

NComputing RX420(RDP) and RX-RDP+ Thin clients

Microsoft Azure Virtual Desktop (AVD) and Windows 365 Cloud PC

Quick Start Guide



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

ABOUT THE PRODUCT:

The RX420(RDP) cloud-ready thin client is built on the Raspberry Pi 4B platform. The RX420(RDP) brings premium performance and native dual display support, providing a rich PC-like experience in an affordable, energy saving device with a small footprint.

The new RX-RDP+ cloud-ready thin client is built on the Raspberry Pi 3B+ platform. The RX-RDP+ brings great performance with an affordable budget for single display computing.

Designed and optimized for **Microsoft Azure Virtual Desktop (AVD)**, **Microsoft Windows 365 Cloud PC**, **Microsoft Remote Desktop Services (RDS)**, **vSpace Pro Enterprise**, **VERDE VDI** and **Remote Access**, both devices deliver a secure computing environment to access virtual desktops and virtual apps.

The RX420(RDP) also comes with integrated local Chromium browser support, provides additional flexibility such as web kiosk mode or productivity mode with direct access of web content and web apps without desktop virtualization. If the use case requires extensive use of local Chromium browser, we recommend users to consider RX440(RDP) which comes with 4GB system RAM to provide additional performance headroom for local browsing activities.

RX420(RDP) and RX-RDP+ configurations and firmware updates can be remotely managed by the IT admin. The RX420(RDP) and RX-RDP+ provide a simple to deploy, centrally managed, high performance virtual desktop, designed and optimized for Microsoft AVD and Windows 365 Cloud PC deployment for organizations of any size.

Features highlights:

- Premium performance and native dual display
- Multimedia enhancement through Microsoft RemoteFX
- [Microsoft AVD](#), [Windows 365 Cloud PC](#), [Microsoft RDS](#), [VERDE VDI](#) & [Remote Access](#), and [vSpace Pro Enterprise](#) desktop virtualization support
- Integrated local Chromium browser support providing additional flexibility for direct access to web content/web apps without desktop virtualization.
- Native Microsoft AVD SDK integration for optimized performance
- NComputing vCAST Streaming technology with SuperRDP software (separate license required)
- Broad USB peripheral support
- Integrated [PMC Endpoint Manager](#) software
- Flexible deployment through Gigabit Ethernet or built-in 2.4/5GHz Wi-Fi
- Low cost of ownership and low power consumption

ABOUT NCOMPUTING'S THIN CLIENT SUPPORT FOR MICROSOFT AVD AND WINDOWS 365

Microsoft AVD is officially supported on NComputing RX420(RDP) and RX-RDP+ thin clients, based on native AVD client integration. The AVD client included supports both AVD Spring 2020, Fall 2019 releases and Windows 365 Cloud PC.

Following are the Azure Virtual Desktop client features that are supported on RX420(RDP) and RX-RDP+ thin clients with firmware version 2.8.9 or higher:

- Microsoft Azure Virtual Desktop (AVD)
 - Spring 2020 release (ARM)
 - Fall 2019 release (Classic)
 - Azure Government Cloud
- Microsoft Windows 365 Cloud PC
- Multi-Factor Authentication (MFA)

- RemoteApp programs and desktops
- Regular vs. Kiosk mode auto-login
- Peripheral devices:
 - USB mass storage
 - HDMI, analog and USB audio
 - USB smart card readers and security keys
 - USB printers and network printers
 - USB webcams for video conferencing
 - Other USB devices through Generic USB redirection

Additionally, the RX420(RDP) thin clients have the following features:

- Native dual display with independent screen rotation
- Local Chromium browser available in stand-alone mode & productivity mode

UNBOXING

When you purchase the RX420(RDP), you will receive it in a box, as shown below.



The following items come with the NComputing RX420(RDP):

1. The NComputing RX420(RDP) thin client
2. Safety information, a notice of certification, and two pages of important notes you will want to read
3. VESA mounting brackets
4. USB power cord, with the corresponding outlet plugs for your region



If you are connecting your RX420(RDP) device to a monitor, you may need to purchase the 'Micro HDMI to HDMI Adapter' kit or 'Micro HDMI to HDMI Cable' kit, as shown below.

