RX-HDX+ and RX420(HDX) Configuration Guide

KNOWLEDGE BASE AND BEST PRACTICES

Low Cost | Great performance | Citrix HDX Ready

RX-HDX+ and RX420(HDX) Configuration Guide

About NComputing

NComputing is a desktop virtualization company with more than 70,000 customers and 20 million daily users in 140 countries. NComputing serves customers large and small, in diverse markets, and with diverse use cases across education, government, and industry segments. NComputing's innovative technology gives customers affordable, easy-to-deploy, high performing virtualization solutions.

NComputing is a charter member of the Citrix HDX SoC Program. NComputing introduced the first SoC (ARM) based thin client with Citrix in 2012. NComputing continues to partner with Citrix on ground-breaking initiatives, including the Citrix Ready Workspace Hub (RX-HDX) based on Raspberry Pi 3, and RX420(HDX) based on Raspberry Pi 4.

About NComputing RX-thin client devices (Citrix Ready Workspace Hub)

NComputing closely collaborates with Citrix and Stratodesk to deliver the Citrix Ready Workspace Hub (RX-HDX and RX420(HDX) devices) for enterprises. The solution provides traditional thin client capabilities with performance, security and manageability in mind, plus the innovative Citrix Casting features to further expand its use cases. Solutions based on RX-HDX and RX420(HDX) are being deployed worldwide in many vertical markets including healthcare, manufacturing, finance, insurance, education, government, retail and services.

The RX-HDX and RX420(HDX) thin clients are produced by NComputing's factory in Korea based on the Raspberry Pi boards that are manufactured in the UK and Japan. Numerous areas were designed and enhanced to make RX-HDX and RX420(HDX) an enterprise-ready thin client. New power button logic was created to enhance the corporate usability and device reliability. Shielded enclosure was custom designed to prevent access to the embedded micro-SD card. Proprietary thermal cooling solution was designed to ensure the device works reliably in rugged environments. Performance is fully optimized through close collaboration with Citrix. Enterprise-grade device management was integrated through partnership with Stratodesk to ensure the device can be managed remotely from any location. Every RX-HDX and RX420(HDX) device has gone through 100% inspection prior to shipping to our customers.

Table of contents

1. Introduction

1.1. Purpose of this configuration guide

The purpose of this configuration guide is to provide comprehensive information about the setup and configuration of NComputing RX-HDX and RX420(HDX) thin client devices.

1.2. Intended audience

NoTouch administrators, Citrix administrators, systems engineers, technical support engineers, help desk personnel.

1.3. Edition history

Guide edition	Release date
1.0.0	November 2018
1.1.0	May 2020

1.3.1. Change log

1.0.0 edition

This is the first edition of the RX-HDX configuration guide.

1.1.0   edition

This is the second edition of the RX-HDX and RX420(HDX) configuration guide.

1.4. How to use the information from this guide

The information from this guide is based and has been verified on the latest publicly released RX-HDX NoTouch OS firmware version, which was the 3.1.169 at the time of writing.

There are several NoTouch settings which exist besides the settings mentioned in this guide. When configuring any RX-HDX and RX420(HDX) device features as described in further sections, no additional settings other than the explicitly mentioned ones should be adjusted. To avoid unexpected behavior all those settings should be kept with their default values.

2. General NoTouch information

2.1. Obtaining NComputing-branded NoTouch Center

Create an account and login to the NComputing Management Portal:
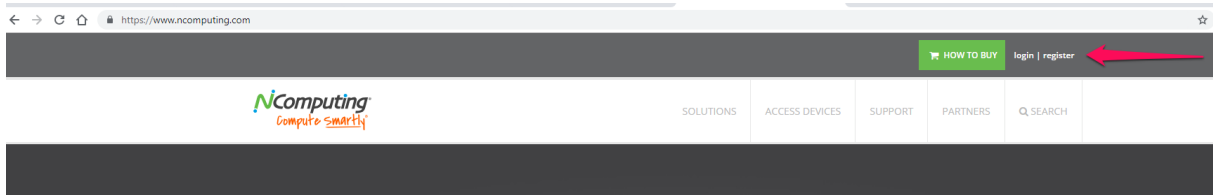
Select 'Management Portal':
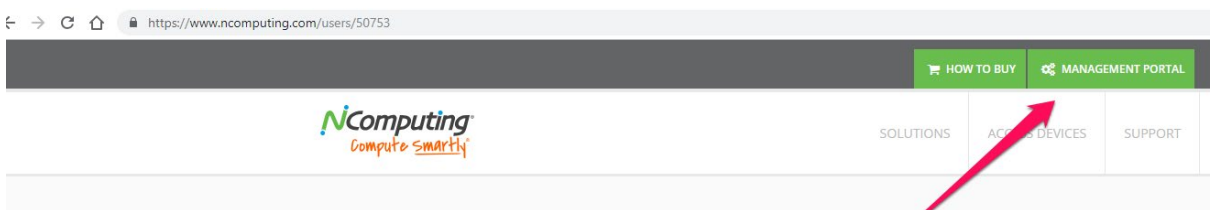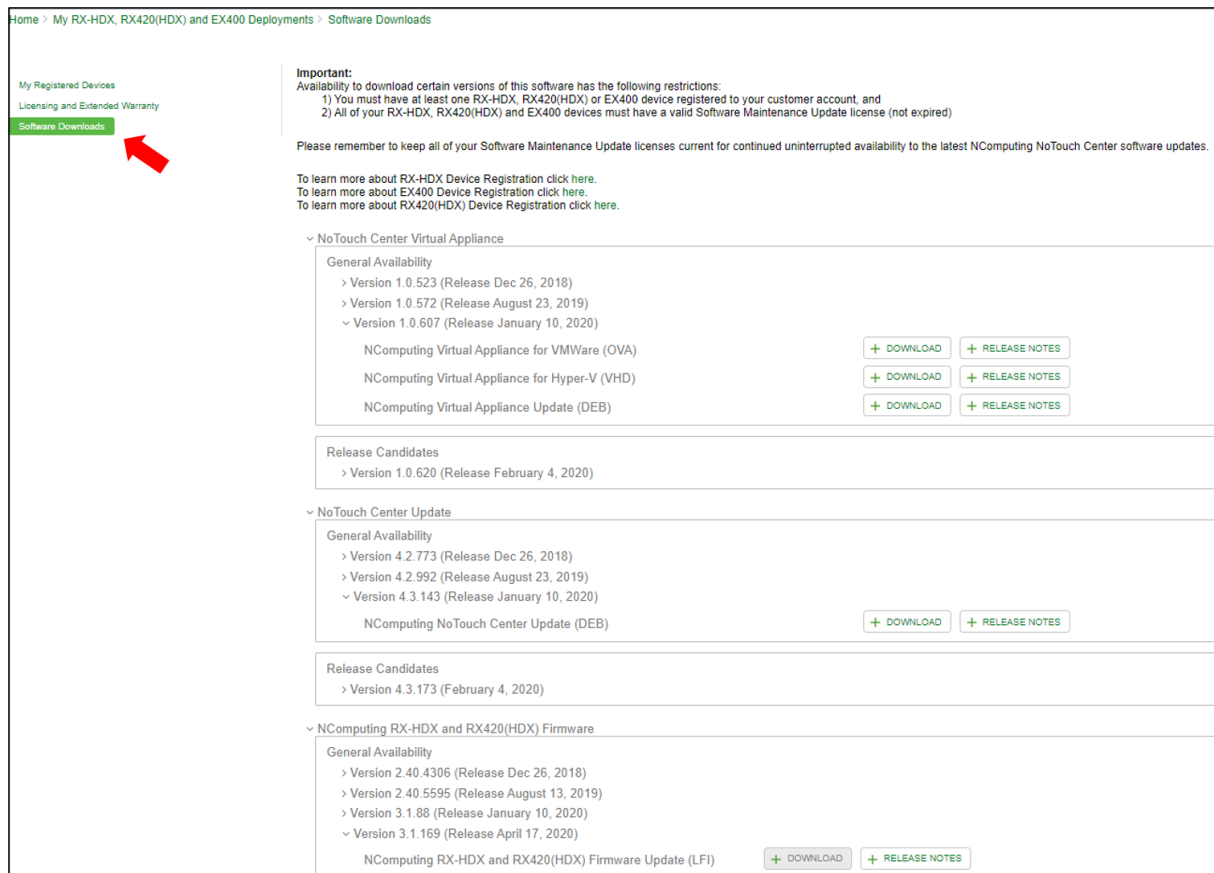
Select 'My RX-HDX, RX420(HDX) and EX400 Deployments':
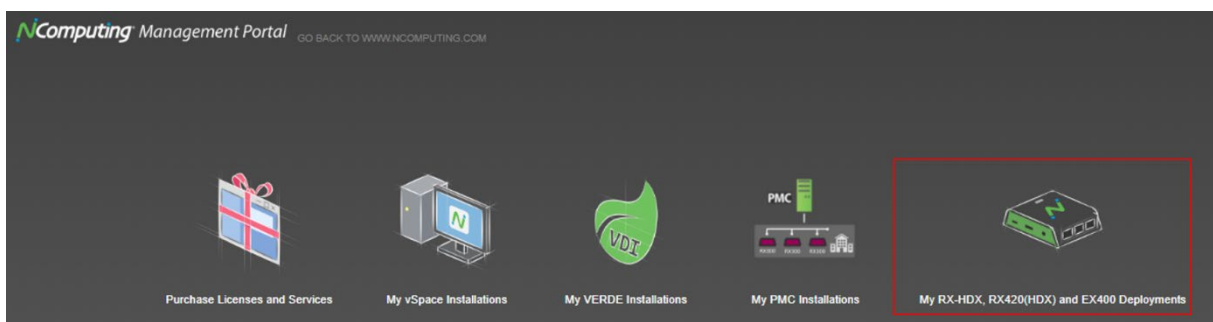
Then under 'Software Downloads' you will see the download links for the NComputing RX-HDX and RX420(HDX) firmware update package (the LFI file) as well as the NoTouch Center virtual appliance

image for Citrix Hypervisor (XenServer) and VMware ESXi (the OVA file), and Microsoft Hyper-V (the VHD file):

3. First-time Configuration Wizard

Out-of-the-box devices as well as devices which have been reset to factory defaults after booting up present the first-time local device configuration wizard allowing you to quickly make the basic device and connection specific setting as needed for your environment.

3.1. Step 1 – Location and Keyboard

When connected to a network with Internet access the device makes use IP address geolocation to pre-select the time zone, country, system locale, and keyboard layout. These settings can be adjusted manually when necessary.

- IMPORTANT: select the correct keyboard layout.

NoTouch OS offers localized user interface for some system locales (like German or French). For other locales the US English language version of the interface will be presented.

3.2. Step 2 – Workspace Hub Configuration

In second step of the configuration wizard a server connection can be configured. This step is optional. When skipped no connection will be configured at that moment. Administrator will have to configure the connections later using the Configuration UI.

Four connection types are available:

Connection type	Connection's parameters
Citrix Workspace Hub	URL(s) – This can be a comma-separated list of website URLs, which will be presented in the background of the Workspace Hub connection. Detailed Workspace Hub settings and configurations can be found in the Citrix Workspace Hub documentation.
Citrix Workspace App	Citrix URL – URL of a Citrix Store, Citrix Gateway, or Citrix Web Interface Services Site, as explained in the 'Configuring Citrix connections' section. Resource – Name of published desktop or application to be automatically started for the user.
Firefox Browser	Start URL – the URL of a website to be automatically opened when the Firefox browser will start.
Chromium Browser	Start URL – the URL of a website to be automatically opened when the Chromium browser will start.

For most connections the 'Automatic start' option can be additionally selected. This will cause the connection to be automatically started on device boot. The Workspace Hub connection, when configured in this step, will always be set to start automatically.

More information about the first-time configuration wizard can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/NoTouch_OS_QuickStart.

3.3. Step 3 – Administrator Password and EULA

In last step a password for protecting the device configuration must be set. This password needs to be at least 5 characters long. It will have to be provided whenever accessing the Configuration UI, as described in next chapter. If at some later time the device will be centrally managed from NoTouch Center, then this password will be replaced by with the 'client admin password' configured in NoTouch Center.

In this wizard step also the Software End User License Agreement of Stratodesk Corporation, who is the original software vendor of the RX-HDX and RX420(HDX) NoTouch OS, must be accepted.

3.4. Skipping the first-time wizard

All the settings which are configurable in steps 1-3 of the wizard are optional and can also be configured later in the Configuration UI, if the user opts to skip the first-time wizard by clicking the green 'Skip wizard' button located on the left-hand side. By doing so the user declares to agree with the terms of the Stratodesk Corporation Software End User License Agreement. The default password is 'admin' for accessing the Configuration UI.

3.5. Central management

The first-time configuration wizard can also be skipped if the devices will be centrally managed from NoTouch Center. The green 'Central management' button located on the left-hand side can be clicked in such case. By default the device is configured with following NoTouch Center management URL: http://tcmgr:8080/easyadmin/servlet/XmlRPC.

This means that:

1. The device will try to resolve in DNS the 'tcmgr' host name. It will use the default (obtained from DHCP) DNS search suffix when querying DNS for the 'tcmgr' host name.
2. When the IP address of 'tcmgr' host will be found the device will try to announce its presence to NoTouch Center expected to be under this address.
3. Device will use for NoTouch Center communication the HTTP protocol on TCP port 8080. This port needs to be open on all firewalls located between the client device subnet and the NoTouch Center system. NoTouch Center will likely redirect the communication to the secure HTTPS protocol and the TCP port 443, so the firewalls must also allow this kind of communication.

