

Global Financial Services, LLC

GFS Advisors, LLC

Business Continuity Plan

Employee Manual

September, 2024

TABLE OF CONTENTS

1. INTRODUCTION	3
2. FIRM POLICY.....	3
Infectious Disease Update:.....	3
3. EMERGENCY RESPONSE TEAM	5
4. KEY EMPLOYEES ASSIGNED TO BCP ROLES	6
5. KEY SERVICE PROVIDERS & CONTACT INFORMATION	6
6. EMPLOYEE CONTACT INFORMATION	7
7. CALL TREE.....	7
8. BUSINESS DISRUPTION ACTION PLAN.....	7
APPENDIX A – Emergency Contact List	8
APPENDIX B – Call Tree.....	8
APPENDIX C – Sophos VPN Instructions for GFS Remote Access.....	8
APPENDIX D – Key Service Providers.....	8

1. INTRODUCTION

Emergencies can occur at any time, without warning. Careful planning can help personnel handle crises and emergencies with appropriate responses. Therefore, it is the responsibility of all employees to be familiar with this Business Continuity Plan (“BCP”).

This BCP applies to: (i) **Global Financial Services, LLC**, a registered broker-dealer with the Financial Industry Regulatory Authority (FINRA) and an Introducing Broker with the National Futures Association; and (ii) **GFS Advisors, LLC**, an investment adviser registered with the U.S. Securities and Exchange Commission, (collectively, “the Firm” or “Global”). This BCP was prepared and is maintained to address the requirements under applicable regulatory rules (e.g., FINRA Rule 4370. Business Continuity Plans and Emergency Contact Information).

2. FIRM POLICY

Global’s policy is to respond to any emergency or significant business disruption by assessing the severity and potential duration of the disruption followed by the implementation of disaster recovery protocols. The priority will be to safeguard the lives of employees, protect customer and Firm assets, and quickly recover and resume operations. Recovery time objective is within 24 hours. However, if Global is unable to recover and resume operations, it will ensure customers' prompt access to funds and securities through clearing firm and custodial relationships.

The BCP anticipates two types of disruptions, localized and systemic. Localized disruptions may affect the Firm’s ability to communicate and conduct business, such as a regional weather event or power outage. However, a systemic disruption may prevent the operation of securities markets or a significant number of firms and/or counterparties, such as a large-scale terrorist attack or a global pandemic¹ involving an infectious disease. Our response to a large-scale systemic disruption may rely more heavily on other organizations and infrastructure, particularly on the capabilities of our clearing firms.

Infectious Disease Update:

Coronavirus Disease (COVID-19) – How to Protect Yourself & Others

Preventive Actions²

The CDC recommends preventive actions to help prevent the spread of COVID-19 and other respiratory diseases, including:

- Get Vaccinated and stay up to date on your COVID-19 vaccines.
 - COVID-19 vaccines are effective at preventing you from getting sick.
 - COVID-19 vaccines are highly effective at preventing severe illness, hospitalizations, and death.

¹ The **World Health Organization** defined a pandemic as “the worldwide spread of a new disease” that affects large numbers of people.

² Source: Center for Disease Control and Prevention.

- Getting vaccinated is the best way to slow the spread of SARS-CoV-2, the virus that causes COVID-19.
- CDC recommends that everyone who is eligible stay up to date on their COVID-19 vaccines, including people with weakened immune systems.
- Wear a mask.
 - Everyone ages 2 years and older should properly wear a well-fitting mask indoors in public in areas where the COVID-19 Community Level is high, regardless of vaccination status.
 - Wear a mask with the best fit, protection, and comfort for you.
 - If you are in an area with a high COVID-19 Community Level and are ages 2 or older, wear a mask indoors in public.
 - If you are sick and need to be around others, or are caring for someone who has COVID-19, wear a mask.
 - If you are at increased risk for severe illness, or live with or spend time with someone at higher risk, speak to your healthcare provider about wearing a mask at medium COVID-19 Community Levels.
 - People who have a condition or are taking medications that weaken their immune system may not be fully protected even if they are up to date on their COVID-19 vaccines. They should talk to their healthcare providers about what additional precautions may be necessary.
- Avoid close contact with people who are sick.
- Avoid touching your eyes, nose, and mouth.
- Stay home when you are sick (if you feel it necessary, consider telecommuting).
- Cover your cough or sneeze with a tissue, then throw the tissue in the trash.
- Clean and disinfect frequently touched objects and surfaces using a regular household cleaning spray or wipe.
- Wash your hands often with soap and water for at least 20 seconds, especially after going to the bathroom; before eating; and after blowing your nose, coughing, or sneezing. If soap and water are not readily available, use an alcohol-based hand sanitizer with at least 60% alcohol. Always wash hands with soap and water if hands are visibly dirty.

For information about handwashing, see [CDC's Handwashing website](#).

For information specific to healthcare, see [CDC's Hand Hygiene in Healthcare Settings](#).

These are everyday habits that can help prevent the spread of several viruses.

