First Mid
BANK & TRUST

First Mid Bank & Trust
Commercial Online Banking

Secure Browser Installation Guide for Windows

First Mid
BANK & TRUST

Commercial Online Banking Secure Browser

Commercial Online Banking Secure Browser is a secure solution that helps to provide a hardened stance against fraud. From new client implementation to ongoing support, COMMERCIAL ONLINE BANKING SECURE BROWSER offers a smooth customer experience.

- Secure Site Access with consistent user & device authentication
- Not susceptible to malware attacks
- Prevents misdirection of users to false sites
- Reduce risk by avoiding sites with malware
- Eliminate hard tokens or 3rd party security products
- Supports SMS or text and one-time passcodes
- Data integrity
- Limits user access to sites, functions, transaction entry and approval
- Supports web and mobile devices

Getting Started - Installation

In order to access Commercial Online Banking, users must install the **Secure Browser** on your PC. First Mid's **Secure Browser** is a java-based application that runs on a user's computer and which provides a captive, safe environment for accessing Commercial Online Banking and other web sites or server-based applications that are permitted to the company by First Mid Bank & Trust. The Secure Browser is a fully self-contained browser that does not use any other commercial browser previously installed on a user's computer, thereby insulating it from any malware that might be attached to those other browsers. Users are allowed access to only web sites and applications (Destinations) defined and configured by the bank. The Secure Browser does not employ an address line, so it is impossible for users to navigate away from entitled sites. **All users are required by First Mid Bank & Trust to use the Secure Browser to access Commercial Online Banking.**

Before You Begin

Ensure You Have:

- Internet connection
- Administrative privileges on the computer where the Secure Browser will be installed
- If you have Anti-Virus software installed, it must allow the Secure Browser to be installed. Contact your IT department to have this site whitelisted.

System Requirements:

NOTE: 32- and 64-bit operating systems are supported.

You can follow these steps to determine which Windows operating system you are using:

1. Click "Start" on your computer.
2. Right click on "My Computer".
3. Select "Properties".
4. In the "System" section, the "System Type" will be listed as either 32-bit Operating System or 64-bit Operating System.

- Windows 7
  - 1 GHz or more SSE2 capable Intel Pentium 4 microprocessor (or later)
  - 2GB of RAM
  - 16 GB (32bit) or 20 GB (64bit) of Hard Drive space (minimum)
- Windows 8, 8.1, and 10
  - 1 GHz or more SSE2 capable Intel Pentium 4 microprocessor (or later)
  - 2GB of RAM (32bit) or 4GB of RAM (64bit)
  - 16 GB (32bit) or 20 GB (64bit) of Hard Drive space (minimum)

  NOTE: The Secure Browser can be installed on Microsoft-manufactured Surface Laptop and Surface Pro (tablet) devices if the full version Windows 10 Pro operating system has been installed. Windows 10 S, the operating system that comes pre-installed on these devices, is not supported as it only allows applications obtained from the Windows Store to be installed.
- Remote Desktop and Virtual Machine installations are supported in most cases. Terminal Servers and installation in environments that use folder redirection are not supported.

Keyboard Compatibility

Computers must have a Personal System/2 (PS/2) style or USB Human Interface Device (HID) keyboard installed.

No Support Provided

We do not support installing the 64-bit version of CCS on a 32-bit version of Windows. We do not support Installing the 32-bit version of CCS on a 64-bit version of Windows.

The following platforms do not support CCS:

- Windows Server
- Windows Phone or Windows 10 Mobile
- Windows 10 S (preinstalled on 2017 Surface Laptop and Surface Pro hardware)

Simple Remote Desktop Protocol (RDP) and virtual machine installations support CCS in most cases. However, we do not support installing in Remote Desktop Services (RDS, formerly Terminal Services) and multi-user thin-client virtual desktop infrastructure (VDI) environments due to common issues with keyboard encryption, snapshot management and folder redirection, depending on how you configured the environment.

Anti-Virus Compatibility

Commercial Center℠: Security is NOT compatible with anti-virus products that utilize Device Control software. The extensive modifications made by this software to the Windows USB device driver and services stack render the system incompatible with the standard methods used to install the encrypted keyboard driver (EKD) included with Commercial Center℠: Security.

