Guide – Cloud Services

Introduction

A customer who has purchased the McLeod System and has chosen to utilize McLeod Software Cloud Services to host their system will have numerous users who will need to establish access. This guide contains important information for users who need access to the system. The following processes are discussed within this guide:

- Accessing the McLeod Software Cloud Services Environment
- Installing & Using Palo Alto GlobalProtect VPN Client
- Self-Service Portal
- Overview – Password Policy
- Working with McLeod Applications in a Remote Environment

Users will need to access the system via Remote Desktop Services. Users will also gain access to a self-service portal, which provides options for passwords, security questions, and contact information. A policy has been set which enforces secure password generation and retrieval for all users. Finally, end-users who are transitioning to McLeod Cloud Services will need guidance in moving from a local application to a remote hosted application.

The appendices below reference general information & miscellaneous setup items:

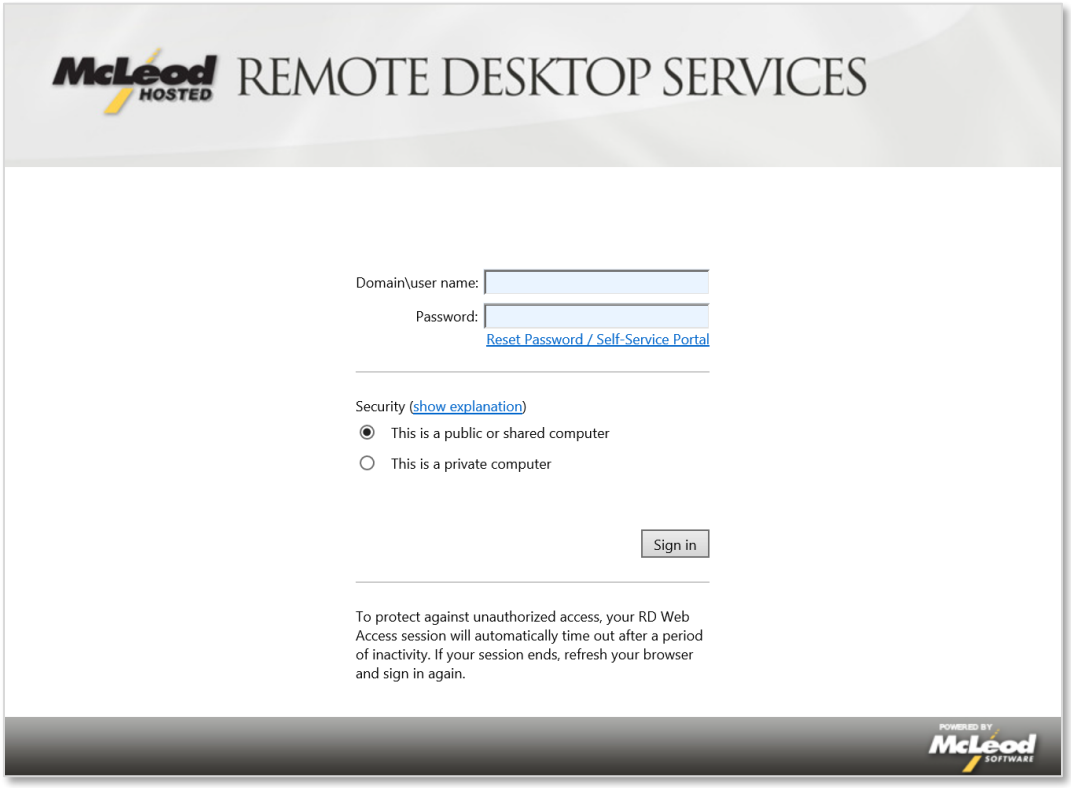
A. McLeod Software Cloud Services Login/User Management
B. How to Install and Use TSPrint Capability
C. Potential Conflicts with Screen Location and Remote Desktop Apps

Please review the sections below for the processes and policies related to onboarding to the McLeod System.

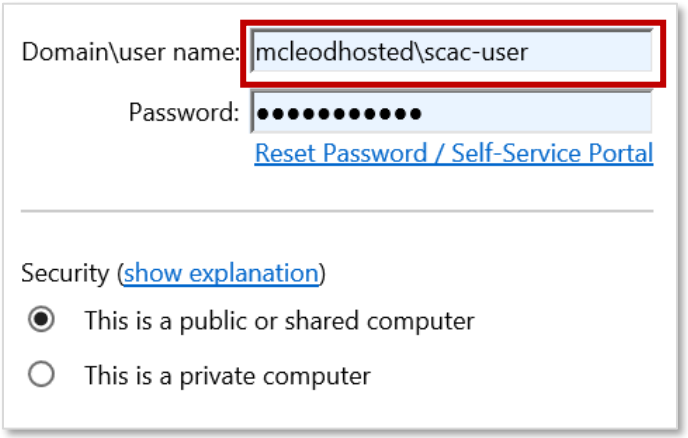
Process

Accessing the McLeod Software Cloud Services Environment

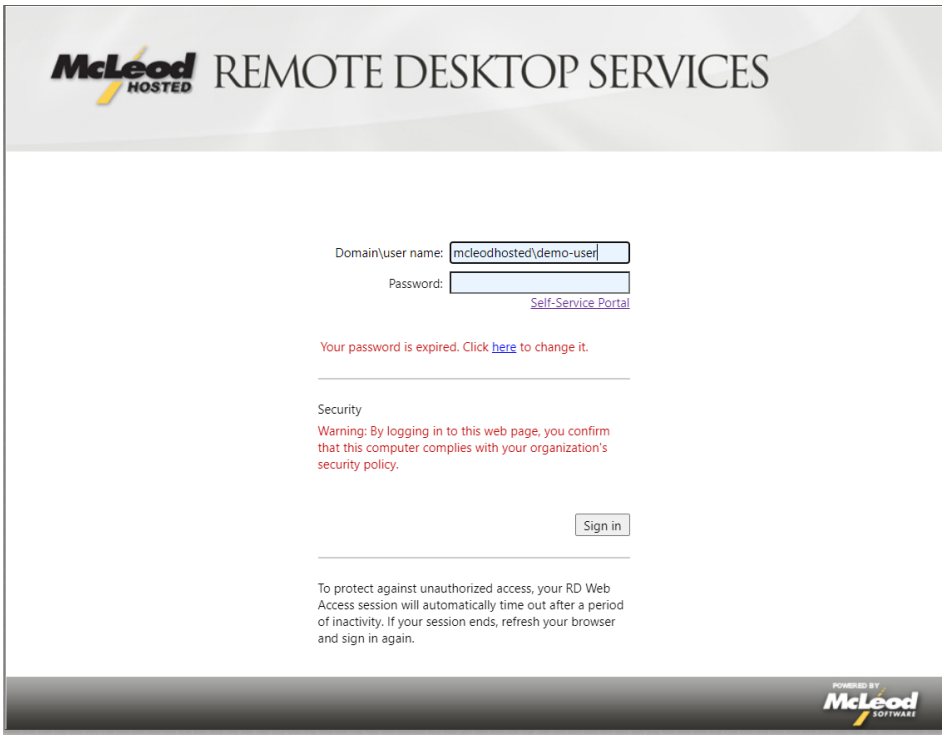
1. Go to https://ammf.mcleodhosted.com to access the McLeod application.



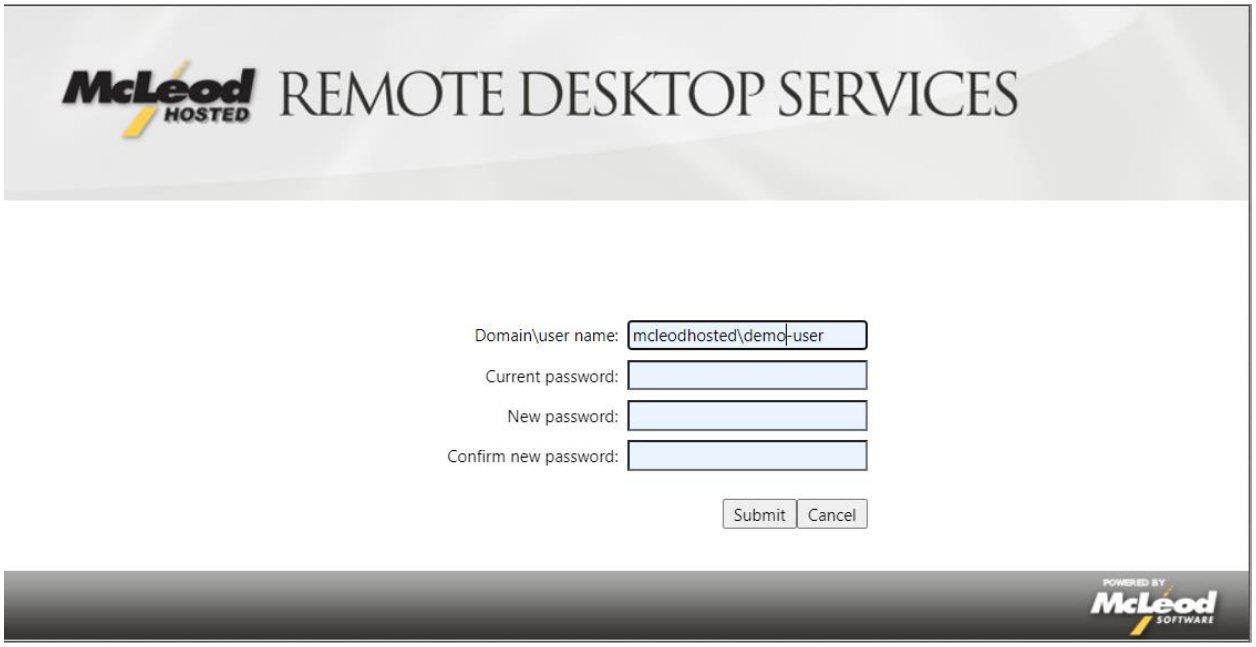
2. In the **Domain\user name** field, enter the appropriate username with "mcleodhosted\ammf-*****" and password.
   a. These credentials are provided to the key users in a separate spreadsheet.
   b. If this is the first time logging in, the user may be asked to reset the password depending on the setup.



3. As referenced in 2b, a first-time user or a user whose password was reset will see the screen below when logging in:

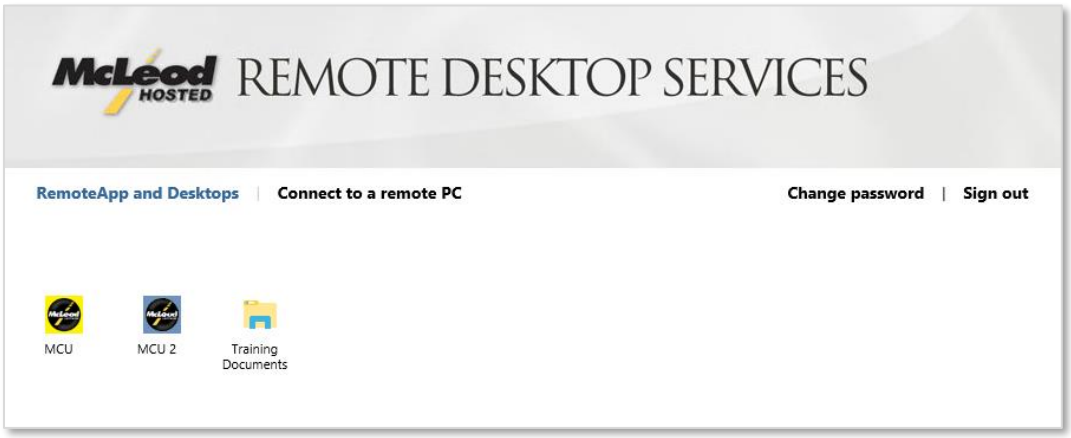


a. Please click "Your password is expired. Click **here** to change it."



b. Current password will be the temporary password provided
c. New password: Please refer to the Password Policy on page 11 of this document.

