

OTCnet System Requirements and Reference Guide

OTCnet Release 2.4

Contents

System and Configuration Requirements	2
OTCnet General Requirements.....	2
Operating System.....	2
System Requirements.....	2
Other Requirements	2
OTCnet Check Processing Requirements.....	3
Additional System Requirements	3
Check Capture Hardware Requirements.....	4
OTCnet Check Capture Offline Application Requirements	4
Additional System Requirements	4
OTCnet Bandwidth Requirements.....	6
Technical Reference Guide	6
For More Information	6

System and Configuration Requirements

This document provides system and configuration requirements for the use of OTCnet Online for deposit reporting and check capture. This document also provides system and configuration requirements for OTCnet Offline, which is available for users performing check processing/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 “OTCnet Check Capture Requirements” and “OTCnet Offline Check Capture Application Requirements” sections for more information.

Operating System

The following Operating System is supported by OTCnet:

- Windows 7 (OTCnet supports both 32-bit and 64-bit versions of the operating system)
- Windows 8.1 (OTCnet supports the 64-bit version of the operating system)
- Windows 10 (OTCnet supports the 64-bit version of the operating system)

System Requirements

The following are requirements necessary to operate OTCnet:

- **Web Browser:** Internet Explorer 10 and 11 (OTCnet supports both 32-bit and 64-bit versions)
 - **Zoom:** Must be set at the web browser default (100% zoom). If zoom is not set to 100%, you may experience issues while using the OTCnet application.
- **Entrust Root Certificates:** 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 and/or Internet Explorer. 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
 - [Entrust Root Certification Authority - G2](#) – install in “Trusted Root Certification Authorities” certificate store on workstation
- **Internet Options Security Settings:**
 - To ensure the highest level of security, the “**Use TLS 1.2**” option should be enabled for all workstations using Windows 7 or higher. For detailed instructions on how to enable TLS 1.2, click or copy and paste the following link:
https://www.fiscal.treasury.gov/fsservices/gov/rvnColl/otcNet/pja_download_install_OTCnet_TLS_Update_09282015.pdf
 - The “**Use TLS 1.0**” option must be enabled in the Advanced Tab within Internet Options for all users who need to access ITIM (i.e. PLSAs and LSAs). ITIM currently only supports the TLS 1.0 protocol, although support for TLS 1.2 will be added in the near future.
- “**Use SSL 2.0**”, “**Use SSL 3.0**”, and “**Use TLS 1.1**” may need to be enabled if any of these settings are required for other applications or web sites.
- **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.
- **Window Resolution:** OTCnet’s supported resolution is 1024x768.

Other Requirements

- **Email Address:** Users must have access to a unique email address to change their initial OTCnet passwords and access the online system.
- **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.

OTCnet Check Processing Requirements

This section outlines additional requirements necessary to perform OTCnet check processing/check scanning. **These requirements are only necessary if OTCnet is utilized for check processing/check scanning.**

Additional System Requirements

The following system requirements are necessary for utilizing OTCnet check processing. These requirements must be performed by a Windows administrator (a user who is logged onto the workstation as a workstation administrator):

- **“Federal Common Policy CA” Root Certificate:** The “Federal Common Policy CA” Root Certificate (also known as the “U.S Government Common Policy” root certificate) must be installed in the “Trusted Root Certification Authorities” certificate store on the “local machine” (all user profiles) of the workstation. This certificate is normally installed by default on all government-owned (and most other) workstations. If the certificate doesn’t exist, it can be downloaded [here](#). Additional information and instructions for obtaining and installing the “Federal Common Policy CA” Root Certificate can be found on the [OTCnet Related Resources](#) webpage.
- **ActiveX must be enabled in browser:** This must be enabled for all user profiles on the workstation that use OTCnet. Instructions for enabling ActiveX are provided below in the Technical Reference Guide.
- **ActiveX Filtering must be disabled in browser (IE10 or 11):** If using IE10 or 11, ActiveX Filtering must be disabled. Further information is provided below in the Technical Reference Guide.
- **Scanner Drivers (.MSI installation file):** Scanner driver and Firmware (provided in an .MSI installation file) must be installed on the workstation. Instructions for obtaining and installing the .MSI file will be provided in a separate document. Further information is provided below in the Technical Reference Guide.
- **Java Runtime Environment (JRE), 32-bit:** The Java Runtime Environment (Java SE 6, Java SE 7, or Java SE 8) must be installed and enabled on the workstation.