A custom NoTouch Center URL (containing a different than 'tcmgr' host name or even an IP address) can be specified as 'Management URL' if your DNS is not set up to resolve the 'tcmgr' host name to an IP address of NoTouch Center.

A NoTouch Center lookup method based on e-mail addresses can be used too. This lookup method also requires special DNS setup, which is described in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/E-mail_based_management_server_lookup.

When using NoTouch Center for central device management additional information specific to each device, like the location, user name, group assignment key, or custom client device host name, can

be provided here. NoTouch Center can leverage this information to automatically assign the NComputing RX-HDX and RX420(HDX) thin client devices to appropriate device group and to create and deliver proper configuration for the device.

3.6 NoTouch Center RX-HDX and RX420(HDX) Client List Device Registration

It is very important to properly register devices on the NComputing Management Portal in order to maintain proper warranty and software maintenance status.

From NoTouch Center Management Console

After obtained the Client List, log into customer's NComputing Management Portal
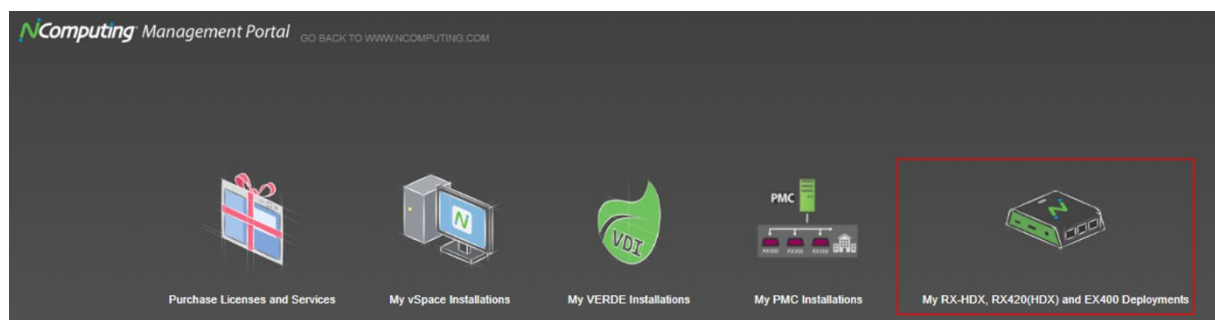
Upload the Client List as instructed
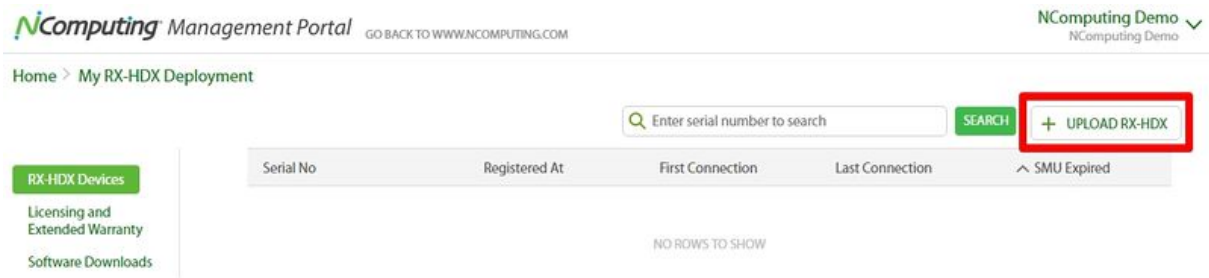
For more information, please reference to KB:

http://rx-hdx.ncomputing.com/kb/NoTouch_Center_RX-HDX_Client_list_for_device_registration

3.7 RMA Request and Process

In the event a irreversible hardware failure has occured, please submit a support ticket with the following information to process the RMA request:

Customer Information

Customer email

Cusotmer phone number

Device model

Device Serial number (minimum of last 8 characters)

Description of the problem

For RMA please include correct return shipping address / contact information / phone number

How to create and submit a support ticket:
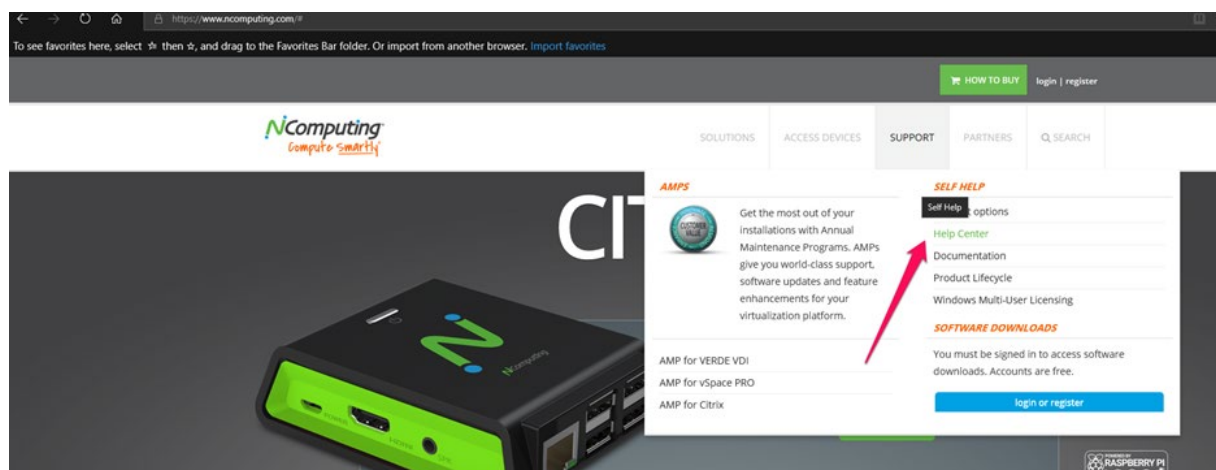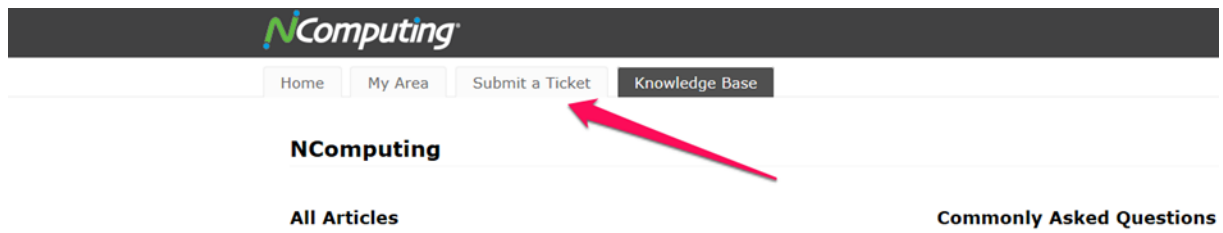
For more information please reference to the following KB:

https://support.ncomputing.com/portal/kb/articles/request-an-rma-return-or-open-a-support-ticket

4. Configuration UI

4.1. Accessing and using the Configuration UI

The RX-HDX and RX420(HDX) device Configuration UI allows you to make device and connection specific setting as needed for your environment. The Configuration UI of RX-HDX and RX420(HDX) thin client devices can be accessed locally (using the keyboard, mouse, and monitor connected to the device), or remotely using any web browser. Generally the same settings can be configured using the local and remote web interface, although some differences exist, which will be explained later.

Local Configuration UI can be opened by:

- Going to Start menu and clicking 'Configuration'.
- Pressing the Ctrl-Alt-c key-combination.

Web-based Configuration UI (the Web-admin UI) can be accessed by opening an HTTP or HTTPS URL containing the IP, hostname, or FQDN of the RX-HDX and RX420(HDX) thin clients. The HTTP URL by default redirects to HTTPS and all further actions will be performed through HTTPS URLs. The TCP 80 and/or 443 ports need to be open on all firewall between the web browser and the managed device to allow access to device's web-based configuration UI.

The Configuration UI, no matter if accessed locally or remotely, will ask for administrator password and a valid password must be provided before the access to any device settings will be granted. The password set when going through the First-time Setup Wizard, or the password set for the device group in NoTouch Center must be provided. When no password has been set in First-time Setup Wizard and the device is not yet connected to NoTouch Center, then the default password is 'admin' (without apostrophes).

The Configuration UI shows on the left-hand side a list of hyperlinks to administrative tasks. The tasks are grouped into Management, System, and Diagnostics categories. The Management category groups tasks related to device and connections management. The System category groups tasks related to device firmware and also includes file management (especially certificates and pictures). The Diagnostics category groups tasks related to device troubleshooting.

Note: The tasks, which require file uploads, are only available when the Configuration UI will be accessed remotely from a web browser.

Whenever any device or connection setting has been modified the change must be saved for the change to take effect. There is the 'Save' button in the lower-right corner of each configuration page, which saves the modified settings when clicked. The system-wide settings (like settings under 'Services') in most cases also require device reboot to take effect. For connection-specific settings the connection needs to be restarted (user logged off and logged on) for the change to take effect.

More information about the Configuration UI can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Configure_NoTouch_OS.

4.2. Configuring basic device settings

4.2.1. Keyboard layout

The configured keyboard layout will be used by connections handled locally (especially web browsers) and also will be reported to remote terminal servers (for Citrix and RDP/FreeRDP connection).

The keyboard layout can be configured with following system-wide NoTouch setting:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Input > Keyboard	Keyboard layout	*Select the keyboard layout appropriate for your country/users.*

Note: RX-HDX device must be rebooted for the above changes to take effect.

4.2.2. Date and time

For user's convenience NoTouch OS displays the current date and time in the system tray of user's taskbar. NoTouch OS needs to know the current date and time to be able to accomplish a much more important task though: to be able check the validity of SSL certificates. As currently most Citrix infrastructures and websites use SSL/TLS to secure the communication ensuring that the RX-HDX and RX420(HDX) thin client devices are able to obtain information about current time becomes very important as it is one of the conditions to avoid SSL/TLS errors.

Because the RX-HDX and RX420(HDX) hardware platforms do not have any battery-powered real-time clock the NoTouch OS must obtain the current date and time after the device boots up. The date and time can be set in Configuration UI. This action (as any other administrative action) requires the user to provide the administrator's password, so this method is not suitable for regular users. NoTouch OS can obtain the current date and time automatically using the Network Time Protocol (NTP).

RX-HDX and RX420(HDX) NoTouch OS is configured by default to obtain the date and time from the public NTP servers available in the ntp.org domain. Following system-wide NoTouch settings can be explicitly configured to obtain the date and time from public NTP servers:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Time	Time zone	*Select the time zone appropriate for your device's country.*
Time	Fetch NTP time on boot	On
Time	Run NTPd	On
Time	Use ntp.org pool if no custom servers given	On

Note: RX-HDX and RX420(HDX) device must be rebooted for the above changes to take effect.

Custom NTP time servers can be added under 'Time > NTP time servers'. It's advisable to have more than one NTP time server address added.

To mitigate potential issues originating from NTP servers unavailability NoTouch OS sets the clock to current firmware build date and time. Then it looks for the information about last system shutdown date and time, and, if found, sets the clock to this date and time. This is to improve the probability of positive SSL/TLS certificate validity verification. Both are better than the January 1st 1970, which the NoTouch OS, as any other Linux system, sets after booting up if no external date and time source is available. At the end, when the device manages to get in touch with the NTP server, it sets the clock to the date and time obtained via NTP.

As NTP is a UDP-based service leveraging port number 123 for successful NTP communication the specified NTP servers must be accessible from RX-HDX devices on the mentioned port.

More information about date and time configuration can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Time_and_time_zone.

- IMPORTANT: incorrect time and date may result in authentication error when establishing Citrix connection.

4.2.3. Display

Primary display considerations

The RX-HDX hardware platform has one integrated HDMI display output. The RX420(HDX) hardware platform comes with dual native micro-HDMI display outputs. No further configuration is necessary when the HDMI output will be used with compatible HDMI monitor at its native resolution. RX-HDX and RX420(HDX) will recognize connected monitor's native resolution and will adjust the HDMI output's settings accordingly. Also HDMI-to-DVI or HDMI-to-DisplayPort adapters can usually be used without any further configuration. Care must be taken when selecting an HDMI-to-DisplayPort adapter, as such adapters are unidirectional. The adapter must be intended to convert the HDMI signal to DisplayPort signal, not vice-versa. HDMI-to-VGA adapters can be used too, but such adapters can have difficulties with returning to RX-HDX and RX420(HDX) the DDC data from the connected VGA monitor. The DDC data contains the information about monitor's native resolution. In such case a particular resolution, ideally a one matching the monitor's native resolution, can be set for the HDMI output.

Primary display resolution settings

Following system-wide NoTouch settings can be configured to set primary display resolution:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Display/Monitor > Monitor > Monitor: *Monitor name*	Screen resolution	*Select the native resolution of connected monitor.*
Display/Monitor > Monitor > Monitor: *Monitor name*	Refresh rate	*Select the highest refresh rate supported by connected monitor.*

In case when the RX-HDX or RX420(HDX) thin client devices are unable at all to detect the presence of the monitor connected through an HDMI-to-VGA adapter (which results with a blank screen) the following NoTouch setting needs to be added:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Raspberry Pi > config.txt > config.txt	Entry	hdmi_force_hotplug=1

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

More information about RX-HDX and RX420(HDX) display configuration can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Display.