4. Once logged in, the user will see icons for the applications available to you. See the example below.

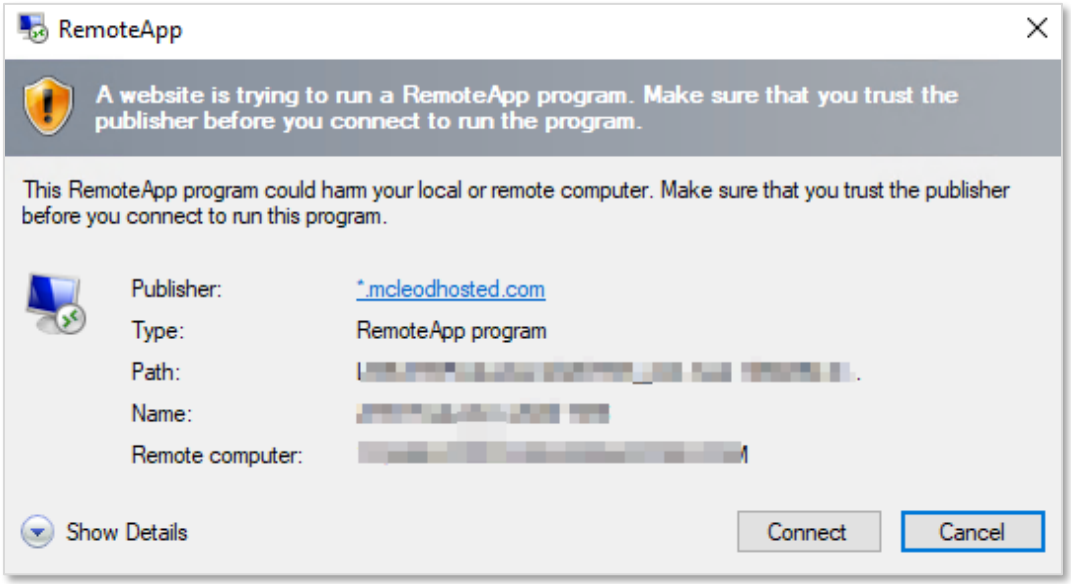


5. Click the application to be opened.

   What happens next depends on the Internet browser being used. Included below are examples for Internet Explorer, Google Chrome, and Mozilla Firefox using the default browser settings.

Internet Explorer

a. After clicking the icon for the application, a pop-up for RemoteApp appears similar to the one below. Click **Connect**.



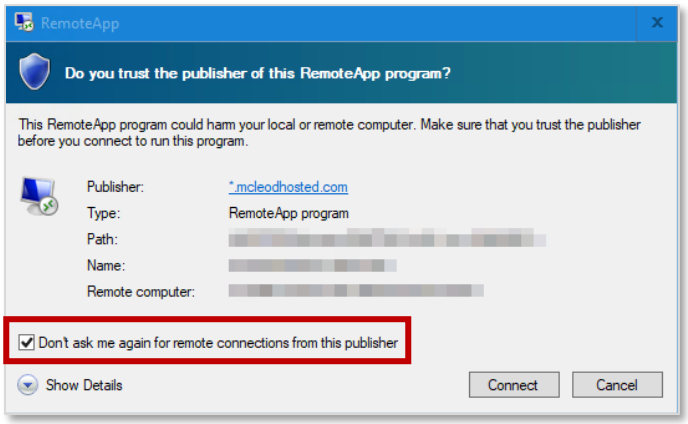
b. RemoteApp will connect and the application should open at the top of your screen.

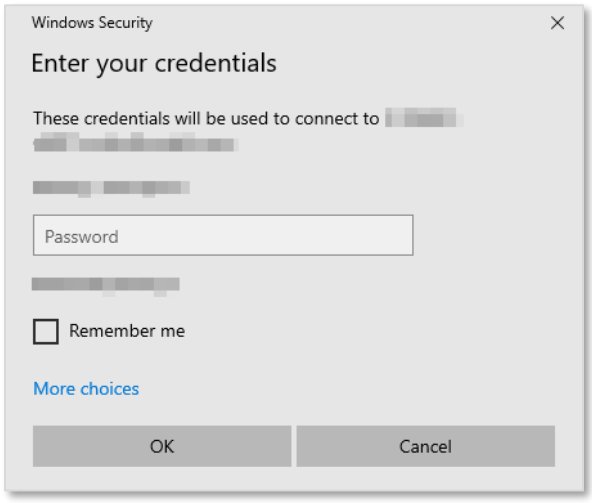
Google Chrome

a. After clicking the icon for the application, the user will download an RDP file. Notice the download status at the bottom left of the screen. See the example below.

b. Double click to open and another pop-up will appear like the image to the right. Optionally, check the **Don't ask me again** checkbox, and then click **Connect**.

c. A **Windows Security** prompt for username and password will appear. This will default to the user that is signed into Windows.

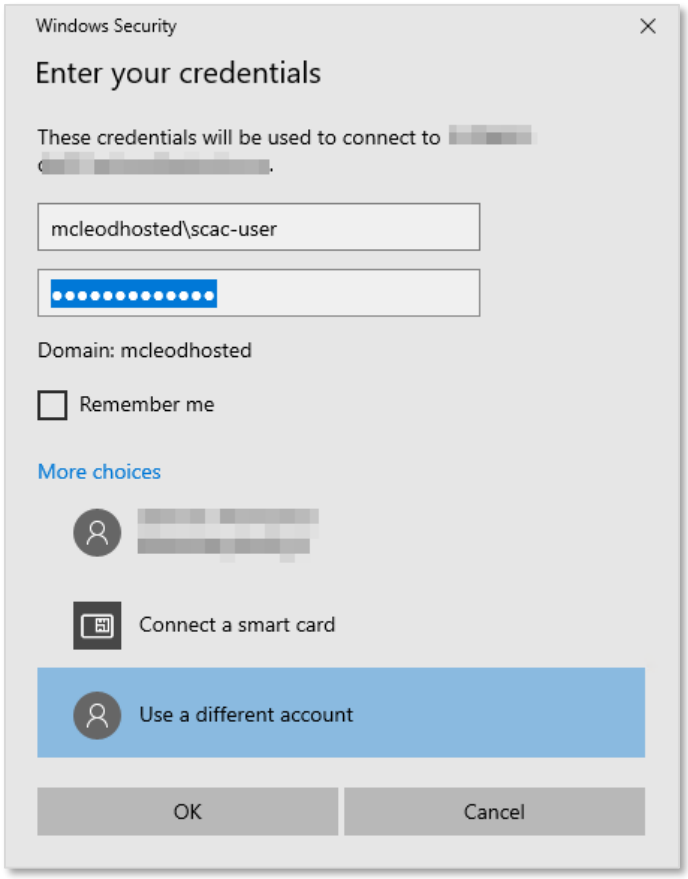




d. Click **More Choices** and then **Use a different account**.

e. Type in the appropriate username and password.

Note: Please use **mcleodhosted** in front of the ammf-***** user, as seen to the right.

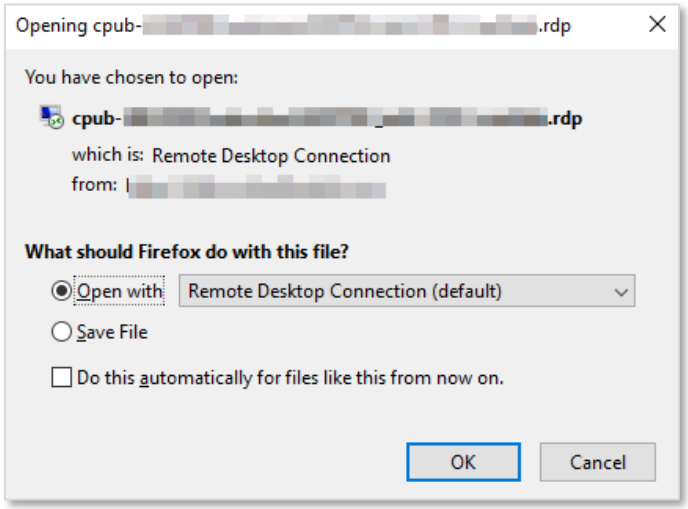


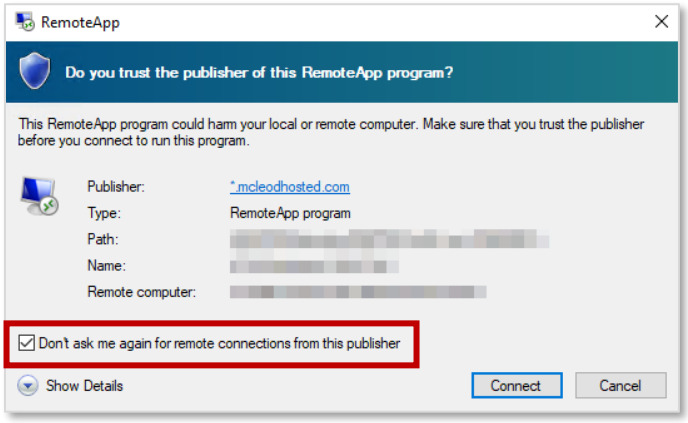
f. Click OK.

g. RemoteApp will connect and the application should open at the top of the screen.

Mozilla Firefox

a. After clicking the icon for the application, the user will be prompted to Open or Save File.
b. Leave the default option checked to open the file and click OK.
c. A **RemoteApp** prompt appears. Optionally, check the **Don't ask me again** checkbox and then click **Connect**.



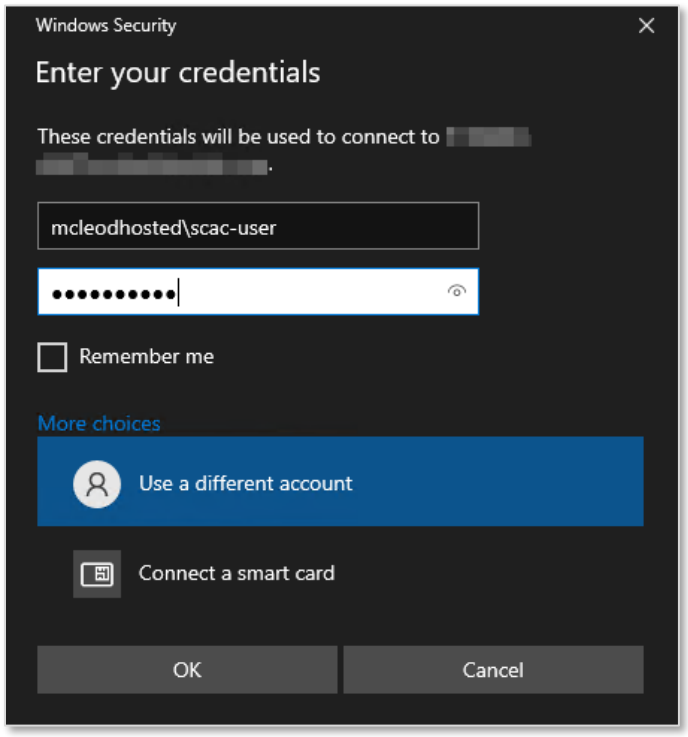


d. Click **More Choices** and then **Use a different account**. Type in the appropriate username and password.

   Note: Please use **mcleodhosted** in front of the ammf-***** user, as seen to the right.

e. Click OK.

f. RemoteApp will connect and the application should open at the top of your screen.

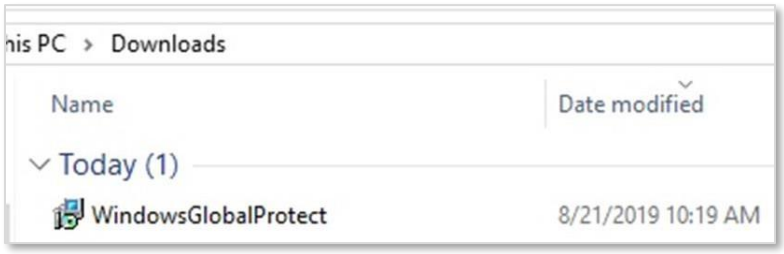


Installing & Using Palo Alto GlobalProtect VPN Client

1. Download the **WindowsGlobalProtect** application using the link below.

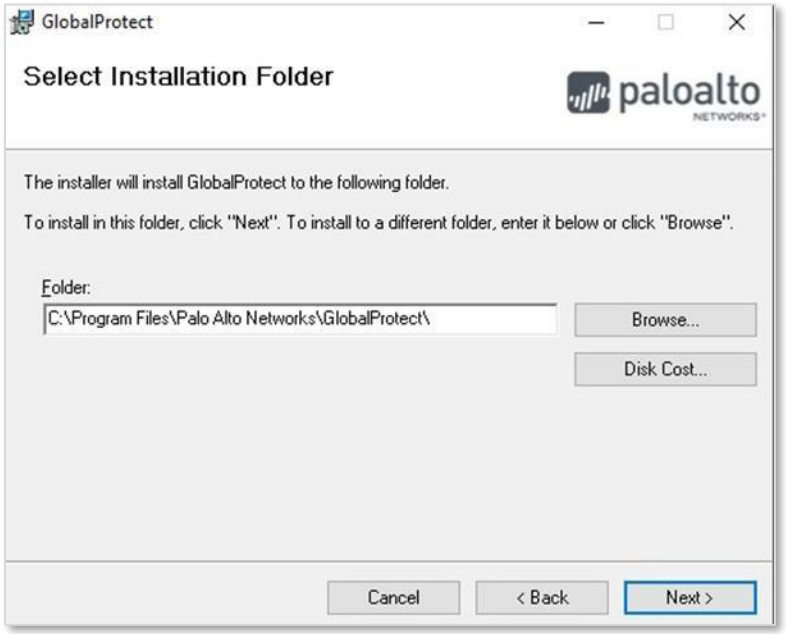
Windows Download	Mac Download

a. Open the downloaded file by double-clicking **WindowsGlobalProtect**.

