

# HOW TO GUIDE

**Working remotely – on demand login**



## Contents

1. What is Azure multi-factor authentication (MFA)? .....	2
2. Pre-requisites .....	2
3. Preparation – first time using your device .....	2
4. Logging in .....	3
5. Common Windows issues: .....	5
6. Logging into third-party services using Azure MFA .....	7
7. Switching between Azure MFA authentication methods .....	8
8. Azure MFA FAQ's .....	15

## 1. What is Azure multi-factor authentication (MFA)?

Azure MFA is a service provided by Microsoft that requires multiple verification methods when logging in. For example a user would need to provide their username and password plus a code sent to them via SMS.

Hiscox utilise this service to provide additional security when logging in to certain systems. The use of MFA significantly reduces the threat of malicious parties accessing Hiscox data.

## 2. Pre-requisites

1. You must be pre-registered with Azure MFA. Please contact the IT service desk if this has not been done.
2. Remote access is supported on Windows and Apple devices. Please note that at present Chromebooks are not supported for remote log in.

## 3. Preparation – first time using your device

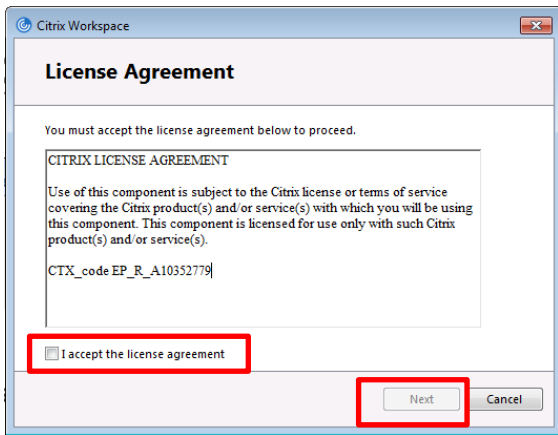
Once you have been sent confirmation that your remote access has been set up, please download Citrix Workspace for your operating system using the following links:

[Citrix Workspace for Windows](#)

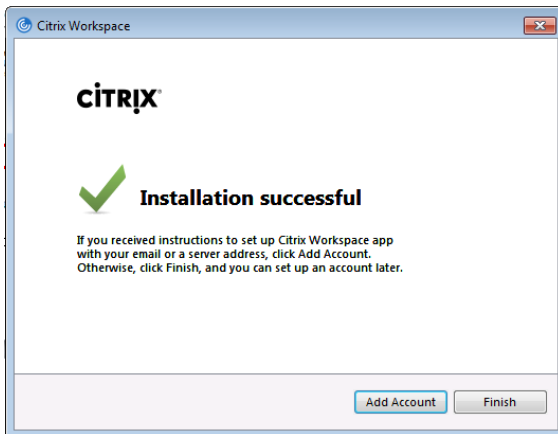
[Citrix Workspace for macOS](#)

If your Mac Book is running an older version then please download: <https://www.citrix.com/downloads/citrix-receiver/mac/receiver-for-mac-latest.html>

Once Receiver or Workspace have downloaded run the download. Select Start and then **tick** to agree the licence and select **Next**



Select **Install** (Do not tick Enable single sign-on)



Select **Finish**

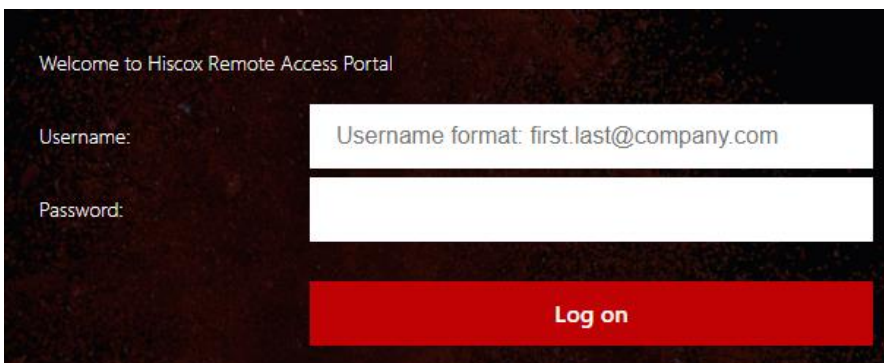
## 4. Logging in

Step 1 – navigate to <https://remote.hiscox.com> - suggested browsers are Chrome, Firefox, Safari and Edge.