It is recommended that the latest release of Java 8, 32-bit be maintained at all times to ensure the highest level of security and OTCnet Check Capture functionality for your workstations. To access information about the latest release of Java 8, click or copy and paste the following link:

<http://www.oracle.com/technetwork/java/javase/downloads/index.html>, and scroll to the section listing the latest Java 8 release. Reference your agency’s internal policies and procedures prior to taking any action.

Java 6 and Java 7 are no longer publically supported by Oracle and are no longer receiving new security updates. The content of some of the Java updates may cause issues and/or inconsistencies with some browser/workstation combinations and OTCnet check scanning. The chart below shows results of our latest Java compatibility testing.

Java Compatibility by Operating System		
	Java Version	Windows 7
Java 6	1.6.0_0 to 1.6.0_45	Limited Compatibility ¹
Java 7	Older Versions of Java 7	Limited Compatibility ^{1,2}
	Latest Version of Java 7	Compatible
Java 8	Latest Version of Java 8	Compatible

¹ You may be prompted to accept security warnings to continue using OTCnet when using an older version of Java.

²The Java security slider in the Java Control Panel may need to be set to **Medium** for these Java versions for OTCnet to function properly.

Java Expiration Dates

To improve Java security, Oracle has implemented an automatic "expiration" of the current Java version whenever a new release with security vulnerability fixes becomes available. The current Java version will automatically expire with the release of the next critical patch update. For systems without connectivity to Oracle Servers via the internet, a secondary mechanism containing a hard coded expiration date retires the previous version of Java one month after the latest scheduled critical patch update is released.

After a new release becomes available or a hard coded expiration date is reached, Java will provide additional warnings and reminders to users to update to the newest version. For information on Java security resources, visit: <http://www.java.com/en/security/>

- **Adobe: All versions of Adobe are compatible with OTCnet, although Adobe X may require web browser configuration changes.**
- **Adobe Reader: Adobe PDF Reader and the PDF Reader Plug-in must be installed on the workstation to support receipt printing. All versions of Adobe are compatible with OTCnet, although Adobe X may require web browser configuration changes. Adobe Reader Version 7.x or higher is required.**

Check Capture Hardware Requirements

The following hardware requirements are necessary for utilizing OTCnet check processing:

- Access to 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 port
- The following table lists the hardware that is compatible with OTCnet. The table also indicates which version of the driver and Firmware is required for each combination of hardware and operating system.

Firmware Version by Scanner and Operating System				
Scanner Type		Operating System		
Scanner Type	Model	Windows 7	Windows 8.1	Windows 10
RDM	EC7000 ^{1,2,3}	1.5.1, 1.6, 2.0.0	2.0.0	2.0.0
Panini	MyVisionX ⁴	1.6, 2.0.0	2.0.0	2.0.0
	VisionX ⁴	1.6, 2.0.0	2.0.0	2.0.0
	I: Deal	1.6, 2.0.0	2.0.0	2.0.0

¹ Supported connection via Serial COM port

² Supported connection via USB or Serial COM

⁴ Panini MyVisionX or VisionX scanners currently configured with Firmware 1.2.1 or 1.5.1 can continue scanning in OTCnet without issue. However, in order to select the VisionX option in the terminal configuration scanner drop-down, Firmware 1.6.0 or 2.0.0 must be installed

Note that Offline users will not be able to use Firmware 1.6.0 or 2.0.0 unless they download the Release 2.1 Offline application or higher. Furthermore, if using the VisionX scanner on Firmware 1.6.0 or 2.0.0, users must select VisionX from the drop- down menu. Users running Firmware 1.6.0 or 2.0.0 with the MyVisionX or VisionX scanners may receive two connectivity messages when the scanner's USB is first connected and after clicking **Start Scan**. Accept the messages and re-click **Start Scan**. If the messages persist, contact the Customer Support Team.

