

Employee Remote Access User Guide

Table of Contents

1.	Overview	1
2.	Using Employee Remote Access	1
2.1	Using Remote Basic Access	2
2.2	Using Remote Clinical Access with a Physical Key Fob	3
2.3	Using Remote Clinical Access with Authenticator App for Soft Token Access	5
3.	Citrix Download	6
3.1	Download and Install	6
4.	Download an Authenticator App for Soft Token Access	9

1. Overview

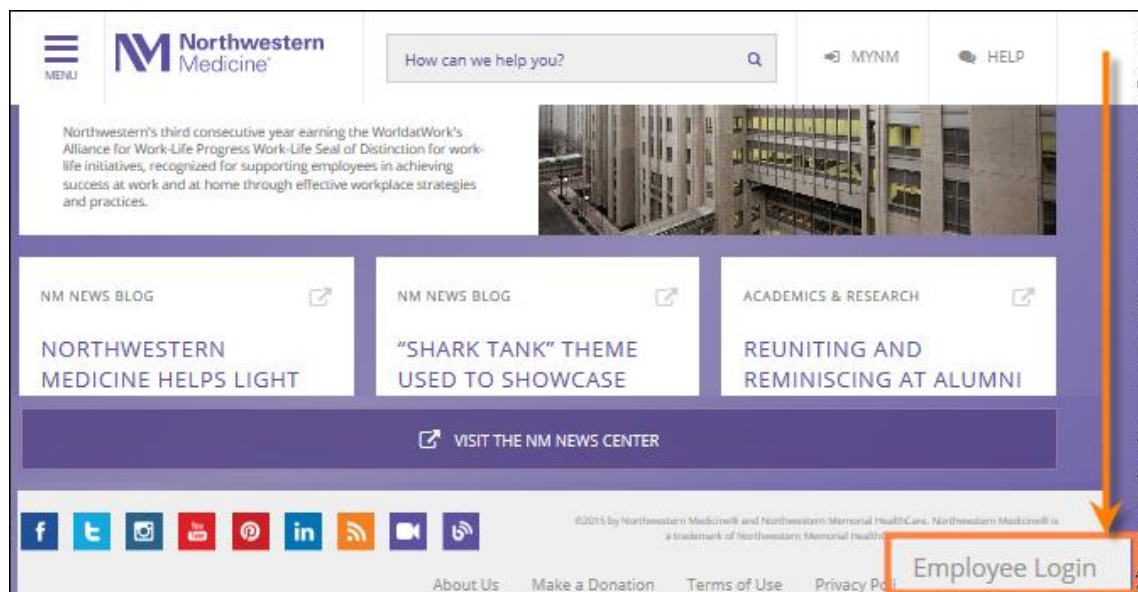
You can access NM Interactive (NMI) from your home using NMHC Employee Remote Access. The applications you can access will depend on your designated access level: **Remote Basic Access** or **Remote Clinical Access**. To use Employee Remote Access your remote computer must have DSL or Broadband Internet Access. Application speed depends on the speed of your internet connection. Some applications require a Citrix plug-in to run properly.

Remote Basic Access provides access to non-clinical and other business-restricted applications. Policies, My NMI, and department pages can be accessed through a second login to NMI Interactive. All NMH employees and physicians are automatically granted access to the Basic Access Level.

Remote Clinical Access provides access to clinical applications as well as business-restricted applications. The login requires additional authentication with the PIN and 6-digit code from the RSA Secure ID (Key fob).

2. Using Employee Remote Access

1. If you are away from the office, you can access NM resources by clicking the **Employee login** link at the bottom of the Northwestern Memorial Hospital commercial website: www.nm.org (below).



Employee Remote Access User Guide

Logging into Remote Basic Access (Continued)

2. Type your NMH username and password (the same username and password you use for NMH email or PowerChart).
3. Click **Logon** or press the enter key on your keyboard.

