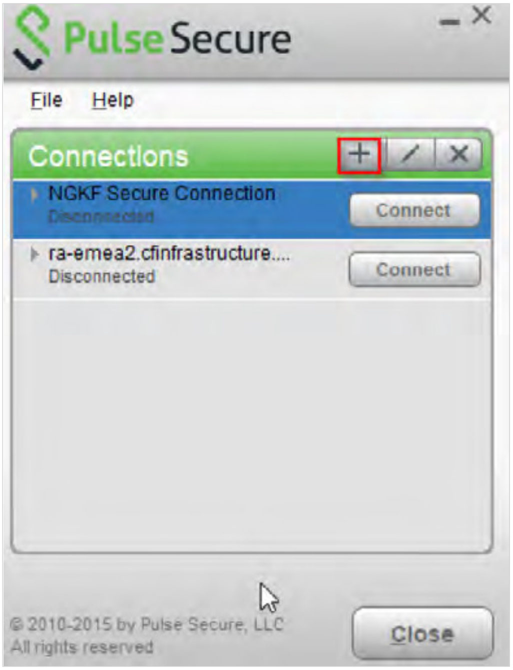
# PULSE
# **SECURE**
## LOG IN

**Pulse Secure Users**
(Corporate Laptop with Pulse Client)

1. You will need to create a new connection in the client. In the Pulse client, click on the **"+" symbol** to create a new connection.

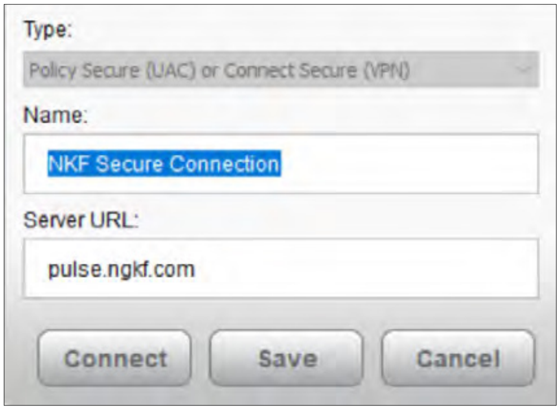


NGKF Secure Connection
Disconnected

ra-emea2.cfinfrastructure....
Disconnected

© 2010-2015 by Pulse Secure, LLC
All rights reserved

2. Set the Connection name to **"NKF Secure Connection,"** and the Server URL to **"pulse.ngkf.com"**



Type:
Policy Secure (UAC) or Connect Secure (VPN)

Name:
NKF Secure Connection

Server URL:
pulse.ngkf.com

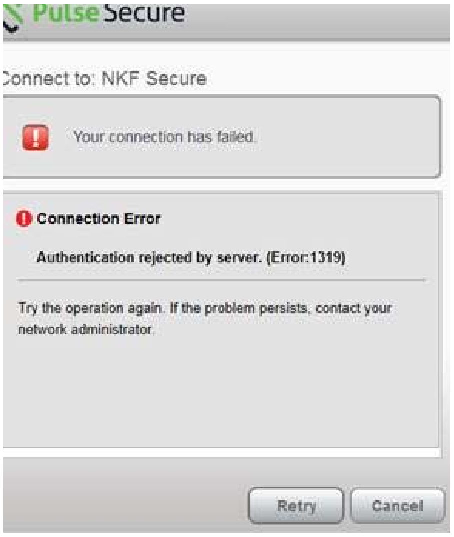
3. **Log in** using the new connection. Once you click **"connect,"** you will be prompted on your mobile phone via SMS, phone call, or mobile app (depending on how you set it up), to **approve the login.** Once approved you will be signed in as normal.

**If your laptop requires a Windows Update or Antivirus Scan, PULSE SECURE will let you know via a pop-up window.*

**TROUBLESHOOTING:**

If you have not signed on to Pulse in a while (Multifactor Authentication may have “forgotten” you) or have not enabled the Multifactor Authentication, please see the below instructions and attempt prior to contacting the Help Desk.

This is the error you will receive is below:



Connect to: NKF Secure

Your connection has failed.

Connection Error

Authentication rejected by server. (Error:1319)

Try the operation again. If the problem persists, contact your network administrator.

**Take these steps to attempt to fix the issue:**

1. login to our authenticator through their online portal at the following link: https://mfa.ngkf.com/multifactorauth/ - Your username will be your email address and password is your regular computer login.
2. The portal will send you an authentication code by whatever means you have set up (I personally get a text message), simply enter the code into the web browser and the authenticator “remembers” your credentials.

# Using Connect.NGKF.com

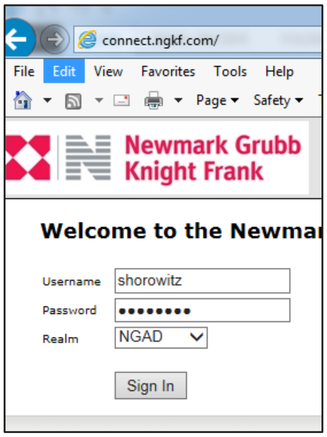
## *Accessing your Windows PC Remotely*

***(MAC Users Needing to Remote to their Windows PC Directions are at the end)***

1. Open up Internet Explorer (if you are using windows 10, Microsoft Edge will not work) and go to Connect.ngfk.com.

2. **YOU MUST** have Microsoft Authenticator set up on your phone and your MFA for Pulse/Connect.NGKF.com prior to connecting. (Please see separate documention for those instructions. File is named ***"mfa-setup-guide.pdf")***

