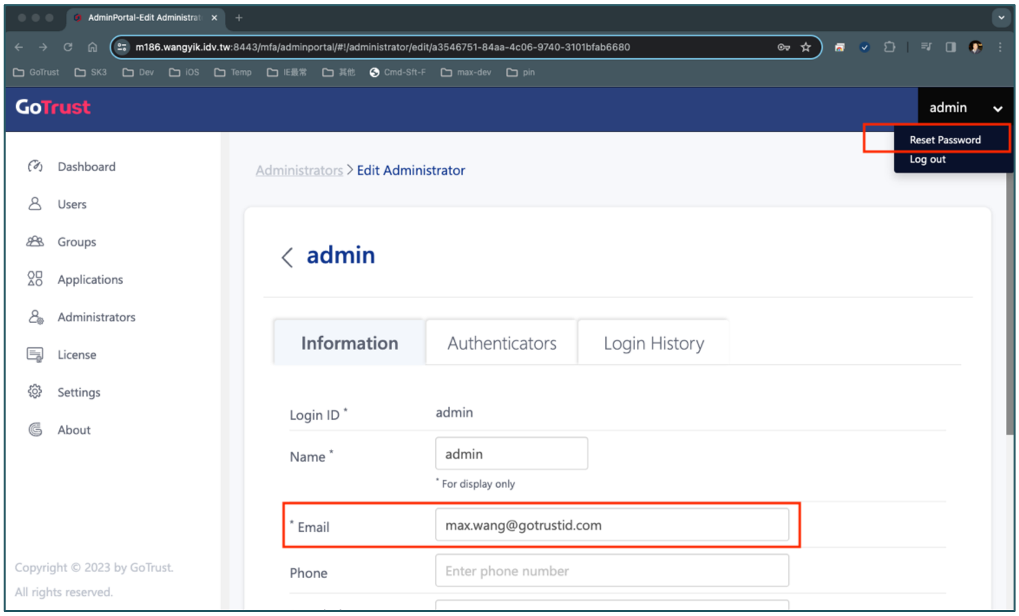
  NOTE: By default setting, you can only access AdminPortal from localhost.
  If you want to access from another computer, you need to edit URL in:
  /home/gotrust/bin/tomcat/webapps/mfa/adminportal/config.json
  (example: "base_api": "https://your-domain.com:8443/mfa/api/v2/admin/")



Copyright © 2022 by GoTrust. All rights reserved.

Change Default Password

- It is highly recommended to create a new admin account and set default "admin" to disabled. If you do not create new account, at least you need to change the default password.
- To change default password, click upper-right corner -> "Reset Password". Also fill the "email" information for admin. It is required if you need to set import account from AD server.