Setting up dual display on RX420(HDX)

The RX420 (HDX) thin client comes with a native dual display.

By default, the system will output the same image on both screens ("**cloned**" mode in our terminology) which is usually a safe bet and also works if there is only one monitor connected. In an office scenario where you have two monitors next to each other, you most probably want to have both monitors being part of a large logical desktop, this is called "**merged**" mode.

In "**merged**" mode, when operating remote desktops such as via Citrix, VMware or RDP, the server-side Windows desktop may or may not know about the actual screen geometry. In the simplest case, server-side Windows may believe that there is a single screen that is 3840 pixels wide, for instance, when the client has two monitors connected with 1920 pixels horizontally each. Now if you maximize a program window, it would be maximized over both screens - and most people feel uncomfortable with that. That means it is important that the server-side Windows instance gets to know about the actual screen geometry on the client-side - and fortunately, this is done automatically the way NoTouch is configured by default. Not all protocols support this, but the Citrix Receiver, VMware Horizon View client, and FreeRDP do and you can tune the settings.

Setting up dual display for RX-HDX with Pi Zero SDA (Part#: 500-0159, SDA-RXHDX)

The RX-HDX hardware platform has one integrated HDMI display output. For scenarios where more than one display is required there are two Secondary Display Adapter (SDA) options. First one is the SDA based on the Raspberry Pi Zero single-board computer. This adapter, in properly configured environments, ensures the best Citrix session performance and user experience, but following facts need to be taken into account for the RX-HDX dual display setup:

- There is no support for connection other than Citrix.
- Only full-screen Citrix published desktop sessions are supported.
- There is no support for Citrix published applications. With Pi Zero SDA published applications can only be displayed on the primary screen.
- There is no support for Workspace App's locally rendered contents, like the Citrix Desktop Viewer Toolbar or Skype for Business video (when using the RealTime Media Engine).
- Both displays (primary and secondary) must have the same resolution and orientation.
- For best performance the full-screen H.264 encoding (video codec for the entire screen) should be used on the server side. Especially the 'Selective H.264' (video codec for actively changing regions) encoding should be avoided.
- XenApp/XenDesktop 7.6 is the minimum supported version of Citrix environment.

RX-HDX

NComputing Pi Zero SDA

1 Connect the secondary monitor to SDA

Secondary Display Monitor
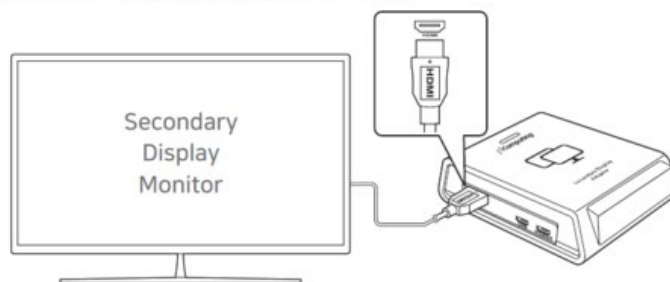
2 Connect SDA to RX-Series, then power on the RX-Series device

Secondary Display Monitor

RX-Series
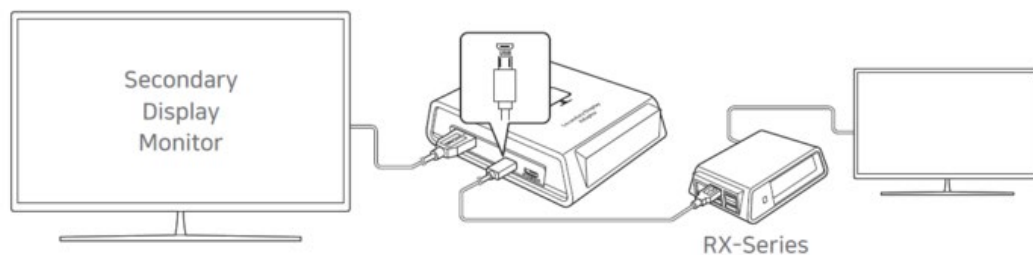
Support for the Pi Zero SDA is enabled by default in NoTouch OS. The following system-wide NoTouch settings can be configured to explicitly enable the Pi Zero SDA support:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Display/Monitor	Multimonitor mode	cloned (same picture on all monitors)

Note: RX-HDX device must be rebooted for the above changes to take effect.

Note: The 'cloned' setting above is not a mistake. The 'Multimonitor mode' must be set exactly like that to enable the Pi Zero SDA. This is the same setting as for single monitor scenarios.

Citrix Policy settings for best Pi Zero SDA performance:

Citrix Policy setting name	Citrix Policy setting value
Use video codec for compression	For the entire screen

When NoTouch OS detects the presence of the Pi Zero SDA it tries to update the SDA firmware components. Information about the firmware can be found under 'Debug information > Citrix SDA'.More information about the Pi Zero SDA configuration can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Multimonitor.

Display settings for DisplayLink DL-165 SDA

Yet another option for scenarios where more than one display is required are the Secondary Display Adapters based on the DisplayLink DL-165 chip. This adapter allows using Citrix published applications on both displays and also can be used for connections other than Citrix.

Following facts have to be taken into account when working with DisplayLink DL-165 based SDAs:

- Both displays (primary and secondary) will work with 16-bits color depth only.
- Citrix Workspace App will report to Citrix server (VDA machine) lack of H.264 support, thus no video codec will be used for session encoding, even if set up to do so with Citrix Policy.
- Graphics performance of the secondary display will be worse than the performance of the primary. It can be noticeable when using multimedia applications or when dragging windows with content, but will be good enough for office or productivity applications.

The following system-wide NoTouch settings must be configured to enable the DL-165 SDA support:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Display/Monitor	Multimonitor mode	merged (all monitors from one desktop)

Note: RX-HDX device must be rebooted for the above changes to take effect.

4.2.4. Audio

The RX-HDX and RX420(HDX) thin client devices can send the audio output to the integrated 3.5mm analog audio jack, to the HDMI interface, or to a connected USB audio device (which can also provide microphone input). Bluetooth audio is not supported. The default audio setting optimizes the USB audio quality and performance.

This may have a negative effect on analog audio. If **analog** audio (headset/speaker) or **HDMI** audio (built-in monitor speaker) is to be used, please follow the instructions to configure the proper audio setting to provide best audio quality and performance.

The following system-wide settings must be configured to optimize NoTouch OS for **analog audio**:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Audio	Standard audio device	analog
Audio > PulseAudio	Timer-based scheduling (tsched)	off

The following system-wide settings must be configured to optimize NoTouch OS for **HDMI audio**:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Audio	Standard audio device	HDMI
Audio > PulseAudio	Timer-based scheduling (tsched)	off
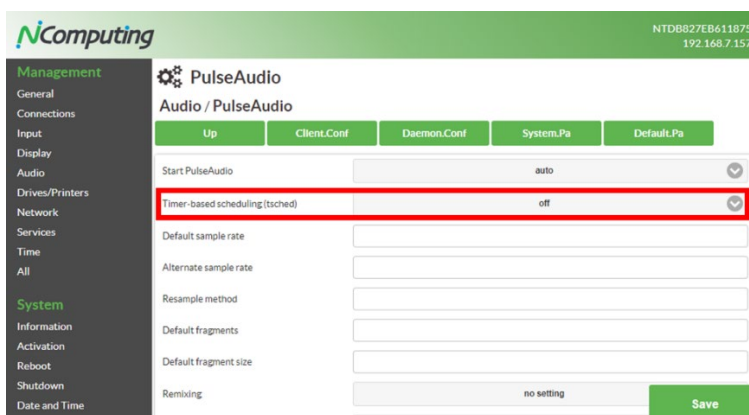
The following system-wide settings must be configured to optimize NoTouch OS for **USB audio**:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Audio	Standard audio device	USB
Audio > PulseAudio	Timer-based scheduling (tsched)	no setting

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.
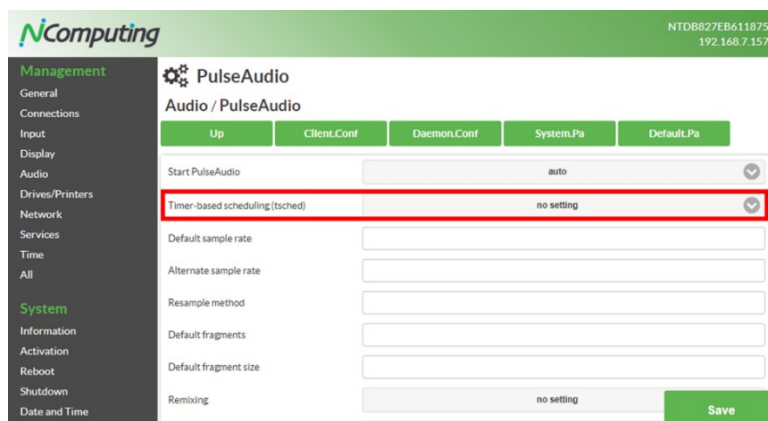
More information about audio configuration can be found in following NComputing Knowledge Base article:

https://support.ncomputing.com/portal/kb/articles/rx-hdx-audio-settings

http://rx-hdx.ncomputing.com/kb/Audio.

4.2.5. Ethernet networking

Ethernet is the default interface which the RX-HDX and RX420(HDX) thin client devices use for communication with the network.

Dynamic configuration of Ethernet interface

The Ethernet interface by default uses the Dynamic Host Configuration Protocol (DHCP) to automatically configure an IPv4 address and other parameters at system start.

The following system-wide NoTouch settings can be configured to explicitly enable dynamic IPv4 configuration for the Ethernet interface:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Network > Interfaces > Ethernet 1	IPv4 configuration	Dynamic (DHCP)

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

Static configuration of Ethernet interface

The following system-wide NoTouch settings can be configured to explicitly enable dynamic IPv4 configuration for the Ethernet interface:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Network > Interfaces > Ethernet 1	IPv4 configuration	Static (Manual)
Network > Interfaces > Ethernet 1	IP address	*The IP address for the Ethernet interface.*
Network > Interfaces > Ethernet 1	Subnet mask	*Network mask for the Ethernet interface.*

NoTouch setting location	NoTouch setting name	NoTouch setting value
Network > Interfaces > Ethernet 1	Gateway	*Default gateway IP address for the Ethernet interface.*

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

More information about Ethernet network interface configuration can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Ethernet.

4.2.6. WiFi networking

Quick and simplest method to configure WiFi on the device is as follow:

1. Issue Ctrl-Alt-w on the device, this will display a window with available SSID
2. Select the desired SSID, if the SSID is hidden, manually input the information.
3. Set the security to "WPA personal"
4. Input the password
5. Click "Change", Save, and reboot the device.

For information on how to configure WiFi network via Configuration UI, please reference to the NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Wireless_LAN.

4.2.7. DNS configuration

When DHCP will be used to configure any of the network interfaces (Ethernet or WiFi) then DHCP will also configure the DNS.

4.2.8. Certification Authority certificates

As most network services nowadays (including the components of Citrix infrastructures deployed on premises) use the SSL/TLS protocols to secure the network communication the endpoint devices, besides knowing the current date and time as explained in the 'Date and Time' section, must also have access to the certificates of the Certification Authorities issuing the SSL certificates for the servers the endpoint devices connect to. NoTouch OS contains around 200 certificates of well known and commonly trusted root and intermediate Certification Authorities. This list is similar to the lists of Certification Authorities, which can be found in popular desktop operating systems and web browsers. If the SSL certificate of the network service the RX-HDX and RX420(HDX) thin client devices is going to communicate with was issued by one of those Certification Authorities, then no further actions are necessary to allow the device the verification of such SSL certificates. When the SSL certificate was issued by a private Certification Authority then the root certificate of such Authority needs to be added to RX-HDX and RX420(HDX) devices. NoTouch OS accepts Certification Authority certificates in PEM (Base64 encoded X.509) format. The file name extension of the certificate file (like .cer, .crt, .der, .pem, …) actually says nothing about the real internal format of the certificate file. Microsoft Windows uses the .cer file name extension for Base64-encoded and binary certificate files.

