Software Token Client User Guide — Desktop

Northwest Bank, serving Coeur d' Alene since 2017

EQUAL HOUSING LENDER Member FDIC

Northwest Bank

Experienced Bankers. Exceptional Service. Customized Solutions. **www.northwest-bank.com**

Software Token Client User Guide — Desktop

Table of Contents

Software Token Client (Soft Token)
For Desktop

Overview

The **Software Token Client (Soft Token)** for Desktop is an application that replaces the need for a physical token (hard token). The Soft Token application generates One-Time Passcodes which are needed upon creation and approval of ACH Payments and Wire Transfers on the **Commercial Online Banking (COB)** platform. This section of the guide will detail how to download and install the desktop version of the Soft Token.

Prerequisites

The Soft Token installation process requires administrator rights in order to install the **Encrypted Keyboard Driver (EKD)** and proceed with installation. Clients are advised to work with their technology resources to establish administrator rights on their PC. After installation, administrator rights are not needed to use the software. If the user does not have the required administrator privileges on their PC, they will receive an error message and be unable to proceed with installation.

Soft Token Download Link

The link to download Soft Token can be found on the COB sign-on page or under **My Settings, Software Token Client, Click Here to Download Token Client.**

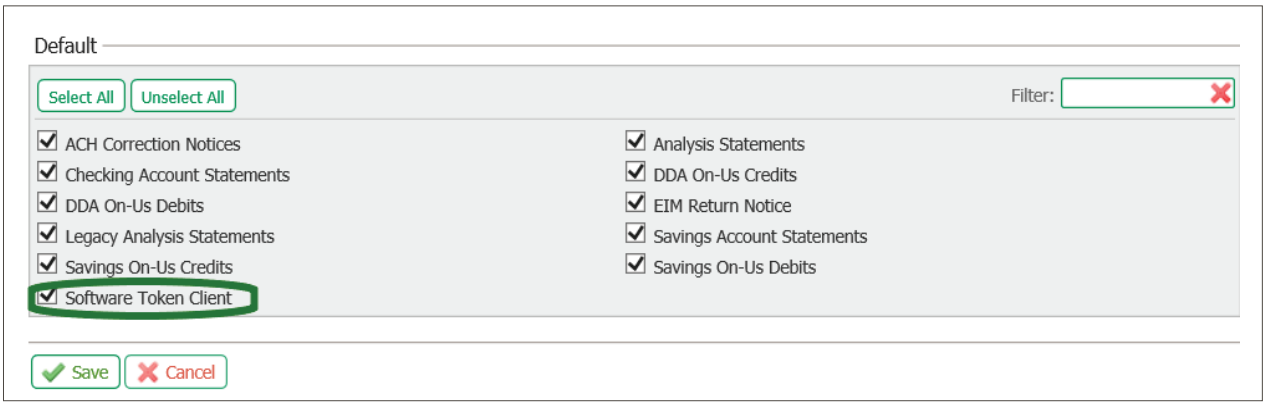
Software Activation Key

A **Software Activation Key (SAK)** is required to download Soft Token. This can be found under each individual user profile but only viewable by bank users and Company Administrators (Admins). To locate a user SAK, bank users and Admins can search for the desired user and select **Edit Profile** to be directed to the user's main profile page where the SAK is stored. Admins can locate their own SAK by selecting **My Settings, My Profile.** The SAK section details remaining uses and the expiration. The activation key is not case sensitive. If a SAK is expired, bank users and Admins can select the **Reset** button to generate a new key.

Permitting a User to Soft Token

Admins must ensure their users are permitted to Soft Token. This is done by selecting the appropriate user from the user list, navigating to **Actions**, then **Services**.