admin

Login ID * admin

Name * admin

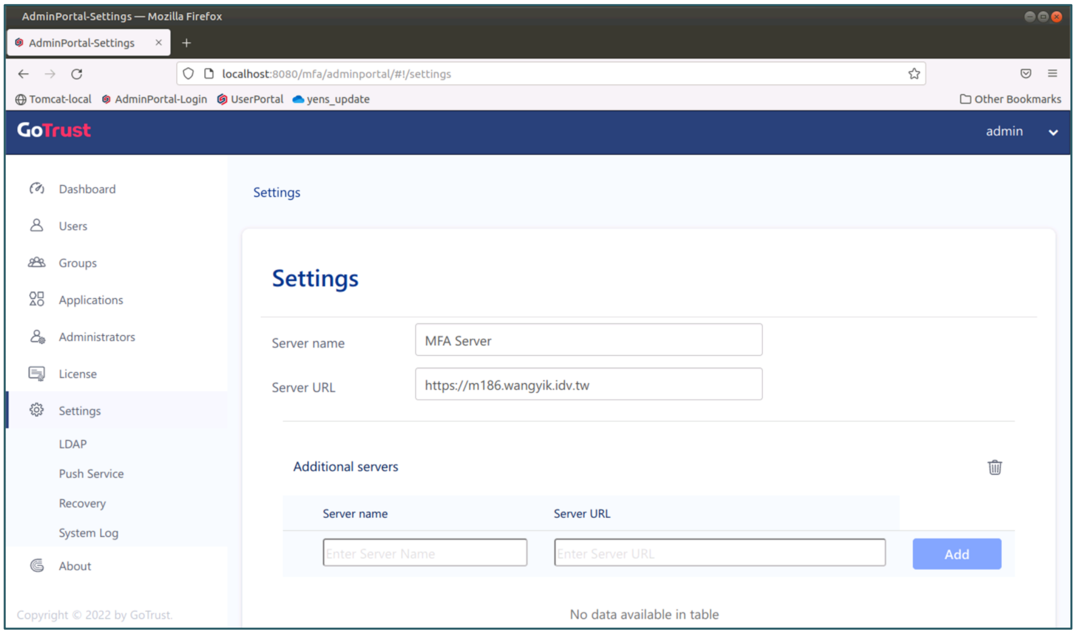
* For display only

* Email max.wang@gotrustid.com

Phone Enter phone number

Setup GoTrust ID Server URL

- AdminPortal > Settings > Server URL > Save Changes



Settings

Server name MFA Server

Server URL https://m186.wangyik.idv.tw

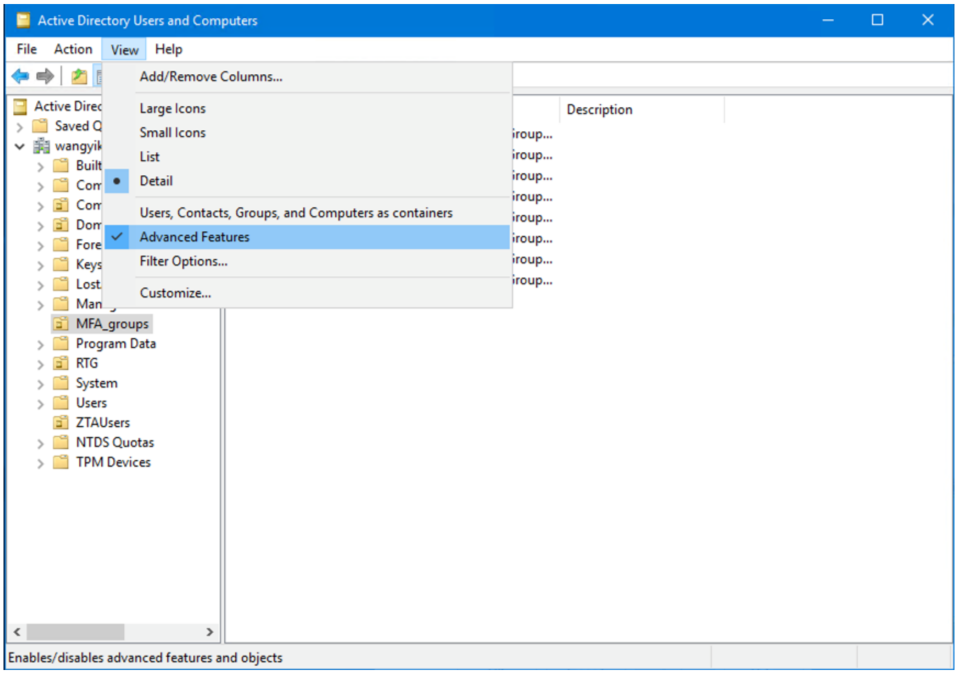
Additional servers

Server name	Server URL
Enter Server Name	Enter Server URL

No data available in table

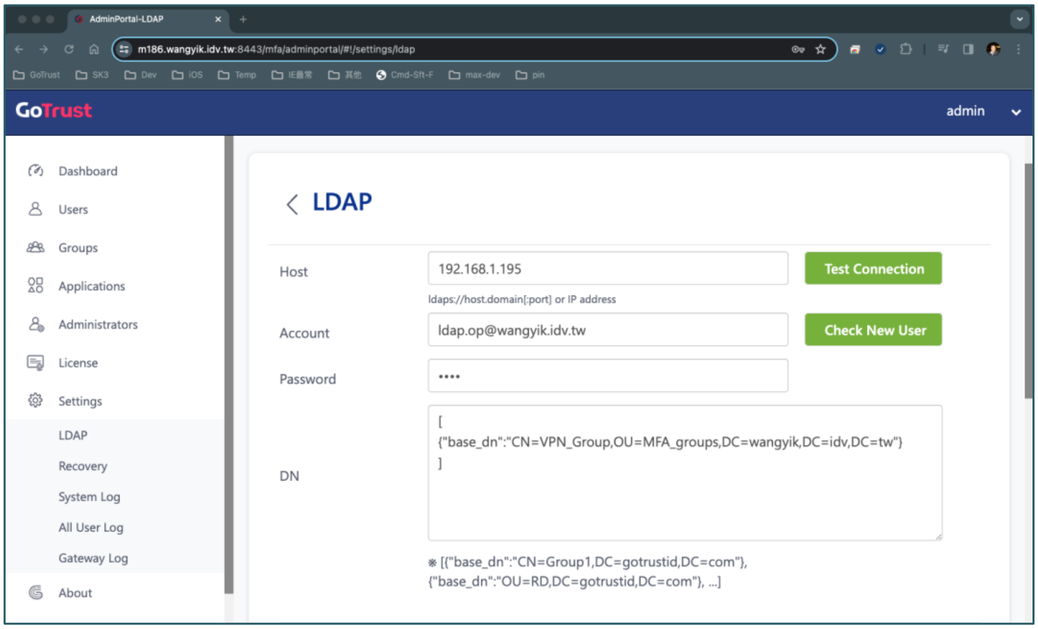
Setup LDAP Connection to AD Server

- Following make an example for "VPN Group", you can reference this concept to create "Computer Login Group" and etc.
- Create an "VPN_Group" on AD server using "Active Directory Users and Computers". NOTE: group name is case sensitive.
- Turn on "Advanced features".



Enables/disables advanced features and objects

- Right click on "VPN_Group" -> Properties -> Attribute Editor -> "distinguishedName", then copy the distinguishedName (DN), which will be used at next step.
- At GoTrust MFA AdminPortal/Settings/LDAP, enter following:
  Host: IP address of AD server
  Account: any AD account with read privilege on AD server
  Password: of above account
  DN (json): [{"base_dn": "the_value_you_copied_at_previous_step"}]



Host: 192.168.1.195

ldaps://host.domain[:port] or IP address

Account: ldap.op@wangyik.idv.tw

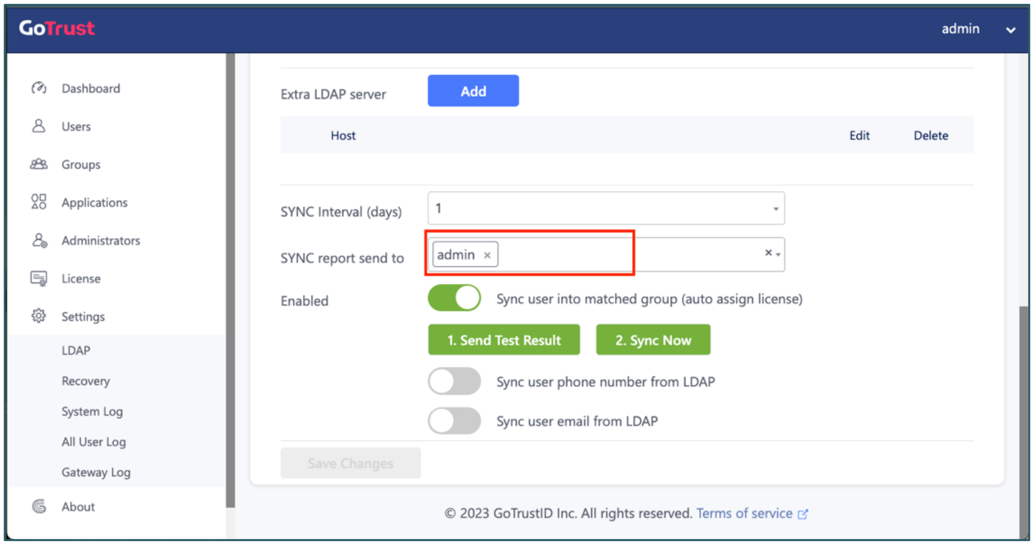
Password: ••••

DN:

```
[
{"base_dn":"CN=VPN_Group,OU=MFA_groups,DC=wangyik,DC=idv,DC=tw"}
]
```

※ [{"base_dn":"CN=Group1,DC=gotrustid,DC=com"}, {"base_dn":"OU=RD,DC=gotrustid,DC=com"}, ...]

- Click [Test Connection] button. Check if success.
- Select one admin with email filled in "SYNC report send to", then click [Save].



Extra LDAP server

SYNC Interval (days): 1

SYNC report send to: admin ×

Enabled: Sync user into matched group (auto assign license)

Sync user phone number from LDAP

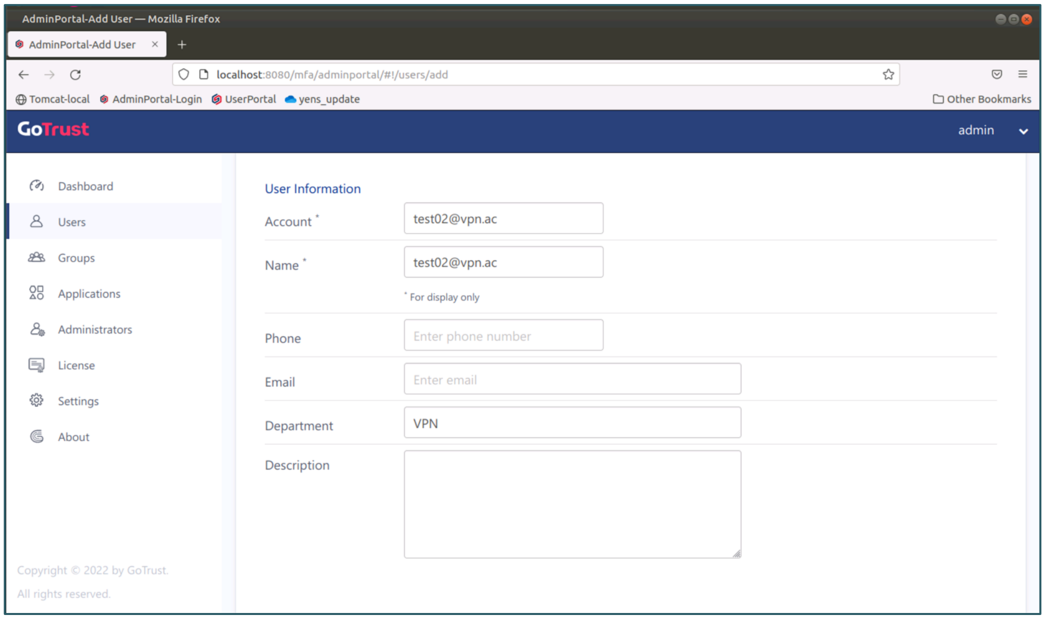
Sync user email from LDAP

© 2023 GoTrustID Inc. All rights reserved. Terms of service

- Click [1.Send Test Result] and check your email to see if success.
  After confirmation, click [2. Sync Now], you can go to "Users" to make sure if users are imported.