NMHC Remote Access
For assistance call 312.926.HELP (4357)

Username
jdoe

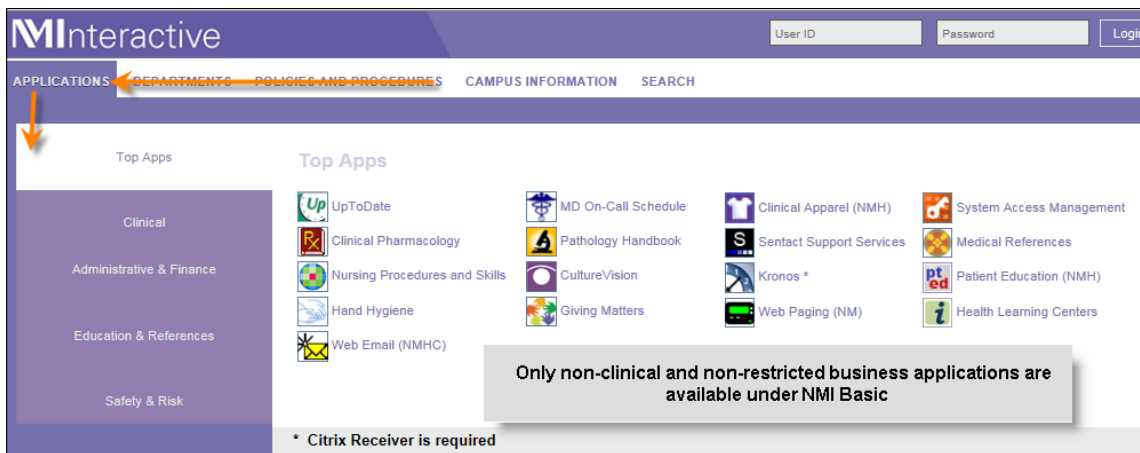
Password

Clinical Application Access
2-Factor Pin+Token (Optional)

Logon

2.1 Using Remote Basic Access

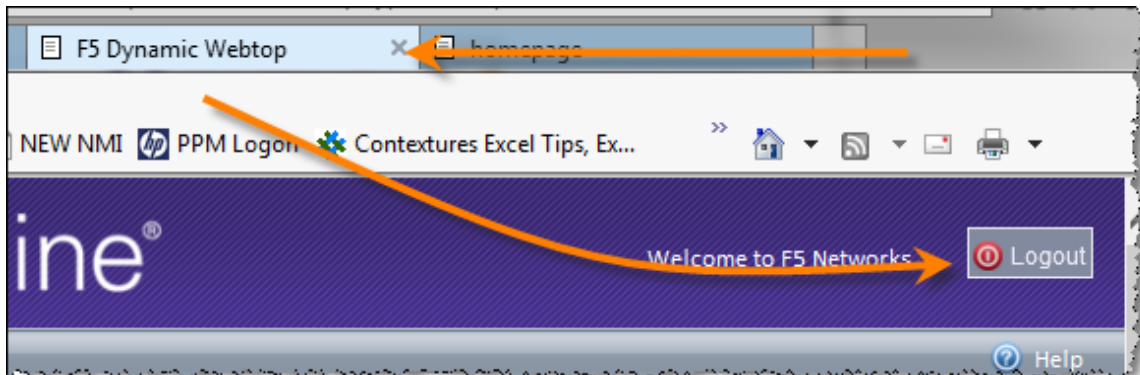
1. Once you login, NM Interactive launches in a new window.
 - Remote Basic Access allows you to access only non-clinical and business-restricted applications.
 - If you do not have an ID and password for a specific application, you will not be able to access the application.