In the event of an emergency or significant business disruption, Global's Chief Operating Officer will assess the situation, and if necessary, make a declaration that emergency conditions exist. If the declaration is made, consistent with FINRA Rule 3110(f)(2)(A)(vii), key employees assigned with business continuity roles will be contacted and directed to work remotely from their homes or another temporary location established in response to the implementation of the business

continuity plan³. Each employee has a BCP Manual which describes the required activities and how those activities should be conducted outside of the office.

3. EMERGENCY RESPONSE TEAM

When circumstances result in a significant business interruption, the Chief Operating Officer will attempt to ascertain the severity and duration of the interruption, and if necessary, make the declaration to invoke emergency protocols. If he determines that emergency conditions indeed exist, he will then notify the Emergency Response Team (level two) to begin their assigned roles pursuant to this BCP Plan. If the Chief Operating Officer is unable to make the declaration, then the responsibility falls to the Chief Compliance Officer. Once contacted, the Emergency Response Team will contact support staff in accordance with Call Tree procedures.

LEVEL ONE:

Jack Bruno (Chief Operating Officer) – has primary responsibility for declaration of emergency protocol.

William Cathriner (Chief Compliance Officer) – has back-up responsibility for declaration of emergency protocol, if the Chief Operating Officer is unable to make the declaration.

LEVEL TWO:

Gordon Bell Dilia Medrano or Carolee Mitchell

Adria Salazar

Gerardo Chapa (primary); Victor Villarreal or Claudia Reyes (back-up)

Daniel Priwin or Juan Carlos Cantu (primary); Bernardo Velez (back-up)

Jose Sepulveda

Alfredo Tellez

³ For regulatory purposes, FINRA defines a "**Branch Office**" as any location where one or more associated persons of a member regularly conducts the business of effecting any transactions in, or inducing or attempting to induce the purchase or sale of, any security, or is held out as such, **excluding a temporary location established in response to the implementation of a business continuity plan.**

4. KEY EMPLOYEES ASSIGNED TO BCP ROLES

Key Employees are listed below with their assigned area of responsibility. Each key employee will call employees as designated by the call tree along with any other employee that is in his/her area to give the status of the business interruption and update them as necessary. Individual job tasks may be assigned to each Global employee as needed.

KEY EMPLOYEES	AREA OF RESPONSIBILITY
Jack Bruno	Operational Assessment, Alternative Communications, and Assuring Customer Access to Funds and Securities Financial Assessment and Critical Banking Constituents
William Cathriner	Regulatory Communications and Alternate Physical Locations
Gordon Bell	Mission Critical Systems, including Access to Network, Phones, and Electronic Communications
Dilia Medrano or Carolee Mitchell	Critical Trading Constituents, including Settlement and TRACE Reporting
Adria Salazar	Phones and Manual Routing of Calls
Gerardo Chapa	Customer Trading and Communications
Daniel Priwin or Juan Carlos Cantu	Customer Trading and Communications
Jose Sepulveda	Customer Trading and Communications
Alfredo Tellez	Customer Trading and Communications

5. KEY SERVICE PROVIDERS & CONTACT INFORMATION

See the list of Key Service Providers and relevant contact information in [Appendix D](#).

6. EMPLOYEE CONTACT INFORMATION

Please retain a copy of the Emergency Contact List in a secure and easily accessible place.
See **Appendix A**: Emergency Contact List – Revised 04/25/2024.

7. CALL TREE

The Call Tree referenced in Appendix B illustrates the protocol for contacting employees in the event that Firm-wide communication is required relative to an emergency or significant business disruption. Employees that cannot be reached within two hours of the implementation of disaster recovery protocols must be reported to Jack Bruno, the head of the Emergency Response Team.

Please retain a copy of the Call Tree in a secure and easily accessible place.
See **Appendix B**: Call Tree – Revised 04/25/2024.

8. BUSINESS DISRUPTION ACTION PLAN

The Emergency Response Team is responsible for carrying out the BCP Action Plan. In this regard, the Response Team will:

1. Ascertain the severity and potential duration of the disruption.
2. Implement disaster recovery protocols.
3. Decision to invoke Dallas recovery site (Regus Workplace Notice to Invoke - Call the 24/7 Invocation Line ph. 972-776-5355).
4. Communicate with employees that disaster recovery protocols are active, alerting Business Constituents as necessary.
5. Verify connectivity for key employees. Employees may connect using the VPN, or in the case of power failure in the Post Oak Building, employees may access mission critical applications directly through the web using a secure internet connection, e.g., a private WiFi network with password protection, bypassing the VPN configuration. Note, the use of public WiFi networks is expressly prohibited under this BCP plan.
 - a. **Virtual Private Network (VPN)** – you can access the Global network through the **Sophos VPN for GFS Remote Access**. To establish VPN access, please see detailed instructions in **Appendix C**. Please note, this may be the only way you can access the network in the event of a significant weather disruption. If you have not installed the new Sophos VPN and need assistance, please contact IT Support via email at support@datavox.net or ph. (713) 881-5353. Note, a successful VPN connection automatically provides access to all applications, as if the employee were sitting in his/her office. However, there are many scenarios that could disrupt this connection, e.g., a loss of power to the building or an office PC that was simply turned off.
 - b. **Raymond James Advisor Access** – employees may access RJ's Advisor Access remotely using RJ's proprietary VPN. To establish direct access to RJ's Advisor Access employee must contact Raymond James IT Department directly at ph. (877) 847-5435.
 - c. **Morgan Stanley** (advisory accounts only) – employees may access MS by using the following link: <https://login.morganstanleyclientserv.com/>.

