



CITIC Telecom CPC



M@il Two-factor Authentication Setup Guide

June 2017



Table of Contents

1. About This Guide.....	3
2. Important Notes	3
3. Enable two-factor authentication feature (Administrator).....	3
4. Enable two-factor authentication feature (User).....	4
5. Web portal access	10
6. Setup MS Outlook (With SmartCLOUD M@il Connector)	10
7. Application code	10
8. One-time codes	11
9. Revoke trusted devices	12
10. Disable two-factor authentication	13

1. About This Guide

This file documents the two-factor authentication features on the web portal, mobile client and Microsoft Outlook client. Two-factor authentication is a technology that provides identification of users with the combination of two different components.

2. Important Notes

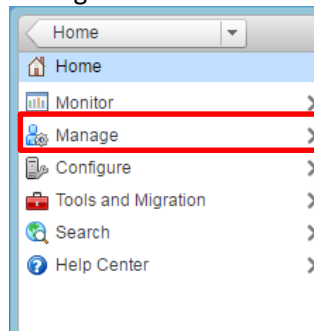
This section documents a list of items that users should be aware of when using SmartCLOUD M@il service.

1. **Mobile One Time Password (OTP) App** – To enable two-factor authentication feature and complete setup for each user, user must install OTP app in his/her owned mobile device.

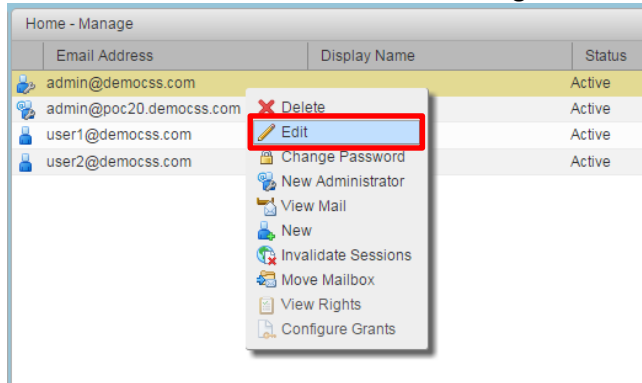
Remark: The recommended OTP app is “**Google Authenticator**” in both iOS and Android devices.

3. Enable two-factor authentication feature (Administrator)

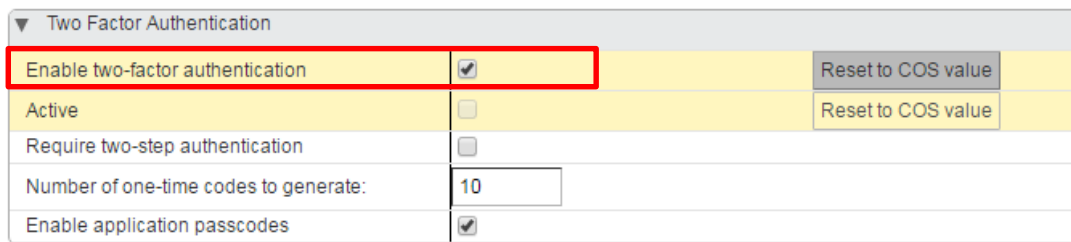
1. Login into admin console → Home → Manage



2. Select the user who need to enable two-factor authentication → Right click → Select “Edit”



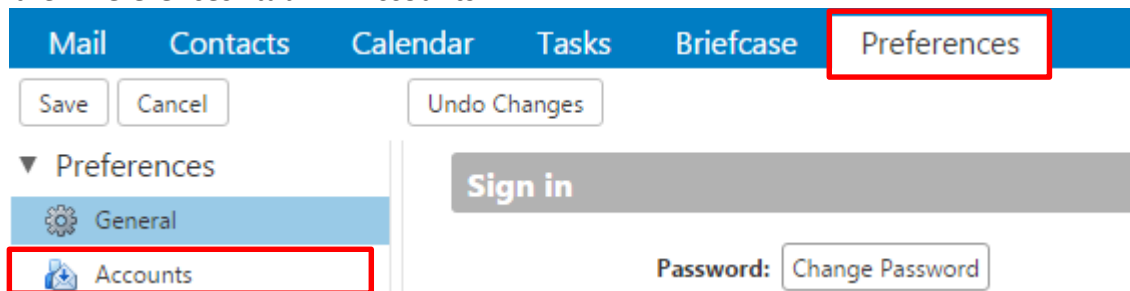
3. In the “Advanced” tab → click “Enable two-factor authentication” to enable two-factor authentication feature to user



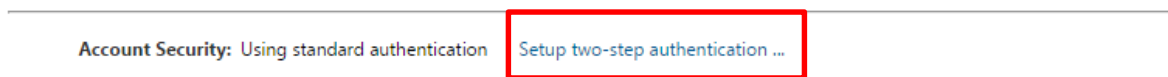
4. Enable two-factor authentication feature (User)

User must login into web portal to enable two-factor authentication.