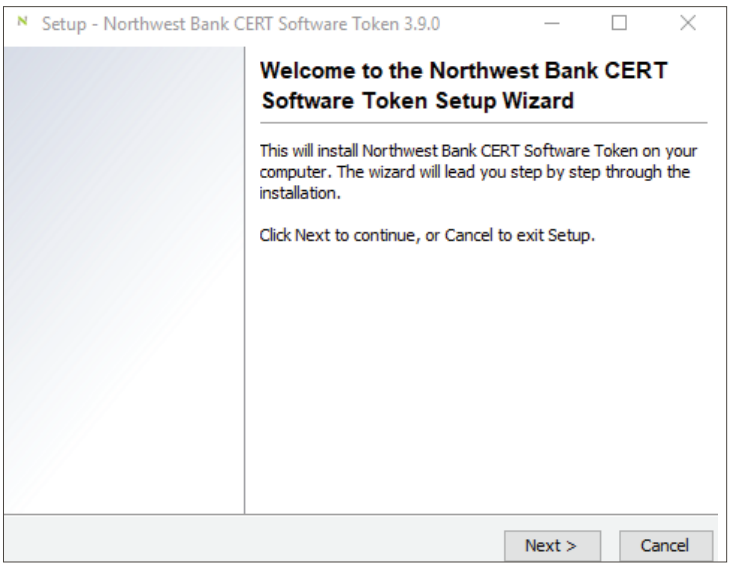
Next, enable the **Software Token Client** checkbox and **Save**.



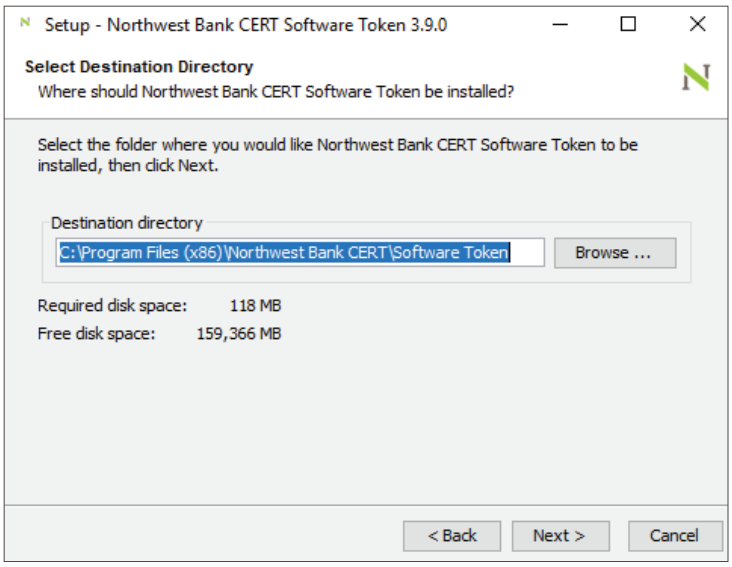
Soft Token Installation

To begin, users select the **Commercial Online Banking Token Client** hyperlink, and **Run** the application. The user will be directed to the setup wizard to continue with the installation process. Please note, this portion of the setup requires the user to have administrator privileges on their PC. See the **Prerequisites** section of this document for additional information on administrator privileges.

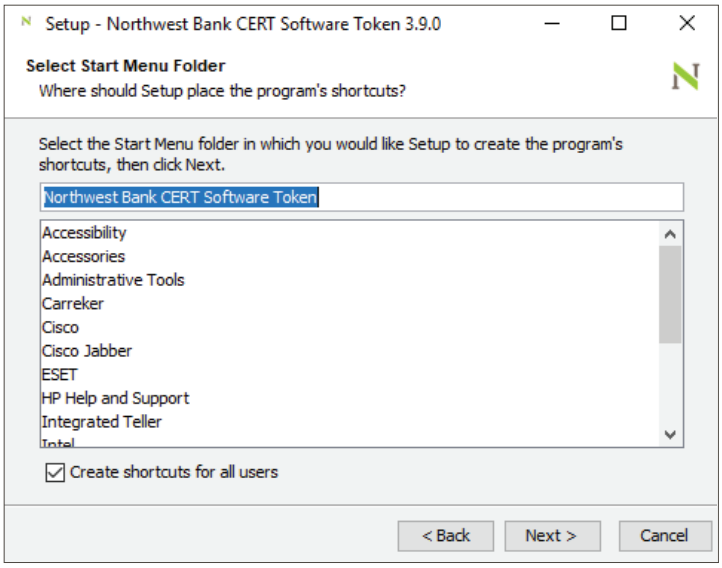
To continue, select **Next** in the **Software Token Setup Wizard** dialog box.