Create User Manually

- You can skip this section if you are importing accounts from AD server.
- AdminPortal > Users > [Add User] >
  (input user data, select proper group) >
  [Add User]



User Information

Account *: test02@vpn.ac

Name *: test02@vpn.ac

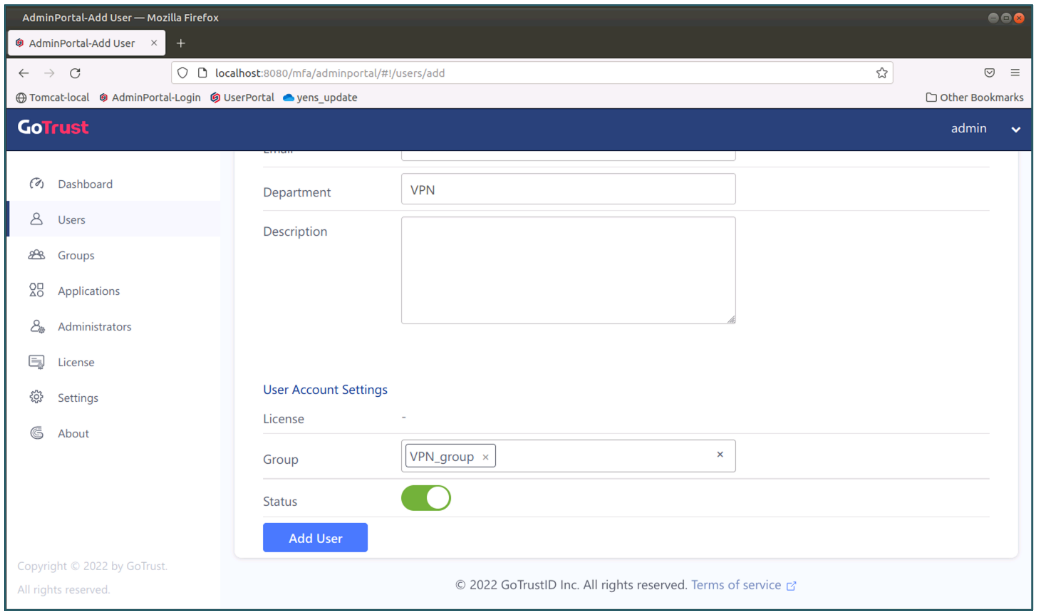
* For display only

Phone: Enter phone number

Email: Enter email

Department: VPN

Description:



Department: VPN

Description:

User Account Settings

License: -

Group: VPN_group ×

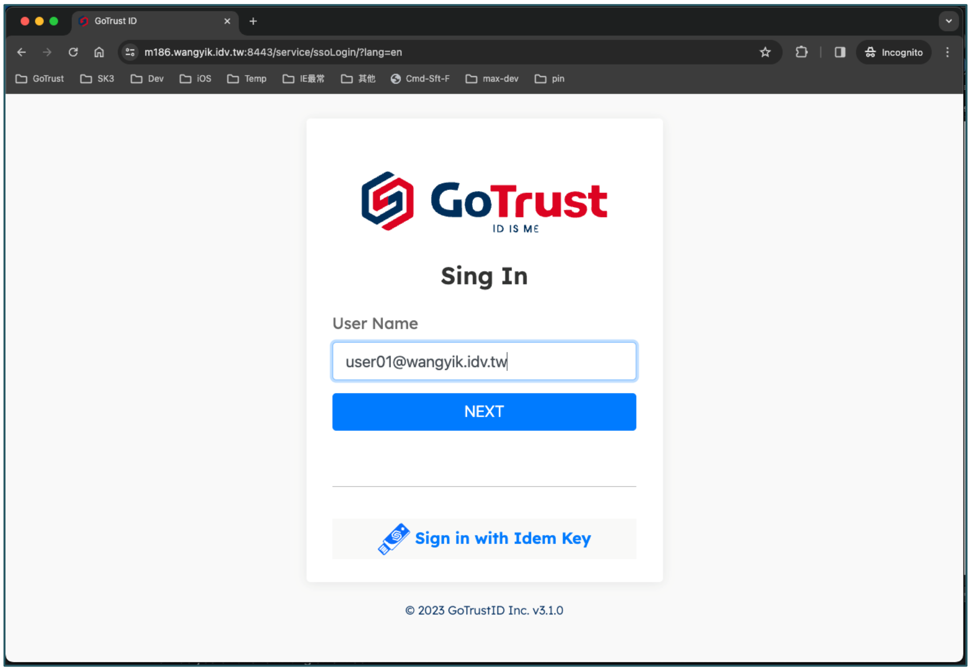
Status: ●

Part 3：GoTrust UserPortal Quick Start

GoTrust UserPortal for Application

Users can manage authenticators by themselves on UserPortal without asking for help from the IT administrator.

- Connect to https://your_domain.com:{port}/service/sso



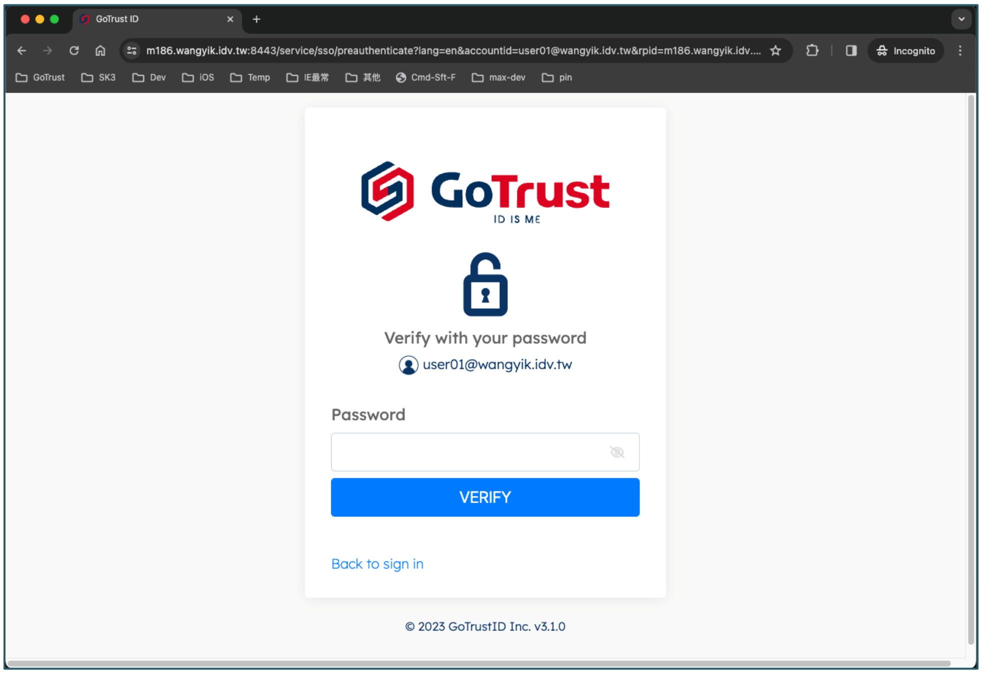
m186.wangyik.idv.tw:8443/service/ssoLogin/?lang=en

Sing In

User Name: user01@wangyik.idv.tw

© 2023 GoTrustID Inc. v3.1.0

- Enter the username and password.
  (AD account which already synchronized into AdminPortal/Users)


GoTrust ID
m186.wangyik.idv.tw:8443/service/sso/preauthenticate?lang=en&accountid=user01@wangyik.idv.tw&rpid=m186.wangyik.idv....
Incognito
GoTrust
SK3
Dev
iOS
Temp
IE最常
其他
Cmd-Sft-F
max-dev
pin
GoTrust
ID IS ME