3. Sign in and select your "Realm" or Domain. (MOST WILL BE ON NGAD)



**Welcome to the Newmar**

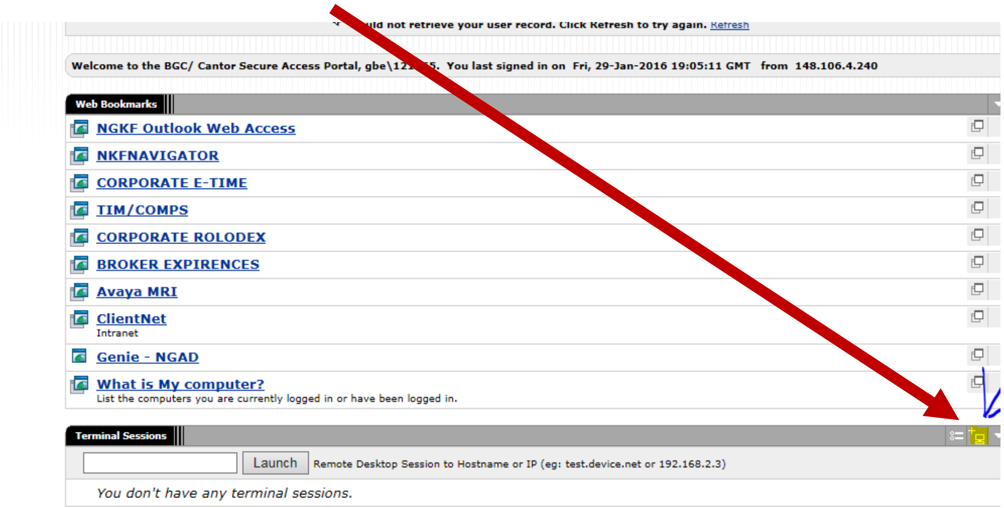
Username: shorowitz

Password: ••••••••

Realm: NGAD

Sign In

4. Select the **add Terminal Services** icon

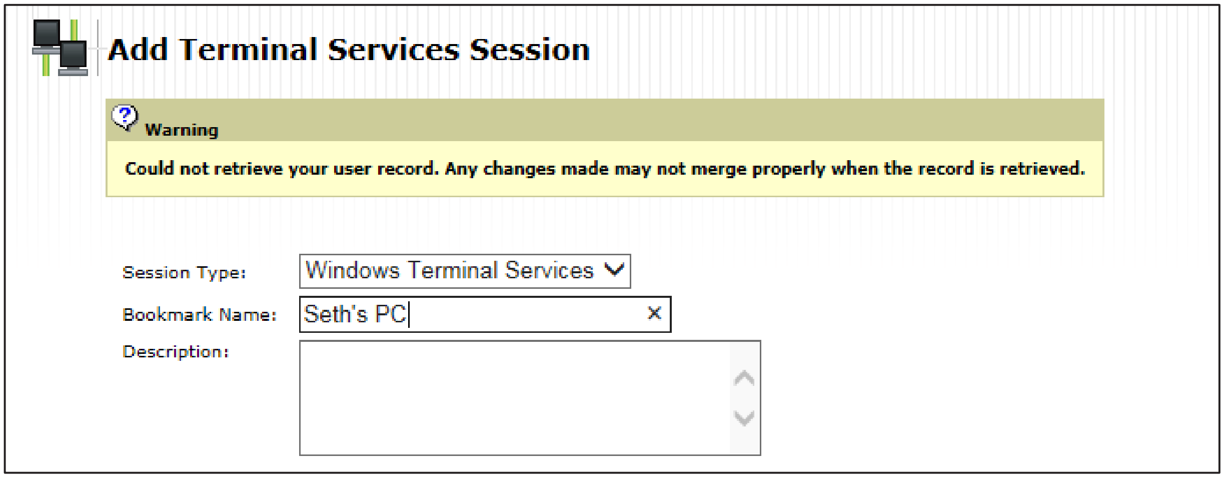


uld not retrieve your user record. Click Refresh to try again. Refresh

Welcome to the BGC/ Cantor Secure Access Portal, gbe\12 5. You last signed in on Fri, 29-Jan-2016 19:05:11 GMT from 148.106.4.240

*You don't have any terminal sessions.*

4. Select your session type as Windows Terminal Services as well as type a Bookmark Name to use as a shortcut.



### Add Terminal Services Session

Warning

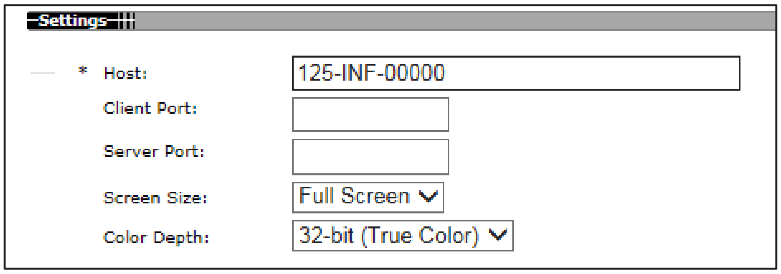
Could not retrieve your user record. Any changes made may not merge properly when the record is retrieved.

Session Type: Windows Terminal Services

Bookmark Name: Seth's PC

Description:

5. Input your Hostname under "***Host/Computer Name***" and change the "***Color Depth***" to 32bit True Color
*You can obtain your Host/Computer Name by going to PC and right-click to access Properties*.



Settings

* Host: 125-INF-00000

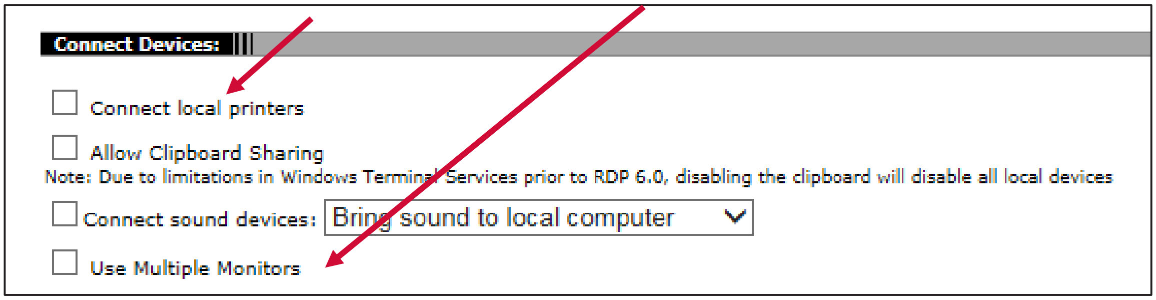
Client Port:

Server Port:

Screen Size: Full Screen

Color Depth: 32-bit (True Color)

6. Select "**Connect local printers**" and "Use **Multiple Monitors**"



Connect Devices:

□ Connect local printers

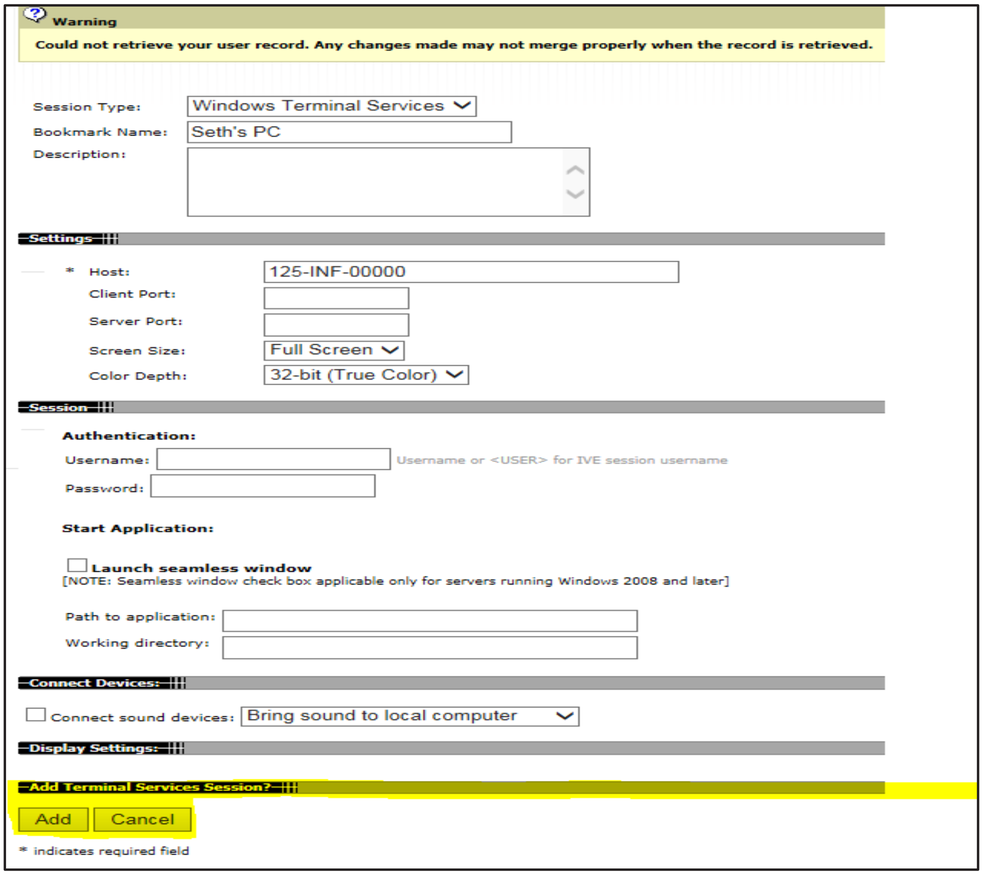
□ Allow Clipboard Sharing

Note: Due to limitations in Windows Terminal Services prior to RDP 6.0, disabling the clipboard will disable all local devices

□ Connect sound devices: Bring sound to local computer

□ Use Multiple Monitors

7. Select “**Add**” to save your settings.



Warning

Could not retrieve your user record. Any changes made may not merge properly when the record is retrieved.

