



Transform Any x86-64 PC and Laptop Into a Secure, Centrally Managed Endpoint

Citrix Workspace app (WSA)
Quick Start Guide



NComputing[®]

400 CONCAR DRIVE 4TH FLOOR | SAN MATEO | CALIFORNIA 94402

ABOUT THE PRODUCT:

NComputing LEAF OS is a next-generation software endpoint solution that transforms any x86-64 PC or laptop into a secure and centrally managed endpoint.

Designed and optimized for **Citrix DaaS, Citrix Virtual Apps and Desktops, Microsoft Azure Virtual Desktop (AVD), Microsoft Windows 365 Cloud PC, Microsoft Remote Desktop Services (RDS), vSpace Pro Enterprise, VERDE VDI and Remote Access**, LEAF OS delivers a secure computing environment to access virtual desktops and virtual apps from any x86-64 system. It can be used as a self-contained operating system when booted from a USB drive. This method leaves the user's existing operating system, files, and hard drive untouched while providing an ideal environment for work-from-home use cases. When users finish their work, a simple reboot to their native OS restores their device to personal use.

Alternatively, LEAF OS can be used to repurpose PCs and laptops by converting any x86-64 hardware from a stand-alone computer to a dedicated thin client by installing directly onto an internal hard drive, removing the old system and files. This method extends the usefulness of aging computers using end-of-life operating systems like Windows 7 while giving users powerful up-to-date desktops.

With integrated local **Chromium browser**, LEAF OS provides additional flexibility such as web kiosk mode or productivity mode with direct access to web contents and web apps without desktop virtualization. Other popular applications, such as local **Microsoft Teams** and **Zoom**, are available too.

LEAF OS devices can be remotely managed by the IT admin. LEAF OS devices provide a simple to deploy, centrally managed, high performance virtual desktop, designed and optimized for Citrix WSA deployment for organization of any size.

Features highlights:

- Premium performance and native dual display
- [Citrix](#), [Microsoft AVD](#), [Windows 365 Cloud PC](#), [Microsoft RDS](#), [VERDE VDI](#) & [Remote Access](#), and [vSpace Pro Enterprise](#) desktop virtualization support
- Integrated local Chromium browser, Microsoft Teams and Zoom applications provide additional flexibility for direct access to unified communication, web content/web apps without desktop virtualization
- Native Citrix WSA integration for optimized performance
- Broad USB peripheral support
- Integrated [PMC Endpoint Manager](#) software
- Flexible deployment through Gigabit Ethernet or Wi-Fi support

ABOUT NCOMPUTING'S LEAF OS SOFTWARE ENDPOINT SUPPORT FOR CITRIX WSA

Citrix Workspace app for Linux, version 21.11, is integrated in LEAF OS 3.5.102 software endpoints.

Supported Citrix environments:

- Citrix DaaS
- Citrix Virtual Apps and Desktops 7 1808 or newer
- Citrix StoreFront 3.0 or newer, StoreFront 1811 or newer (including connections through Citrix Gateways)
- Citrix XenApp/XenDesktop 7.6 or newer
- Citrix Web Interface 5.4

Supported NComputing PMC Endpoint Manager versions:

- PMC 2.9.4 or newer versions

Supported peripheral device classes:

- Native (functional) redirection:
 - Mass storage
 - HDMI, DisplayPort, USB, and analog audio
 - USB and network printers
 - Webcams
 - Smart card readers and security keys
 - Serial ports
- Generic USB redirection for other USB devices

Additionally, the LEAF OS software endpoints have the following features:

- Native dual display support with independent screen rotation
- Local applications:
 - Chromium browser
 - Microsoft Teams
 - Zoom
 - Custom applications (deployed from a package or defined as a system application)
- Support for LEAF OS extension modules

LEAF OS SOFTWARE ENDPOINT - CITRIX WORKSPACE APP QUICK START GUIDE

Time zone mapping

Citrix Workspace app integrated in LEAF OS devices supports mapping of client's time zone. On the Citrix Virtual Desktop Agent side, the **Use local time of client** Citrix Policy setting can be used for controlling this feature. To enable the mapping of client's time zone, this policy setting must be set to **Use client time zone**. By default (when not configured), this Citrix Policy setting is set to **Use server time zone**.

STEP (1) INSTALL LEAF OS SOFTWARE ENDPOINT

Skip this step if you are using [NComputing EX500 thin client](#).

Download and prepare LEAF OS installation

1. From NComputing Software Download page, select "LEAF OS" and download the compressed image (i.e. ZIP).
2. Extract the .IMG file (~2GB) from the downloaded .ZIP file.
3. Create a bootable LEAF OS installer USB memory stick (use at least 4GB or higher capability):
 - a. Use a flashing application like the [Win32 Disk Imager](#) or [balenaEtcher](#) to write the image into your USB stick.
4. Pick an x86-64 PC/laptop (BIOS or UEFI).
 - a. Access the PC/laptop's [Boot Menu](#) or change the PC/laptop BIOS setting to set external USB storage device at the top of the booting priority list.