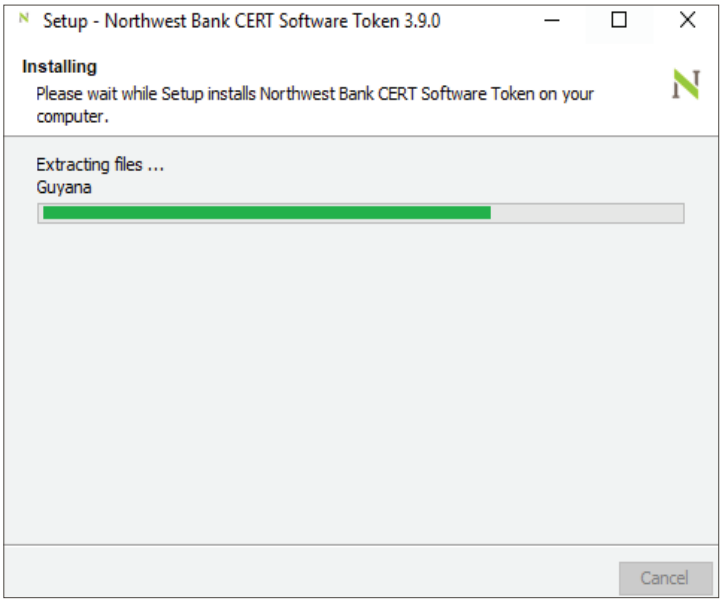
Next, select a destination directory. The default location can be accepted or another directory can be specified. To specify a different location, type the directory into the text field or use the **Browse** button to navigate to the preferred destination. Select **Next** to continue.



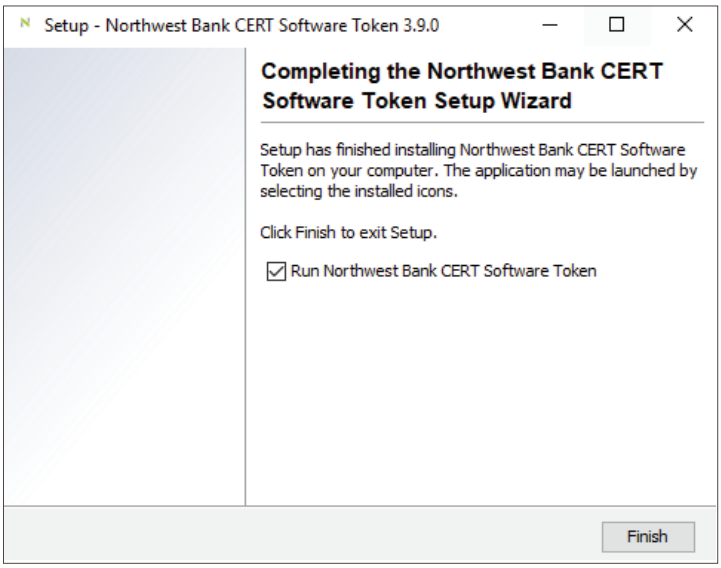
A shortcut in the **Windows Start Menu** folder will begin installing.