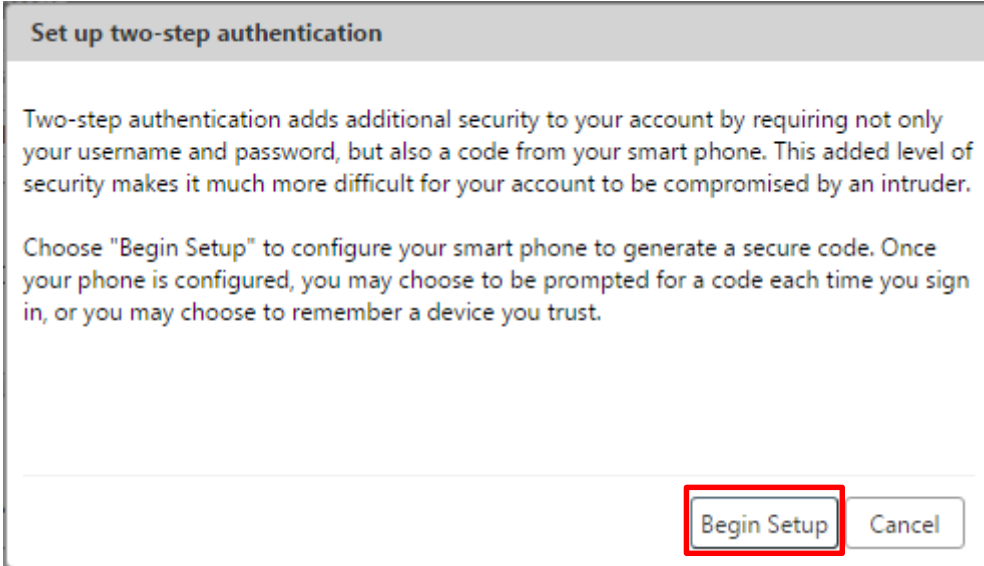
1. In the “Preferences” tab → “Accounts”



2. Click “Setup two-step authentication” to setup two-factor authentication



3. A pop-up window will be shown as below, click “**Begin Setup**”.



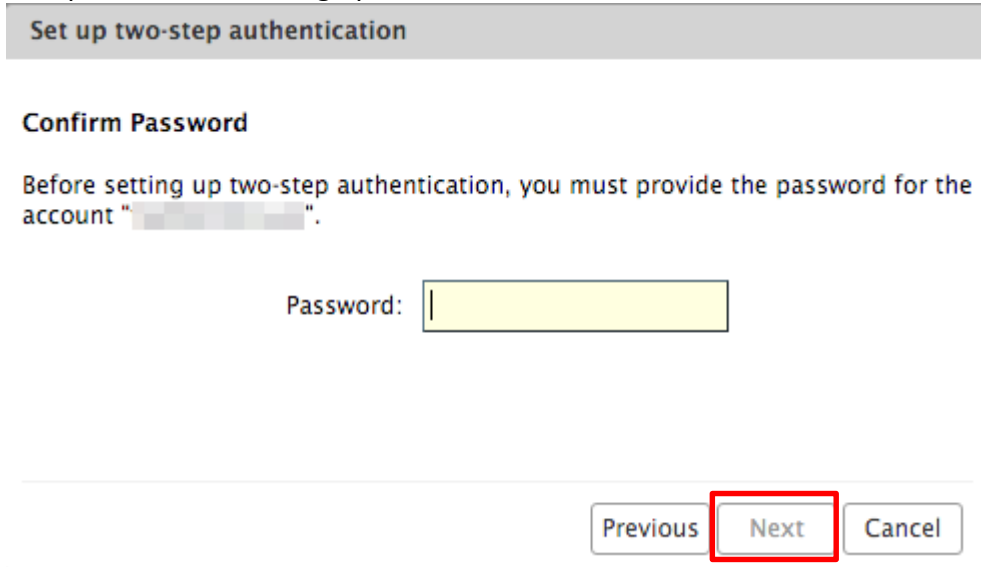
Set up two-step authentication

Two-step authentication adds additional security to your account by requiring not only your username and password, but also a code from your smart phone. This added level of security makes it much more difficult for your account to be compromised by an intruder.