If the EKD is installed on systems that have been exposed to Device Control software, the previously modified driver and services stack can become corrupted, resulting in serious system stability/usability issues. Symptoms include:

- Unresponsive keyboards and mice
- Disabled USB ports
- Non-functioning USB devices such as printers or USB storage devices (flash drives, external hard drives, etc.)
- Fatal Encrypted Keyboard error messages during Commercial Center℠: Security start-up

Commercial Center℠: Security should not be installed on any PCs that currently have or have ever had Device Control software installed. These issues may persist even after the incompatible software is uninstalled. Some products that use the Device Control technology do not fully or cleanly uninstall the Device Control files and settings, and fail to restore the system to its normal state upon product removal. Full recovery from these issues may require reinstalling the Windows operating system.

The following antivirus software has been identified as having Device Control software, and there is known to be incompatible:

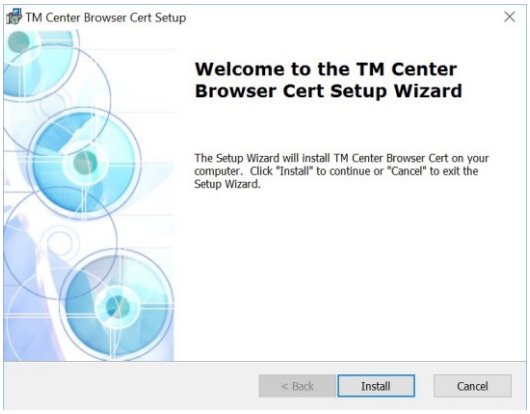
- Lumension Device Control module for Lumension Endpoint Management and Security Suite (a.k.a. Lumension Endpoint Security Device Control, LES DC)
    - All versions
- Ivanti Endpoint Security Device Control (a.k.a. HEAT Endpoint Security Device Control) and all Ivanti products that integrate the Device Control technology
    - All versions
- ThreatTrack Security VIPRE Antivirus Business Premium
    - All 7.5.x versions subsequent to and including 7.5.5819
- ThreatTrack Security VIPRE Endpoint Security, ThreatTrack VIPRE Advanced Security, and any VIPRE product that incorporates the Device Control technology
    - Versions 9.6 and later

Any product using the same licensed Device Control technology as the products above but not specifically listed here.

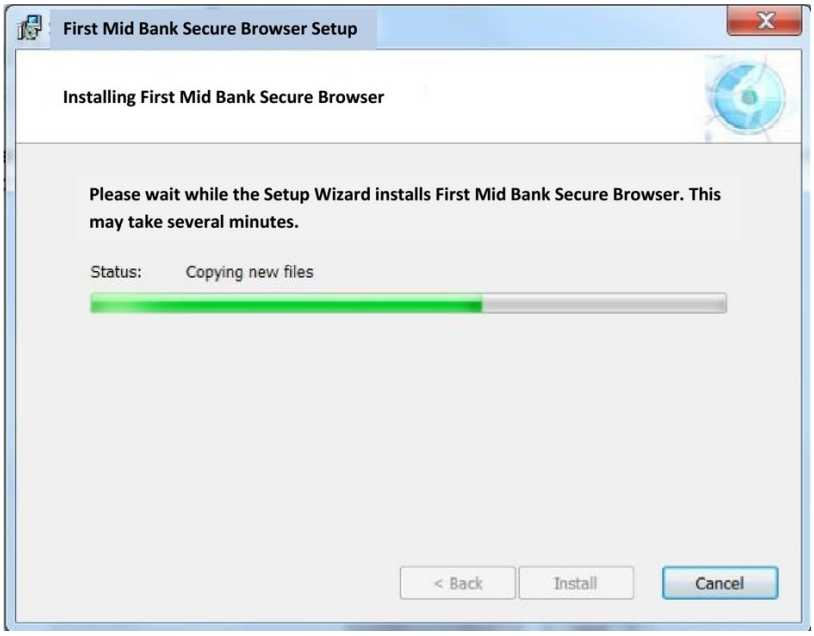
Each Commercial Online Banking user will be required to install the Secure Browser.

Please **choose the secure browser link for your computer system** by clicking HERE and select the “Download First Mid Commercial Online Banking Secure Browser” link (first option).

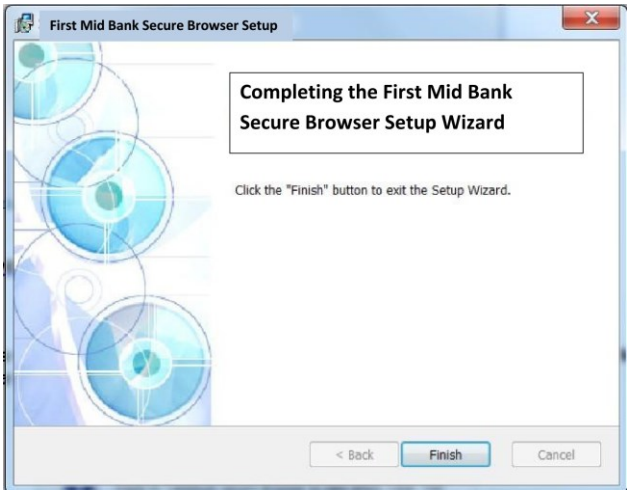
After clicking the link, you will see the following page. Select **Install** to continue.