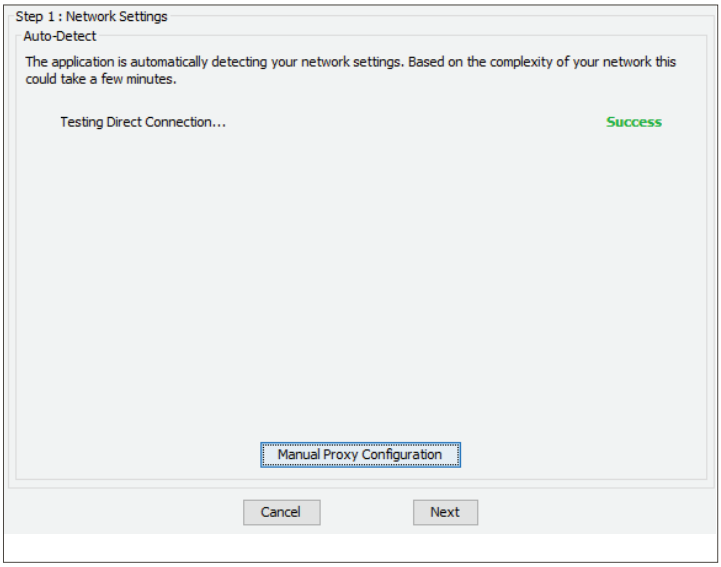
Upon installation, the system will display a green progress bar as the process advances, listing the files being installed.



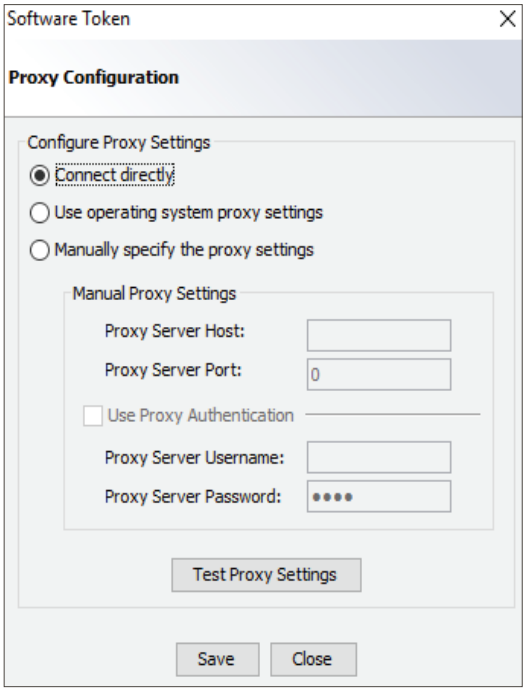
After the files are installed, a window will present stating the setup has finished installing. Select **Finish** to register the Soft Token.



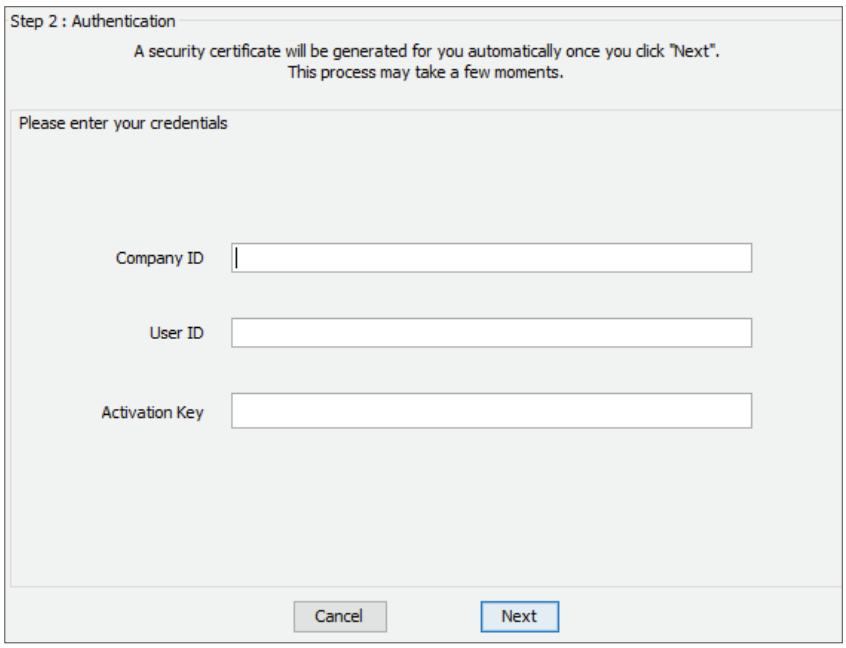
The next step in the installation process is for the system to Auto-Detect communication between Soft Token and Online Messenger. If the connection is successful, select **Next** to continue.



