



# Keypasco Proxy Installation Guide

V1.5

權利專有聲明

本文件包含來毅數位科技股份有限公司的機密與專有資訊，它僅供您作為評估是否採用本文  
件所述之服務之用。未經來毅數位科技股份有限公司明示的書面同意，上述資訊的一部或全  
部，不得影印、使用、重製、上載、刊登、改作、或揭露予任何第三人作為任何其他目的之  
用。

Proprietary Statement

This Document contains the confidential and proprietary information of Lydsec Digital  
Technology Co., Ltd., which is only for your evaluation of whether to use the services  
described in this document. Without the express written consent of Lydsec Digital  
Technology Co., Ltd., part or all of the above information may not be photocopied, used,  
reproduced, uploaded, published, modified, or disclosed to any third party for any other  
purpose.



## Reversion history

ISSUE	DATE	AUTHOR	COMMENT
V1.2	2025-02-08	Brian Chen	<ol style="list-style-type: none"><li>1. Modify to support create self-signed certificate automatically.</li><li>2. Simplify the installation process</li></ol>
V1.3	2025-02-26	Brian Chen	<ol style="list-style-type: none"><li>1. Add Bypass Borgen server information section</li><li>2. Add Keypasco Proxy testing steps</li></ol>
V1.4	2025-03-18	Brian Chen	<ol style="list-style-type: none"><li>1. Auto add FQDN or localhost and password for pfx</li><li>2. Auto search Lydsecmfa.zip file</li><li>3. Set default log path</li><li>4. Set default local user “kpadmin”</li><li>5. Auto open Microsoft edge and show url at the end of powershell</li></ol>
V1.5	2025-03-29	Brian Chen	<ol style="list-style-type: none"><li>1. Add ClientApi setting</li></ol>



## Table of Contents

<b>1</b>	<b>INTRODUCTION.....</b>	<b>4</b>
1.1	SCOPE .....	4
1.2	KNOWLEDGE PREREQUISITES .....	4
<b>2</b>	<b>KEYPASCO PROXY PREREQUISITES .....</b>	<b>5</b>
2.1	HARDWARE REQUIREMENTS .....	5
2.2	SUPPORTED OPERATING SYSTEMS.....	5
2.3	SUPPORTED DATABASE .....	5
<b>3</b>	<b>INSTALLATION OVERVIEW.....</b>	<b>6</b>
<b>4</b>	<b>INSTALLING KEYPASCO PROXY ON WINDOWS .....</b>	<b>7</b>
4.1	PRE-REQUEST: .....	7
4.2	PROVIDED BY LYDSEC .....	7
4.3	RUNNING STEPS FOR PROXY INSTALL .....	7
4.4	BYPASS BORGEN SERVER INFORMATION .....	9
4.5	TESTING.....	10
4.6	PROBLEMS .....	16



# 1 Introduction

## 1.1 Scope

This document is intended for users installing and configuring the Keypasco Proxy.

## 1.2 Knowledge Prerequisites

- Basic understanding of Windows Server

Confidential



## 2 Keypasco Proxy Prerequisites

This chapter lists the requirements and supports environment for installing Keypasco Proxy.