Choose "Begin Setup" to configure your smart phone to generate a secure code. Once your phone is configured, you may choose to be prompted for a code each time you sign in, or you may choose to remember a device you trust.

Begin Setup Cancel

4. Enter user’s password for setting up two-factor authentication, click “**Next**”.



Set up two-step authentication

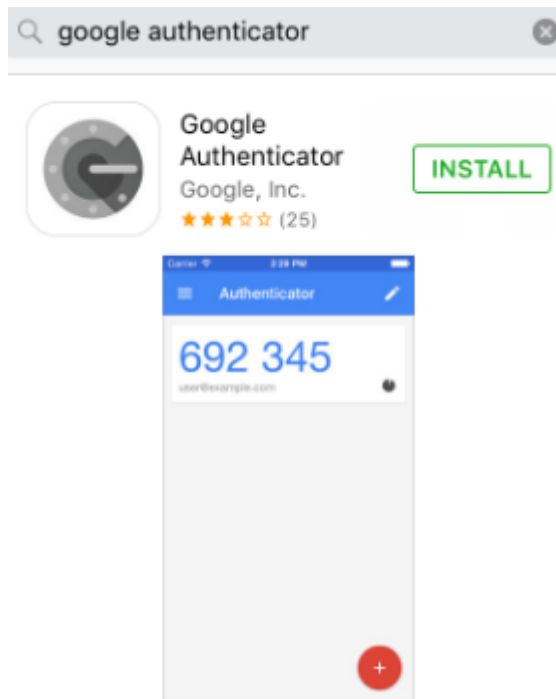
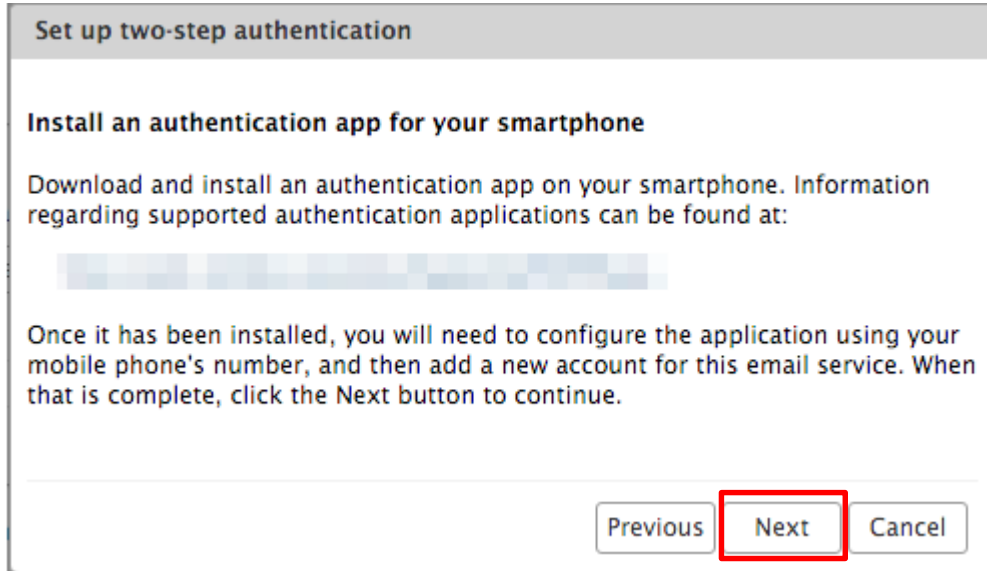
Confirm Password

Before setting up two-step authentication, you must provide the password for the account "[redacted]".

