Carolinas HealthCare System

SecureConnect
Remote Access Instructions

Information Security

February, 2014

Confidential Information Enclosed:

The enclosed information is confidential and/or legally privileged. It is intended only for the use by individual(s) and entities with a Business Associate Agreement signed with Carolinas Healthcare System. If you are not an intended recipient of this document, please notify the sender immediately and delete the material from any computer. Do not deliver, distribute or copy this document, and do not disclose its contents or take any action in reliance on the information it contains. Thank you.

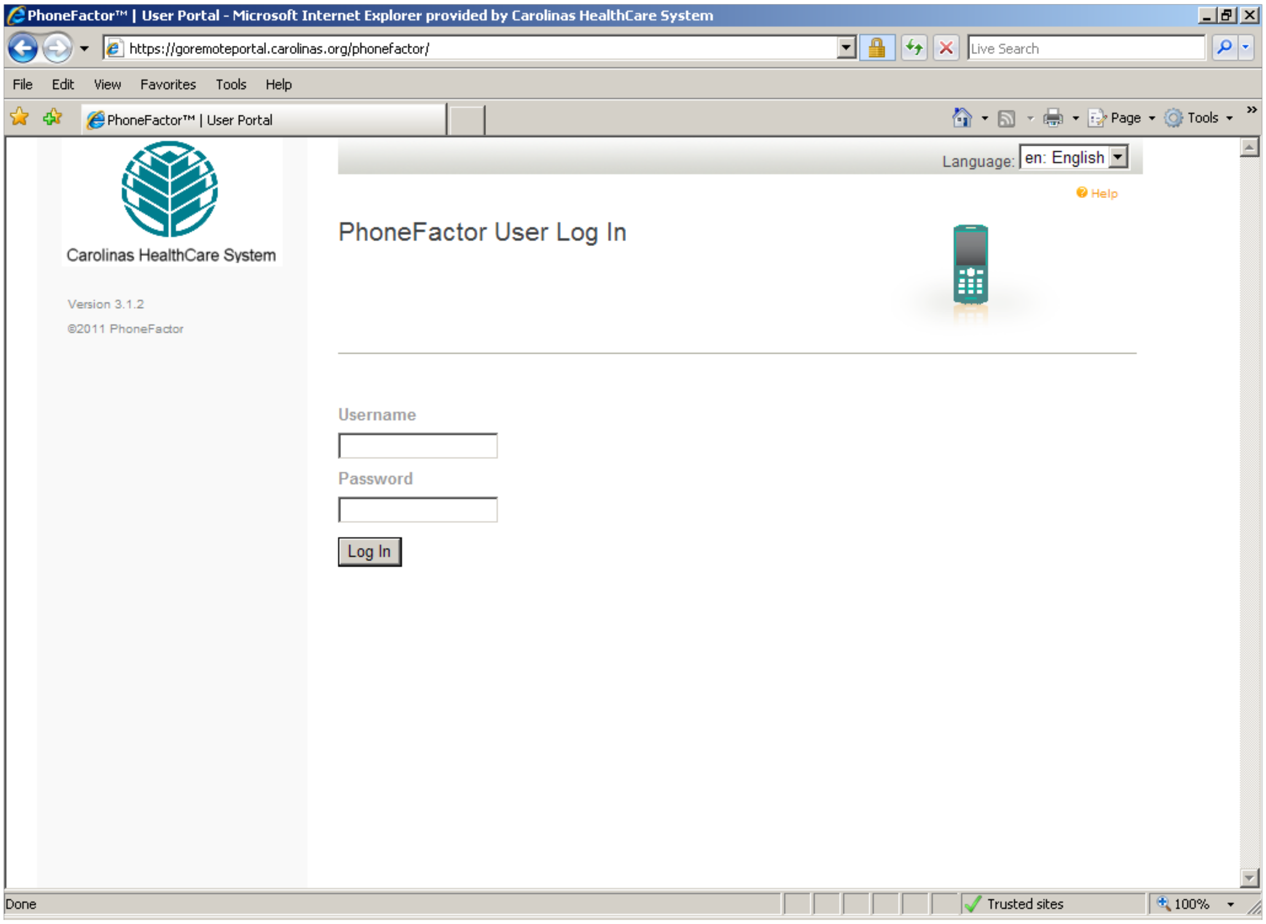
Instructions for CHS Employees to Access SecureConnect

Section 1. Registering your account in the goRemote portal

To set up your access to SecureConnect.Carolinas.org and/or goRemote.Carolinas.org, please follow the instructions below:

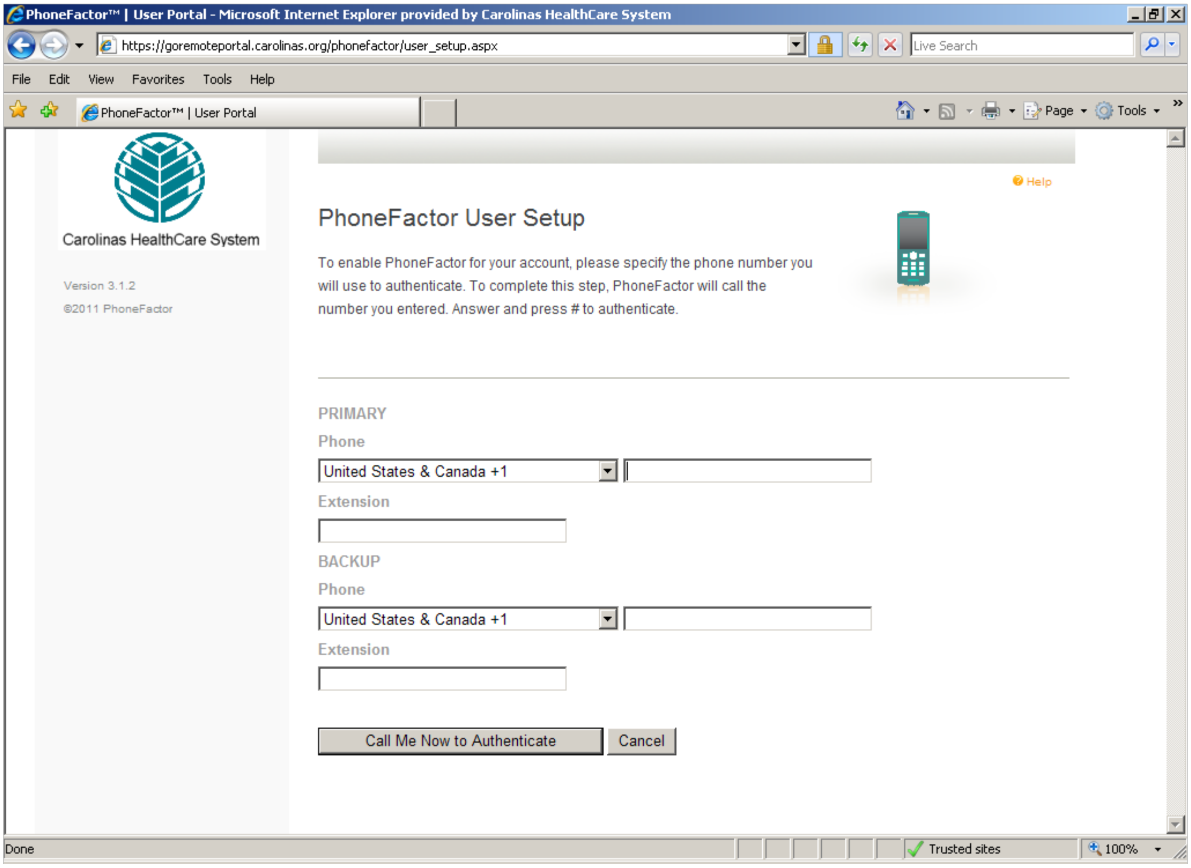
Please note: You must also be in the correct Active Directory group to access SecureConnect. This access is not granted to everyone by default. If you are not a member, and you are entering your credentials properly, you will receive this message: (Invalid username or password.Please re-enter your user information). If you have never logged into remote access, you need to ensure your manager has put in an OSR for this access. If you have had remote access before, you should call the CHS Support Center @ 704-446-6161 to discuss the issues with your account.

