VeEX Inc.
2827 Lakeview Court
Fremont, CA 94538
tel: +1.510.651.0500
fax: +1.510.651.0505

Support Bulletin

UX400 Browser-based Remote & Java™ Plug-in Compatibility

O0218-03

August 28, 2015

UX400 and UX400R platforms running Rootfs 1.3.1 and Common 05.04.26 (or newer) no longer require Java plug-in to work with the latest web browsers. Since plug-ins are being abandoned, for security reasons, VeEX has converted the 'Platform Remote Control' (screen mirroring) and multi-user 'Remote Test Sessions' applications into JavaScript and no longer suffer from security blocking. The UX400 is now compatible with the new Microsoft Edge and Google Chrome browsers. Upgrading to the latest Rootfs and Common software is highly recommended and encouraged.

UX400 and UX400R test platforms, running Rootfs 1.3.0 and Common 05.04.20, or older versions, require Java plug-in to offer convenient browser-based Remote Control (screen mirroring) and multi-user Remote Test Sessions. If for any reason you can't keep the UX400 system software up-to-date (e.g. company policy, restricted internet access, bandwidth, etc.), please follow the procedure described in the next page.

Keeping the UX400 Up-to-Date

First step: Make sure the UX400 is running the latest Platform versions. Please download the latest UX400-Rootfs and UX400-Common install packages from www.veexinc.com >Products and Solutions >UX Series >UX400 >Software

- UX400 Rootfs 01.03.01 or newer
- UX400 Common 05.04.26 or newer

Unzip both files and copy the resulting ux400-veex-rootfs-x86.tar.gz and ux400-local-v300.tar.gz to the root of a FAT32 USB memory stick, along with any other test module updates. Insert the memory stick in one of the UX400's USB ports.

To start the software upgrade process, turn UX400 the ON by simultaneously pressing the Power and Light buttons. Release the Power button after the first tone (beep), but keep holding the Light button until a second tone is heard. Check the Common and Rootfs versions boxes and press Upgrade. The test set will turn itself off at the end.

Turn UX400 the ON, let ant remaining installation processes to finish and connect its Ethernet Management Port to a LAN outlet or WAN port to stablish an IP session. Just like in any other true Remote Access applications, the use of static routable IP addresses is recommended. In local LAN environments DHCP could be used, but be aware that the UX400's IP address may change from time to time, requiring the repeat of the procedure below when/if that happens.

Web Browser Compatibility

In 2013 Google announced that Chrome will no longer support the NPAPI (Netscape) plug-in and the newly introduced Microsoft® Edge doesn't support plug-ins at all. This means that the latest browsers don't support Java plug-in.
Newer versions of UX400 System software address this and are fully compatible with Edge (Win10), Internet Explorer 11 (Win), Chrome (Win, Mac, Linux, Android, iOS), Firefox (Win, Mac, Linux, Android), Safari (Mac, iOS). Please upgrade the UX400 Rootfs and Common software to the latest versions from www.veexinc.com.

If for some reason you are not able or allowed to update to the latest UX400 system software and your company has standardized on Chrome or Microsoft, please consider the following alternatives to the address the Java plug-in support:

- For Chrome browser, please refer to the following Chrome (https://developer.chrome.com/extensions/npapi) and Java (https://java.com/en/download/faq/chrome.xml) guides to make an informed decision on how to proceed.
- Win10 still comes with Internet Explorer 11, which can continue to be used to access outdated UX400 remotely.

How to Resolve Java™ (Blocking) Compatibility Issues with earlier versions of UX400 Browser-based Remote Control

The popular NPAPI Java plug-in is considered insecure by many industry experts, to the point that it is no longer supported by newer browsers. On the other hand, Oracle® has been busy releasing multiple Java™ updates (2014 - 2015). In the process they have abolished the Medium security level setting and instead created a new Super Secured level, in which Java may not trust its own applications or even let users decide whether to take the risk of running them or not. This change affected some UX400 web-browser based remote GUI features. Before, Java used to warn users and gave them the option to bypass the warning. Most recent updates allow users to bring back some of that functionality, but the procedure may vary from browser to browser.

- Please note that IT departments may also have some blocking rules of their own in place, for the Network and/or PCs, that may also affect the access to the UX400 web-based Screen Mirroring (Remote Control) and Multi-user Remote Test Sessions

Here are the basic recommendations to regain control of UX400 (procedures and results may vary, depending on the network environment, OS and browser)

Java Security Settings

Depending on the Java version installed in the computer, the type of browser and the environment set for the network, you may get different errors messages, ranging from the ports (22, 80, 5900-5902, 8023) being blocked by your IT department, to blocking messages from Java itself or the web browser.