**Note:** For the best security and experience, please ensure your browser is up to date with the latest updates.

Enter your Hiscox email address i.e. [firstname.lastname@hiscox.com](mailto:firstname.lastname@hiscox.com) and usual login password.

Select the **Log on** button



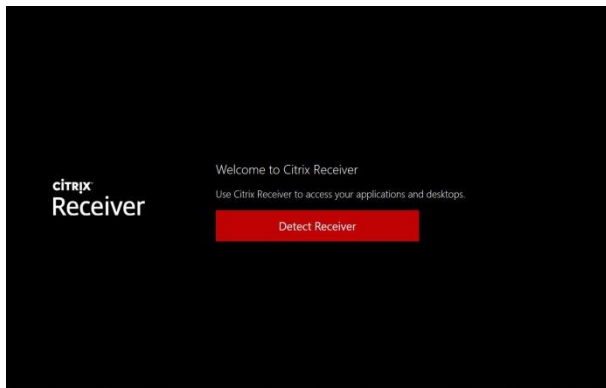
Step 2 – you will be redirected to additional authentication page to enter an Azure MFA code

In the password field, enter your Azure MFA verification code. Depending on your settings this may arrive via SMS or the Microsoft authenticator app.



After successfully authenticating you will be taken to the Citrix remote access portal where a list of available desktops will be displayed.

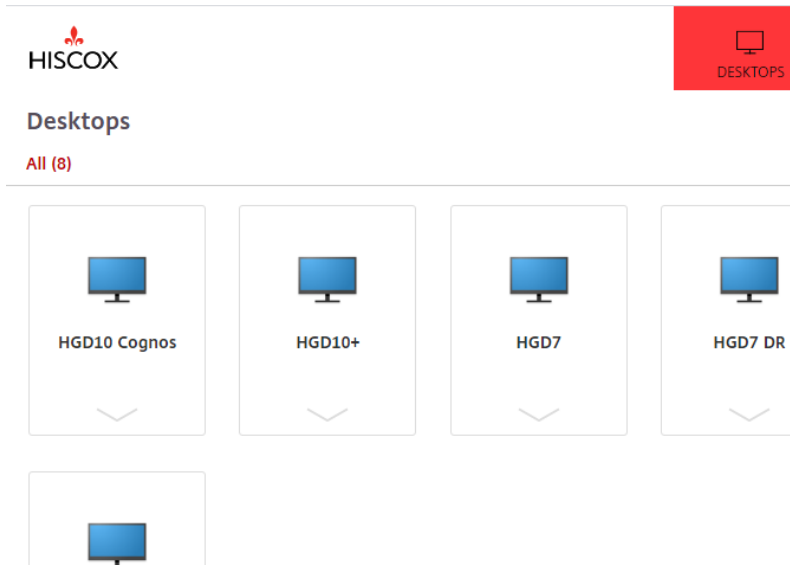
If this is the first time logging into the system from that device you may get to the following screen. If so, select **Detect Receiver**.



At the next screen – if you already have Citrix Receiver or Citrix Workspace installed select **Already Installed**.

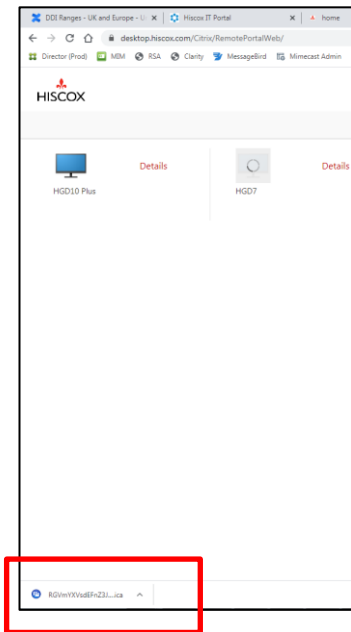
If you don't have Citrix received or Citrix Workspace installed start at the beginning of this document and install the relevant program before continuing.