### 2.1 Hardware Requirements

- 4 cores CPU
- 8G RAM
- 50G Hard Disk

### 2.2 Supported Operating Systems

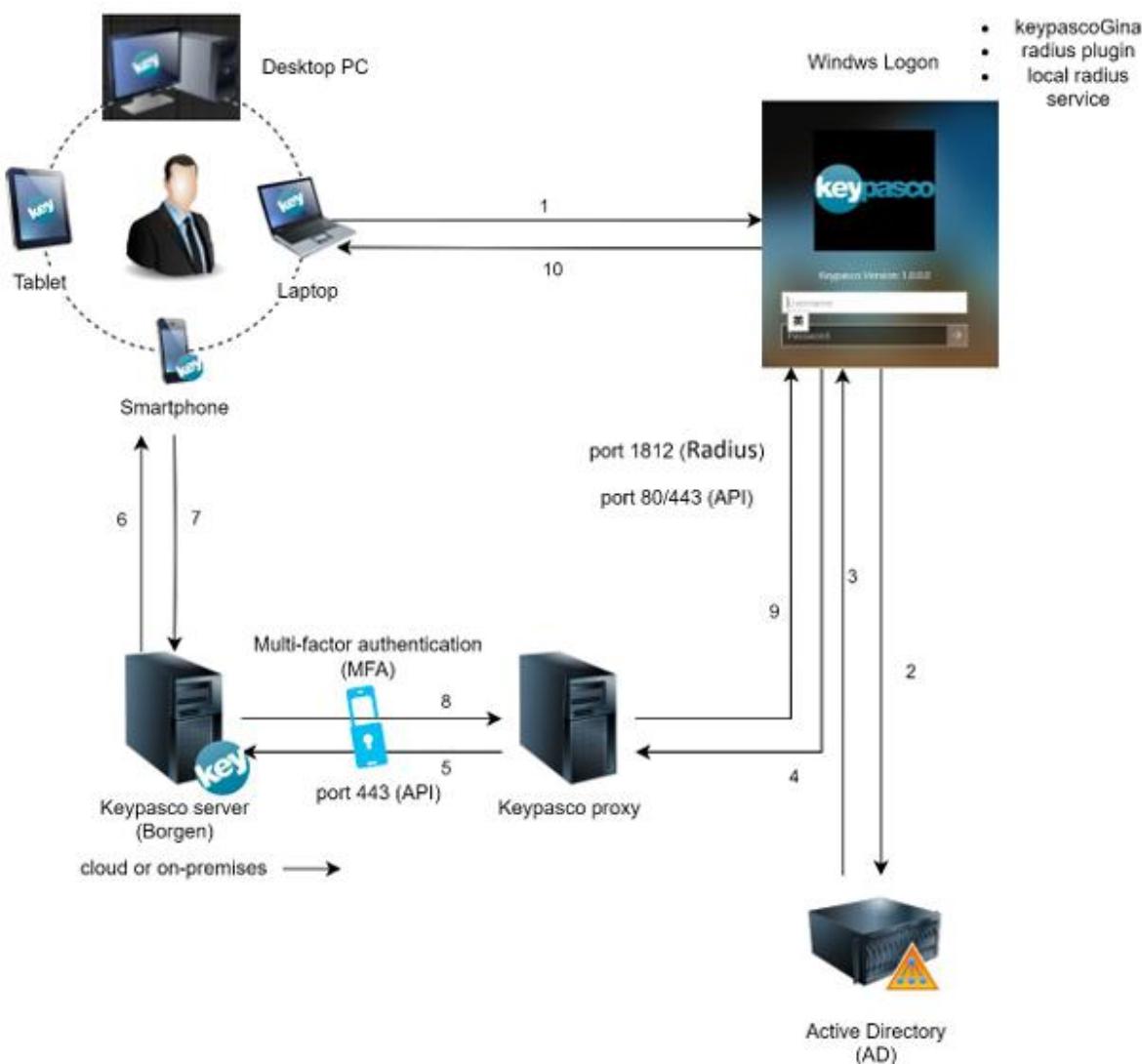
- Windows Server 2019/2022

### 2.3 Supported Database

- SQLite -- default
- PostgreSQL
- MS SQL

## 3 Installation Overview

Having Keypasco MFA as additional authentication



## 4 Installing Keypasco Proxy on Windows

### 4.1 Pre-request:

- Need KeypascoProxyInstall\_V1.x.zip which is the installing script for Keypasco Proxy
- Get the Keypasco proxy install package Lydsecmfa-V1.016.xx-1.43.zip and copy to KeypascoProxyInstaller\_V1.0x folder
- Prepare SSL certificate (.pfx) and password (Suggested)
- Revise the “P12Path” in the .\files\ iniData.json of the package  
(Please refer [4.4 Bypass Borgen Server Information for detailing information](#))



```
...{  
    "BorgenServer": "api2tokyo.keypascoid.com",  
    "P12Path": "C:\\\\Keypasco\\\\KeypascoProxyInstaller\\\\files\\\\keypasco-demo_mfaproxy-new.p12",  
    "P12Password": "mfaproxy",  
    "ICP": "keypasco-demo",  
    "ClientApi": "api22.keypascoid.com"  
}
```

### 4.2 Provided by Lydsec

- Keypasco Borgen certificate (.p12) and password
- FQDN of Borgen server
- ICP

(This information might be pre-defined in iniData.json by Lydsec)

### 4.3 Running Steps for Proxy Install

1. Unzip KeypascoProxyInstall\_V1.x.zip to any working folder
2. Copy Lydsecmfa-V1.016.xx-1.43.zip to the unzipped folder KeypascoProxyInstall
3. Check the contents of iniData.json in KeypascoProxyInstall\files

**Case1:** use your own SSL certification(.pfx)

- Copy SSL certificate(.pfx) to KeypascoProxyInstall\files and type pfx password in KeypascoProxyInstall\files \pfx.pwd

**Case2:** use self-signed SSL certification

- Please make sure there is no .pfx file in KeypascoProxyInstall\files



## Start Install

- Open PowerShell by Administrator
- Run .\Unblock.bat
- Run .\KProxySetting.ps1 in Powershell under KeypascoProxyInstall folder