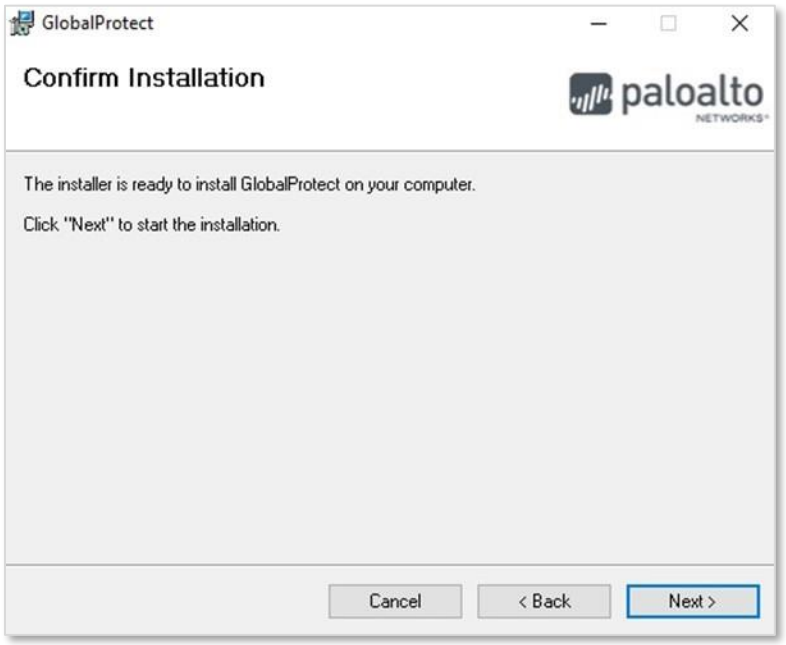


b. Start the Installation Wizard by clicking **Next**.

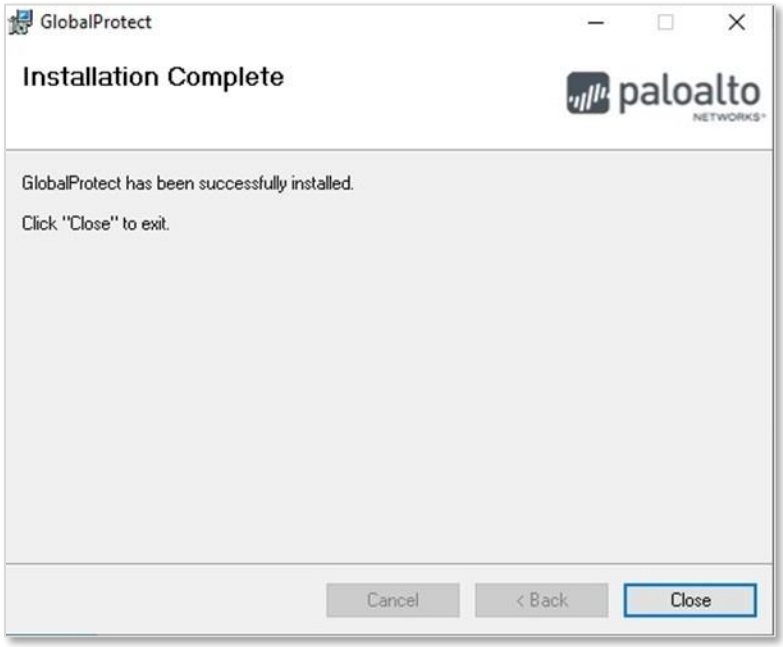
c. Use the default installation location and click **Next**.



d. Click **Next** to start the installation instance.



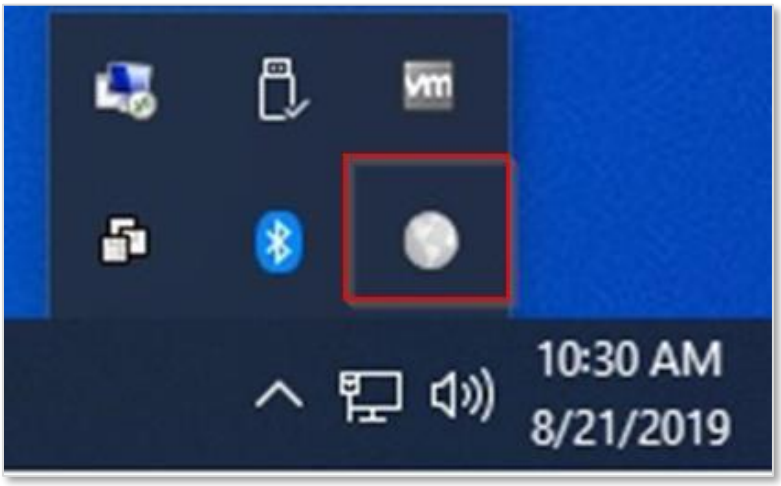
e. Wait for Install to complete.

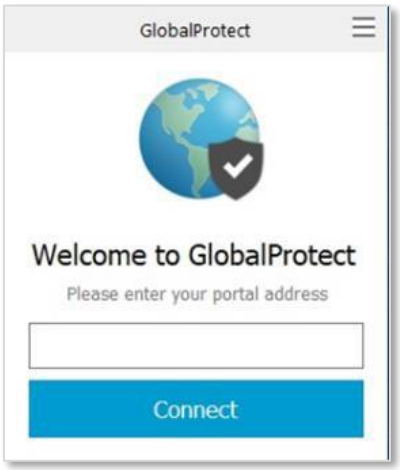


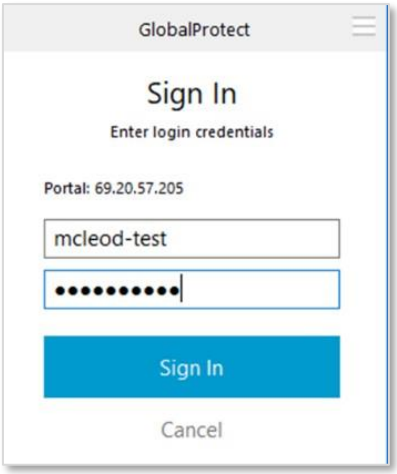
2. Click the **GlobalProtect** icon in the system tray.
   a. Select the correct **portal address**:
      i. nsh.mcleodhosted.com

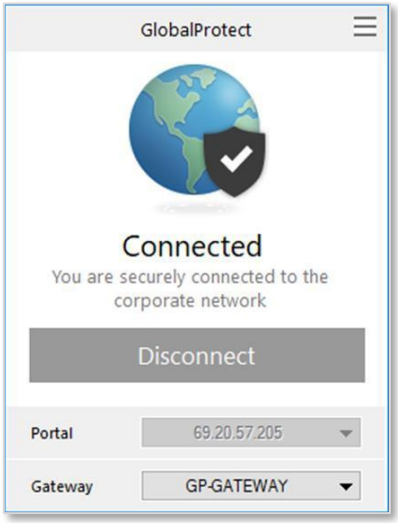
      Note: The Cloud Services team can provide this information if the user is unsure which portal address is correct.

   b. Input the McLeod Username and Password.
   c. Click **Sign In** and the connection will be established.





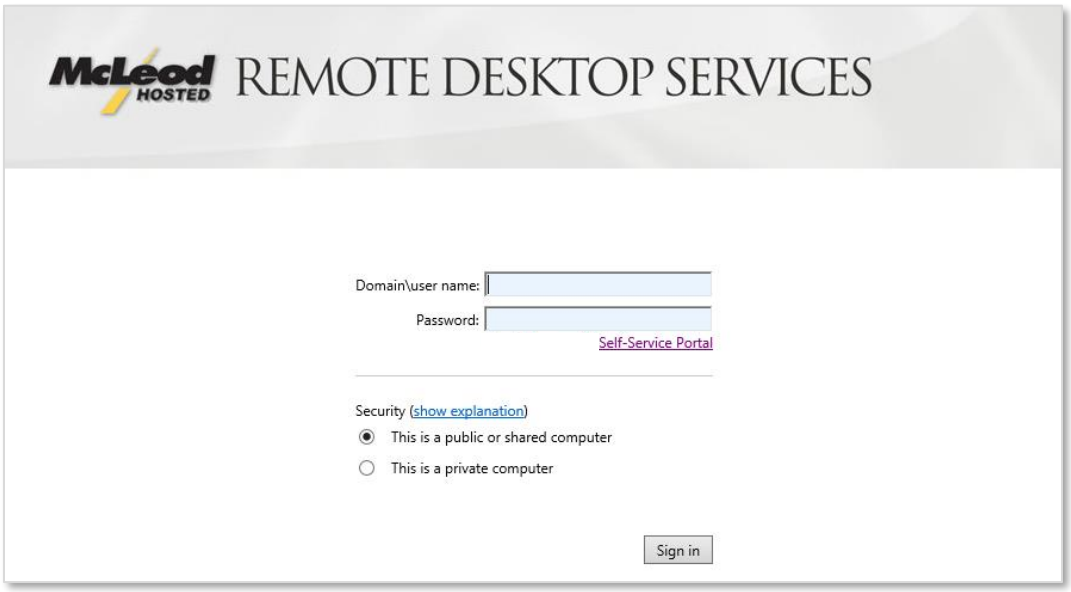




Self-Service

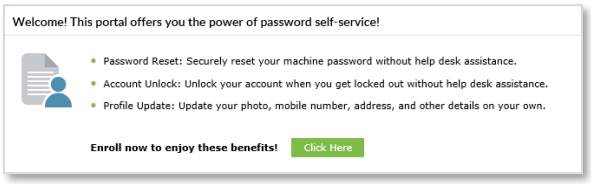
1. From the **McLeod hosted portal** page, click the **Self-Service Portal** link below the Password field. Alternatively, use the URL below:

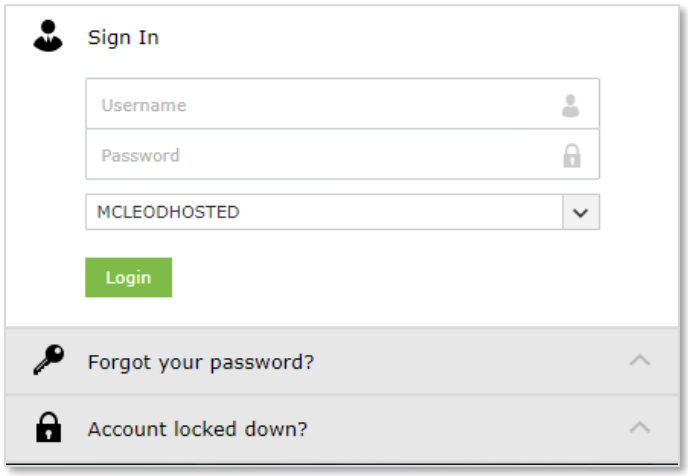
   https://selfservice.mcleodhosted.com:9251/showLogin.cc?logoutFromSSO=true



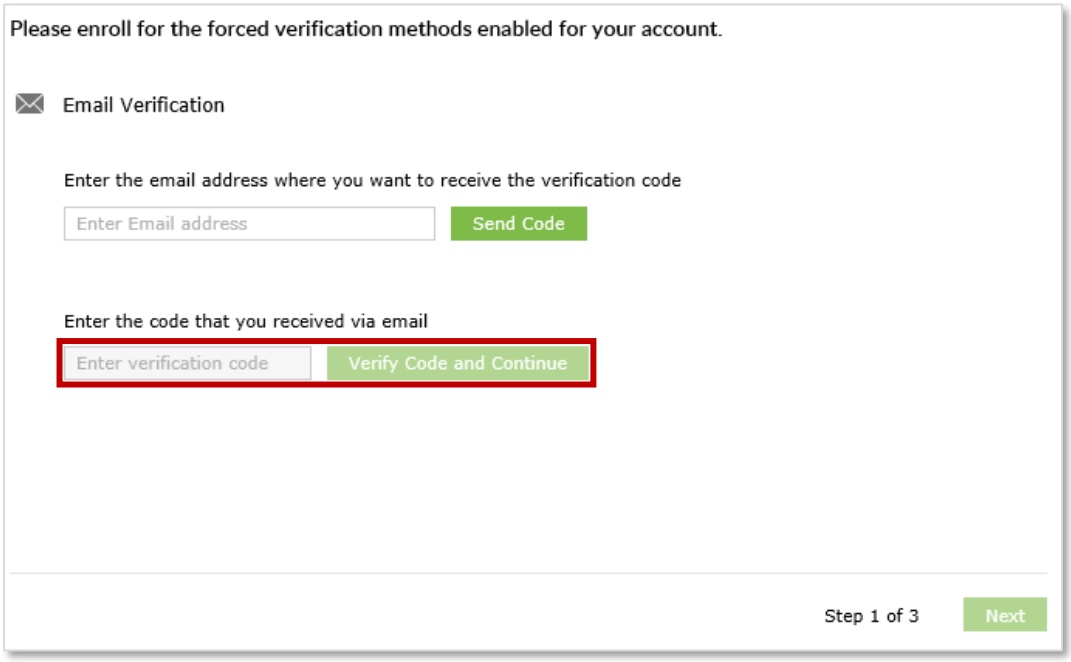
2. Login using the ammf-xxxxx user and password.