Verify with your password

user01@wangyik.idv.tw

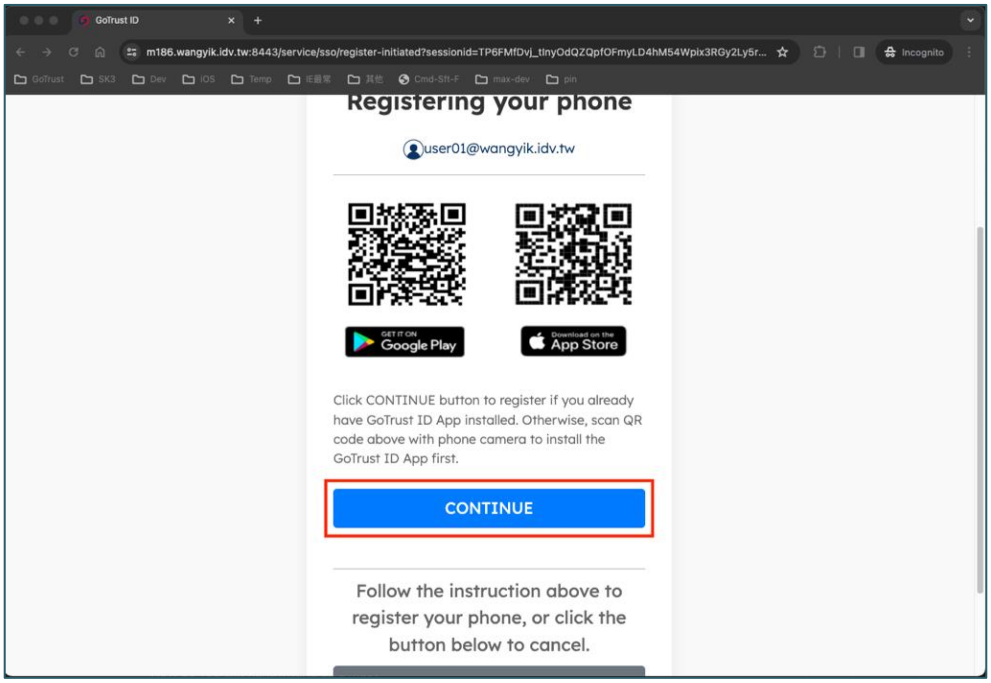
Password

VERIFY

Back to sign in

© 2023 GoTrustID Inc. v3.1.0

- Example to register GoTrust ID mobile app.
  Click [Register Phone], then use QR code to download mobile app from Store.
  If you have GoTrust ID installed, click [Continue]


GoTrust ID
m186.wangyik.idv.tw:8443/service/sso/register-initiated?sessionid=TP6FMfDvj_tlnyOdQZQpfOFmyLD4hM54Wpix3RGy2Ly5r...
Incognito
GoTrust
SK3
Dev
iOS
Temp
IE最常
其他
Cmd-Sft-F
max-dev
pin
GET IT ON
Google Play
Download on the
App Store

Registering your phone

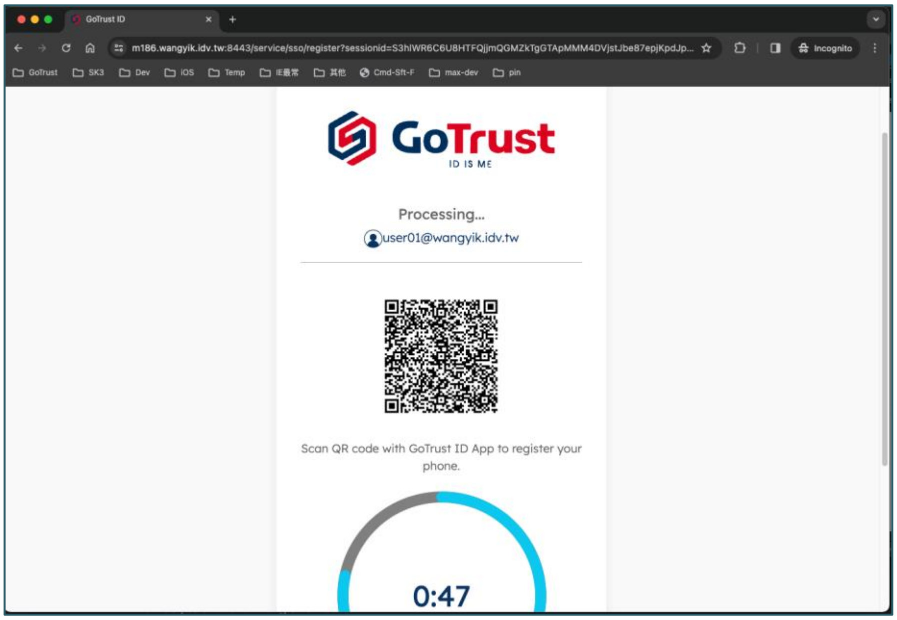
user01@wangyik.idv.tw

Click CONTINUE button to register if you already have GoTrust ID App installed. Otherwise, scan QR code above with phone camera to install the GoTrust ID App first.

CONTINUE

Follow the instruction above to register your phone, or click the button below to cancel.

- Using GoTrust ID mobile app to scan QR Code, and pass the biometric verification.

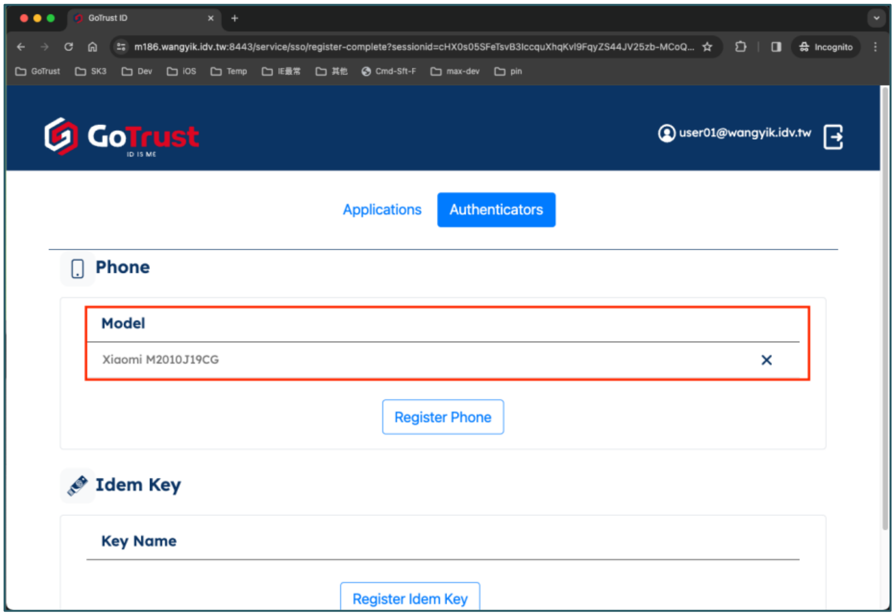

GoTrust ID
m186.wangyik.idv.tw:8443/service/sso/register?sessionid=S3hlWR6C6U8HTFQjjmQGMZkTgGTApMMM4DVjstJbe87epjKpdJp...
Incognito
GoTrust
SK3
Dev
iOS
Temp
IE最常
其他
Cmd-Sft-F
max-dev
pin
GoTrust
ID IS ME
0:47

Processing...

user01@wangyik.idv.tw

Scan QR code with GoTrust ID App to register your phone.

- Registration done.
  Next time you need to use mobile phone to login UserPortal.



Phone

Model
Xiaomi M2010J19CG ✕

Idem Key

Key Name

Part 4 : Desktop Login

Safeguard Workstation From Desktop Login

Passwordless Login

- No password required and no password entry available.

Login Anytime and Anywhere (Online or Offline)

- Even if the computer or mobile phone is offline, user can still login via mobile phone BLE or security code or use Idem Key.

Authenticator

- User can login by phone authenticator or Idem Key.

Single User Mode or Shared Computer Multiple User Mode

- Single user mode can prevent other domain user from logining your computer. Dedicated entry designed for IT troubleshooting.
- Shared computer multiple user mode can be configured by demand.