## Parameters Description:

- Restore Web.config: [Y]es/[N]o to restore the backup Web.config file if the backup file exists (Default: Yes)
- Restore initConfig.ini: [Y]es/[N]o to restore the backup initConfig.ini file if the backup file exists (Default: Yes)
- Use PostggrSQL: [Y]es/[N]o to use PostggrSQL (Default: No)
- PostgreSQL Server [Example: 10.0.1.xxx]: PostgreSQL server url
- PostgreSQL DB name: DB name
- PostgreSQL user name: DB user name
- PostgreSQL user password: DB user password
- Borgen server FQDN: FQDN of Borgen server
- Certificate(P12) full path: full path of certificate file
- Certificate(P12) password: password of certificate file
- Customer ID(ICP): ICP of Borgen server
- AD Domain: AD domain

```

use customer certificate
Thumbprint: 052C01A2889F11606FC12218A39FA7AFB119370F

Success Restart Needed Exit Code      Feature Result
True    No           NoChangeNeeded {}

PSPath          : Microsoft.PowerShell.Security\Certificate::LocalMachine\My\052C01A2889F11606FC12218A39FA7AFB119370F
PSParentPath    : Microsoft.PowerShell.Security\Certificate::LocalMachine\My
PSChildName     : 052C01A2889F11606FC12218A39FA7AFB119370F
PSIsContainer   : False
Archived        : False
Extensions      : {System.Security.Cryptography.Oid, System.Security.Cryptography.Oid, System.Security.Cryptography.Oid, System.Security.Cryptography.Oid}
FriendlyName    : System.Security.Cryptography.X509Certificates.X500DistinguishedName
IssuerName      : 2030/3/18 上午 07:48:15
NotAfter        : 2027/3/18 上午 07:38:14
HasPrivateKey   : True
PrivateKey      : System.Security.Cryptography.X509Certificates.PublicKey
RawData         : {48, 130, 3, 81...}
SerialNumber    : 7933736CD8EC14A54C59C4625CFB2930
SubjectName     : System.Security.Cryptography.X509Certificates.X500DistinguishedName
SignatureAlgorithm: System.Security.Cryptography.Oid
Thumbprint       : 052C01A2889F11606FC12218A39FA7AFB119370F
Version         : 3
Handle          : 2488252973488
Issuer          : CN=testmfa181.es2016.lydsec.com
Subject         : CN=testmfa181.es2016.lydsec.com
EnhancedKeyUsageList: {用戶驗證 (1.3.6.1.5.5.7.3.2), 伺服器驗證 (1.3.6.1.5.5.7.3.1)}
DnsNameList     : {testmfa181.es2016.lydsec.com}
SendAsTrustedIssuer: False
EnrollmentPolicyEndPoint: Microsoft.CertificateServices.Commands.EnrollmentEndPointProperty
EnrollmentServerEndPoint: Microsoft.CertificateServices.Commands.EnrollmentEndPointProperty
PolicyId        :

"Default Web Site" 已順利停止
已新增 SITE 物件 "MFA"
已新增 APP 物件 "MFA/"
已新增 VDIR 物件 "MFA"
已新增 APPPOOL 物件 "MFA"

SSL 憑證新增成功

已變更 APPPOOL 物件 "MFA"
已變更 APP 物件 "MFA/"
已變更 APP 物件 "MFA/"
'MFA' 已順利啟動。
Use PostgreSQL(Default: No) [Y/N]: n
Borgen server FQDN: api2tokyo.keypascoind.com
Certificate(P12) full path: C:\Keypasco\KeypascoProxyInstaller\files\keypasco-demo_mfaproxy-new.p12
Certificate(P12) password: mfaproxy
Customer ID(ICP): keypasco-demo
AD Domain:
Operation complete!
https://testmfa181.es2016.lydsec.com

PS C:\Keypasco\KeypascoProxyInstaller> -

```

## 4.4 Bypass Borgen server information

Create a JSON file name **iniData.json** in KeypascoProxyInstaller\_V1.0x\files\ folder and input the correct Borgen information. The KProxySetting.ps1 will load this file to process the installation.

Example:

```

{
  "BorgenServer": "api2tokyo.keypascoind.com",
  "P12Path": "C:\\\\Keypasco\\\\KeypascoProxyInstaller\\\\files\\\\keypasco-demo_mfaproxy-new.p12",
  "P12Password": "mfaproxy",
  "ICP": "keypasco-demo",
  "ClientApi": "api22.keypascoind.com"
}

```

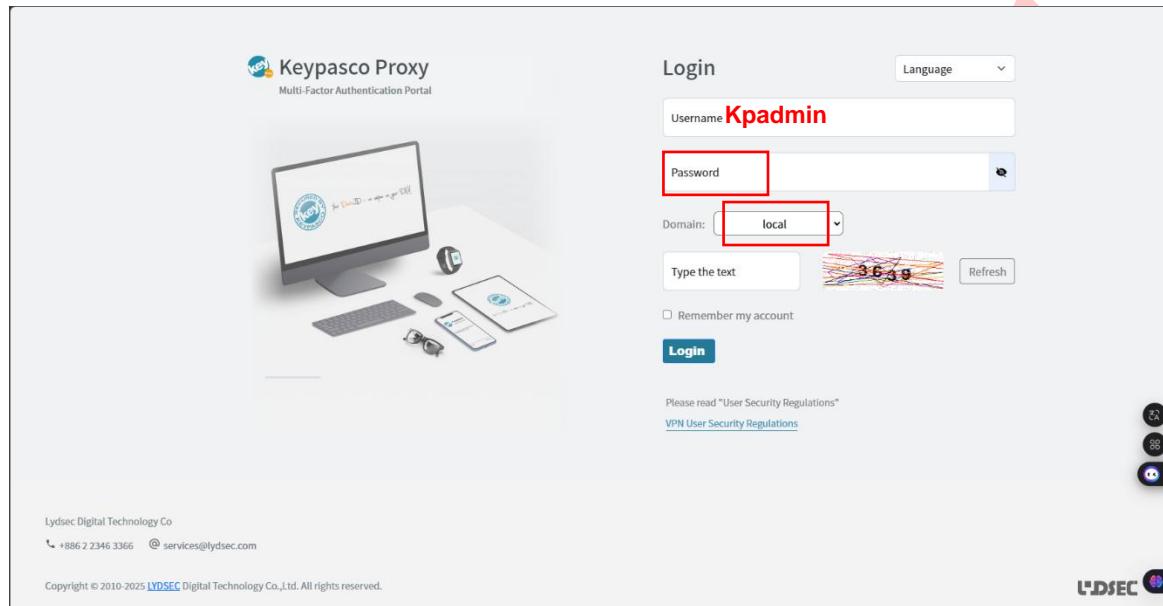
### Parameters Description:

