Trinity Connect Portal Guide

Developed by Benjamin Carrigan, Trinity Health Information Services

Overview

The Trinity Connect Portal is the webpage utilized for remote VPN access and/or remote access to Epic/EpicCare Link.

If you are familiar with the Trinity Connect Portal you can access this page from our SJCloud webpage or by clicking here or from the following URL: https://connect.trinity-health.org/

Instructions for logging into the connect portal can be found in the last portion of this guide.

For further support please visit https://www.trinity-health.org/helpmeconnect or contact the helpdesk at 315-448-5607 and advise the technician to "reference KB0080758 SY - Using The Trinity Connect Portal"

Remote support can be obtained at the time of your call by going to: http://fastsupport.com
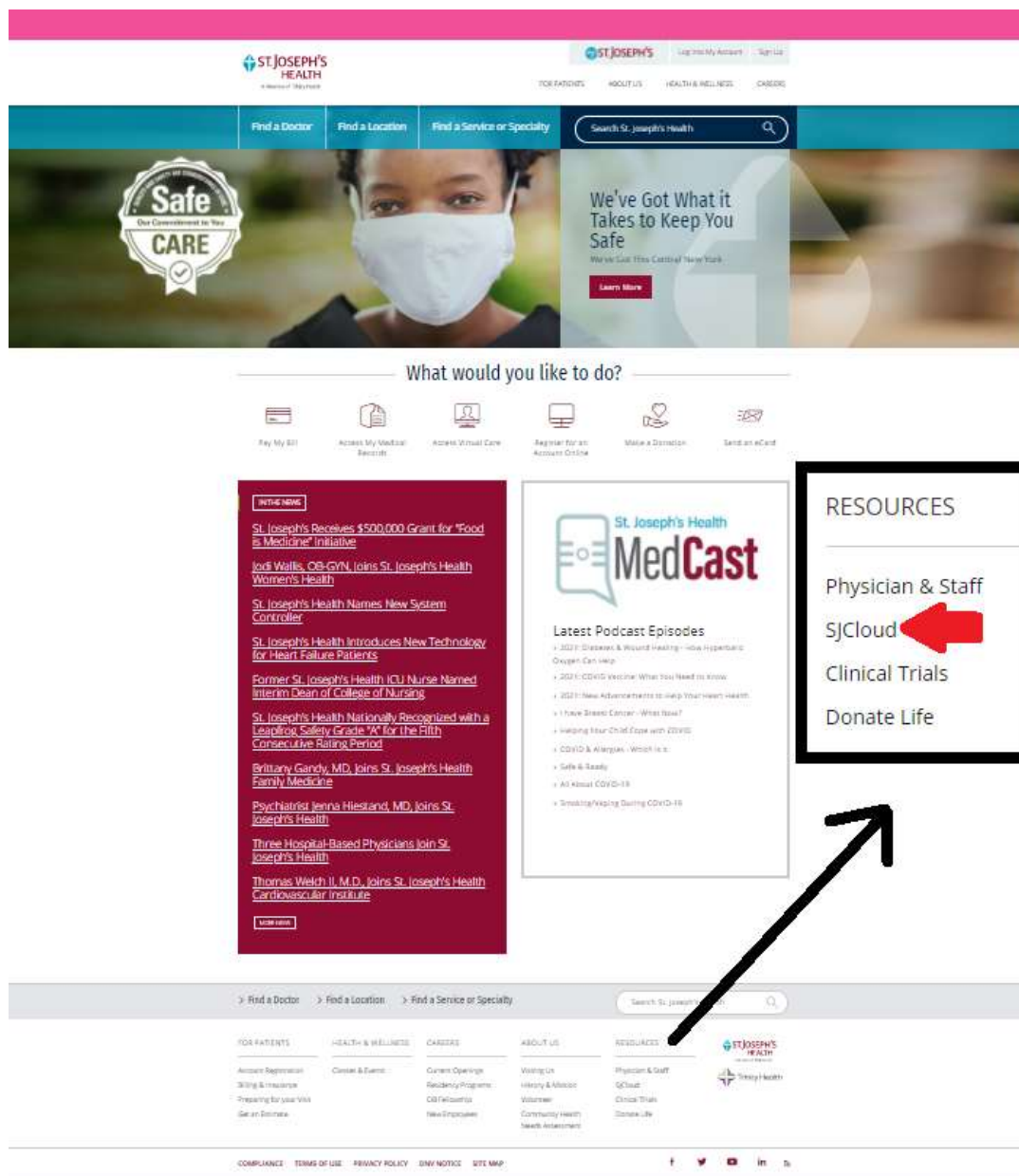
Table of Contents

SJCloud

This guide will reference the SJCloud webpage in several places.

To reach this page go to www.sjhsyr.org and navigate to our SJCloud page by scrolling to the bottom of the webpage and clicking on SJCloud underneath the resources menu on the bottom right of the page.

