OTCnet System Requirements & Reference Guide

Release 4.13
June 2025

Contents

System and Configuration Requirements

This document provides system and configuration requirements for the use of OTCnet Online for Deposit Reporting, Check Capture, and Card Processing. This document also provides system and configuration requirements for OTCnet Offline, which is available for users performing Check Processing or Check Scanning in areas with low bandwidth and/or unreliable internet connectivity.

OTCnet General Requirements

This section details the system and configuration requirements necessary to utilize all OTCnet functionality. Additional requirements are necessary for OTCnet Check Capture. Refer to the "Check Capture" section for more information.

Operating System and Java Environment

The following Operating Systems and Java Environments are supported by OTCnet:

- Windows 11 and Windows 10 (OTCnet supports the 64-bit version of the operating system)
- Java 8, 11, 17, or 21. OTCnet supports:
  - JDK distributions from Oracle (paid licenses)
  - JDK and JRE distributions from Adoptium and Amazon Corretto (open source licenses)

System Requirements

The following are requirements necessary to operate OTCnet:

- **Web Browsers:**
  - Microsoft Edge (Version 79 or higher)
  - Google Chrome (OTCnet supports the 64-bit version)
  - **PDF Documents Setting:**
    - Disable the PDF Documents Setting within your browser to see PDFs in the PDF preview pane.
    - If the PDF Documents Setting is enabled, reports can only be opened for download and are not displayed within the application.
    - This option can be found in Chrome browser by navigating to: Chrome browser > 3 vertical dots in upper right > Settings > Click on "Advanced" > Site Settings (under "Privacy and security") > PDF documents (under "Permissions").
- **Entrust Root Certificates:**
  - The following two certificates must be installed in the certificate store on your workstation. These certificates are typically installed by default with the operating system or browser. If they do not exist or have been removed, you will need to have your agency install the certificates:
    - Entrust Certification Authority - L1K – install in "Intermediate Certification Authorities" certificate store on the local machine.
    - Entrust Root Certification Authority - G2 – install in "Trusted Root Certification Authorities" certificate store on the local machine.
  - The following certificate must be manually installed: RDM Update Root Certification
- **Internet Options Security Settings:** To ensure connectivity to OTCnet, the "**Use TLS 1.2**" and/or **"Use TLS 1.3"** option(s) must be enabled for all workstations using Windows 10 or Windows 11.
- **Ports:** Router/Firewall Administrators must ensure and verify that outbound ACL (Access Control List) has complete https access, on port 443.
- **Workstation Memory:** 2 GB physical memory is required; 4 GB is recommended.
- **Free Disk Space:** 100 MB of free disk space is required.
- **Screen Resolution:** The recommended minimum resolution for OTCnet is 1024x768.
- **Java Versions:** Java versions 8, 11, 17, or 21 are necessary for check processing and card processing. OTCnet supports JDK distributions from Oracle and JDK/JRE distributions from Adoptium and Amazon Corretto.

Other Requirements

- **Access to OTCnet:** OTCnet Online can only be accessed using **PIV**, **PIV-I**, **CAC** or **ID.me**. Users who were issued PIV or CAC credentials must use their PIV/CAC credentials to access OTCnet. Users who were not issued (or whose organization cannot issue) PIV, PIV-I or CAC credentials must use ID.me to access OTCnet. Note that users issued with PIV or CAC credentials are not authorized to use an ID.me account to access OTCnet.
- **New users (PIV/CAC)**: New users to OTCnet who are PIV/CAC users must perform the following steps to gain access to OTCnet:
    1. Access https://www.otcnet.for.fiscal.treasury.gov using the PIV/CAC option on the OTCnet login page. If this is the first time the user has accessed any Fiscal Service system, service or application using their PIV/CAC credentials, they will be prompted to enter their email address, and once entered, an authorization code will be sent to this email address. The code must be entered to create their Fiscal Service CAIA identity; the user will see the following message: "***An entitlement request has been submitted to enable privileged access to OTCnet***."
    2. After performing step 1, the user must contact their OTCnet PLSA or LSA and ask them to assign the authorized OTCnet role(s) and high-level OTCnet organization(s) to their Fiscal Service CAIA identity.
    3. Once the PLSA/LSA informs the user that they have completed step 2, the user must log into OTCnet again: https://www.otcnet.for.fiscal.treasury.gov. Upon doing so, the user will see the message: "***Thank you for logging into OTCnet. You have completed the steps to request access to the application.***"
    4. After the user completes step 3, they must contact their PLSA/LSA again and ask them to assign the authorized OTCnet roles and endpoints to their OTCnet account. Once the PLSA/LSA completes this task, the user will have full access to OTCnet. After access is gained, the user will receive an email titled **"Welcome to OTCnet."**