- BorgenServer: FQDN of Borgen server

- P12Path: full path of certificate file
- P12Password: password of certificate file
- ICP: ICP of Borgen server
- ClientApi: Client API url

## 4.5 Testing

- Open browser and enter: <https://localhost> or FQDN
- Login with the local user “**kpadmin**” with P12 password



Keypasco Proxy  
Multi-Factor Authentication Portal

Login

Username **Kpadmin**

Password

Domain: local

Type the text **3639**

Remember my account

**Login**

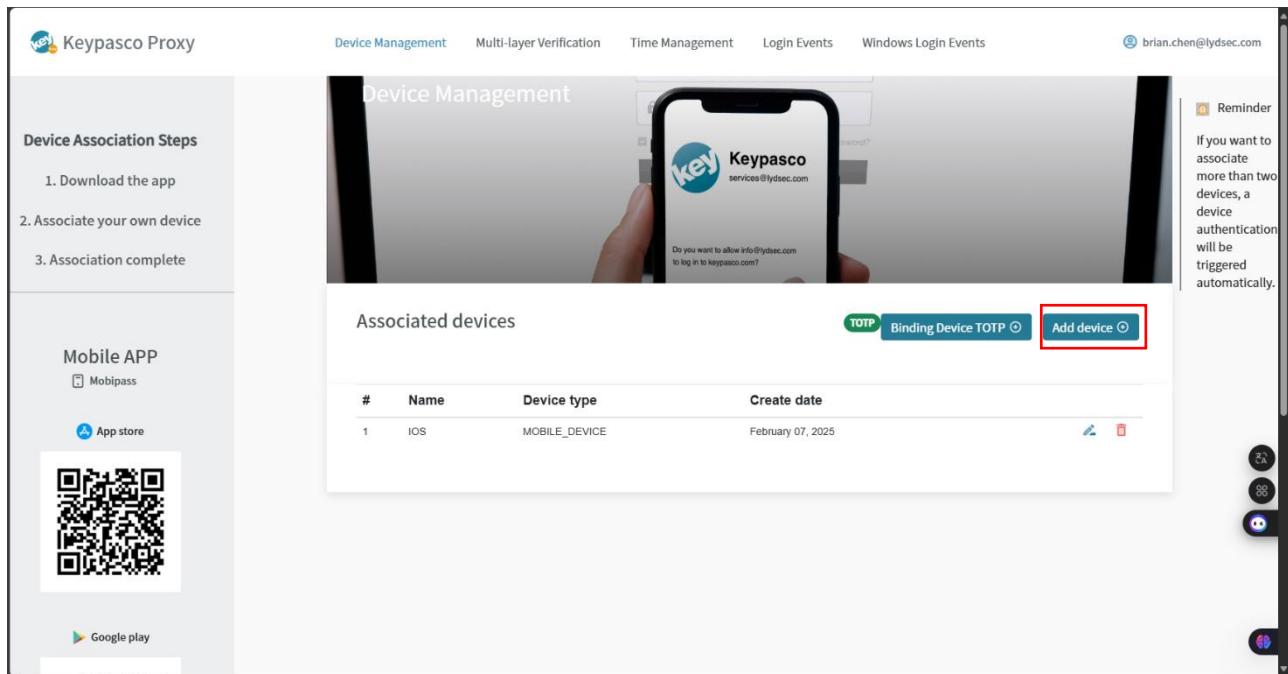
Please read "User Security Regulations"  
[VPN User Security Regulations](#)

Lydsec Digital Technology Co.  
+886 2 2346 3366 @ services@lydsec.com

Copyright © 2010-2025 LYDSEC Digital Technology Co.,Ltd. All rights reserved.