3. Click the **Click Here** button.

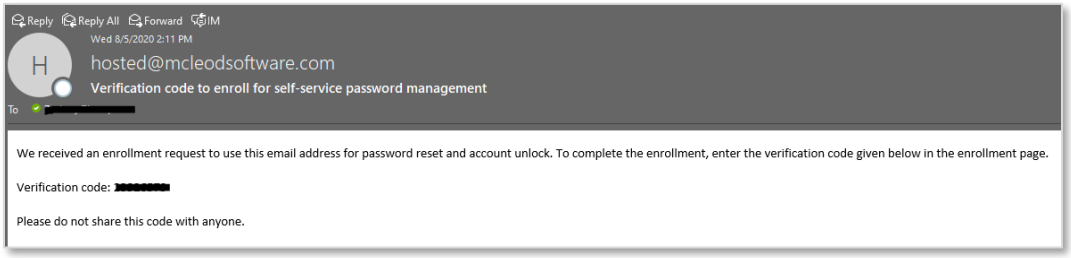




4. Enter an appropriate email address and click **Send Code**.

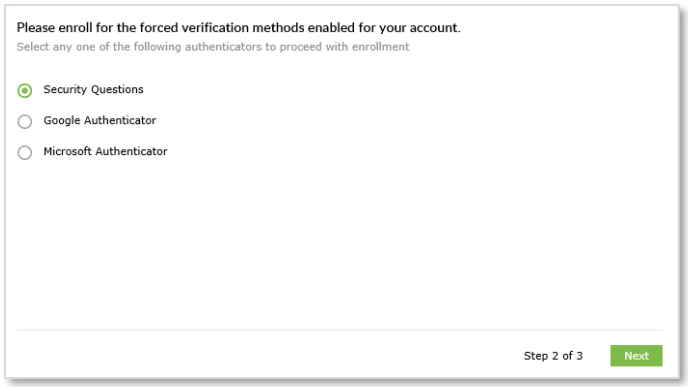


5. The user will receive an email like the one below.

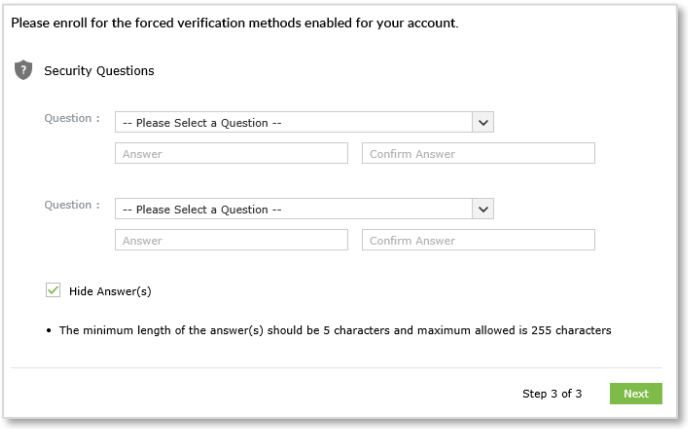


6. Enter the Verification Code provided in the email in the **Enter verification code** field and click **Verify Code and Continue**.

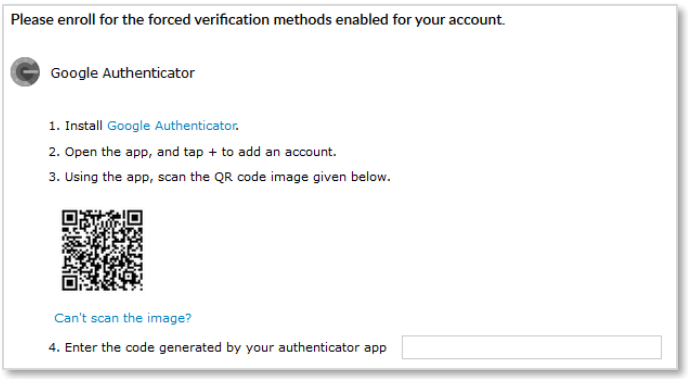
7. Please choose a preferred verification authenticator method.

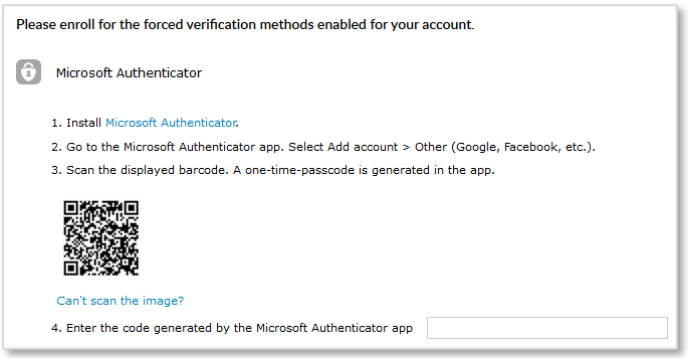


8. If the choice was “Security Questions”, the following window appears.
   a. Select two **Questions** and provide and confirm valid **Answers** in the fields provided.
   b. Click **Next**.

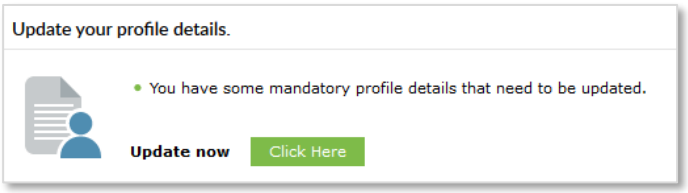


9. If the choice was either “Google Authenticator” or “Microsoft Authenticator“, then one of the following windows will appear.
   a. Enter the code generated by the application.
   b. Click **Next**.

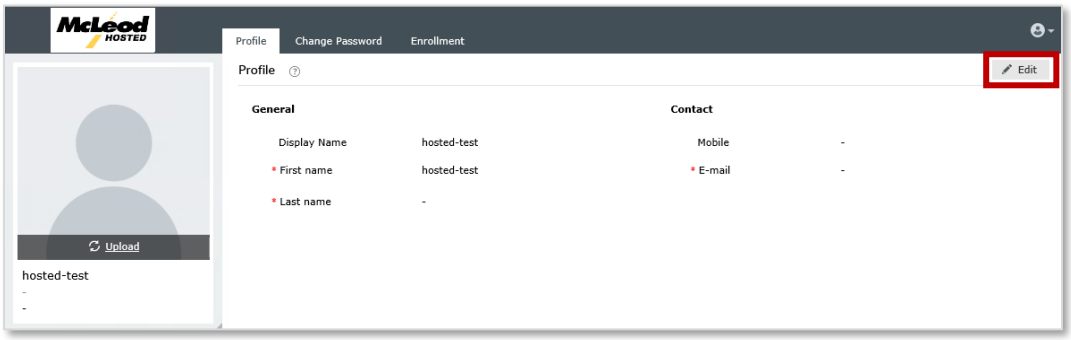




10. Update profile details. Click the **Click Here** button.

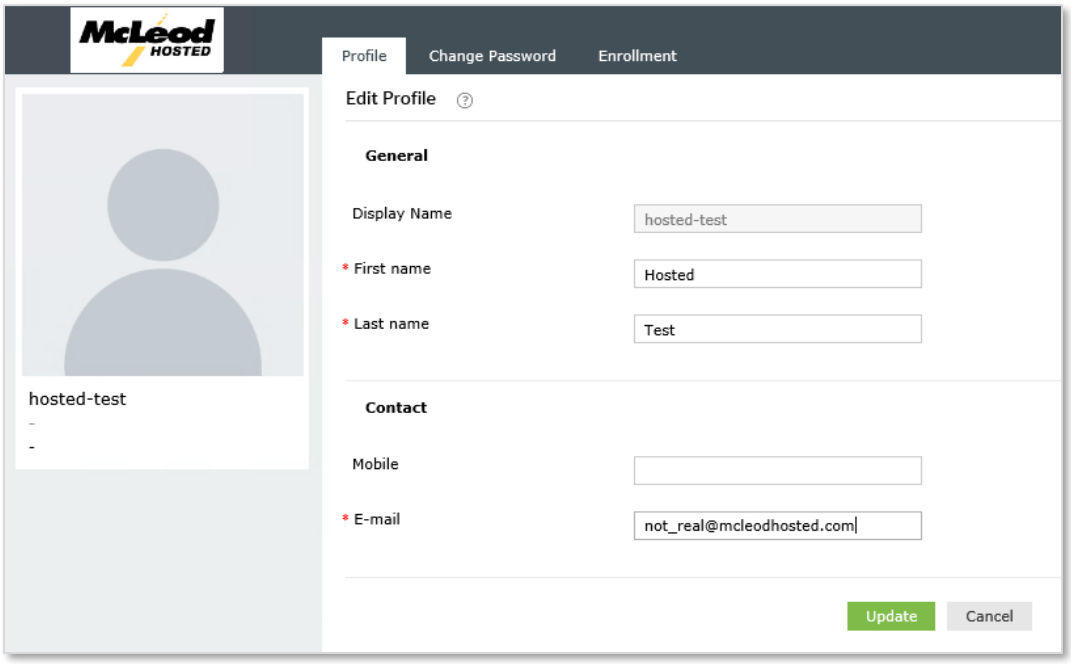


11. On the **Profile** window, click the **Edit** button on the upper far right of the window.



12. On the **Edit Profile** window, update the **First name**, **Last name,** and **E-mail** fields and click **Update**.

Caution: It is important to note that adding a Mobile number in the Profile screen means that the user opts in to future communications using that mobile number. Please do not add a Mobile number if the user does not want McLeod Cloud Services to use it to communicate in the future.



13. The user is redirected to the **Profile** window. An email will be sent verifying these changes.

Overview – Password Policy

The password policy will be as follows.

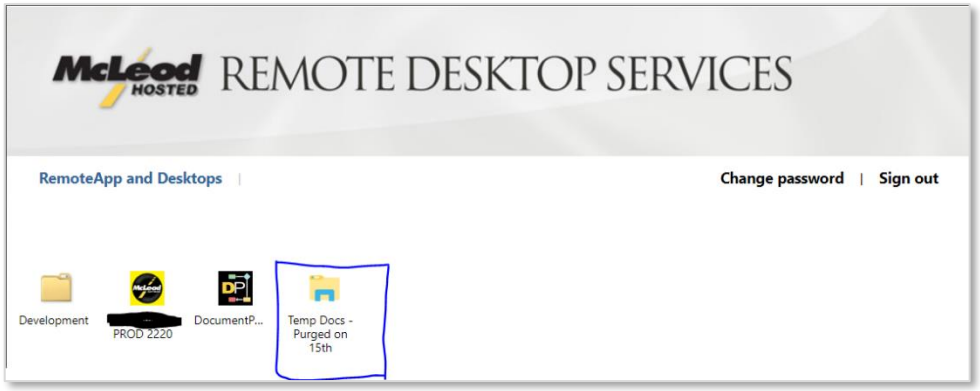
- Minimum Password Length – 8 characters
- Enforce Password History – Remembers Last 12 Passwords
- Maximum Password Age – 180 days
- A user password must meet the following complexity requirements:
  - A password cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters
  - The password must contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (i.e., !, $, #, %)
- A user account will be locked out for failed password attempts. See below:
  - Number of failed login attempts allowed – 10
  - Reset failed login attempts count after (mins) – 10
  - The account will be locked out for a duration of (mins) – 60

Working with McLeod Applications in a Remote Environment

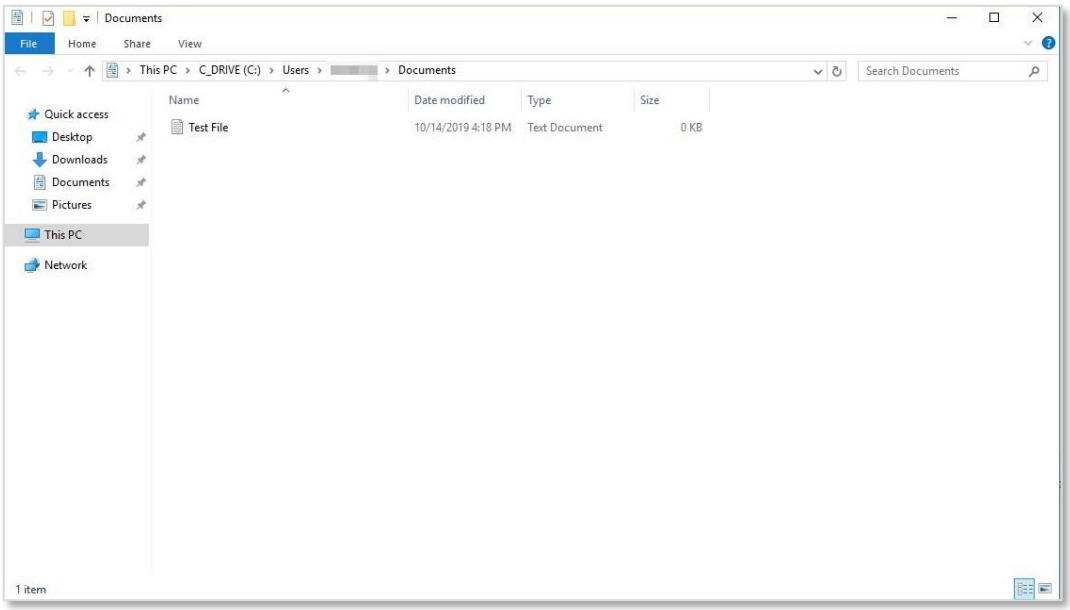
Saving Files to Local Machine

The process for saving files from the McLeod System to a local machine will require some additional steps compared to running the McLeod System locally.