Deployment

Install GoTrust ID Desktop App

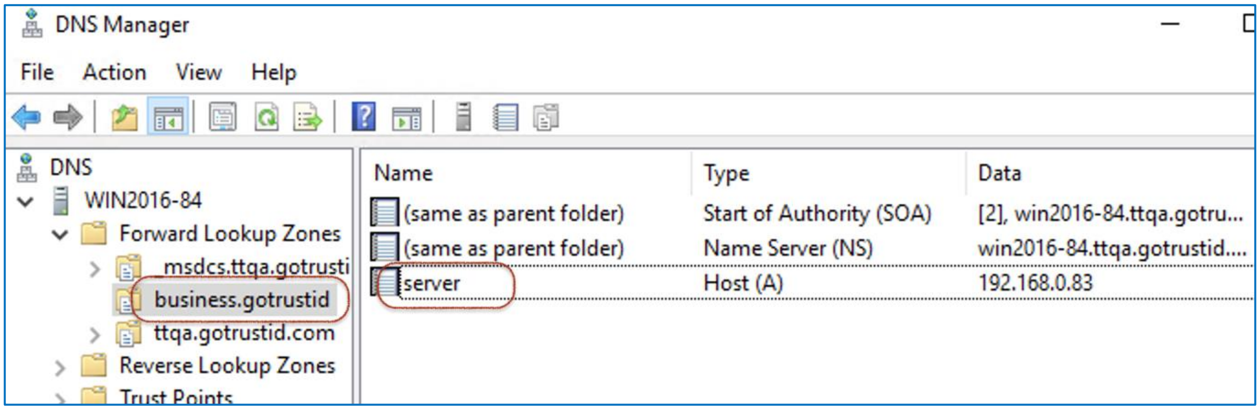
- Manually or use GPO, installation tools, antimalware services to install GoTrust ID Desktop App.
- Support Windows 10/11, macOS, Windows Server 2016/2019.
- Seamlessly fit into Active Directory login without extra settings.

Version Update Function

- GoTrust ID Desktop App version update function can be activated in AdminPortal.

Connect GoTrust ID Desktop App with GOTRUST ID Server

- Create DNS Forward Lookup Zones as business.gotrustid, Host Name as server with mapping GoTrust ID Server IP address.



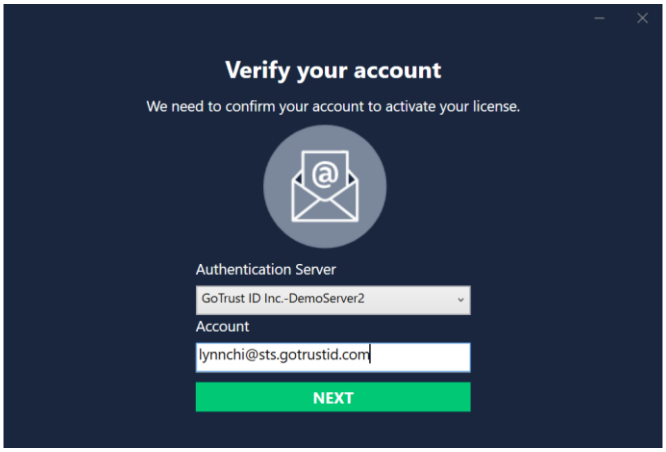
Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2], win2016-84.ttqa.gotru...
(same as parent folder)	Name Server (NS)	win2016-84.ttqa.gotrustid....
server	Host (A)	192.168.0.83

- After configuration, GoTrust ID Desktop App will automatically connect with GoTrust ID server at first launch.

Registration and How to Manage Desktop Login Authenticator

Easy Registration

- Confirm company server name and enter a company account (e.g. lynnchi@sts.gotrustid.com) and press “Next”.



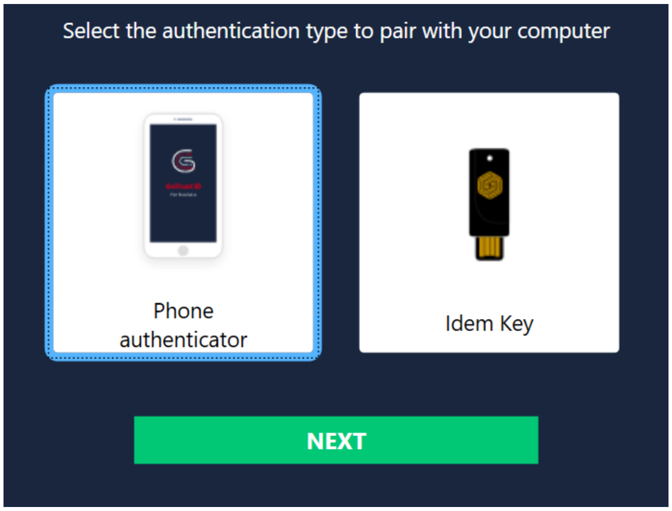
Verify your account

We need to confirm your account to activate your license.

Authentication Server: GoTrust ID Inc.-DemoServer2

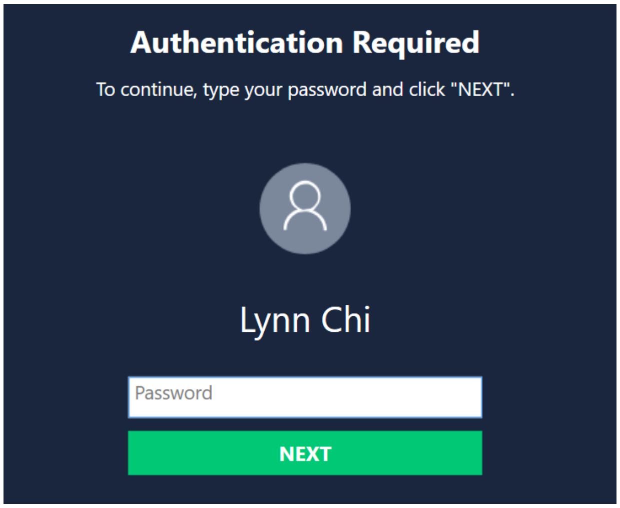
Account: lynnchi@sts.gotrustid.com

- Select phone authenticator to pair with your computer and press “Next”.



Select the authentication type to pair with your computer

- Type PC login password to verify it’s you and press “Next”.

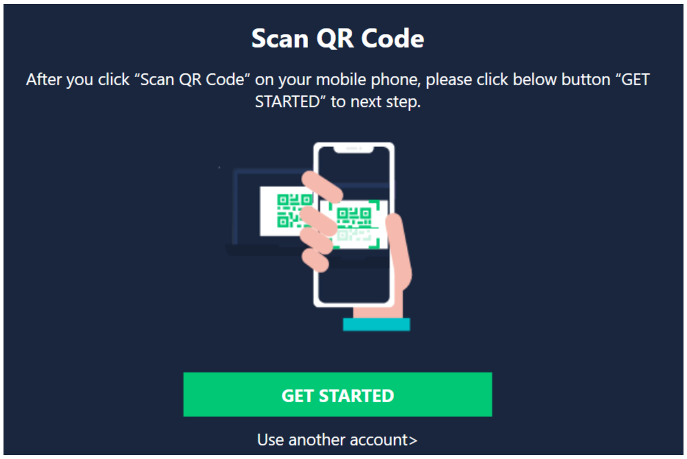


Authentication Required

To continue, type your password and click "NEXT".

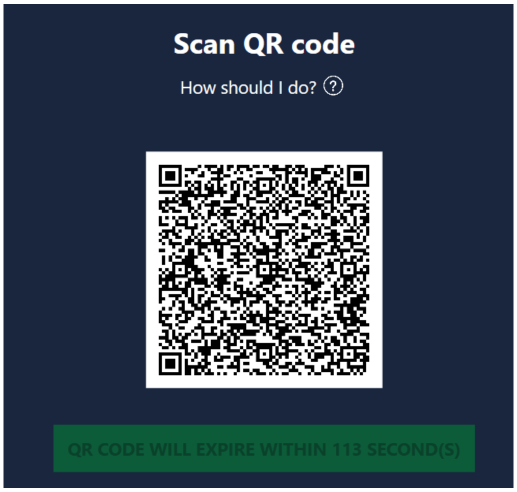
Lynn Chi

- Open GoTrust ID mobile app, tap the floating action button ⊞ on the phone and press “Get Started” on PC page to display QR code. Use phone to scan QR code.
[PC page]



Scan QR Code

After you click “Scan QR Code” on your mobile phone, please click below button “GET STARTED” to next step.