Inside the box, you will receive two Micro HDMI to HDMI cables that will allow you to connect two HDMI compatible displays to your NComputing RX420(RDP) device.

Make sure the Micro HDMI to HDMI cable is fully inserted into the port on the RX420(RDP). If not, you may experience issues with flashing or dysfunctional displays.





Important! Please do not disconnect the RX420(RDP) from its power source before proper shutdown, as it may damage the device.

To properly shut down the device, use the shutdown menu item within the firmware. Alternatively, if you must, hold the power button down for more than 7 seconds until the device powers down.

RX420(RDP) AND RX-RDP+ AVD QUICK START GUIDE

AVD and Windows 365 virtual machine configuration for best user experience:

The AVD clients integrated in RX420(RDP) and RX-RDP+ devices support the use of H.264/AVC encoding (Advanced Video Codec) in AVD sessions. Using AVC ensures the best AVD user experience. To take advantage of this H.264/AVC graphics mode, the following Group Policy setting **must be enabled**:

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment: Prioritize H.264/AVC 444 graphics mode for Remote Desktop Connections

In simplest case, this Group Policy setting can be configured on the local machine with Local Group Policy Editor (gpedit.msc).

AVD and Windows 365 virtual machine configuration for webcam redirection:

The AVD clients integrated in RX420(RDP) and RX-RDP+ devices support the native (functional) redirection of USB webcams. To ensure proper webcam redirection, please make sure that the following Group Policy setting is not enabled:

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection: Do not allow video capture redirection

In simplest case, this Group Policy setting can be configured on the local machine with Local Group Policy Editor (gpedit.msc).

Additionally, each user under Settings > Privacy > Camera, needs to allow the applications to access the camera.

Note: Webcams described as driverless Windows webcams (webcam not requiring any special vendor drivers to work on Windows) or Video for Linux version 2 compliant webcams should work. To preserve the network bandwidth when using redirected webcams, the device firmware uses the hardware-based H.264 encoder to compress the webcam's video stream before sending it to AVD session.

AVD and Windows 365 virtual machine configuration for printers redirection:

The AVD clients integrated in RX420(RDP) and RX-RDP+ devices support the native (functional) redirection of local printers. USB and network printers are supported. To ensure proper printers redirection, please make sure that the following Group Policy setting is not enabled:

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Printer Redirection: Do not allow client printer redirection

Printer drivers appropriate for the redirected printers must be installed on the AVD VM for successful printers redirection. 'x64, Type 3 - User Mode' printer drivers need to be installed. The 'Remote Desktop Easy Print' driver cannot be used with printers redirected from RX420(RDP) or RX-RDP+ thin clients. To prevent the attempts to use this unsupported driver, the following Group Policy setting can be disabled in Computer Configuration or User Configuration

Computer/User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Printer Redirection: Use Remote Desktop Easy Print printer driver first

In simplest case, the above mentioned Group Policy settings can be configured on the local machine with Local Group Policy Editor (gpedit.msc).

AVD and Windows 365 virtual machine configuration for smart cards redirection:

The AVD clients integrated in RX420(RDP) and RX-RDP+ devices support the native (functional) redirection of smart cards (smart card readers). CCID-compliant and ACS smart card readers are supported. Refer to firmware Release Notes for full list of supported smart card readers. To ensure proper smart cards redirection, please make sure that the following Group Policy setting is not enabled:

Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection: Do not allow smart card device redirection

In simplest case, this Group Policy setting can be configured on the local machine with Local Group Policy Editor (gpedit.msc).

AVD and Windows 365 virtual machine configuration for Generic USB redirection of peripheral devices:

The RDP and AVD clients integrated in RX420(RDP) and RX-RDP+ devices support the Generic USB redirection of peripheral devices. In Windows Server 2016/2019 and Windows 10 the 'Do not allow supported Plug and Play device redirection' Group Policy setting is enabled by default (when not configured), which prevents the Generic USB redirection of the peripheral devices to those operating systems. This Group Policy setting can be found under 'Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection'.