- d. **Pershing** (advisory accounts only) – employees may access Pershing through Netx360 link: <https://www2.netx360.com/portal/login>.
 - e. **Outlook Email** – employees can access Outlook Emails remotely by going to Microsoft Office 365 (link: outlook.office365.com) from any PC, just enter your Global email address and network password to access your Firm.
- 6. Ensure phones are redirected to qualified personnel and auto-attendant is activated.
 - 7. Contact clearing firm and other key service vendors as needed.
 - 8. If necessary, add message to Firm website advising customers on how they may access their funds and securities. The Firm will provide the custodian's contact information in the event clients cannot access their information through the online service.

See also...

APPENDIX A – Emergency Contact List

APPENDIX B – Call Tree

APPENDIX C – Sophos VPN Instructions for GFS Remote Access

APPENDIX D – Key Service Providers

Emergency Contact List

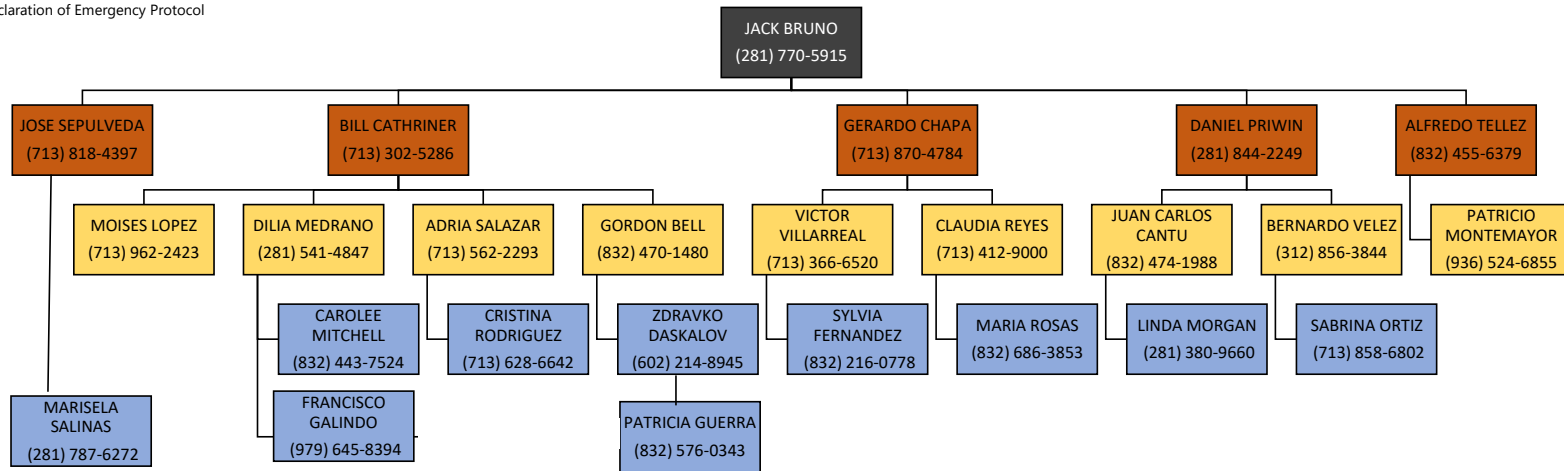
[illegible]

Appendix B - Call Tree

Revised: 09/20/2024

Level One
Level Two
Level Three
Level Four
Level Five

Declaration of Emergency Protocol



APPENDIX C

VPN Connectivity

For employees of Global Financial Services, LLC and GFS Advisors, LLC ("Global")

When connecting remotely, in order to effect continuity of working operations, Global employees utilize secure, VPN connection for remote access to all company networks and applications.

Remote Device Configuration

Global has ensured availability for each Employee, whether or not they use an Apple MAC device or a Windows based personal computer.

- **Windows Users:**
GFS-VPN.pdf
Enrolling your device in DUO.pdf
- **MacBook/MacOS USERS:**
Downloading and Installing Tunnelblick.pdf
Enrolling your device in DUO.pdf

Multifactor Authentication

Additionally, for security purposes Global utilizes Dual Factor Authentication through the DUO Security, Inc. application, which happens to be the same one utilized by FINRA for its Gateway applications.

Installing the Sophos Connect VPN

Open your web browser and go to the link: **https://12.157.21.138:8443**

If you get an error saying “Your connection isn’t private”.

- Click “Advanced” and more information will appear at the bottom.
- Click “Continue to 12.157.21.138 (unsafe)”.



Your connection is not private

Attackers might be trying to steal your information from **75.148.131.125** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

💡 To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Back to safety

This server could not prove that it is **75.148.131.125**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 75.148.131.125 \(unsafe\)](#)



Once on the website, input your user name, password, and the captcha.

- Your Username and password will be the same that you use to log into your computer with.

