VIRTUAL PRIVATE NETWORK (VPN) GUIDE

Business Continuity Planning

Version 5

Post Date: 7/21/2020

DEFINITION

Virtual Private Network (VPN) is a technology used to extend a private network (LAUSD Network) across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. **With VPN, you can access District Applications from anywhere, day or night**.

This is a resource that is ideal for those who perform essential business functions to maintain business continuity during a disruption and may require the access to District applications outside of their work location. The **Virtual Private Network (VPN) Guide** details step by step instructions on how to request and access District applications through VPN.

PREREQUISITE

- VPN access is granted for the purpose of business continuity. You must first obtain approval from your Department Director or Designee. Next, generate an ITD service ticket for a **VPN Account** through https://lausd-myit.onbmc.com. Under the justification section, please list the applications(s) or web addresses that you need access to. Next, route the ticket to the ITD Security Team for review and approval.

- Requested users must be listed in the departments' **Business Continuity Plan (BCP), Appendix A – Employee Telephone Lists** and be marked **Y (Yes)** under the column **Provides Essential Function?**

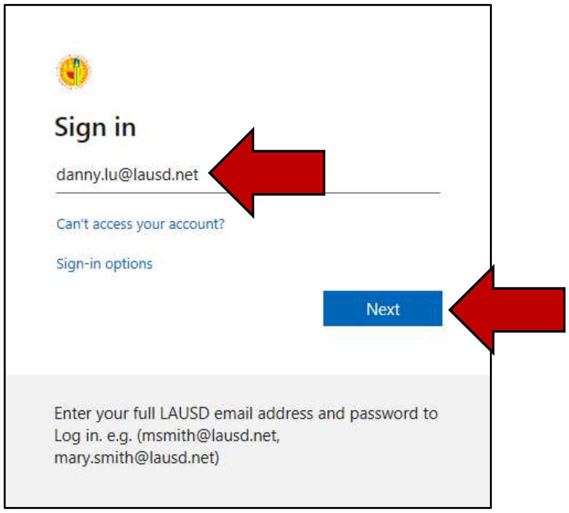
- To protect the district from security breaches such as cyberattacks, access to the VPN requires a Multi-Factor Authentication (MFA). MFA is a secondary method to verify it is really you who are attempting access, in addition to providing your district Single Sign-on username and password. MFA may be accomplished through receiving a call/text or through the Microsoft Authenticator mobile application installed on the users' smart device. **All individuals requesting VPN must have a mobile device and agree to the use of MFA on that device**.

TABLE OF CONTENTS

NOTE: *This guide is designed for Windows and Mac end-user devices. If you have a Chromebook or a Tablet device, please see the* ***VPN Guide for Chromebooks Job Aide****.*

1. REGISTER FOR MULTI-FACTOR AUTHENTICATION (MFA) ACCOUNT (ONE TIME ACTIVITY)

Go to the https://aka.ms/mfasetup. You will then be taken to the Microsoft Online Sign in screen. Enter your full LAUSD **email address** and click **next**.



Sign in

danny.lu@lausd.net

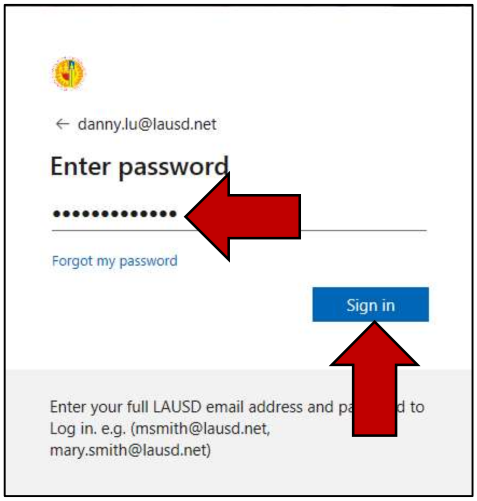
Can't access your account?

Sign-in options

Next

Enter your full LAUSD email address and password to Log in. e.g. (msmith@lausd.net, mary.smith@lausd.net)

Enter your LAUSD email **password** and click **Sign in**. Next, you will receive a new window for **More information required**. Click on **Next**.



← danny.lu@lausd.net

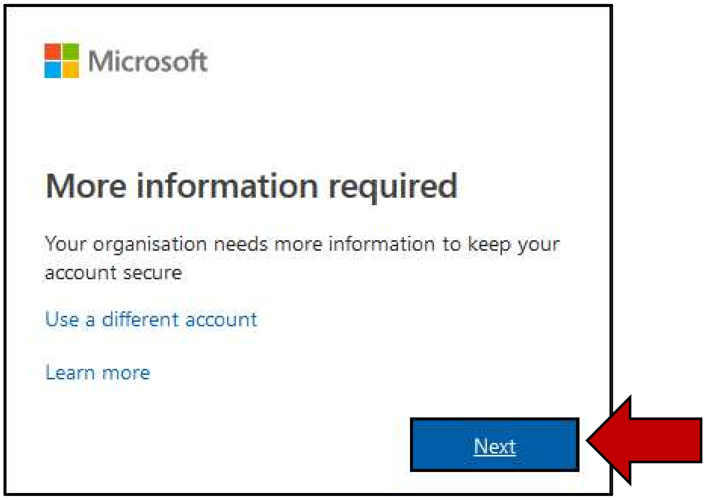
Enter password

•••••••••••••

Forgot my password

Sign in

Enter your full LAUSD email address and pa d to Log in. e.g. (msmith@lausd.net, mary.smith@lausd.net)



Microsoft

More information required

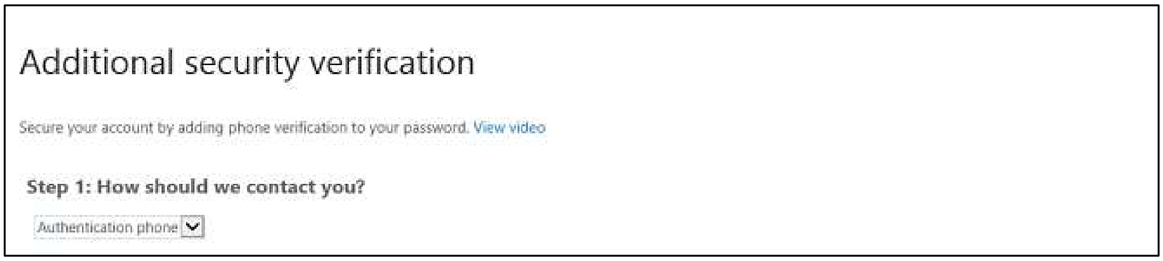
Your organisation needs more information to keep your account secure

Use a different account

Learn more

Next

The **Additional security verification** page will appear.



Additional security verification

Secure your account by adding phone verification to your password. View video

Step 1: How should we contact you?

Authentication phone

In the enrollment process, you will be able to specify your preferred method to verify your identity **(choose only ONE method).** This can be any of the following options listed in the table below.

Method		Description
1	Mobile Phone Call **(Default)**	Places an automated voice call to the authentication phone number. The user answers the call and presses # in the phone keypad to authenticate.
2	Mobile Phone Text Message	Sends a text message containing a verification code to the user. The user is prompted to either reply to the text message with the verification code or to enter the verification code into the sign-in interface.
3	Mobile App	Pushes a notification to the Microsoft Authenticator mobile app on the user's smartphone or tablet. The user taps Verify in the app to authenticate.

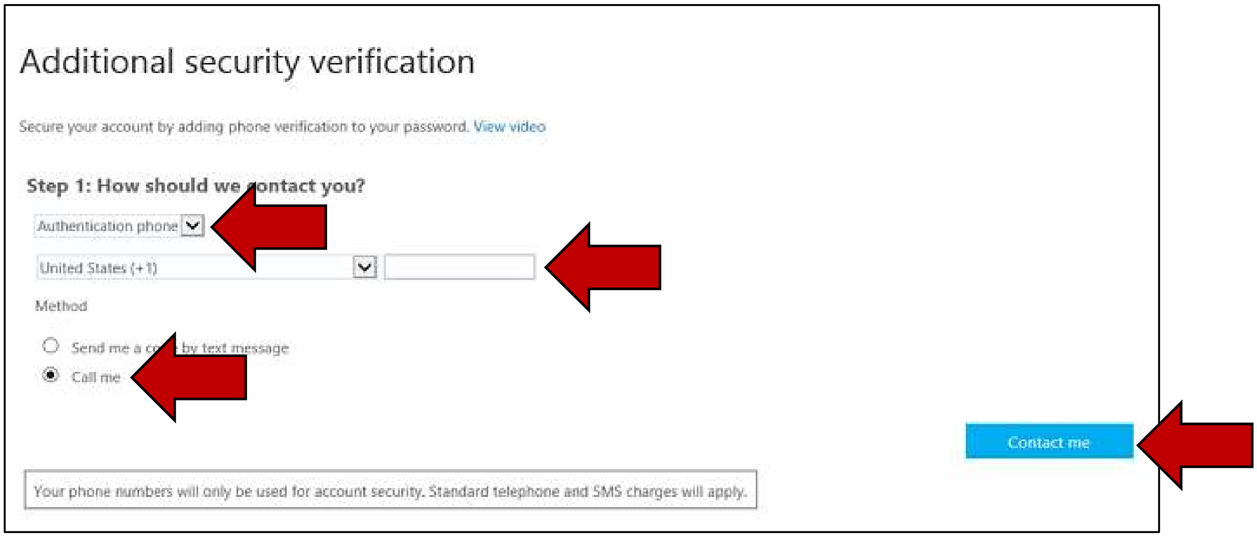
For additional information, you may access the Microsoft page: https://docs.microsoft.com/en-us/enterprise-mobility-security/solutions/fasttrack-how-to-enroll-in-mfa#mobile-phone

Method 1: Mobile Phone Call

In the **Additional security verification** page. Under **Step 1: How should we contact you?** select **Authentication phone**.

In the **country or region** box, select **United States (+1)**. In the box next to the country or region box, type your **10-digit mobile phone number** (include the area code – no dashes).

Select **Call me** as the method and click the **Next** button.



Additional security verification

Secure your account by adding phone verification to your password. View video

Step 1: How should we contact you?

Authentication phone

United States (+1)

Method

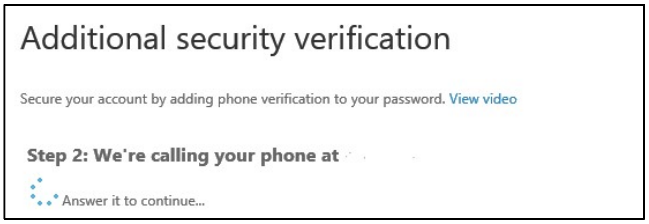
○ Send me a code by text message

● Call me

Contact me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Next, you will receive a phone call from a **1-855-XXX-XXXX** number to confirm the request.