Real certificate file format can be quickly determined by opening the certificate file in a text editor, like WordPad. If the file will contain random binary characters, then the file is in binary (DER) format:
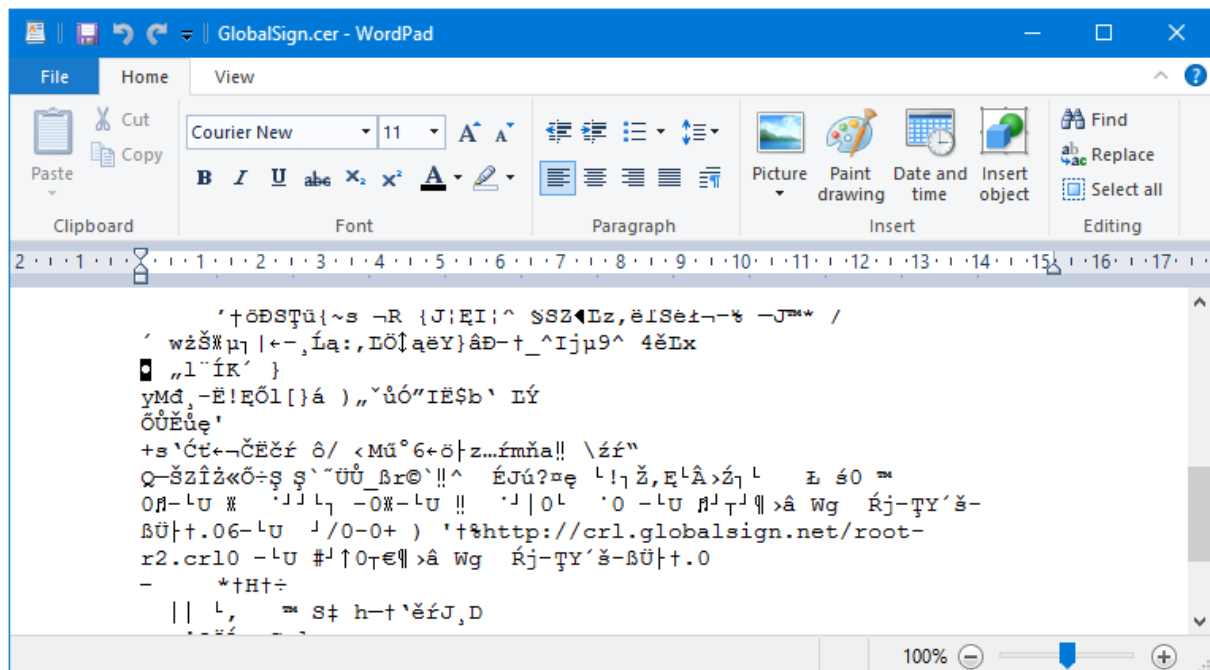
If the file will contain nicely formatted ASCII characters only, will start with
'-----BEGIN CERTIFICATE-----' and end with '-----END CERTIFICATE-----', then the file is in PEM format and can be added to RX-HDX and RX420(HDX) thin client devices:
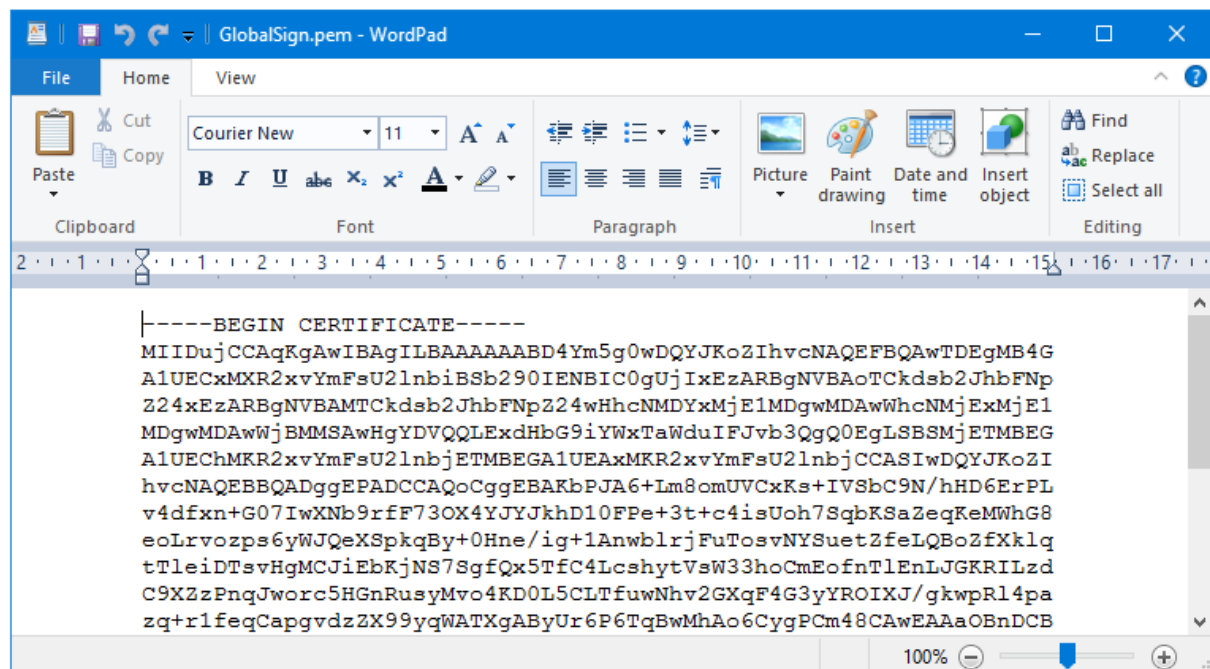
Certificate files can be easily converted from DER to PEM format by opening them in Microsoft Windows, clicking the 'Copy to file' button on the 'Details' tab, and selecting 'Base-64 encoded X.509' format in next step.

Certification Authority certificates can be uploaded to RX-HDX and RX420(HDX) NoTouch OS devices through the Web-based Configuration UI. Web-based Configuration UI (the Web-admin UI) can be accessed by opening an HTTP or HTTPS URL containing the IP, hostname, or FQDN of the RX-HDX and RX420(HDX) thin clients (HTTP URL by default redirects to HTTPS). The 'Certificates' option (not to be confused with 'Citrix Interm. Certs') under System category allows the actual certificate upload.

More information about certificate management in NoTouch OS can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Certificates.

4.2.9. Preparing for remote management with NoTouch Center

For information on how to prepare NoTouch Center virtual appliance (VM), please reference to the NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Category:NoTouch_OS_Initial_Setup

4.3. Configuring advanced device settings

4.3.1. Defining hotkeys

Predefined and commonly used hotkeys (shortcuts) in NoTouch desktop:

- Ctrl-Alt-w: display windows with available WiFi SSID information
- Ctrl-Alt-s: dislplay system (device) information, i.e. network, firmware, control management, etc.
- Ctrl-Alt-c: display Configuration UI login window

For information on additional predefined hotkeys and how to define custom hotkeys, please reference to the NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Hotkeys

4.4. Updating device firmware

There are multiple methods to update device firmware, on device via NoTouch OS and via NoTouch Center the central device management software.

New device firmware can be downloaded via NComputing Management Portal with valid software maintenance agreement.

4.4.1 Updating Device Firmware on NoToch OS

On device firmware update can be done via a USB thumb drive that contains the new firmware, or via direct file transfer from a connected PC/Laptop, or via a HTTP file server file download.

For detail on how to update firmware on device please refer to the following KB:

http://rx-hdx.ncomputing.com/kb/Firmware_Update

4.4.2 Updating Device Firmware via NoTouch Center

Log into NoTouch Center, on the main page, select "Resources" then "VDI Client Image". On the subsequent page, drag and drop the new device firmware to upload the file. Please do not change the firmware update file name, as the update process will check the file name for validation.
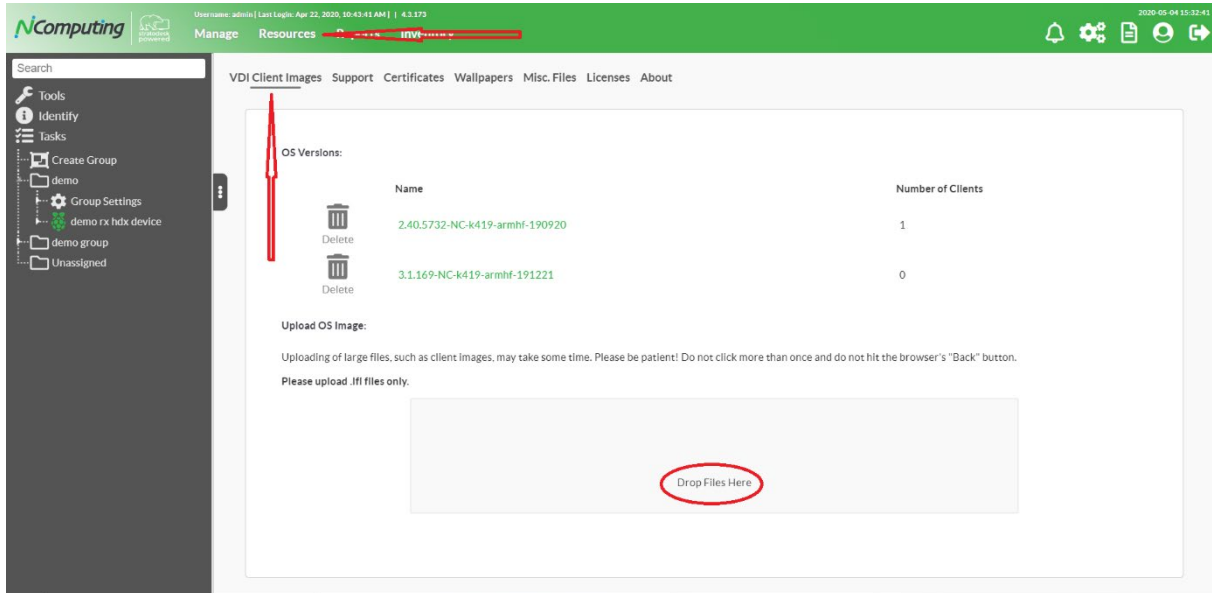
After device firmware has been uploaded, select the appropriate "Group Settings" to configurate firmware update settings

On the Configuration page, scroll down to the middle of the page and find the following settings "Client OS Image" and "Client OS Image Update Mode"

If there are multiple device firmwares on the NoTouch Center, select the desired version from the dropdown menu.

There are three update mode options: "Never", "At Announce" or "At Reboot", "At Announce" starts firmware update immediately after an announcement is made by the NoTouch Center. "At Reboot" requires a device reboot to initiate firmware update during the device reboot process. Device will auto reboot after firmware update is successful.
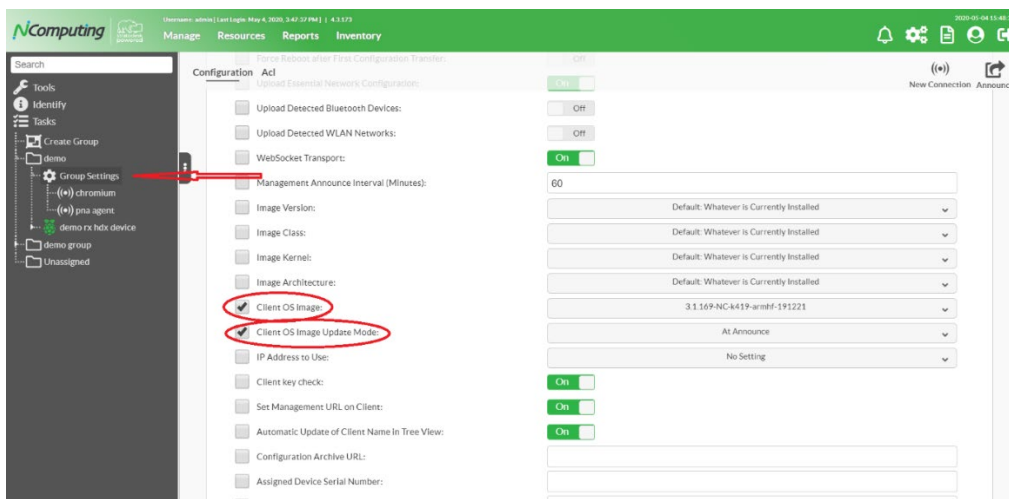
5. Configuring Citrix connections

The main functionality of NComputing RX-HDX and RX420(HDX) thin client devices are acting as a Citrix clients. The Citrix Workspace App (formerly known as Citrix Receiver) is contained in NoTouch OS and allows user authentication, published resources enumeration, and published resource launching in Citrix environments consisting of Citrix Virtual Apps and Desktops (XenApp and XenDesktop) systems. Citrix connections can be brokered by the legacy Web Interface 5.4, by StoreFront, or by Citrix Gateways (NetScaler Gateways). Also the unique Citrix Workspace Hub functionality, which allows roaming and casting desktops from other Citrix Workspace Apps, can be enabled on NComputing RX-HDX and RX420(HDX) thin clients.

Note: All the connection-specific configuration settings described in subsequent sections of this chapter will only take effect when the connection will be restarted. For Citrix connections the user must be logged off and then logged on again for the configuration changes to take effect.

5.1. Citrix Workspace App Connection

To add a connection which will be brokered by Citrix Workspace App (formally StoreFront) open the Configuration UI, go to Connections, and click the 'Add' button to create a new connection.

Following settings must be configured for StoreFront connections:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection*	Connection name	*Give a descriptive name to the new connection.*
Connections > *Connection*	Connection mode	Citrix/WorkSpace App
Connections > *Connection*	Connection target (server name, IP, URL)	*HTTPS URL of Workspace App target.*

It's advisable to always specify a complete Store URL as the 'Connection target' parameter (like: https://storefront.company.local/Citrix/StoreName/discovery). Shortened forms of the Store URL should be avoided.

More information about configuring Workspace App connections can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Citrix_Receiver_configuration#Browser-based_login

5.2. Citrix Gateway connections

To add a connection which will be brokered by StoreFront located behind a Citrix Gateway (Citrix NetScaler Gateway), open the Configuration UI, go to Connections, and click the 'Add' button to create a new connection.