Use case #1 - live boot LEAF OS using USB memory stick

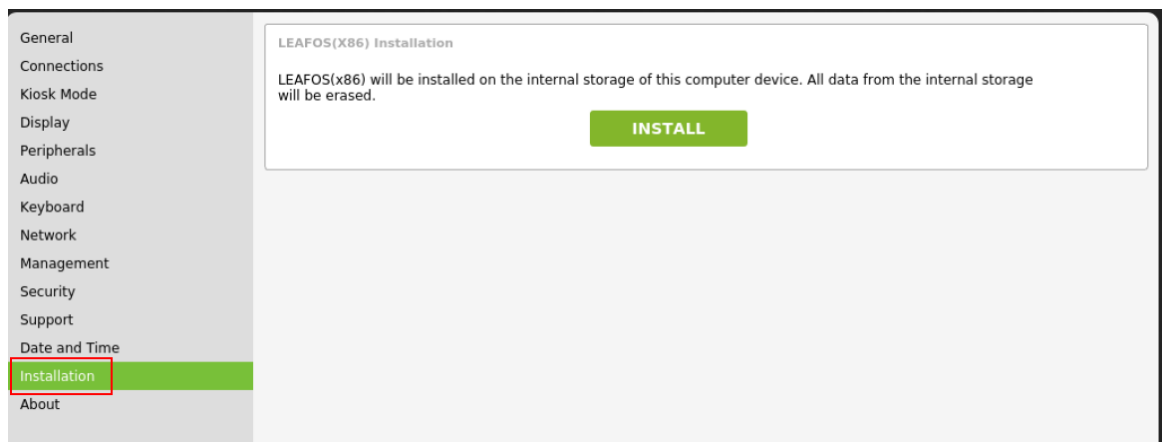
By default, your device will always live boot LEAF OS from the connected USB flash drive. There will be no changes to the PC/laptop's internal HDD.

1. Connect the x86-64 PC/laptop to Ethernet or Wi-Fi network.
2. Connect the bootable USB memory stick (prepared according to the instructions above) to the PC or laptop and power it up. The PC or laptop will perform live boot from the connected LEAF OS memory stick. Please refer to '[LEAF OS Live Boot from USB flash Drive Guide](#)' document on how to perform USB live boot of LEAF OS on PCs/laptops across different manufacturers.
3. It may take 10-20 seconds to bring up the LEAF OS UI (similar to RX420(RDP) thin client) during the power up. Please be patient.
4. Once the LEAF OS UI is up, you will see the LEAF OS device activation window. Please move to step (2) below to activate the device.

Use case #2 - flash LEAF OS into HDD/SSD/eMMC/NVMe internal storage to boot from

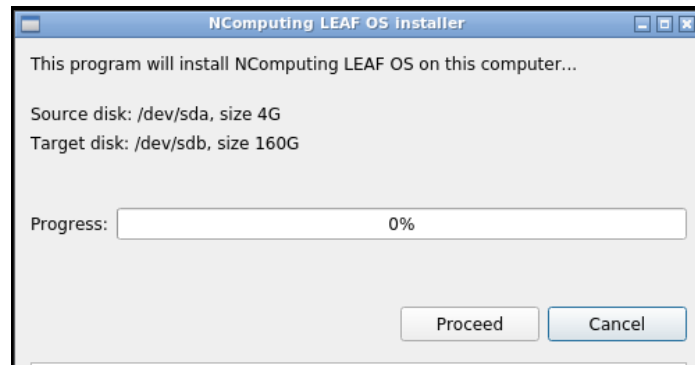
Your device's internal storage will be wiped and flashed with LEAF OS. When you boot the device, the LEAF OS will be directly booted from the internal HDD/SSD/eMMC/NVMe storage.

1. Follow the same procedures above to live boot LEAF OS on the device using the connected USB memory stick.
2. Once the LEAF OS UI is up, navigate to the '**Installation**' tab and click on 'Install' (see screenshot below). There are additional warning messages to inform the admin/user that the 'Install' process will erase the internal storage of the selected device.



3. Once you click on 'Install' and click 'OK' on the warning message, wait few seconds until the NComputing LEAF OS Installer window appears. It will prompt you to confirm to proceed flashing LEAF OS to the internal storage. Click the [Proceed] button to confirm and proceed. Once the

HDD/SSD/eMMC/NVMe storage is flashed, you will be prompted to shut the PC/laptop down and reboot.



The installation process may take several minutes. Please wait until it is finished. Once the internal storage is flashed, you will be prompted to shut the PC/laptop down and reboot.

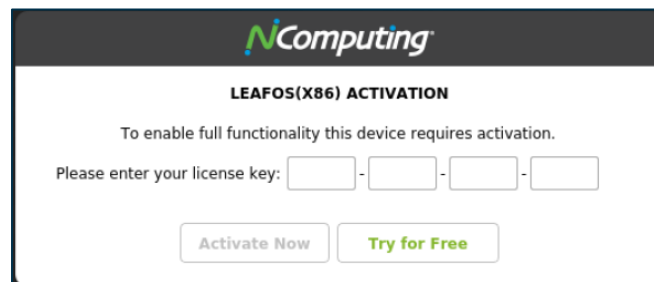
4. Remove the USB stick with LEAF OS installer and power up the computer again. LEAF OS will boot directly from the internal storage. Once the LEAF OS UI is up, you will see the LEAF OS device activation window. Please move to step (2) below to activate the device.

STEP (2) ACTIVATE LEAF OS SOFTWARE ENDPOINT

1. Once the LEAF OS device is boot up, you will see the following device activation window.

If you already have a valid LEAF OS license key, enter it (one time action) and click on '**Activate Now**'.

If you don't have a LEAF OS license, click on '**Try for Free**' to start the free trial. The free trial duration is subject to change. At the time of this writing, LEAF OS free trial is 7 days on 3rd party hardware and 60 days on NComputing EX500 thin client.



2. The device should be activated within seconds. Once the device is activated, you can connect to the selected desktop virtualization environment (e.g. Citrix, AVD, RDS, vSpace Pro, VERDE VDI) and start working.

STEP (3) SELECT THE 'CITRIX WORKSPACE APP' DEVICE OPERATION MODE

LEAF OS software endpoint can operate in several different modes. To select the 'Citrix Workspace app' operation mode, navigate to **Settings > General**, select **Citrix Workspace app** and click 'Apply' to save.

The screenshot shows the 'General' settings page. On the left is a navigation menu with 'General' selected. The main content area is divided into two sections: 'DEVICE OPERATION MODE' and 'DEVICE PROTECTION'. Under 'DEVICE OPERATION MODE', there are several buttons: 'AVD Client', 'Citrix Workspace app' (highlighted in green), 'RDP Client', 'vSpace Client', 'VERDE VDI Client', and 'Local Applications'. Below this is the 'DEVICE NAME' field with the value 'LEAFOS-X86-01'. There are also empty fields for 'SUBNET TAG' and 'ASSET TAG'. The 'DEVICE PROTECTION' section has a checkbox for 'Password protection of device settings' which is unchecked, followed by 'Enter password' and 'Confirm password' fields, both containing masked characters.