1. **Open a browser window on your device** (Internet Explorer, FireFox, and Safari for MacOS are supported). Browse to https://goRemoteportal.carolinas.org


PhoneFactor™ | User Portal - Microsoft Internet Explorer provided by Carolinas HealthCare System
https://goremoteportal.carolinas.org/phonefactor/
Live Search
File
Edit
View
Favorites
Tools
Help
PhoneFactor™ | User Portal
Page
Tools
Carolinas HealthCare System
Version 3.1.2
©2011 PhoneFactor
Language: en: English
Help
PhoneFactor User Log In
Username
Password
Log In
Done
Trusted sites
100%

1. **Enter your active directory username and password** – This is the same username and password you use to log in to a CHS computer normally, and then **click "Log In"**.

2. **The PhoneFactor User Setup page will display** – Enter the primary and backup phone numbers you will use to authenticate and then click **"Call Me Now to Authenticate."**


PhoneFactor™ | User Portal - Microsoft Internet Explorer provided by Carolinas HealthCare System
https://goremoteportal.carolinas.org/phonefactor/user_setup.aspx
Live Search
File
Edit
View
Favorites
Tools
Help
PhoneFactor™ | User Portal
Page
Tools
Carolinas HealthCare System
Version 3.1.2
©2011 PhoneFactor
Help
Done
Trusted sites
100%

PhoneFactor User Setup

To enable PhoneFactor for your account, please specify the phone number you will use to authenticate. To complete this step, PhoneFactor will call the number you entered. Answer and press # to authenticate.

PRIMARY

Phone

United States & Canada +1

Extension

BACKUP

Phone

United States & Canada +1

Extension

Call Me Now to Authenticate | Cancel

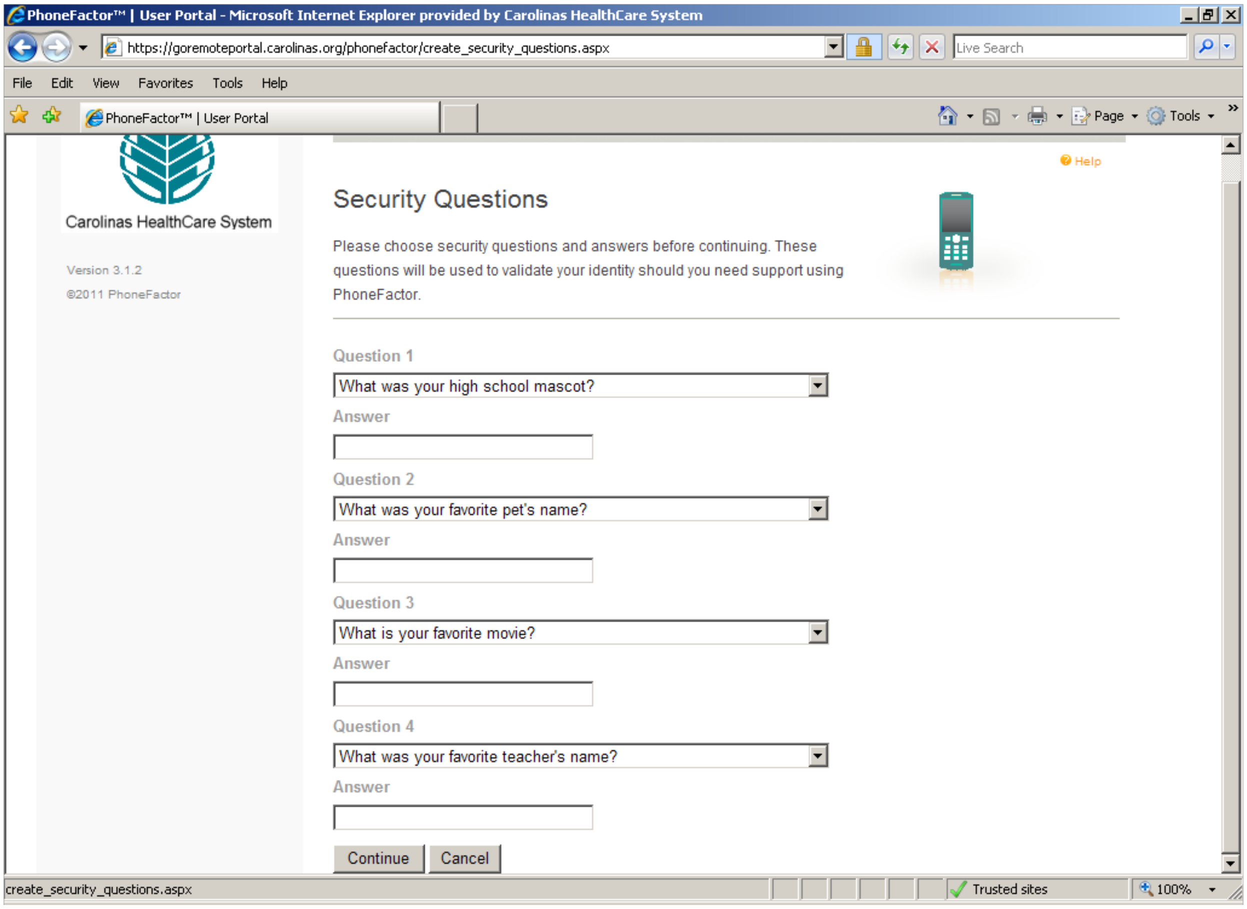
3. ***The PhoneFactor system will call your primary phone number first.*** If no response is received during the primary call, your secondary number will be called. If these are not answered, your registration cannot be completed.

   - ***Following your complete registration***: If you do not have your phone with you or are not near another phone that could be used; please review the information at the bottom of this guide in **Section 3** for additional instruction.

During the 1st call/registration and when you attempt to authenticate in future sessions for remote access:

4. **You will receive a call from 704-446-6161 on the phone number you registered. Answer the phone and press the # key and then hang up the phone to conclude the authentication request.**

During 1st call registration: After pressing the # key, the goRemote **"Security Questions"** setup page will display as mentioned above. Each of these questions should be completed to finish your registration.