Following settings must be configured for Citrix Gateway connections:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection*	Connection name	*Give a descriptive name to the new connection.*

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection*	Connection mode	Citrix/StoreFront
Connections > *Connection*	Connection target (server name, IP, URL)	*HTTPS URL of target Citrix Gateway (possibly also indicating what Store to connect to).*

Pre-selecting the Store when StoreFront with multiple Stores is located behind the Gateway

When a Store configured on a StoreFront server will be accessed directly (without going through Citrix Gateway) then the store name is included in connection target URL and there is no doubt which Store should handle the brokering requests. In scenarios when a StoreFront server hosting multiple Stores will be accessed through Citrix Gateway then the user authentication will be handled directly on the Gateway, but the enumeration of the published resources will be ceded to a Store on the StoreFront server. If Citrix Gateway is not configured to use any specific Store by default then the Citrix Workspace App, to allow the user to select the Store to proceed with, shows a list of Stores which are present on the StoreFront server located behind the Citrix Gateway. This can be confusing to some users and to avoid this confusion the name of the Store to go with can be specified as part of the Citrix Gateway, like: https://gateway.company.com?StoreName. More information about this option can be found in Citrix product documentation:

https://docs.citrix.com/en-us/citrix-workspace-app-for-linux/secure.html#connecting-through-citrix-gateway.

Avoiding duplicated logon prompts

When configuring RX-HDX and RX420(HDX) thin client devices for Citrix Gateway connections it is very important to make sure, that the StoreFront which will broker the published resources to RX-HDX and RX420(HDX) users is configured properly. Special attention must be paid to StoreFront's beacons configuration when the devices will access the Citrix Gateway from the Internet. The internal beacon URLs must not be accessible in such case, especially no StoreFront servers must be accessible under internal beacon's URL. Not fulfilling this requirement will result in duplicated credentials prompts being presented to the users. SSL issues can appear too when devices located in the Internet configured to work through Citrix Gateways will suddenly manage to connect to some (especially internal) StoreFront servers which will present SSL certificates signed by private Certificate Authority, for which the devices accessing the infrastructure from the Internet will likely not have the root or intermediate certificates. Only the external beacon URL(s) and the connection target URL (set to Citrix Gateway URL) should be accessible from the device connecting from the Internet to avoid issues.

5.3. PNAgent connections

To add a connection which will be brokered by Citrix Web Interface Services Site (PNAgent site, StoreFront XenApp Services site) open the Configuration UI, go to Connections, and click the 'Add' button to create a new connection.

Following settings must be configured for PNAgent connections:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection*	Connection name	*Give a descriptive name to the new connection.*
Connections > *Connection*	Connection mode	Legacy Citrix/Program Neighborhood (PNA)
Connections > *Connection*	Connection target (server name, IP, URL)	*HTTP or HTTPS URL of target Citrix Web Interface Services Site.*

It's advisable to always specify a complete Services Site URL as the 'Connection target' parameter (like: https://wiserver.company.local/Citrix/PNAgentSiteName/config.xml). Shortened forms of the Services Site URL should be avoided.

More information about configuring Citrix PNAgent connections can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Citrix_Receiver_configuration#Non-StoreFront_XenApp

5.4. Workspace Hub connections

To add a connection which will turn the NComputing RX-HDX and RX420(HDX) thin client devices into Citrix Workspace Hub open the Configuration UI, go to Connections, and click the 'Add' button to create a new connection.

Following settings must be configured to enable Citrix Workspace Hub:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection*	Connection name	*Give a descriptive name to the new connection.*
Connections > *Connection*	Connection mode	Citrix/Workspace Hub
Connections > *Connection*	Connection target (server name, IP, URL)	*Comma-separated list of URLs pointing to websites, which will be opened on subsequent pages of Workspace Hub background.*

Please refer to the following Citrix documentation on the detailed Workspace Hub user guide:

https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/devices/workspace-hub.html

5.5. Skype for Business optimization

The Citrix HDX Realtime Media Engine (RTME) is the client-side component of the Citrix HDX Realtime Optimization Pack for Skype for Business. RX-HDX and RX420(HDX) thin clients come with RTME integration; by default, the HDX Realtime Media Engine is disable and must be enabled for the Citrix connection to optimize the Skype for Business experience. for information on how to enable RTME on RX-HDX and RX420(HDX) thin clients, please reference to the NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Citrix_Receiver_configuration

section: HDX RealTime Media Engine (RTME)

6. Redirecting peripheral devices to Citrix sessions

6.1. General information

There are two methods of peripheral devices redirection: the functional redirection and the generic USB redirection. The methods differ in the way how the device is handled on both sides of the terminal connection. The functional and the generic USB redirection methods <u>are mutually exclusive</u>. One method should be disabled when the other one has to be used.

<u>Functional redirection</u>

The functional redirection provides an optimized native redirection for supported peripheral devices. It always requires some kind of peripheral device handling on the client side. Device driver, dedicated service, or a daemon might be necessary on the client side for the functional redirection. During functional redirection the device-specific application-layer communication gets redirected to the Citrix session. How the peripheral device is connected to the client device (USB, serial port, network, etc.) does not matter for the functional redirection. The redirected device not always appears in the Device Manager inside Citrix session. The functional redirection is usually the best choice for Citrix Virtual Apps (XenApp) connections, where multiple users have to share the resources of a single server (VDA machine), as the server-side components ensure that the redirected device will be visible and accessible in appropriate session only. The functional redirection, if it is available for particular device type, usually also provides optimized (e.g. ensuring best performance) support for Citrix Virtual Desktops (XenDesktop) VDI sessions.

<u>Generic USB redirection</u>

Generic USB redirection, in contrast to functional redirection, does not require any device specific driver, service, nor daemon on the client side to handle the redirected peripheral device. The 'Citrix USB forwarder' daemon must be enabled under NoTouch OS 'Configuration > Services > Citrix USB' though. With the generic USB redirection the low-level USB communication between the virtual USB hub and the USB device gets redirected. Obviously only devices connected to client's USB ports can be handled. The USB device connected to client's USB port gets detected by the 'Citrix remote USB bus' hub assigned to the user's Citrix session on the server side. The necessary device driver software must be installed on the Citrix server (VDA machine). Other device-specific software components must be installed on the Citrix server (VDA) side too. The peripheral device forwarded with generic USB redirection always appears in the Device Manger inside Citrix session as connected to 'Citrix remote USB bus'. Historically the generic USB redirection was an option for Citrix XenDesktop VDI (with desktop OS) connection only. Lately also the Citrix Virtual Apps (XenApp) servers support this method, the condition though is a modern server OS (Windows Server 2012, or newer), where the "per-session USB devices" are supported. For Citrix Virtual Apps and Desktops (XenApp and XenDesktop) the generic USB redirection is the last resort option for peripheral devices, for which the functional redirection does not exist. This method works fine for Citrix Virtual Desktops (XenDesktop) connections where one single user works in Console session and no other users compete to share the same peripheral device. This method might work for Citrix Virtual Apps (XenApp) connections too if no device specific software (like a service expecting the user to work in Console session) must be installed besides the device driver (which must be multi-session capable).

Comparison of functional and generic USB device redirection

For some peripheral device classes only the functional redirection is possible, for some other only the generic USB redirection. There are peripheral devices for which both methods can be used, but the functional redirection in such case is usually the best choice. Only when the application software which needs to communicate with the peripheral device is having issues with the functional redirection the generic USB redirection should be used.

Peripheral device	Functional (native) redirection	Generic USB redirection	Preferred redirection method
Mass storage	Possible	Possible	Functional
Smart card readers	Possible	Impossible	Functional
Printers	Possible	Possible	Functional
Scanners	Impossible	Possible	Generic USB
Serial ports	Possible	Possible	Functional
Audio	Possible	Impossible	Functional
Webcams	Possible	Possible	Functional
Human Interface Devices (other than keyboards and mice)	Impossible	Possible	Generic USB
Fingerprint readers	Impossible	Possible	Generic USB
Signature pads (serial)	Possible	Possible	Functional
Signature pads (HID)	Impossible	Possible	Generic USB
Clipboard	Possible	Impossible	Functional
Bluetooth adapters	Impossible	Impossible	-
3G modems	Impossible	Impossible	-

6.2. Redirecting specific peripheral devices

Server-side configuration for functional redirection

The Citrix Policies (which are configurable in Citrix Studio on the Desktop Delivery Controller) usually allow the functional redirection of most popular peripheral devices by default. For readers' convenience the Citrix Policy settings which control the functional redirection of different peripheral devices will be listed in each device-specific sections below.

Server-side configuration for generic USB redirection

If the generic USB redirection needs to be used for particular peripheral device then a Citrix Policy needs to be created on the Desktop Delivery Controller and made applicable to user session to enable the necessary server-side mechanisms. These mechanisms are disabled by default.

Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

6.2.1. Mass storage

Functional redirection of mass storage devices

The functional redirection of mass storage device is enabled by default on RX-HDX and RX420(HDX) clients and no special actions must be taken to get it working. The functional redirection of mass storage devices can be explicitly enabled in NoTouch OS or NoTouch Center under connection's Citrix Workspace App settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local drives	On
Connections > *Connection* > Citrix Workspace App	Dynamic local drives mapping	On

Citrix Policy settings for functional mass storage redirection:

Citrix Policy setting name	Citrix Policy setting value
Client drive redirection	Allowed
Auto connect client drives	Enabled
Client fixed drives	Allowed
Client removable drives	Allowed
Client network drives	Allowed
Client optical drives	Allowed
Client USB redirection rules	Deny: Class=08

Note: The 'Client USB redirection rules' Citrix Policy setting must be configured to exclude USB mass storage devices (Deny: Class=08) only if the 'Client USB device redirection' Citrix Policy setting is enabled to allow generic USB redirection of some other devices.

Generic USB redirection of mass storage devices

The generic USB redirection of mass storage devices can be enabled with following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Start Citrix USB forwarder	with Citrix connection

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The generic USB redirection of mass storage devices can be enabled with following per-connection settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local drives	off
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	On

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Desktop Appliance Mode for USB devices	on

Citrix Policy settings for generic USB redirection of mass storage devices:

Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

6.2.2. Smart card readers

Functional redirection of smart card readers

Functional redirection of smart card readers requires enabling the smart card reader support on the RX-HDX and RX420(HDX) client sides. The Linux components responsible for this support are the PC/SC daemon and the PC/SC driver for the smart card reader. NoTouch OS contains the driver for CCID-compliant smart card readers, as well as few additional dedicated smart card reader drivers (ACS, OmniKey). You can check whether your smart card reader is supported by the CCID driver by visiting following web pages:

https://ccid.apdu.fr/ccid/supported.html, https://ccid.apdu.fr/ccid/shouldwork.html.

To enable functional redirection of smart card readers configure following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Smartcard	Smartcard service (PCSC)	On
Services > Smartcard	Device driver for smartcard	*Try 'All' or 'CCID' first of all. For ACS or OmniKey readers select the dedicated driver.*

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

There are no Citrix Policy settings for controlling the redirection of smart card readers and smart cards.

Generic USB redirection of smart card readers

Generic USB redirection of smart card readers is not possible.

6.2.3. Printers

General information about functional redirection of client printers

Locally connected USB printers and network printers (JetDirect, RAW, AppSocket) are supported, but some models can be problematic. Low-cost GDI printers should be avoided. More advanced printers understanding the PCL and/or PostScript languages are advisable and should work. The CUPS (Common Unix Printing Subsystem) daemon must be enabled on the RX-HDX and RX420(HDX)

devices for the functional printer redirection. CUPS provides local printing support which Citrix Workspace App relies on.

Citrix Universal Print Driver is not supported. Native Windows printer drivers must be installed on all Citrix servers (VDA machines) to which the local USB printers will be redirected.

ThinPrint is not supported.

Functional redirection of USB printers

To enable functional redirection of USB printers, configure the following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > CUPS Printing	CUPS	On
Services > CUPS Printing	Bind CUPS-LPD service to localhost	On

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

Besides enabling the CUPS daemon, the USB printer must be added to device configuration. This must be accomplished under 'Drives/Printers > Printers'. After adding a new printer, the following printer-specific NoTouch settings must be configured:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Drives/Printers > Printers > Printer: *Printer name*	Printer name	*The name of the local printer. This name will be reported to Citrix session. Printer names can't contain spaces.*
Drives/Printers > Printers > Printer: *Printer name*	Port	USB 1 *Note: As USB port numbering is non-deterministic connecting more than one USB printer should be avoided, as it can end-up with print jobs being produced using wrong Windows printer driver.*
Drives/Printers > Printers > Printer: *Printer name*	Windows printer driver name	*The exact name of the Windows printer driver to be used inside Citrix session for the redirected client printer.*

The functional redirection of local printers is enabled by default. It can be explicitly enabled in NoTouch OS or NoTouch Center under connection's Citrix Workspace App settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local printers	On

Citrix Policy settings for functional redirection of USB printers:

Citrix Policy setting name	Citrix Policy setting value
Client printer redirection	Allowed
Auto-create client printers	Auto-create all client printers
Universal print driver usage	Use only printer model specific drivers

As Citrix Universal Print Driver cannot be used with the RX-HDX and RX420(HDX) thin client devices the printer model specific drivers <u>must be installed on all Citrix servers (VDA machines)</u> where the RX-HDX and RX420(HDX) devices will start the sessions. The list of Windows printer drivers installed on Citrix server (VDA machine) can be obtained with following command:

```
wmic /NameSpace:\\Root\CIMV2 path Win32_PrinterDriver GET Name
```

The command output will be a list of installed printer drivers with comma-separated driver properties in form of:

Driver_name,driver_class,driver_architecture

For functional redirection of client printers, the class 3 driver for Windows x64 architecture (assuming the VDA OS is 64-bit) should be selected. <u>Class 4 drivers are known to cause issues with functional redirection of client printers.</u>

Example

The 'wmic' command provided following output:

```
C:\>wmic /NameSpace:\\Root\CIMV2 path Win32_PrinterDriver GET Name

Name
HP Color LaserJet CM1312 MFP PCL6 Class Driver,4,Windows x64
Canon Inkjet iP100 series,4,Windows x64
Microsoft XPS Document Writer v4,4,Windows x64
HP Deskjet 5520 series,3,Windows x64
Generic / Text Only,3,Windows x64
Canon D400-450 UFRII LT XPS,3,Windows x64
```

One of the listed printer drivers is 'HP Deskjet 5520 series', which is a class 3, 64-bit Windows printer driver. If a printer using this driver should be redirected from the RX-HDX and RX420(HDX) thin client

devices to Citrix session, then this driver name should be used literally as the value of the 'Windows printer driver name' NoTouch Setting:

With the above configuration Citrix Workspace App will report to Citrix session the presence of the local 'HP_DJ5520' printer and request the Citrix server (the VDA machine) to use the 'HP Deskjet 5520 series' Windows printer driver for the printer created in the session. The NoTouch OS of the RX-HDX and RX420(HDX) client devices will also internally create a local printer with the name 'HP_DJ5520' and will use the USB port for the communication with it.