SOPHOS

Username


Password

CAPTCHA
 

Enter the CAPTCHA code

Login

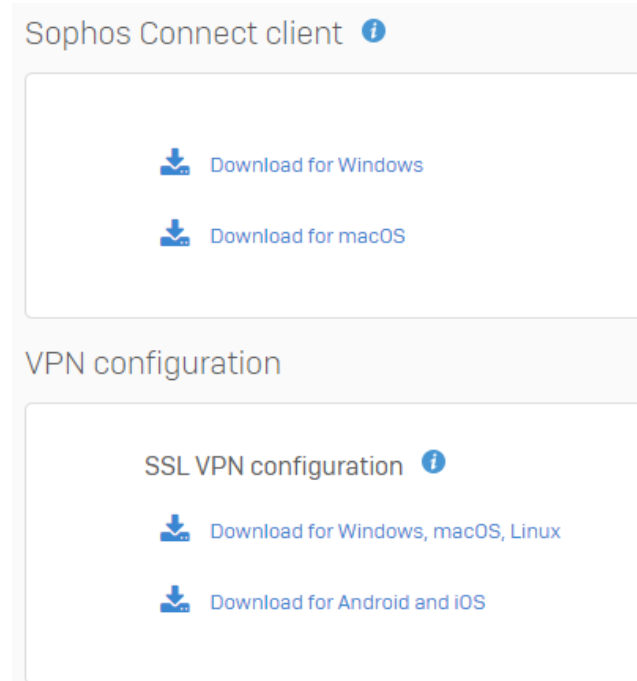
© 2024 Sophos Ltd


User Portal

Installing the Sophos Connect VPN

After you sign in, you will see “Sophos Connect Client” and “VPP configuration”.

- Download and install the Sophos Connect Client.
- Once installed, download the “SSL VPN confirmation”.
- Double click the downloaded SSL configuration file and it will automatically set up your VPN.



Once installed and set up, search for the application “Sophos Connect” and run it.

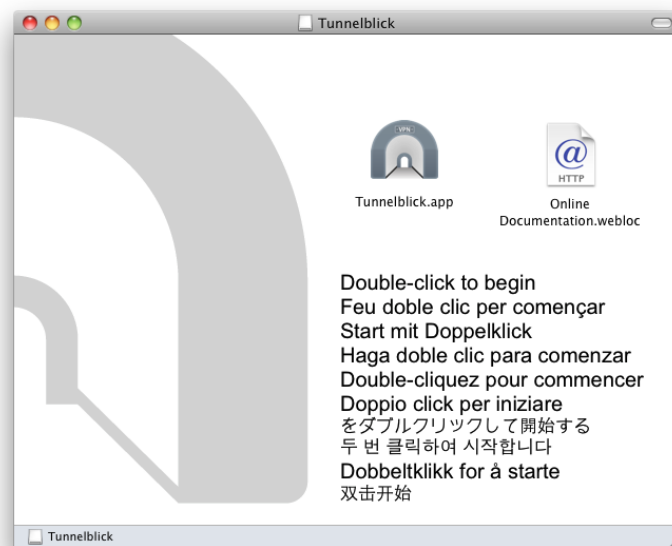
You should now have an IP address 12.157.21.138 and the words “Connect” on the top right.

- Click “Connect” – This should automatically sign you in and connect the VPN.

Once connected, you can go to your shared files like normal.

Downloading and Installing Tunnelblick

1. Follow this link to download the Tunnelblick application (<https://tunnelblick.net/downloads.html>). Depending on your browser and its settings, you may need to double-click the downloaded disk image file to mount the disk image. A window similar to the following will appear:



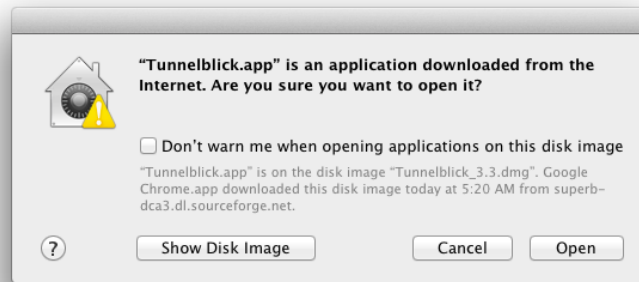
2. To start the installation process, Control-click the Tunnelblick icon and click "Open" and a new window will appear.

If the window is similar to the following:



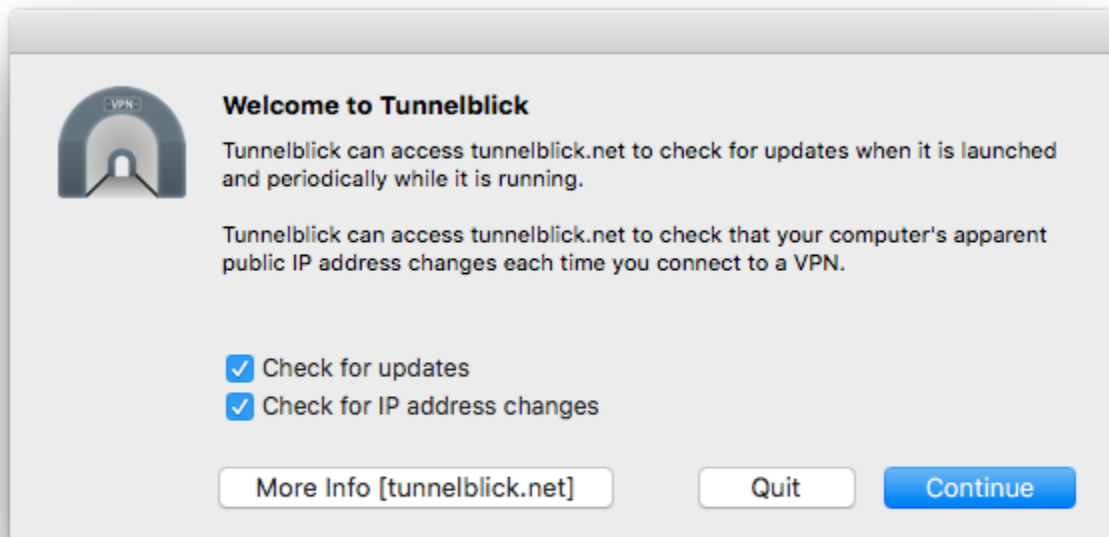
3. then your security settings do not allow you to open files that are not from the Mac App Store by double-clicking. You should click "OK" (the window will disappear), then Control-click the Tunnelblick icon and click "Open" to open the file. A new window will appear.

If the window is similar to the following:



4. then click the "Open" button to continue. The window will disappear and a new window will appear.

A window similar to the following window should now be displayed:



5. Specify whether or not you wish to have Tunnelblick check for updates each time it is launched. When an update is available, you will be given a choice of whether to install the update or not. Tunnelblick checks for updates by making a request to the tunnelblick.net website each time it is launched, and every 24 hours thereafter while it is running. As part of its normal website operation, the website keeps a log which includes information about such requests; see tunnelblick.net Privacy for details.

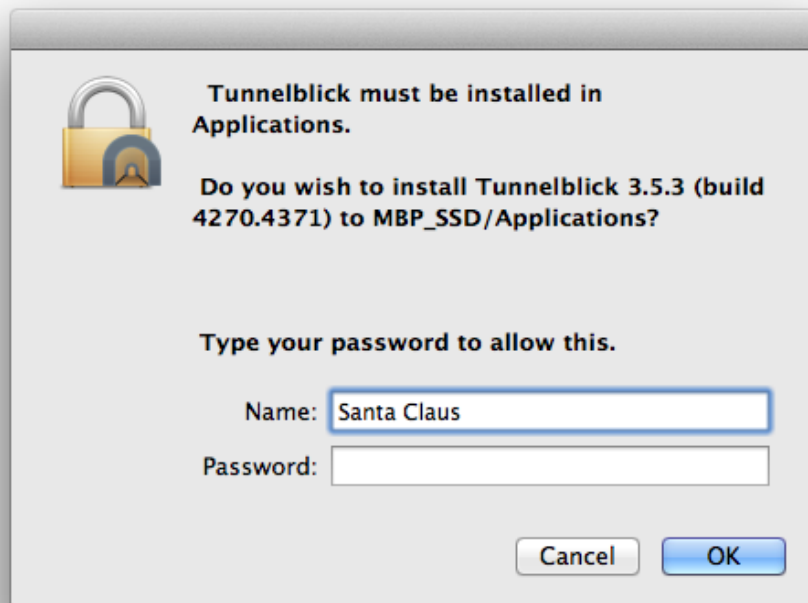
Specify if Tunnelblick should check that your computer's apparent public IP address changes when you connect. This checking may help insure that your configuration is correct, and may help Tunnelblick diagnose DNS problems. Tunnelblick does this checking by making a request to the tunnelblick.net website before each attempt to connect to a VPN and after a successful connection is made. As part of its normal website operation, the website keeps a log which includes information about such requests; see tunnelblick.net Privacy for details.

At any time after installation, you can check for an update by clicking the "Check Now" button on the "Preferences" panel of the "VPN Details" window.

At any time after installation, you can change checking for IP address changes individually for each configuration.

Check or un-check boxes to reflect your initial setup and click "Continue". The window will disappear and a new window will appear.

A window similar to the following window should now be displayed:

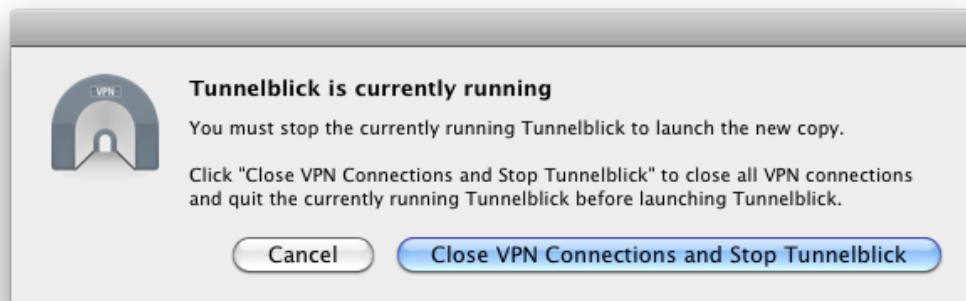


6. If you are reinstalling, upgrading, or downgrading Tunnelblick, the window will show the version number of the current copy and of the new copy. The current copy of Tunnelblick will be put in the Trash before it is replaced.