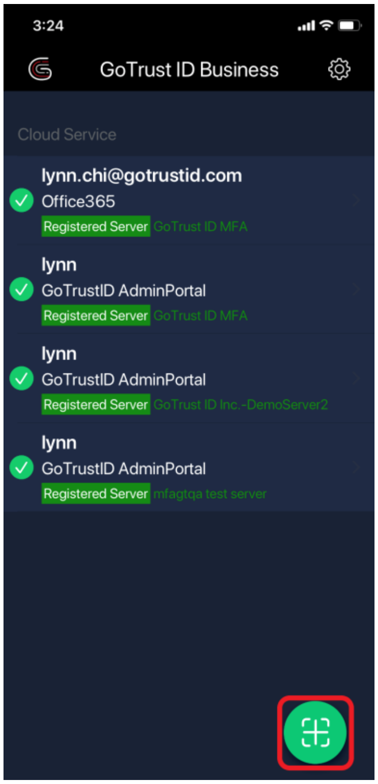


Scan QR code

How should I do? ?

QR CODE WILL EXPIRE WITHIN 113 SECOND(S)

[Mobile page]



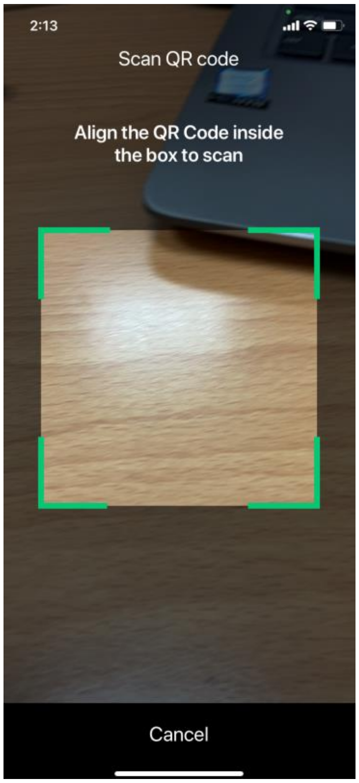
Cloud Service

lynn.chi@gotrustid.com
Office365
Registered Server GoTrust ID MFA

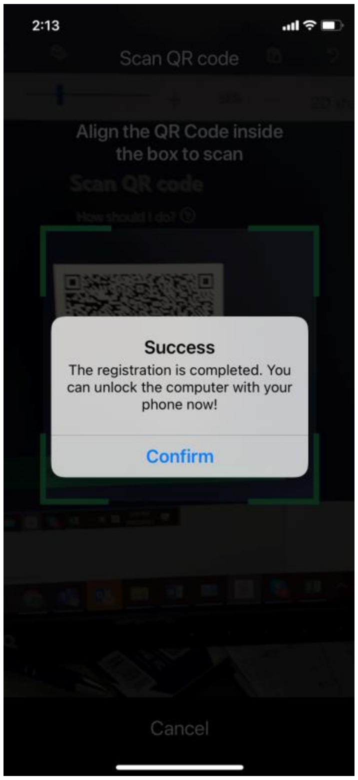
lynn
GoTrustID AdminPortal
Registered Server GoTrust ID MFA

lynn
GoTrustID AdminPortal
Registered Server GoTrust ID Inc.-DemoServer2

lynn
GoTrustID AdminPortal
Registered Server mfagtqa test server



Align the QR Code inside the box to scan

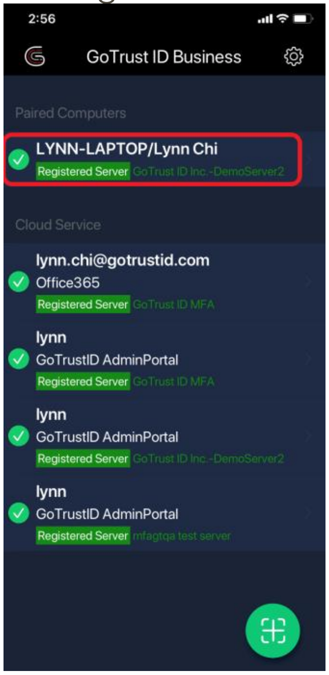


Success

The registration is completed. You can unlock the computer with your phone now!

Confirm

- Mobile app shows the enrolled PC device and desktop app (Device Management page) lists the enrolled authenticator. User can now experience GoTrust ID computer login. Note: The last authenticator is not allowed to remove by user. If you need to change authenticator, you can remove the old one after adding a new one.



Paired Computers

LYNN-LAPTOP/Lynn Chi
Registered Server GoTrust ID Inc.-DemoServer2

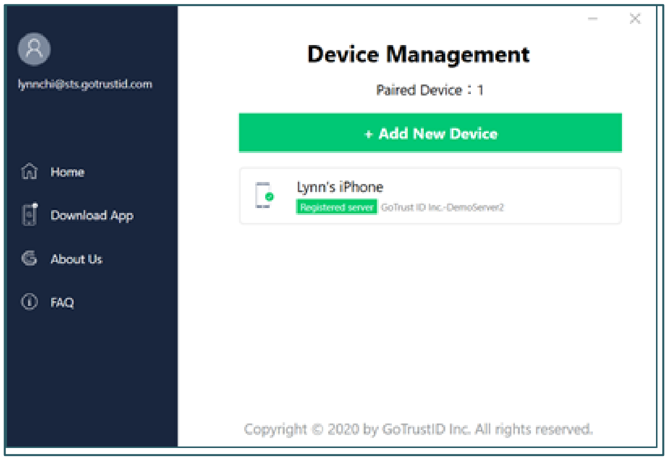
Cloud Service

lynn.chi@gotrustid.com
Office365
Registered Server GoTrust ID MFA

lynn
GoTrustID AdminPortal
Registered Server GoTrust ID MFA

lynn
GoTrustID AdminPortal
Registered Server GoTrust ID Inc.-DemoServer2

lynn
GoTrustID AdminPortal
Registered Server mfagtqa test server



Device Management

Paired Device : 1

+ Add New Device

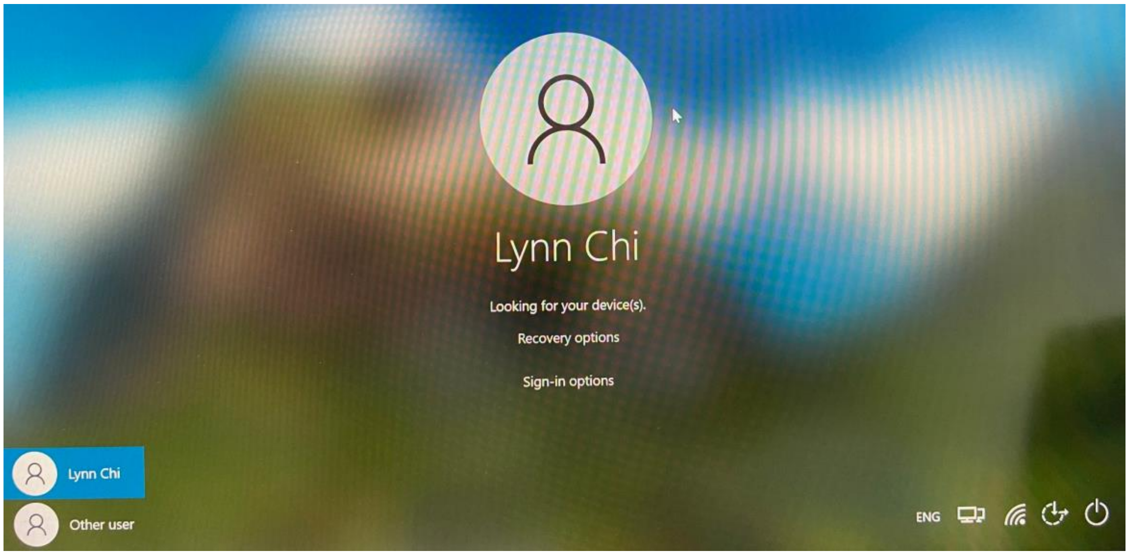
Lynn's iPhone
Registered server GoTrust ID Inc.-DemoServer2

Copyright © 2020 by GoTrustID Inc. All rights reserved.