Session Type: Windows Terminal Services

Bookmark Name: Seth's PC

Description:

**Settings**

* Host: 125-INF-00000

Client Port:

Server Port:

Screen Size: Full Screen

Color Depth: 32-bit (True Color)

**Session**

**Authentication:**

Username: Username or <USER> for IVE session username

Password:

**Start Application:**

□ **Launch seamless window**
[NOTE: Seamless window check box applicable only for servers running Windows 2008 and later]

Path to application:

Working directory:

**Connect Devices:**

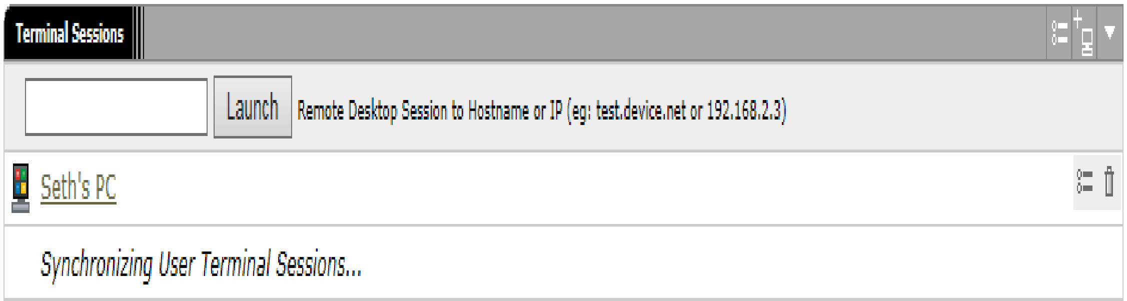
□ Connect sound devices: Bring sound to local computer

**Display Settings:**

**Add Terminal Services Session?**

* indicates required field

8. Click on the **Bookmark Name Hyperlink** to gain access to your Windows PC

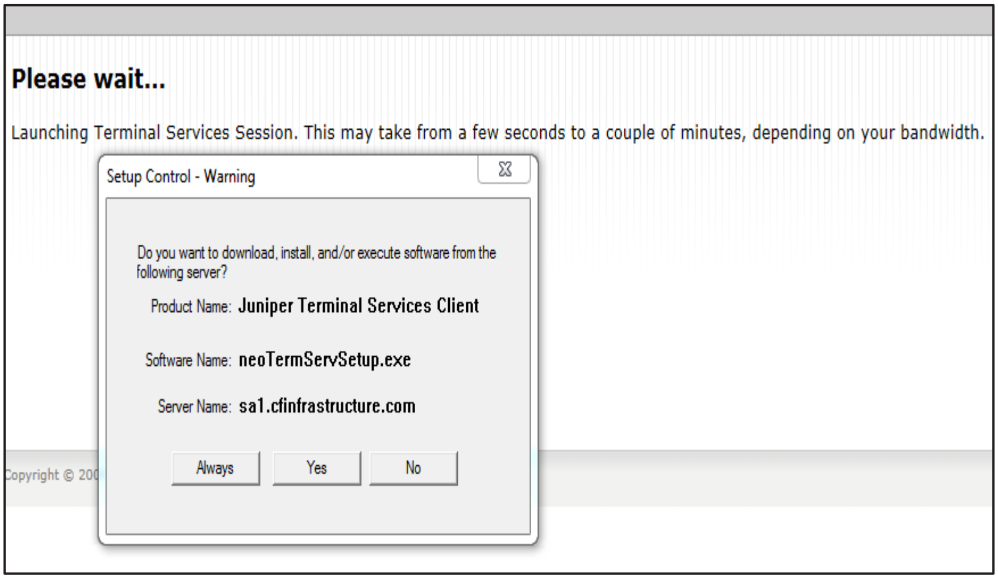


Remote Desktop Session to Hostname or IP (eg: test.device.net or 192.168.2.3)

Seth's PC

Synchronizing User Terminal Sessions...

9. It will prompt you to install essential software. Select “**Always**”



**Please wait...**

Launching Terminal Services Session. This may take from a few seconds to a couple of minutes, depending on your bandwidth.

Setup Control - Warning

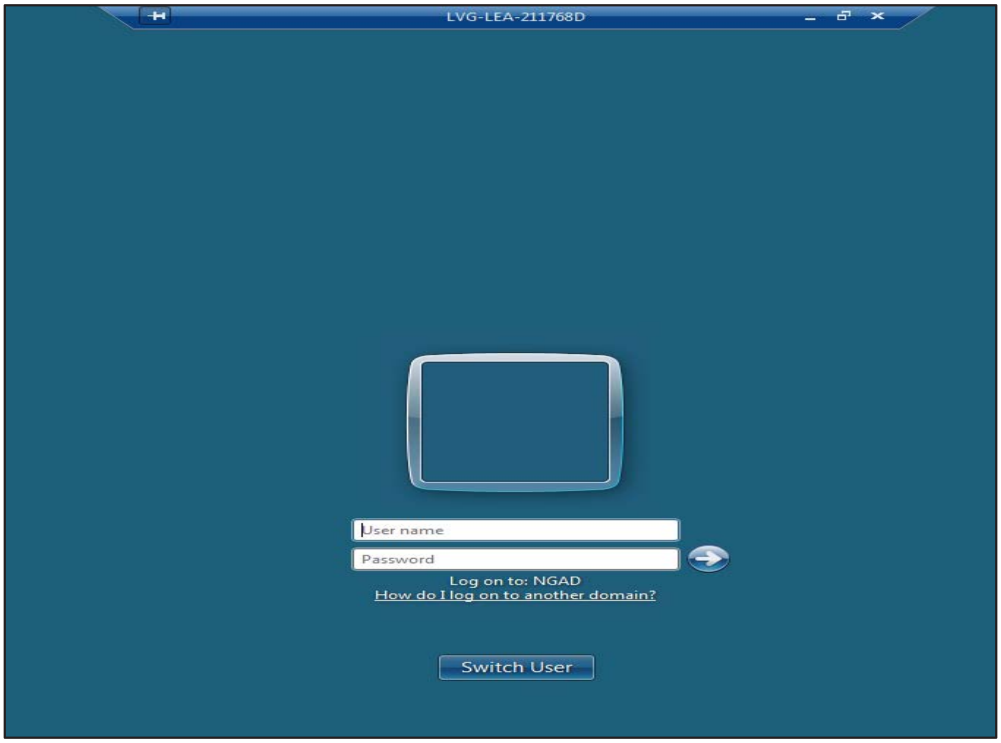
Do you want to download, install, and/or execute software from the following server?

Product Name: Juniper Terminal Services Client

Software Name: neoTermServSetup.exe

Server Name: sa1.cfinfrastructure.com

10. Login as you normally would to your PC.



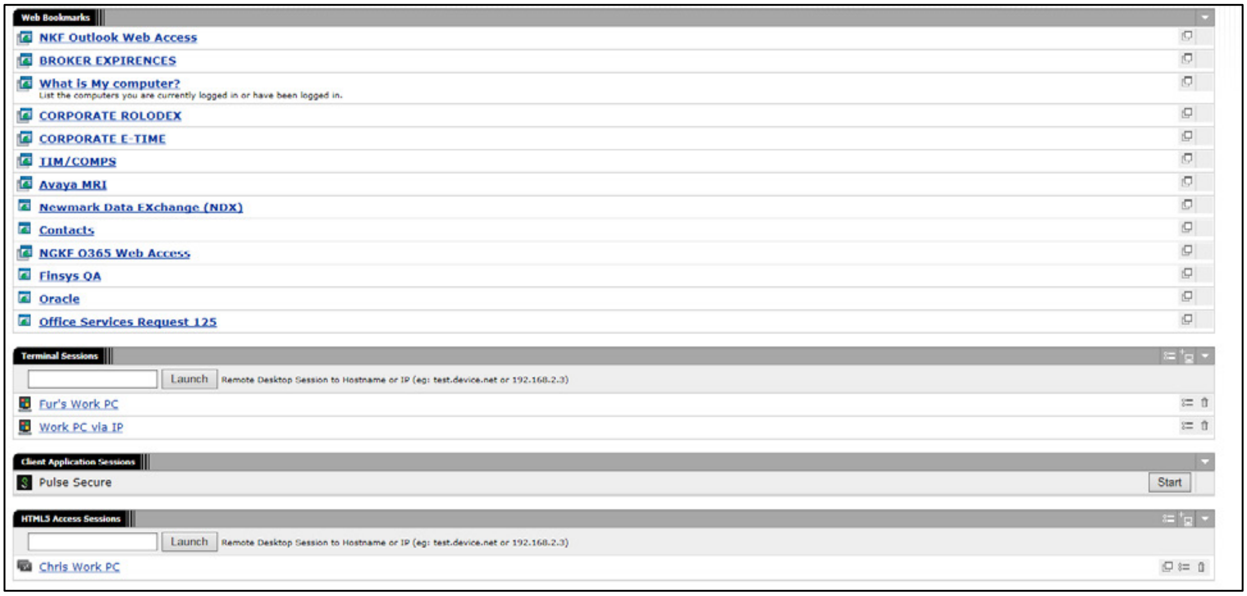
11. You are now connected to your PC.