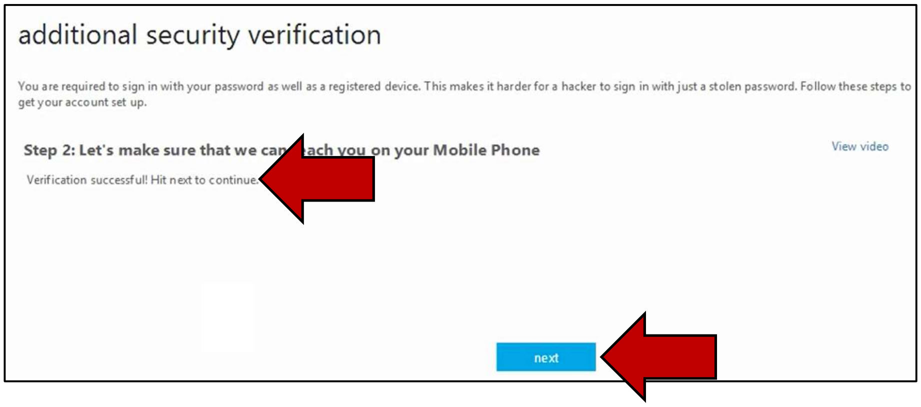
Additional security verification

Secure your account by adding phone verification to your password. View video

Step 2: We're calling your phone at

Answer it to continue...

The automated message will request you to **Press # key** to finish your verification. Once you have verified the request, the browser page will display **Verification successful!** Click the **next** button to complete the setup.



additional security verification

You are required to sign in with your password as well as a registered device. This makes it harder for a hacker to sign in with just a stolen password. Follow these steps to get your account set up.

Step 2: Let's make sure that we can reach you on your Mobile Phone

Verification successful! Hit next to continue.

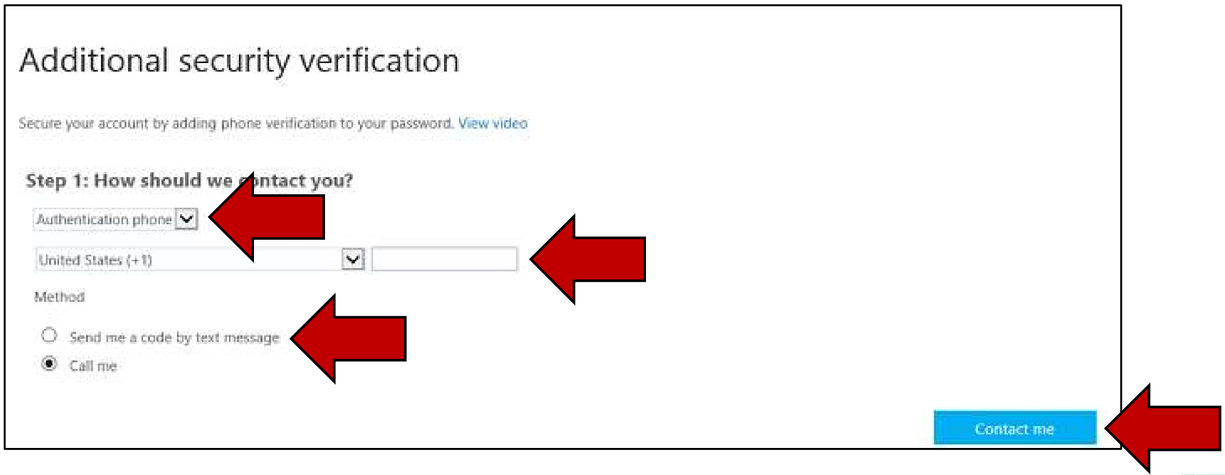
Congratulations! You are now configured to MFA through the mobile phone call method. **If this is the method you selected, you may now go to page 11 to download the AnyConnect Client Software. If you want to change your method, go to page 10.**

Method 2: Mobile Phone Text Message

In the **Additional security verification** page. Under **Step 1: How should we contact you?** select **Authentication phone**.

In the **country or region** box, select **United States (+1)**. In the box next to the country or region box, type your **10-digit mobile phone number** (include the area code – no dashes).

Select **Send me a code by text message** as the method and click the **Next** button.



Additional security verification

Secure your account by adding phone verification to your password. View video

Step 1: How should we contact you?

Authentication phone

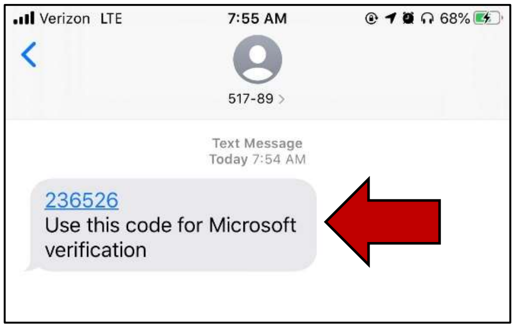
United States (+1)

Method

○ Send me a code by text message

● Call me

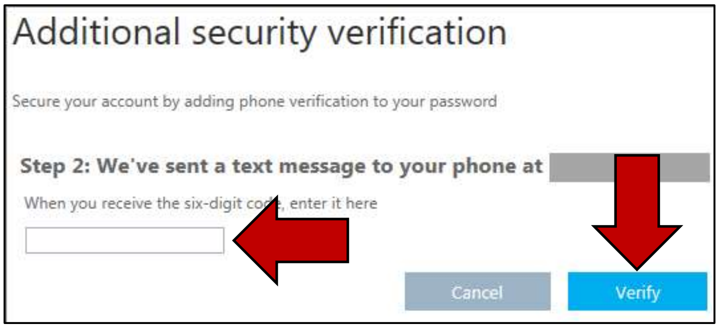
A 6-digit code will be texted to you. Enter this code in the box that is displayed in the browser.


Verizon LTE 7:55 AM 68%

517-89 >

Text Message
Today 7:54 AM

236526
Use this code for Microsoft verification

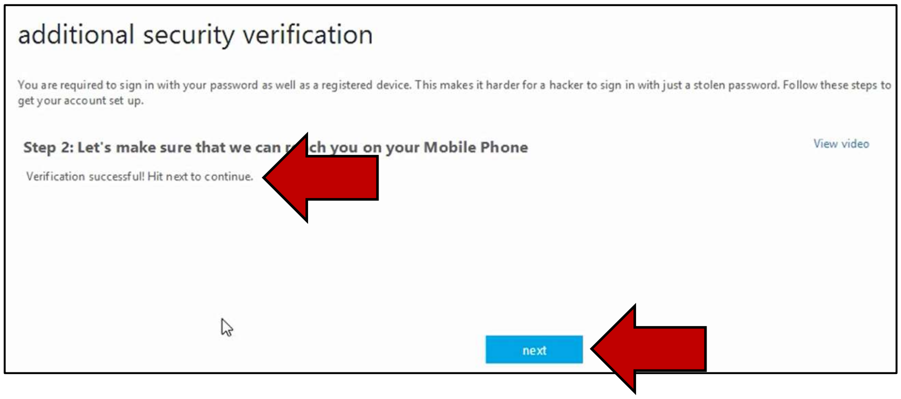

Additional security verification

Secure your account by adding phone verification to your password

Step 2: We've sent a text message to your phone at [redacted]

When you receive the six-digit code, enter it here

Once you have verified the request, the browser will display **Verification successful!** Click the **next** button to complete the setup.


additional security verification

You are required to sign in with your password as well as a registered device. This makes it harder for a hacker to sign in with just a stolen password. Follow these steps to get your account set up.

Step 2: Let's make sure that we can reach you on your Mobile Phone

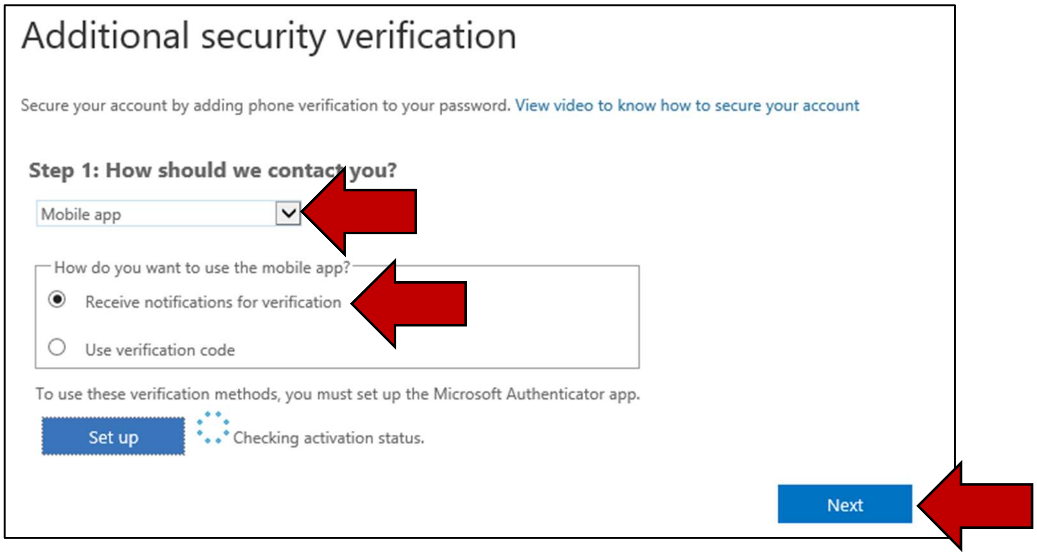
Verification successful! Hit next to continue.

Congratulations! You are now configured to MFA through the mobile phone text message method. **If this is the method you selected, you may now go to page 11 to download the AnyConnect Client Software. If you want to change your method, go to page 10.**

Method 3: Mobile App

In the **Additional security verification** page. Under **Step 1: How should we contact you?** select **Mobile app**.

Check the **Receive notifications for verification** and click **Next**.


Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

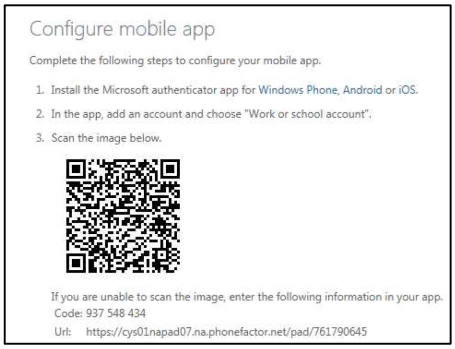
● Receive notifications for verification

○ Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Checking activation status.

This will start the configuration for your account to use the mobile application. You will see a QR code you have to scan with your phone to setup the app.