STEP (4) CONFIGURE CITRIX WORKSPACE APP SETTINGS

Following Citrix Workspace app settings can be configured:

The screenshot shows the 'Connections' settings page. The left navigation menu has 'Connections' selected. The main content area is titled 'CITRIX CONNECTION SETTINGS'. It includes a 'Store URL' field with the value 'https://sf.company.local/Citrix/Store/discovery'. Below are several checkboxes: 'Auto-launch' (unchecked), 'Guest mode' (unchecked with an info icon), 'Show Desktop Viewer Toolbar' (checked), 'Enable H.264 support' (checked), 'Allow HDX Adaptive Transport' (unchecked), 'Allow Session Reliability' (unchecked), 'Enable Microsoft Teams optimization' (checked), 'Enable Browser Content Redirection' (checked), and 'Enable Local Applications' (checked). There is a 'Workspace app window size' dropdown menu set to 'Default' and a 'Custom parameters' text input field.

- **Store URL** - the URL of the Citrix Store the Citrix Workspace app will connect to. Store URL must generally be an HTTPS URL. For successful communication, the Citrix Workspace app components must not encounter any issues related to the Store URL certificate. Especially, the SSL certificated of the web server hosting Citrix Store must be signed by a Certificate Authority the LEAF OS device trusts. If the certificate has not been issue by a well-known and commonly-trusted Certification Authority, then the certificate of the Root Certification Authority (and depending on how the certificate chain

presented by the web server looks like, possibly also the certificates of Intermediate Certification Authorities) will have to be added to LEAF OS device. This can be done under **Security** settings. Please refer to the dedicated section below.

- **Auto-launch** - when enabled, the Citrix Workspace app will be automatically launched.
- **Guest mode** - when enabled, the information cached by Citrix Workspace app (e.g., the list of published resources and their icons) will be wiped out from the device when the user exits the Citrix Workspace app session. By default, the guest mode is not enabled, and the list of Citrix resources remains on the device, even if it is rebooted.
- **Show Desktop Viewer Toolbar** - when enabled, the Citrix Desktop Viewer Toolbar will appear in published desktop sessions. As the Desktop Viewer Toolbar is solely a client functionality, this setting takes precedence over the Desktop Viewer Toolbar settings possibly configured on the StoreFront or Web Interface server.
- **Enable H.264 support** - when enabled, the device will be ready to use the H.264 codec (also known as video codec) for the entire desktop session screen or for the actively changing regions of the desktop session screen. The H.264 codec ensures the best user experience when using multimedia applications. On the Citrix Virtual Desktop Agent side, the **Use video codec for compression** Citrix Policy setting can be used for controlling this feature. To allow the use of the H.264 codec, this policy setting should not be set to **Do not use video codec**. By default (when not configured), this Citrix Policy setting is set to **Use when preferred**, which means that the VDA machine will try to choose the best variant of the codec based on the VDA type and session behavior. To enforce full-screen H.264 encoding, the **Use video codec** Citrix Policy setting should be set to **For the entire screen**.

Note: The H.264 codec can effectively be used only with screen resolutions up to 1920x1080.

- **Allow HDX Adaptive Transport** - when enabled, the device will try to use the HDX Adaptive Transport protocol (also known as Enlightened Data Transport protocol, EDT, or UDP transport) for Citrix connections. If establishing the session with Adaptive Transport is not possible, Citrix Workspace app will fall back to TCP transport.
On the Citrix Virtual Desktop Agent side, the **HDX Adaptive Transport** Citrix Policy setting can be used for controlling this feature. To allow Adaptive Transport, this policy setting should not be set to **Off**. By default (when not configured), this Citrix Policy setting is set to **Preferred**, which means that the data transport to the VDA machine takes place over the Citrix EDT protocol, that is build on top of UDP, with automatic fallback to TCP.
- **Allow Session Reliability** - when enabled, the device will try to use the Session Reliability feature (Common Gateway Protocol) in Citrix connections. In case of session disconnects caused by network problems, Citrix Workspace app will freeze the session screen and will try to re-establish the connection in the background.
On the Citrix Virtual Desktop Agent side, the **Session reliability connections** Citrix Policy setting can be used for controlling this feature. To allow Session Reliability, this policy setting should not be set to **Prohibited**. By default (when not configured), this Citrix Policy setting is set to **Allowed**.
- **Enable Microsoft Teams optimization** - when enabled, the optimization mechanisms for Microsoft Teams will be enabled. The processing and transmission of audio and video data will happen on the LEAF OS device, which will offload the network connection to the Citrix VDA machine as well as VDA's CPU.
On the Citrix Virtual Desktop Agent side, the **Microsoft Teams redirection** Citrix Policy setting can be used for controlling the Teams Optimization feature. To allow Teams Optimization, this policy setting should not be set to **Prohibited**. By default (when not configured), this Citrix Policy setting is set to **Allowed**. Refer to the 'Troubleshooting HDX Optimization for Microsoft Teams' article from Citrix Knowledge Base for more information: <https://support.citrix.com/article/CTX253754>.
- **Enable Browser Content Redirection** - when enabled, the rendering of the contents presented by supported web browsers (Google Chrome and Microsoft Edge) when accessing configured web pages will happen on the LEAF OS device. This will offload the Virtual Desktop Agent machine.
On the Citrix VDA side, the **Browser Content Redirection** Citrix Policy can be used for controlling this

feature. To allow Browser Content Redirection, this policy setting should not be set to **Prohibited**. By default (when not configured), this Citrix Policy setting is set to **Allowed**. Refer to the 'How to Troubleshooting Browser Content Redirection' article from Citrix Knowledge Base for more information: <https://support.citrix.com/article/CTX230052>.