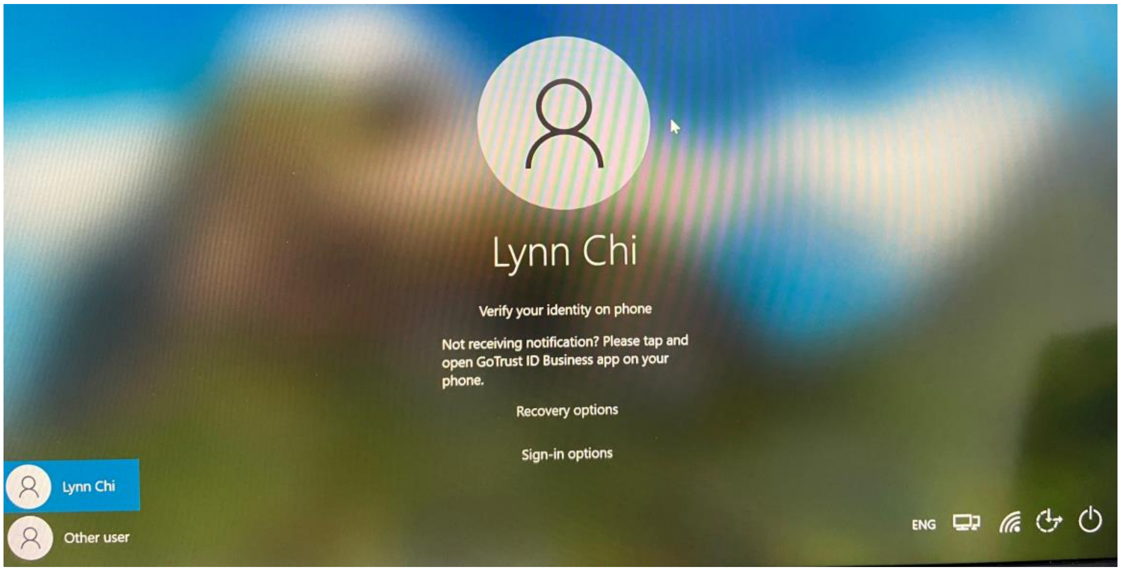
Desktop Login Flow

Windows example

- User will receive push notification on mobile after pressing any key on PC to initiate login process. Note: Please make sure to open GoTrust ID mobile app first if you want to use BLE to login.



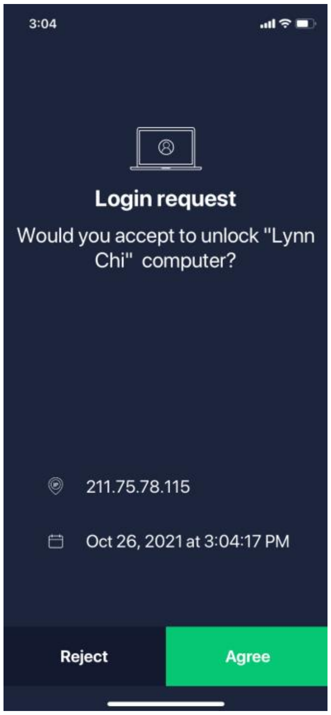
Looking for your device(s).



Verify your identity on phone

Not receiving notification? Please tap and open GoTrust ID Business app on your phone.

- Mobile receives login request, after pressing “Agree” the user is presented with the phone’s biometric authentication option (fingerprint or face ID). Once verified the user will be successfully logged in.



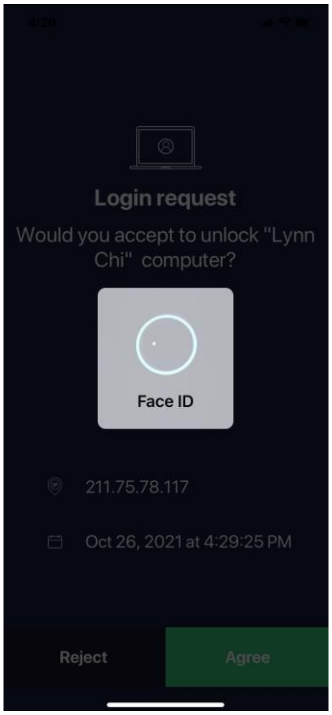
3:04

Login request

Would you accept to unlock "Lynn Chi" computer?

211.75.78.115

Oct 26, 2021 at 3:04:17 PM



Login request

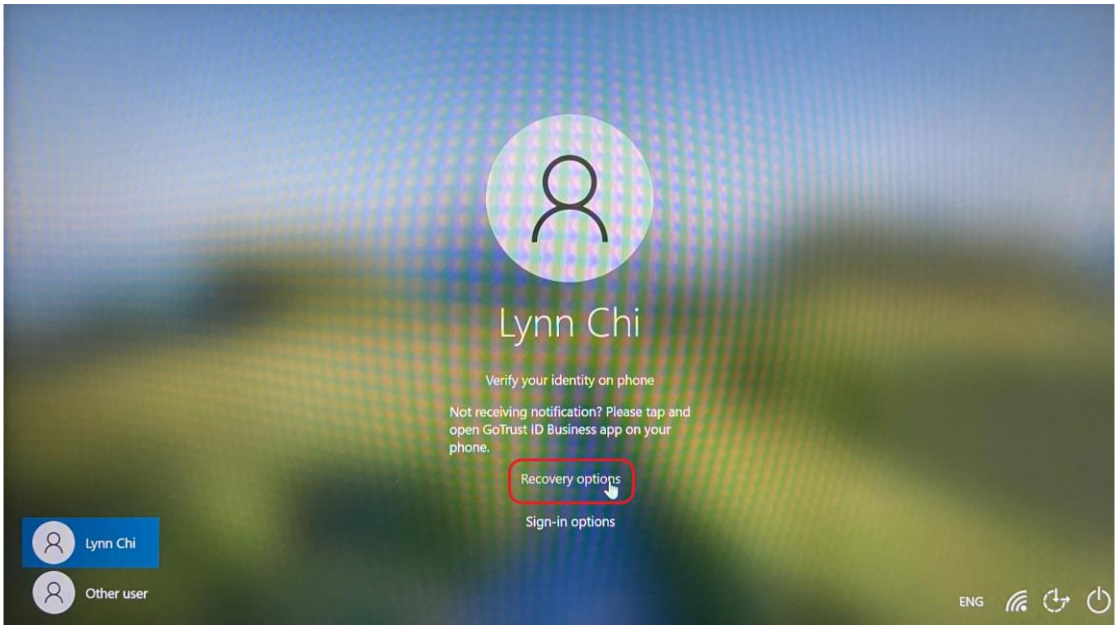
Would you accept to unlock "Lynn Chi" computer?

211.75.78.117

Oct 26, 2021 at 4:29:25 PM

Recovery Options – In-App Security Code

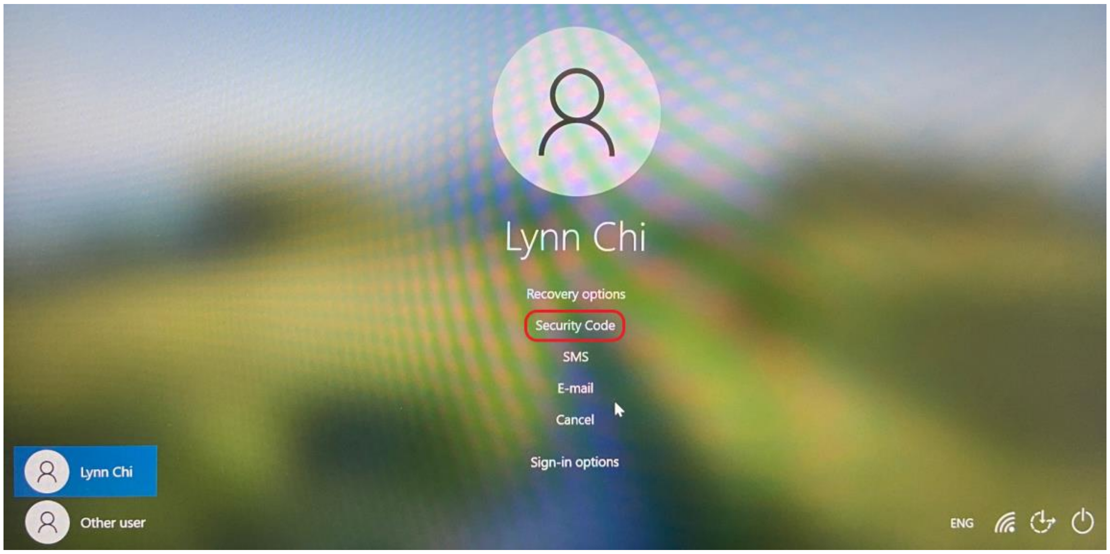
- Click “Recovery options”-> Choose “Security Code”, you can see the input field.