This will result with the printer being redirected to the Citrix session:
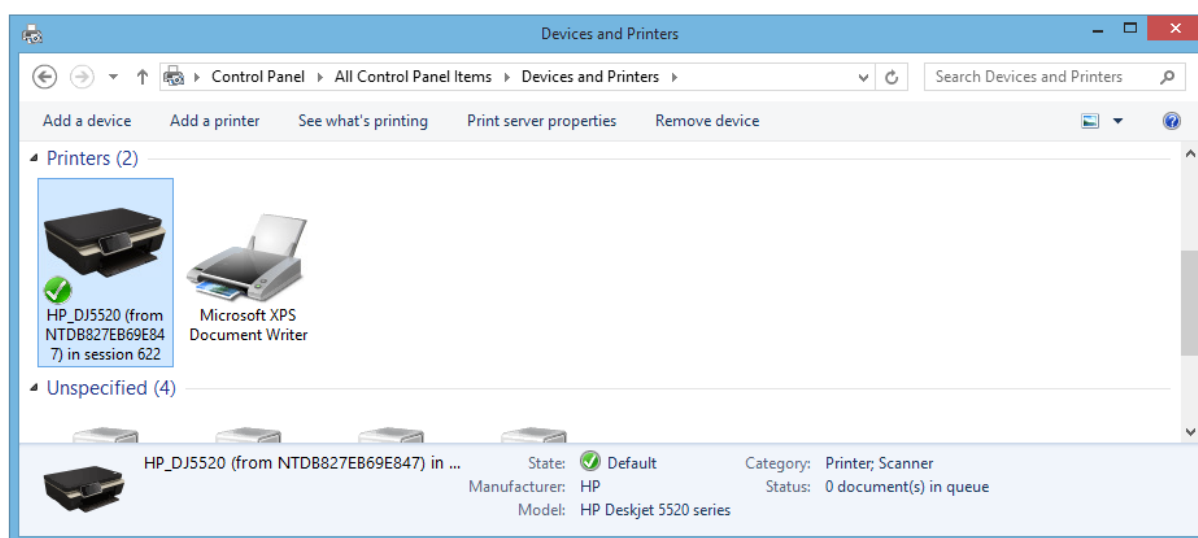
Functional redirection of network printers

With NoTouch OS running on NComputing RX-HDX and RX420(HDX) devices not only local USB printers can be redirected to Citrix session, but also network printers. Network printers supporting the HP JetDirect (sometimes referred to as 'RAW print servers', 'TCP 9100 print servers', or print servers supporting the AppSocket protocol) can be redirected in similar way as local USB printers.

To enable functional redirection of network printers, configure following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > CUPS Printing	CUPS	On

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > CUPS Printing	Bind CUPS-LPD service to localhost	On

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

Besides enabling the CUPS daemon the network printer must be added to device configuration. This must be accomplished under 'Drives/Printers > Printers'. After adding a new printer, the following printer-specific NoTouch settings must be configured:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Drives/Printers > Printers > Printer: *Printer name*	Printer name	*The name of the local printer. This name will be reported to Citrix session. Printer name can't contain spaces.*
Drives/Printers > Printers > Printer: *Printer name*	Port	Remote Printer
Drives/Printers > Printers > Printer: *Printer name*	Windows printer driver name	*The exact name of the Windows printer driver to be used inside Citrix session for the redirected client printer.*
Drives/Printers > Printers > Printer: *Printer name*	Print server name/address	*IP address or FQDN of the network printer.*
Drives/Printers > Printers > Printer: *Printer name*	TCP printing port	9100

The functional redirection of local printers (network printers are considered to be local too) is enabled by default. It can be explicitly enabled in NoTouch OS or NoTouch Center under connection's Citrix Workspace App settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local printers	On

Citrix Policy settings for functional redirection of network printers:

Citrix Policy setting name	Citrix Policy setting value
Client printer redirection	Allowed
Auto-create client printers	Auto-create all client printers
Universal print driver usage	Use only printer model specific drivers

As Citrix Universal Print Driver cannot be used with the RX-HDX and RX420(HDX) devices the printer model specific drivers must be installed on all Citrix servers (VDA machines) where the RX-HDX and RX420(HDX) devices will start the sessions. The list of Windows printer drivers installed on Citrix server (VDA machine) can be obtained with following command:

```
wmic /NameSpace:\\Root\CIMV2 path Win32_PrinterDriver GET Name
```

The command output will be a list of installed printer drivers with comma-separated driver properties in form of:

Driver_name,driver_class,driver_architecture

For functional redirection of client printers, the class 3 drivers for Windows x64 architecture (assuming the VDA OS is 64-bit) should be selected. Class 4 drivers are known to cause issues with functional redirection of client printers.

Example

The 'wmic' command provided following output:

```
C:\>wmic /NameSpace:\\Root\CIMV2 path Win32_PrinterDriver GET Name

Name
HP Color LaserJet CM1312 MFP PCL6 Class Driver,4,Windows x64
Canon Inkjet iP100 series,4,Windows x64
Microsoft XPS Document Writer v4,4,Windows x64
HP Deskjet 5520 series,3,Windows x64
Generic / Text Only,3,Windows x64
Canon D400-450 UFRII LT XPS,3,Windows x64
```

One of the listed printer drivers is 'HP Deskjet 5520 series', which is a class 3, 64-bit Windows printer driver. If a network printer using this driver should be redirected from the RX-HDX and RX420(HDX) client devices to Citrix session, then this driver name should be used literally as the value of the 'Windows printer driver name' NoTouch Setting:

With the above configuration Citrix Workspace App will report to Citrix session the presence of the local 'HP_DJ5520_network' printer and request the Citrix server (the VDA machine) to use the 'HP Deskjet 5520 series' Windows printer driver for the printer created in the session. The RX-HDX and RX420(HDX) client devices will also create a local printer with the name 'HP_DJ5520_network' and communicate with it using the JetDirect protocol over the specified IP address and TCP port 9100. This will result with the printer being redirected to the Citrix session:
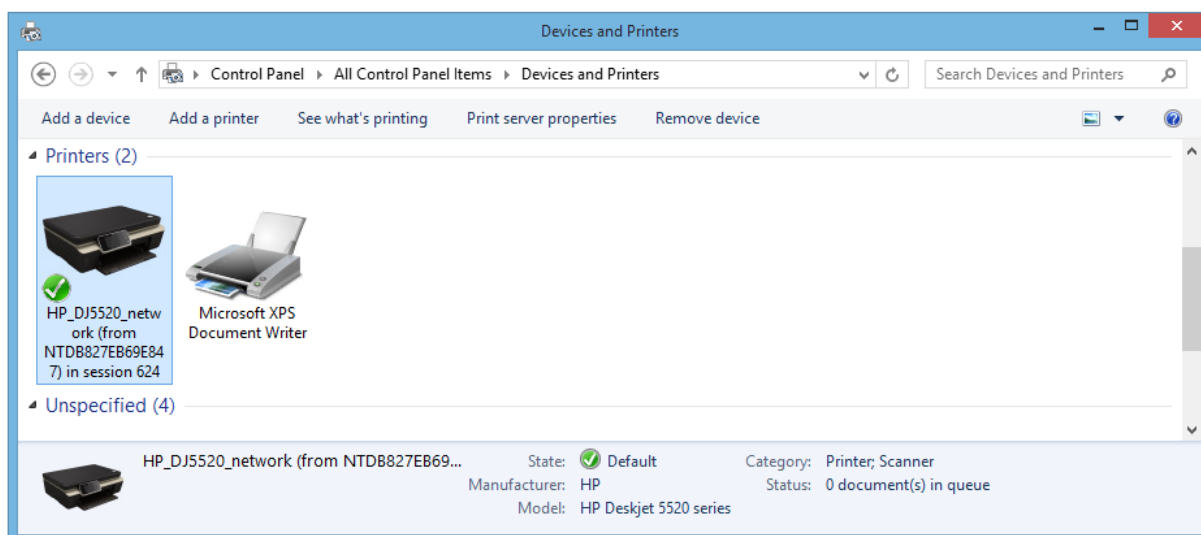
Troubleshooting issues with functional redirection of USB or network printers

Note: Contents for this section will be provided in future edition of this guide.

Generic USB redirection of USB printers

The generic USB redirection of USB printers can be enabled with following NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Start Citrix USB forwarder	with Citrix connection
Services > CUPS Printing	CUPS	off

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The generic USB redirection of printers can be enabled with following per-connection settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local printers	off
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	On
Connections > *Connection* > Citrix Workspace App	Desktop Appliance Mode for USB devices	on

Note: The connection must be restarted for the above changes to take effect.

Citrix Policy settings for generic USB redirection of mass printers:

Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

6.2.4. Serial ports

Functional redirection of serial ports

Although the NComputing RX-HDX and RX420(HDX) thin client devices do not have any user accessible serial ports some customers might need to connect to the thin clients and to redirect to Citrix sessions certain serial devices. Typical examples are receipt printers, cash drawers, magnetic stripe readers, some signature pads, specialized hardware appliances, etc. Such devices are accessed from the controlling application by referring to Windows serial port names, like COM1, COM2, … If the application runs in a Citrix session, then the serial port of the client device must be redirected to the Citrix server (VDA machine) to make the serial device accessible by the controlling application. USB-to-serial adapters can be connected to RX-HDX and RX420(HDX) thin clients to create the serial ports where the actual serial devices can be connected. Some peripheral devices have the USB-to-serial adapter module integrated and only expose the USB interface, but actually they act and must be handled as serial devices. The NoTouch OS running on the RX-HDX and RX420(HDX) thin clients contains a selection of drivers for different USB-to-serial adapters. Drivers for the most popular adapters based on the Prolific pl2303 and FTDI chipsets are included.

The functional redirection of serial ports is enabled by default. It can be explicitly enabled in NoTouch OS or NoTouch Center under connection's Citrix Workspace App settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local serial/COM ports	On

NoTouch OS by default configures Citrix Workspace App to look for four local serial ports. These are:

- /dev/ttyS0
- /dev/ttyS1
- /dev/usb/tts/0
- /dev/ttyUSB0

Optionally (if enabled) the '/dev/ttyACM0' serial port can be included too. This configuration does not exactly match the specifics of the RX-HDX and RX420(HDX) hardware platform. The /dev/ttyUSB0 port, which most likely will be created after connecting to RX-HDX and RX420(HDX) a USB-to-serial adapter, will be reported to Citrix server as the local COM4 port. This is often not the desired behavior and working around it requires some additional setup (like creating a user logon script) for the Citrix server (VDA machine). To avoid this additional server-side setup we advise to explicitly configure Citrix Workspace App to report the right number of local serial ports. The Linux device names representing each serial port should also be explicitly specified. To achieve that some user defined Citrix Workspace App parameters must be added to Citrix connection configuration.

To specify the correct number of local serial ports to be redirected the following user defined parameter needs to be added:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter1*	Target INI file	wfclient.ini
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter1*	Target section in INI file	WFClient
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter1*	Key	LastComPortNum
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter1*	Value	*Desired number of serial ports to be redirected.*

For each local serial port the following user defined parameter needs to be added separately:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter2*	Target INI file	wfclient.ini
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter2*	Target section in INI file	WFClient
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter2*	Key	ComPort1 *Note: Use ComPort2, ComPort3, and so on, for subsequent ports.*
Connections > *Connection* > Citrix Workspace App > User Defined > *wfclient_parameter2*	Value	*Linux device name of the COM port.*

Functional redirection of serial ports and generic USB redirection of USB-to-serial adapters are mutually exclusive. To prevent possible interferences between both mechanisms the generic USB redirection should be disabled under connection's Citrix Workspace App settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	off

Alternatively, when the generic USB redirection is necessary for some other USB devices (and thus must stay turned on), the USB-to-serial adapter (identified by its VID and PID) should be excluded from the generic USB redirection with the following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Deny devices	vid=*Adapter's VID* pid=*Adapter's PID*, class=02,class=09,class=03 subclass=01 prot=01,class=03 subclass=01 prot=02,class=0a,class=0b,class=0e,class=e0

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The USB classes specified here are the standard exclusions of generic USB redirection. They must be explicitly added here, as creating a custom 'Deny devices' rule removes the default deny rules.

Citrix Policy settings for functional redirection of serial ports:

Citrix Policy setting name	Citrix Policy setting value
Client COM port redirection	Allowed
Auto-connect client COM ports	Enabled

For older systems, like XenApp/XenDesktop 7.6, where this policy does not exist, please refer to:

https://support.citrix.com/article/CTX139345.