The name and password of a computer administrator is needed to install Tunnelblick. Tunnelblick's imbedded OpenVPN needs root privileges because it needs to modify network settings by configuring new network devices, changing routes, and adding and removing nameservers. Because we don't want you to enter your administrator account name and password every time you start a VPN connection, Tunnelblick installs a program that allows it to start a VPN connection with super user rights. Tunnelblick uses your administrator account name and password so it can install this program. Tunnelblick also secures itself from being modified.

Click the "OK" button to install Tunnelblick to your hard drive. It should take only a few seconds to install Tunnelblick.

When the installation is complete a new window should appear, similar to the following:



7. When the installation has finished, a notification will be displayed.

When there are no configurations (which is usually the case for a new installation of Tunnelblick), the configuration helper will appear:

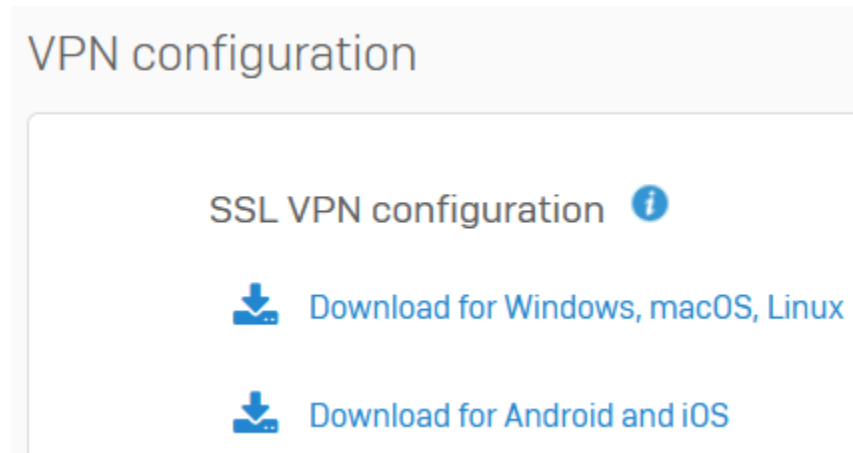


Installing Configurations

Download the Sophos configuration file

1. In the Sophos user portal, under VPN configuration, click Download configuration for macOS.

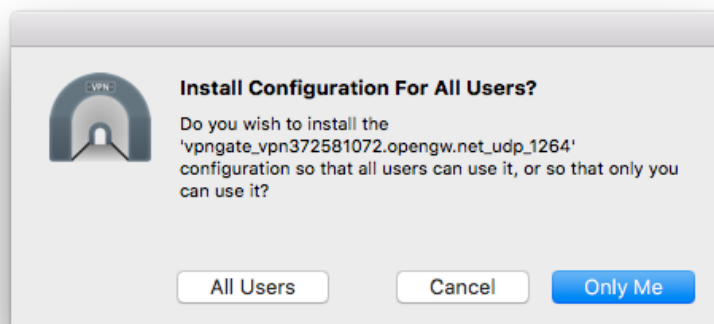
This downloads a .ovpn file.



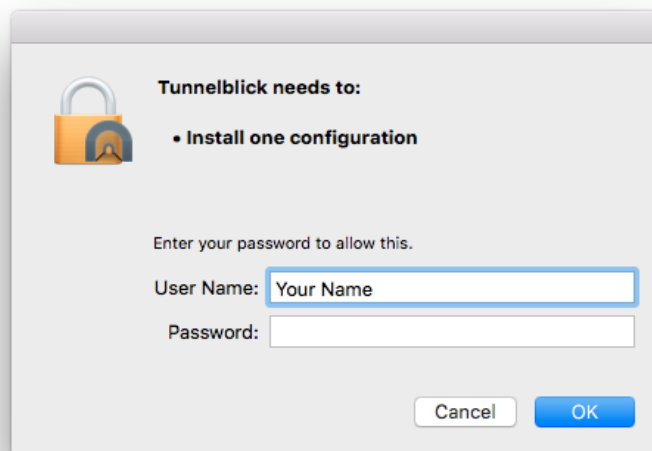
2. Once you have downloaded the configuration, launch Tunnelblick if it is not already running, and then install a configuration by dragging it and dropping it on the Tunnelblick icon in the menu bar.

If you have more than one configuration to install, you may select all of them and then drag-and-drop them on the icon to install them all at once.