- Type "Configure Java" in the (Windows®) search box and run the highlighted app.
- Click on the "About" button to confirm the Java version installed in your PC. The version that allowed you to configure the security level to Medium was Java version 1.7.0_25-b15 (also known as Version 7 update 25). Versions may be different for WinXP, Win7, Win8.1 and Win10 (This document focuses on supported Windows™ 7, 8.1 and 10 since updates for XP are no longer published and newer Java versions are not guaranteed by Oracle to work with XP).
- In the "Security" tab check the "☑ Enable Java content in browser" box
- If it shows a slider and allows you to move it down to Medium, select Medium. Newer versions only offer High and Very High, so in that case select High.
- In the same tab, open the "Edit Site List…" to white-list the UX400's IP address. You must include the http:// prefix (e.g. http://192.168.0.103) or it may get rejected.
- Click on "Apply" to save the changes.

Web Browser Security Settings

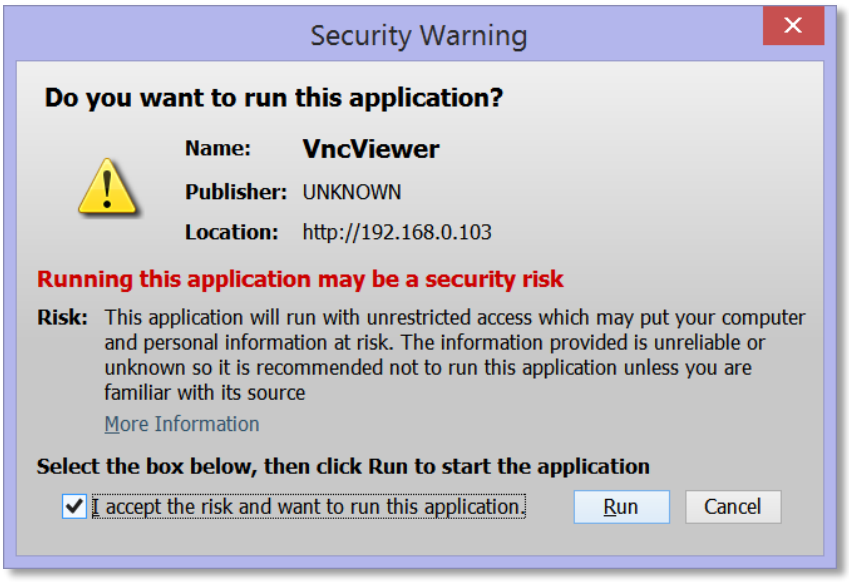
Different browsers may show different behaviors and this is also valid for the way they may show the Java compatibility errors (nothing at all, some error message, a detailed error message, a puzzle piece without further information, etc.)

- Open the Web Browser
- Go to "Internet Options", open the "Security" tab, select the "Trusted Sites" icon and click on the "Sites" button
- Enter the UX400's IP address. You must include the https:// prefix (e.g. https://192.168.0.103) and click on "Add"
- Click on "Close" and then "Apply"

Some users may be required to re-launch the browser in Administrator Mode. To do this, right-click on the browser short-cut and select "Run as administrator".

Make sure that the current Ethernet/Internet connection, Wi-Fi or LAN, is labeled as a Private Network.

Type the UX400 IP address in the browser's Search/Address bar to access its web interface. When the Remote Control (main screen mirroring) or Remote Test Session (individual test sessions) are accessed, the browser should display the Java "waiting" logo and the message below. Check the "☑ I accept the risk…" and click on the "Run" button to get the remote GUI session going



The web-based screen mirroring functions (Remote Control and Remote Test Sessions) use a VNC protocol. If you are still having trouble seeing the main UX400 or test session GUI, please check with your IT department if any restrictions have been imposed to the network, ports, applications and/or PC.

- Note: Any standard VNC client, like RealVNC™, can also be used to remote control the main UX400 GUI.

TCP Ports used by UX400

VNC screen mirroring, browser-based Remote Control, multi-user Remote Test Sessions and CLI Telnet/SSH sessions use the following ports:

- 22, 80, 5900-5907, 6900, 8023, 11000, 11100

An up-to-date list of applicable ports can be found in the UX400 >Utilities >Settings >Remote Access

For more up-to-date information, please visit the Support section at www.veexinc.com or contact us at customercare@veexinc.com