PhoneFactor™ | User Portal - Microsoft Internet Explorer provided by Carolinas HealthCare System
https://goremoteportal.carolinas.org/phonefactor/create_security_questions.aspx
Live Search
File
Edit
View
Favorites
Tools
Help
PhoneFactor™ | User Portal
Page
Tools
Help
create_security_questions.aspx
Trusted sites
100%

Carolinas HealthCare System

Version 3.1.2

©2011 PhoneFactor

Security Questions

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

Question 1

What was your high school mascot?

Answer

Question 2

What was your favorite pet's name?

Answer

Question 3

What is your favorite movie?

Answer

Question 4

What was your favorite teacher's name?

Answer

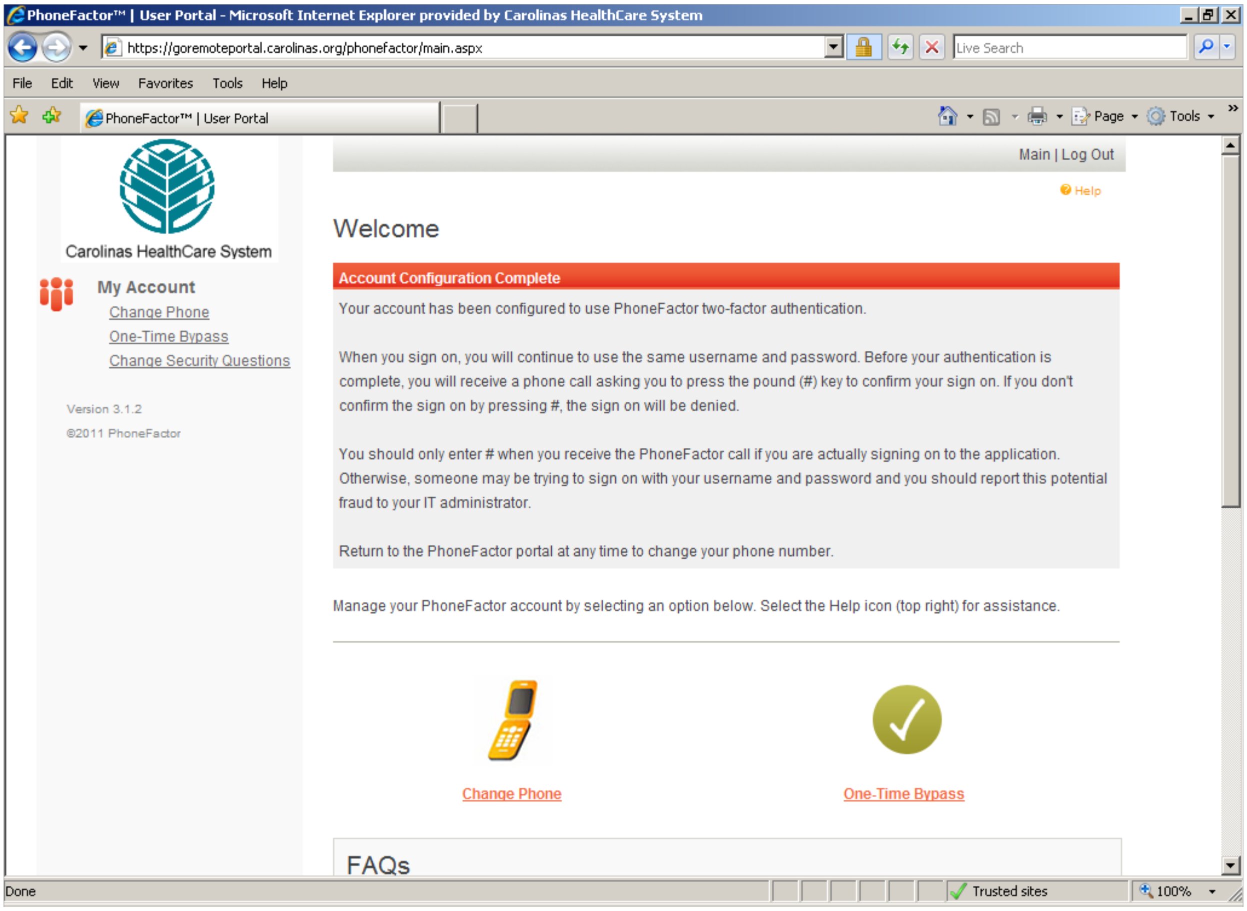
Continue Cancel

5. **Fill out the four security questions.** You may select different questions by clicking on the drop down lists. You must provide answers for all four security questions.

6. After filling in all four security questions, **click "Continue**."

7. The goRemote portal "**Welcome"** screen will display. (shown on next page)

8. Your registration is complete.


PhoneFactor™ | User Portal - Microsoft Internet Explorer provided by Carolinas HealthCare System
https://goremoteportal.carolinas.org/phonefactor/main.aspx
Live Search
File Edit View Favorites Tools Help
PhoneFactor™ | User Portal
Page Tools
Carolinas HealthCare System
My Account
Change Phone
One-Time Bypass
Change Security Questions
Version 3.1.2
©2011 PhoneFactor
Main | Log Out
Help
Change Phone
One-Time Bypass
Done
Trusted sites
100%

Welcome

Account Configuration Complete

Your account has been configured to use PhoneFactor two-factor authentication.

When you sign on, you will continue to use the same username and password. Before your authentication is complete, you will receive a phone call asking you to press the pound (#) key to confirm your sign on. If you don't confirm the sign on by pressing #, the sign on will be denied.

You should only enter # when you receive the PhoneFactor call 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.

Return to the PhoneFactor portal at any time to change your phone number.

Manage your PhoneFactor account by selecting an option below. Select the Help icon (top right) for assistance.

FAQs

9. At this point, your account has been properly setup and you are ready to log in using the remote access method of your choice. The **SecureConnect or goRemote** log in pages can now be visited to continue your remote access.