For agencies installing Firmware Version 2.0.0, there are two prerequisite VC++ redistributable packages that are required to be installed prior to using 2.0.0. The names and download links to these packages are detailed below:

- Microsoft Visual C++ 2005 SP1 Redistributable Package (x86): <https://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=5638>
- Microsoft Visual C++ 2010 SP1 Redistributable Package (x86): <http://www.microsoft.com/en-us/download/details.aspx?id=8328>

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. **These requirements are only necessary for the OTCnet Offline Check Capture Application.**

Additional System Requirements

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

- **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. It is recommended that an external hard drive or network drive is used instead of a local folder for storage on the individual Offline terminal. An external hard drive or network drive with 150 MB free disk space or USB flash drive is advised.
- **Java Access Bridge:** For 508 users, the Java Access Bridge must be installed on the workstation for Check Processing Offline to support the reading of a few browser pop-up windows. For 32-bit or 64-bit operating systems, JAWS 16 or higher must be used with Java Access Bridge 2.0.2 installed. For instructions on installing the Java Access Bridge, click or copy and paste the following link:
<https://www.fiscal.treasury.gov/fsservices/gov/rvnColl/otcNet/InstallationStepsforJavaAccessBridgewithJAWS16.pdf>
- **Security Update Installers – Security Update Installer 1.2.0 & OTCnet Security Update January 2014**
Agencies installing OTCnet Offline Release 1.4 after March 14, 2014 need to install the repackaged Release 1.4 Offline software, titled **OTCNET-1.4.0**, and the **Security Update Installer-1.2.0**.
- **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:\OTCnet_prod\data
 - C:\OTCnet_prod\log
 - C:\OTCnet_prod\server\logs

All folders and subfolders within the main Offline application folder (except the three 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 three folders specified above, you must apply the “*Modify*”, “*Read & execute*”, “*List folder contents*”, “*Read*” and “*Write*” permissions to the three 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 based on the Operating System used at the terminal.

Windows 7:

C:\Users*\AppData\Local\Temp*jetty-0.0.0.0-XXXX-otcnet-offline.war-_otcnet-any\
C:\Users*\AppData\Local\Temp*JRCJN\
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.

Also, note that users should apply the appropriate McAfee Exclusion above based on the Server HTTPS Port used in the OTCnet Offline installation process. During the installation process of OTCnet Offline, 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; however, users must use Port inputted during the installation process.

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/or the Offline client
- A 512 KBPS connection is recommended to utilize the OTCnet Online application
- A 512 KBPS connection is recommended to utilize the OTCnet Offline application when uploading batches

Technical Reference Guide

This section provides further information to your agency system administrator on the system and configuration requirements needed for the online use of OTCnet. **Check Scanning and Check Processing requirements are only necessary if OTCnet is used for check processing/check scanning.** 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: Entrust Root Certificates:** 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 and/or Internet Explorer. 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
 - [Entrust Root Certification Authority - G2](#) – install in “Trusted Root Certification Authorities” certificate store on workstation
- **Internet Options Security Settings: “Use TLS 1.0”** must be enabled in the advanced tab of Internet Options for all user profiles on the workstation. 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 1.0**” is enabled in order to access both ITIM and OTCnet from the same browser. If the workstation is using Windows 7 or higher, “**Use TLS 1.2**” must be enabled to ensure the highest level of security to use OTCnet.

Check Capture

- **ActiveX must be enabled in browser:** If you cannot add the OTCnet URL to the Trusted Sites Zone, or if your organization does not enable ActiveX in the Trusted Sites Zone for your workstations, you will need to enable ActiveX in all Zones for all user profiles on each OTCnet workstation in order to support check processing. Use the following browser settings to securely enable ActiveX:
 - Allow previously unused ActiveX controls to run without prompt -> **Disable**
 - Allow Scriptlets -> **Disable**
 - Automatic prompting for ActiveX controls -> **Disable**
 - Binary and script behaviors -> **Enable**
 - Display video and animation on a webpage that does not use external media player -> **Disable**
 - Download signed ActiveX controls -> **Prompt**
 - Download unsigned ActiveX controls -> **Disable**
 - Initialize and script ActiveX controls not marked as safe for scripting -> **Disable**
 - Run ActiveX controls and plug-ins -> **Enable**
 - Script ActiveX controls marked safe for scripting -> **Enable**
- **JavaScript must be enabled in browser:** If you cannot add the OTCnet URL to the Trusted Sites Zone, or if your organization does not enable JavaScript in the Trusted Sites Zone for workstations, you will need to enable JavaScript in all Zones for all user profiles on each OTCnet workstation to use check processing.
- **ActiveX Filtering in browser (IE10 or 11):** If using IE10 or 11, ActiveX Filtering must be disabled.
- **Scanner Drivers (.MSI installation file):** Scanner driver and Firmware (provided in an .MSI installation file) must be installed on the workstation. Instructions for obtaining and installing the .MSI file can be found in the OTCnet Web Based Training, Module 6.3: [Download and Install Firmware](#).

For More Information

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