Bookmark or memorize the location of this page, you will need this for future reference.

Setting up Your Trinity Health Network Account / Getting Started

Verify your Network Username and Password are valid.

    a) Go to the [Trinity Password Self Service Page](#) from SJCloud.

    b) Login on the presented login screen with your network username and password.

If your login successfully brings you to the main menu your username and password are valid. If your login is rejected contact the helpdesk for assistance at 315-448-5607.

Your username and password will be used every time you login to the Trinity Connect Portal.

Verify you have a valid Microsoft Account / UPN.

    a) If you are an employee of St. Josephs and/or Trinity Health your UPN will be your email address. *Example: Benjamin.carrigan@sjhsyr.org*

    b) If you are a non-employee your UPN will typically be [firstname.lastname@sjhsyr.org](#) or [firstname.lastname@trinity-health.org](#) . . *Example: Benjamin.carrigan@sjhsyr.org*

Your UPN is what you will need to register for Multifactor Authentication (MFA)

To confirm your UPN contact the helpdesk for assistance at 315-448-5607.

Multifactor Authentication (MFA)

Like other applications you may be familiar with such as your bank, an additional multi-factor security method called Multifactor Authentication (MFA) is required in order to login to the Trinity Connect Portal every time you login.

Multi Factor Authentication (MFA) can be setup as either a **phone call** to your phone *or* by using the **Microsoft Authenticator app** which can be installed on your smart phone. You will only need to setup one of these two methods to meet the security requirement.

As a requirement for other apps supported by Trinity Health such as Workday or Outlook Mobile Multifactor Authentication (MFA) may already be setup. If MFA is already setup it does not need to be setup an additional time for the Trinity Connect Portal.

To setup MFA:
1) Go to the MFA Administration webpage from SJCloud, or by navigating directly to https://aka.ms/mfasetup

2) Sign in using your SJH Email / UPN and Trinity network password.
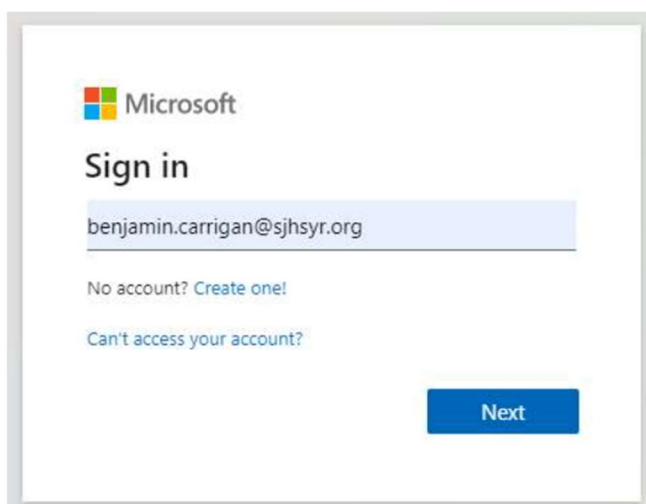
3) If you are prompted to stay signed in on a shared PC, click No.

4) On the more information required screen click Next.

5) You will have the choice to setup MFA as a phone call that occurs each time you login to trinity-connect (Method #1) or as an application on your phone that will be used to approve each sign on every time you login (Method #2).
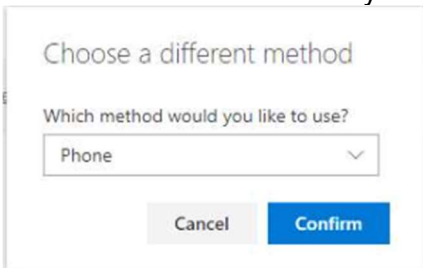
   Choose if you wish to set up MFA as a phone call or use an app on your phone. Follow the below instructions based on this choice.
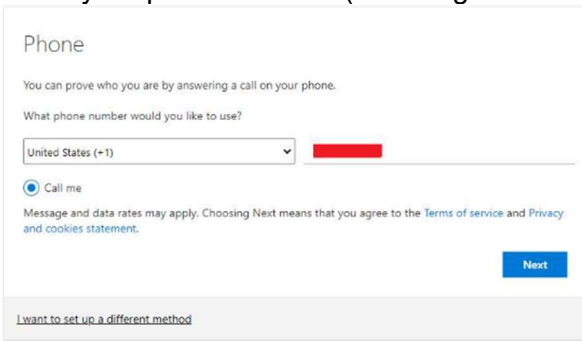
Method #1 Phone Call

   a) Click on the small text below I want to set up a different method.
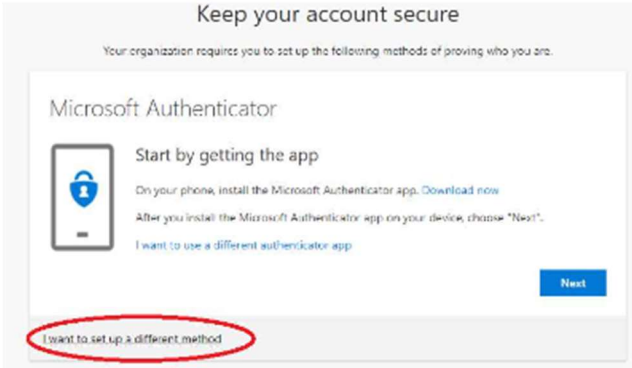
   b) When asked which method you would like to use select Phone then click Confirm.