You will then be taken to the Citrix remote access portal:



Click once on the desktop you would like to connect to.

If an .ica file is downloaded you can click on the download and select open.

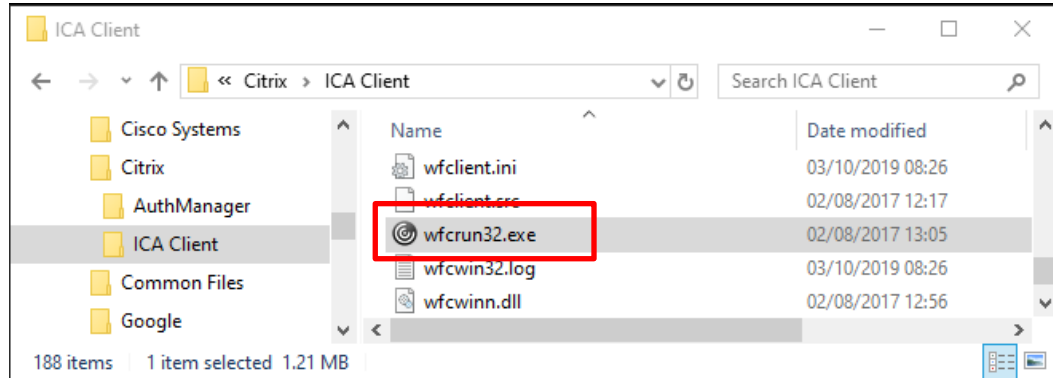


This will open your Citrix session in a new window.

## 5. Common Windows issues

- I have downloaded and install Citrix Receiver but when I click on HGD10 or HGD10+ icon I get an error message 'Do you want to open or save xxxxx.ica from remote.hiscox.com' or nothing happens.
- If you get this message you will need to associate the ICA file with Citrix received or Citrix Workspace by doing the following:
  - using Windows explorer, go to the downloads folder and search for that ICA file;
  - right-click on to the ICA file and then select the open with option;
  - click More Apps and Look for another app on my PC;

- browse to find the Citrix connection manager (C:\Program Files (x86)\Citrix\ICA Client\wfcrun32.exe) and then click OK;

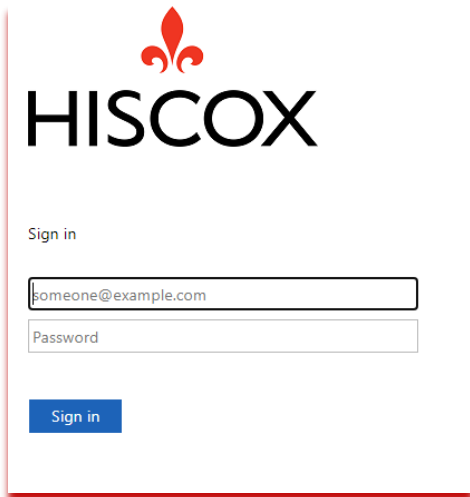


- you are likely to get an error message that there has been a failure as your login would have timed out. However, once the file is associated with the ICA File in your downloads should have an icon similar to this and the next time you log in the .ica file should open correctly and your session should start.

## 6. Logging into third-party services using Azure MFA

Step 1 – navigate to the login URL for the third-party service you want to use.

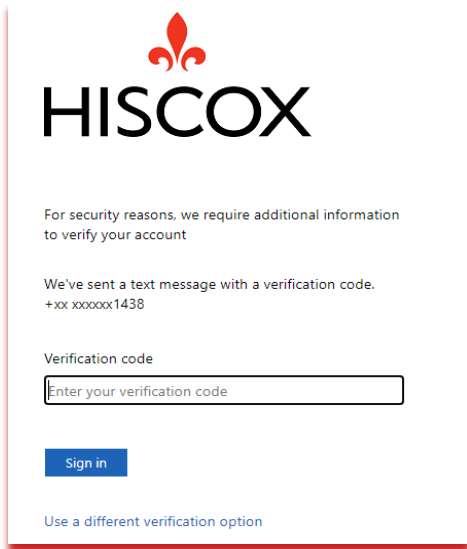
Step 2 – when attempting to login you will be redirected to a Hiscox login screen:



The screenshot shows the Hiscox login screen. It features the Hiscox logo at the top, followed by the text 'Sign in'. Below this are two input fields: one for an email address (containing 'someone@example.com') and one for a password. A blue 'Sign in' button is located at the bottom of the form.