Employee Remote Access User Guide

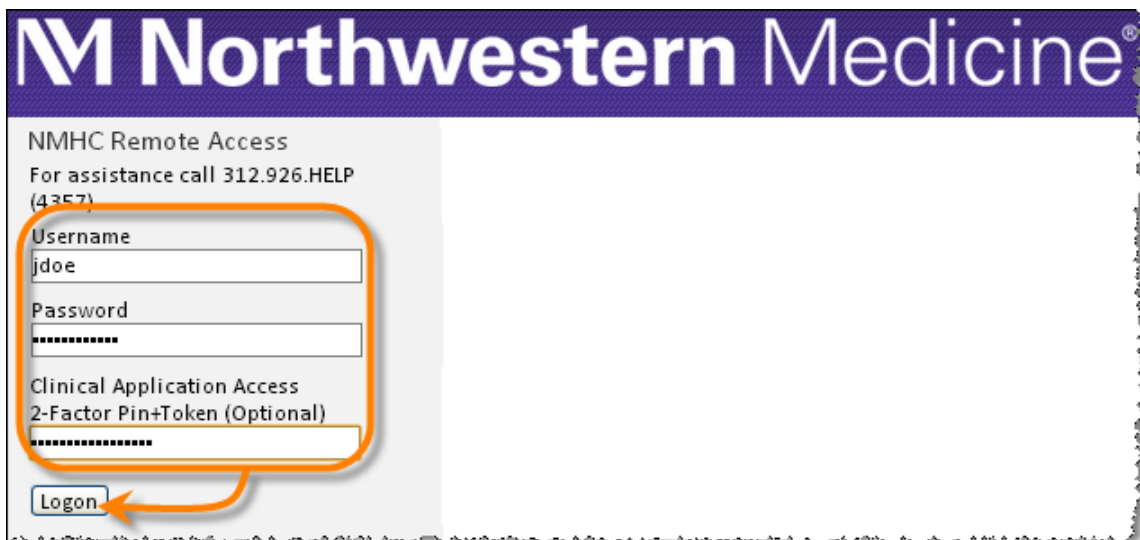
2.1.a Logging out of Remote Basic Access

Click the right-hand X to close the window or click the *F5 Dynamic Webtop* tab and click **Logout**.



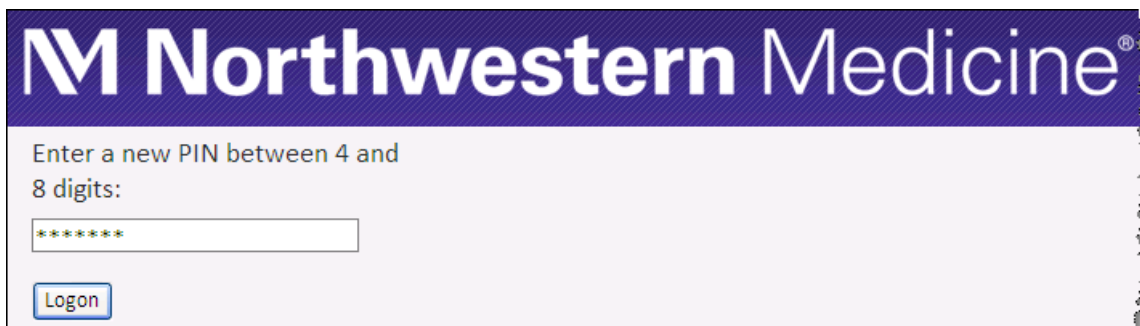
2.2 Using Remote Clinical Access with a Physical Key Fob