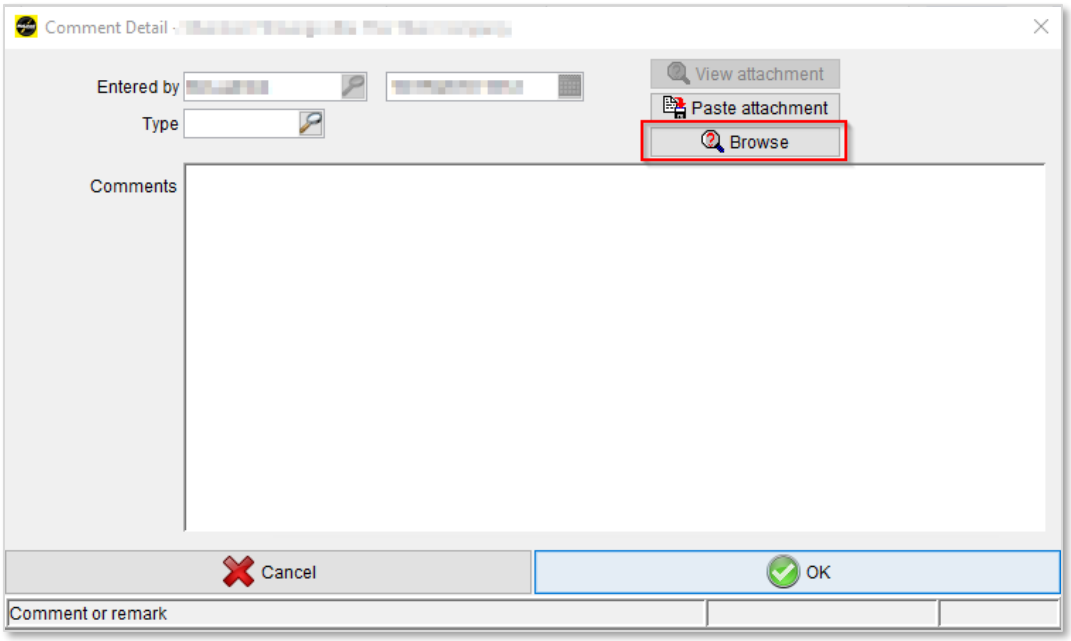
1. When saving a file to a local computer, first launch the Temp Docs shortcut from RemoteApp and Desktops page by clicking the **Temp Docs – Purged on 15th** icon.



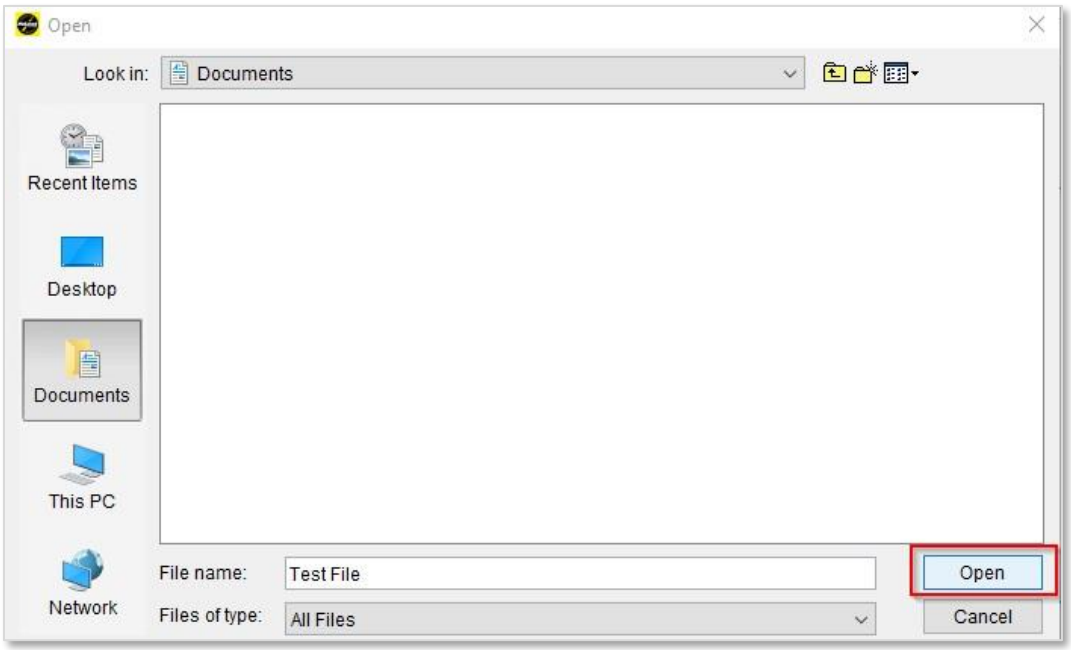
The Terminal Server Documents folder is displayed.



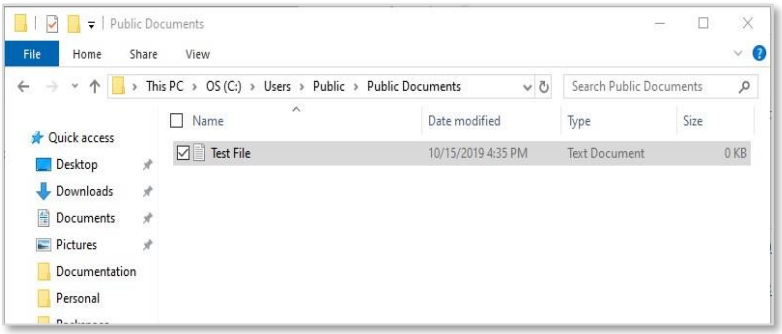
2. Next, click **Save** or **Browse** on any document window. The **Documents** folder will display by default.



3. Name the file, then click **Open** or **Save**.

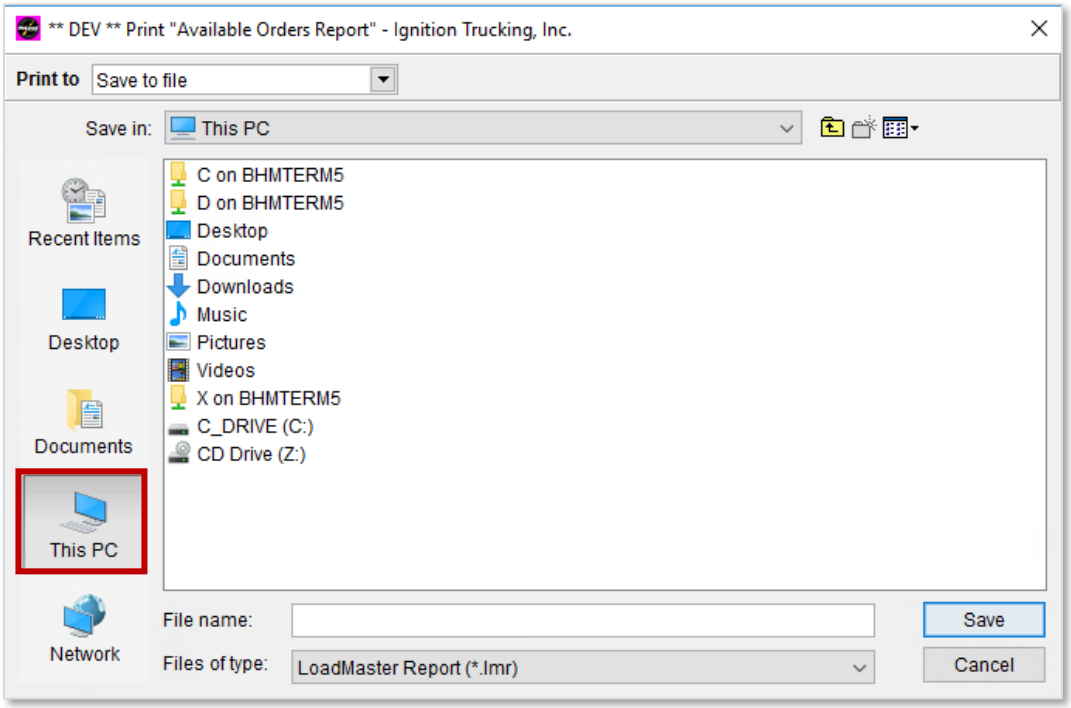


4. Finally, **copy the file** from the Temp Docs folder to any folder on the local computer.

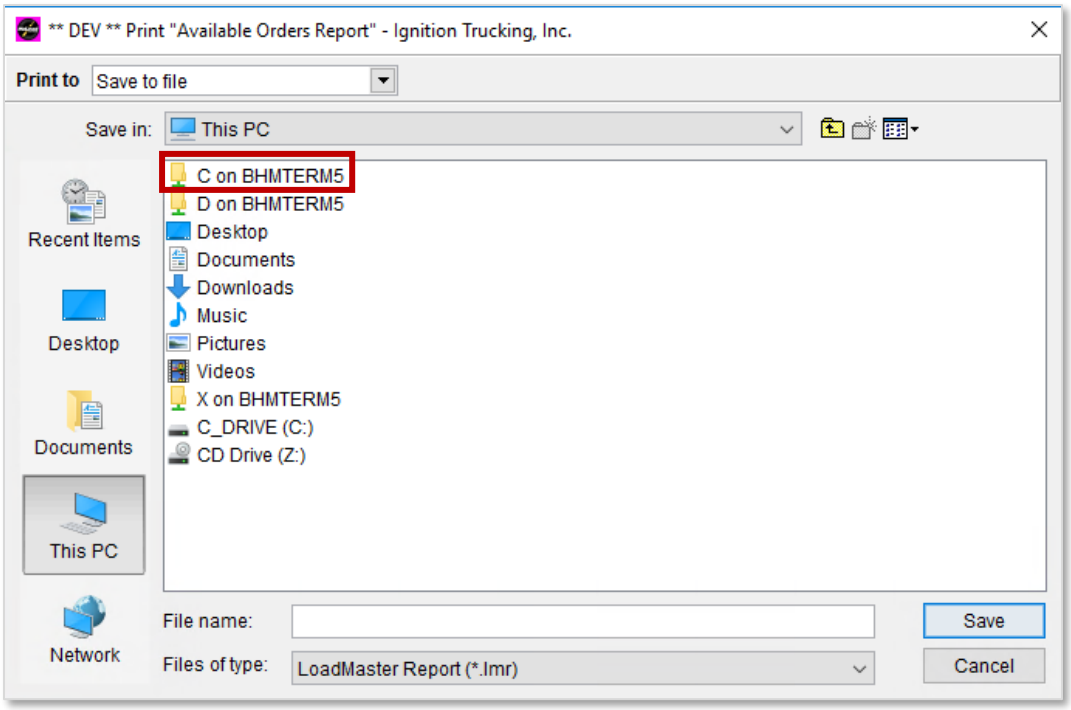


Saving Files to Local Machine – Alternate Method

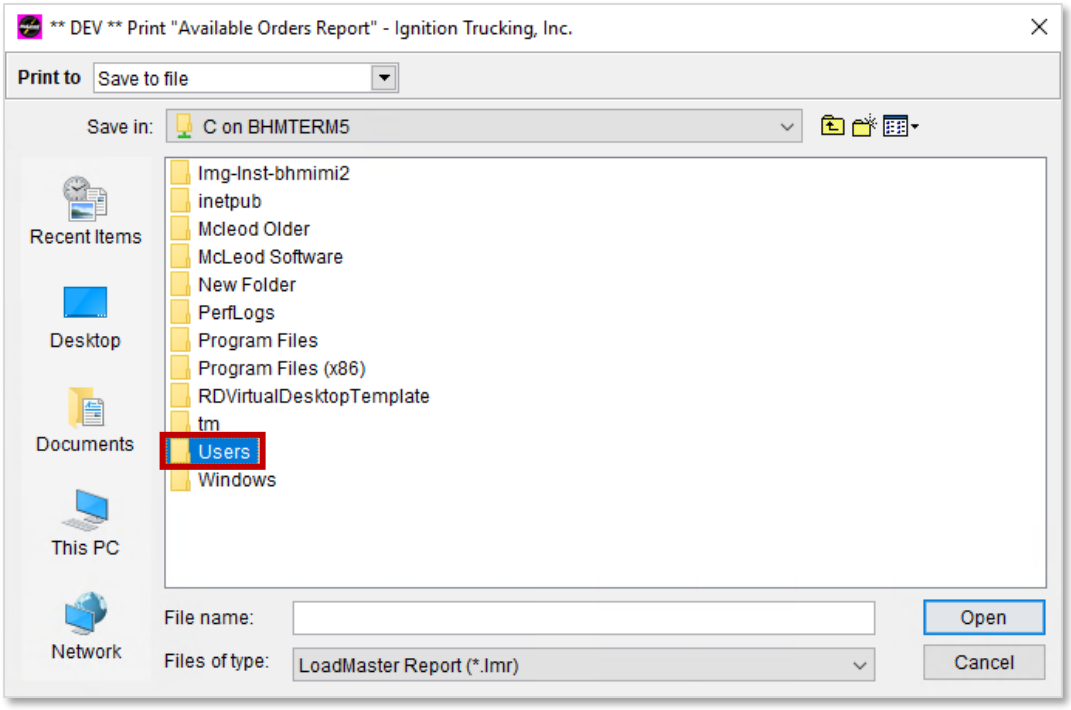
5. When saving a file from the McLeod System to a local machine, click the **Computer** icon in the left pane.