Enter your email address i.e. [firstname.lastname@hiscox.com](mailto:firstname.lastname@hiscox.com) followed by your normal login password.

Step 3 – you may then be asked for additional information in the form of an Azure MFA token code. Depending on your setup this may arrive via SMS or the Microsoft authenticator app.



The screenshot shows a mobile-style login verification screen. At the top is the HISCOX logo. Below it, a message states: "For security reasons, we require additional information to verify your account". This is followed by another message: "We've sent a text message with a verification code. +xx xxxxxx1438". A label "Verification code" is positioned above a text input field containing the placeholder "Enter your verification code". Below the input field is a blue "Sign in" button. At the bottom, there is a link that says "Use a different verification option".

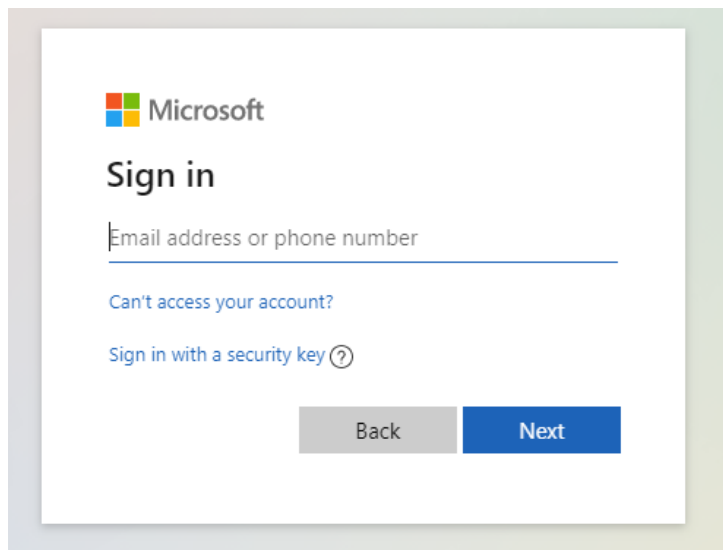
## 7. Switching between Azure MFA authentication methods

Currently there are four methods supported within Hiscox for Azure MFA.

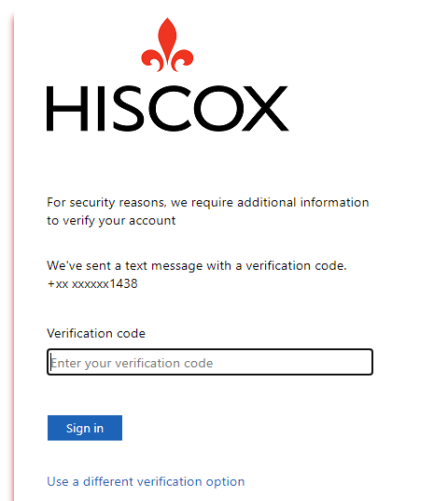
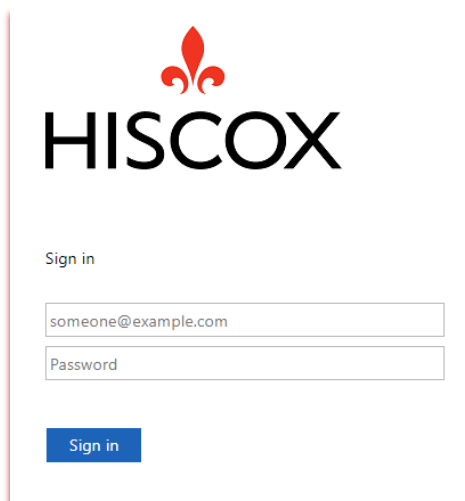
1. Microsoft authenticator app – push notification.
2. Microsoft authenticator app – token code.
3. SMS.
4. Phone call.