   c) Enter your phone number (including area code) and click the Next button.

d) Within moments you will receive a phone call from a 855 number, answer the phone call on your phone and press the # key when prompted to very your sign in.

e) When finished click Next then click Done. This will complete the MFA setup and your web browser on your PC may be closed.

Method #2 Microsoft Authenticator (app)

a) Click on the Next button. The click on the Next button again. A QR code will appear on your PC screen, leave this up on your screen for now.
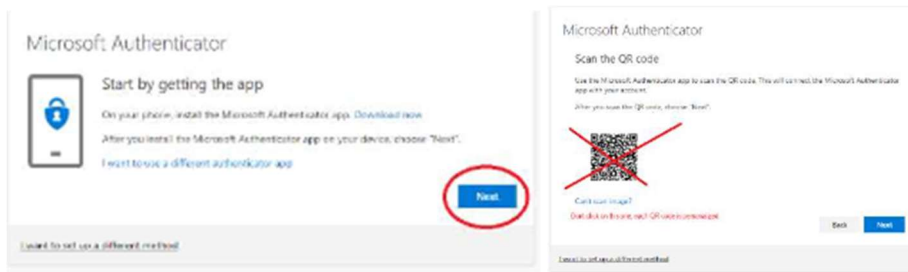
b) Install the Microsoft Authenticator app on your phone from the google play store or the apple app store. When finished open the Microsoft Authenticator app on your phone. You may be asked to agree to terms and conditions upon opening the app.

c) When prompted click Scan a QR. You will be asked to allow camera access and allow notifications allow both.

d) Using your phone scan, the QR code the is currently displayed on your PC.

e) Click the next screen and it will ask you to test this. Click the Next button on your PC and when prompted click the approve button on your phone.
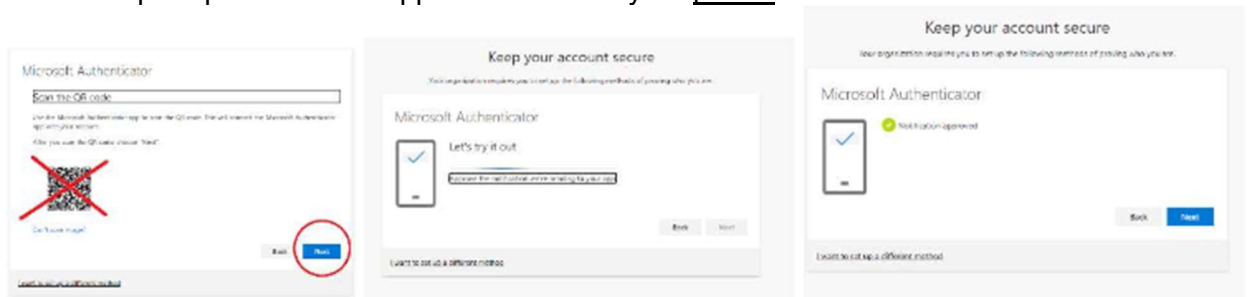
f) When finished click the done button. This will complete the MFA setup and your web browser on your PC may be closed.

Installing Citrix Workspace, NSG, and NSEE

Citrix Workspace
This is the software used to open citrix based applications on the Trinity Connect Portal. If you have been issued a loaner or work from home device by information services then your PC will already include this software. If not Citrix Workspace can be downloaded by:

a) Navigate to receiver.citrix.com from SJCloud using your PCs web browser. You will be redirected to a download link which corresponds to your type of device and be asked to install citrix workspace.

b) Download the latest copy of citrix workspace for your device and install it. Note if your company has restrictions placed on your PC your IT administrator may need to assist you with this.

c) When finished if you are asked to add an account do not add an account.

NetScaler Gateway (NSG)
This is the software used to establish a remote connection to St. Josephs / Trinity Health when using the Trinity Connect Portal. If you have been issued a loaner or work from home device by information services then your PC will already include this software.

If not you will be prompted to install this software the first time you attempt to utilize the Trinity Connect Portal. This file may also be obtained from the SJCloud page. Note if your company has restrictions placed on your PC your IT administrator may need to assist you with this.


NetScaler Endpoint Analysis (NSG)
This is the software used to analyze your device to ensure it meets the requirements to utilize the Trinity Connect Portal. If you have been issued a loaner or work from home PC by information services then your PC will already include this software.

If not you will be prompted to install this software the first time you attempt to utilize the Trinity Connect Portal. This file may also be obtained from the SJCloud page. Note if your company has restrictions placed on your PC your IT administrator may need to assist you with this.