Configure mobile app

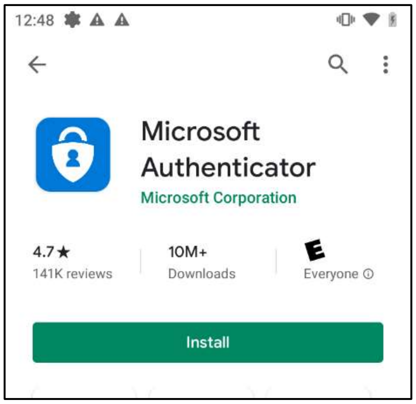
Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

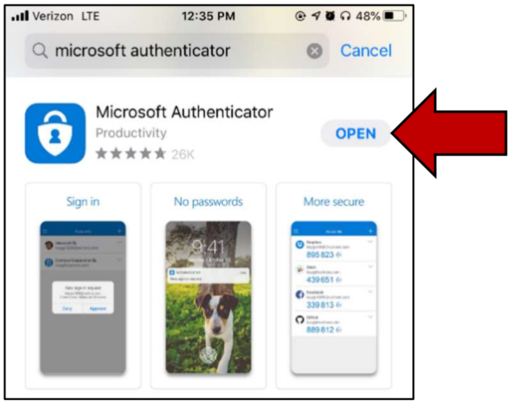
If you are unable to scan the image, enter the following information in your app.
Code: 937 548 434
Url: https://cys01napad07.na.phonefactor.net/pad/761790645

On your mobile device, open the App Store (Apple iOS) or Google Play store (Android) app and search for **Microsoft Authenticator**.

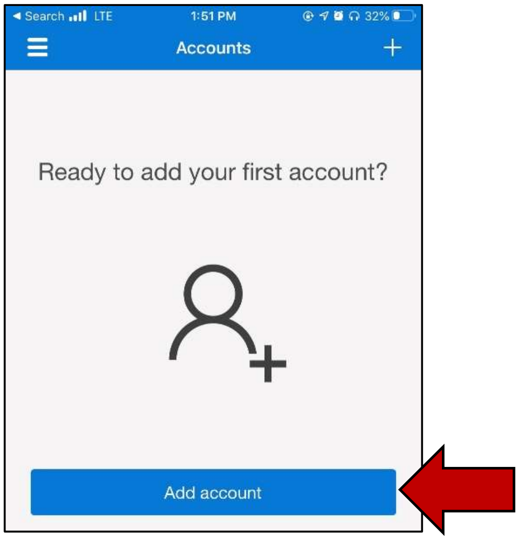
Download the **Microsoft Authenticator** application.



Open the **Microsoft Authenticator** mobile application.



In the **Microsoft Authenticator** mobile application, press **Add account**.

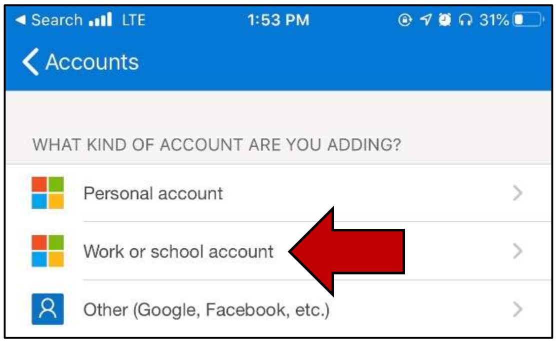


◂ Search LTE 1:51 PM 32%

Accounts

Ready to add your first account?

Next, press **Work or school account**.

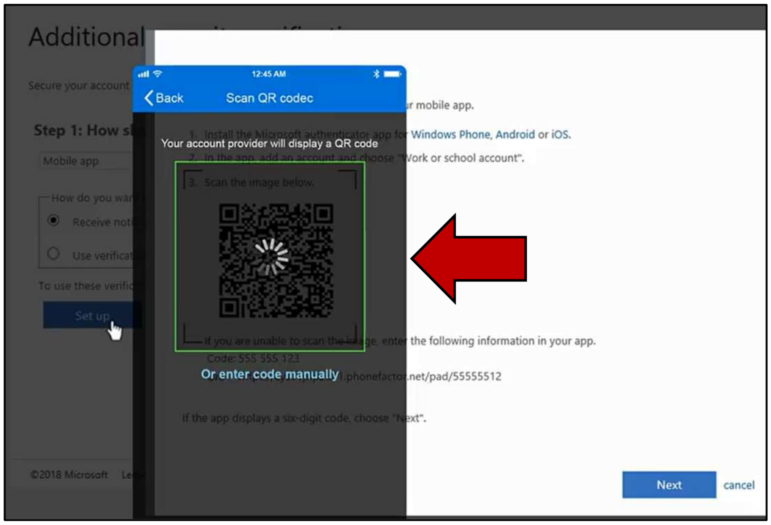


◂ Search LTE 1:53 PM 31%

Accounts

WHAT KIND OF ACCOUNT ARE YOU ADDING?

This will open the camera on your phone to scan the QR code on your computer screen.



Additional

Secure your account

Step 1: How s

Mobile app

How do you wan

● Receive noti

○ Use verificat

To use these verific

Set up

12:45 AM

Back Scan QR codec

Your account provider will display a QR code

r mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.

2. In the app, add an account and choose "Work or school account".

3. Scan the image below.

If you are unable to scan the image, enter the following information in your app.

Code: 555 555 123

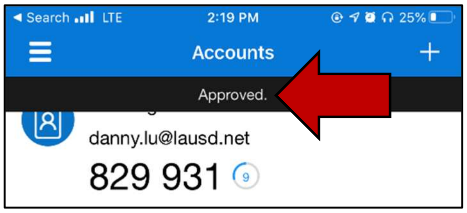
Or enter code manually

.phonefactor.net/pad/55555512

If the app displays a six-digit code, choose "Next".

©2018 Microsoft

When the account has been added, the **Microsoft Authenticator** app will display an **Approved** message.

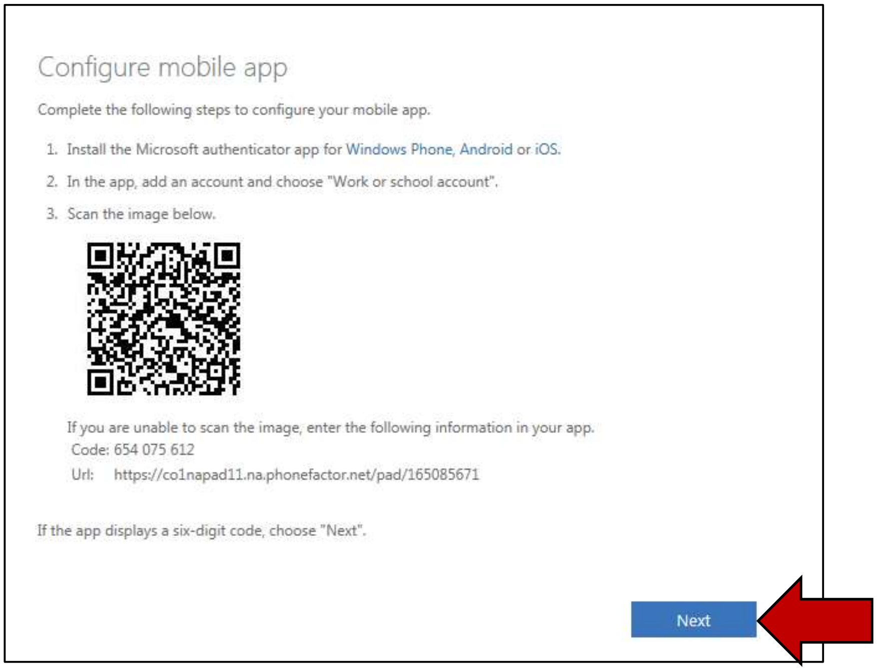


Approved.

danny.lu@lausd.net

829 931

On the browser screen, click **Next**.



Configure mobile app

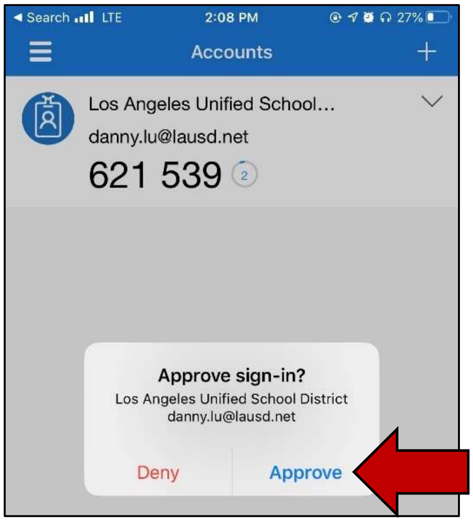
Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.

If you are unable to scan the image, enter the following information in your app.
Code: 654 075 612
Url: https://co1napad11.na.phonefactor.net/pad/165085671

If the app displays a six-digit code, choose "Next".

The system will then send a notification to your phone to approve the sign-in. Press **Approve**.



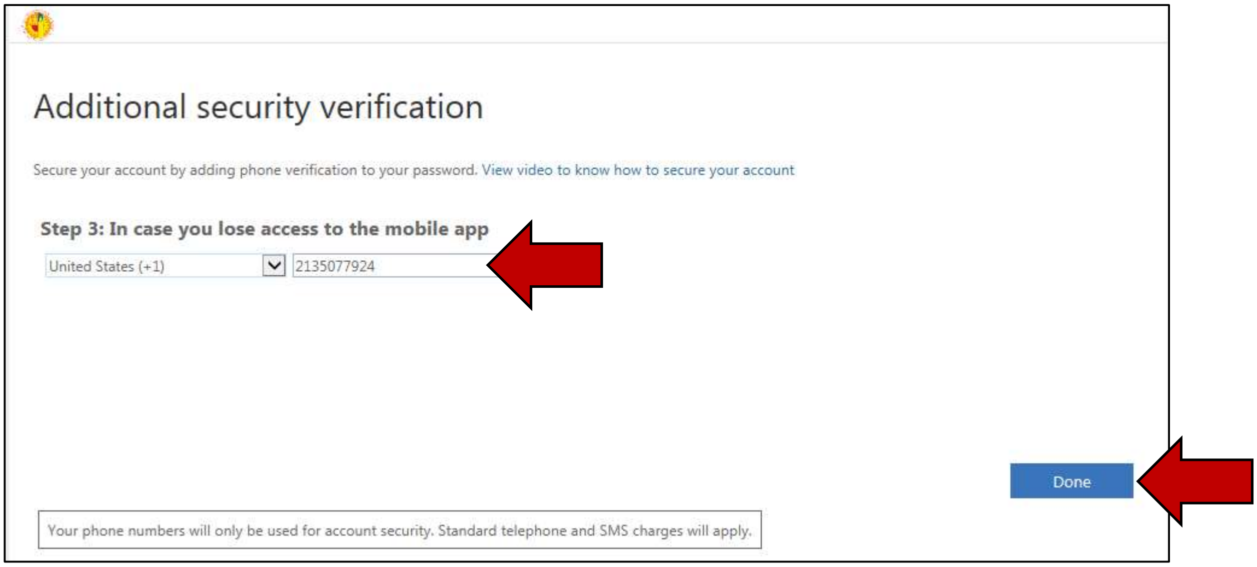
Los Angeles Unified School…

danny.lu@lausd.net

621 539

Approve sign-in?
Los Angeles Unified School District
danny.lu@lausd.net

Last, enter a **phone number** in case you lose your mobile application. Click **Done** when finish.