LYDSEC

- Click “Add Device” to bind device



**Device Association Steps**

- Download the app
- Associate your own device
- Association complete

**Mobile APP**

Mobipass  
App store  
QR code  
Google play

**Device Management**

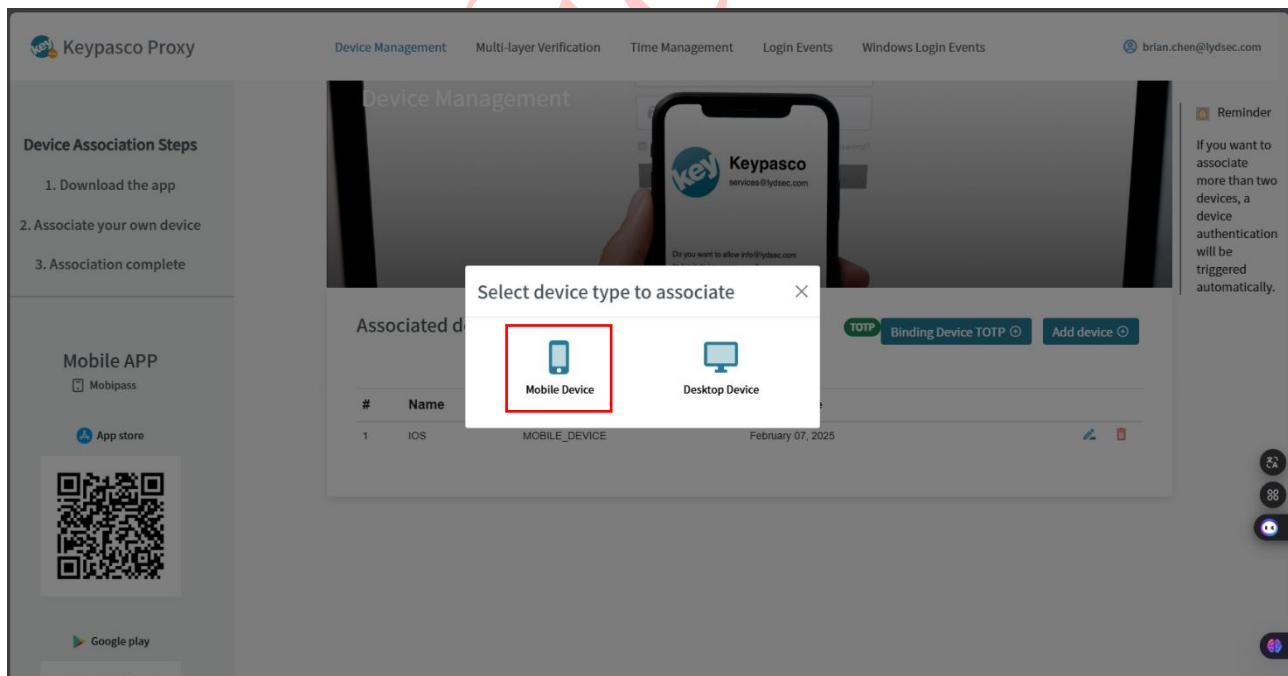
**Associated devices**

#	Name	Device type	Create date
1	IOS	MOBILE_DEVICE	February 07, 2025

**Reminder**  
If you want to associate more than two devices, a device authentication will be triggered automatically.

**Add device**

- Select “Mobile Device”



**Device Association Steps**

- Download the app
- Associate your own device
- Association complete

**Mobile APP**

Mobipass  
App store  
QR code  
Google play

**Device Management**

**Select device type to associate**

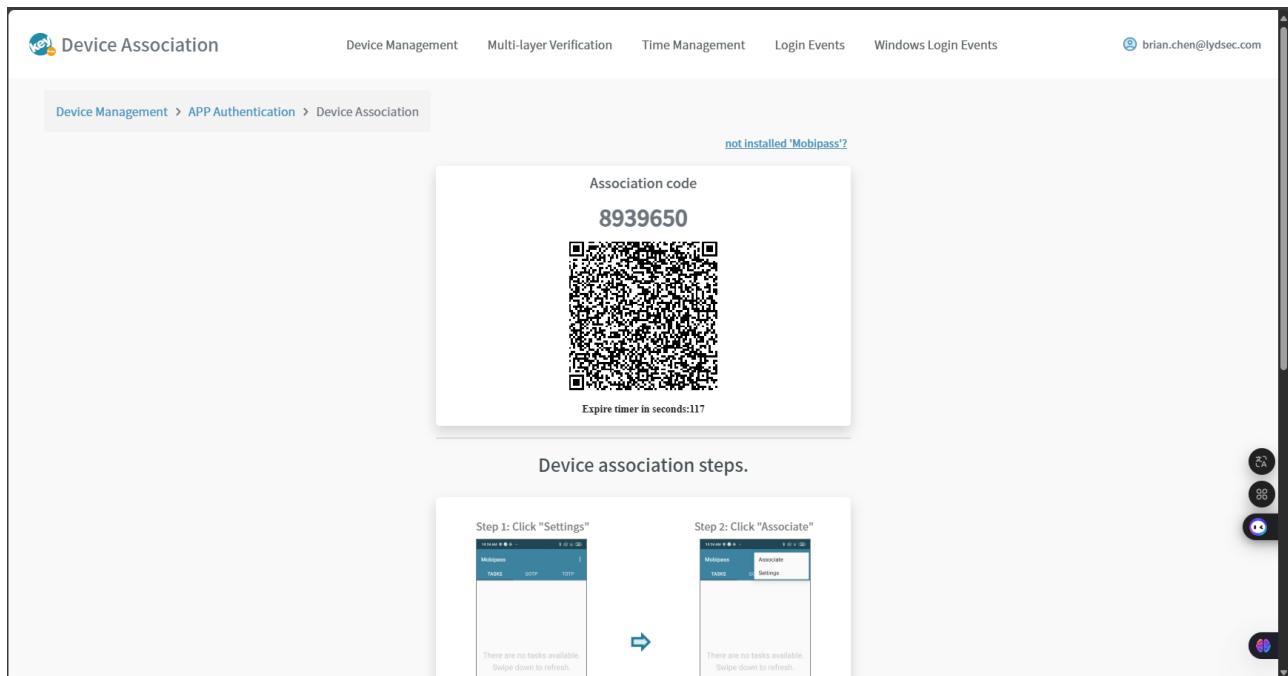
#	Name	Device type	Create date
1	IOS	MOBILE_DEVICE	February 07, 2025