Using the Trinity Connect Portal (Windows)

Note this section is intended for PC's running windows. If using a non windows machine please refer to the other sections of this guide.

1) Navigate to the Trinity Connect Portal login page. This can be accessed via SJCloud or directly by navigating to: https://connect.trinity-health.org/

    a) If this is your first time you may be prompted to install the NetScaler Endpoint Encryption and NetScaler Gateway software. To install this click download then click run / open. Then click Next then click Install.

    b) During your first several connections your PC will ask for permissions. When presented with a popup from the NetScaler Gateway:
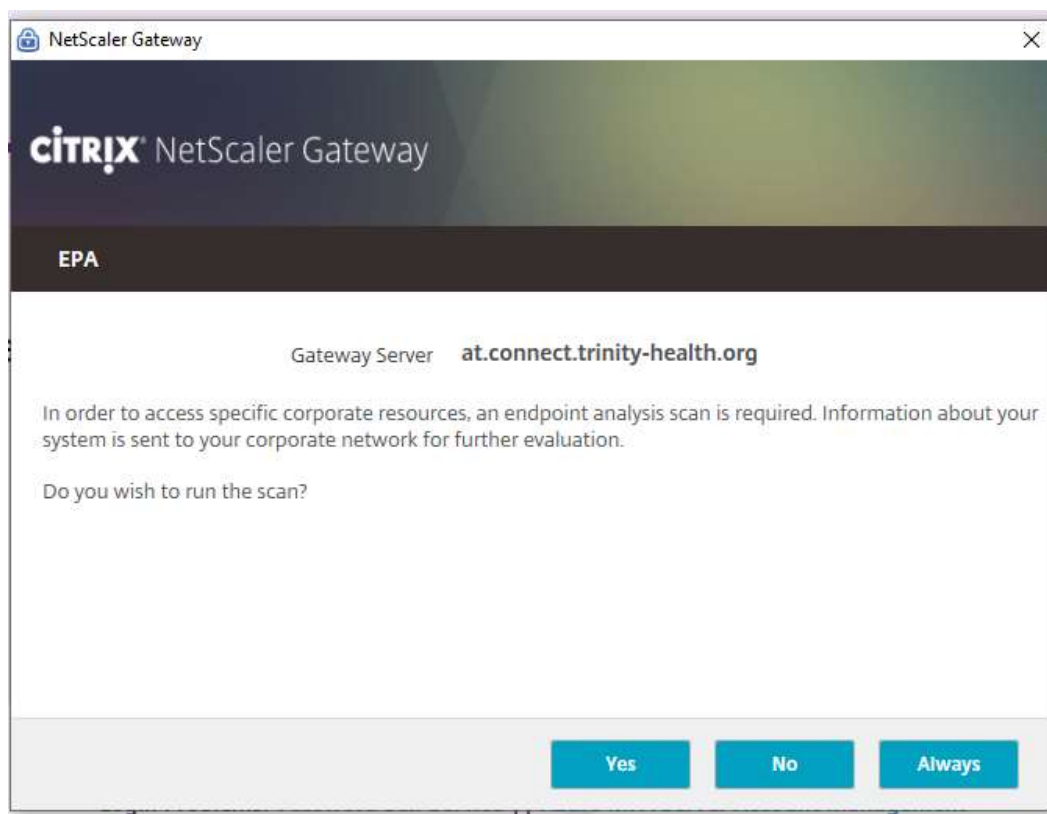
    c) Click **Always** then on the window that appears click **Always allow…** then click **Open**
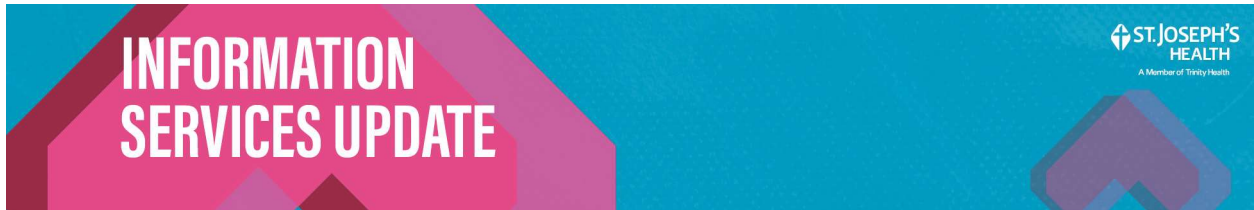
2) Login using your network username and password and select a domain of **Syracuse** then click Login
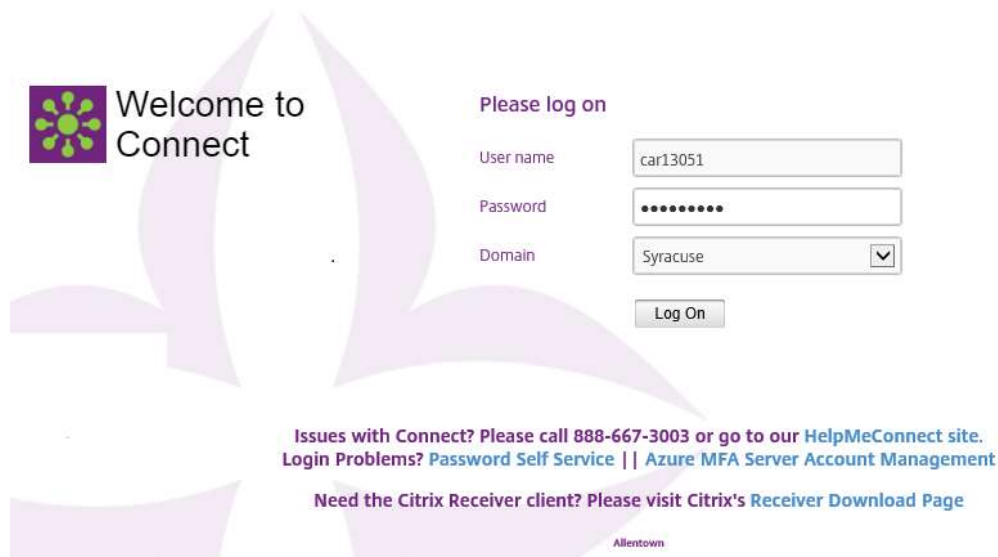
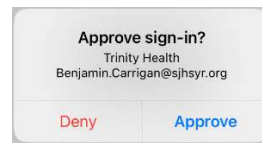*Upon clicking login, it will appear as if nothing has happened.*