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 3: In case you lose access to the mobile app

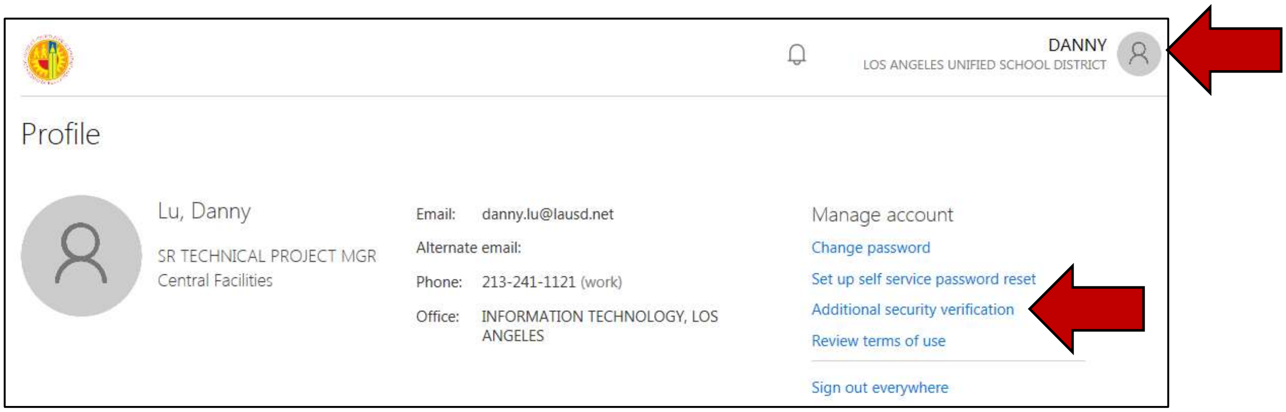
United States (+1) 2135077924

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Congratulations! You are now configured to MFA through the mobile app method.   **If this is the method you selected, you may now go to page 11 to download the AnyConnect Client Software. If you want to change your method, go to page 10.**

OPTIONAL: CHANGE SECURITY VERIFICATION METHOD

If you want to review or make changes to your security verification information, click on **Additional security verification** under the **manage account** profile. If you have already closed your browser, you can access your profile page here: https://account.activedirectory.windowsazure.com/r/#/profile



DANNY
LOS ANGELES UNIFIED SCHOOL DISTRICT

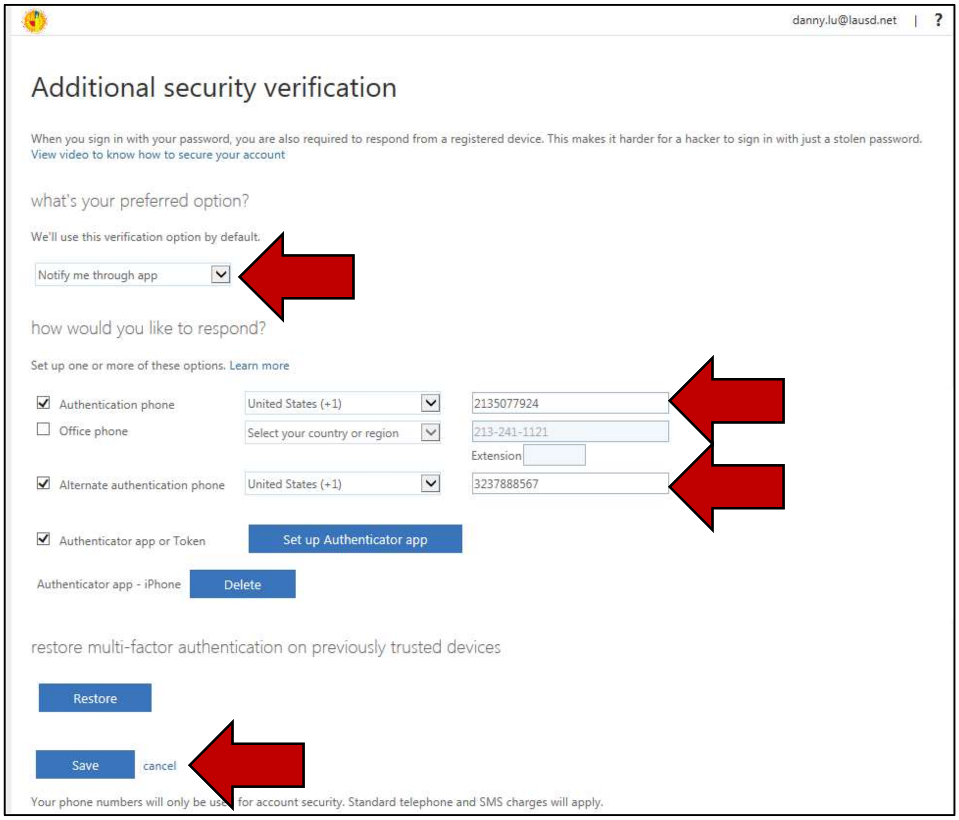
Profile

Lu, Danny
SR TECHNICAL PROJECT MGR
Central Facilities

Email: danny.lu@lausd.net
Alternate email:
Phone: 213-241-1121 (work)
Office: INFORMATION TECHNOLOGY, LOS ANGELES

Manage account
Change password
Set up self service password reset
Additional security verification
Review terms of use
Sign out everywhere

You will be taken to the **Additional security verification** page. In this page, you can update the verification option, authentication phone number or alternate authentication phone number. Press the **Save** button to confirm the request.



danny.lu@lausd.net | ?

Additional security verification

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
View video to know how to secure your account

what's your preferred option?

We'll use this verification option by default.

Notify me through app

how would you like to respond?

Set up one or more of these options. Learn more

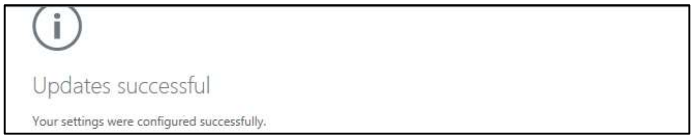
☑ Authentication phone | United States (+1) | 2135077924
☐ Office phone | Select your country or region | 213-241-1121 | Extension
☑ Alternate authentication phone | United States (+1) | 3237888567
☑ Authenticator app or Token | Set up Authenticator app
Authenticator app - iPhone | Delete

restore multi-factor authentication on previously trusted devices

Restore

Save cancel

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.



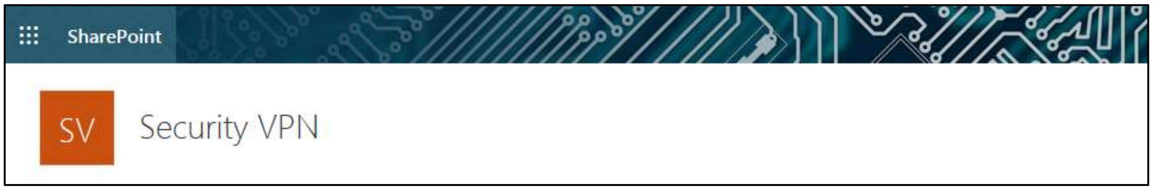
Updates successful

Your settings were configured successfully.

2. DOWNLOAD THE ANYCONNECT CLIENT SOFTWARE ON THE DEVICE YOU WILL BE CONNECTING THROUGH VPN (ONE TIME ACTIVITY PER DEVICE)

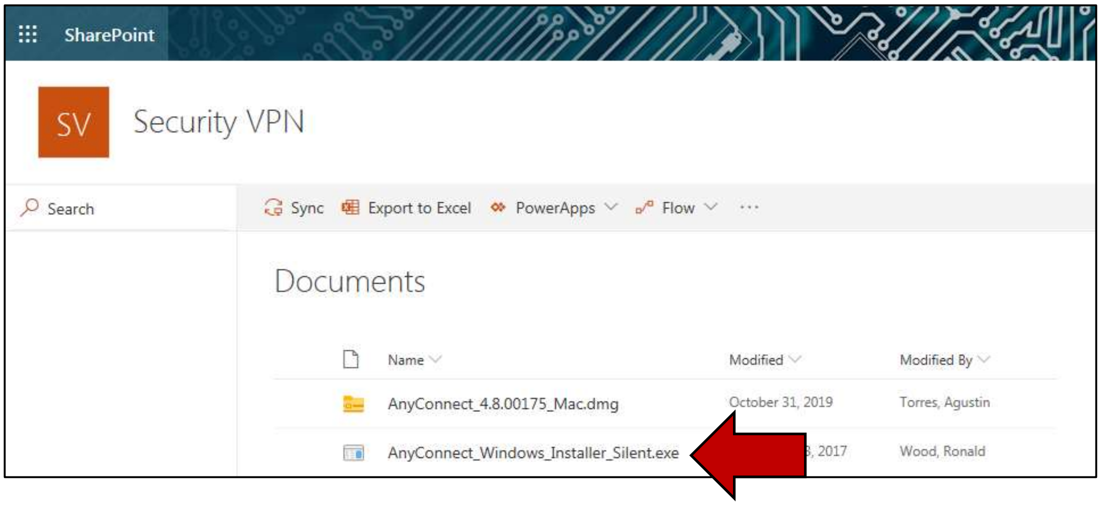
On a web browser (Chrome, Internet Explorer, Edge, Safari), type in or click the following URL to download **AnyConnect** client software:
https://lausd.sharepoint.com/sites/itd_sts/network_security/vpn/Shared%20Documents

The URL will take you to the **Security VPN** SharePoint folder. You may have to login with your District Single Sign-on account.



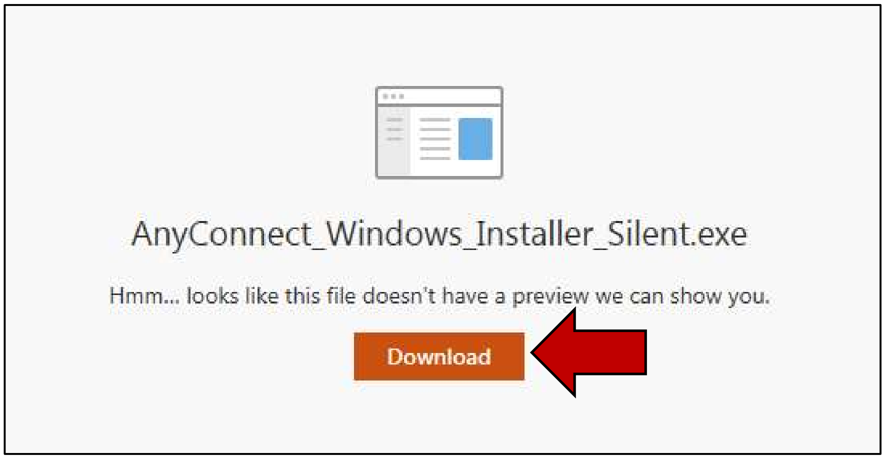
WINDOWS OPERATING SYSTEM USER (If you have a MAC, go to page 13)

Click on the **AnyConnect_Windows_Installer_Silent.exe** file to download the AnyConnect software.