# For MAC users Using their Personal Machine

# To Remote to their Windows PC at Work

**Steps 1 – 3** are the same as above

4. Go to the HTML5 Access Sessions Section



Web Bookmarks

NKF Outlook Web Access

BROKER EXPIRENCES

What is My computer?
List the computers you are currently logged in or have been logged in.

CORPORATE ROLODEX

CORPORATE E-TIME

TIM/COMPS

Avaya MRI

Newmark Data EXchange (NDX)

Contacts

NGKF O365 Web Access

Finsys QA

Oracle

Office Services Request 125

Terminal Sessions

Launch Remote Desktop Session to Hostname or IP (eg: test.device.net or 192.168.2.3)

Fur's Work PC

Work PC via IP

Client Application Sessions

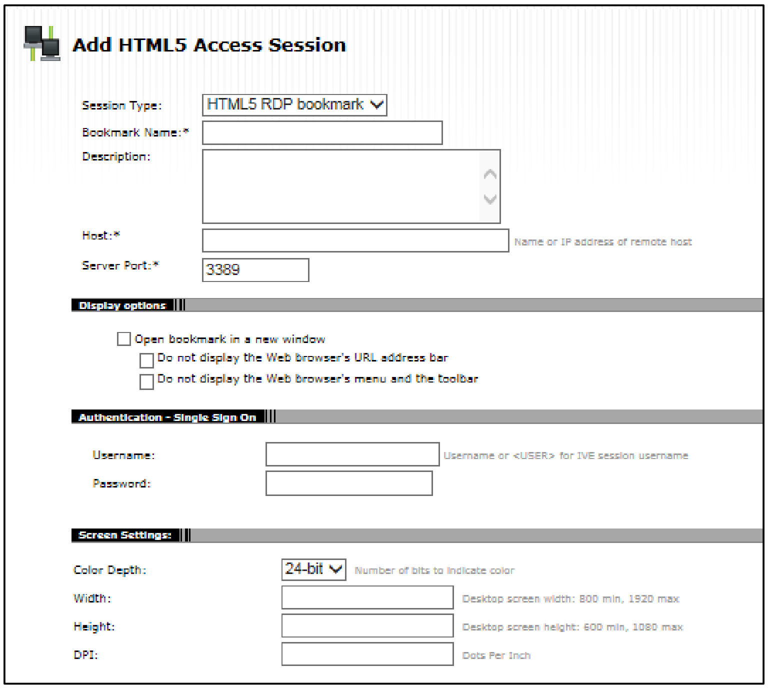
Pulse Secure Start

HTML5 Access Sessions

Launch Remote Desktop Session to Hostname or IP (eg: test.device.net or 192.168.2.3)

Chris Work PC

5. Click on the "**Add HTML5 Access Session**"- You will see the screen below



Add HTML5 Access Session

Session Type: HTML5 RDP bookmark

Bookmark Name:*

Description:

Host:* Name or IP address of remote host

Server Port:* 3389

Display options

□ Open bookmark in a new window

□ Do not display the Web browser's URL address bar

□ Do not display the Web browser's menu and the toolbar

Authentication - Single Sign On

Username: Username or <USER> for IVE session username

Password:

Screen Settings:

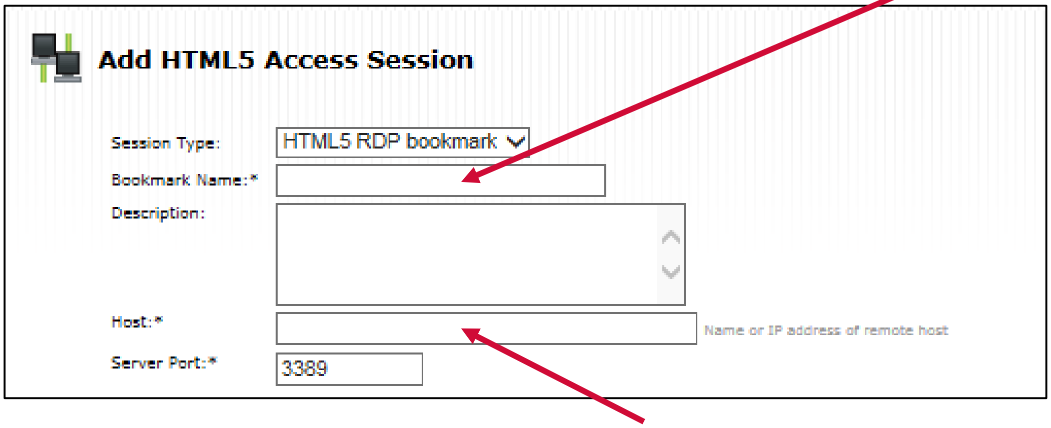
Color Depth: 24-bit Number of bits to indicate color

Width: Desktop screen width: 800 min, 1920 max

Height: Desktop screen height: 600 min, 1080 max

DPI: Dots Per Inch

6. Select your session type as **HTML5 RDP Bookmark** as well as type a **Bookmark Name** to use as a shortcut. *(**Example** – Your Name Work PC)*



**Add HTML5 Access Session**

Session Type: HTML5 RDP bookmark

Bookmark Name:*

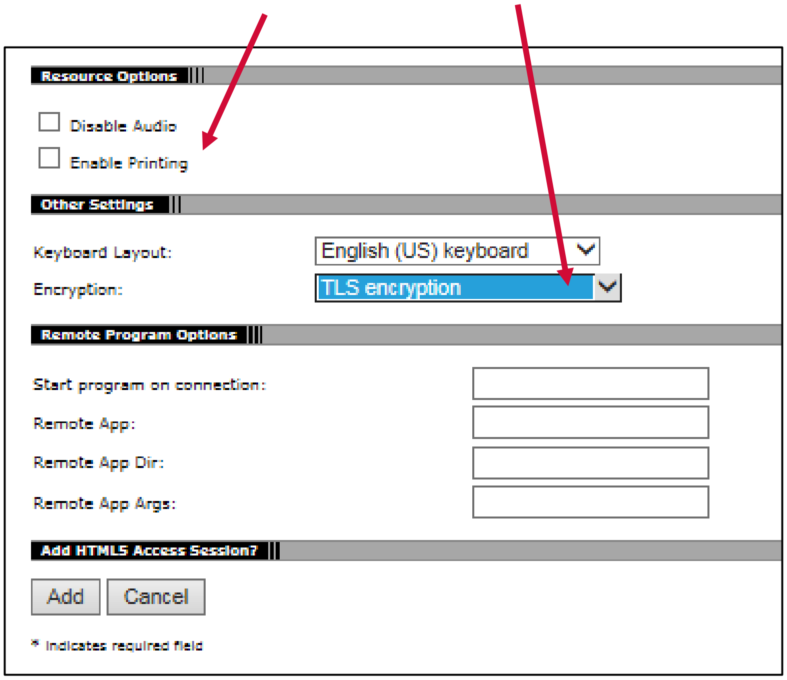
Description:

Host:* — Name or IP address of remote host

Server Port:* 3389

7. Input your Hostname under "***Host/Computer Name***" and change the "***Color Depth***" to 32bit True Color You can obtain your Host/Computer Name by going to PC and right-click to access Properties.