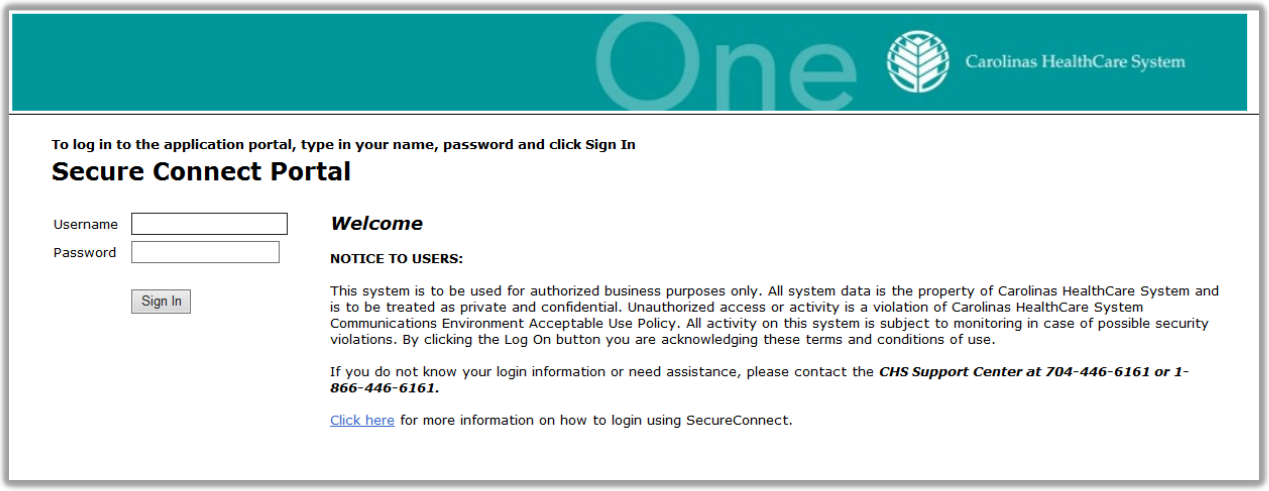
10. **Please log out** of the goRemote portal page **by clicking "Log Out"** in the upper right hand corner of the page.

11. You can return to the **goRemote portal** page at any time to change/update your registered phone numbers or change your security questions.

Section 2. Logging into SecureConnect.carolinas.org

To log in to the network remotely using SecureConnect, please follow these steps:

1. **Open a browser window** on your computer (Internet Explorer, FireFox, and Safari on MacOS are supported). **In the address bar, type:** SecureConnect.carolinas.org.



To log in to the application portal, type in your name, password and click Sign In

Secure Connect Portal

Welcome

NOTICE TO USERS:

This system is to be used for authorized business purposes only. All system data is the property of Carolinas HealthCare System and is to be treated as private and confidential. Unauthorized access or activity is a violation of Carolinas HealthCare System Communications Environment Acceptable Use Policy. All activity on this system is subject to monitoring in case of possible security violations. By clicking the Log On button you are acknowledging these terms and conditions of use.

If you do not know your login information or need assistance, please contact the ***CHS Support Center at 704-446-6161 or 1-866-446-6161.***

Click here for more information on how to login using SecureConnect.

2. **Enter** your **username and password** and click **Sign In.**

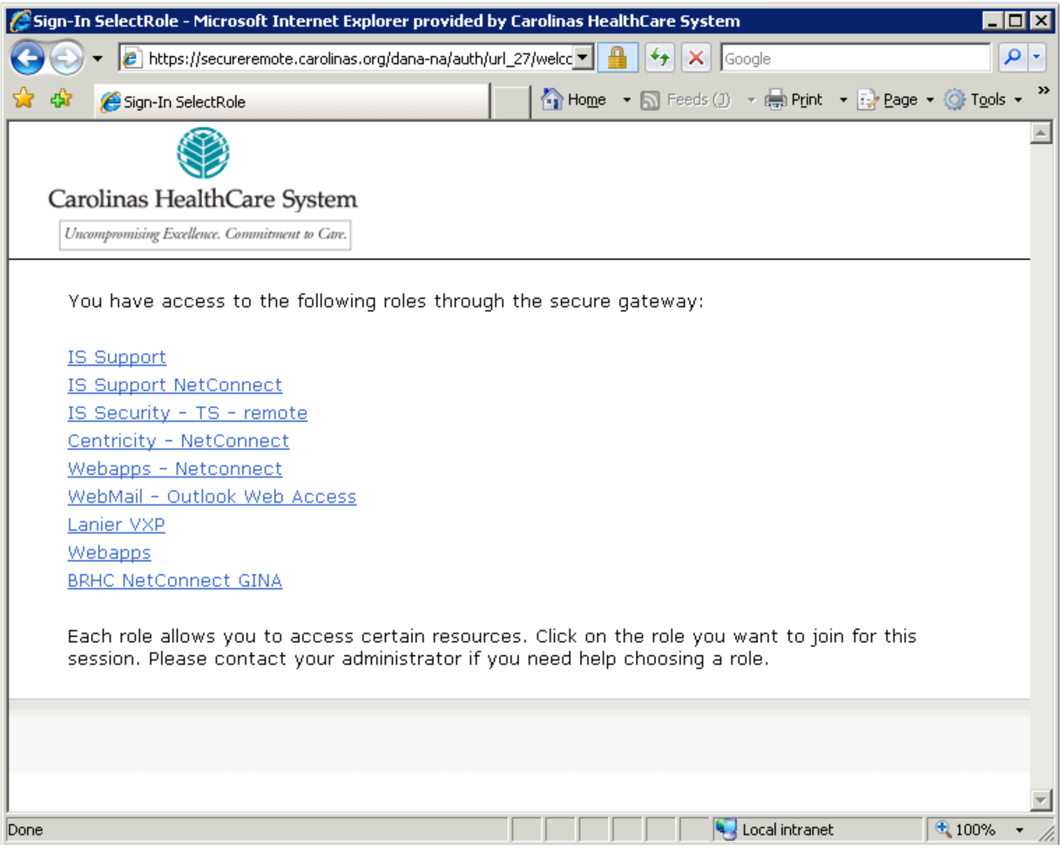
3. **You will receive a call from 704-446-6161** on your primary registered number.

4. **Answer the phone and press the # key**. If you do not have access to your primary number, wait and your secondary number will be called (assuming the call to your primary number is not answered and responded to). If you do not have access to either your primary or secondary numbers; see **Section 3** for information on how to log in using your security questions.

5. After authentication via phone or security questions, the log in process will continue, and you will begin the log in process for SecureConnect. If this is your first time accessing via the VPN (NetConnect) based solution you will have some additional steps.

6. The most common steps encountered are detailed below:

7. If you see a page requesting you to click a **role: Click on the link for WebApps–NetConnect.**



Sign-In SelectRole - Microsoft Internet Explorer provided by Carolinas HealthCare System
https://secureremote.carolinas.org/dana-na/auth/url_27/welcc
Google
Sign-In SelectRole
Home
Feeds (J)
Print
Page
Tools
Carolinas HealthCare System
Uncompromising Excellence. Commitment to Care.
Done
Local intranet
100%

You have access to the following roles through the secure gateway:

IS Support
IS Support NetConnect
IS Security - TS - remote
Centricity - NetConnect
Webapps - Netconnect
WebMail - Outlook Web Access
Lanier VXP
Webapps
BRHC NetConnect GINA

Each role allows you to access certain resources. Click on the role you want to join for this session. Please contact your administrator if you need help choosing a role.

- If you are not required to choose a role, or do not see a role selection page such as above, this is normal. You have automatically been logged in with the default role.