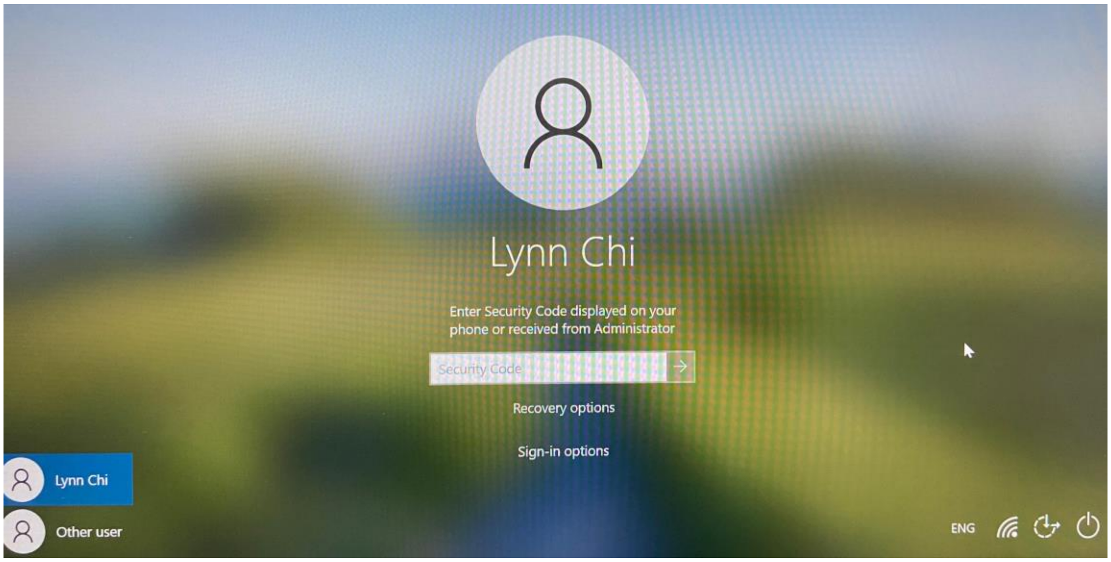


Lynn Chi

Verify your identity on phone

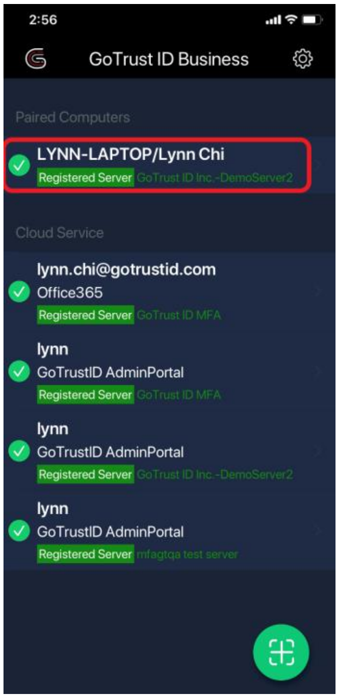
Not receiving notification? Please tap and open GoTrust ID Business app on your phone.





Enter Security Code displayed on your phone or received from Administrator

- Click the paired computer name on mobile (see the red mark below), the user is presented with the phone’s biometric authentication option (fingerprint or face ID). Once verified the security code will be shown. Please insert the code to the input field on PC.
  The blue line under the security code on the mobile indicates the valid time for the code, which is 30 seconds.



2:56

GoTrust ID Business

Paired Computers

LYNN-LAPTOP/Lynn Chi
Registered Server GoTrust ID Inc.-DemoServer2

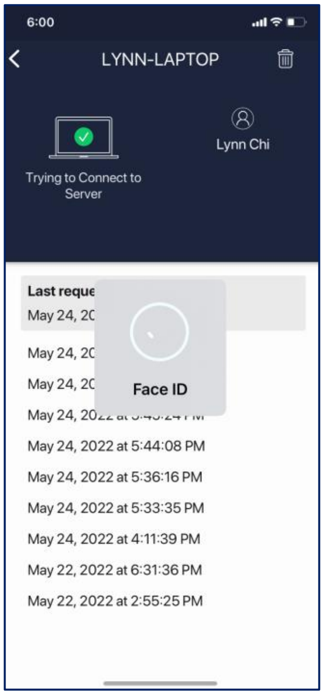
Cloud Service

lynn.chi@gotrustid.com
Office365
Registered Server GoTrust ID MFA

lynn
GoTrustID AdminPortal
Registered Server GoTrust ID MFA

lynn
GoTrustID AdminPortal
Registered Server GoTrust ID Inc.-DemoServer2

lynn
GoTrustID AdminPortal
Registered Server mfagtqa test server



6:00

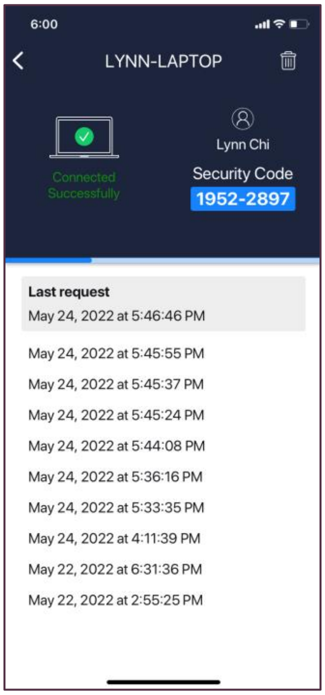
LYNN-LAPTOP

Trying to Connect to Server

Lynn Chi

Face ID

Last reque
May 24, 20
May 24, 20
May 24, 20
May 24, 202
May 24, 2022 at 5:44:08 PM
May 24, 2022 at 5:36:16 PM
May 24, 2022 at 5:33:35 PM
May 24, 2022 at 4:11:39 PM
May 22, 2022 at 6:31:36 PM
May 22, 2022 at 2:55:25 PM



6:00

LYNN-LAPTOP

Connected Successfully

Lynn Chi

Security Code
1952-2897

Last request
May 24, 2022 at 5:46:46 PM
May 24, 2022 at 5:45:55 PM
May 24, 2022 at 5:45:37 PM
May 24, 2022 at 5:45:24 PM
May 24, 2022 at 5:44:08 PM
May 24, 2022 at 5:36:16 PM
May 24, 2022 at 5:33:35 PM
May 24, 2022 at 4:11:39 PM
May 22, 2022 at 6:31:36 PM
May 22, 2022 at 2:55:25 PM

- The input field on PC can also insert the security code the user received from a corporate administrator.
  To learn how to get a security code in AdminPortal, please refer to AdminPortal User Guide Section 6. Users.

Login Method in an Offline Environment

- User can choose either way below to login
  - Mobile BLE login
  - In-App security code
  - Security code generated from AdminPortal
  - GoTrust Idem Key

Login Method when Phone is Unavailable

- User can choose either way below to login
  - Security code generated from AdminPortal
  - GoTrust Idem Key

Thank you for experiencing amazing login with GoTrust!