**Reminder**  
If you want to associate more than two devices, a device authentication will be triggered automatically.

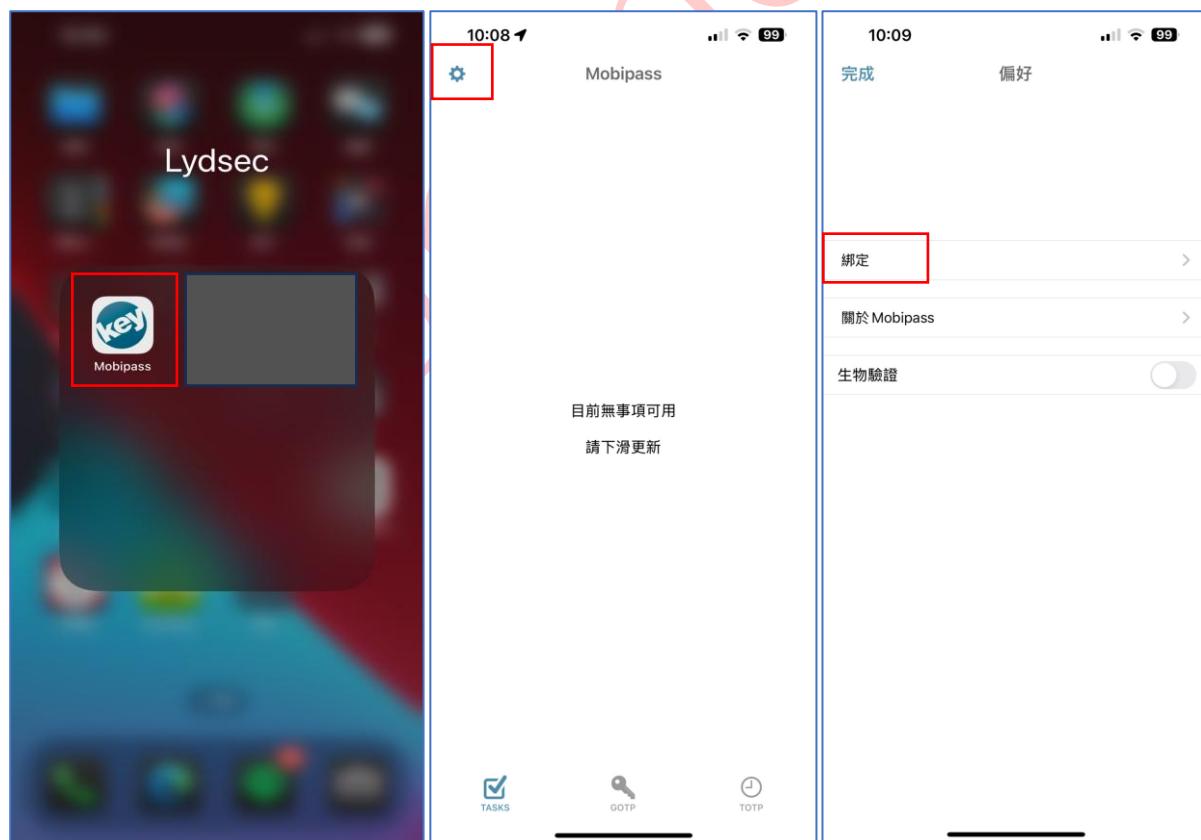
**Mobile Device**

**Desktop Device**

- The QRcode opened for mobile device binding

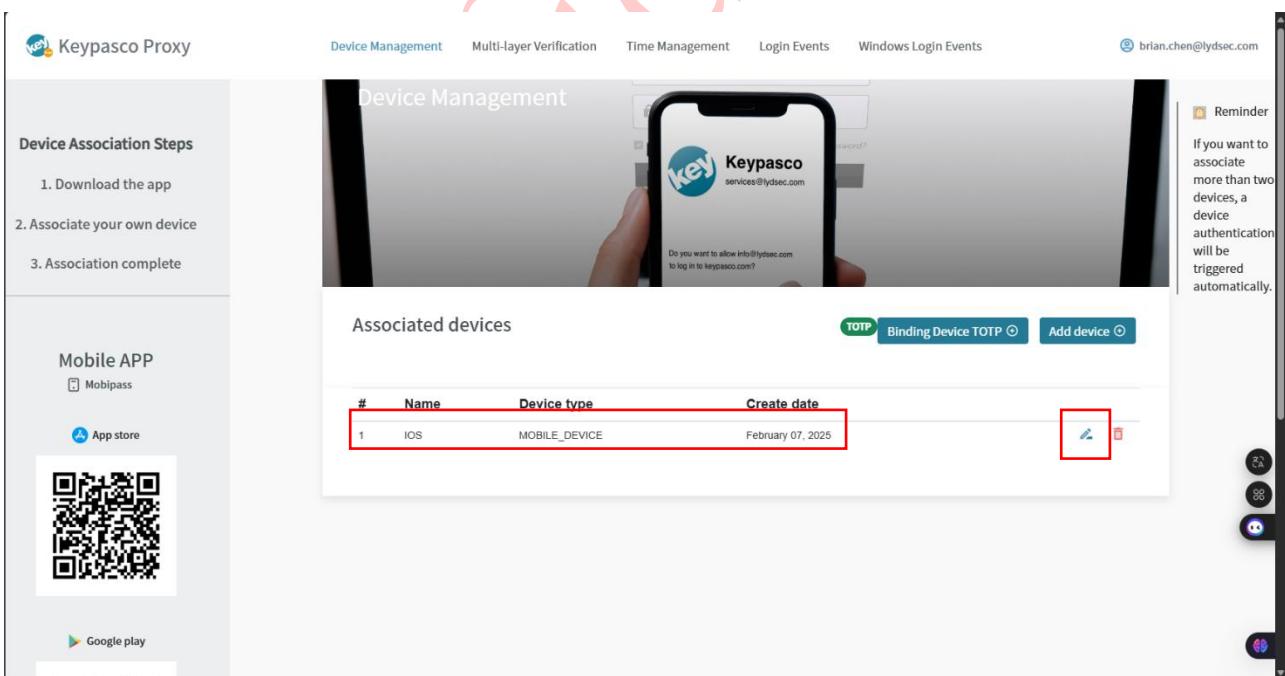


- Install Android/iOS application “Mobipass”
- Open it and scan QRcode to bind your device





- Show binding device information
- Click "Modify Device Name"



The screenshot shows the Keypasco Proxy web interface. On the left, there's a sidebar for 'Device Association Steps' with three steps: 1. Download the app, 2. Associate your own device, 3. Association complete. Below that is a section for 'Mobile APP' with download links for Mobicpass (Google play) and App store, and a QR code. The main area shows 'Device Management' with a sub-section 'Associated devices'. It lists one device: 'Name: IOS', 'Device type: MOBILE\_DEVICE', and 'Create date: February 07, 2025'. There are edit and delete icons next to the device