- **Enable Local Applications** - when enabled, the local applications (Chromium browser, Teams client, Zoom client or custom applications) enabled on the LEAF OS device will be made available for the user besides Citrix Workspace app. Support for LEAF OS system extensions and custom local Linux applications is possible. Please refer to the following KB article for details: [Overview of LEAFOS 3rd party \(custom\) application support](#)
- **Workspace app window size** - selection of the Citrix Workspace app (Self-Service GUI) window size.
- **Custom parameters** - additional parameters, which can be injected into Citrix Workspace app configuration files.

Configuring custom parameters for Citrix Workspace app

LEAF OS allows injecting new or modifying existing parameters in given sections of the following Citrix Workspace app configuration files:

- wfclient.ini
- All_Regions.ini
- module.ini

Please refer to the 'Citrix Workspace app for Linux OEM Reference Guide' (<https://developer-docs.citrix.com/projects/workspace-app-for-linux-oem-guide/en/latest/reference-information/#configuration-files>) for the information about the Citrix Workspace app configuration files, their entries and values.

The syntax of the custom parameters is:

```
<filename.ini>:[<section>]<key>=<value>;<filename.ini>:[<section>]<key>=<value>;...
```

- **<filename.ini>** must be one of the above mentioned configuration files.
- **<section>** is the name of the section in the configuration file, where the parameter (key) will be injected or modified.
- **<key>** is the name of the parameter to be injected or modified.
- **<value>** is the value the parameter will be set to.

Multiple custom parameters can be specified in one custom parameters line. In such case they need to be separated with semicolons (without preceding or following whitespaces).

Example:

```
wfclient.ini:[WFClient]HDXWebCamWidth=1280;wfclient.ini:[WFClient]HDXWebCamHeight=720
```

The above line defines two custom parameters for the wfclient.ini file and adds the following entries to the [WFClient] section of that file:

```
HDXWebCamWidth=1280  
HDXWebCamHeight=720
```

The above will set the picture resolution of 1280x720 for the Citrix HDX Webcam redirected with the Citrix HDX RealTime Video Compression feature.

Time zone mapping

Citrix Workspace app integrated in LEAF OS supports mapping of the client's time zone. Time zone can be selected under **Date and Time** settings.

On the Citrix Virtual Desktop Agent side, the **Use local time of client** Citrix Policy setting can be used for controlling this feature. To enable the mapping of client's time zone, this policy setting must be set to **Use client time zone**. By default (when not configured), this Citrix Policy setting is set to **Use server time zone**.

Keyboard layout mapping

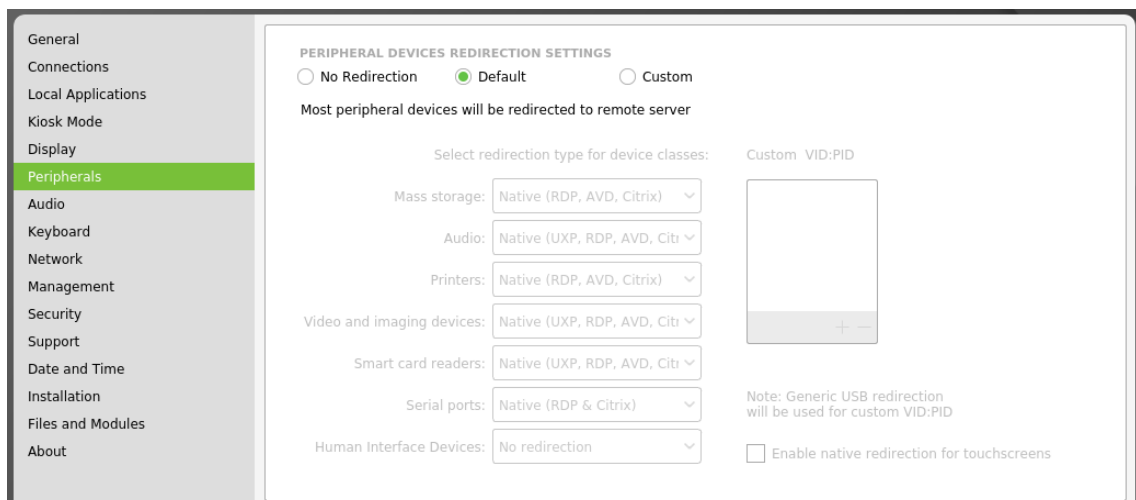
Citrix Workspace app reports to the Virtual Desktop Agent machine the information about the keyboard layout configured locally on the client device. The selected keyboard layout will be used in the Citrix sessions connected from the device. There is no Citrix Policy setting for controlling the keyboard layout mapping feature. This feature is enabled by default.

Deploying Certification Authority certificates

Citrix Workspace app needs to trust the issuer of the SSL server certificate presented by the web server hosting the Citrix Store. If necessary (e.g. when using organization's own Certification Authority), to establish this necessary trust relationship, the certificates of Root and Intermediate Certification Authorities (X.509 certificates) can be added to LEAF OS devices under the **Security** settings. LEAF OS accepts Base64-encoded Certification Authority certificates. The Base64-encoded X.509 certificate format is commonly known as PEM format. Please refer to the 'Security Settings' section of 'LEAF OS and RX-series User and Configuration Guide' for more information (you will find the download link in the '[Additional Resources](#)' section below).

STEP (5) OPTIONAL - CONFIGURE PERIPHERAL DEVICE REDIRECTIONS

Navigate to **Peripherals** tab to configure the redirection of peripheral devices. The optimum redirection settings are already pre-selected for all supported classes of peripheral in the **Default** settings. The best behavior will be achieved when using the native (functional) redirection. For Citrix sessions, the native redirection is available for mass storage devices, audio devices, printers, webcams, smart card readers, and serial ports. Administrators can customize the settings and enable or disable redirection for selected classes of peripheral devices by selecting the **Custom** option.