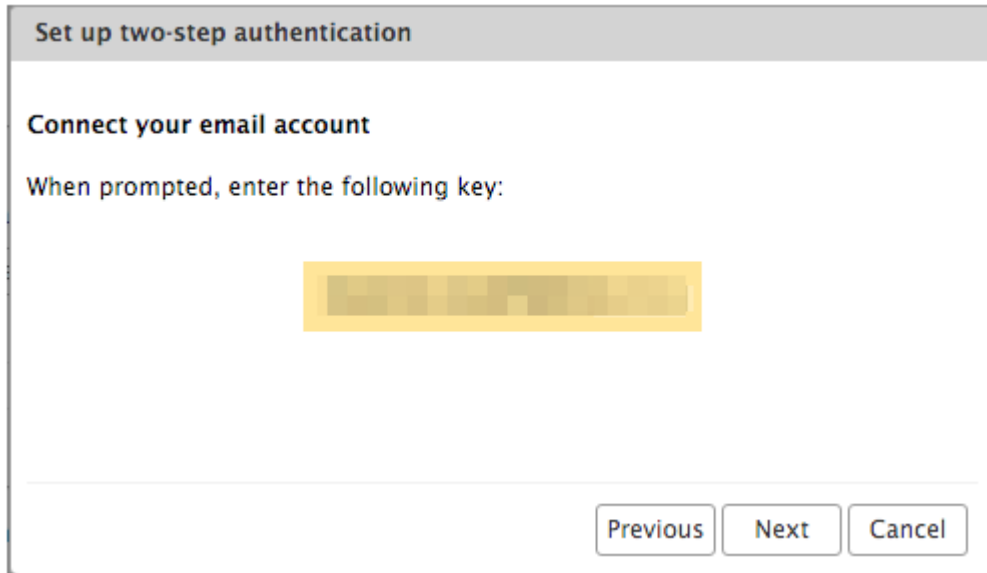
Password:

Previous **Next** Cancel

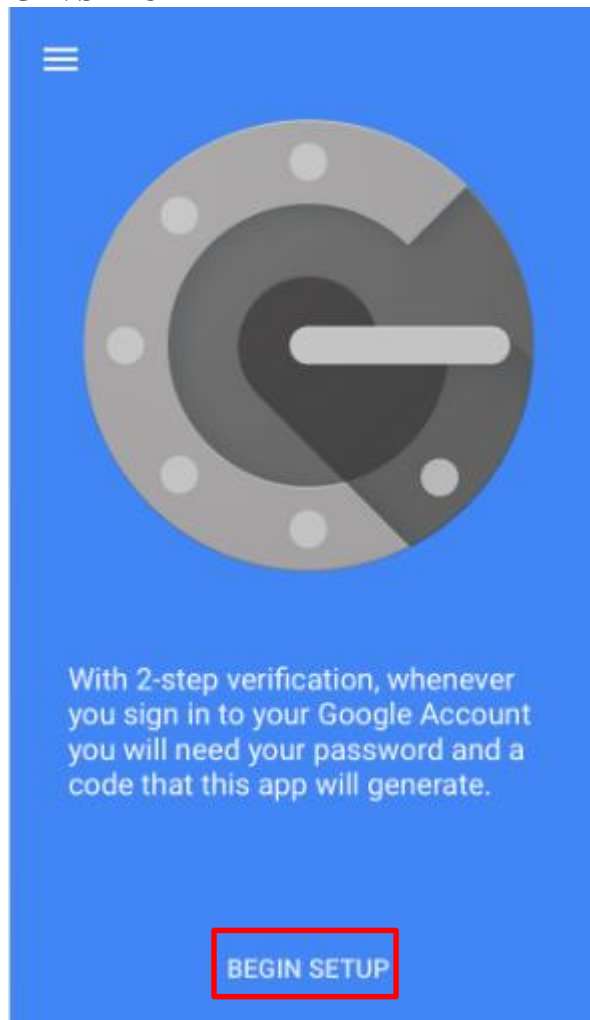
5. Install an OTP app into user’s mobile device, click “Next”. (In the App Store or Play Store, search by “Google authenticator”, then click “Install”.)



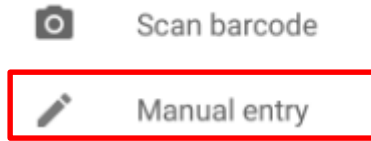
- Once installed the app in the mobile device, the wizard will show a unique key that the user must enter in the OTP app.