entry. A reminder note on the right says: 'Reminder: If you want to associate more than two devices, a device authentication will be triggered automatically.'

Keypasco Proxy

Device Management Multi-layer Verification Time Management Login Events Windows Login Events brian.chen@lydsec.com

**Device Association Steps**

1. Download the app
2. Associate your own device
3. Association complete

**Mobile APP**

Mobipass

App store

Google play

Reminder

If you want to associate more than two devices, a device authentication will be triggered automatically.

Please perform device authentication first

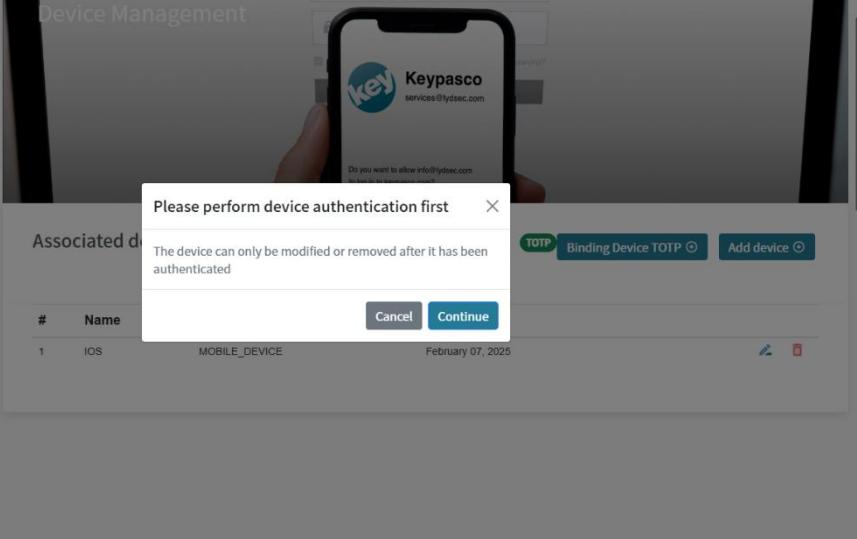
The device can only be modified or removed after it has been authenticated

Associated devices

#	Name		Date
1	IOS	MOBILE_DEVICE	February 07, 2025

TOTP Binding Device TOTP Add device

Cancel Continue



- Select “App Authentication”

Keypasco Proxy

Device Management Multi-layer Verification Time Management Login Events Windows Login Events brian.chen@lydsec.com