  *The PLSA/LSA may assign the new user's roles and endpoints in advance by using the "Import User" functionality in the OTCnet application in lieu of completing Steps 3-4.
- **New users (ID.me)**: New users to OTCnet who are existing or new ID.me users must perform the following steps to gain access to OTCnet:
    1. Access https://www.otcnet.for.fiscal.treasury.gov using the ID.me option on the OTCnet login page. If the user does not have an existing ID.me account, they must click on the "**Create an ID.me account"** link on the ID.me login page to create their ID.me account, ensuring that they use their work email to create the account. ID.me account creation requires selecting an MFA option (see table below) and performing identity proofing. Identity proofing is a one-time process requiring the user to enter their SSN and to submit a picture/scan of a valid government ID (e.g., a passport or driver's license) and a selfie photo to confirm the user's identity. Upon successful ID.me account creation (for new ID.me users) or successful authentication (for existing ID.me account users), the user will see the following message: "***An entitlement request has been submitted to enable privileged access to OTCnet***."
    2. After completing step 1, the user must follow steps 2 through 4 detailed in the "**New users (PIV/CAC)**" section.
- **Multi-Factor Authentication (MFA)**: As described above, OTCnet Online users who are ID.me users will be prompted to set up multifactor authentication when creating their ID.me accounts. Listed below are the ID.me MFA options with the corresponding requirements:

ID.me MFA option	Requirements
1. Device Unlock: Complete sign in using your computer, smartphone, or tablet.	A computer or mobile device (smartphone or tablet).
2. Push Notification: Receive a notification via your ID.me Authenticator app on your mobile device and press to confirm.	A mobile device and the ID.me Authenticator app.
3. Code Generator: Enter a 6-digit verification code found in the ID.me Authenticator (or other TOTP authenticator) app.	A mobile device and the ID.me Authenticator app, or a TOTP authenticator app running on a desktop/computer or mobile device.
4. Text Message or Phone Call: Receive a text or phone call and enter the verification code.	A mobile phone that accepts text messages or phone calls or a landline phone.

ID.me MFA option	Requirements
5. FIDO Security Key: Use a physical security key (insert or tap) with your device.	A USB/YubiKey security key
6. NFC-Enabled Mobile Security Key: Enroll a YubiKey security key for secure mobile authentication.	A mobile phone that supports NFC, with the ID.me Authenticator app installed and NFC-enabled YubiKey security key

- All OTCnet users are required to use MFA to access OTCnet. Please see the user description below with corresponding permitted MFA options.

User Description	Allowable MFA option
User who has PIV, PIV-I or CAC credentials	PIV/CAC
Financial or Fiscal agent user for BFS who does not have PIV/CAC credentials and who is restricted from using mobile devices in their operating environment	ID.me MFA option 1 (using computer only) ID.me MFA option 5 (YubiKey)
User who *is not* a Financial or Fiscal Agent for BFS and who does not have PIV/CAC credentials, but who is restricted from using mobile devices in their operating environment	ID.me MFA option 1 (using computer only) ID.me MFA option 3 (using desktop authenticator app) ID.me MFA option 4 (using landline phone only) ID.me MFA option 5 (YubiKey)
User who is not a Financial or Fiscal Agent for BFS and who does not have PIV/CAC credentials	All ID.me MFA options: ID.me option 1 ID.me option 2 ID.me option 3 ID.me option 4 ID.me option 5 (YubiKey) ID.me option 6 (YubiKey NFC)