1. Type your NMH ID, password and your PIN+Token.
2. Click **Logon**.



2.2.a First-time Logon for Remote Clinical Access

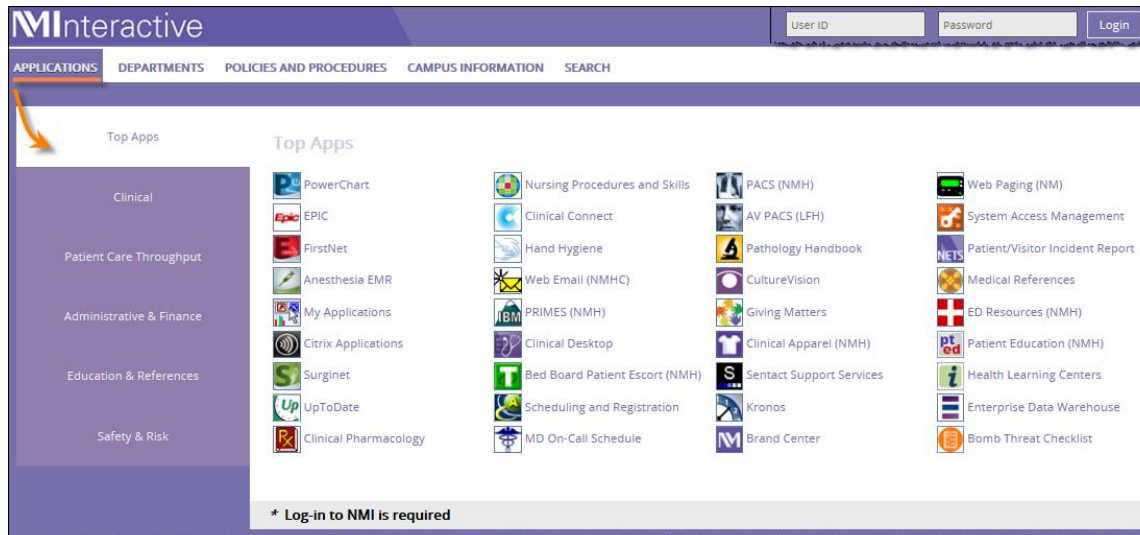
1. The first time you logon, you will be prompted to change your pin. Press the **Y** key on your keyboard to continue.
2. Type your new PIN and click **Logon**.



Employee Remote Access User Guide

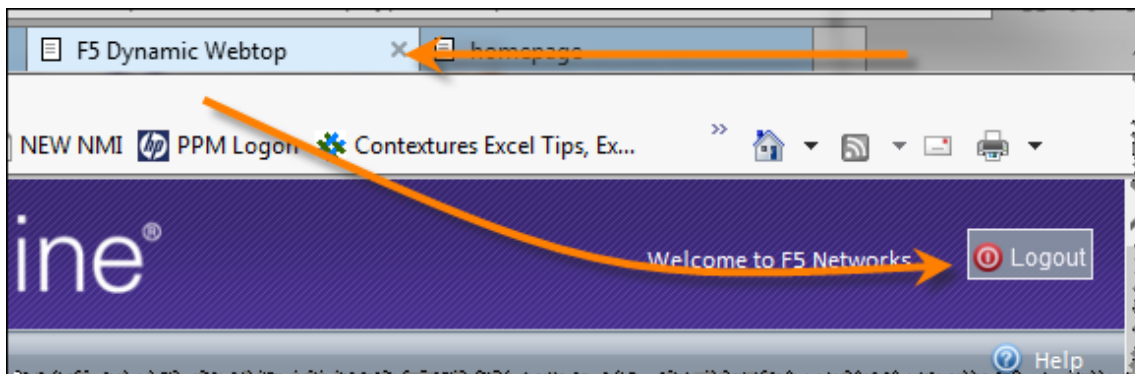
2.2.b Remote Clinical Access Applications

1. The NM Interactive page launches in a new window.
2. Click on any application tab and logon with your application ID and password. If you do not have an ID and password for a specific application, you will not be able to access the application.



2.2.c Logging Out of Clinical Remote Access

Click the right-hand X to close the window or click the *F5 Dynamic Webtop* tab and click **Logout**.