A window similar to the following will appear:



3. Click the button for the type of installation you wish, and a window similar to the following will appear:



ENROLLING YOUR DEVICE INTO DUO

- 1. You will receive an email the below email. You will need to download the DUO application from the Apple app store or the Google Play store depending on if you have an iPhone or an Android device.**

This email will help you add your <account-name> account to Duo Mobile on this device:

<555-555-5555>

Just tap this link from <phone-number>, or copy and paste it into Duo Mobile manually:

Dou-activation-link.com

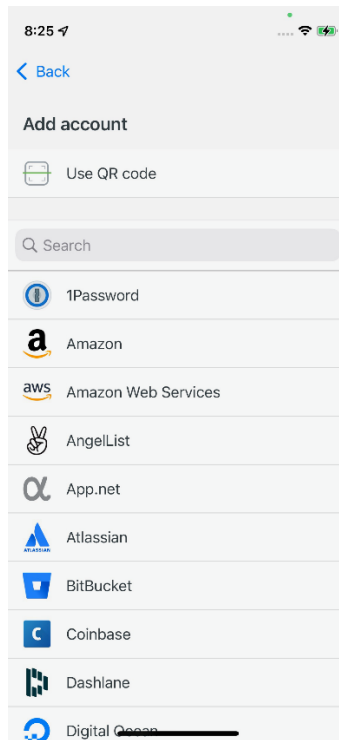


Don't have Duo Mobile yet? Install it first:

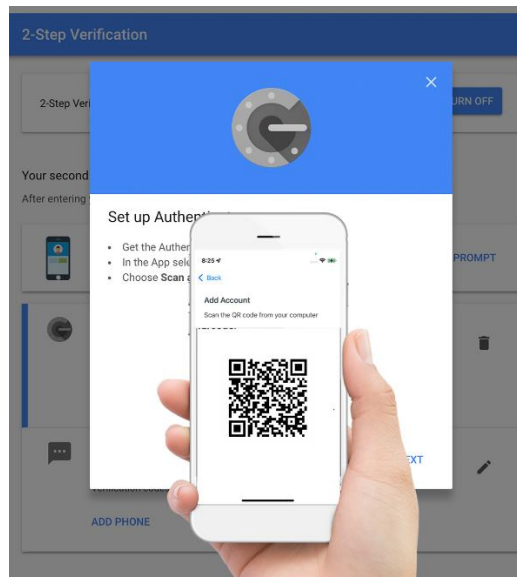
iPhone: <https://itunes.apple.com/us/app/duo-mobile/id422663827>

Android: <https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>

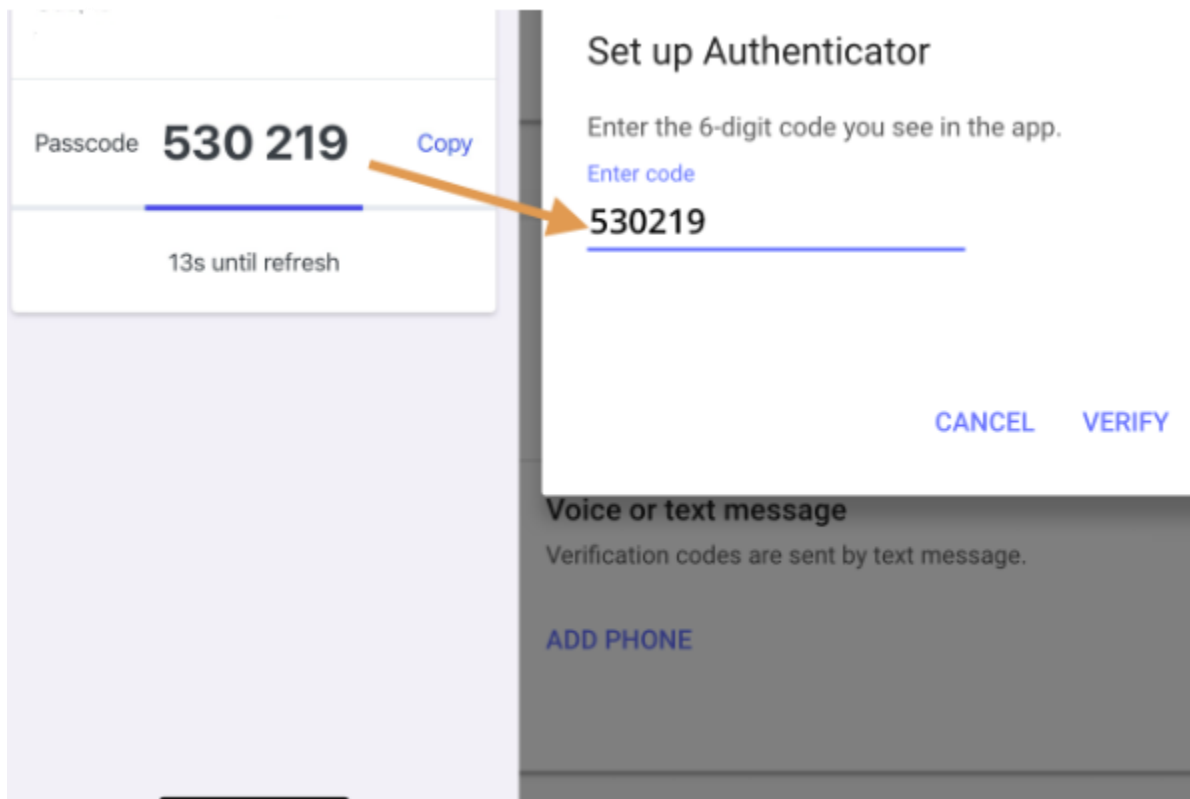
2. After installing the DUO application on you mobile device, select the add new account option, and the select 'Use QR code'



3. Use Duo Mobile to scan the application's QR code shown on your screen.



4. Give the new account a name in Duo Mobile and tap Save to return to the accounts list.
5. Tap the indicator next to the account name in Duo Mobile to generate a passcode which expires in 30 seconds. Type the passcode (without a space) into the application's verification prompt on your computer to verify that the passcode generator is working properly. Then click "Next" or "Finish" or whatever link completes authenticator app registration.