8. Check off "**Enable Printing**"
9. Under Encryption, select "**TLS encryption**"



**Resource Options**

□ Disable Audio

□ Enable Printing

**Other Settings**

Keyboard Layout: English (US) keyboard

Encryption: TLS encryption

**Remote Program Options**

Start program on connection:

Remote App:

Remote App Dir:

Remote App Args:

**Add HTML5 Access Session?**

* Indicates required field

10. Click "**Add**" to save your settings.

11. Click on the **Bookmark Name Hyperlink** to gain access to your Windows PC

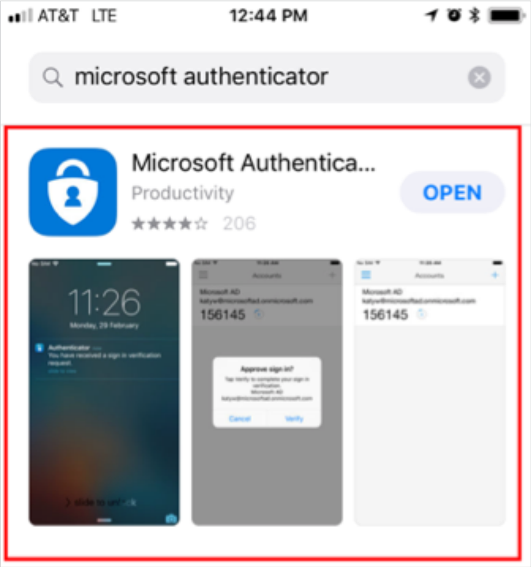
# MULTI-FACTOR **AUTHENTICATION**

## APP INSTALLATION

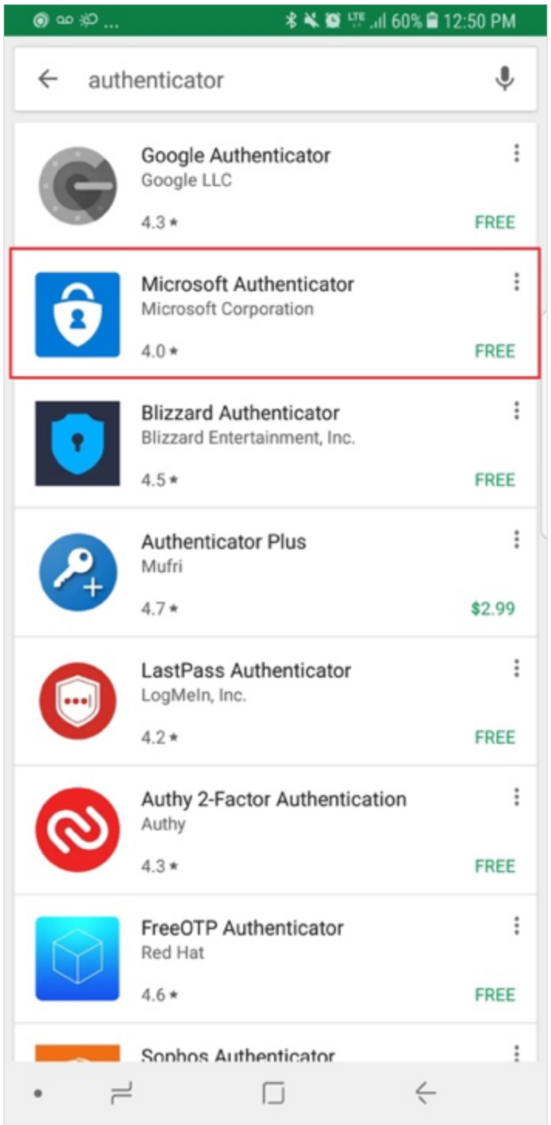
1. Install **Microsoft Authenticator** app from Apple App Store or Google Play store

   From the app store search for **“Microsoft Authenticator”**

   ***NOTE: Do not select Google Authenticator***



APPLE IPHONE APP STORE



| App | Developer | Rating | Price |
|---|---|---|---|
| Google Authenticator | Google LLC | 4.3 ★ | FREE |
| Microsoft Authenticator | Microsoft Corporation | 4.0 ★ | FREE |
| Blizzard Authenticator | Blizzard Entertainment, Inc. | 4.5 ★ | FREE |
| Authenticator Plus | Mufri | 4.7 ★ | $2.99 |
| LastPass Authenticator | LogMeIn, Inc. | 4.2 ★ | FREE |
| Authy 2-Factor Authentication | Authy | 4.3 ★ | FREE |
| FreeOTP Authenticator | Red Hat | 4.6 ★ | FREE |
| Sophos Authenticator | | | |

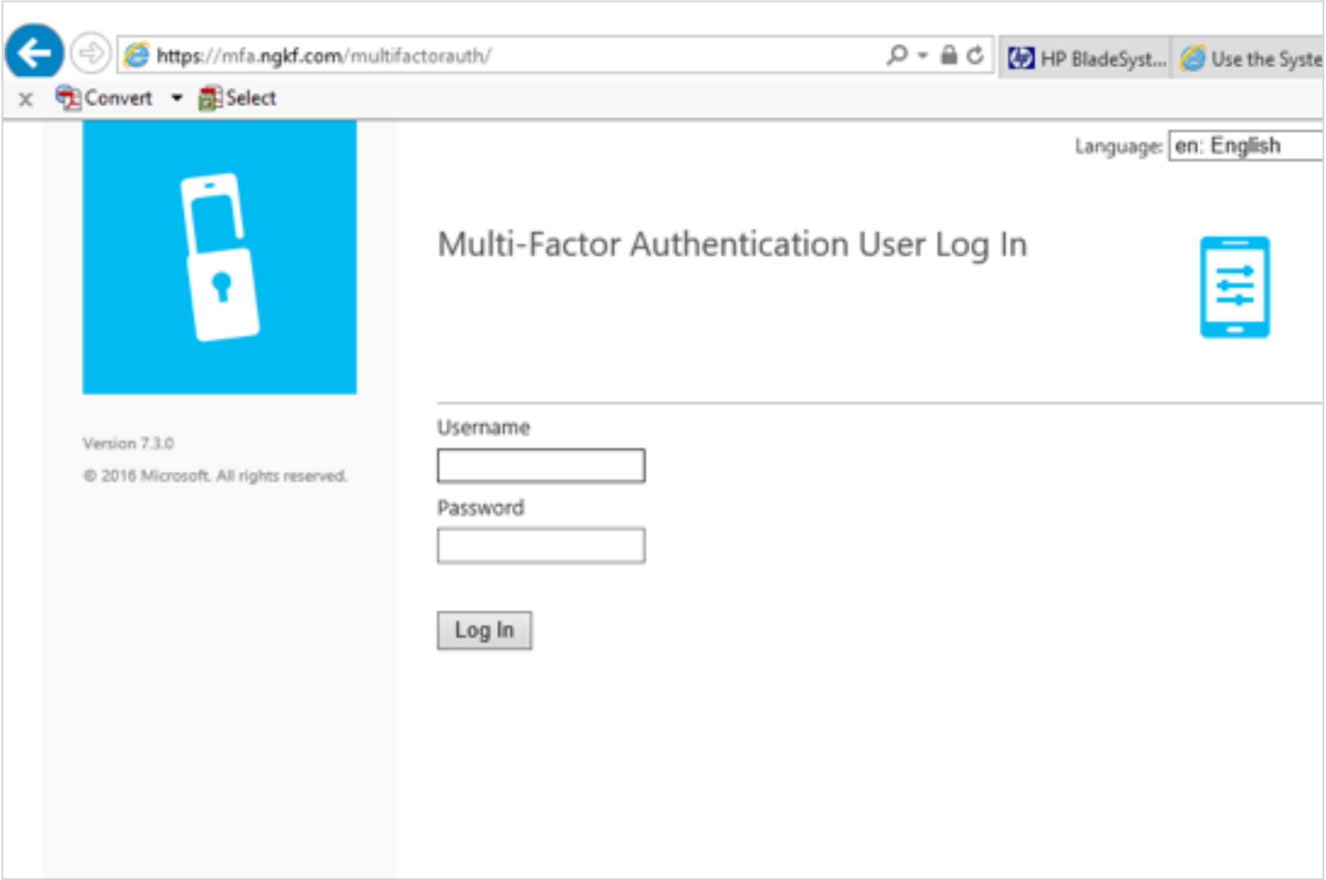
ANDROID PLAY STORE

Once app is installed on your smart device, proceed to the next section

# LOG IN

2. In a web browser on PC, go to
   **HTTPS://mfa.ngkf.com/multifactorauth**

3. Log in to the website with your Newmark User ID and Password and press **Enter**



Multi-Factor Authentication User Log In

Username

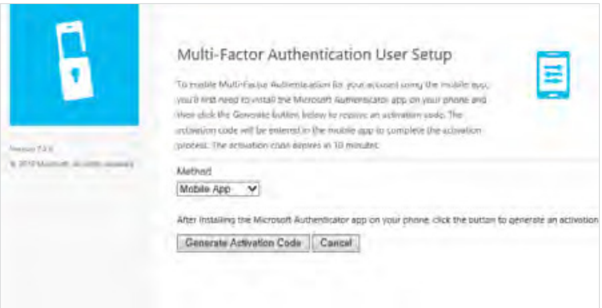
Password

## FIRST VISIT TO THE SITE

4. If this is the first time you are logging in to the site, you will be presented with the **Multi-Factor Authentication User Setup**

5. Select your Method of setup from the dropdown

   *Note: The default is "Mobile APP"*



Multi-Factor Authentication User Setup

To enable Multi-Factor Authentication for your account using the mobile app, you'll first need to install the Microsoft Authenticator app on your phone and then click the Generate button below to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes.