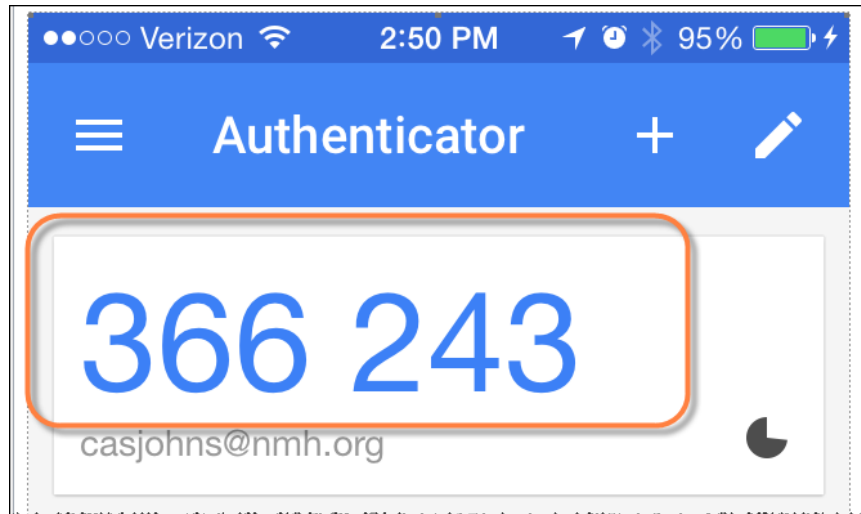


Employee Remote Access User Guide

2.3 Using Remote Clinical Access with Authenticator App for Soft Token Access

2.3.a Initial Setup

1. Before You Begin: [Download an Authenticator App for Soft Token Access](#) (page 9)
2. Scan the barcode you received in your welcome email.
3. Launch NM Employee Remote access (at nm.org).
4. Enter your username and password.
5. Open the Authenticator app you installed. The current time-based access code is displayed on your phone.



6. Enter that code in the Clinical Application Access.... field and click Logon.
NOTE: You do not need to use the PIN - just the code that displays on your phone.

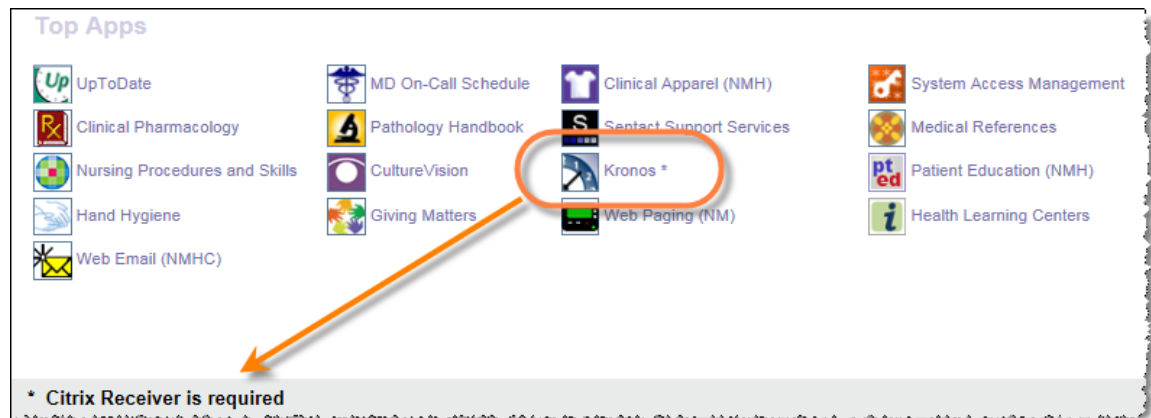


7. Remote Clinical Access will launch, click the NMI icon to continue.
8. Delete the email. The next time you logon into Remote Clinical Access, just the Authenticator on your phone.