- For more information and step-by-step guides on how to register with OTCnet, please view the OTCnet Training Website.
- Supported File Formats: OTCnet Reports are only made available in Adobe PDF, Microsoft Word, and Microsoft Excel file formats. To view reports, ensure that your workstation has these programs installed. Google Chrome or Microsoft Edge users can view PDF files in their browser.

OTCnet Local Bridge (OLB) System Requirements

OLB Prerequisites
The OLB is an application which must be installed on all workstations performing Check Capture, Check Processing, Card Processing, OTC Kiosk Tablet transactions, and terminal configuration operations.

- OLB v2.7.0.1 will require Java Runtime Environment (JRE) or Java Development Kit (JDK) version 11, 17, or 21 to be installed and managed on all workstations requiring the OLB.
- Older OLB versions will still be supported by older Java versions. If you wish to continue using JRE/JDK version 8, you will need to use the previous OLB v2.6.0.5.

Installing the OLB
During installation, the OLB application is configured to use JRE or JDK. The latest OLB version 2.7.0.1 is compatible with JRE/JDK versions 11, 17 or 21. It is not compatible with Java version 8.

If you recently upgraded to Windows 10 or Windows 11 and the OLB desktop icon no longer successfully starts the OLB, please reinstall the OLB before attempting to start the OLB again. You will need to reconfigure the OLB startup property file (as shown above) with the Java runtime location if you are using an external (i.e., workstation installed) Java runtime with the OLB.

For more information and step-by-step guides on how to download and install the OLB, visit the following webpages:

- Download, Install, and Upgrade the OTCnet Local Bridge (OLB) Application Training Module: https://fiscal.treasury.gov/otcnet/training/wbt/content/MOD08/08.01/story.html
- OTCnet Local Bridge (OLB) Information and Resources: https://fiscal.treasury.gov/otcnet/local-bridge-information-resources.html

- OTCnet Training Website - Printable Job Aids and simulations for downloading, installing, and starting the OLB (Modules 2.1, 8.1):
https://fiscal.treasury.gov/otcnet/training/wbt/content/course_OTC/menu_all.htm

Upgrading the OLB
The newest OLB (v2.7.0.1) requires Java 11, 17, or 21 to run the upgraded version. OLB v2.7.0.1 is not compatible with Java version 8. It is strongly recommended that you have the latest OLB version installed on your workstation, if possible. Older OLB versions will still be supported by older Java versions.

For more information and step-by-step guides on how to upgrade the OLB, visit the following webpages:

- Download, Install, and Upgrade the OTCnet Local Bridge (OLB) Application Training Module:
https://fiscal.treasury.gov/otcnet/training/wbt/content/MOD08/08.01/story.html
- Upgrade the OTCnet Local Bridge (OLB) Application Printable Job Aid:
https://fiscal.treasury.gov/otcnet/training/wbt/content/_resources/PJA/pja_upgrade_olb_app.pdf
- OTCnet Local Bridge (OLB) Application FAQ:
https://fiscal.treasury.gov/files/otcnet/OTCnetLocalBridge(OLB)RolloutFrequentlyAskedQuestions.pdf

OTCnet Check Processing Requirements
This section outlines additional requirements necessary to perform OTCnet Check Processing.

Additional System Requirements
A Windows Administrator (who is logged onto the OTCnet workstation as a workstation administrator) must perform the following tasks to comply with the Check Processing requirements:

- **Install Scanner Drivers:** A Scanner Driver and Firmware (provided in an installation file) must be installed on the workstation. Instructions for obtaining and installing the installation file and further information can be found in the Technical Reference Guide.
- **Ensure Adobe and Adobe Reader's Compatibility with OTCnet:** All versions of Adobe are compatible with OTCnet, although Adobe X may require web browser configuration changes. Google Chrome or Microsoft Edge users may view PDFs in-browser. Adobe Reader Version 7 or higher is required.