Name	Modified	Modified By
AnyConnect_4.8.00175_Mac.dmg	October 31, 2019	Torres, Agustin
AnyConnect_Windows_Installer_Silent.exe	, 2017	Wood, Ronald

Next, you will be taken to the Download page. Press the **Download** button.

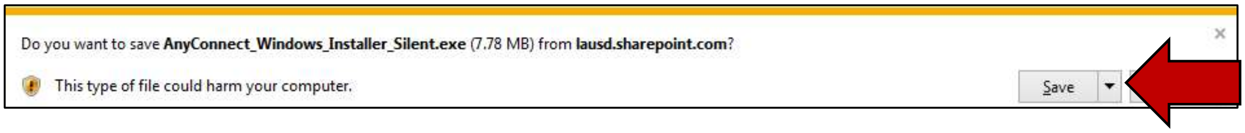


AnyConnect_Windows_Installer_Silent.exe

Hmm... looks like this file doesn't have a preview we can show you.

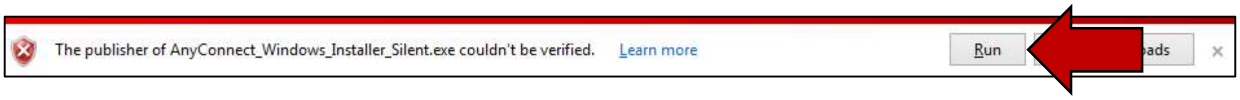
Depending on your browser, a pop up may appear, press the **Run** (Chrome) or **Save** and then **Run** (Internet Explorer).

Internet Explorer/Edge



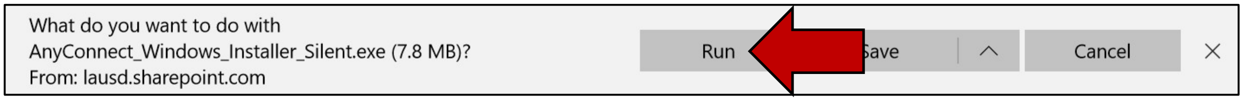
Do you want to save **AnyConnect_Windows_Installer_Silent.exe** (7.78 MB) from **lausd.sharepoint.com**?

This type of file could harm your computer.



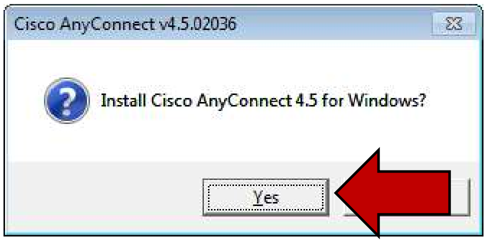
The publisher of AnyConnect_Windows_Installer_Silent.exe couldn't be verified.

Chrome



What do you want to do with AnyConnect_Windows_Installer_Silent.exe (7.8 MB)?
From: lausd.sharepoint.com

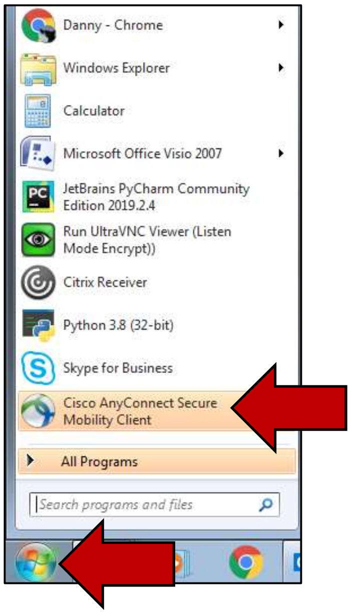
Next, the **Cisco AnyConnect** window will appear. Press the **Yes** button.



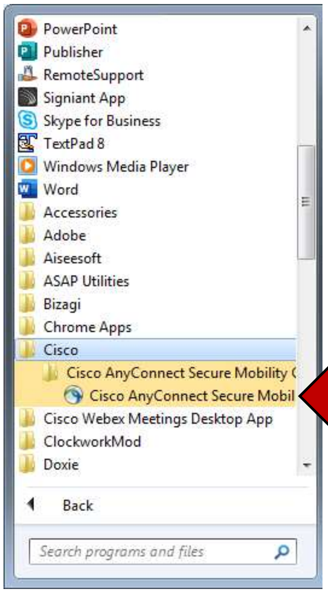
Cisco AnyConnect v4.5.02036

Install Cisco AnyConnect 4.5 for Windows?

The software will install in the background. You can confirm if it was installed if it you press the **windows/start** button and see the **Cisco AnyConnect Secure Mobility Client**. You can also go to **All Programs** and search for the **Cisco** folder.



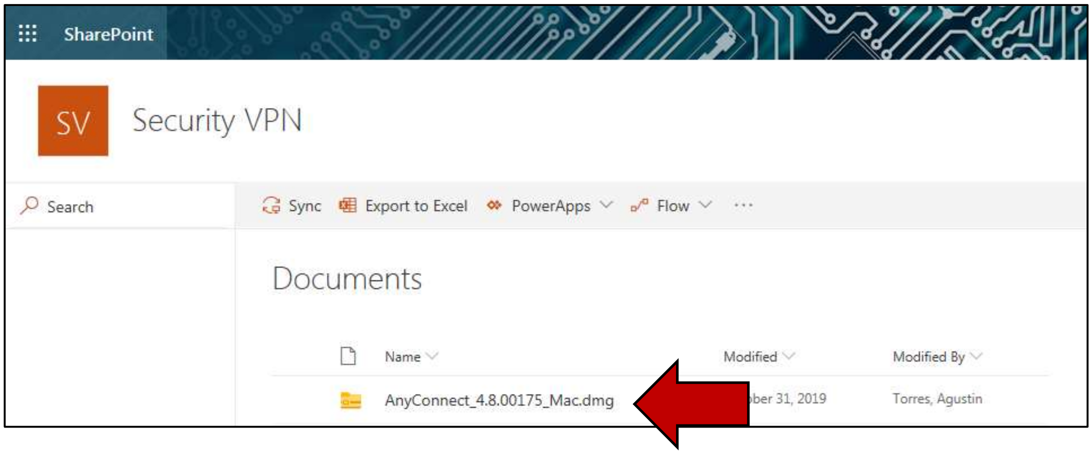
Danny - Chrome
Windows Explorer
Calculator
Microsoft Office Visio 2007
JetBrains PyCharm Community Edition 2019.2.4
Run UltraVNC Viewer (Listen Mode Encrypt))
Citrix Receiver
Python 3.8 (32-bit)
Skype for Business
Cisco AnyConnect Secure Mobility Client
All Programs
Search programs and files



Congratulations! You have just downloaded and installed the Cisco AnyConnect Secure Mobility Client on your Windows machine. **You may now go to page 15 to connect to VPN and access district applications.**

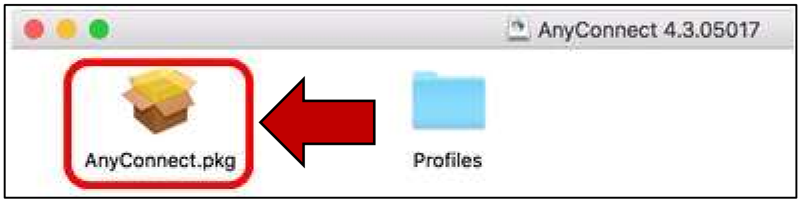
APPLE (MAC) OPERATING SYSTEM USER

Click on the **AnyConnect_4.8.00275_Mac.dmg** file to download the AnyConnect software.

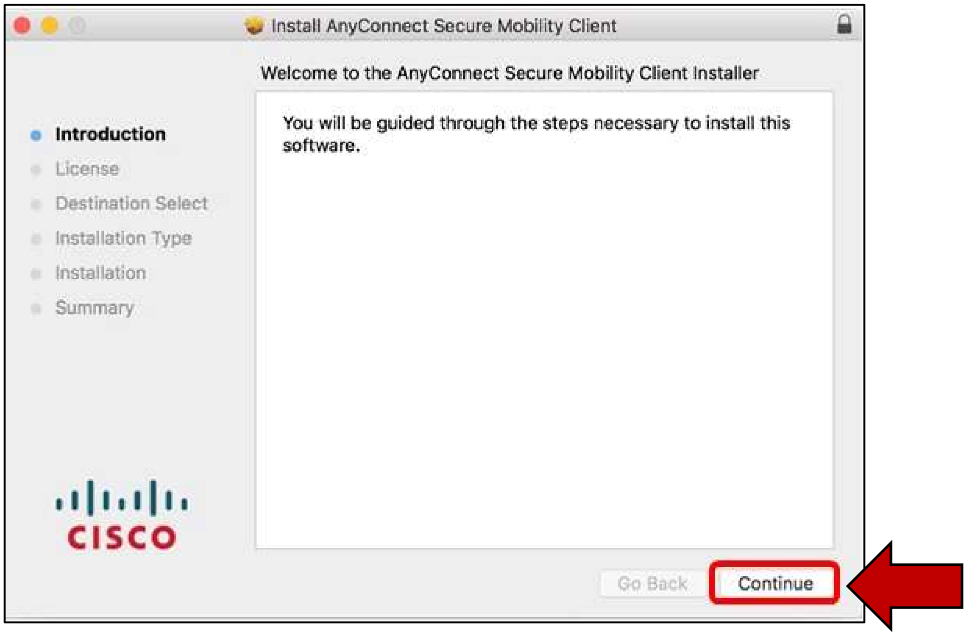


APPLE (MAC) OPERATING SYSTEM USER

You may be taken to a window with two files, **AnyConnect.pkg** and **Profiles**. If this is the case, click on **AnyConnect.pkg**.