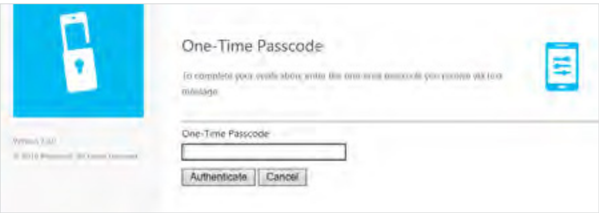
Method: Mobile App

After installing the Microsoft Authenticator app on your phone, click the button to generate an activation

Proceed to Step 6 on next page

## CHANGING OLD MFA SETUP

4. If you already have **Multi-Factor Authentication** set up on your mobile device, the page will prompt you for a 6-digit MFA Code that would be texted to the device. (If Authenticator app is your default method, select "Approve.")



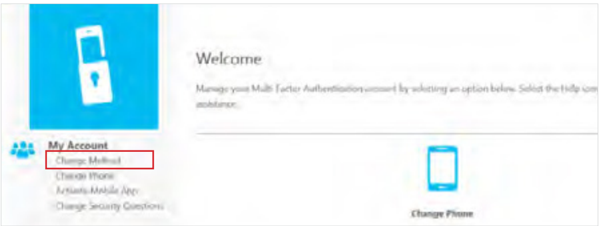
One-Time Passcode

To complete your verification, enter the one-time passcode you receive via text message.

One-Time Passcode:

Enter the 6-digit MFA Code from your smart device on the web site and click the **Authenticate** button

5. Under My Account, select **"Change Method"**

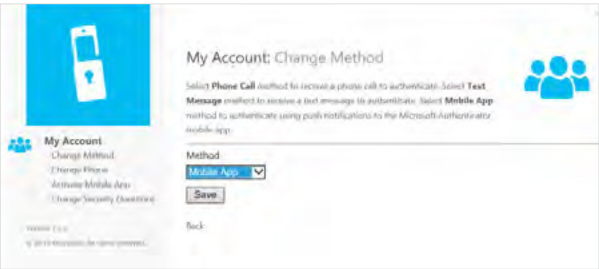


Welcome

Manage your Multi-Factor Authentication account by selecting an option below. Select the Help icon assistance.

Choose **"Mobile App"** if it is showing "Text Message"

Click **Save**



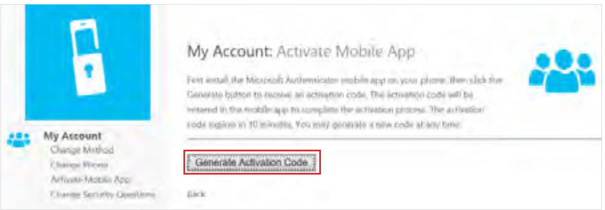
My Account: Change Method

Select **Phone Call** method to receive a phone call to authenticate. Select **Text Message** method to receive a text message to authenticate. Select **Mobile App** method to authenticate using push notifications to the Microsoft Authenticator mobile app.

Method: Mobile App

Under My Account, select **"Activate Mobile App"**

Select **Generate Activation Code** button

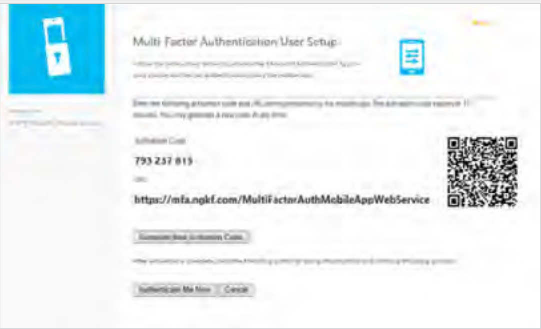


My Account: Activate Mobile App

First install the Microsoft Authenticator mobile app on your phone. Then click the Generate button to receive an activation code. The activation code will be entered in the mobile app to complete the activation process. The activation code expires in 10 minutes. You may generate a new code at any time.

MOBILE
## APP SETUP

6. Click on the **Generate Activation Code** button



Multi Factor Authentication User Setup

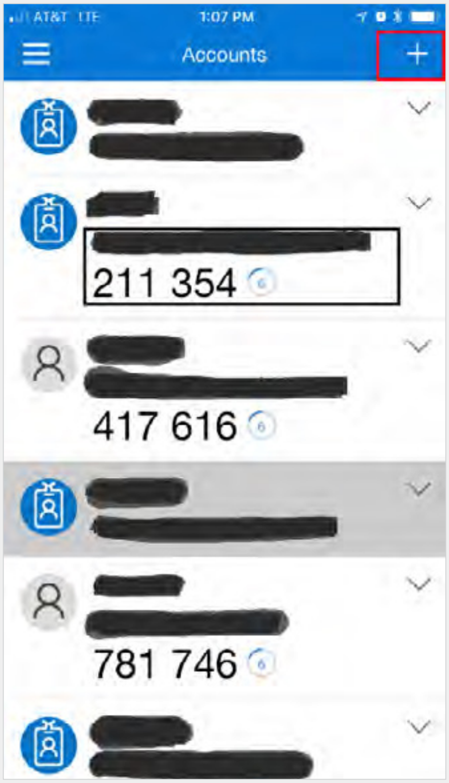
Activation Code

793 237 815

https://mfa.ngkf.com/MultiFactorAuthMobileAppWebService

7. On your smart device, open the **Microsoft Authenticator** app

8. Click on the **"+" button** in the upper right corner



[redacted]

[redacted]

211 354

[redacted]

417 616

[redacted]

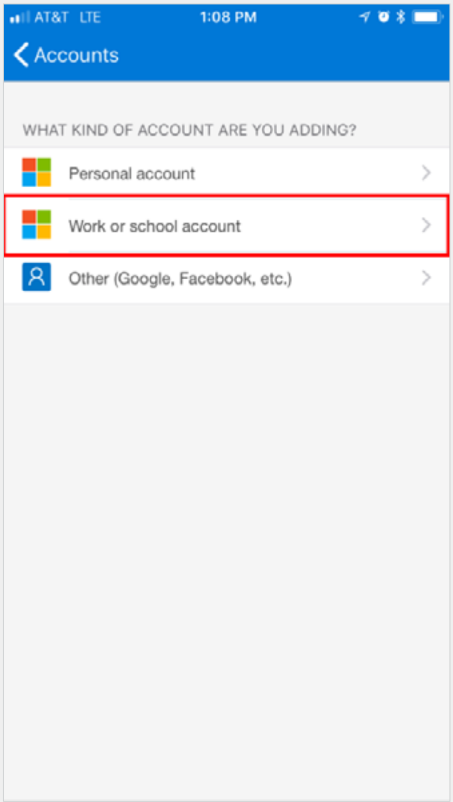
[redacted]

781 746

[redacted]