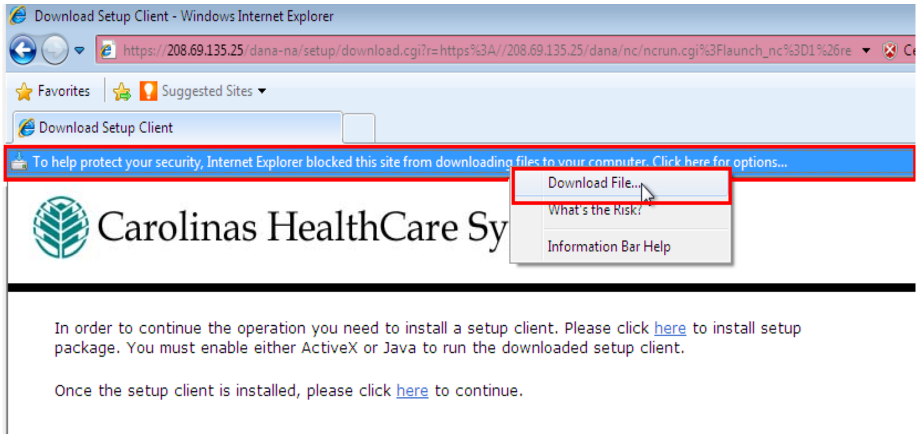
- After completing the authentication step, you will have **additional steps** to follow if this is the **first time** you have logged in from a computer, or if you have not been a previous SecureRemote user from this device. If you have used SecureRemote from the device previously, you can skip to step **11**.

- SecureConnect is a VPN based solution – meaning **additional software** must be installed on the PC in order to connect. If you are not the owner of this computer or do not have the correct permissions, you will need to use the goRemote remote access solution instead.

- Because of the variety of computers with different operating systems that can be used for remote access, it is not possible to detail **every possible prompt that you can receive** when installing the software. However, it is important to know that you will be prompted *in some way* to install the Juniper Software. This will be absolutely necessary to connect using SecureConnect.

Here are some examples of alerts and messages you may encounter when connecting for the first time:

8. Active X Message:

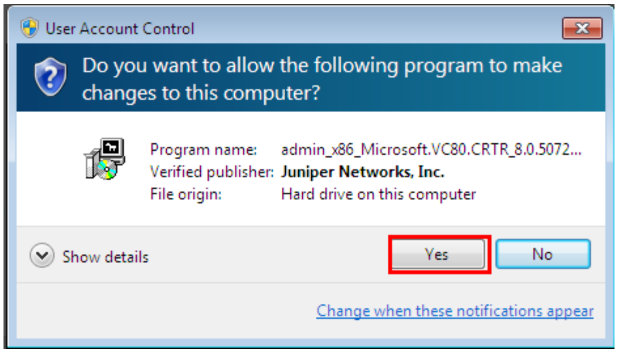

Download Setup Client - Windows Internet Explorer
https://208.69.135.25/dana-na/setup/download.cgi?r=https%3A//208.69.135.25/dana/nc/ncrun.cgi%3Flaunch_nc%3D1%26re
Favorites
Suggested Sites
Download Setup Client
Download File...
What's the Risk?
Information Bar Help
Carolinas HealthCare Sy

To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...

In order to continue the operation you need to install a setup client. Please click here to install setup package. You must enable either ActiveX or Java to run the downloaded setup client.

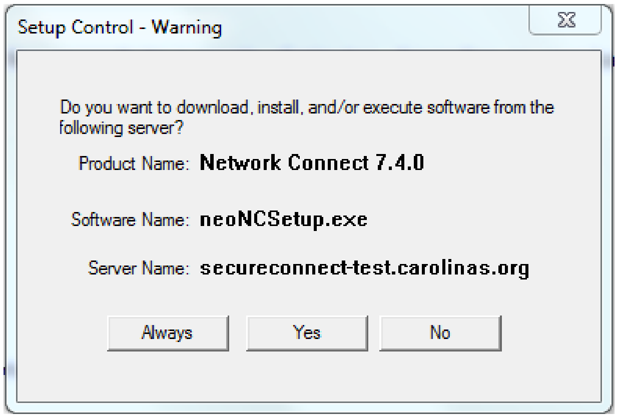
Once the setup client is installed, please click here to continue.

9. Internet Explorer Message:



Do you want to allow the following program to make changes to this computer?

Program name: admin_x86_Microsoft.VC80.CRTR_8.0.5072...
Verified publisher: **Juniper Networks, Inc.**
File origin: Hard drive on this computer



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

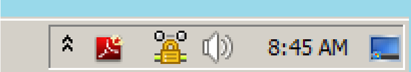
Product Name: **Network Connect 7.4.0**

Software Name: **neoNCSetup.exe**

Server Name: **secureconnect-test.carolinas.org**

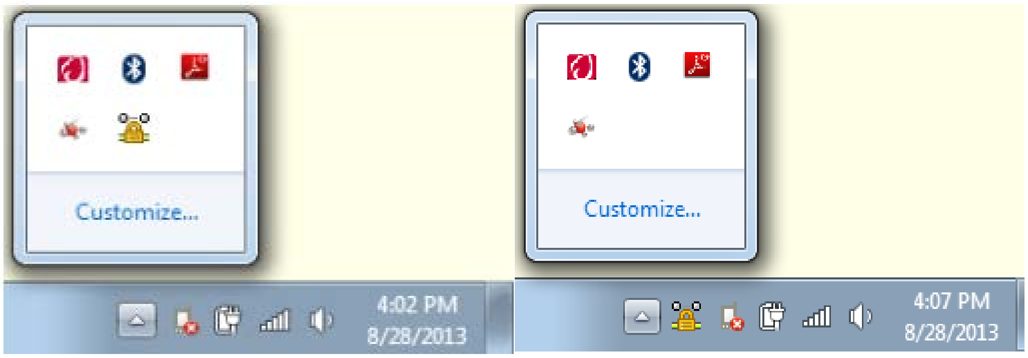
10. **IMPORTANT:** These steps are required in order to access SecureConnect from the PC you are on. You will need to click “YES”, “Allow”, and “Always Trust” from most computers to allow the software to install.

11. Once the install is complete, you will be directed to your WebApps log in for convenience. (This WebApps launch page will not work with Mac Safari users). They will need to point a browser to webapps.carolinas.org, due to Safari browser restrictions. You can ensure your install is complete and that you are connected by looking for the “gold lock” as shown in the image below.



12. This **“gold lock”** symbol is of **utmost importance** to this connection type.

    If you have the “gold lock,” this indicates that you are connected. If you do not see the “gold lock,” this does not necessarily mean you are not connected. (Depending on your operating system the “gold lock” can be hidden from view as shown in the image below).



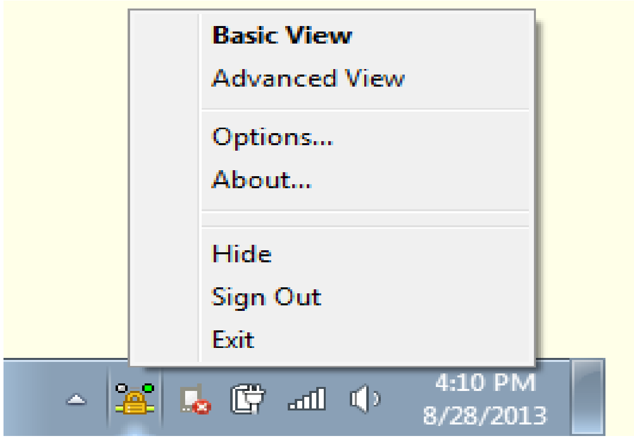
13. We recommend that you click and drag the “gold lock” icon out of this notification area, and down beside the up-arrow where it is show above.