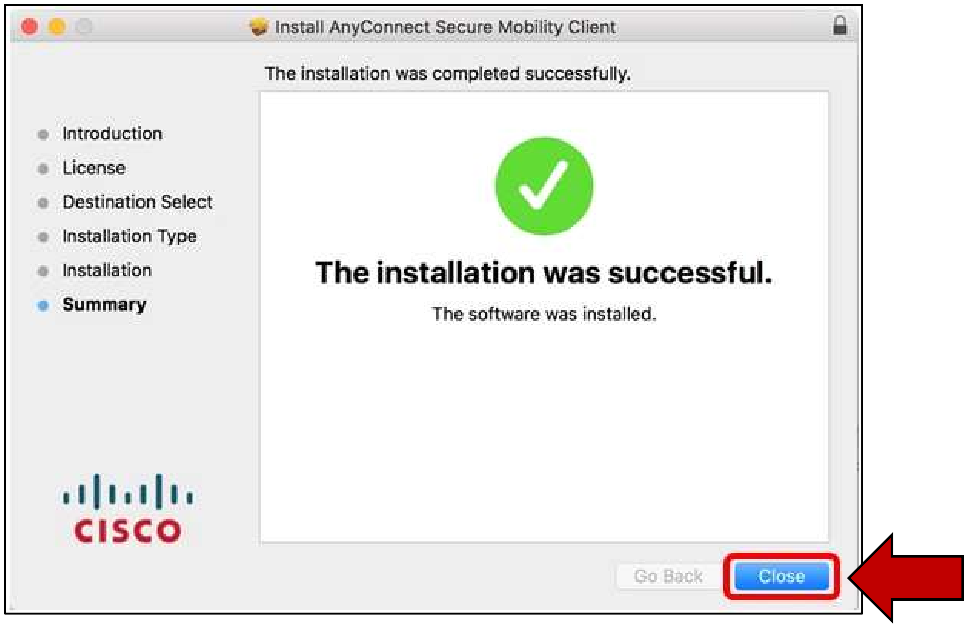


Next, you will be taken to the **Install AnyConnect Secure Mobility Client** window. Click on **Continue** and follow the prompts (**Agree to Terms, Install Software**) until you get to the **Installation was Successful** box and click the **Close** button.



Welcome to the AnyConnect Secure Mobility Client Installer

You will be guided through the steps necessary to install this software.

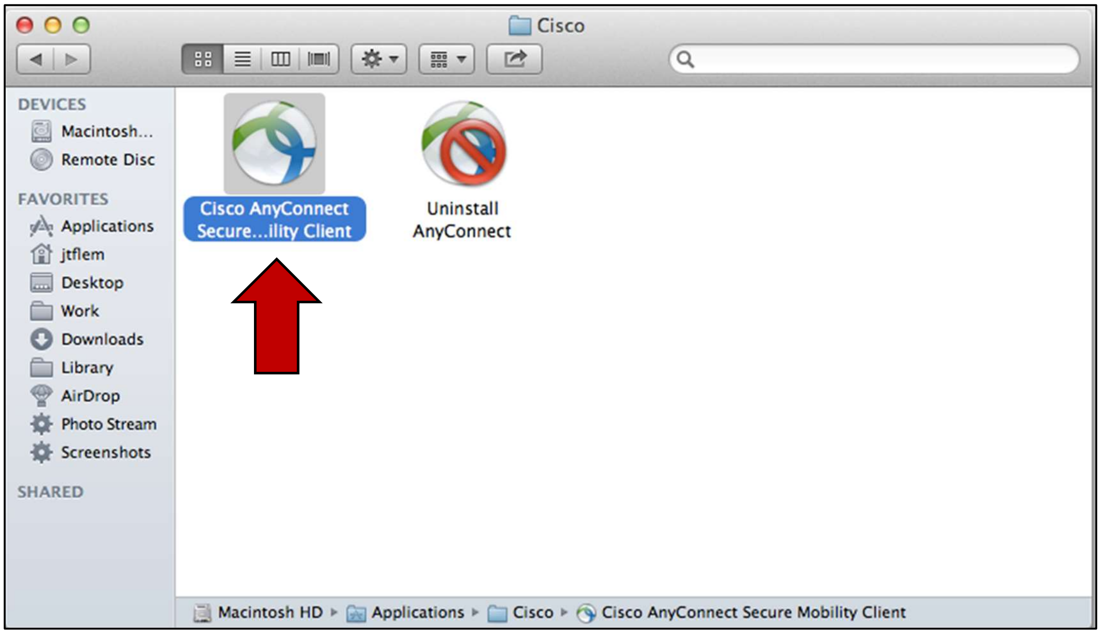


The installation was completed successfully.

The installation was successful.

The software was installed.

If you installed the software successfully, you could verify by going to **Cisco** folder located in the **Applications** folder and you will see the **Cisco AnyConnect Secure Mobility Client** icon.
Finder → Applications → Cisco.



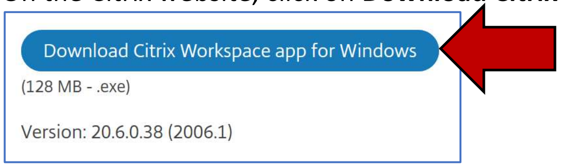
Congratulations! You have just downloaded and installed the Cisco AnyConnect Secure Mobility Client on your Apple (MAC) machine. **You may now go to page 15 to connect to VPN and access district applications.**

3. DOWNLOAD CITRIX WORKSPACE APP (ONE TIME ACTIVITY)

WINDOWS OPERATING SYSTEM USER

On a web browser (Chrome, Edge, Firefox), type in or click the following URL to download and install the **Citrix Workspace App**: https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html

On the Citrix website, click on **Download Citrix Workspace app for Windows**.



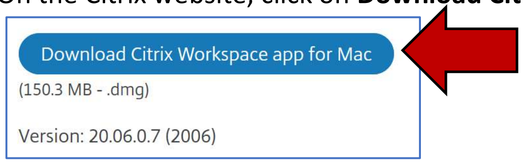
(128 MB - .exe)

Version: 20.6.0.38 (2006.1)

APPLE (MAC) OPERATING SYSTEM USER

On a web browser (Chrome, Firefox, Safari), type in or click the following URL to download and install the **Citrix Workspace App**: https://www.citrix.com/downloads/workspace-app/mac/workspace-app-for-mac-latest.html

On the Citrix website, click on **Download Citrix Workspace App for Mac**.



(150.3 MB - .dmg)

Version: 20.06.0.7 (2006)

Note: If you have an older Apple OS version 10.12 or under, type in or click the following URL to download and install the **Citrix Workspace App**: https://www.citrix.com/downloads/workspace-app/legacy-receiver-for-mac/workspace-app-for-mac-latest.html

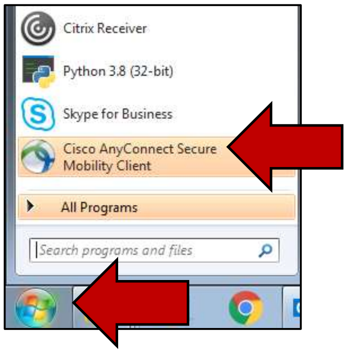
During the Citrix Receiver install process, you may get a window asking for you to **Add Account**, if so, **do not enter your email.** Press the **Close/Finish** button.

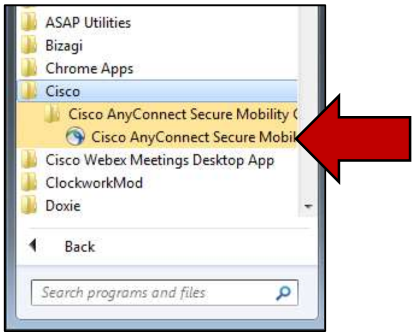
4. CONNECT TO VPN (PERFORM EVERY TIME)

Open the **Cisco AnyConnect Secure Mobility Client** application.

WINDOWS OPERATING SYSTEM USER

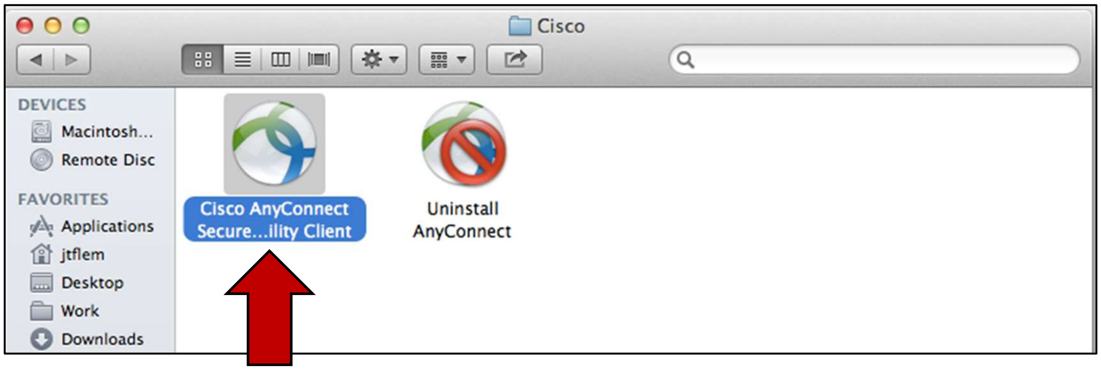
Click on the **Start** button and look for the Cisco folder and click on the **Cisco AnyConnect Secure Mobility Client** application.


Citrix Receiver
Python 3.8 (32-bit)
Skype for Business
Cisco AnyConnect Secure Mobility Client
All Programs
Search programs and files

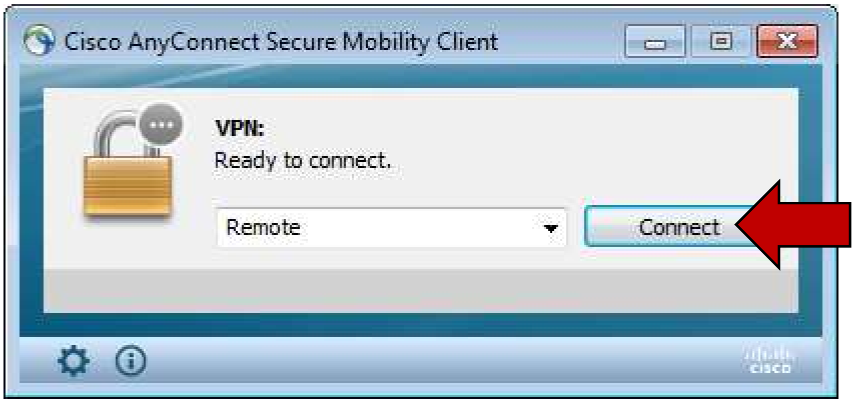

ASAP Utilities
Bizagi
Chrome Apps
Cisco
Cisco AnyConnect Secure Mobility C
Cisco AnyConnect Secure Mobil
Cisco Webex Meetings Desktop App
ClockworkMod
Doxie
Back
Search programs and files

APPLE (MAC) OPERATING SYSTEM USER

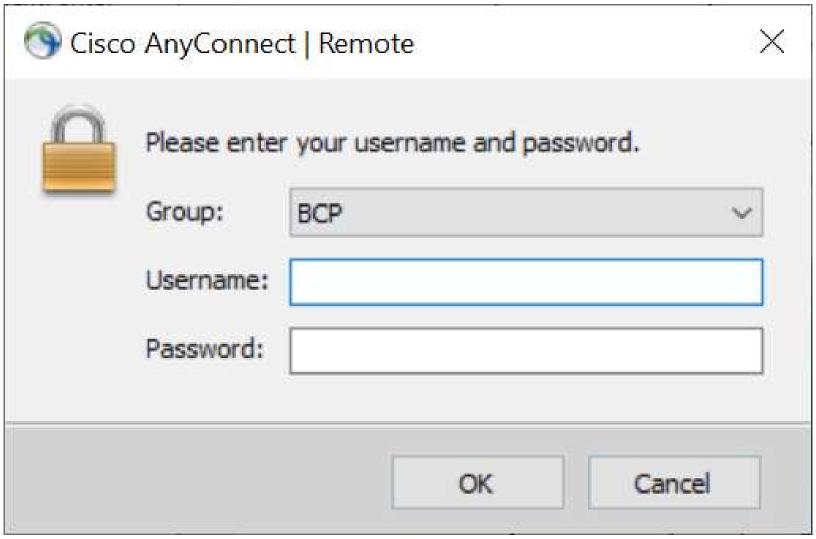
Go to the **Cisco** folder located in the **Applications** folder and click on the **Cisco AnyConnect Secure Mobility Client** icon.