Employee Remote Access User Guide

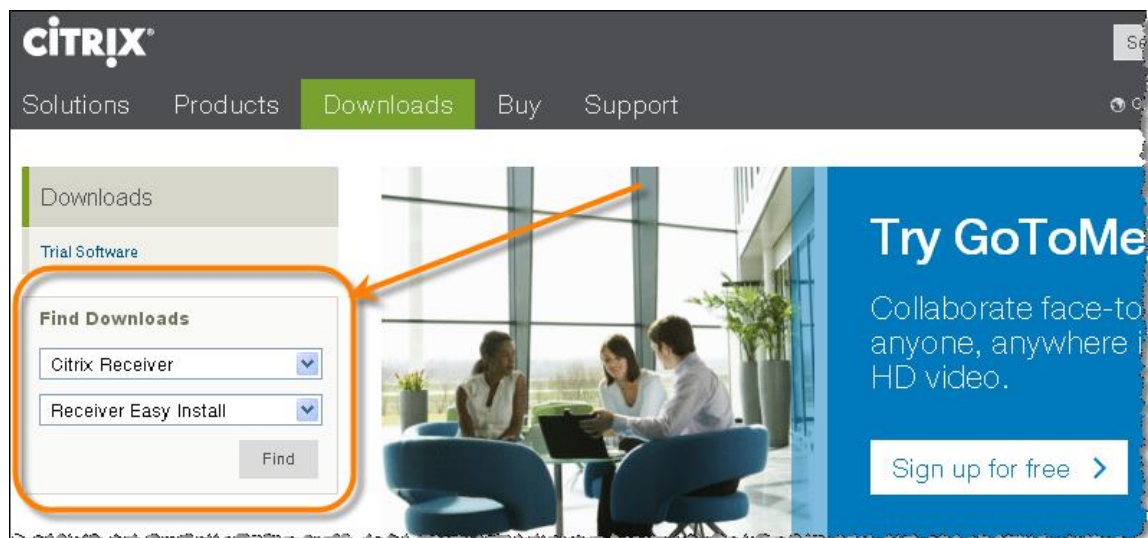
3. Citrix Download

Some applications require a Citrix plug-in to run remotely. These applications will have an asterisk symbol "*" by the icon. You will need to install Citrix manually to run these applications.



3.1 Download and Install

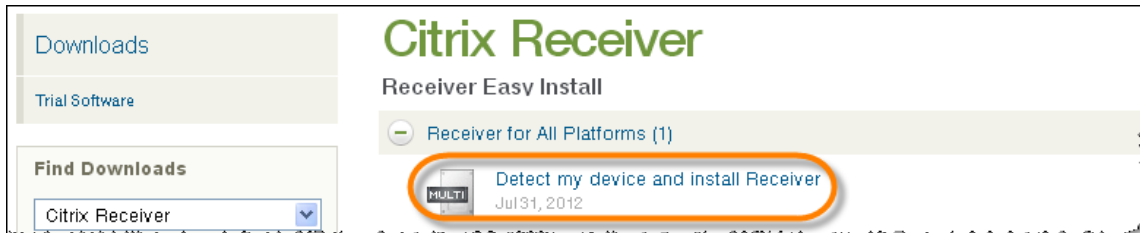
1. To download the most recent Citrix client, visit the Citrix download site at:
<http://www.citrix.com/downloads>
2. Under *Downloads*, select "**Citrix Receiver**" from the *Select Product* field and "**Receiver Easy Install**" from the *Select a Download type* field. Click **Find**.



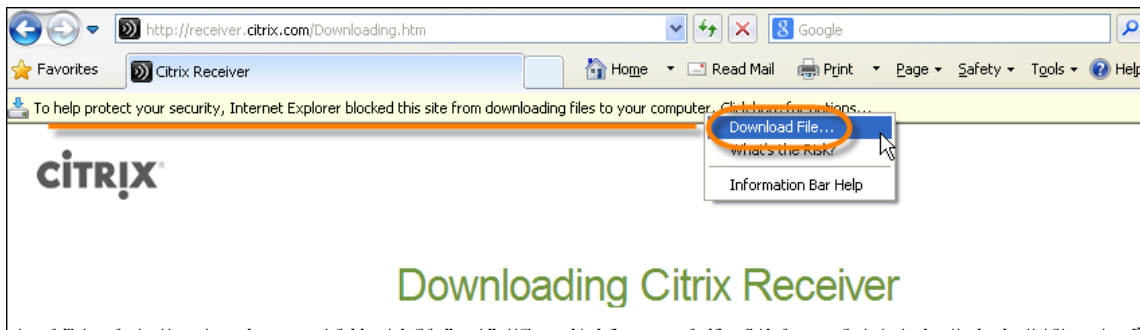
Employee Remote Access User Guide

Download and Install (Continued)