Server-side control over native/functional redirection of peripheral devices

The **Peripherals** settings of LEAF OS allow enabling or disabling the selected redirection type for different device classes. However, these client-side settings cannot overwrite the settings, which are configured on the server side. The redirections will only work when the server will not prevent them. The following paragraphs describe the Citrix Policy settings, which can be used for controlling the native/functional redirection of peripherals on the Virtual Desktop Agent side.

Mass storage

On the Citrix Virtual Desktop Agent side, the **Client drive redirection** Citrix Policy setting can be used for controlling this feature. To allow the native redirection of mass storage devices, this policy setting should not be set to **Prohibited**. By default (when not configured), this Citrix Policy setting is set to **Allowed**.

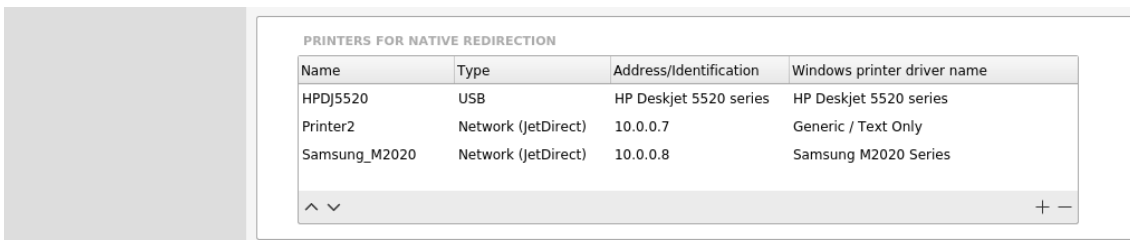
Audio

On the Citrix Virtual Desktop Agent side, the **Client audio redirection** and **Client microphone redirection** Citrix Policy settings can be used for controlling this feature. To allow audio output (speakers) redirection, the **Client audio redirection** policy setting should not be set to **Prohibited**. To allow audio input (microphone) redirection, both the **Client audio redirection** and the **Client microphone redirection** policy settings should not be set to **Prohibited**. By default (when not configured), these Citrix Policy settings are set to **Allowed**.

Printers

Citrix Workspace app integrated in LEAF OS supports the native (functional) redirection of USB and network (JetDirect) printers. On the Citrix Virtual Desktop Agent side, the **Client printer redirection** Citrix Policy setting can be used for controlling this feature. To allow the native redirection of printers, the **Client printer redirection** policy setting should not be set to **Prohibited**. By default (when not configured), this Citrix Policy setting is set to **Allowed**.

The native redirection of printers requires the printers to be defined locally on the LEAF OS device. When adding USB printers, a USB printer identification string needs to be specified. It can be also pulled from the USB printer, if it is connected. This serves the purpose of identifying the different USB printers, when multiple USB printer will be connected. In case of single USB printer, this field can be left empty. For each configured printer, the exact name of corresponding Windows printer driver must be specified. This driver must be installed on the Citrix VDA machine for successful printer redirection.



Name	Type	Address/Identification	Windows printer driver name
HPDJ5520	USB	HP Deskjet 5520 series	HP Deskjet 5520 series
Printer2	Network (JetDirect)	10.0.0.7	Generic / Text Only
Samsung_M2020	Network (JetDirect)	10.0.0.8	Samsung M2020 Series

The first printer from the list will be configured as the default printer and will also become the default printer in the Citrix session.

Printer drivers appropriate for the redirected printers must be installed on the Citrix VDA machines for successful printers redirection. 'x64, Type 3 - User Mode' printer drivers need to be installed. The Citrix universal print driver cannot be used with printers redirected from LEAF OS devices. To prevent attempts to use this unsupported driver, the **Universal print driver usage** Citrix Policy setting can be set to **Use only printer model specific drivers**.

Webcams (video devices)

There is no Citrix Policy setting for controlling the webcam redirection (actually known as HDX RealTime Video Compression) feature on the Virtual Desktop Agent side. This feature is enabled by default.

Smart cards readers

Citrix Workspace app integrated in LEAF OS supports the native (functional) redirection of smart cards (smart card readers). CCID-compliant and ACS smart card readers are supported. Refer to LEAF OS Release Notes for full list of supported smart card readers.

There is no Citrix Policy setting for controlling the smart cards redirection feature on the Virtual Desktop Agent side. This feature is enabled by default.

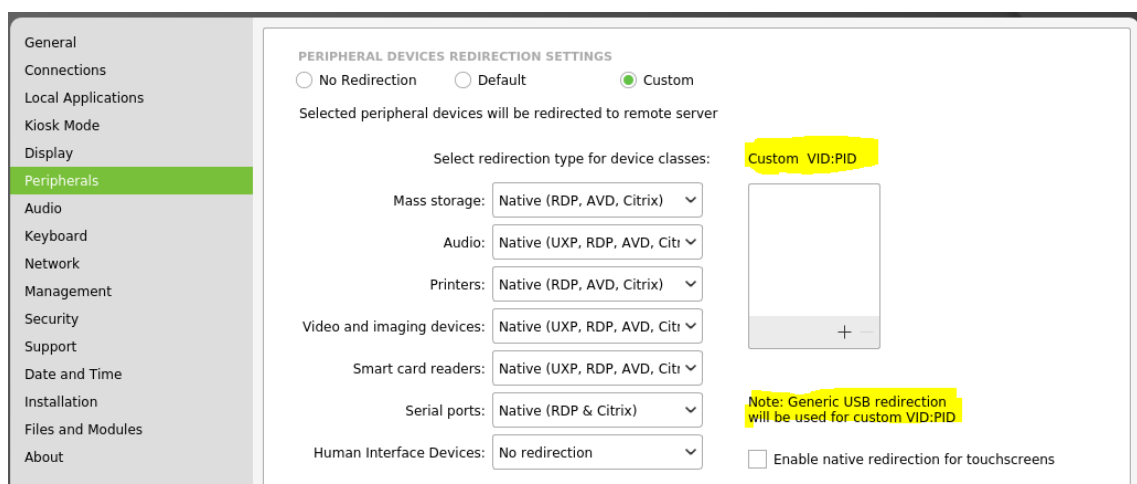
Serial ports

The /dev/ttyUSB0, /dev/ttyUSB1, /dev/ttyACM0 and /dev/ttyACM1 serial devices will be redirected as client's COM1, COM2, COM3 and COM4 ports, accordingly.