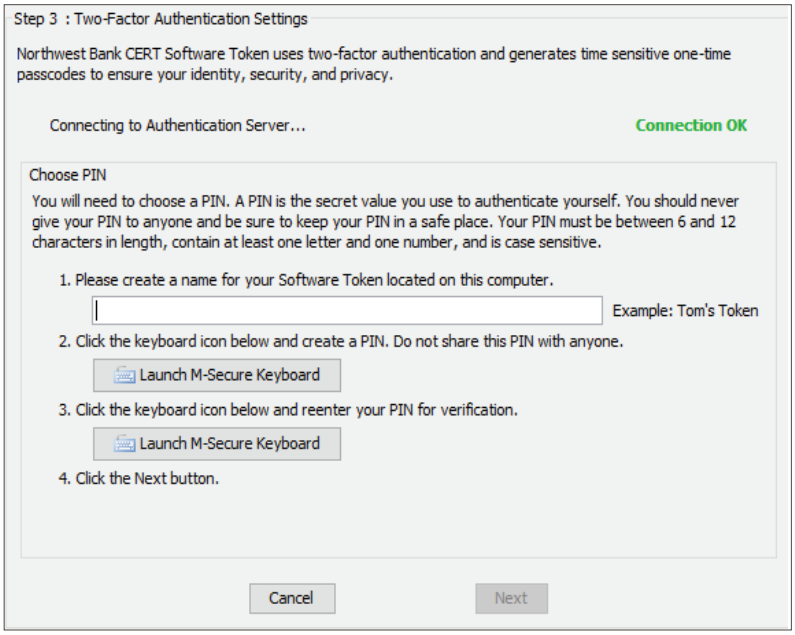
If there is a firewall in place, communication may need to be manually configured. Access to a proxy server requires providing the proxy server host name or IP address and the port number. If authentication is required, select the **Use Proxy Authentication** checkbox and enter the proxy server username and password.



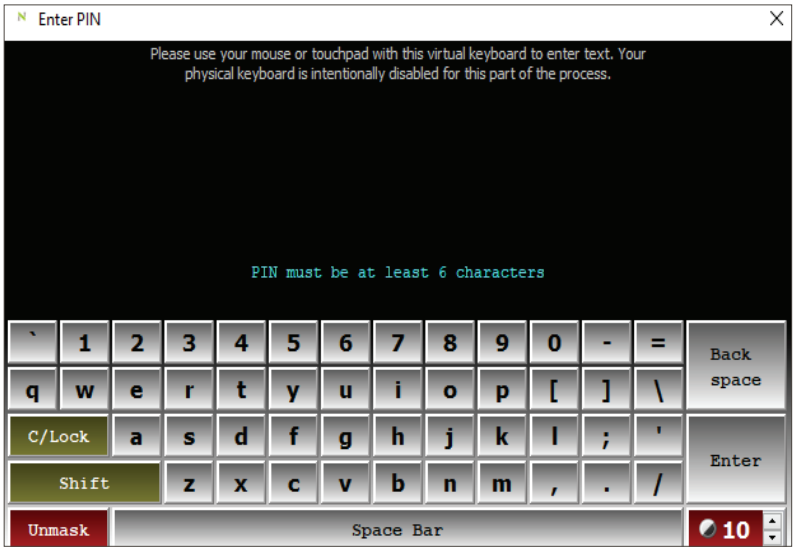
The user must enter their **Company ID**, their **User ID**, and their **SAK** (see the **Software Activation Key** section of this document for additional information).



The user will be prompted to name the Soft Token and create a **Personal Identification Number (PIN)** to be used at login. The PIN must consist of 6-12 alphanumeric characters, at least one upper case and lower case letter, and a number. The **Launch M-Secure Keyboard** button opens a virtual keyboard that encrypts keystrokes. Using this, enter a PIN, re-enter the PIN to ensure there were no keying errors, and select **Next** to continue.