Next, the **Cisco AnyConnect Security Mobility Client** window will appear. Press the **Connect** button.



Next, the **Cisco AnyConnect | Remote** window will appear.



Cisco AnyConnect | Remote

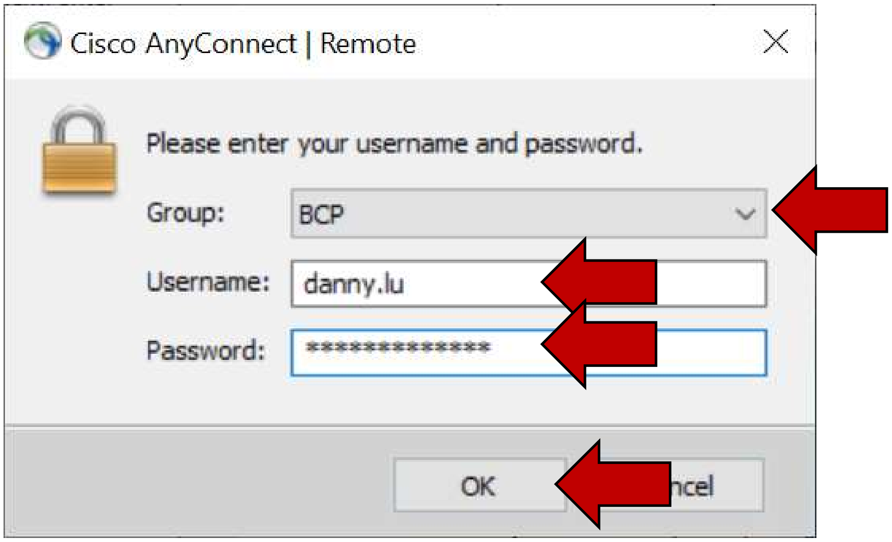
Please enter your username and password.

Group: BCP

Username:

Password:

Please make sure the **Group** name is **BCP**, if not, select **BCP** from the dropdown. Next, enter your Single Sign-On (email) username and password (e.g. danny.lu). Do not add domain name (@lausd.net). Press **OK** when done.



Cisco AnyConnect | Remote

Please enter your username and password.

Group: BCP

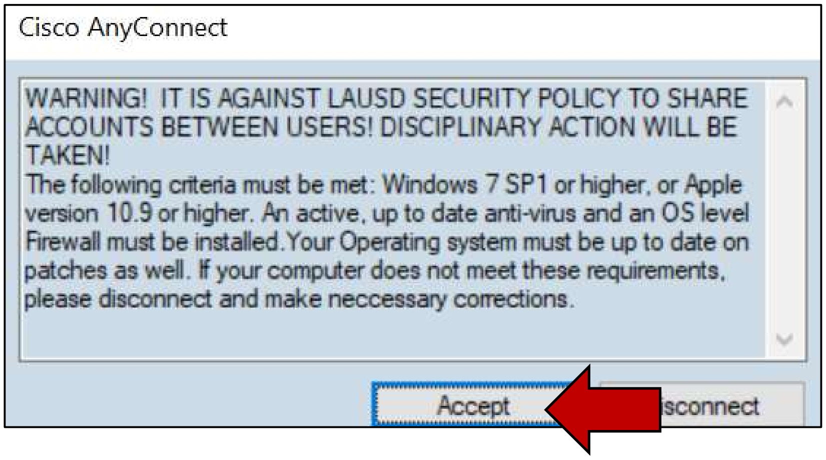
Username: danny.lu

Password: **************

Note: Some user may have a different VPN profile where they are required to select a different Group name (e.g. 2factorMFA/Production). If you were given a different group name, please select that value; if not, please select BCP.

After you press the **OK** button, this will trigger the Multi-Factor Authentication (MFA). **Depending on the MFA method you selected, you will either get a phone call, text or prompt from the mobile application to approve the request.**

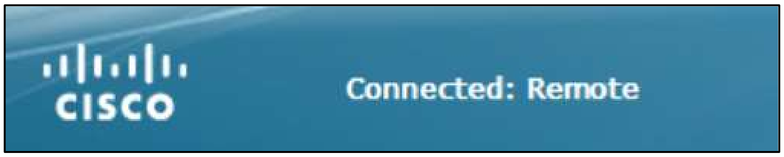
Next, a **Cisco AnyConnect** warning will appear. Press the **Accept** button.



Cisco AnyConnect

WARNING! IT IS AGAINST LAUSD SECURITY POLICY TO SHARE ACCOUNTS BETWEEN USERS! DISCIPLINARY ACTION WILL BE TAKEN!
The following criteria must be met: Windows 7 SP1 or higher, or Apple version 10.9 or higher. An active, up to date anti-virus and an OS level Firewall must be installed.Your Operating system must be up to date on patches as well. If your computer does not meet these requirements, please disconnect and make neccessary corrections.

Next, a **Cisco Connected: Remote** window will appear.

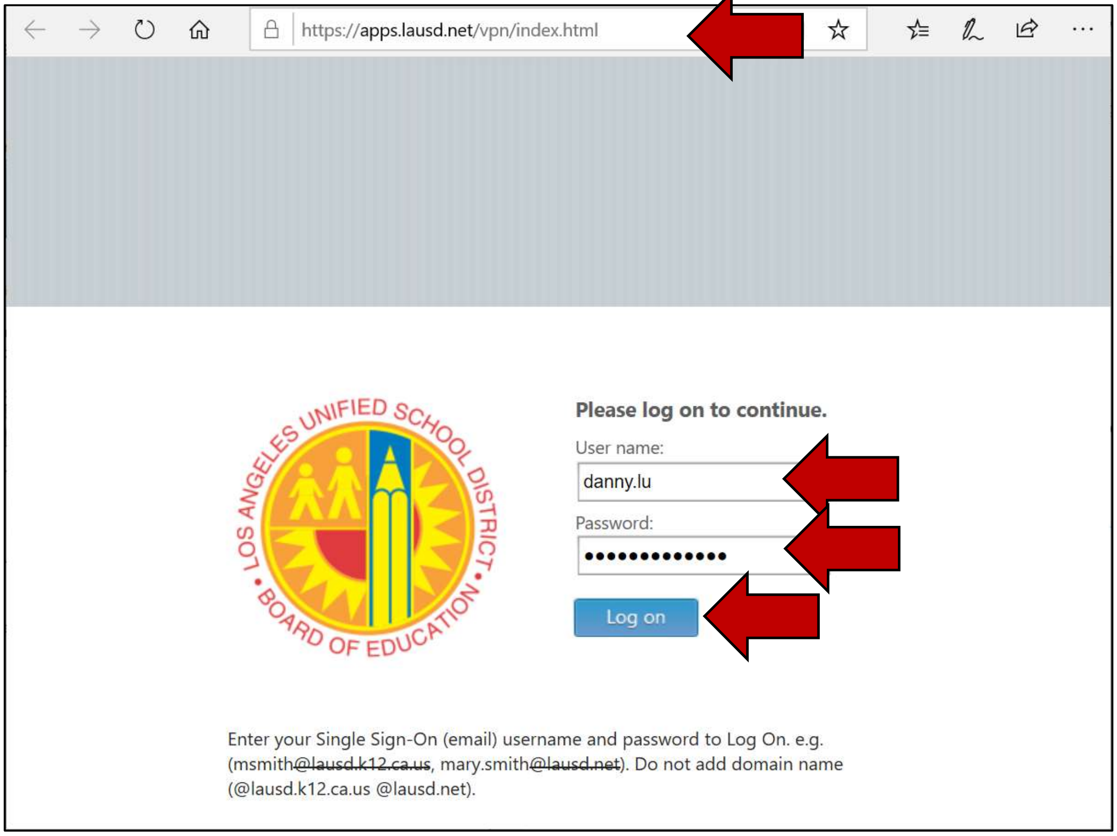


Congratulations, you have just successfully connected to the LAUSD Network through VPN. You may now access District application(s) that are in the district firewall.

5. HOW TO CONNECT TO SAP

To access SAP after you have connected to VPN, open your web browser (e.g. Chrome) and go to https://apps.lausd.net

You will be taken to the login screen where you need to enter your District Single Sign-on **username** and **password** and press the **Log on** button.



https://apps.lausd.net/vpn/index.html
LOS ANGELES UNIFIED SCHOOL DISTRICT • BOARD OF EDUCATION •
Log on

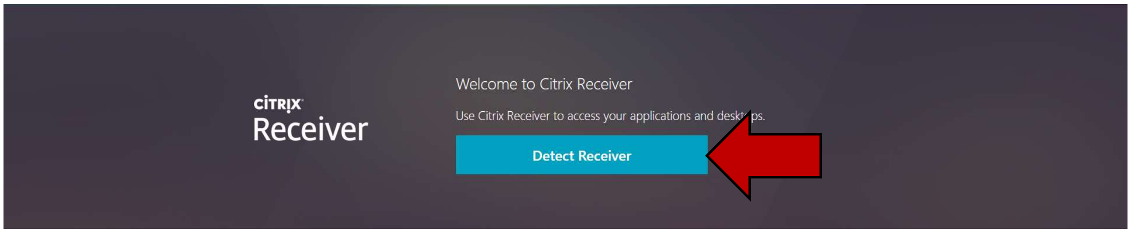
Please log on to continue.

User name: danny.lu

Password: •••••••••••••

Enter your Single Sign-On (email) username and password to Log On. e.g. (msmith~~@lausd.k12.ca.us~~, mary.smith~~@lausd.net~~). Do not add domain name (@lausd.k12.ca.us @lausd.net).