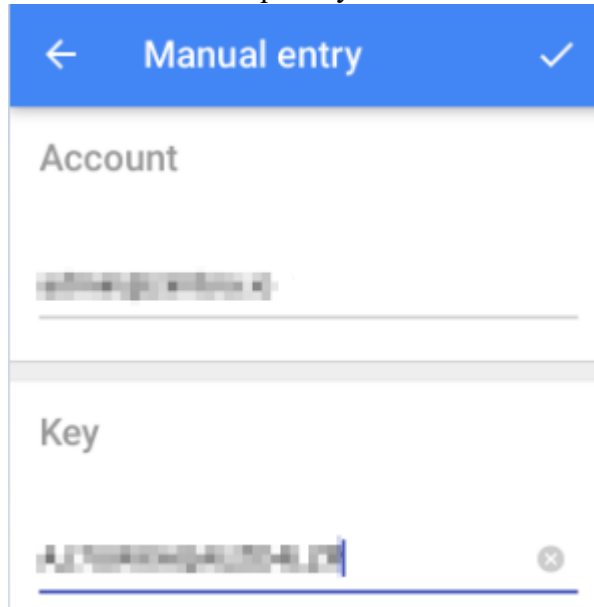
Open OTP app, select “**BEGIN SETUP**”



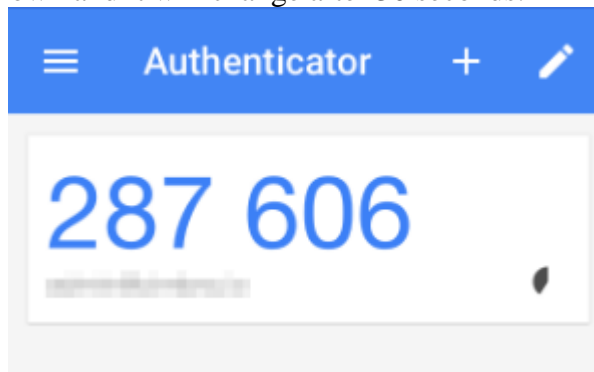
Select “Manual entry”



Enter email address in “Account” and the unique key from web client in “Key”



The 6-digit code will be shown and it will change after 30 seconds.



7. Finish the configuration in the web client, enter the 6-digit code showing in the OTP app and click “Next”.

Set up two-step authentication

Enter code to confirm setup

Once you have entered the key, enter the 6-digit verification code generated by the authentication app.

Code :

Previous
Next
Cancel

8. The two-factor authentication is now enabled.

Set up two-step authentication

Success!

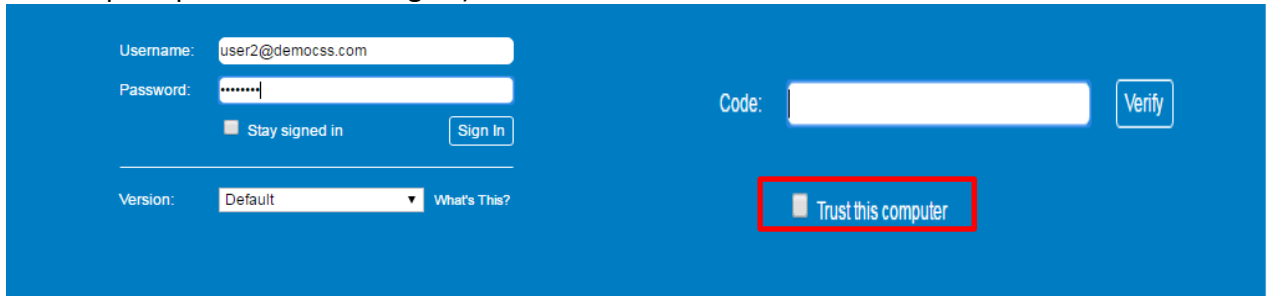
You have successfully configured your authentication app to provide security codes for this email service. You will be prompted for a code each time you sign in. In the event you don't have access to your phone, you may also print out a set of one-time codes that can be used to sign in.

Click "Finish" to complete setup and activate two-step authentication for your account.

Finish

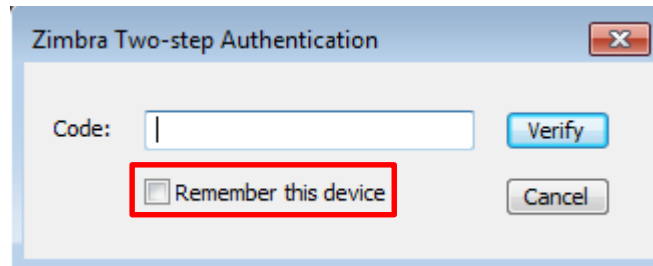
5. Web portal access

1. After setup two-factor authentication, every time login web portal, platform will request the 6-digit code from OTP app to verify your login (User can select “Trust this computer” and it will not prompt to enter code again)