On the Citrix Virtual Desktop Agent side, the **Client COM port redirection** Citrix Policy setting can be used for controlling this feature. To allow the native redirection of serial ports, this policy setting must be set to **Enabled**. By default (when not configured), this Citrix Policy settings is set to **Disabled**.

Generic USB redirection of peripheral devices

Citrix Workspace app integrated in LEAF OS devices supports the **Generic USB redirection** of most peripheral device classes (excluding the smart card readers). However, wherever possible the native redirection should be used, as in the majority of cases it is the most reliable and best optimized redirection method. The **Generic USB redirection** should generally be used only as the last resort method for device classes (like HID devices), for which no native redirection method exists. LEAF OS tries determining the USB classes of connected USB devices and only attempts to use the Generic USB redirection for that device, where the **Generic** method has been really selected. USB devices which in their USB descriptors contain the Vendor Specific Class (0xFF) cannot be automatically categorized by LEAF OS and must be added to the Custom VID:PID list to be redirected in the **Generic** way.



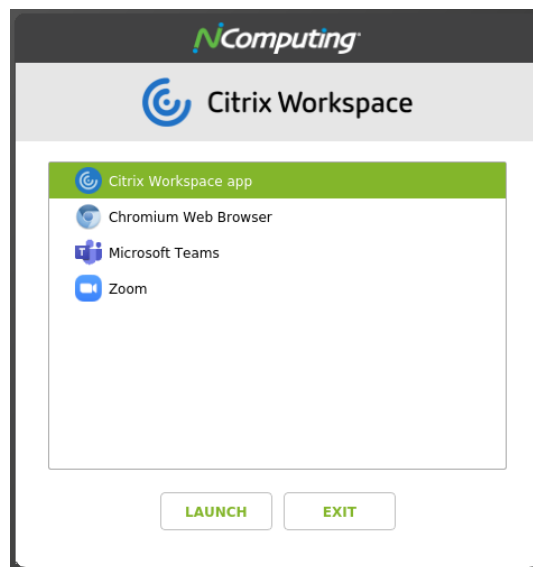
On the Citrix Virtual Desktop Agent side, the **Client USB device redirection** Citrix Policy setting can be used for controlling this feature. To enable the generic redirection of USB devices, this policy setting must be set to **Allowed**. By default (when not configured), this Citrix Policy setting is set to **Prohibited**.

STEP (6) LOGIN TO CITRIX ACCOUNT

Depending on the state of the **Auto-launch** option, LEAF OS in Citrix Workspace app mode will present to the user the below pop-up window (when the **Auto-launch** option will not be enabled) or will automatically proceed to Citrix Workspace app and launch it.



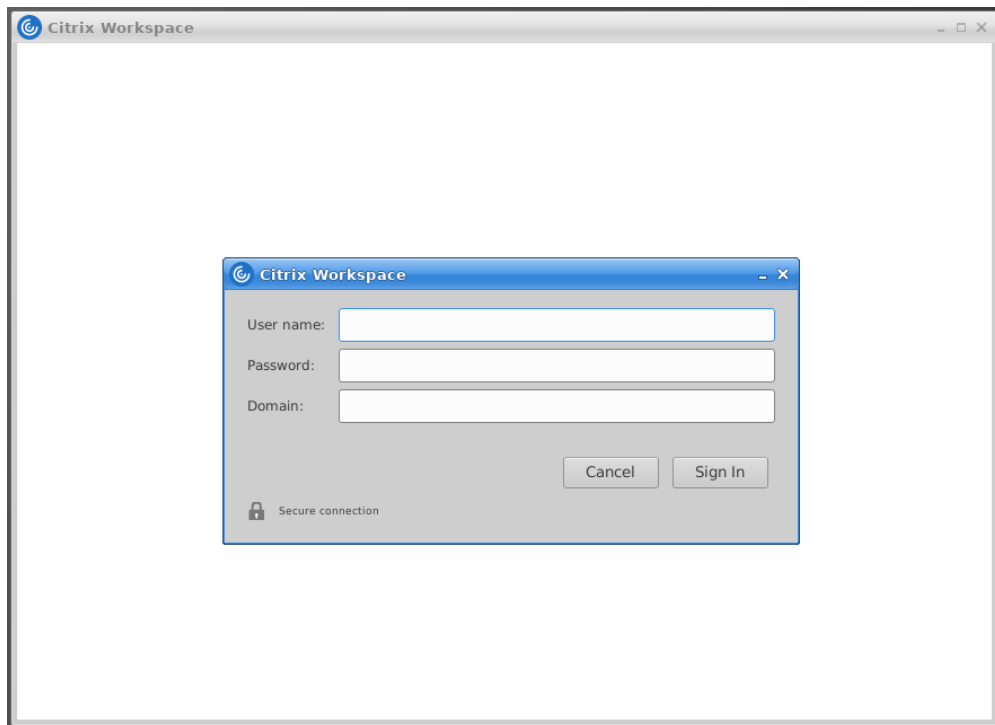
Local Applications, when enabled, will be presented besides the Citrix Workspace app. If the **Local Applications** will not be enabled under **Connections** settings, then the Citrix Workspace app will also be started automatically, as it will be the only item presented to the user on the below list.