6. After you complete the initial enrollment of your mobile device into DUO, you will be prompted to accept all Microsoft 365 logins through the DUO application in order to log in to your account. (Note: you may need to enable push notification with the DUO app if the login prompt does not appear automatically when you attempt to sign in)

Appendix D - Key Service Providers

No.	Service	Service Provider	Contact	Phone	Website/Add'l Information
1	BCP Recovery Site	Regus Workplace-Dallas, TX	Notice to Invoke	972-776-5355	www.regus.com
2	Building Management / Four Oaks Place	Transwestern	Property Management: Jack Gregoire	713-552-802	jack.gregoire@transwestern.com http://www.fouroaksplace.com/
3	Clearing Firm	Raymond James & Associates, Inc.	Division Manager: Steve Reilly	817-368-9860	steve.reilly@raymondjames.com
4	Clearing Firm	Raymond James & Associates, Inc.	RIA & Custody Services	727-567-3990	ccd-servicerequests@raymondjames.com Business Hours: Mon.thru Fri. 6:30 a.m. to 9:00 p.m. ET; Sat. & Sun. 8:00 a.m. to 8:00 p.m. ET
5	Clearing Firm	Raymond James & Associates, Inc.	IT Support: Technology Service Center	877-847-5435	jorge.perdomo@pershing.com
6	Clearing Firm	Pershing, LLC	Jessica Krajewski	321-249-4538	Cecelia.marshall@pershing.com
7	Clearing / Custody	Pershing, LLC & PAS	Cecilia Marshall	303-486-1206; Cell: 303-929-8733	michelle.ward@morganstanley.com
8	Custody	Morgan Stanley	Michelle Ward	212-315-6338	Victorian@datavox.com
9	Data Back-up and Recovery	Datavox	Victoria Navidad	713-881-7415	support@globalrelay.net
10	E-Mail Archiving	Global Relay	Support Desk	866-484-6630	support@appriver.com
11	E-Mail Encryption	AppRiver	Support Desk	866-223-4645	https://www.att.com/contactus/smb/index/internet.html?tab=2
12	Internet	AT&T	Customer Service	800-221-0000	https://business.comcast.com/help-and-support/contact-us
13	Internet	Xfinity	Customer Service	800-391-3000	support@datavox.net
14	IT Help Desk	Datavox	Customer Service	713-881-5315	Tech Support: Mon. thru Fri. 24-Hrs cashpro.assistant@bankofamerica.com by phone Mon. thru Fri. 7:00 a.m. to 9:00 p.m. ET Ph: 888-589-3473
15	Operating Bank Account	Bank of America CashPro	User Access: Jack Bruno	713-968-0400 Ext. 460, 429, or 436	brady.perniciaro@finra.org
16	Regulator	FINRA - New Orleans Dist. 5 Office	Brady Perniciaro	504-522-6527	dfw@sec.gov
17	Regulator	U.S. Securities and Exchange Commission - Ft. Worth Office	Marshall Gandy - National Director of Examinations	817-978-3821	smiller127@bloomberg.net
18	Trading	Bloomberg	Sam Miller	212-617-8843	etrifton@wpengine.com
19	Website Host	WP Engine	Trafton Esler	877-973-6446	bgureshi@sscinc.com
20	Portfolio Accounting	SS&C Advent	Ben Quireshi	972-896-0314	gianna.lussier@unit21.ai
21	Trans Monitoring	Unit 21	Gianna Lussier		

Appendix D - Key Service Providers

No.	Service	Service Provider	Contact	Phone	Website/Add'l Information
22	Data Storage	Laserfische	Taylor Pope: Books & Records Coordinator - Cities Digital	651.714.2800 ext. 126	Taylor.Pope@citiesdigital.com
23	Software Interface	Sherweb Office 365	Cloud Solutions Team	888-567-6610	cst@sherweb.com
24	Client Vetting	LexisNexus	Khelsia Jones	678-694-2757	khelsia.jones@lexisnexisrisk.com
25	Coms Security	Proofpoint	Cloud Solutions Team	888-567-6610	cst@sherweb.com
26	VPN Services	Sophos Limited	Victoria Navidad	713-881-7415	Victorian@datavox.com
27	Multiple Apps	Bloomberg	John Vazquez	212-617-0409	jvazquez84@bloomberg.net
28	Bond Mkt Trading	MarketAxess	Lauren Solomon	469-753-4828	lsoloman@marketaccess.com
29	Accounting	Financial Operations Principal	Roshni Drepaui	347-635-2555	rdrepaui@dfpartners.com
30	Compliance Consultants	Bates Consulting	Rhonda Davis	281-755-2458	rdavis@batesgroup.com