Section 508 of the Rehabilitation Act of 1973 requires federal agencies to ensure their information technology is accessible to individuals with disabilities.

Commercially available screen readers, such as NVDA, JAWS, and Narrator, are compatible with Google Chrome and MS Edge browsers and respective operating systems and can be used successfully with OTCnet. There may be subtle differences in the users' experience based on the choice of screen reader, but OTCnet is designed and developed to produce the best possible experience for the largest possible audience.

Assistive Technology (AT) Users must perform the following tasks:

- Configure the OTCnet terminal to allow receipt printing automatically.
- Install Java 8, 11, 17, or 21.
- Install Java Access Bridge on workstations for Check Processing Offline to support the reading of browser pop-up windows.
- Use JAWS 16 or higher with Java Access Bridge 2.0.2. Java Access Bridge is included in the Java SE Runtime Environment.
- To Verify Java Access Bridge is enabled in Window OS:

    1. Go to Start > Control Panel > Ease of Access > Ease of Access Center.
    2. Select 'Use the computer without a display.'
    3. In the section 'Other programs installed' select the check box 'Enable Java Access Bridge' (you may have to scroll down).

Note: *After enabling Java Access Bridge, restart Assistive Technology (AT) software (JAWS) and Java applications (OLB or Offline) that use the accessibility API.*

- If a standalone Java Access Bridge version is required, follow instructions on installing the Java Access Bridge: https://fiscal.treasury.gov/files/otcnet/InstallationStepsforJavaAccessBridgewithJAWS16.pdf
- Alternatively, enable the Ease of Access Narrator by pressing Windows logo Key +U, and select 'Narrator' in Settings.

Additional Resources: JAWS information, Narrator Keyboard Commands, Basic Accessibility Guidance, and other Accessibility resources can be found on the OTCnet Resources page.

Check Capture Hardware Requirements

The following hardware is necessary for OTCnet Check Processing:

- Access a printer from the workstation where you will be using OTCnet for Check Processing.
- A compatible check scanner connected to the workstation with an available USB 2.0 or 3.0 port.
- The following table lists OTCnet compatible hardware and indicates what Firmware is required for each hardware and operating system.
- The OTCnet firmware file is downloaded from OTCnet by the **Check Capture Administrator**.
- The drivers for the scanners are included in the OTCnet Firmware, no separate installation is needed.

Check Capture Requirements	
Operating System	Windows 10, Windows 11
Browser	Chrome, Microsoft Edge (Version 79+)
Firmware	4.3.0, 4.4.0[1]*
Scanner Models Supported[2]	RDM EC7000i Panini MyVision X RDM EC9100i Panini Vision X RDM EC9600i Panini Vision 1 RDM EC9603 Panini I:Deal RDM EC9700i
OLB Version	2.6.0.3 2.6.0.5 2.7.0.1
Compatible External JRE Required	JRE 8[5] 64bit, JRE 11, JRE 17, JRE 21
Java Applets / Java Runtime Support	Not Supported

Please see the table below for prerequisite packages required for each firmware version.

Firmware Version by Scanner and Operating System		
Operating System	Windows 10, Windows 11	
Microsoft .NET Framework	4.5.2 or newer	
OTCnet Firmware	4.2.0	4.3.0, 4.4.0
Microsoft Visual C++ Redistributable Package	VC++ 2015-2019 (x64)	Installed by Firmware Installer.

---

[1] Firmwares 4.3.0 and 4.4.0 are only compatible with OLB versions 2.3.0 and above. Firmware 4.4.0 is required for the RDM EC9600i and EC9700i scanner models. We recommend upgrading to the latest firmware and OLB version.
[2] All RDM devices are no longer available for sale. Existing devices will remain compatible with OTCnet.

