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 \rightarrow Home \rightarrow Manage





2. Select the user who need to enable two-factor authentication \rightarrow Right click \rightarrow Select "Edit"



 In the "Advanced" tab → click "Enable two-factor authentication" to enable two-factor authentication feature to user

Two Factor Authentication							
Enable two-factor authentication 🖉 Reset to COS value							
Active			Reset to COS value				
Require two-step authentication							
Number of one-time codes to generate:	10						
Enable application passcodes							

4. Enable two-factor authentication feature (User)

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

1. In the "Preferences" tab \rightarrow "Accounts"

Mail	Contacts	Calendar	Tasks	Briefcase	Preferences	
Save	Cancel	Undo C	hanges			
▼ Prefer	ences	Sic	an in			
🔅 Gen	eral		,			
👌 Acco	ounts			Password: Cha	ange Password	

2. Click "Setup two-step authentication" to setup two-factor authentication

unt Security: Using standard authentication Setup two-st
--



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 "_____".

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**".)



中信國際電訊CPC

CITIC TELECOM CPC

6. 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"

With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.
BEGIN SETUP

中信國際電訊CPC

CITIC TELECOM CPC

Select "Manual entry"				
	0	Scan barcode		
		Manual entry		
Enter email address in "Acc	count"	and the unique key fro	m web client in	"Key"
	÷	Manual entry	~	
	Acco	ount		
	-	(particulo)		
	Key			
	ACT	ALMONTON D	0	

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

中信國際電訊CPC

5. Web portal access

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

Deserved						
Password:	••••••		Cor	de:		Verify
	Stay signed in	Sign In	000			, veiniy
Version:	Default 🔹 🔻	What's This?		Trust f	his computer	

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: <u>http://www.citictel-cpc.com/smartcloud_mail/Outlook_Client_guide.pdf</u>)*
- 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)

Zimbra Two-st	ep Authentication	×
Code:	emember this device	Verify Cancel

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".									
	Mail Contacts		Calenc	dar	Tasks	Briefcase	Preferer	nces	
	Save Cancel		Undo Changes						
	 Preferences General 			Ac	counts				
					counts				
	🖄 Acc	ounts		A	Account Name	2	Status	Email Ac	

Amember of CITIC TELECOM INTERNATIONAL 中信國際電訊集團成員



3. Click "Add Application Code".

J.	CHER Add	Application couc .				
	Арр	ications: Create passcodes for applications that don't support	two-step authentication			
		Name	Created	Last Used		
			No results found.			
		Add Application Code Revoke Code				
л	Enter annli	cation name click "Next"				
4.		Add Application Code				
		Add Application Code				
	If your application does not support two-step authentication, generate to authorize the application the first time you use it to sign in to your					
		Application Name:	Outlook without connector			
				Next Cancel		
5.	System wil	generate an application pas	scode.			
	·	Add Application Code				
		Enter this passcode when using the application for the first time to sign in to account. This passcode gives your application permission to access your acc				
		Application Passcode:	RFSALANSXUAFA	YDT		

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	-
Add Application Code Revoke Code		

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.

Close

- 1. Login to web portal
- 2. Go to "Preferences" \rightarrow "Accounts".

	Mail	Contacts	Calendar	Tasks	Briefcase	Preferen	ces
	Save	Cancel	Undo (Changes			
	▼ Prefer	ences eral	Ad	counts			
	🔬 Acc	ounts		Account Nam	e	Status	Email Ac
3. Clic	k " view ".						
	Account	Security: Using	two-step authent	ication Dis	able two-step au	thentication	
	One-tir	ne Codes: 10 unu	used 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.

One-time Codes	
D 5 Q S M M 3 I	M 5 E W G T 3 X
ΡVAVKHKX	F 5 5 X S 4 Z 5
I Z U E G U 2 X	ΜΙΧQΥ4QC
РВВСQСКМ	PUSQCCLF
OVFR6LC3	C F Z C S W R D
Generate New Codes	Print Cancel

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" \rightarrow "Accounts".



Amember of CITIC TELECOM INTERNATIONAL 中信國際電訊集團成員 3. User can select "revoke this device" or "revoke all other devices".



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



 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".

Revo	ke All Other Trusted Devices
1	Revoking trusted status for all other devices means that you will again need to provide a code in addition to your password to access your account. Are you sure you want to revoke all other devices?
	Revoke All Cancel

10. Disable two-factor authentication

User can disable two-factor authentication in web portal.

In user web portal, click "Disable two-step authentication ..."
 Account Security: Using two-step authentication
 Disable two-step authentication
 Obsolute two-step authentication
 Are you sure you want to disable two-step authentication?
 Ves No
 - End of Document

CITIC TELECOM INTERNATIONAL CPC LIMITED 20/F Lincoln House, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong T: 852 2170 7101 F: 852 2795 1262 W: www.citictel-cpc.com A member of CITIC TELECOM INTERNATIONAL 中信國際電訊集團成員