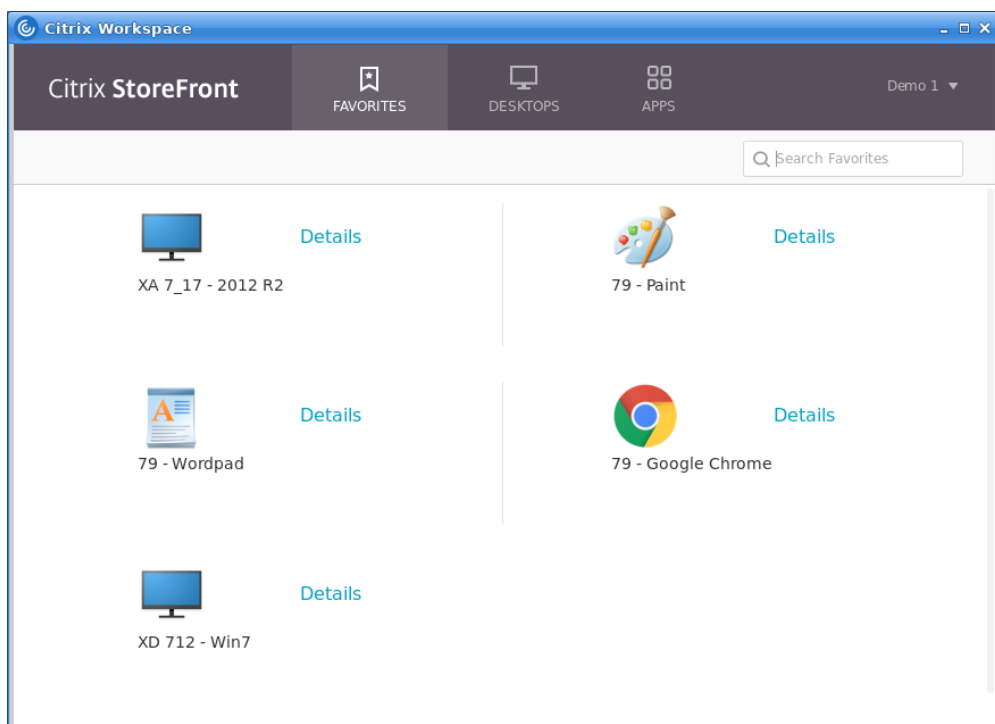
When the Citrix Workspace app is launched, it will automatically connect to the Citrix Store with the URL specified in Connections configuration.

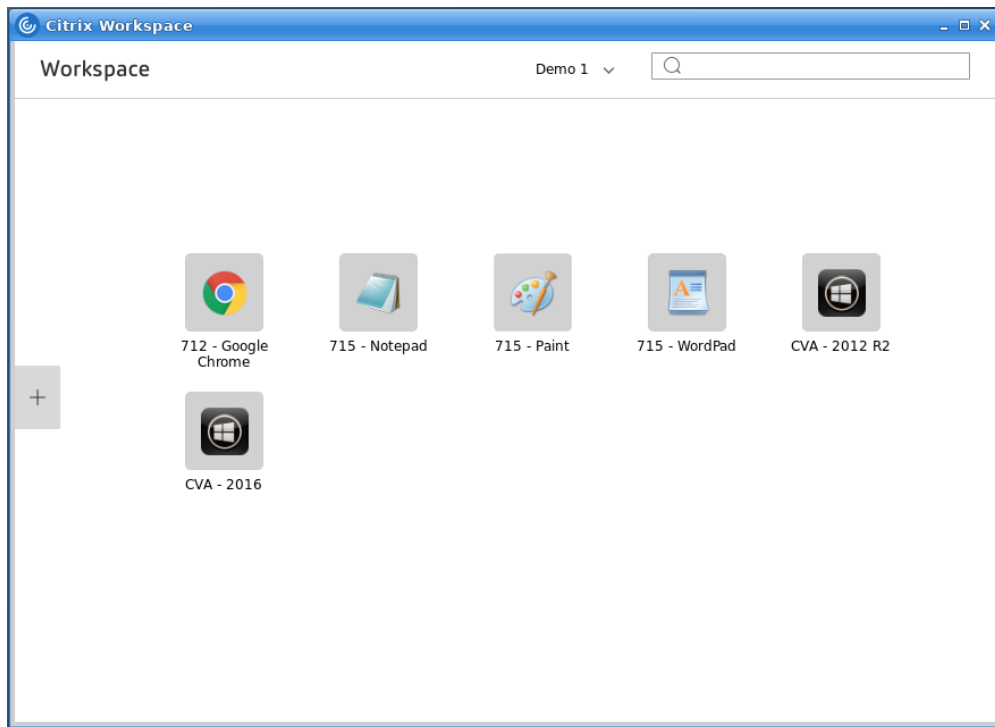
STEP (7) ACCESSING CITRIX PUBLISHED RESOURCES

When the Citrix Workspace app GUI starts, depending on what is behind the Store URL, it will present to the user the logon window or a logon page.



After successful authentication, the published Citrix resources will be presented to the user. Users will have the ability to launch the resources, as well as to subscribe (add to favorites) to new resources or cancel the existing subscriptions.





Published desktops will be launched in full-screen mode. Published applications will be launched in “seamless” mode (will appear in separate windows and behave in the same way as local applications).