### Switching between Azure MFA authentication methods

- Navigate to <https://myaccount.microsoft.com/>

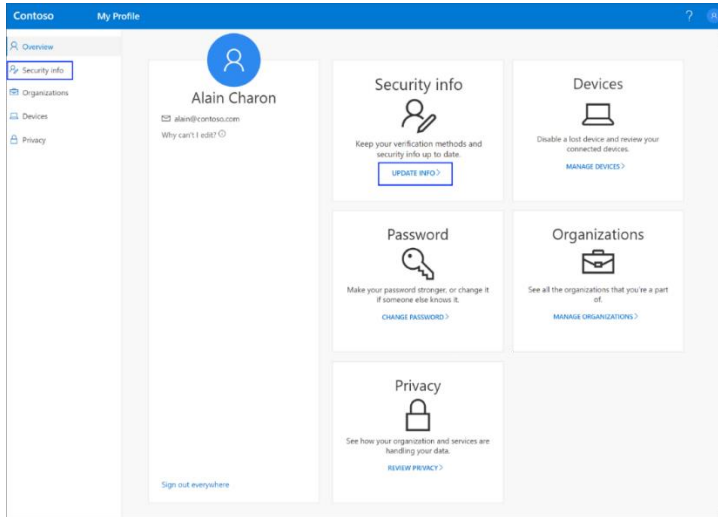


- Enter your Hiscox Email address i.e. [firstname.lastname@hiscox.com](mailto:firstname.lastname@hiscox.com) and click **Next**.
- You will be redirected to a Hiscox login screen. Complete the login.

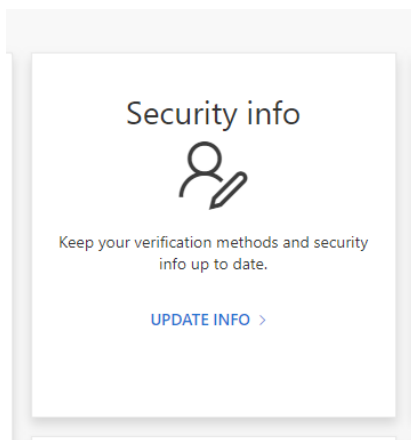




- Once you have authenticated you will be redirected to an Azure MFA setup page:

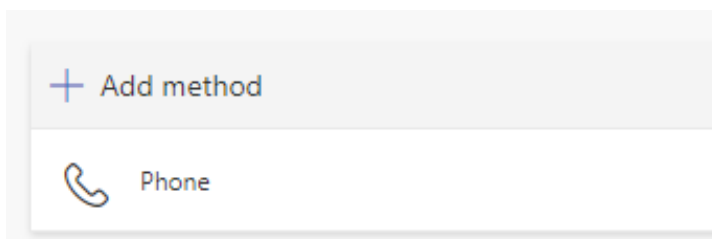


- Select **Security info** and click on **Update Info**

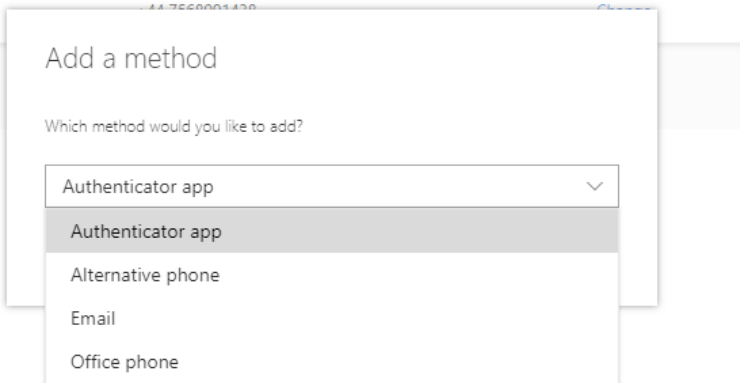


You will then be presented with a final page where you can update your authentication settings.