6. Under other, select C: on (the local PC Name)

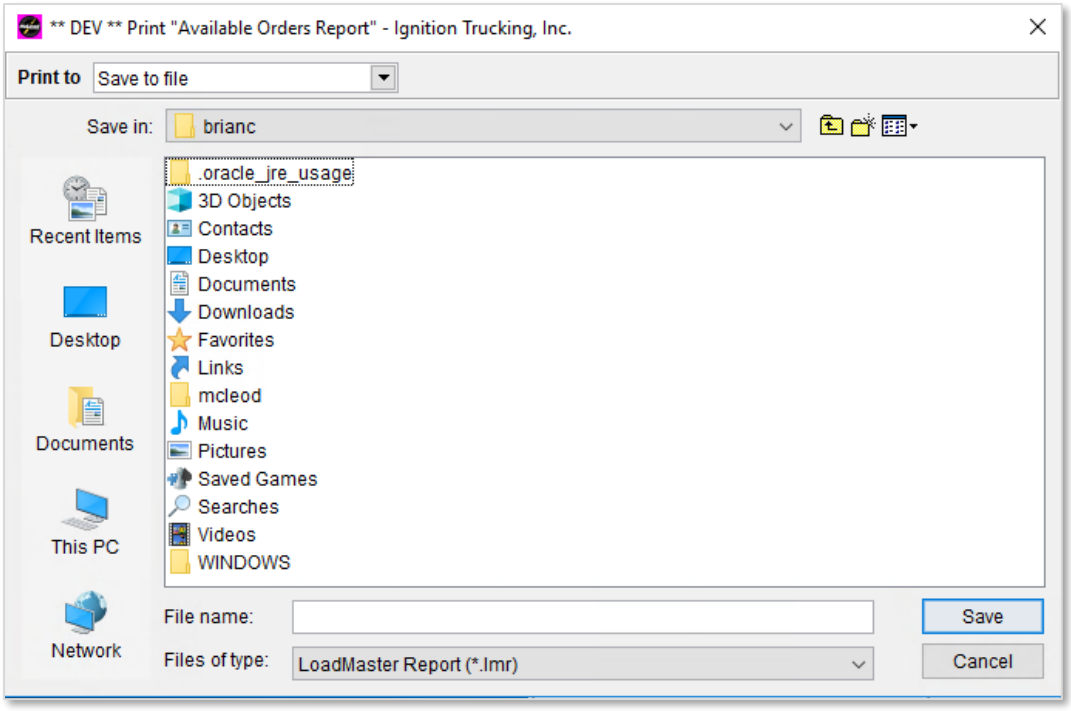


7. Next, open the **Users** folder.



8. Then, open the correct user folder corresponding to the Windows login used.

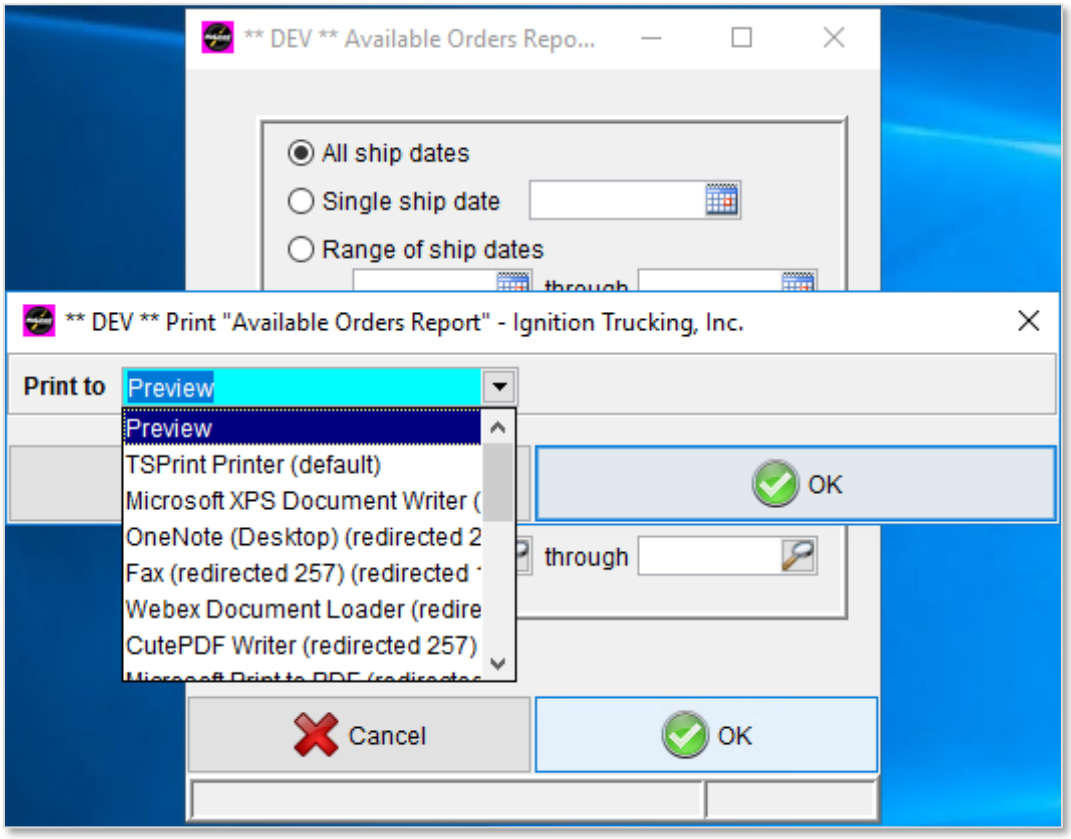
9. Finally, Choose the desired save location within the local file folders and click the **Save** button.



Printing

The process for printing will change as the application is no longer running on a local machine. A user must first install **TSPrint** on their machine (IT personnel may have already completed this for you). Instructions for installing **TSPrint** are included in Appendix B.

10. When **printing** from the application select from the dialogue box **TSPrint Printer (Default).**



11. Pick up the newly printed documents on the default printer normally used.

Tip: To change which printer "TSPrint Default" prints, simply change the default printer on The local machine.

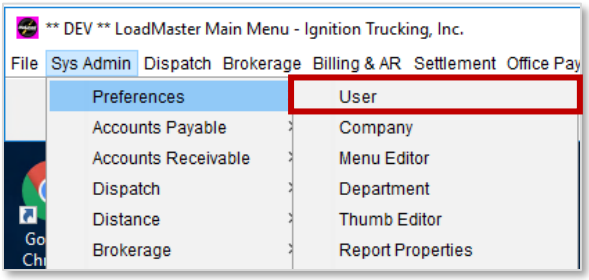
New User Creation

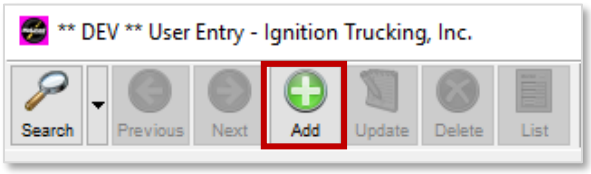
12. To create new users, simply submit a request to your **ammf@mcleodsoftware.com** email noting a new user in the subject line.

Note: All users are separated and identified using their AMMF Code-First Initial Last Name (up to 10 total characters) Example: "ammf-uname".

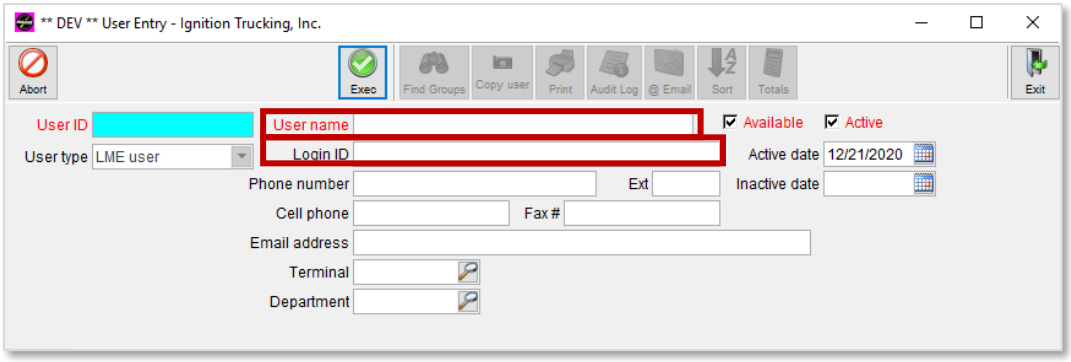
13. Once provided with the username and password, the user will need to add the hosted username to the "**Login id**" field of the **User** entry screen (**Sys Admin | Preferences | User**).

14. If creating a new user, select Add on the menu at the top of the screen. Otherwise, Update an existing record.





15. Enter the user's information.



a. Enter the user's First and Last name in the **User name** field.
b. Enter the hosted username in the **Login ID** field.
c. Optionally (depending on specific company configuration), input the **User ID.** If master code generation is enabled, allow the McLeod System to select a User ID.

16. Finally, once the user is configured select Exec to save.

Email

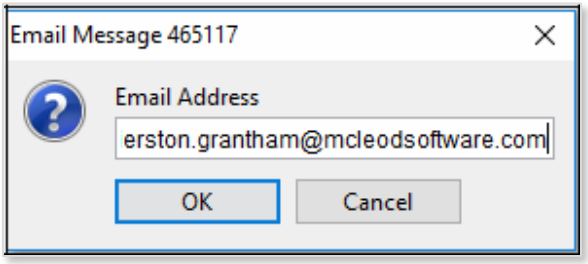
Starting with LoadMaster and PowerBroker v15.2, email configuration is built into the software and can be updated on the fly. The email control screens are located in the following 3 places:

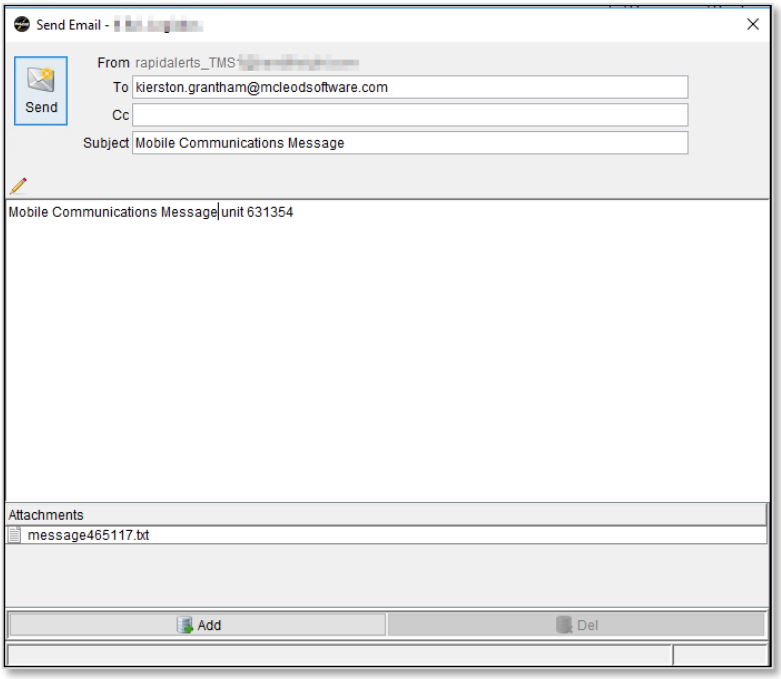
- Company-wide settings – **Sys Admin | Preferences | Company | Outgoing Email**
- User-specific overrides – **Sys Admin | Preferences | User | Outgoing Email**
- Function-specific overrides, such as settlement email – **Sys Admin | Email | Email Profiles**

Caution: In the McLeod Systems older than v15.2, email configuration is located in multiple files within the software. Editing these files requires a working knowledge of how the software functions. Due to this complexity, please contact support to assist with any changes to your email integration.