3) Authenticate with your chosen method of Multifactor Authentication (MFA).

You will then either receive a phone call (Method #1) or a notification from the Microsoft Authenticator Mobile App (Method #2). Authenticate based on how you set up your additional security method.

Call from 1-855-###-####   Or

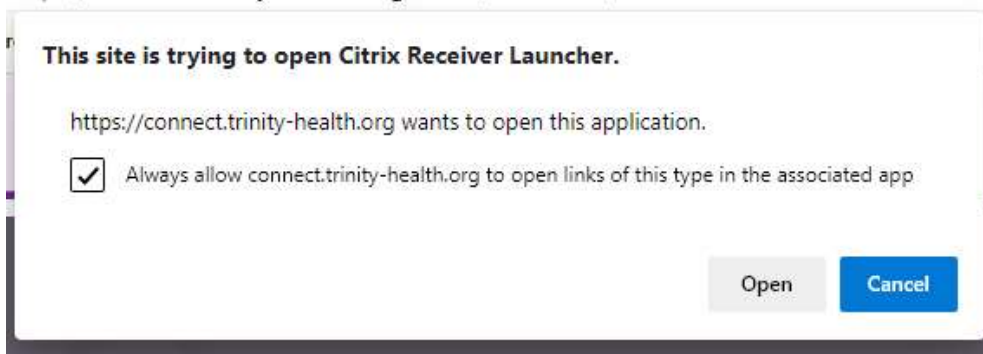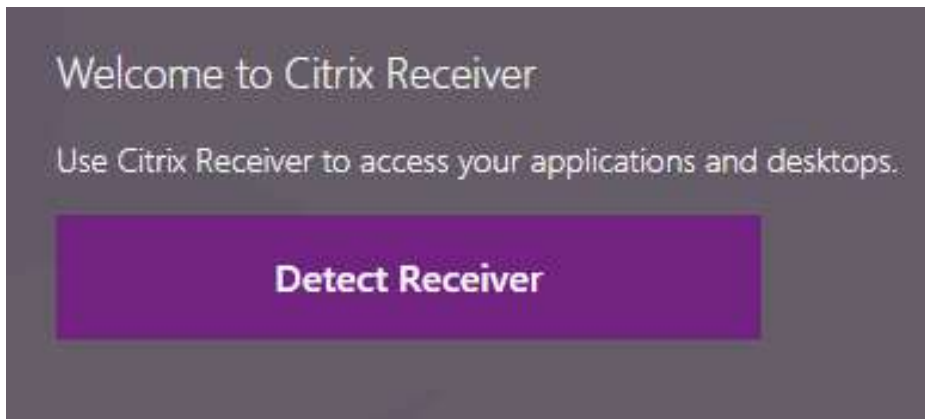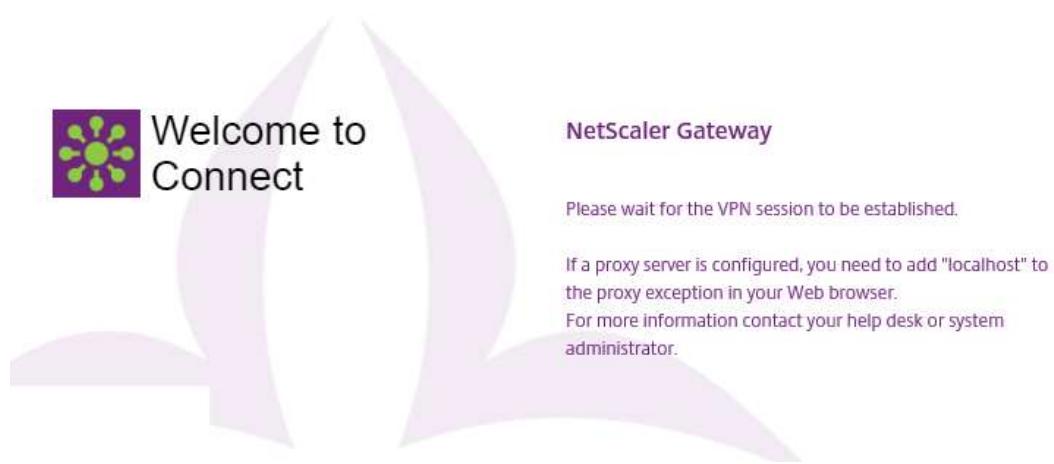   Method #1   Method #2