14. This will allow you to always see the “gold lock” to know when you are “connected,” and most importantly, to remind you of the step necessary to properly “log out.” **(Step 17)**

15. If you are connected with the “gold lock” as shown above, you are now able to use the “WebApps” page that auto-launched, or you can close it if you do not need it during this session.

16. Ultimately, when the “gold lock” shows as “connected,” you are allowed to access nearly any network resource you normally would during the course of your business day when on the CHS network. For example, you will have access to internal websites such as *PeopleConnect* and *PhysicianConnect* through your local browser windows, email through local Outlook instead of through Citrix WebApps, the Microsoft Lync client, as well as many other network resources.

17. The SecureConnect “gold lock” session will last for 10 hours. If you disconnect without logging off of this session, it will be suspended until you either re-authenticate or will time-out automatically after 10 hours from when you first connected for the day. When you are done for the day or are going to exceed your 10 hour session limit, **it is very important to “Sign Out.”** The easiest way to do this is to “right click” on the “gold lock” and then to choose “sign out” to properly terminate the session.



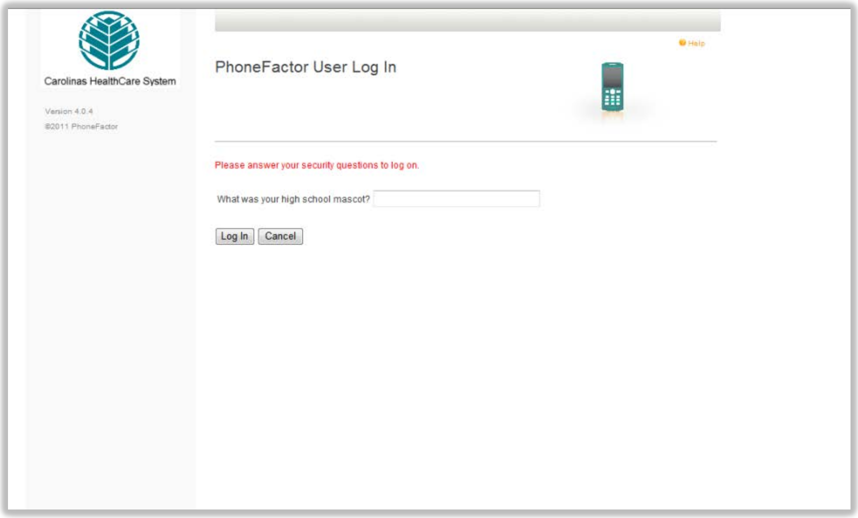
18. If you sign out in this manner, you will be gracefully logged out of the SecureConnect system and will be ending your session on the network in the correct way. If you do not, you will find when you attempt to access SecureConnect at a later time (you will receive a “Page cannot be displayed” or similar error message from your browser). This is due to security controls that are placed on the VPN sessions as to not allow hackers to take control of these disconnected sessions. If you find yourself in this situation, please see **Section 4: Troubleshooting SecureConnect.**

19. If you have properly **signed out** of the session, the next time you are ready to access SecureConnect, the log in page will successfully open on your PC and you will be able to connect to SecureConnect without issue. If you are having any problem with the SecureConnect page not opening, please refer to **Section 4**.

Section 3. Logging into SecureConnect.carolinas.org without phone access

1. You can return to the goRemote portal page at any time to change/update your registered phone numbers or change your security questions. Your Security Questions can be utilized to access goRemote and the goRemote portal, but not with other remote access products, including SecureConnect, Webmail, or via mobile devices with Citrix Receiver.

2. If you are attempting to log in to the portal and you do not have your phone, you will be presented with one of your four registered security questions to complete your authentication in the browser window.



Carolinas HealthCare System

Version 4.0.4

©2011 PhoneFactor

Help

PhoneFactor User Log In

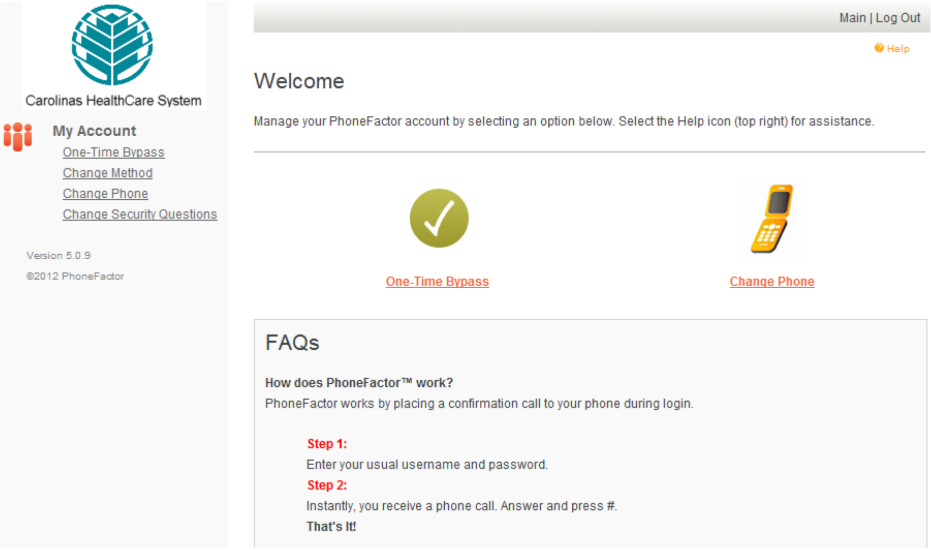
Please answer your security questions to log on.

What was your high school mascot?

Log In | Cancel

3. **Answer the security question and click "Log In."** *NOTE: Answers are not case sensitive.*

4. After clicking **"Log In"**, the login process will continue, and you will be logged into the portal that contains your registered information. You have the option of updating the phone information you have previously registered now in the "**My Account**" area, or using a **"One Time Bypass".**



Carolinas HealthCare System

My Account

- One-Time Bypass
- Change Method
- Change Phone
- Change Security Questions

Version 5.0.9

©2012 PhoneFactor

Main | Log Out

Help

Welcome

Manage your PhoneFactor account by selecting an option below. Select the Help icon (top right) for assistance.