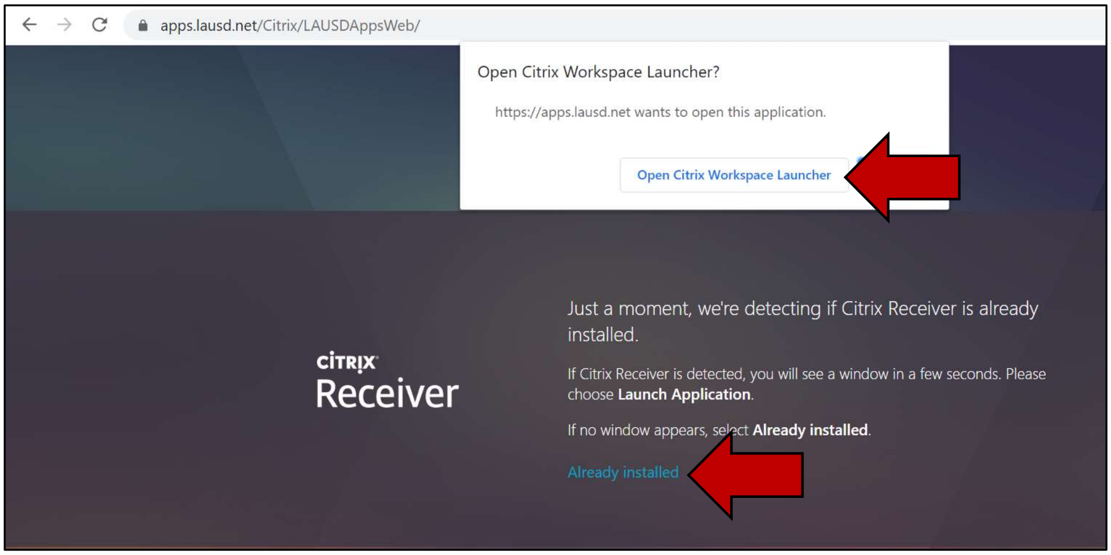
Next, you may be taken to the **Citrix Receiver** page. Click **Detect Receiver**



Welcome to Citrix Receiver

Use Citrix Receiver to access your applications and desktops.

Next, you may get a popup, click the **Open Citrix Workspace Launcher** button, if not, select **Already Installed**.


apps.lausd.net/Citrix/LAUSDAppsWeb/
Open Citrix Workspace Launcher
CITRIX
Receiver
Already installed

Open Citrix Workspace Launcher?

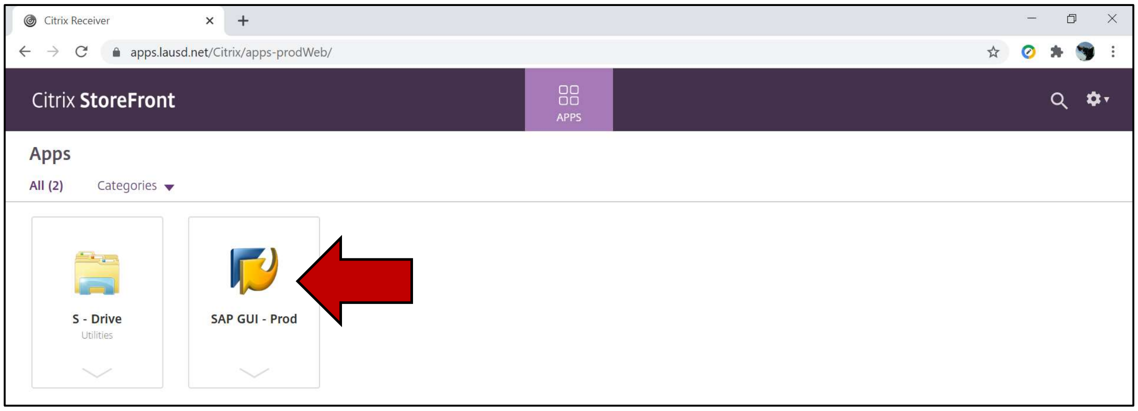
https://apps.lausd.net wants to open this application.

Just a moment, we're detecting if Citrix Receiver is already installed.

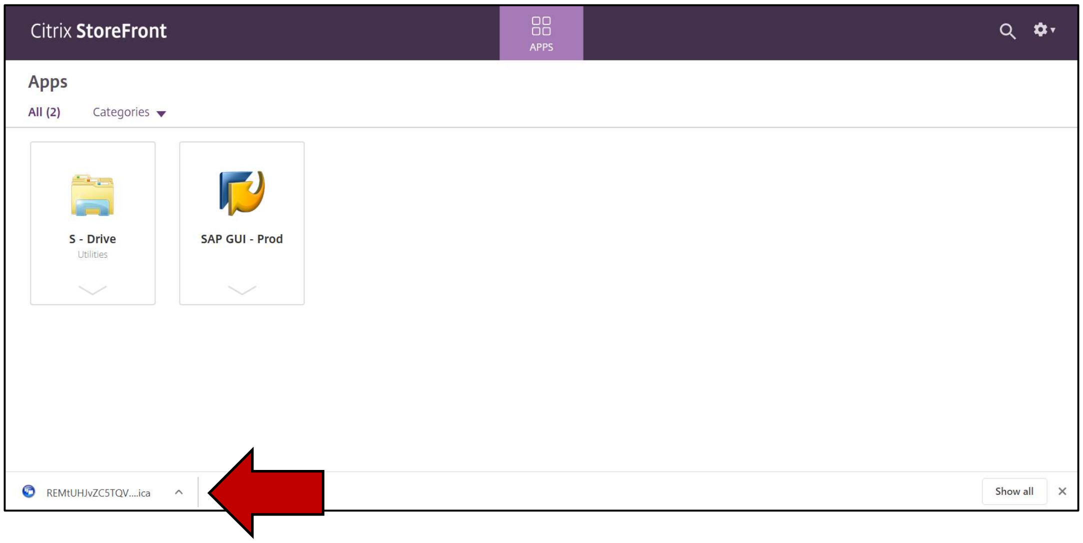
If Citrix Receiver is detected, you will see a window in a few seconds. Please choose **Launch Application**.

If no window appears, select **Already installed**.

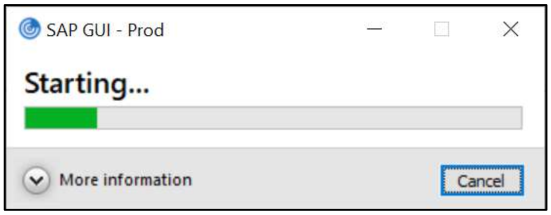
You will then be taken to the **Citrix Storefront** page where you will see the **SAP GUI**. Click on the **SAP GUI** icon.



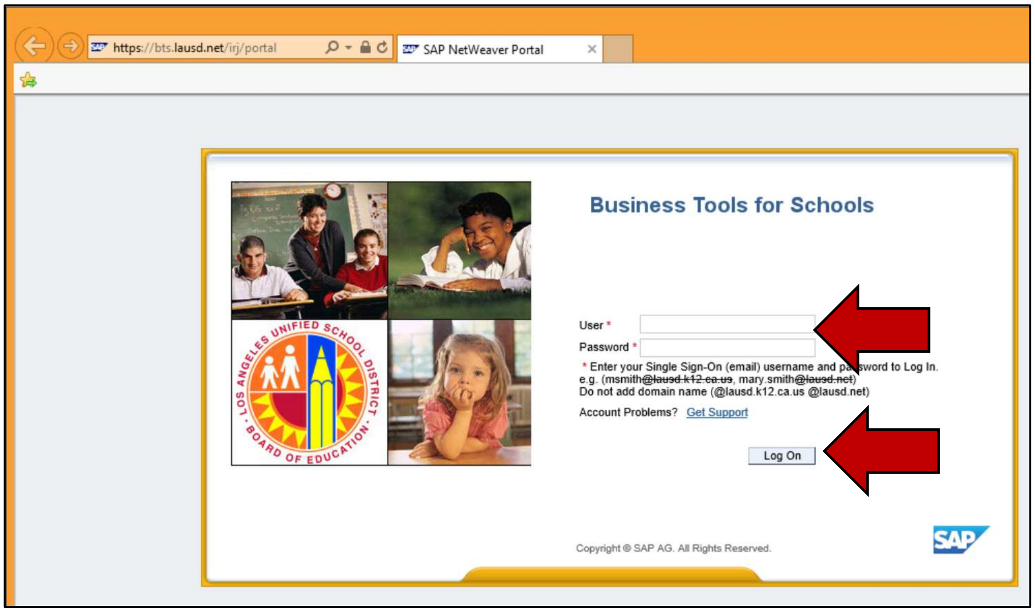
You might get a file download on the bottom, click on the file to open.



The **SAP GUI - Prod** window will appear.



Next, a new window will appear with the **Business Tools for School** login. Enter your **username** and **password** to access SAP.



* Enter your Single Sign-On (email) username and password to Log In.
e.g. (msmith~~@lausd.k12.ca.us~~, mary.smith~~@lausd.net~~)
Do not add domain name (@lausd.k12.ca.us @lausd.net)

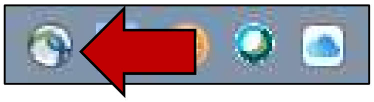
Account Problems? Get Support

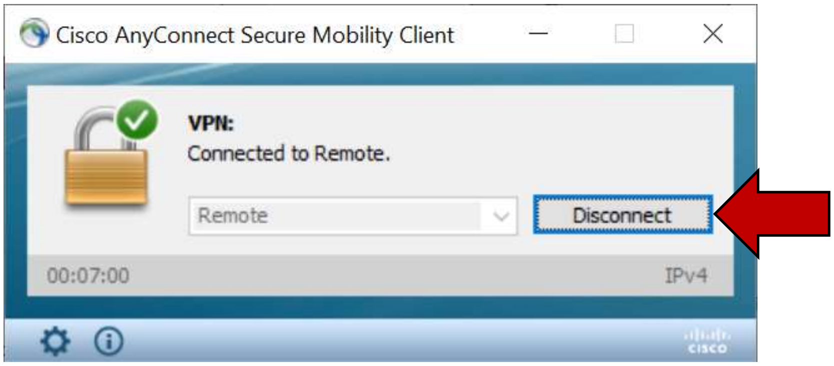
Copyright © SAP AG. All Rights Reserved.

Congratulations! You have just signed into SAP.

6. HOW TO DISCONNECT FROM VPN

To disconnect the VPN and go back to your original network connection, open the **Cisco AnyConnect Secure Mobility Client** icon on your tool bar and select **Disconnect**.





Cisco AnyConnect Secure Mobility Client

VPN:
Connected to Remote.

Remote

Should you have any questions on this guide or have issues connecting to VPN and/or accessing District Applications after connecting, please contact the ITD Helpdesk at 213-241-5200 or the ITD Helpdesk Chat (Monday-Friday, 7:00am-4:00pm) at https://achieve.lausd.net/chat.