If you do not do this your PC will remain on this screen and after two minutes you will need to start over by closing your browser and returning to the trinity connect page.

4) If prompted click **Detect Receiver** then check the box to **Always allow…** then click **open**.

Welcome to Citrix Receiver

Use Citrix Receiver to access your applications and desktops.

Detect Receiver

This site is trying to open Citrix Receiver Launcher.

https://connect.trinity-health.org wants to open this application.

☑ Always allow connect.trinity-health.org to open links of this type in the associated app

Open   Cancel

5) The following page will display for several seconds then move to the next page. No action is required. If the page does not move to the next page, reboot your PC.

Welcome to Connect

NetScaler Gateway

Please wait for the VPN session to be established.

If a proxy server is configured, you need to add "localhost" to the proxy exception in your Web browser.
For more information contact your help desk or system administrator.

6) You will then be taken to the Citrix Gateway and be connected to the Trinity Connect Portal. You will see a list of applications available to you.
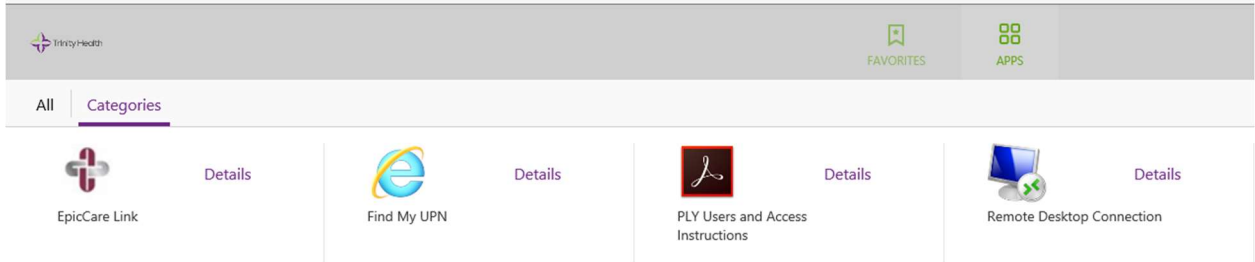
Note the apps shown in this document are not the same applications that will be available to you.

7) You are on the Trinity Connect Portal and may utilize it for up to 12 hours before your connection will time out and you will have to reconnect.

If you are utilizing the Trinity Connect Portal from a loaner or work from home device issued by information services you my minimize your Trinity Connect Portal window and continue working on that PC as if it were connected at one of our locations.

To launch an application, click on it, a small loading bar will appear and the application will load.

If you are missing the Remote Desktop Connection application contact the helpdesk at 315-448-5607 so they may submit a request to the SY-Security team to provide you with this application.

If you are an employee and are missing any other application from your list have your manager submit a Security Access Request (SAR) on your behalf requesting the missing application.

If you are a non-employee and are missing any other application from your list contact your SJH representative or have your manager contact your SJH representative so they may submit a Security Access Request (SAR) on your behalf requesting the missing application.

Using the Trinity Connect Portal (MAC)

Note this section is intended for PC's running MAC OS. If using a non MAC OS machine please refer to the other sections of this guide.
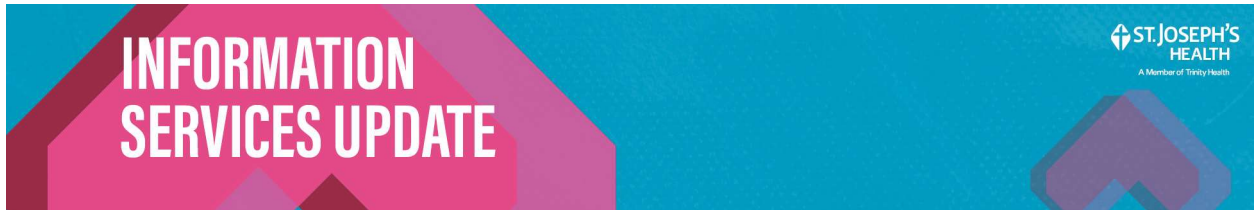
1) Update your current operating system to MAC OS Big Sur. Failure to do so may result in a failed connection attempt or incapability with the Trinity Connect Portal.