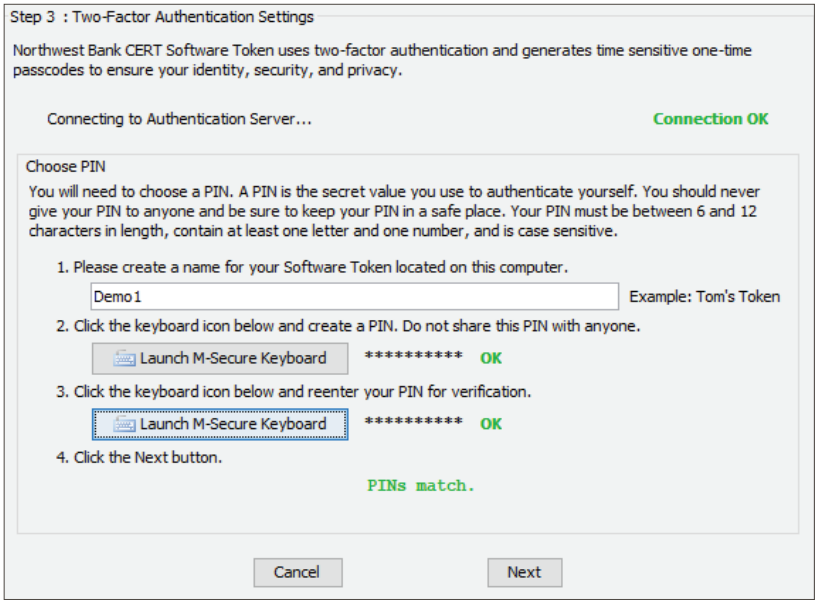


When the user launches the **M-Secure Keyboard**, they will be presented with a black screen and keyboard accessible only by mouse (or touchscreen if applicable), as the physical keyboard is intentionally disabled. Users may opt to utilize the **Unmask** button to ensure they have created the PIN correctly.

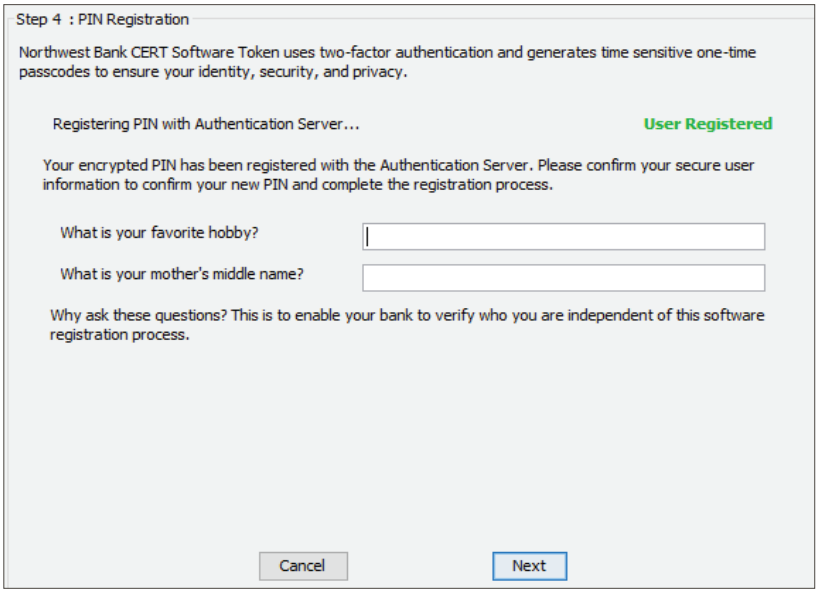


The user will follow the same steps when prompted to **Verify** the PIN.