	VC++ 2015-2019 (x86)	Requisites included by Firmware Installer.
	VC++ 2010 (x86)	Requisites included* *For issues with RDM 7000 scanner, Install VC++ 2010 (x86) redistributable package and reboot

OTCnet firmware versions 2.0.0-4.4.0 require VC++ redistributable packages to be installed prior to installing firmware. When users upgrade their firmware, we recommend installing the required VC++ redistributable package and rebooting their computer before upgrading their firmware and launching the OLB.

Download Links:

Microsoft Visual C++ 2010 SP1 (x86):   https://www.microsoft.com/en-us/download/details.aspx?id=26999

OTCnet Check Capture Offline Application Requirements

This section details the additional system and configuration requirements necessary to use OTCnet Offline, which is available for users performing Check Processing/Check Scanning in areas with low bandwidth and/or unreliable internet connectivity.

Offline	
Firmware and OLB Compatibility Matrix	
Offline Version	4.13.0
Operating System	Windows 10, Windows 11
Browser	Google Chrome, Microsoft Edge (Version 79+)[3]
Firmware	4.2.0, 4.3.0, 4.4.0
Scanner Models Supported	RDM EC7000i RDM EC9100i RDM EC9600i RDM EC9603 RDM EC9700i Panini MyVision X Panini Vision X Panini Vision 1 Panini I:Deal
Offline External JRE Compatibility	JRE 11

Additional System Requirements

The following system requirements are necessary to use the OTCnet Offline application.

- **Free Disk Space:** 600 MB additional disk space. 350 MB is required to install the application; 250 MB is recommended to accommodate transaction and audit log data.
- **Secondary Storage:** Secondary storage is required. An external hard drive or network drive with 150 MB free disk space or USB flash drive is advised.
- **Windows User Permissions:** OTCnet users must *not* have Windows administrator access to the workstation on which the Offline application is installed. In addition, all workstation users must have "write" permissions to the following subfolders within the Offline application's main installation folder:

    - *C:\ProgramData\OTCnet_prod\data*
    - *C:\ProgramData\OTCnet_prod\server*

---

[3] It is advised to set the default browser to the preferred browser (either Google Chrome or Microsoft Edge) for the Offline application.

All folders and subfolders within the main Offline application folder (except the two folders specified above) must be set to "read-only" permissions for all OTCnet users on the workstation. To ensure "read-only" permissions are set for the OTCnet root folder and its subfolders, apply the following permissions to the OTCnet root folder: "*Read & execute*," "*List folder contents*" and "*Read*," for all workstation users (typically applied for the "*Authenticated Users*" and "*Users*"/"Domain Users" groups on the workstation).

To set "write" permissions for the two folders specified above, you must apply the "*Modify*," "*Read & execute*," "*List folder contents*", "*Read*" and "*Write*" permissions to the two folders for all workstation users (typically applied for the "*Authenticated Users*" and "*Users*"/"Domain Users" groups on the workstation).

If upgrading OTCnet, set all OTCnet folders to "write," run the upgrade installer, then follow the above instructions to set the folder permissions accordingly.

Failure to follow this requirement may result in application exploits for which agencies will have to assume responsibility.

- **McAfee Exclusion:** McAfee Antivirus users that experience slow application startup times are advised to implement the following exclusions:

    Windows 10:
    C:\Users*\AppData\Local\Temp*\jetty-0.0.0.0-XXXX-otcnet-offline.war-_otcnet-any-\
    C:\Users*\AppData\Local\Temp*\JRCJNI\
    C:\OTCnet_prod\

The McAfee Exclusion C:\OTCnet_prod\ is based on the default install location for OTCnet. Users should apply the appropriate McAfee Exclusion above based on the install location of OTCnet selected during the installation process. During the installation process of OTCnet Offline, users have the option to select the location to install.