Example

Serial port created with a USB-to-serial adapter needs to be redirected to the Citrix session. To determine the Linux device name for the serial port the 'dmesg' command can be executed in RX-HDX's Console (or SSH session) immediately after physically connecting the USB-to-serial adapter. At the end of 'dmesg' output lines similar to the following will appear:

```
[ 7305.321487] usb 1-1.2: new full-speed USB device number 5 using dwc_otg
[ 7305.453712] usb 1-1.2: New USB device found, idVendor=067b, idProduct=2303
[ 7305.453722] usb 1-1.2: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[ 7305.453726] usb 1-1.2: Product: USB-Serial Controller D
[ 7305.453730] usb 1-1.2: Manufacturer: Prolific Technology Inc.
[ 7305.495419] usbcore: registered new interface driver usbserial
[ 7305.495462] usbcore: registered new interface driver usbserial_generic
[ 7305.495490] usbserial: USB Serial support registered for generic
[ 7305.511765] usbcore: registered new interface driver pl2303
[ 7305.511810] usbserial: USB Serial support registered for pl2303
[ 7305.511883] pl2303 1-1.2:1.0: pl2303 converter detected
[ 7305.516463] usb 1-1.2: pl2303 converter now attached to ttyUSB0
```

The above output indicates that an adapter with chipset manufactured by Prolific Technology Inc. has been connected. Adapter's USB Vendor ID (VID) is 067b, the Product ID (PID) is 2303. The 'usbserial' and 'pl2303' drivers were loaded, and the ttyUSB0 port (/dev/ttyUSB0) was created. If this is the only local serial port which needs to be redirected to be redirected then the following user defined parameters for the Workspace App must be added to Citrix connection:

User defined

Connections / NCAWS-EU / Citrix Workspace App / User defined / wfclient.ini [WFClient] ComPort1=/dev/ttyUSB0

Target INI file	wfclient.ini
Target section in INI file	WFClient
Key	ComPort1
Value	/dev/ttyUSB0

If the generic USB redirection has to be used for some other devices, then the VID and PID pair of the USB-to-serial adapter ('vid=067b pid=2303' in this example) must be excluded from the generic USB redirection. The 'Deny device' list must be set to: 'vid=067b pid=2303,class=02,class=09,class=03 subclass=01 prot=01,class=03 subclass=01 prot=02,class=0a,class=0b,class=0e,class=e0'. Please note that there are no spaces after the commas used to separate the list entries.

The USB classes specified here are the standard exclusions of generic USB redirection. They must be explicitly added here, as creating a custom 'Deny devices' rule removes the default deny rules.

Citrix USB

Services / Citrix USB

Start Citrix USB forwarder	with Citrix connection
Allow devices	
Deny devices	vid=067b pid=2303,class=02,class=09,class=03 subclass=01 prot=01,class=03 subclass=01 prot=02,cla

The 'net use' command can be executed in Command Prompt inside the Citrix session to verify if the RX-HDX and RX420(HDX) client's COM1 port (/dev/ttyUSB0) has been redirected:

```
C:\>net use

New connections will be remembered.


Status       Local    Remote                    Network
-------------------------------------------------------------------------
             COM1     \\Client\COM1:            Citrix Client Network

The command completed successfully.
```

Indeed, client's COM1 port has been redirected to session's COM1 port. Now any application launched in this Citrix session can open the COM1 port and communicate with the serial device connected to the USB-to-serial adapter.

Troubleshooting issues with functional redirection of serial ports

Note: Contents for this section will be provided in future edition of this guide.

Generic USB redirection of serial ports (USB-to-serial adapters)

Besides functional redirection also the generic USB redirection can be used for the serial ports. In this case the USB-to-serial adapter will be redirected to the Citrix session as a USB device, not the serial port. This method should be used when the application running on the Citrix server (VDA machine) has issues with accessing the serial device through the serial port redirected in the functional way. This method should work in Citrix Virtual Desktops (XenDesktop) sessions. It can also work for Citrix Virtual Apps (XenApp) sessions if the VDA runs on a modern OS (Windows Server 2012 or newer). Device driver appropriate for the redirected USB-to-serial adapter must be installed on the Citrix server (VDA machine).

The generic USB redirection of USB-to-serial adapters can be enabled with following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Start Citrix USB forwarder	with Citrix connection

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The generic USB redirection of USB-to-serial adapters can be enabled with following per-connection settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Map local serial/COM ports	off
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	On
Connections > *Connection* > Citrix Workspace App	Desktop Appliance Mode for USB devices	on

Citrix Policy settings for generic USB redirection of USB-to-serial adapters:

Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

6.2.5. Document scanners

Functional redirection of document scanners

Functional redirection of document scanners is not possible.

Generic USB redirection of document scanners

The generic USB redirection of document scanners can be enabled with following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Start Citrix USB forwarder	with Citrix connection

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The generic USB redirection of document scanners can be enabled with following per-connection settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	On
Connections > *Connection* > Citrix Workspace App	Desktop Appliance Mode for USB devices	on

Citrix Policy settings for generic USB redirection of document scanners:

Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

6.2.6. Audio

The RX-HDX and RX420(HDX) thin client devices can send the audio output to the integrated 3.5mm analog audio jack, to the HDMI interface, or to a connected USB audio device (which can also provide microphone input). Bluetooth audio is not supported.

Functional redirection of audio

The functional redirection of audio can be used for all types of supported audio devices (analog, HDMI, USB). Inside of the Citrix sessions users can use the virtual 'Citrix HDX Audio' playback and recording devices.

Functional redirection of client audio is enabled by default and optimized for USB audio.

Following system-wide NoTouch settings must be configured to optimize the functional redirection of analog audio:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Audio	Standard audio device	Analog
Audio > PulseAudio	Timer-based scheduling (tsched)	off

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

Following system-wide NoTouch settings must be configured to optimize the functional redirection of HDMI audio:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Audio	Standard audio device	HDMI
Audio > PulseAudio	Timer-based scheduling (tsched)	off

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

Following system-wide NoTouch settings must be configured to optimize the functional redirection of USB audio:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Audio	Standard audio device	USB
Audio > PulseAudio	Timer-based scheduling (tsched)	no setting

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The functional redirection of client audio is enabled by default for Citrix connections. It can be explicitly enabled in NoTouch OS or NoTouch Center under connection's Citrix Workspace App settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Audio output	High Quality
Connections > *Connection* > Citrix Workspace App	Audio input/microphone	On

Note: The 'Audio output' setting can also be set to 'Medium Quality' or 'Low Quality' to save network bandwidth at the cost of audio quality, or set to 'off' to disable the functional redirection of client audio

Generic USB redirection of audio devices

Note: Contents for this section will be provided in future edition of this guide.

6.2.7. Webcams

Functional redirection of webcams

Functional redirection of webcams leverages the 'HDX RealTime webcam video compression' feature of Citrix Virtual Apps and Desktop (XenApp and XenDesktop) systems. Functional webcam redirection offers an optimized support, as the video stream obtained from the webcam will be compressed before being sent to Citrix session. Such approach greatly reduces the amount of data sent over the network and lowers network bandwidth consumption. As the encoding happens with the help of RX-HDX's and RX420(HDX) hardware-based H.264 encoder also the RX-HDX and RX420(HDX) client device's CPU does not get overloaded, which ensures good user session responsiveness.

Only 'Video for Linux V2' (v4l2) compliant webcams can be used for functional redirection, as they provide standardized interface to the video device. Such webcams are sometimes referred to as UVC (USB video class) devices or 'driverless Windows webcams', as no driver installation is required to use them on Windows systems.

Virtual 'Citrix HDX Web Camera' device becomes available for user applications running in Citrix sessions. This virtual webcam provides the video stream originating from the webcam connected to RX-HDX and RX420(HDX) thin client devices.

The functional redirection of webcams is enabled by default. It can be explicitly enabled in NoTouch OS or NoTouch Center under connection's Citrix Workspace App HDX/Multimedia settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App > HDX/Multimedia	HDX RealTime webcam video compression	on

There are no Citrix Policy settings for controlling the functional redirection of webcams.

Generic USB redirection of webcams

When the connected webcam is not Video for Linux V2 compliant and requires special drivers, which are not present in NoTouch OS of RX-HDX and RX420(HDX) then the generic USB redirection remains the only way to redirect such webcam. It is important to remember though, that generic USB redirection is not the optimal webcam redirection method and unlike the functional redirection (depending on webcam model) it may require transmission of big amounts of uncompressed video data from the thin client device to Citrix session. Also the framerate of the video provided by the webcam redirected in the generic way will be lower compared to webcam redirected in functional way.

As the default redirection method for webcams is the functional redirection the USB video class devices (class=0e) are by default excluded from generic USB redirection. The '0e' class, or the specific webcam device identified by Vendor ID (VID) and Product ID (PID) pair, must be explicitly added to the 'Allow devices' list of Citrix USB forwarder service.

The generic USB redirection of webcams can be enabled with following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Start Citrix USB forwarder	with Citrix connection
Services > Citrix USB	Allow devices	vid=*Webcam's VID* pid=*Webcam's PID*

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The VID and PID of the connected webcam can be found in the output of the 'dmesg' command executed in RX-HDX and RX420(HDX) Linux console (or in SSH session) immediately after physically attaching the webcam to the RX-HDX and RX420(HDX) thin client devices.

The generic USB redirection of webcams can be enabled with following per-connection settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	On
Connections > *Connection* > Citrix Workspace App	Desktop Appliance Mode for USB devices	On

Citrix Policy settings for generic USB redirection of webcams:

| Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

Example

A Creative Labs VF0640 Live! Cam Socialize webcam connected to RX-HDX thin client device needs to be redirected in generic way to Citrix session. 'dmesg' output contains the following:

```
[12159.251396] usb 1-1.5: USB disconnect, device number 6
[12162.121510] usb 1-1.5: new high-speed USB device number 7 using dwc_otg
[12162.281906] usb 1-1.5: New USB device found, idVendor=041e, idProduct=4083
[12162.281917] usb 1-1.5: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[12162.281922] usb 1-1.5: Product: VF0640 Live! Cam Socialize
[12162.281926] usb 1-1.5: Manufacturer: Creative Labs
[12162.281930] usb 1-1.5: SerialNumber: OI251716
[12162.283911] uvcvideo: Found UVC 1.00 device VF0640 Live! Cam Socialize (041e:4083)
```

The Vendor ID of this webcam is 041e. The Product ID is 4083.

'vid=041e pid=4083' must be specified as the value for the 'Allow devices' NoTouch setting:
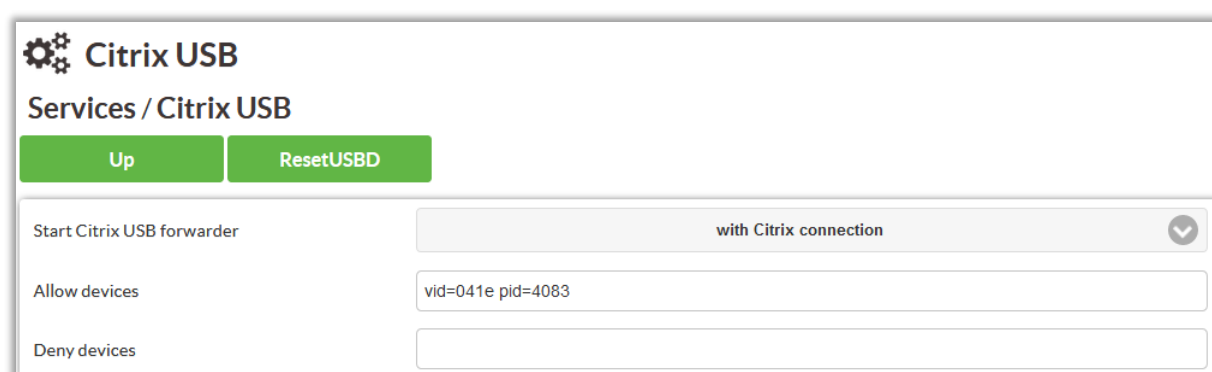
The above configuration results with the Creative Labs VF0640 webcam being redirected as a generic USB device:
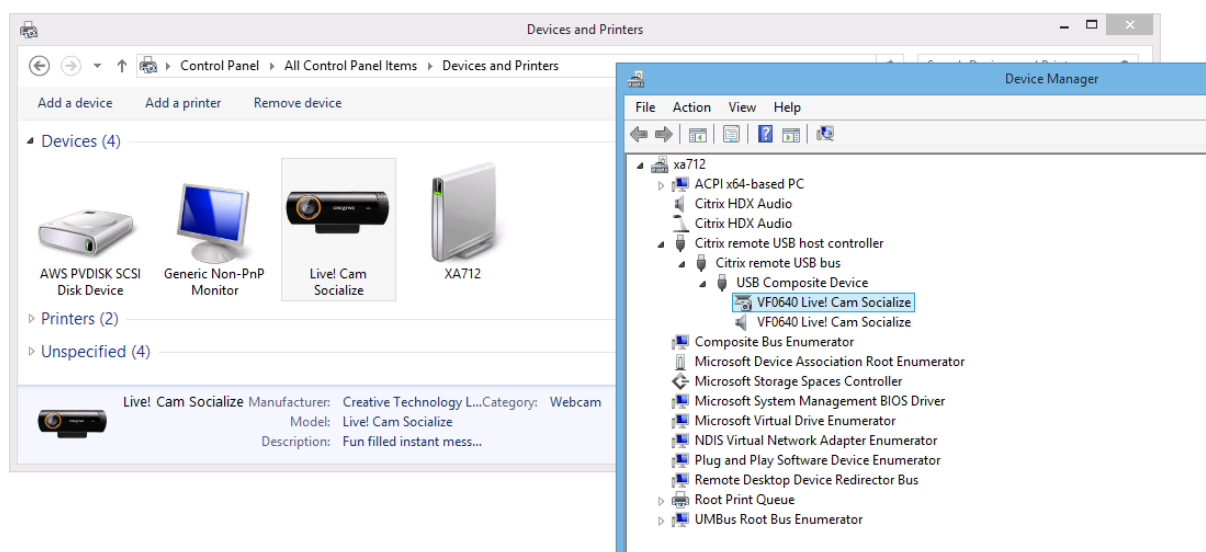
6.2.8. Human Interface Devices

Functional redirection of Human Interface Devices

Citrix Workspace App uses the functional redirection for keyboard and mouse HIDs only. This also covers touch screens acting as mice. No other Human Interface Devices can be redirected in the functional way.