MOBILE
## APP SETUP

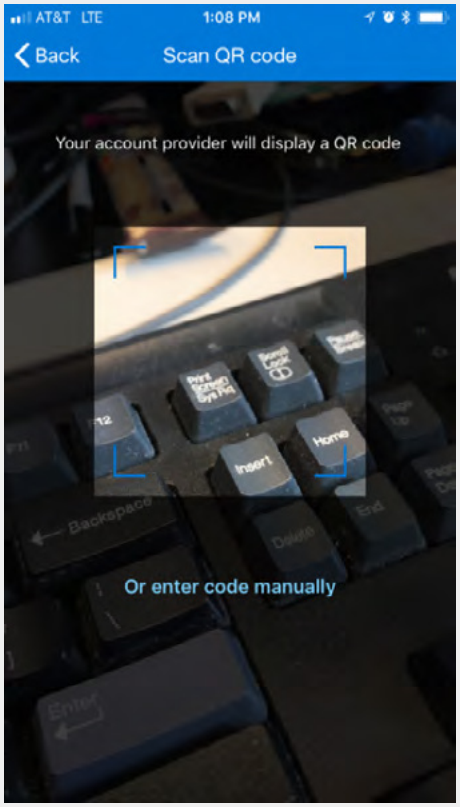
9. Select **"Work or school account"**



WHAT KIND OF ACCOUNT ARE YOU ADDING?

## MOBILE
## **APP SETUP**

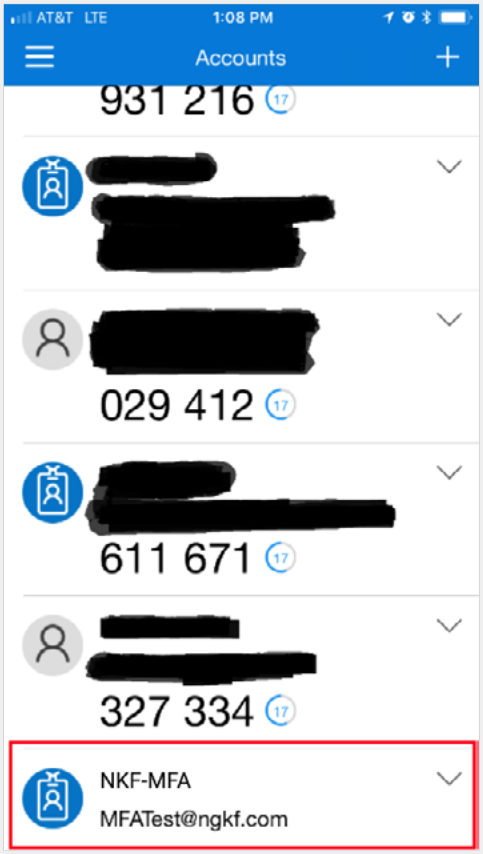
10. Once the QR scanning screen opens, **scan the QR code generated in your browser** (you may have to grant authenticator app access to your camera)



Your account provider will display a QR code

## MOBILE
## **APP SETUP**

11. The app should return to the main screen and list the new **NKF-MFA account**



931 216

[redacted]

[redacted]

029 412

[redacted]

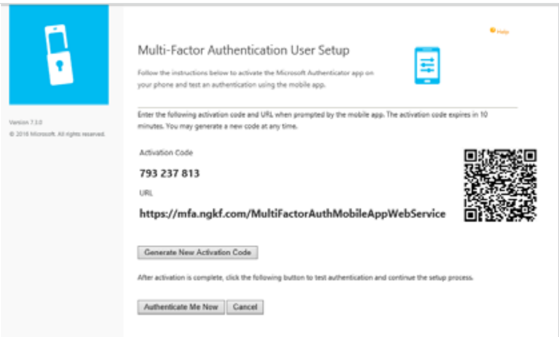
611 671

[redacted]

327 334

NKF-MFA
MFATest@ngkf.com

12. Back in the web browser, click on **Authenticate Me Now** to continue the setup process



Multi-Factor Authentication User Setup

Follow the instructions below to activate the Microsoft Authenticator app on your phone and test an authentication using the mobile app.

Enter the following activation code and URL when prompted by the mobile app. The activation code expires in 10 minutes. You may generate a new code at any time.

Activation Code

793 237 813

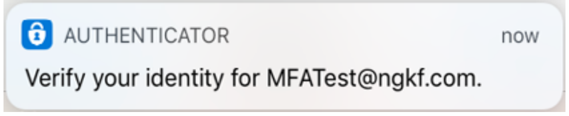
URL

https://mfa.ngkf.com/MultiFactorAuthMobileAppWebService

After activation is complete, click the following button to test authentication and continue the setup process.

Help
Generate New Activation Code
Authenticate Me Now
Cancel
Version 7.3.0
© 2016 Microsoft. All rights reserved.

13. A **notification** should appear on your smart device

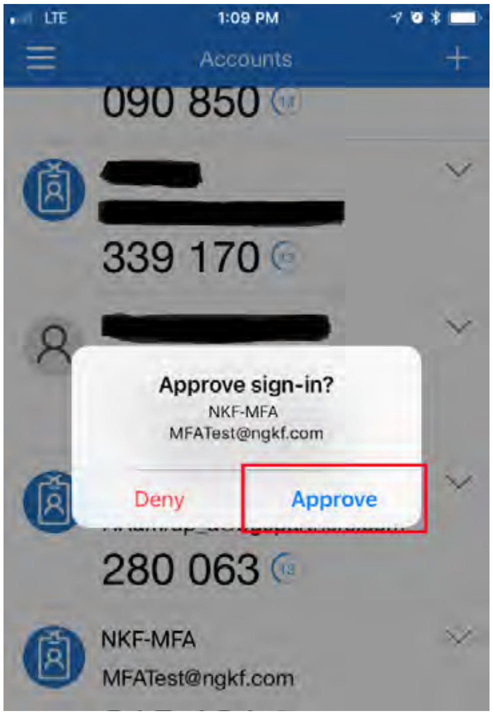


Verify your identity for MFATest@ngkf.com.

14. Click on the notification or open the **Microsoft Authenticator** app

15. A pop up should open in the app asking to approve the sign-in

Click **Approve**

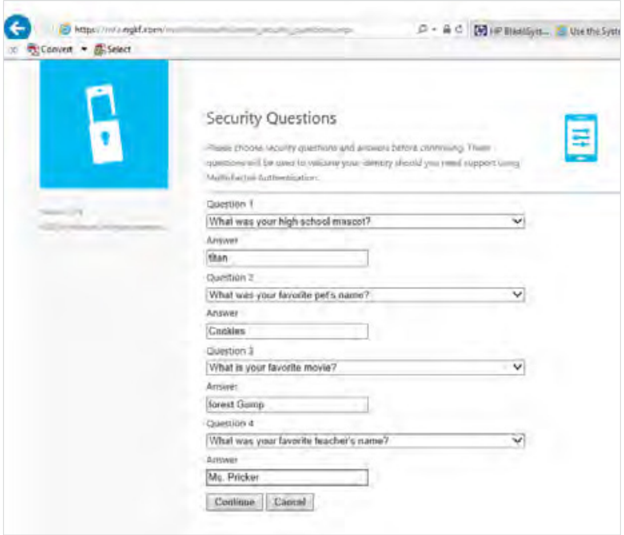


Approve sign-in?

NKF-MFA

MFATest@ngkf.com

16. The web site will continue to the **Security Questions Screen.** Answer four (4) questions of your choice and click continue.



Security Questions

Please choose security questions and answers before continuing. These questions will be used to validate your identity should you need support using Multi-Factor Authentication.

Question 1

What was your high school mascot?

Answer

titan

Question 2

What was your favorite pet's name?

Answer

Cookies

Question 3

What is your favorite movie?