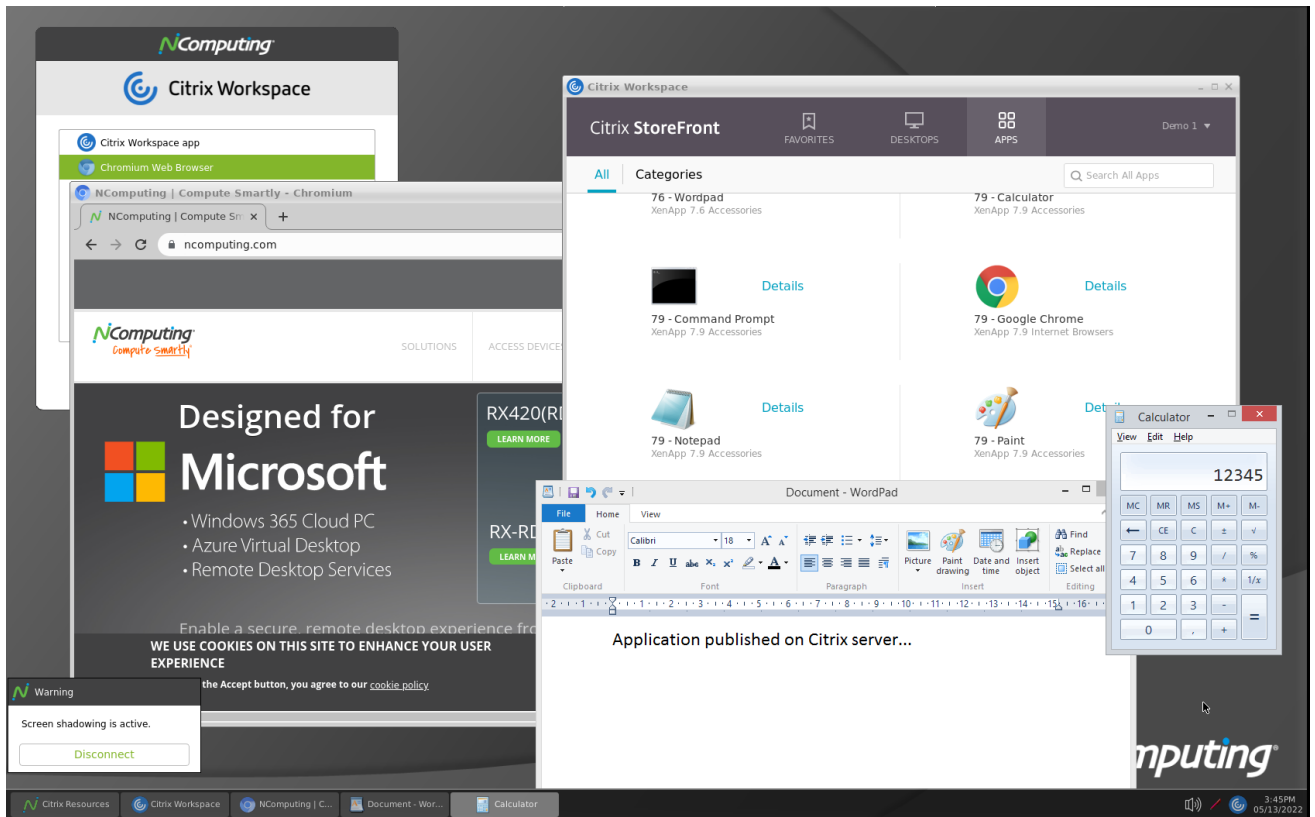
Using the Desktop Viewer Toolbar is the simplest way of switching between full-screen published desktops, or between the desktops and the local GUI (the **Home** icon).



STEP (8) ACCESS LOCAL APPLICATIONS IN CITRIX SESSION

LEAF OS software endpoint allow users to multi-task between Citrix sessions and the built-in local Chromium browser, Microsoft Teams and Zoom applications, providing added flexibility for direct access to unified communications (including video conferencing), web content and web apps without going through desktop virtualization. The local applications, when enabled in Citrix connection settings, will be presented besides Citrix Workspace app in the **Citrix Workspace** window.

Switching between all kinds of applications (published on Citrix servers and available locally in LEAF OS) can be done by clicking the application shortcuts on the local taskbar or with the Ctrl-Alt-Arrow Up/Down key-combination.



ADDITIONAL RESOURCES

LEAF OS software endpoint and RX420(RDP) User and Configuration Guide

LEAF OS and RX420(RDP) are easy-to-use and provision. For users who want to learn how to use advanced features and/or customizations, please refer to the LEAF OS and RX420(RDP) User and Configuration Guide:

<https://ncomputing.box.com/shared/static/310pp20tfhh4aqc6x4nj14sxch52q360.pdf>

PMC Endpoint Manager Quick Start Guide

NComputing PMC is an endpoint management system designed and developed to remotely manage NComputing access devices.

Please refer to the PMC Quick Start Guide:

<https://support.ncomputing.com/portal/en/kb/articles/pmc-2-5-0-quick-start-guide>

Key features of PMC include:

- Ability to manage devices located in local- and wide-area networks, devices located behind firewalls and NAT-routers, including devices of work-from-home users.
- Ability to edit configuration of selected devices and to push configurations to multiple devices (through device profiles).
- Ability to securely shadow all manage devices' screens.

- Ability to request and collect troubleshooting information from managed devices.
- Ability to schedule device firmware updates.
- Readiness to support future device families, models, and configuration versions by uploading configuration definition files.
- Hosting files (firmware, certificates, wallpapers) for managed devices.
- Deployment as virtual appliance compatible with industry-standard hypervisors and Azure Cloud.
- Easy to use web-based user interface, accessible from any network location.
- Dashboard view with auto-refreshing summary information.
- Detailed event logging with filtering capability.
- Ability to export the contents of all PMC lists.
- Ability to mark selected devices as lost or found.
- Ability to revoke LEAF OS licenses.

CONTACTING TECHNICAL SUPPORT AND ADDITIONAL RESOURCES

For Citrix related questions or feedback, please visit [NComputing knowledge base](#) or [NComputing support page](#).

Disclaimer

Information contained in this document may have been obtained from internal testing or from a third party. This information is for informational purposes only. Information may be changed or updated without notice. NComputing reserves the right to make improvements and/or changes in the products, programs and/or specifications described herein anytime without notice.

All NComputing software is subject to NComputing intellectual property rights and may be used only in conjunction with Genuine NComputing hardware and in accordance to the NComputing End User Licensing Agreement and Terms of Use.

www.ncomputing.com

© Copyright 2022 NComputing Global, Inc. All rights reserved. NComputing is the property of NComputing Global, Inc. Other trademarks and trade names are the property of their respective owners. Specifications are subject to change without notice. Performance may vary, depending on the configuration of the shared computer.