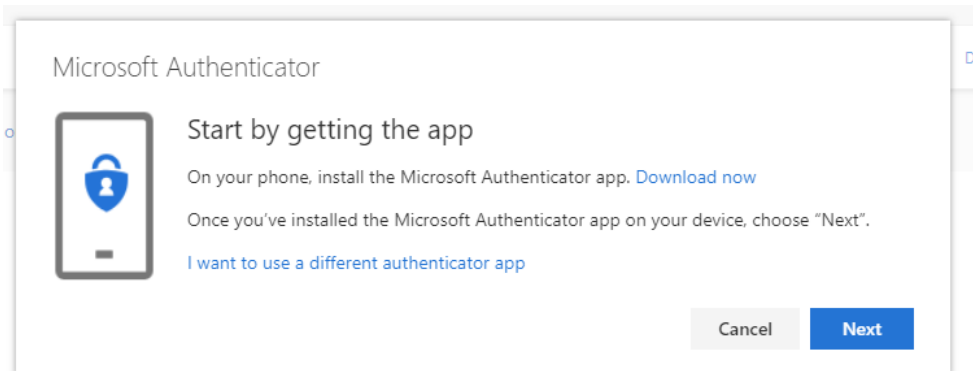
Click on **Add Method** as shown below



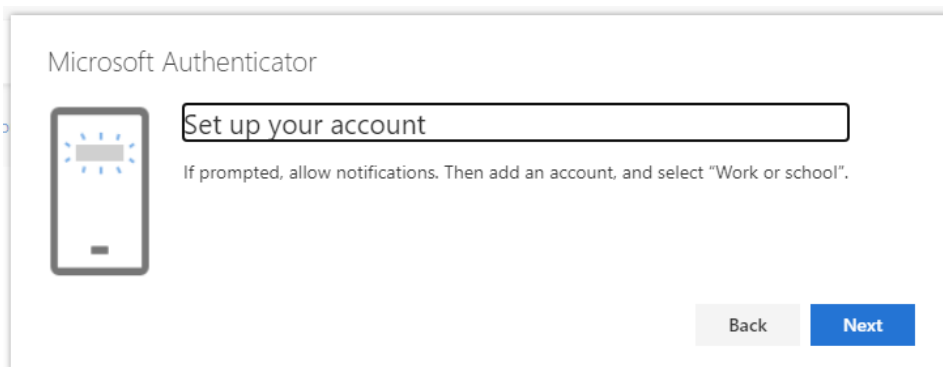
Once you click on 'Add a Method' window you will then be promoted to select your preferred authentication method and follow on screen instruction.



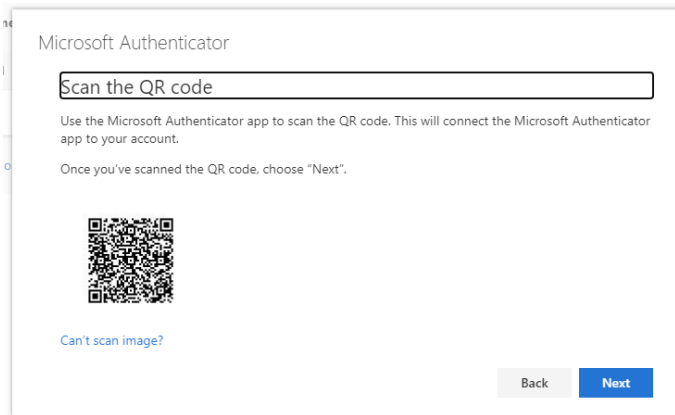
In this case we are switching from text message to authenticator app. The instructions on your screen will guide you through the steps you need to take.



Click **Next**



Click **Next**



You may receive a prompt asking whether to allow the app to access your camera. You must select **Allow** so the authenticator app can access your camera to take a picture of the QR code in the next step.