One-Time Bypass

Change Phone

FAQs

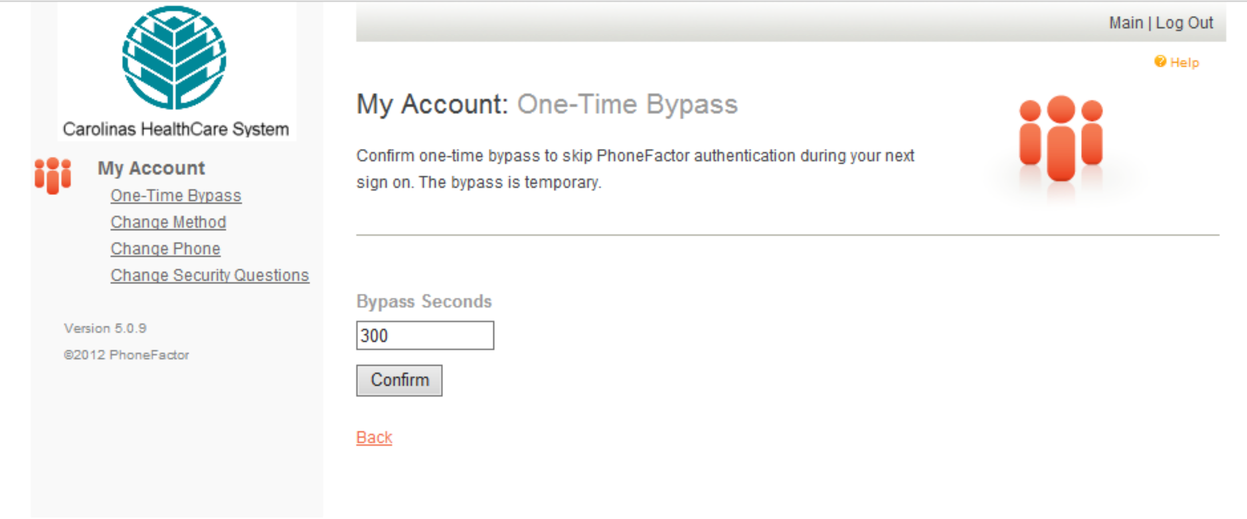
How does PhoneFactor™ work?

PhoneFactor works by placing a confirmation call to your phone during login.

Step 1:
Enter your usual username and password.
Step 2:
Instantly, you receive a phone call. Answer and press #.
That's It!

Section 3.1 Logging into the SecureConnect with a “One Time Bypass”

1. Click the **“One Time Bypass”** option on the goRemote Portal page, and you will be presented with the page below.

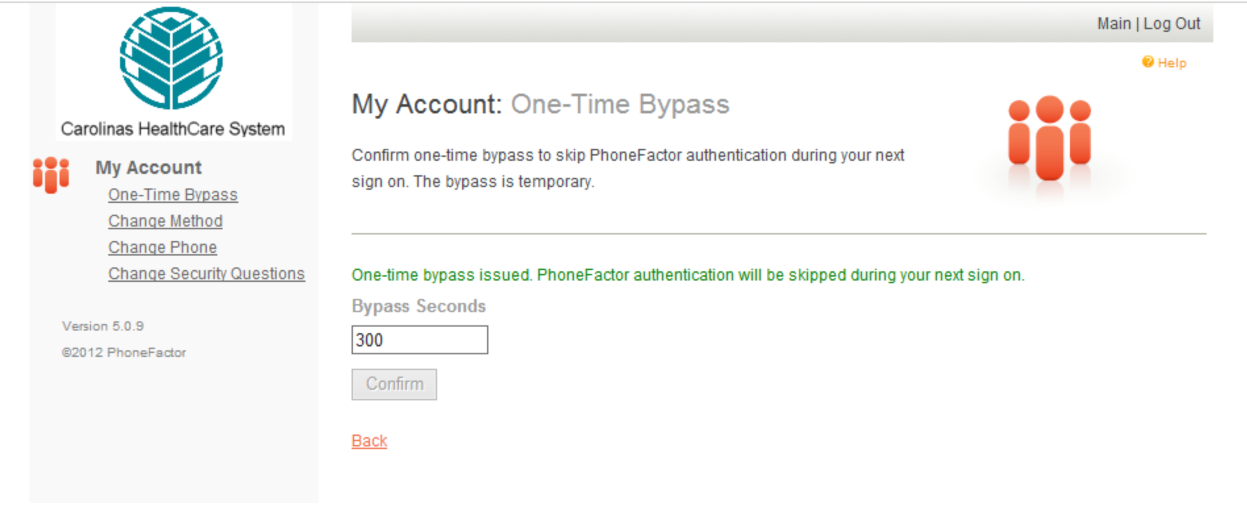


My Account: One-Time Bypass

Confirm one-time bypass to skip PhoneFactor authentication during your next sign on. The bypass is temporary.

Bypass Seconds: 300

2. Click **“Confirm” –** Pressing this will give you **“300 seconds or 5 Minutes”** to log in to SecureConnect **without a phone call.**



My Account: One-Time Bypass

Confirm one-time bypass to skip PhoneFactor authentication during your next sign on. The bypass is temporary.

One-time bypass issued. PhoneFactor authentication will be skipped during your next sign on.

Bypass Seconds: 300

3. Return to the SecureConnect login page:

4. **Enter** your **username and password** and click **“Sign In.”**

5. You will then have direct access without a phone call.

Section 4 Troubleshooting SecureConnect – Login/Logout

1. Eventually, anyone may encounter situations where their PC is having a problem connecting to SecureConnect. The reason, more often than not, stems from software issues with your PC or from the installed VPN client on the PC being logged off improperly.

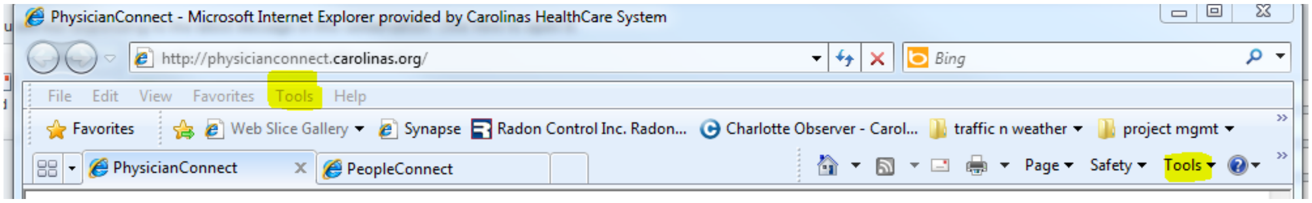
    - Failure to log off properly can cause security controls to be placed on the session when logging back in. This causes the server which you are attempting to connect to reject your session.

    - When this occurs, you will notice that instead of loading the SecureConnect login page, the browser returns a "Page cannot be displayed" or similar message.

2. If this occurs, please confirm that you are actually connected to the Internet by changing the URL in the address bar of your browser to another website, such as: http://www.google.com. If you are still receiving "Page cannot be displayed" or similar message after attempting other sites, this likely indicates that you either do not have Internet access in your current location, or that you may need to check the wireless signal or network cable you are using to connect to the Internet.

