

OCFS Apple iPad-2 Pilot User Quick Guide

Final Documentation for Apple iPad-2 Pilot

July 2012



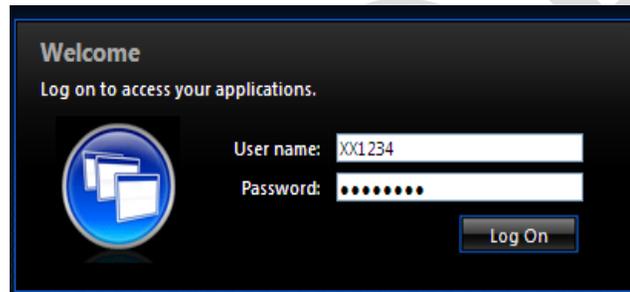
Note: Before using your new Apple iPad-2 device, please check with your LAN Administrator for registration and setup.

To access CONNECTIONS

Before you can access CONNECTIONS, you must first download Citrix Receiver from the App Store. It is a free download.



1. From Desktop, single tap on Safari
2. Type in the CONNECTION web address: <https://connections.ocfs.ny.gov>
3. Select "Add a Bookmark" to save the CONNECTIONS address for later use
4. Enter your HSEN credentials and click the Login button:



5. On the resulting Citrix Applications window, tap on the CONNECTIONS icon.

6. Select Open in "Citrix"

Working with Citrix Receiver

1. If you hit the Home button and leave CONNECTIONS, selecting the Citrix Receiver app in the Open Apps view will return you to CONNECTIONS in the same session you left (within 15 minutes only).
2. If you leave CONNECTIONS and open or access another app, your CONNECTIONS session will be disconnected. To get back into CONNECTIONS, click on the Citrix icon.
3. Copy & Paste – The clipboard on the Apple iPad-2 does not see text as text when trying to paste into CONNECTIONS. To allow pasting of data into CONNECTIONS you must follow these steps:
 - a. Place your cursor in the Progress Note or other Narrative field .
 - b. On the virtual keyboard in the top left corner select the letter "A" (with a "T" next to it).
 - c. In the text field, paste what's been copied.
 - d. After pasting, press the Send button to the right. Then press Done. The text has now been pasted into CONNECTIONS.

For Additional Assistance Contact:

-  **LAN Administrator** for assistance and escalation to the OCFS Application Help mailbox ocfs.sm.conn_app@ocfs.state.ny.us to address a support issue when necessary.
-  **Apple.Com:** www.help.apple.com/ipad/5/interface/

User Security Dos and Don'ts for the Apple iPad

The user will read the OCFS Apple iPad-2 Pilot User Quick Guide which contains, among other information, the website location where general security information can be located. Additionally please refer to OCFS Internet Security information at: <http://www.ocfs.state.ny.us/connect/security/>

The user will familiarize her/himself with security information contained in this guide and in the referenced material prior to using the device and will maintain the secure configuration of the device.

The user will access OCFS and NYS Directory Services Applications via log-on banners and will read the security, privacy and acceptable use information displayed prior to the use of the application.

The user will not install any hardware to the Apple iPad-2 without the express prior consent of OCFS.

The user will not upload any confidential information to any third party hosting service.

The user will transfer confidential information from the iPad to the State network in a timely way and delete confidential information from the device regularly. The user will remove confidential information from the portable device after it has been transferred to the State network.

The user will provide secure storage for Apple iPad-2 and other technology equipment when not in use. Should an OCFS issued iPad be lost or stolen, the loss must be reported immediately to the police and to your supervisor and LAN Administrator, and report any lost or stolen equipment to OCFS-IT, completing and sending the OCFS-4440 Lost or Stolen Equipment form by e-mail to "comctrup@ocfs.state.ny.us"

The user will maintain the security of the data contained on any storage device according to the applicable rules and regulations pertaining to child welfare information, including but not limited to 18 NYCRR Part 466.

The user will only use secure methods (that meet encryption requirements) to transmit confidential information. If you need assistance with transmitting confidential information, please see your supervisor or LAN Administrator. The Guidelines for Using Electronic Communication for Sharing Case Specific Information are located on the OCFS Intranet at: <http://ocfs.state.nyenet/connect/security>

The user will maintain the device per the direction of OCFS and will not change security settings on the device without express permission from the OCFS ISO or designee.

The user will be familiar with her/his organization's security plan and, as appropriate, policies and procedures which address the following areas of equipment security: (i) physical security of equipment resources to protect equipment from theft and unauthorized use; (ii) software and data security; (iii) personnel security; (iv) contingency plans to meet critical processing needs in the event of short-or long-term interruption of service; and (v) designation of an organization Security Manager.

The user will contact her/his site contact who will contact the Application Help mail box at ocfs.sm.conn_app@ocfs.state.ny.us to address a support issue when necessary.

For more detailed information, refer to the Case Work Contact agreement that is associated with the distribution of these iPads via your site contact.

You may direct security questions to the OCFS Acceptable Use mailbox at: acceptable.use@ocfs.state.ny.us

NOTE when you sign into CONNECTIONS or any OCFS application you will find a Logon Warning that gives you information about acceptable use, confidentiality, and privacy expectations. Failure to comply with these standards may have serious consequences. Anyone, including employees, third parties, contractors, or volunteers who violates or fails to comply with the confidentiality provisions of the applicable laws and regulations may be subject to a variety of administrative actions and discipline, including but not limited to loss of employment or contract termination, in addition to criminal and/or civil prosecution.

*** WARNING ***

Warning: This system and all data accessed through it are confidential and proprietary to the State of New York access is limited to authorized employees and legally designated agents and only for authorized purposes. Also these systems access data maintained by other government groups access thereto must also be authorized. Unauthorized access to or release of State of New York systems/data or other government data may result in civil liability and/or criminal prosecution. Any use of this system may be accessed read copied and used for any purpose the State of New York deems proper - users have no expectation of privacy. Use of the system whether authorized or not constitutes express consent for the State of New York to intercept copy and reuse any material entered on this terminal. This notice shall not be interpreted to compromise the rights of nonuser data subjects.