   To update your OS:

   a) Click the Apple Icon on the top left of your apple menu
   b) Click system information, a new window will open.
   c) Click Update, a new window will open. This window will tell you your current OS and present you with the option to update your OS if an update is available.

2) Navigate to the MAC Specific Trinity Connect Portal login page. This can be accessed via SJCloud or directly by navigating to: https://macs.connect.trinity-health.org/

   a) If this is your first time you may be prompted to install the NetScaler Endpoint Encryption and NetScaler Gateway software. To install this click download then click run / open. Then click Next then click Install.

   b) During your first several connections your PC will ask for permissions. When presented with a popup from the NetScaler Gateway:

   c) Click Always then on the window that appears click Always allow… then click Open

3) Login using your network username and password and select a domain of Syracuse then click Login

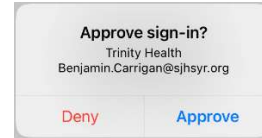***Upon clicking login, it will appear as if nothing has happened.***

4) Authenticate with your chosen method of Multifactor Authentication (MFA).

You will then either receive a phone call (Method #1) or a notification from the Microsoft Authenticator Mobile App (Method #2). Authenticate based on how you set up your additional security method.

Approve sign-in?
Trinity Health
Benjamin.Carrigan@sjhsyr.org

Deny   Approve

Call from 1-855-###-####   Or

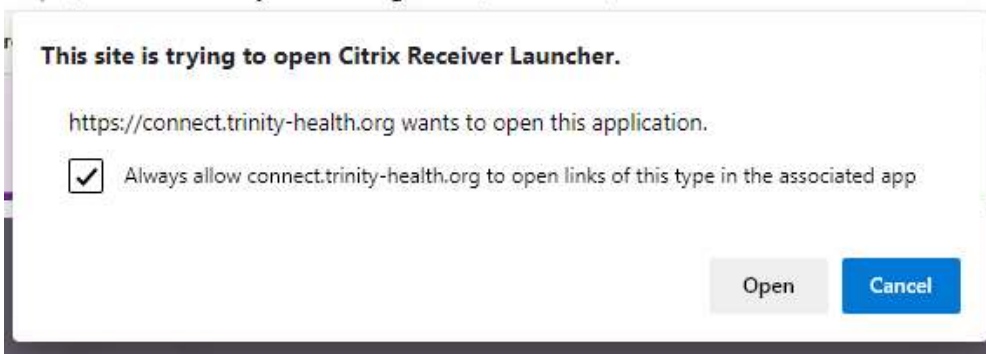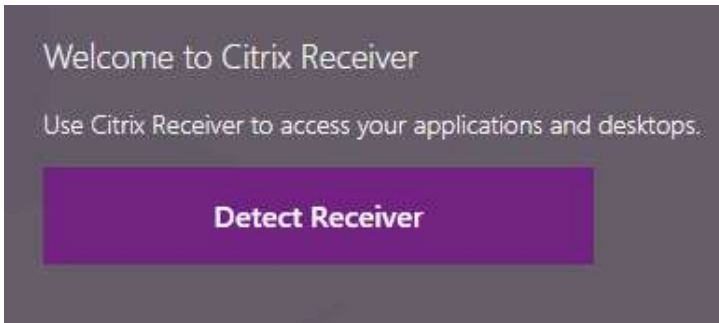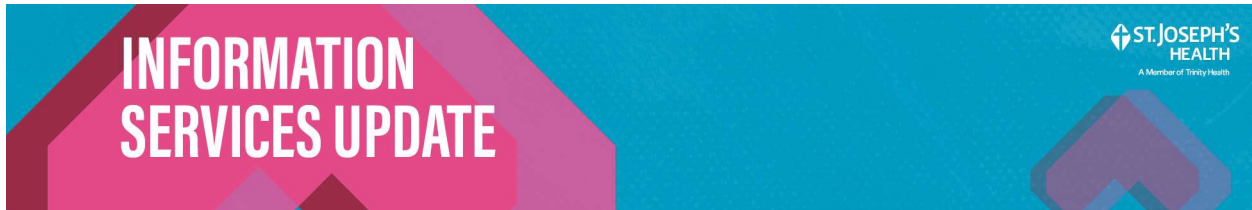Method #1   Method #2

__If you do not do this your PC will remain on this screen and after two minutes you will need to start over by closing your browser and returning to the trinity connect page.__

5) If prompted click **Detect Receiver** then check the box to **Always allow…** then click **open**.