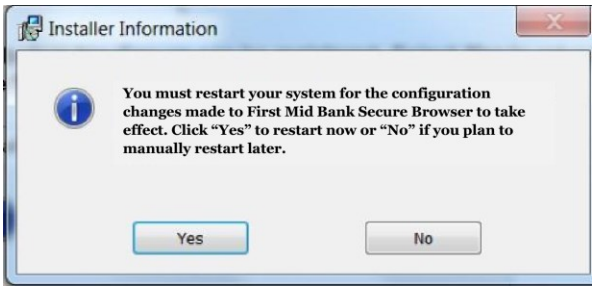
The Secure Browser will begin installing its files and folders. If prompted, confirm that Secure Browser should be allowed to make changes to the PC.



Select **Finish** once the installation has completed.



A reboot is required before The Secure Browser can be registered. Select **Yes** to reboot now, or **No** to reboot at a later time.



Important: If your computer contains malware, the Secure Browser Installer will detect this and will not complete installation. Please contact your company's IT department to remove any malware before trying to install again.

Activation/Registration

After you have downloaded and installed the secure browser, a computer restart will be required before completing activation.

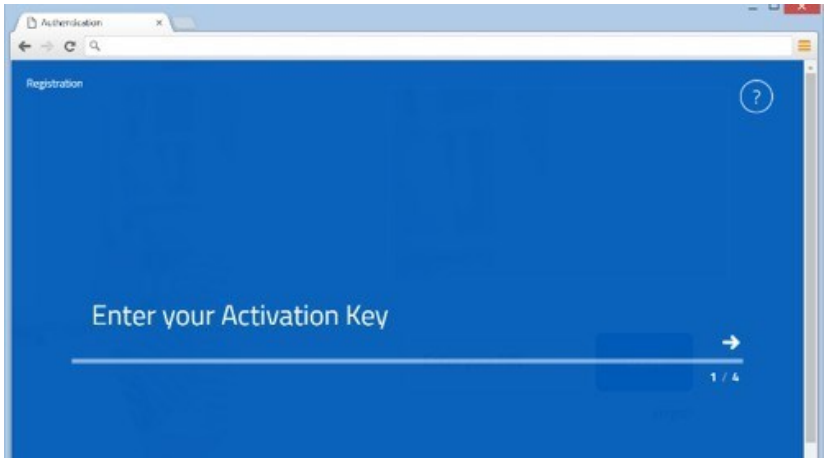
To activate/register your secure browser, ensure you have the following:

- Internet connection
- **Administrative privileges** on the computer where First Mid Secure Browser will be installed
- Activation Key – provided by **treasuryservices@firstmid.com**

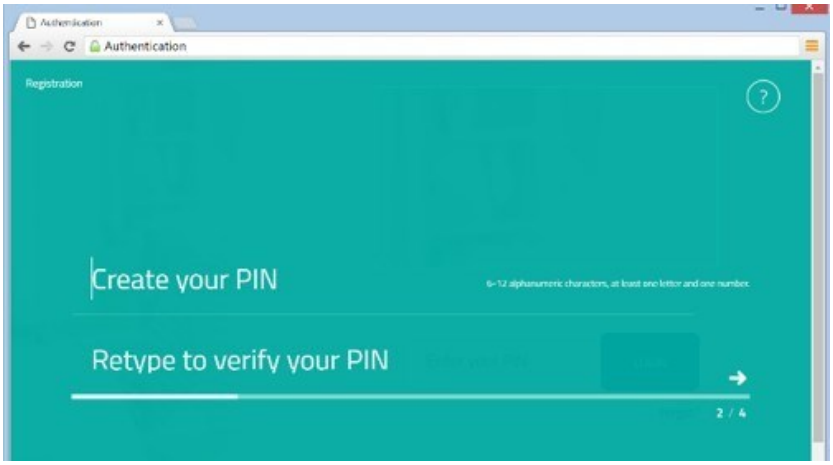
To Begin Registration

After performing the reboot, launch **Secure Browser** by locating and selecting the new **icon** that has been created on the desktop.