6. Setup MS Outlook (With SmartCLOUD M@il Connector)

1. Follow the normal procedure to setup MS Outlook with SmartCLOUD M@il Connector (Ref link: http://www.citictel-cpc.com/smartcloud_mail/Outlook_Client_guide.pdf)
2. After input the login information, Outlook will prompt to input 6-digit code from OTP app, then click “Verify”. (User can select “Trust this computer” and it will not prompt to enter code again)

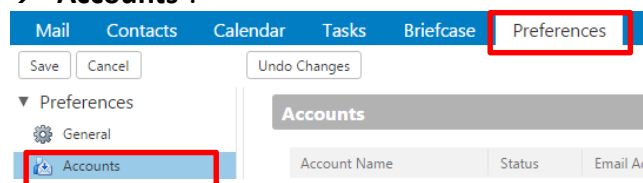


7. Application code

To access SmartCLOUD M@il platform with using mobile client, Outlook client (**without SmartCLOUD M@il connector installed**), user who enabled two-factor authentication need to generate an **application code**, this is a code that user will be used as “password”.

Remark: Application code can't share to different applications

1. Login into web portal.
2. Go to “Preferences” → “Accounts”.



3. Click “Add Application Code”.

Applications: Create passcodes for applications that don't support two-step authentication

Name	Created	Last Used
No results found.		

4. Enter application name, click “Next”.

Add Application Code

If your application does not support two-step authentication, generate a passcode to authorize the application the first time you use it to sign in to your account.

Application Name:

5. System will generate an application passcode.

Add Application Code

Enter this passcode when using the application for the first time to sign in to your account. This passcode gives your application permission to access your account.

Application Passcode: **RFSALANSXUAFAYDT**

6. User can view/add/revoke the application codes.

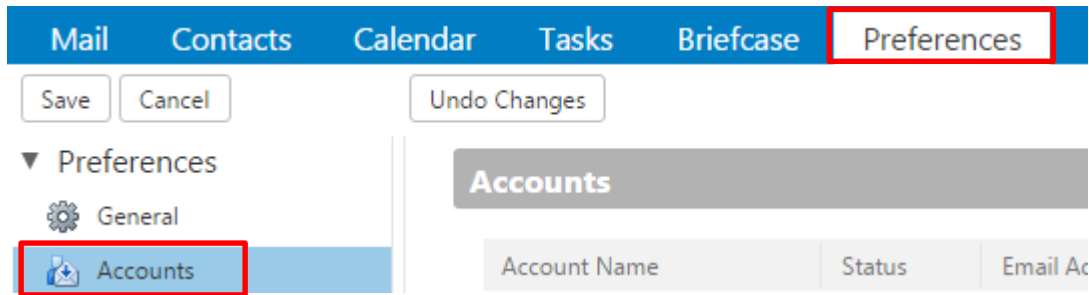
Applications: Create passcodes for applications that don't support two-step authentication

Name	Created	Last Used
Outlook without connector	1/6/17	-

8. One-time code

There may be some situations when the mobile can't generate passcode through OTP app or the device has been lost...etc. For those cases, user can generate multiple codes to use in case of emergency.

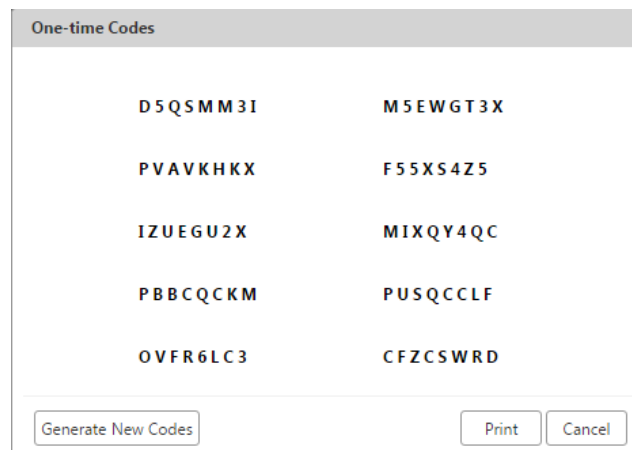
1. Login to web portal
2. Go to “Preferences” → “Accounts”.