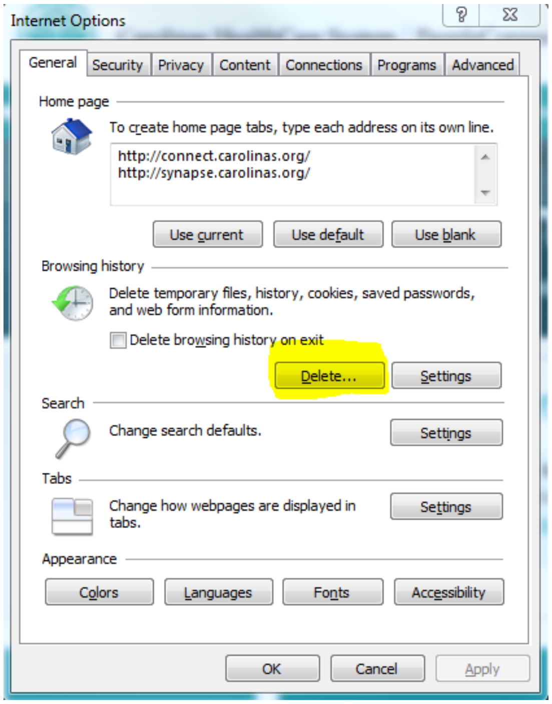
3. If you are able to open another website but not SecureConnect, the most common issue would arise from improper logout. This occurs from not choosing to **"Sign Out"** of the VPN Client or "**gold lock**" as detailed in **Section 2.17.** However, this can also be caused by unintentional reasons as well, such as the loss of Internet connection, a laptop going into suspend/sleep/power-save mode, power loss to PC, power loss to the modem, closing the laptop cover to transport it, or even weather-related events. These types of unexpected reasons for disconnection may make it impossible to use the **"Sign Out"** option out correctly. Regardless of the reason, the following steps show how to resolve a problem where your Internet connection is up (you can get to Google or other websites), but attempting to open SecureConnect gives a "Page cannot be displayed" or similar error.

4. In Internet Explorer, you will need to "Delete Browsing History." This process is sometimes referred to as "clearing cache and cookies." Navigate to this setting by clicking on either of the "Tools" menus in Internet Explorer. (highlighted in yellow below)


PhysicianConnect - Microsoft Internet Explorer provided by Carolinas HealthCare System
http://physicianconnect.carolinas.org/
Bing
File
Edit
View
Favorites
Tools
Help
Favorites
Web Slice Gallery
Synapse
Radon Control Inc. Radon...
Charlotte Observer - Carol...
traffic n weather
project mgmt
PhysicianConnect
PeopleConnect
Page
Safety
Tools

5. Next, choose "Internet Options."

6. The page below will be displayed. You will need to click on the **"Delete"** button. (highlighted in yellow below)



To create home page tabs, type each address on its own line.

http://connect.carolinas.org/
http://synapse.carolinas.org/

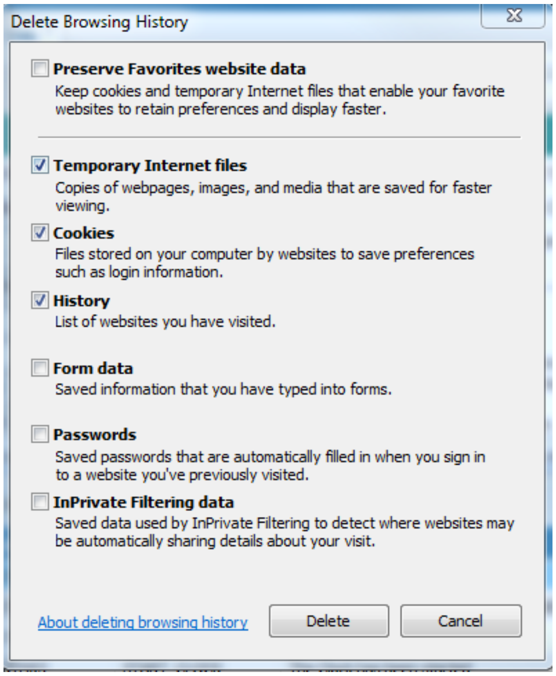
Delete temporary files, history, cookies, saved passwords, and web form information.

☐ Delete browsing history on exit

Change search defaults.

Change how webpages are displayed in tabs.

7. Next, the following screen will displayed.



☐ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

☑ **History**
List of websites you have visited.

☐ **Form data**
Saved information that you have typed into forms.

☐ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

☐ **InPrivate Filtering data**
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.

8. In Internet Explorer version 7 and higher, **you must uncheck** the "Preserve Favorites website data" when deleting the history for the SecureConnect cleanup to occur properly.

9. Click the **"Delete"** button and then wait for the items to delete.

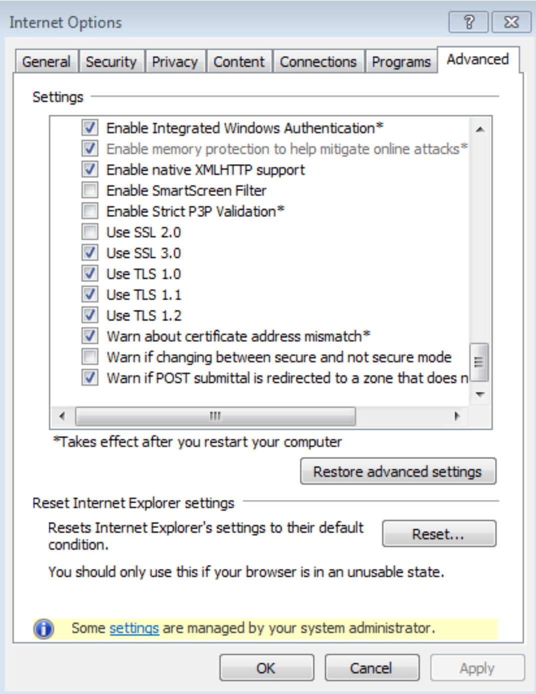
10. Close and reopen the browser. After logging in to SecureConnect, you may be directed to a page that prompts you to reconnect to your existing session. On this page, click on the option to "continue the session."

Section 4.1 Troubleshooting SecureConnect – TLS Browser Setting

1. Due to Payment Card Industry (PCI) regulations and general security controls, CHS has adopted the best practice of requiring end-user browser to support Transport Layer Security (TLS).

2. You can check the Internet options in Internet Explorer to ensure that TLS 1.0 is enabled. If this is not enabled in the browser, you will likely receive the "Page cannot be displayed" or similar error instead of the SecureConnect login screen.

3. To check for TLS:
   a. Open Internet Explorer.
   b. Navigate to this setting by clicking on either of the "Tools" menus in Internet Explorer.
   c. Next, choose "Internet Options"
   d. Click on the "Advanced" tab
   e. Scroll to the bottom of the window and ensure that "Use TLS 1.0" is checked. (see screen shot below)
   f. Click "Apply," and then "OK."



☑ Enable Integrated Windows Authentication*
☑ Enable memory protection to help mitigate online attacks*
☑ Enable native XMLHTTP support
□ Enable SmartScreen Filter
□ Enable Strict P3P Validation*
□ Use SSL 2.0
☑ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
□ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Some settings are managed by your system administrator.

4. Close and reopen the browser, then attempt to open the SecureConnect URL again.

If these steps do not help you successfully log in using CHS remote access, please contact the Information Services Support Center at 704-446-6161.