Enter the **Activation Key** that has been provided by the bank and select the **Continue arrow.**

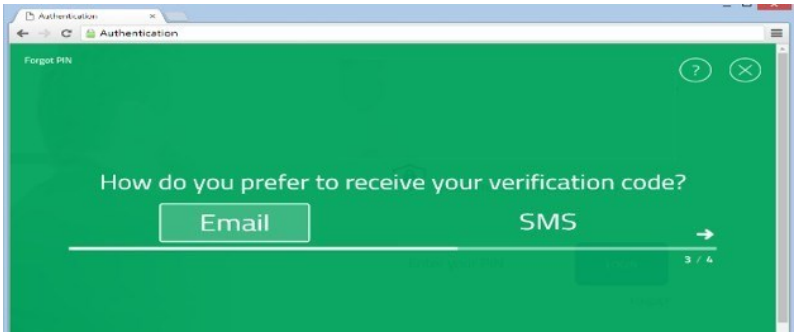


Next create the **PIN** to use for login, and select the **Continue arrow.** Please make note of the PIN as you will use it to log on following registration. **PIN must be between 6 to 12 characters, letters and numbers only.**

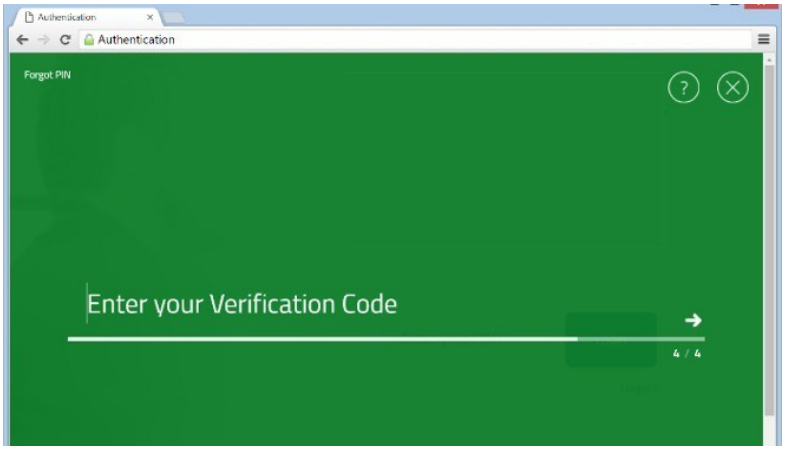


To confirm your identity, a user verification code will be delivered to you that must be entered on the next screen. Select if this code should be delivered via **Email** or **SMS**, then select the **Continue arrow.**

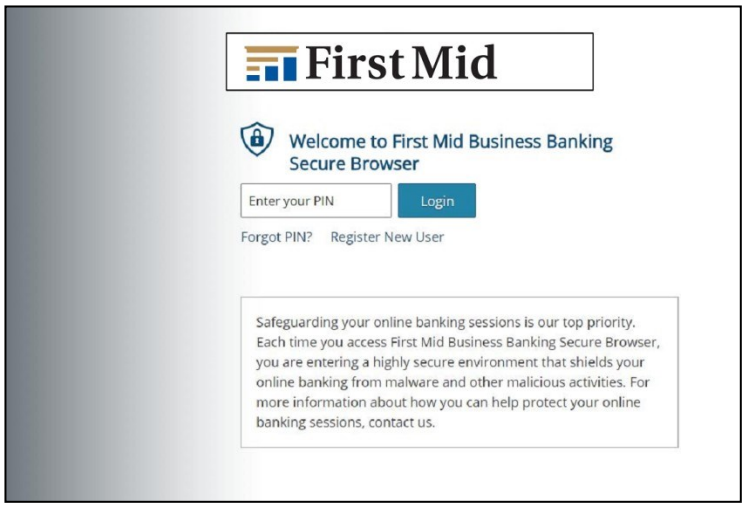
Note: **Email** is the preferred method.



Enter the user verification code that has been delivered, and then select the Continue arrow.



Installation and registration are now complete. Use the PIN that was created in activation/registration step 2 to login and access online banking.



Commercial Online Banking Secure Browser Homepage

Moving around through Navigator is very intuitive. From the **Messenger Center**, you are able to select from a customized selections menu. The same selections appear within the URL drop down.

Additional Users: Additional users may use the same secure browser, but will need to be added by a user with Administrative rights.

Our business is supporting your business. That's why we're here to answer your questions and assist with your business transactions.
For Technical Support:
1-833-680-5110
Monday – Friday 8:30 a.m. – 5:00 p.m. (CST)
treasuryservices@firstmid.freshdesk.com