3. Click “view”.

Account Security: Using two-step authentication [Disable two-step authentication ...](#)
One-time Codes: 10 unused codes [View](#)
Trusted Devices: You have 0 trusted device [revoke this device](#) [revoke all other devices](#)

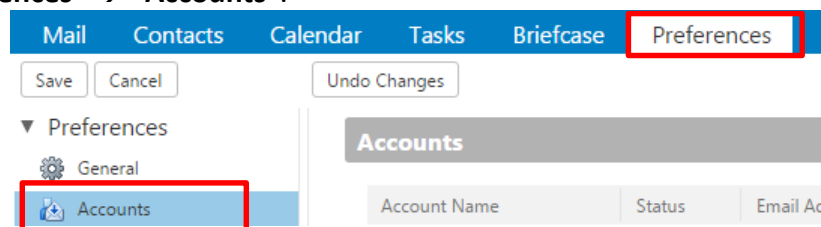
4. System will display multiple codes, user can re-generate new codes, print out those codes for emergency.



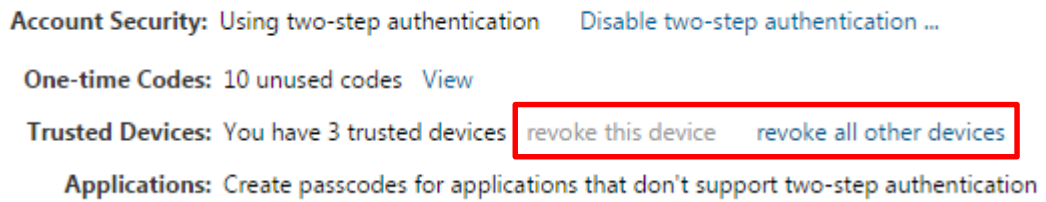
9. Revoke trusted devices

User can revoke trusted devices, then user will again need to provide 6-digit code to access the platform.

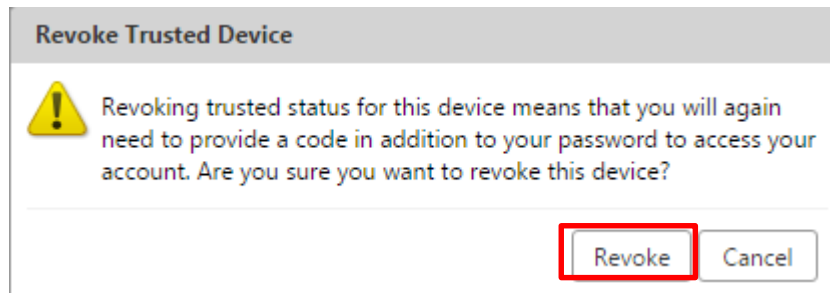
1. Login to the web portal.
2. Go to “Preferences” → “Accounts”.



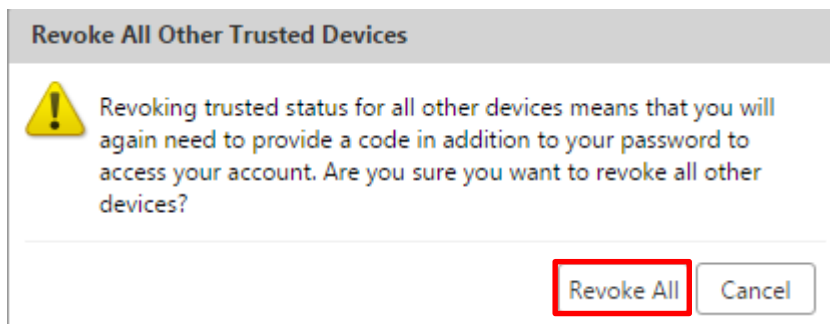
3. User can select “**revoke this device**” or “**revoke all other devices**”.



4. When user selected “**revoke this device**” (To revoke web portal only), a warning windows will display, click “**Revoke**”.



5. User also can select “**revoke all other devices**” (To revoke all type of trusted devices including web portal, Outlook client and mobile client), a warning windows will display, click “**Revoke All**”.



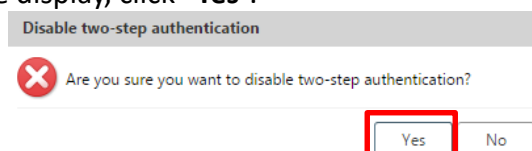
10. Disable two-factor authentication

User can disable two-factor authentication in web portal.

1. In user web portal, click “**Disable two-step authentication ...**”

Account Security: Using two-step authentication **Disable two-step authentication ...**

2. Warning message will be display, click “**Yes**”.



- End of Document -