Generic USB redirection of Human Interface Devices

There are some Human Interface Devices, like fingerprint (or other biometric) readers, some signature pads, foot pedals, etc. which require redirection to be recognized by applications running on the Citrix servers (VDA machines). As functional redirection for such devices is not available the generic USB redirection can be used for them and the 'per-session USB devices' feature of modern Microsoft operating systems will isolate the devices and make them available in right user session only.

The generic USB redirection of Human Interface Devices (HIDs) can be enabled with following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Citrix USB	Start Citrix USB forwarder	with Citrix connection
Services > Citrix USB	Allow devices	vid=*HID's VID* pid=*HID's PID*

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

The VID and PID of the connected Human Interface Device can be found in the output of the 'dmesg' command executed in RX-HDX and RX420(HDX) Linux console (or in SSH session) immediately after physically attaching the HID to the RX-HDX and RX420(HDX) thin client devices.

The generic USB redirection of HIDs can be enabled with following per-connection settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Connections > *Connection* > Citrix Workspace App	Generic USB forwarding	On
Connections > *Connection* > Citrix Workspace App	Desktop Appliance Mode for USB devices	On

Citrix Policy settings for generic USB redirection of webcams:

Citrix Policy setting name	Citrix Policy setting value
Client USB device redirection	Allowed

Example

A Philips Speech Processing foot pedal Human Interface Device connected to RX-HDX or RX420(HDX) thin client needs to be redirected in generic way to Citrix session. 'dmesg' output contains the following:

```
[20488.511539] usb 1-1.5: new low-speed USB device number 10 using dwc_otg
[20488.684401] usb 1-1.5: New USB device found, idVendor=0911, idProduct=1844
[20488.684413] usb 1-1.5: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[20488.684418] usb 1-1.5: Product: Footcontrol USB
[20488.684422] usb 1-1.5: Manufacturer: Philips Speech Processing
[20488.715201] input: Philips Speech Processing Footcontrol USB as
/devices/platform/soc/3f980000.usb/usb1/1-1/1-1.5/1-1.5:1.0/0003:0911:1844.0007/input/input7
[20488.791887] hid-generic 0003:0911:1844.0007: input,hidraw2: USB HID v1.00 Joystick [Philips
Speech Processing Footcontrol USB] on usb-3f980000.usb-1.5/input0
```

The Vendor ID of this HID is 0911. The Product ID is 1844.

'vid=0911 pid=1844' must be specified as the value for the 'Allow devices' NoTouch setting:

The above configuration results with the Philips Speech Processing foot pedal Human Interface Device being redirected as a generic USB device:
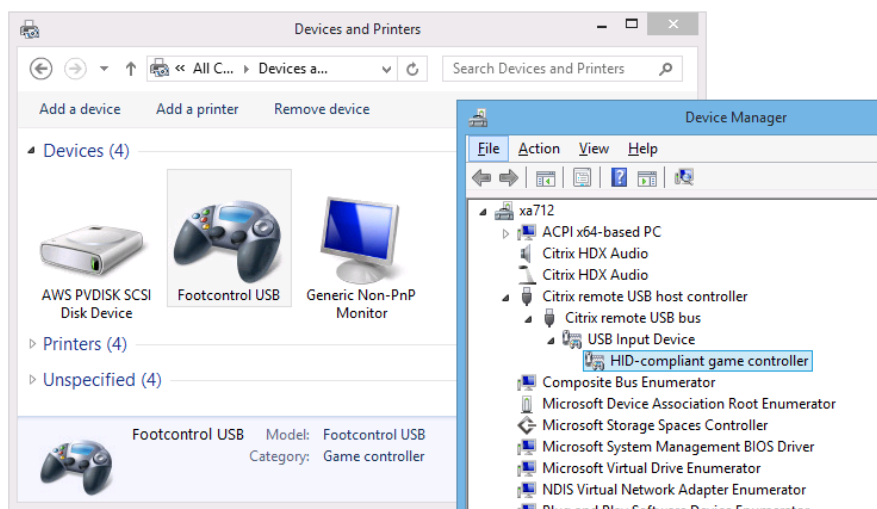
6.2.9. Fingerprint (and other biometric) readers

Many biometric devices, especially fingerprint readers, belong to the Human Interface Device USB class. As no functional redirection is possible for biometric readers the generic USB redirection is the only way to redirect them. Refer to the 'Generic USB redirection of Human Interface Devices' section for the information how to set up the redirection.

6.2.10. Signature pads (serial)

Some signature pad, despite of the fact that they only expose the USB interface, actually contain USB-to-serial adapter modules integrated and the user application communicates with them through

a serial (COM) port. To determine what kind of USB device the signature pad actually is the 'dmesg' command can be executed. If its output will contain lines similar to:

```
[ 7305.511810] usbserial: USB Serial support registered for FTDI USB Serial Device
[ 7305.511883] ftdi_sio 1-1.2:1.0: FTDI USB Serial Device converter detected
[ 7305.516463] usb 1-1.2: FTDI USB Serial Device converter now attached to ttyUSB0
```

then it will indicate that the 'usbserial' driver was loaded and a serial device, 'ttyUSB0' in this example, was created and the signature pad needs to be handled as a serial device.

Refer to the 'Functional redirection of serial ports' section for the information how to redirect signature pads acting as serial ports. If the functional redirection method does not work well for the signature pad try the generic USB redirection, as described in the 'Generic USB redirection of serial ports (USB-to-serial adapters)' section.

If 'dmesg' output will contain lines similar to:

```
[2374.303690] input: Wacom Co.,Ltd. Wacom Intuos Pro M Pen as
/devices/pci0000:00/0000:00:14.0/usb1/1-4/1-4:1.0/0003:056A:0357.000B/input/input23
[2374.303940] wacom 0003:056A:0357.000B: hidraw3: USB HID v1.10 Mouse [Wacom Co.,Ltd. Wacom
Intuos Pro M] on usb-0000:00:14.0-4/input0
```

then it will indicate that the connected device is a HID and must be handles as described in next section.

6.2.11. Signature pads (HID)

Refer to the 'Generic USB redirection of Human Interface Devices' section for the information how to redirect signature pads acting as Human Interface Devices.

6.2.12. Clipboard

Clipboard redirection is enabled by default in RX-HDX and RX420(HDX) thin client devices and can be used to copy/paste objects (text, bitmaps, etc.) between published applications and/or desktops running on same or different Citrix servers (VDA machines). No NoTouch OS configuration is necessary to enable clipboard redirection.

Citrix Policy settings for functional clipboard redirection:

Citrix Policy setting name	Citrix Policy setting value
Client clipboard redirection	Allowed

7. Printing from local applications

Printing from local applications (especially from locally running web browser) is supported, but is limited to the few PPD drivers, which are present in the RX-HDX and RX420(HDX) NoTouch OS by default.

Local printing should be possible with USB and HP JetDirect network printers.

Note: More contents for this section will be provided in future edition of this guide.

8. Troubleshooting devices

8.1. Enabling screen shadowing

Screen shadowing allows an administrator to see what the RX-HDX and RX420(HDX) thin client user has on his or her screen. This can be the local device UI with some local applications, like the Configuration UI, Citrix Workspace App, or web browser, but it can also be a terminal session on a remote server (Citrix, RDSH, etc.).

Note: Shadowing of Citrix sessions is only possible when the session does not use the video codec (H.264) for which the Workspace App utilizes the hardware-accelerated decoder. Shadowing of the hardware-accelerated H.264 decoder output's is not possible.

The VNC (Remote Framebuffer, RFB) protocol will be used for RX-HDX and RX420(HDX) screen shadowing. Any VNC Viewer application can be used to shadow the RX-HDX screen.

Screen shadowing can be enabled with following system-wide NoTouch settings:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > Screen shadowing	Mode	shared
Services > Screen shadowing	Shadowing password	*The password for screen shadowing.*

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

There are few additional parameters on the 'Services > Screen shadowing' configuration page which can be used to adjust shadowing behavior when necessary:

- Mode – Default value: off. Screen shadowing is disabled by default.
  Other possible selections are:
    - once – the VNC server will stop when the VNC Viewer will disconnect.
    - only one – only one VNC Viewer will be able to connect. Connection attempts from other VNC Viewers will be rejected.
    - replace – newly connected VNC Viewer will disconnect previously connected VNC Viewer.
    - shared – allows multiple VNC Viewers to connect to the same RX-HDX or RX420(HDX) device at the same time.
- Ask user at new connection – Default value: off. When set to On the user will have to acknowledge the screen shadowing request.
- Shadowing TCP port – there is no default value. TCP port 5900 (which is standard VNC port) will be used when no other port number is specified.
- Remind user of running VNC shadowing – Default value: On. A red overlay message will notify the user that somebody is shadowing the RX-HDX and RX420(HDX) screen.

8.2. Enabling SSH access

Sometimes, for example to be able to execute some commands when troubleshooting RX-HDX or RX420(HDX) issues, it is useful to have access to the Linux shell of NoTouch OS. Although such shell

access is possible with the Console, which can be opened by a Configuration UI user, the ability to open a Linux shell session from a remote workstation is often a more convenient option. The NoTouch OS contains an SSH server, which is enabled by default and allows remote Linux shell access.

To explicitly enable remote access through the SSH protocol the following NoTouch settings can be configured:

NoTouch setting location	NoTouch setting name	NoTouch setting value
Services > SSH server	Enable SSH service	On

Note: RX-HDX and RX420(HDX) devices must be rebooted for the above changes to take effect.

With the SSH server enabled any SSH client application (like PuTTY for Windows) can be used to start a Linux shell session on RX-HDX and RX420(HDX) devices. The local 'notouchadm' user account with the password specified during initial device setup can be used for logging on. Then the 'notouchadm' user can elevate his permissions and become the 'root' user by executing the 'su' command.

More information about SSH access can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/SSH_login.

8.3. Resetting to factory defaults

Sometimes when an RX-HDX or RX420(HDX) thin client device has been reconfigured multiple times, especially if it was reconfigured multiple times by different administrators, and behaves in unexpected way, instead of reviewing and possibly adjusting numerous NoTouch settings, it is easier and quicker to reset the device to its factory defaults and start the configuration from scratch.

Reset to factory defaults can be accomplished in several ways:

- On the device via Configuration UI – select 'Factory defaults' in System section.
- Remotely via web browser connected to Web-admin UI – select 'Factory defaults' in System section. This option is advisable when being unable to access the local Configuration UI (e.g. because the screen stays blank), but the device still has network connectivity.
- With the Keyboard – reset to factory defaults can be initiated by pressing and holding down the Shift and Control keys when the device will be powered on. A directly connected USB keyboard must be used for that. KVM switches or wireless keyboards are known to disallow this kind of factory reset. If the device will recognize the factory reset hotkey it will ask for confirmation. The answer 'yes' needs to be entered and the Enter key must be pressed within 10 seconds to proceed with the reset to factory defaults. More information about this method can be found in following NComputing Knowledge Base article: https://support.ncomputing.com/portal/kb/articles/rx-hdx-factory-reset
- Via NoTouch Center – Select the appropriate device and execute 'Factory Reset' on the 'Actions' page.

Note: If you are managing your device via NoTouch Center and performed a factory reset on the local device, you will have to do a MKey Auth Token reset in NoTouch Center to re-generate the secure communication token. Select the appropriate device, go to 'Actions' page, and execute the 'Reset

MKey Auth Token' action. More information can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/MKey_Authentication.

8.4. Creating support files

When a technical issue with RX-HDX or RX420(HDX) thin client device occurs which requires escalation to NComputing support a support file can be created on the affected device. This support file contains a snapshot of current device state, including hardware information, device configuration, uploaded certificates, numerous log files, outputs of multiple system commands, files created by local applications (like Citrix Workspace App), etc.

Support file can be created by opening the Configuration UI and clicking the 'Support file' hyperlink in the Diagnostics section on the left-hand side. If that action will be executed from Web-admin UI then the web browser will offer support file download after a while. If that action will be executed from local Configuration UI then the support file will be saved to a USB memory stick, which must be connected to the RX-HDX and RX420(HDX) thin client device before initiating the action.

More information about support files can be found in following NComputing Knowledge Base article:

http://rx-hdx.ncomputing.com/kb/Retrieve_a_Support_File.