Note: If you utilize Google Apps/Gmail as your organization's email service, please see Appendix C for additional setup instructions

Emails sent from the cloud services environment will use the java mail screen (instead of launching to a local email program) and will look similar to the below screenshot. It will use the company email settings unless the user override is set up on a user profile.





Email Links

The **Email Screen Link** button (Usually displayed as **@ Email**) normally allows a user to send a hyperlink to another user. When used this function would take the user to the linked screen or record. This will no longer work correctly when accessed through a normal email client. This occurs because the user is working through a remote session, which involves running the program on a different machine than the local computer.

When a user tries to click the link in the email from the local machine, the link will fail to find the McLeod System software on the local computer and will not open successfully. A screenshot of this menu option and the error when accessing from a local machine are provided below.

Tip: This button can be disabled using the screen level permissions in the permission manager so that users will not try to send screen links via email.

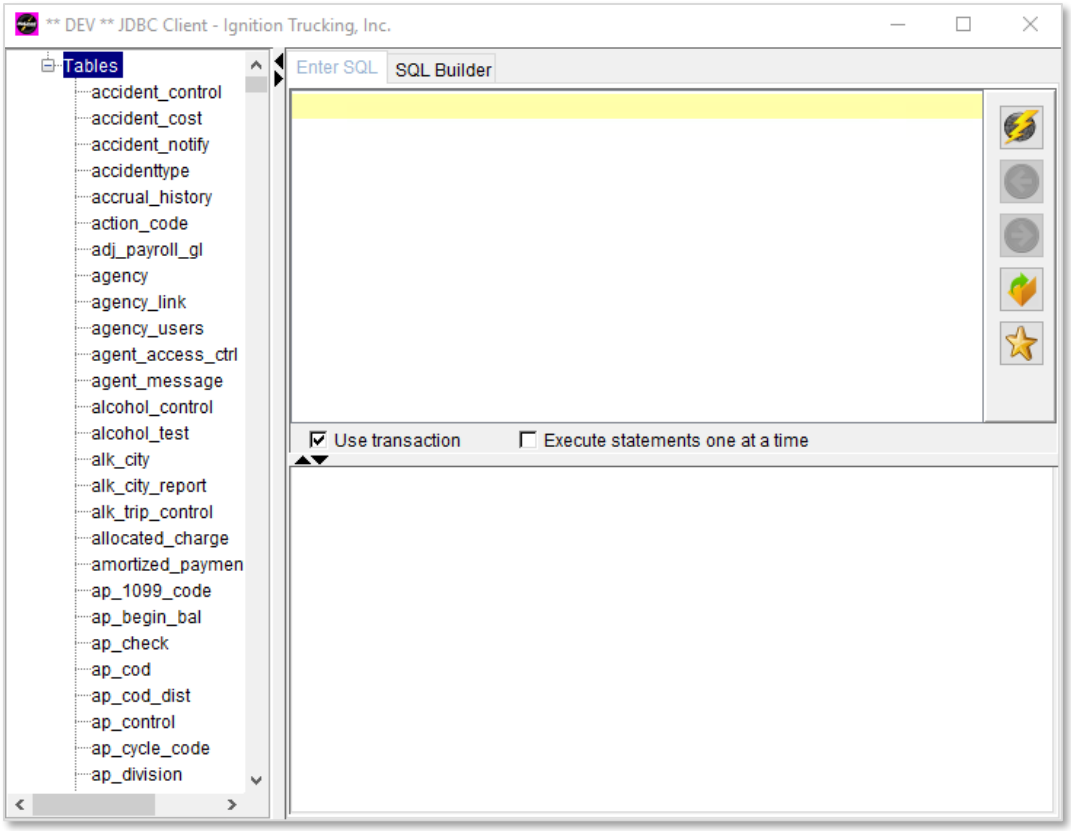
Database Access

Advanced users will notice that they are unable to access the Cloud Services databases *directly* through tools such as Microsoft SQL Studio. This is done primarily for data protection and security. However, for any power users or IT staff that would require this access, there is a built-in database tool within The McLeod System & Powerbroker that can provide access to query and update the database tables called the "**JDBC Client**" which can be accessed from the main menu under **Sys Admin | Utilities | JDBC Client.**

Note: The McLeod Account Manager and Cloud Services team can assist in running most queries, by request.

Caution: It is highly recommended that this tool be permissioned off via the **Permission Manager** for non-key or power users, as it provides access to the LoadMaster and PowerBroker databases.

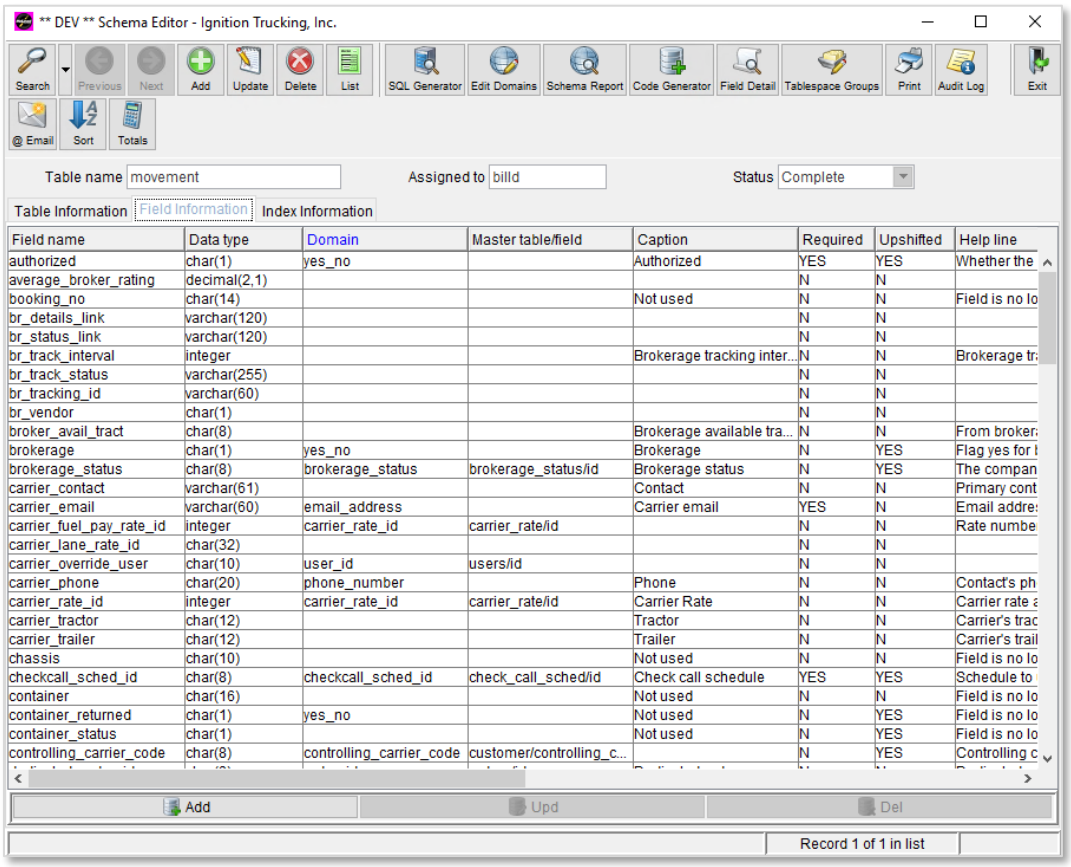
Warning: Use extreme care when implementing this tool, or when writing any SQL commands. Correcting data corruptions caused by SQL commands written by end-users can result in billable charges for data recovery performed by the McLeod support team.



Updating Database Schema

Similar to the general database access, users will not be granted the elevated permissions required to adjust the database schema. This would normally be done in situations such as adding new fields to a screen or changing data types for a field. This is not recommended even for non-cloud services customers as changes to fields or tables can have negative impacts on McLeod System functionality if not fully tested. However, if changes are required, they can be tested and performed by the McLeod Software support team.

Note: The McLeod Account manager and Cloud Services team can assist with any required schema edits.



Appendix A – McLeod Software Cloud Services Login/User Management

As with all requests, support must be requested through your organization's designated Key Users by contacting the McLeod front desk at **205-823-5100** or by emailing ammf@mcleodsoftware.com.

Starting on your Go-Live Date, User Creation/Deactivation will be requested by emailing ammf@mcleodsoftware.com.

New User Creation:

1) Email ammf@mcleodsoftware.com with your new user's name – McLeod Managed Services will send login credentials to the Key User through email.

2) Customer will navigate to ***Sys Admin – Preferences – User*** to add this user to LoadMaster/PowerBroker.

User Deactivation:

1) Email ammf@mcleodsoftware.com with the Login ID that needs to be deactivated.

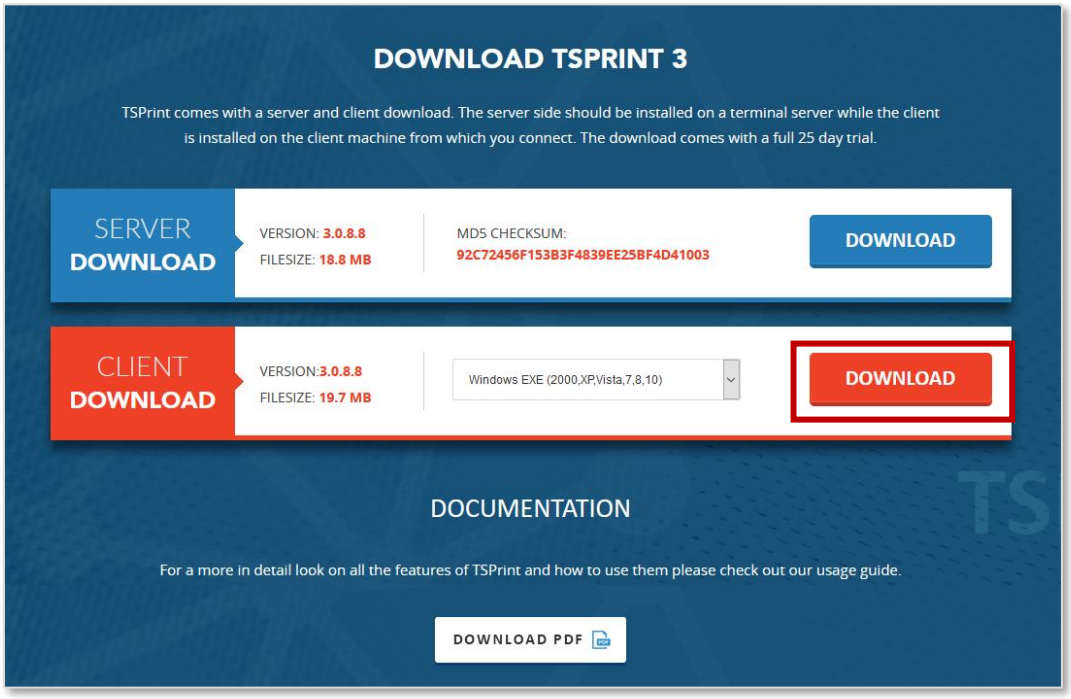
2) Customer will navigate to ***Sys Admin – Preferences – User*** to Inactivate this user.

Warning: Failure to request user deactivation may result in unexpected Monthly charges.