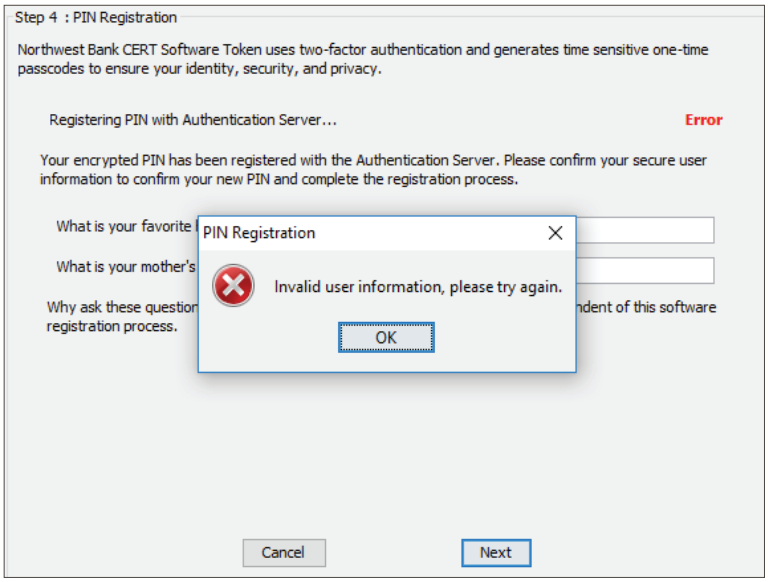
If all the information was entered correctly, the user will be presented with confirmation messages in green and any errors will be presented in red.



The last step to complete the PIN registration process is to verify user identity by answering two security questions, these are the same questions and answers found on the user profile.



If the information entered does not match the user profile, the error *Invalid user information, please try again* will present.

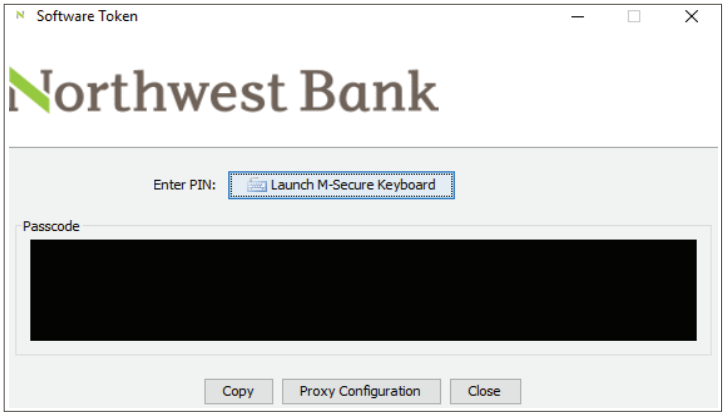


If there are no errors, the installation process has been completed.

Note: To launch the M-Secure Keyboard after installation, there should be a shortcut to the token on the desktop. If not, for Windows 7, go to the **Start Menu**, locate and select the Launch M-Secure Keyboard button. For Windows 10, go to **Recently Added**, locate and launch. The Soft Token can also be located in programs, C: Drive and pin to the desktop.

Using the Soft Token

To use the Soft Token, launch the application, and **Enter PIN** using the **M-Secure Keyboard**. All generated passcodes expire after 60 seconds.



Payment Processing and Payment Approval

Dual custody clients who use ACH Payments and/or Wire Transfers must authentic (re-verifiy) upon creation and approval of payments before payments can be released for processing. Default browser clients have one of two options for reverification, Soft Token or Out-of-Band PIN to generate and Out-of-Band passcode. Clients who are on single custody will only be prompted for reverification upon the creation of payments. Users can access their reverification preferences under **My Profile, My Credentials, Reverification Preferences**. Soft Token is not supported in Secure Browser and is not an applicable reverification option for Secure Browser clients.

Forgotten PIN

There is no PIN reset for Soft Token. In the case of a forgotten PIN, clients have to uninstall and reinstall the Soft Token or find and remove the file with the name ending in ".wkt" (for WiKID Token). The PIN is integral to the token identity, therefore resetting a token simply destroys the old token and creates a new one. This process is completed by an uninstallation and reinstallation. After the Soft Token is uninstalled, or the file is deleted, clients must follow the same installation process to create a new Soft Token.