## 8. Azure MFA FAQs

### 1. What should I do if I don't receive a response on phone?

Attempt up to five times in five minutes to get a SMS for authentication. Microsoft uses multiple providers for delivering calls and SMS messages. If this approach doesn't work, open a support ticket with IT service desk. Third-party security apps may also block the verification code text message or phone call. If using a third-party security app, try disabling the protection, then request another MFA verification code be sent.

Try this	Guidance info
Restart your mobile device	Sometimes your device just needs a refresh. When you restart your device, all background processes and services are ended. The restart also shuts down the core components of your device. Any service or component is refreshed when you restart your device.
Verify your security information is correct	Make sure your security verification method information is accurate, especially your phone numbers. If you put in the wrong phone number, all of your alerts will go to that incorrect number. Fortunately, that user won't be able to do anything with the alerts, but it also won't help you sign-in to your account. To make sure your information is correct, see the instructions in the <a href="#">Manage your two-factor verification method settings</a> article.
Verify your notifications are turned on	Make sure your mobile device has notifications turned on. Ensure the following notification modes are allowed: <ul style="list-style-type: none"> <li>• phone calls;</li> <li>• your authentication app;</li> <li>• your text messaging app.</li> </ul> <p>Ensure these modes create an alert that is <i>visible</i> on your device.</p>
Make sure you have a device signal and Internet connection	Make sure your phone calls and text messages are getting through to your mobile device. Have a friend call you and send you a text message to make sure you receive both. If you don't receive the call or text, first check to make sure your mobile device is turned on. If your device is turned on, but you're still not receiving the call or text, there's probably a problem with your network. You'll need to talk to your provider. If you often have signal-related problems, we recommend you install and use the <a href="#">Microsoft authenticator app</a> on your mobile device. The authenticator app can generate random security codes for sign-in, without requiring any cell signal or Internet connection.

Try this	Guidance info
Turn off <b>Do not disturb</b>	Make sure you haven't turned on the <b>Do not disturb</b> feature for your mobile device. When this feature is turned on, notifications aren't allowed to alert you on your mobile device. Refer to your mobile device's manual for instructions about how to turn off this feature.
Check your battery-related settings	If you set your battery optimisation to stop less frequently used apps from remaining active in the background, your notification system has probably been affected. Try turning off battery optimisation for both your authentication app and your messaging app. Then try to sign-in to your account again.
Disable third-party security apps	Some phone security apps block text messages and phone calls from annoying unknown callers. A security app might prevent your phone from receiving the verification code. Try disabling any third-party security apps on your phone, and then request that another verification code be sent.

**2. I don't have my mobile device with me or I lost my mobile phone**

It happens. You left your mobile device at home, and now you can't use your phone to verify who you are. Maybe you previously added an alternative method to sign in to your account, such as through your office phone.

If so, you can use this alternative method now. If you never added an alternative verification method, you can contact IT service Help desk for assistance.

**3. I have a new phone number and I want to add it**

If you have a new phone number, you'll need to update your security verification method details. This enables your verification prompts to go to the right location. To update your verification method, follow the steps in the how to change my authentication provider section of this article and under add a method use 'phone number' instead of 'authenticator app' and follow on-screen instructions.

If this process is not working for you then please contact IT service desk to help you update your mobile information.

Hiscox  
1 Great St Helen's  
London EC3A 6HX  
United Kingdom

Location	External	Internal
<b>Belgium</b>	+32 2 788 26 41	432641
<b>Bermuda</b>	+1 441 278 8799	898799
<b>France</b>	+33 1 53 21 83 09	558309
<b>Germany</b>	+49 89 545 801 999	471999
<b>Ireland</b>	+353 1 238 1875	411875
<b>Luxembourg</b>	+352 24 61 32 99	443299
<b>Netherlands</b>	+31 20 799 1899	421899
<b>Portugal</b>	+351 21 319 1059	521059
<b>Spain</b>	+34 910 38 68 99	506899
<b>UK</b>	+44 20 7448 6543	116543
<b>USA</b>	+1 877 456 4911	116543

E [servicedesk@hiscox.com](mailto:servicedesk@hiscox.com)  
[www.hiscox.co.uk](http://www.hiscox.co.uk)