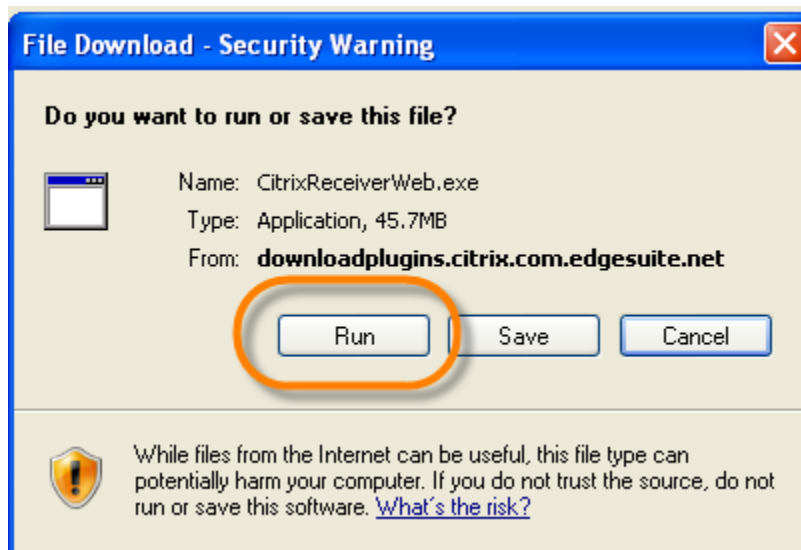
3. On the *Citrix Receiver* page, click **Detect my device and install Receiver**.



4. When prompted click **Download Receiver for...** button.
5. Checkmark **I agree to Terms...** to accept the licensing agreement. Click **Continue**.
6. If your security or popup blocker settings stop the download, allow the download to continue.



7. When prompted, click **Run**.



Employee Remote Access User Guide

Download and Install (Continued)

8. If you receive a second prompt, click **Run** again.
9. The *Citrix Receiver Setup* window launches, click **Install**.



10. The software will install.
11. After installation, launch Automatic Time Reporting or any other application that requires Citrix.

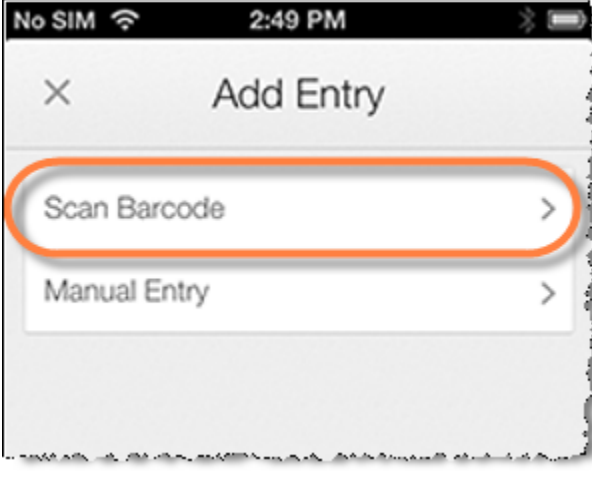
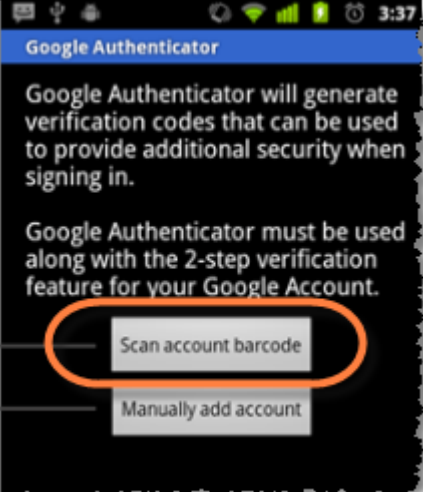
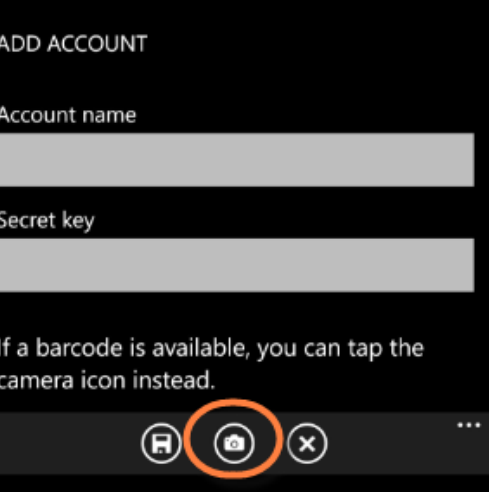
Employee Remote Access User Guide