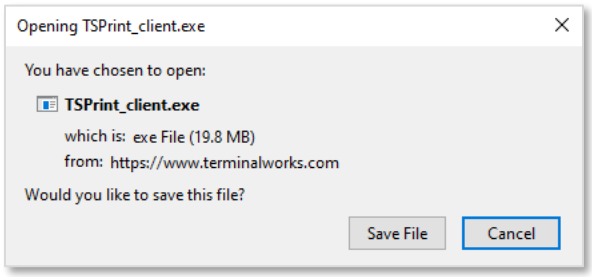
Appendix B – How to Install and Use TSPrint Capability

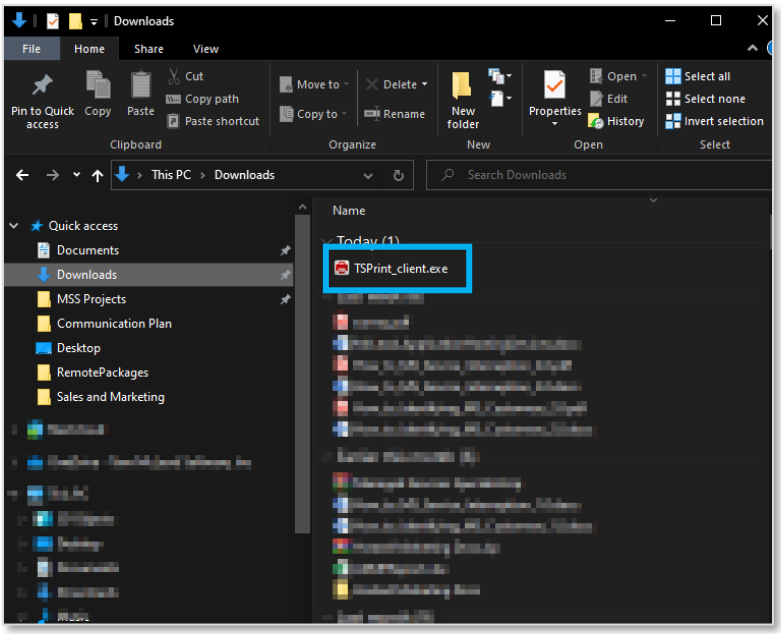
1. Visit http://www.terminalworks.com/remote-desktop-printing/downloads

2. Choose the correct Client Download option from the drop-down and click “Download”

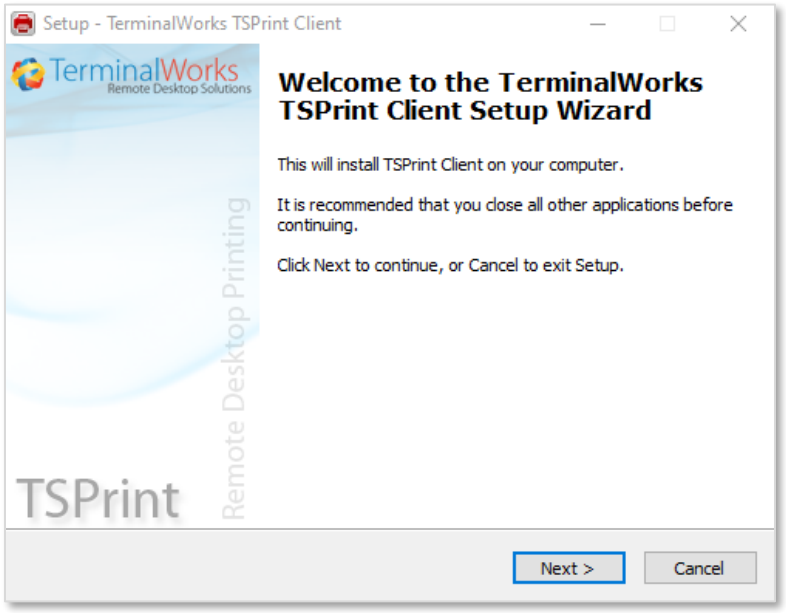


a. Once the client has finished downloading, run the tsprint.exe from your computer

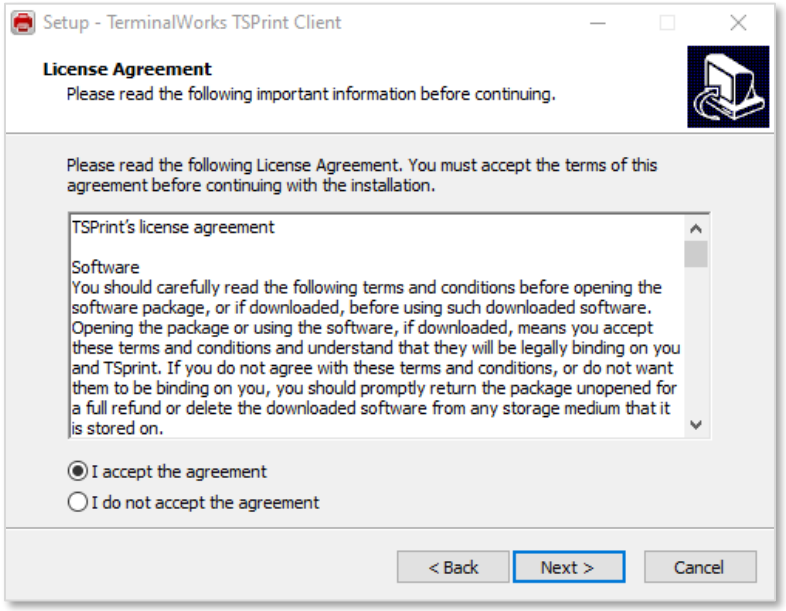




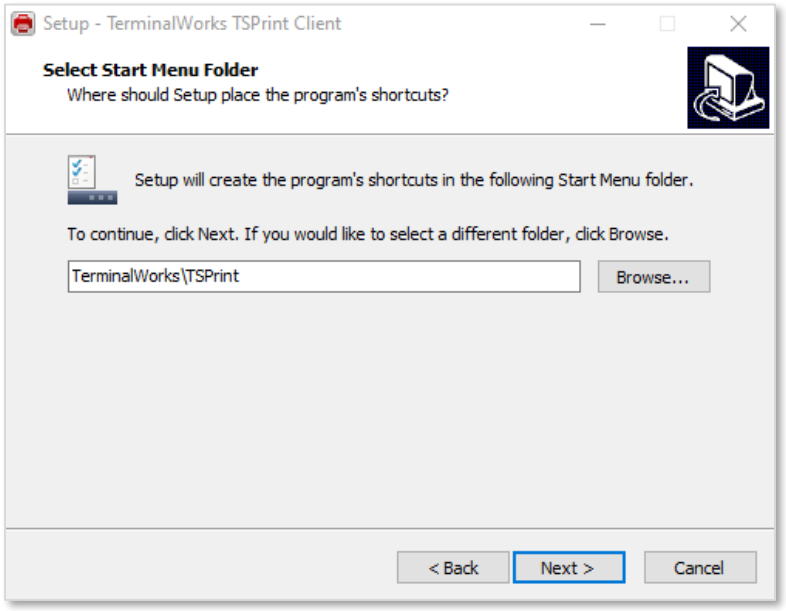
b. Click **Next**.



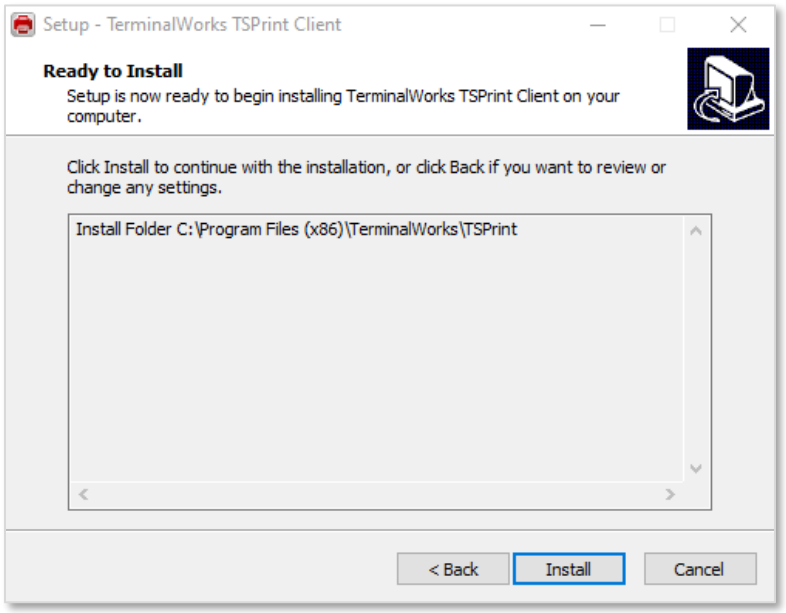
c. **Toggle** the **I accept the agreement** option and click **Next**, then click **Next** again.



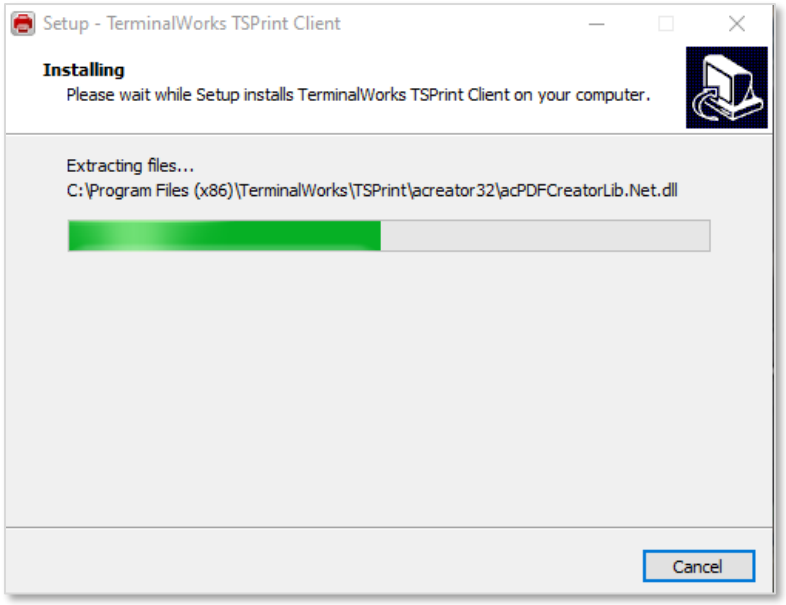
d. The setup program defaults to the following folder for shortcuts. Use the default installation location and click **Next**.



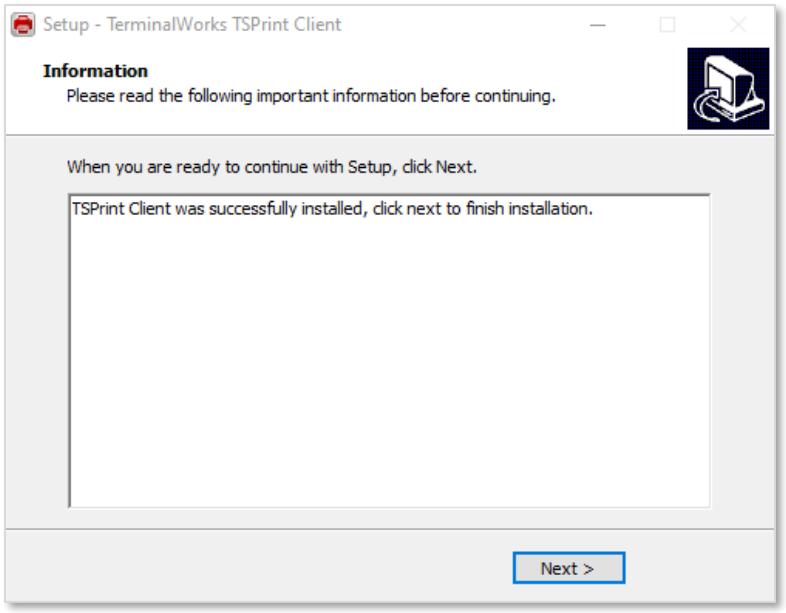
e. Click **Install**.



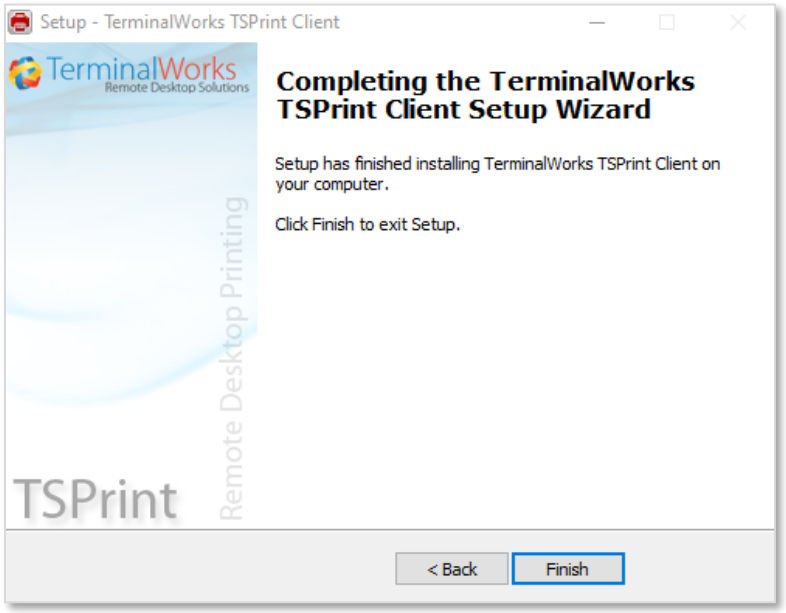
f. Allow time for the installation process to complete.



g. The program indicates that the TSPrint Client was successfully installed. Click **Next**.



h. Click **Finish**.



The TSPrint Client has now been installed.

Appendix C - Potential Conflicts with Screen Location and Remote Desktop Apps

Due to applications running as a Remote Desktop App, conflicts can emerge where screens popping up can cause the system to appear "frozen" for a user. This is due to a screen requiring input appearing behind or outside of your current monitor configuration. Not all users encounter this issue but may result in needing to disable certain pop ups or additional code to be deployed to your environment.

Known settings that can be cause screens to be inaccessible:

- User Settings
    - Save Screen Sizes and Positions
    - Add/Update Confirmation
- Google Places
    - Following Settings do not disable Google Places, but rather the automatic pop up for Google Places
        - Enable Location Add through Google Places
        - Enable Customer Add through Google Places
        - Enable Google Places for stop Lookup