Answer

forest Gump

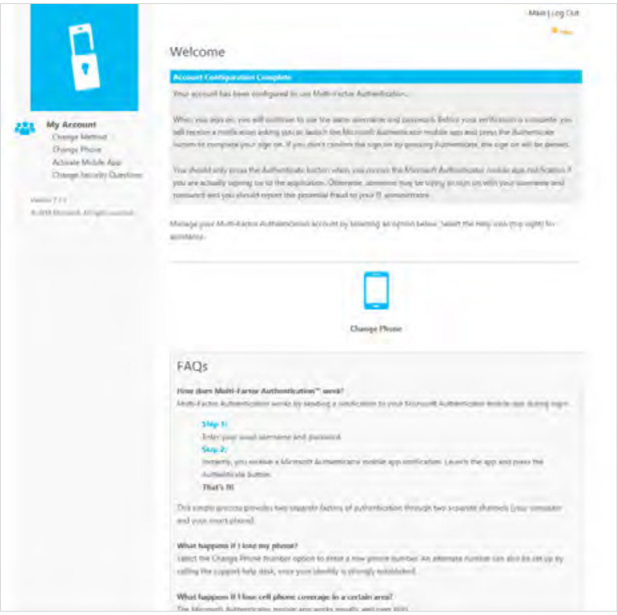
Question 4

What was your favorite teacher's name?

Answer

Ms. Pricker

17. Your registration is now complete. You will be now be at the Welcome screen that contains useful FAQs and link to change your account.



Welcome

**Account Configuration Complete**

Your account has been configured to use Multi-Factor Authentication.

When you sign on, you will continue to use the same username and password. Before your verification is complete, you will receive a notification asking you to launch the Microsoft Authenticator mobile app and press the Authenticate button to complete your sign on. If you don't confirm the sign on by pressing Authenticate, the sign on will be denied.

You should only press the Authenticate button when you receive the Microsoft Authenticator mobile app notification if you are actually signing on to the application. Otherwise, someone may be trying to sign on with your username and password and you should report this potential fraud to your IT administrator.

Manage your Multi-Factor Authentication account by selecting an option below. Select the Help link (top right) for assistance.

FAQs

**How does Multi-Factor Authentication™ work?**

Multi-Factor Authentication works by sending a notification to your Microsoft Authenticator mobile app during login.

Step 1:

Enter your usual username and password.

Step 2:

Instantly, you receive a Microsoft Authenticator mobile app notification. Launch the app and press the Authenticate button.

**That's it!**

This simple process provides two separate factors of authentication through two separate channels (your computer and your smart phone).

**What happens if I lose my phone?**

Select the Change Phone Number option to enter a new phone number. An alternate number can also be set up by calling the support help desk, once your identity is strongly established.

**What happens if I lose cell phone coverage in a certain area?**

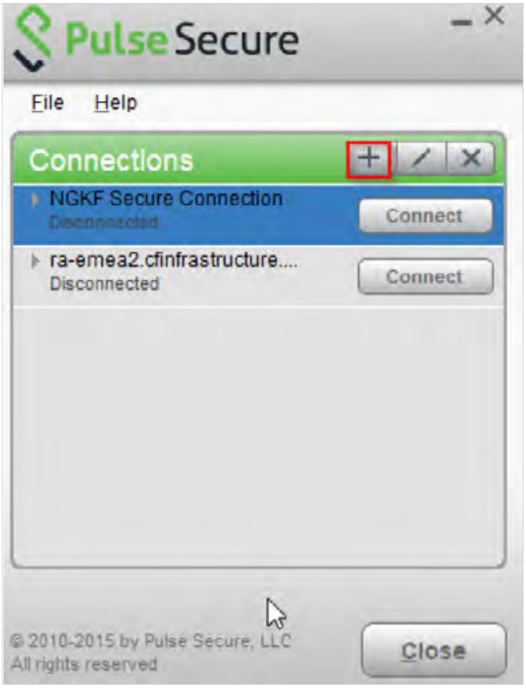
The Microsoft Authenticator mobile app works equally well over WiFi.

**Pulse Secure Users**
(Corporate Laptop with Pulse Client)

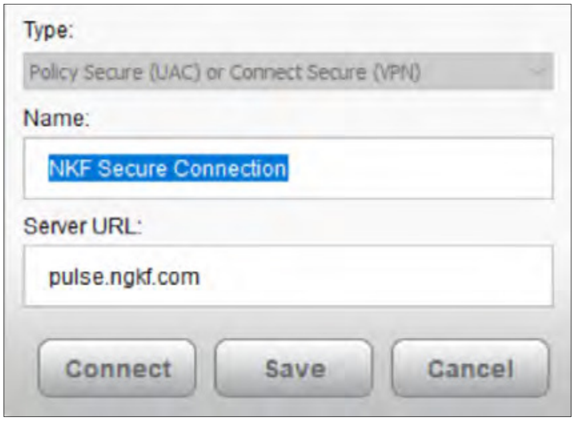
# PULSE **SECURE**

## LOG IN

1. You will need to create a new connection in the client. In the Pulse client, click on the **"+" symbol** to create a new connection.



2. Set the Connection name to **"NKF Secure Connection,"** and the Server URL to **"pulse.ngkf.com"**


Type: Policy Secure (UAC) or Connect Secure (VPN)

Name: NKF Secure Connection

Server URL: pulse.ngkf.com

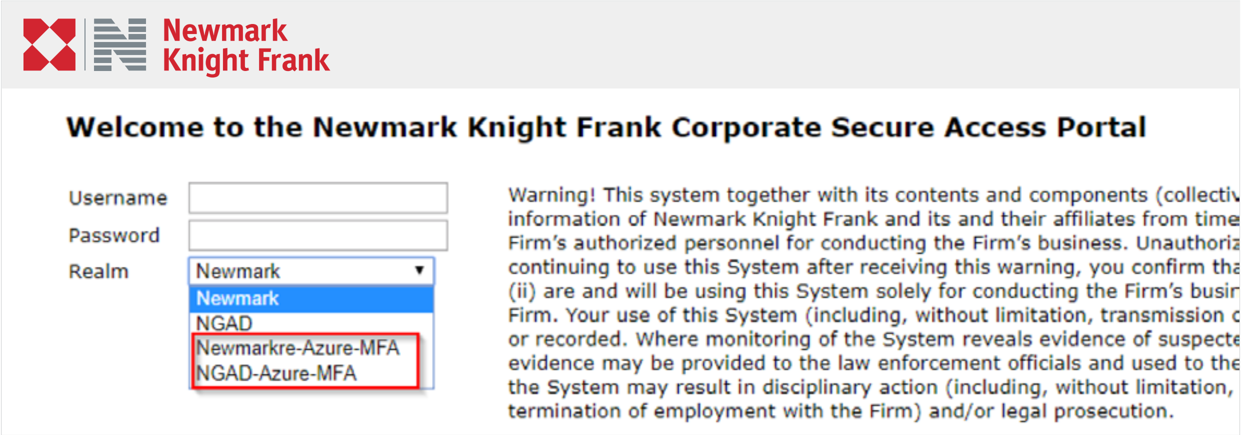
3. **Log in** using the new connection. Once you click **"connect,"** you will be prompted on your mobile phone via SMS, phone call, or mobile app (depending on how you set it up), to **approve the login.** Once approved you will be signed in as normal.

**If your laptop requires a Windows Update or Antivirus Scan, PULSE SECURE will let you know via a pop-up window.*

NEWMARK

# CONNECT.NGKF.COM
# USERS
## LOG IN

1. When you select the Realm dropdown on the sign-in page, you will see the options for MFA for NGAD and Newmarkre domains. **Select the MFA realm** for your domain, and enter your credentials as normal.



Welcome to the Newmark Knight Frank Corporate Secure Access Portal

Username

Password

Realm: Newmark

Warning! This system together with its contents and components (collectiv
information of Newmark Knight Frank and its and their affiliates from time
Firm's authorized personnel for conducting the Firm's business. Unauthoriz
continuing to use this System after receiving this warning, you confirm tha
(ii) are and will be using this System solely for conducting the Firm's busir
Firm. Your use of this System (including, without limitation, transmission c
or recorded. Where monitoring of the System reveals evidence of suspecte
evidence may be provided to the law enforcement officials and used to the
the System may result in disciplinary action (including, without limitation,
termination of employment with the Firm) and/or legal prosecution.

2. Once you click sign in, you will be prompted on your mobile phone via SMS, phone call, or mobile app (depending on how you set it up), to **approve the login.** Once approved you will be signed in as normal.