4. Download an Authenticator App for Soft Token Access

Note: You must be approved and have your account configured for this access.

iPhone	Android	Windows Phone
Requirements To use Google Authenticator on your iPhone, iPod Touch, or iPad, you must have iOS 5.0 or later. In addition, in order to set up the app on your iPhone using a QR code, you must have a 3G model or later.	Requirements To use Google Authenticator on your Android device, it must be running Android version 2.1 or later.	Requirements Windows Phone devices must be version 7.5 or later.
Downloading the app <ol style="list-style-type: none"> 1. Visit the App Store. 2. Search for Google Authenticator. 3. Download and install the application. 	Downloading the app <ol style="list-style-type: none"> 1. Visit Google Play. 2. Search for Google Authenticator. 3. Download and install the application. 	Downloading the app <ol style="list-style-type: none"> 1. Visit the Store. 2. Search for Google Authenticator. 3. Download and install the application.
Setting up the app <ol style="list-style-type: none"> 1. On your phone, open the Google Authenticator application. 2. Tap the plus icon. 3. Tap Time Based. 4. To link your phone to your account Tap "Scan Barcode" and then point your camera at the QR code provided in this email. 	Setting up the app <ol style="list-style-type: none"> 1. On your phone, open the Google Authenticator application. 2. Click the Add an account button. 3. Select Scan account barcode and then point your camera at the QR code provided in this email. <p><i>Note: If the Authenticator app cannot locate a barcode scanner app on your phone, you might be prompted to download and install one</i></p>	Setting up the app <ol style="list-style-type: none"> 1. On your phone, open the Authenticator application. 2. Tap the plus icon 3. Tap the camera icon then point your camera at the QR code provided in this email.

Employee Remote Access User Guide

iPhone	Android	Windows Phone
 <p>The iPhone screen shows the 'Add Entry' interface. At the top, there is a close button (X) and the title 'Add Entry'. Below the title, there are two options: 'Scan Barcode' and 'Manual Entry', each with a right-pointing arrow. The 'Scan Barcode' option is highlighted with an orange oval.</p>	 <p>The Android screen shows the Google Authenticator app. At the top, there is a blue header with the text 'Google Authenticator'. Below the header, there is a paragraph of text: 'Google Authenticator will generate verification codes that can be used to provide additional security when signing in.' Below this text, there is another paragraph: 'Google Authenticator must be used along with the 2-step verification feature for your Google Account.' At the bottom, there are two buttons: 'Scan account barcode' and 'Manually add account'. The 'Scan account barcode' button is highlighted with an orange oval.</p>	 <p>The Windows Phone screen shows the 'ADD ACCOUNT' interface. At the top, there is a title 'ADD ACCOUNT'. Below the title, there are two input fields: 'Account name' and 'Secret key'. Below these fields, there is a paragraph of text: 'If a barcode is available, you can tap the camera icon instead.' At the bottom, there are three icons: a camera icon, a close button (X), and a more options button (three dots). The camera icon is highlighted with an orange oval.</p>