Welcome to Citrix Receiver

Use Citrix Receiver to access your applications and desktops.

Detect Receiver

This site is trying to open Citrix Receiver Launcher.

https://connect.trinity-health.org wants to open this application.

☑ Always allow connect.trinity-health.org to open links of this type in the associated app

Open   Cancel

6) You will then be taken to the Citrix Gateway and be connected to the Trinity Connect Portal. You will see a list of applications available to you.
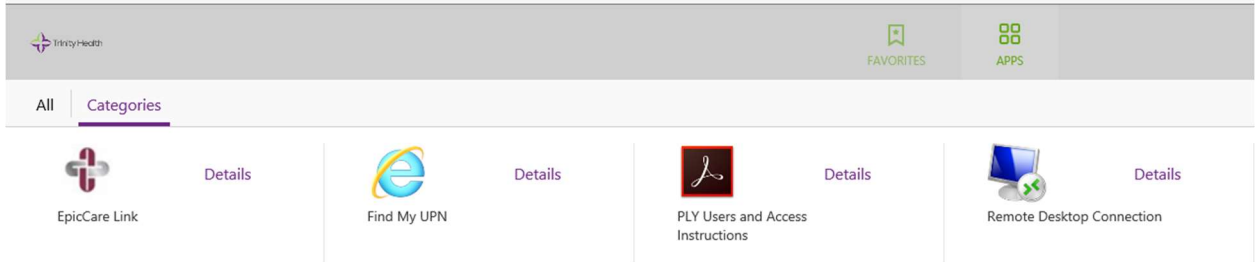
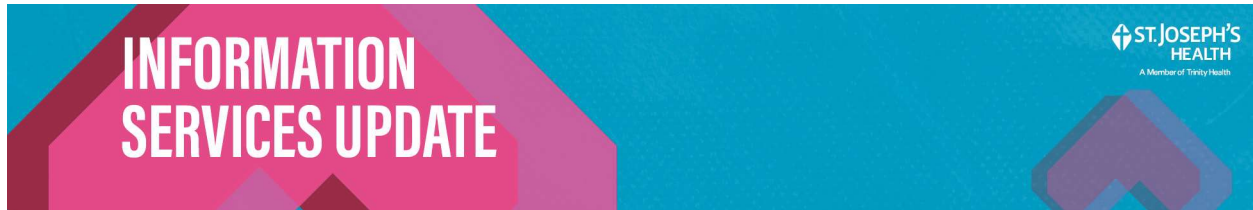***Note the apps shown in this document are not the same applications that will be available to you.***

7) You are on the Trinity Connect Portal and may utilize it for up to 12 hours before your connection will time out and you will have to reconnect.

To launch an application, click on it, a small loading bar will appear and the application will load.

If you are missing the Remote Desktop Connection application contact the helpdesk at 315-448-5607 so they may submit a request to the SY-Security team to provide you with this application.

If you are an employee and are missing any other application from your list have your manager submit a Security Access Request (SAR) on your behalf requesting the missing application.

If you are a non-employee and are missing any other application from your list contact your SJH representative or have your manager contact your SJH representative so they may submit a Security Access Request (SAR) on your behalf requesting the missing application.

Using the Trinity Connect Portal (Android / IOS)

Note this section is intended for Phones and Tablets. If you are not using a phone or tablet please refer to the other sections of this guide.

It should also be noted this method of remote access is not as user friendly as other methods and will require an advanced understanding of navigating a phone or tablet to utilize.

1) Download Citrix Workspace from the Google Playstore or the Apple Appstore.

2) Launch Citrix Workspace, when prompted tap **Get Started**

3) You will be asked to enter an email address or store list, when prompted enter:
   https://syrreceiver.connect.trinity-health.org

4) Tap **Continue**

5) Enter your Trinity Network Username and Password then tap **Sign In**.

6) Authenticate with your chosen method of Multifactor Authentication (MFA).

   You will then either receive a phone call (Method #1) or a notification from the Microsoft Authenticator Mobile App (Method #2). Authenticate based on how you set up your additional security method.

Call from 1-855-###-####   Or
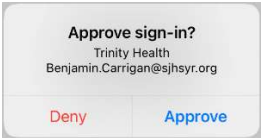
Method #1   Method #2

If you do not do this your device will remain on this screen and after two minutes you will need to start over by closing the app and reopening it.

7) You will be taken to the Citrix Gateway, and presented with your favorited applications. By default no applications will be favorited.

   To launch an application, click on it, a small loading bar will appear and the application will load.

If you are missing the Remote Desktop Connection application contact the helpdesk at 315-448-5607 so they may submit a request to the SY-Security team to provide you with this application.

If you are an employee and are missing any other application from your list have your manager submit a Security Access Request (SAR) on your behalf requesting the missing application.

If you are a non-employee and are missing any other application from your list contact your SJH representative or have your manager contact your SJH representative so they may submit a Security Access Request (SAR) on your behalf requesting the missing application.