**Device Association Steps**

1. Download the app
2. Associate your own device
3. Association complete

**Mobile APP**

Mobipass

App store

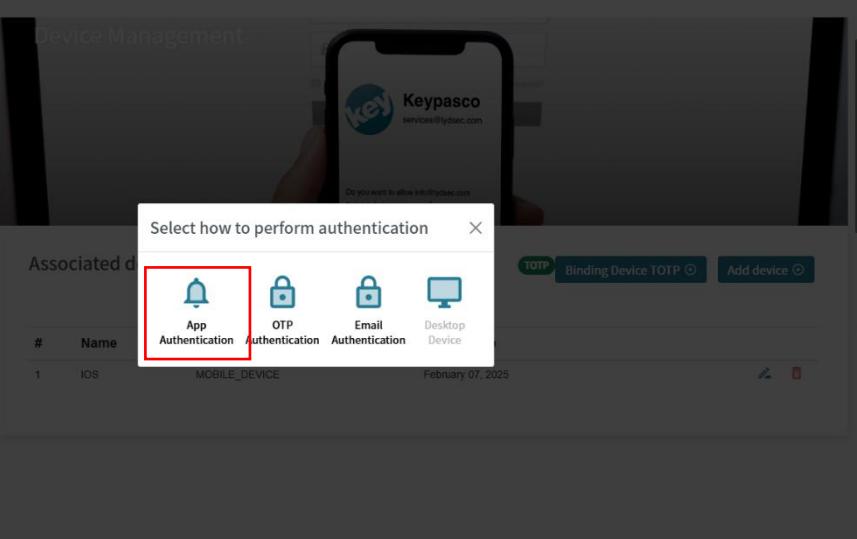
Google play

Reminder

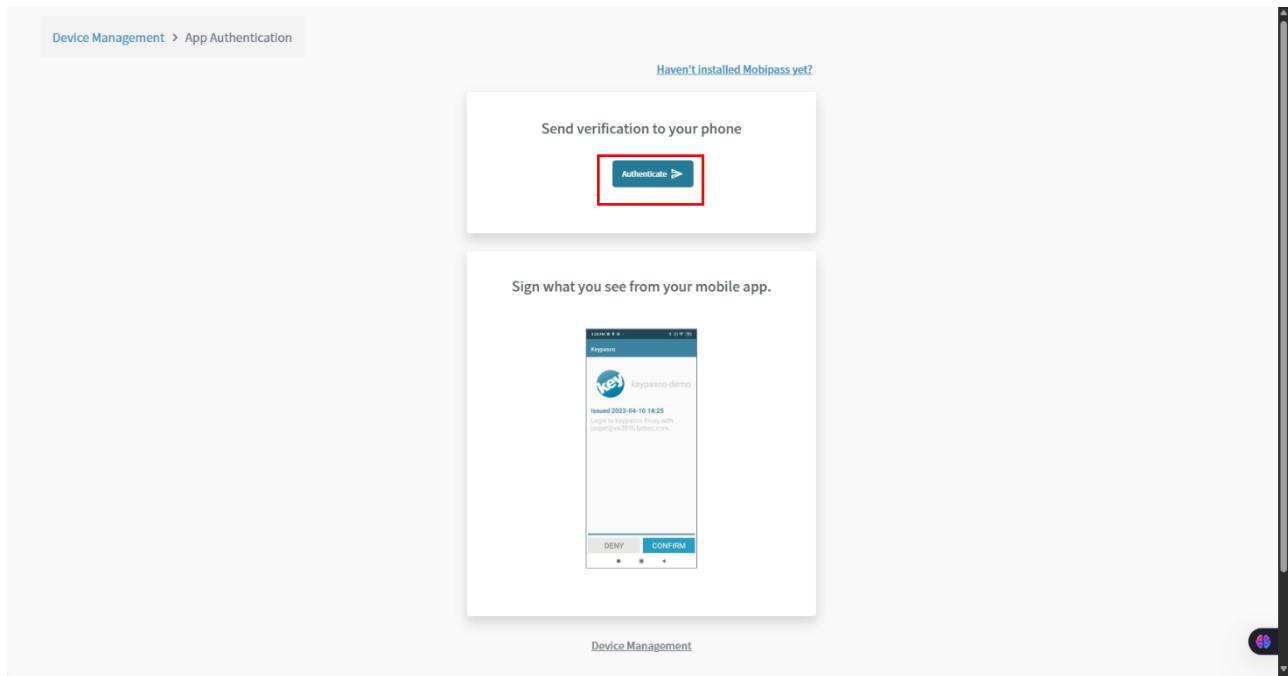
If you want to associate more than two devices, a device authentication will be triggered automatically.

Select how to perform authentication

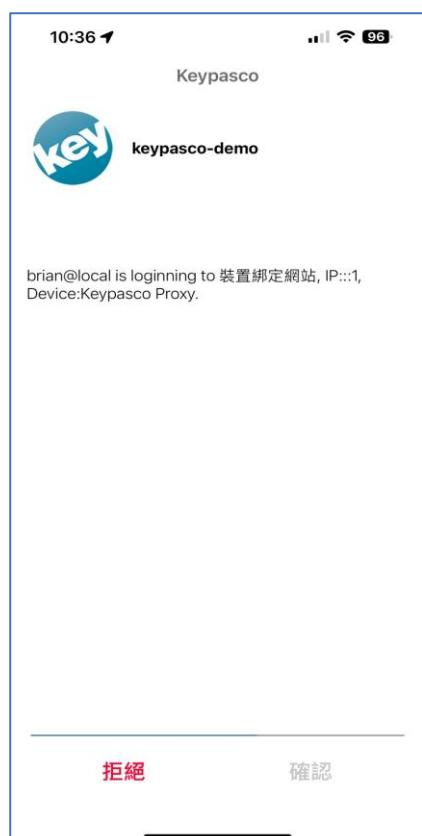
App Authentication	OTP Authentication	Email Authentication	Desktop Device
--------------------	--------------------	----------------------	----------------



- Click “Authenticate”



- The binding device will receive the push message





## 4.6 Problems

- If the problem “xxx.ps1 cannot be loaded because the execution of scripts is disabled on this system.” run follow command to get the permission.

```
>Set-ExecutionPolicy Unrestricted
```

or

```
>Unblock-File -Path "C:\Path\To\ KProxySetting.ps1"
```