Users should apply the appropriate McAfee Exclusion above based on the Server HTTPS Port used in the OTCnet Offline installation process. During OTCnet Offline installation, users have the option to input the Server HTTPS Port or keep the default Port setting. The McAfee Exclusions above use the Server HTTPS Port X; users must use Port input during the installation process.

OTCnet Card Processing Requirements

This section details the additional system and configuration requirements necessary to utilize OTCnet Card Processing, which is available for users accepting credit, debit, and gift card payments.

Card Processing Requirements	
Operating System	Windows 10, Windows 11
Browsers	Google Chrome, Microsoft Edge (Version 79+)
Firmware	N/A
Card Processing Terminal Supported[4]	Verifone M440
Receipt Printer	Any Windows printer that supports 8.5"x 11" paper or 80mm 3.125in printer (optional) for receipt printing
OLB Version	2.6.0.5 2.7.0.1

OLB Compatible External JRE Required	JRE 8[5] 64bit, JRE 11, JRE 17, JRE 21

Additional System Requirements for Verifone Devices

The following system requirements are necessary to use OTCnet Card Processing.

Existing Verifone MX925 users will need to upgrade to OLB v2.6.0.2 and above to continue using existing card terminals. For more information on upgrading the OLB, please refer to the section above titled "Upgrading the OLB."

The port setting information below is the latest information from Verifone but is subject to change. Agencies should confirm the production port settings with Verifone for their Verifone terminal device before deploying in production.
Port Settings for PAYware Connect Gateway:
- Primary URL: https://vhq.verifone.com/MessagingServer/MessageHandler.asmx
- IP Addresses: 199.71.106.30, 199.71.107.160
- Port: 443

Additional System Requirements for 80 Millimeter (3.125 Inch) Receipt Printer Devices

Additional drivers may need to be installed for 80mm (3.125 in) receipt printer devices. Please refer to the vendor of your selected printer to determine additional driver information.

OTCnet Bandwidth Requirements
This section provides the minimum internet connectivity recommendations for setting up and utilizing OTCnet.

Bandwidth
- A 1.2 MBPS connection is recommended to download the OTCnet Scanner Firmware and the Offline client.
- A 512 KBPS connection is recommended to utilize the OTCnet Offline application when uploading batches.
- A 512 KBPS connection is recommended to utilize the OTCnet Online application.

Technical Reference Guide
This section provides further information to your agency's system administrator on the system and configuration requirements needed for OTCnet Online. Your agency's OTCnet Point of Contact (PoC) has the Deployment Specialist's contact information, should you require assistance.

OTCnet General Requirements

- **Entrust Root Certificate:** The following two certificates must be installed in the certificate store on your workstation. These certificates are normally installed by default with the operating system. If they do not exist or have been removed, you will need to have your agency install/re-install the certificates:
  - Entrust Certification Authority - L1K – install in "Intermediate Certification Authorities" certificate store on workstation.
    - https://web.entrust.com/root-certificates/entrust_l1k.cer
  - Entrust Root Certification Authority - G2 – install in "Trusted Root Certification Authorities" certificate store on workstation.
    - https://web.entrust.com/root-certificates/entrust_g2_ca.cer
  - RDM Update Root Certification – The following certificate must be manually installed.
    - https://downloads.itms-online.com/scm/SCM_RDM_Root_Cert_Update.exe

- **Internet Options Security Settings:** Multiple TLS (Transport Layer Security) versions may be available in your browser settings and at least one of these is normally enabled by default. You must ensure **"Use TLS 1.2"** and/or **"Use TLS 1.3"** is enabled to ensure connectivity between OTCnet and your browser.

Check Capture

- **Scanner Drivers (installation file):** Scanner driver and Firmware (provided in an installation file) must be installed on the workstation. Instructions for downloading and installing the installation file can be found in the OTCnet Printable Job Aids, Module 7.3:
    - Download Firmware & Install Firmware

To learn more, access the OTCnet website, email us at FiscalService.OTCDeployment@citi.com, or call 703-377-5586.