To be able to use the Generic USB redirection of RX420(RDP) and RX-RDP+ peripheral devices, this policy must be explicitly disabled. This Group Policy setting can be deployed through Active Directory Group

Policy Objects or, in simplest case, it can be configured on the local machine with Local Group Policy Editor (gpedit.msc).

In Windows Server 2012 R2, Windows 8.1 and older Windows server and desktop operating systems the Remote Desktop Services by default allows the redirection of supported plug and play devices, thus the 'Do not allow supported Plug and Play device redirection' Group Policy setting does not need to be altered.

STEP (1) UPDATE FIRMWARE

There are multiple ways to update the firmware:

- **Method 1: Update firmware using URL**

At the time of this writing, version 3.3.12 is the latest firmware. Be sure to check <https://www.ncomputing.com/support/downloads> to ensure you're using the latest firmware version.

Enter the following NComputing's web URL (**please note it is case sensitive**) to download and install this version of firmware directly to the RX420(RDP) and RX-RDP+ device:

<http://firmware.ncomputing.com/RX420/rx4x0-rdp-3.3.12.upd>

General
Connections
Kiosk Mode
Display
Peripherals
Audio
Keyboard
Network
Management
Security
Support
Date and Time
About

UPDATE FIRMWARE FROM...

☒ FTP/HTTP URL ☐ USB stick

This selection allows you to update firmware by entering a specific FTP or web server URL and a specified firmware file.

FTP/HTTP URL:

Username:

Password:

UPDATE

TROUBLESHOOTING

COLLECT LOGS FACTORY RESET

APPLY Cancel

- **Method 2: Update firmware using a USB memory stick**

- Download the 'rx4x0-rdp-3.3.12.upd' and save it to a USB memory stick.

- Insert the USB stick into RX420(RDP) and RX-RDP+.
- On the RX420(RDP) and RX-RDP+ device open the Setup GUI and go to the 'Support' section.
- Select 'Update from the USB memory stick' and select the firmware update file displayed in the pop-up. Click the 'Update button'.

General
Connections
Kiosk Mode
Display
Peripherals
Audio
Keyboard
Network
Management
Security
Support
Date and Time
About

UPDATE FIRMWARE FROM...

☐ FTP/HTTP URL ☒ USB stick

This selection allows you to update your device using update package stored on a USB stick.

Please select USB device:

Device	Partition label or ID
/dev/sda1	6680-40BF

REFRESH

Please select update package:

Update package file name

- rx-rdp-2.11.0.upd
- rx4x0-rdp-1.5.13.upd
- rx4x0-rdp-1.5.14.upd
- rx4x0-rdp-1.5.15.upd

UPDATE

TROUBLESHOOTING

COLLECT LOGS FACTORY RESET

APPLY Cancel

- **Method 3:** Update firmware via NComputing's PMC Endpoint Manager software

The device firmware can be updated from supported version of PMC (version 2.7.0 and higher version). Follow the below steps to perform the firmware update on remote RX420(RDP) and RX-RDP+ devices:

- Logon to PMC as a user with administrative privileges, open the Menu, go to 'Administration > Files'.
- Select 'Firmware Image' as file type.
- Click the 'Choose file' button and select the 'rx4x0-rdp-3.3.12.upd' file.
- Click the 'Upload file' button to upload the firmware package.
- Schedule the update date and time, or opt to update now.
- Click the 'Apply' button.

If 'Update now' was chosen, then within 30 seconds the device will receive a request to initiate the firmware update. On remote devices the process can be followed by observing the Audit Events log on the Dashboard. The firmware update process will take a while and should not be interrupted. Firmware update will end with a device reboot.

STEP (2) SELECT THE 'AVD CLIENT' DEVICE OPERATION MODE

RX420(RDP) can operate in several different modes. To select 'AVD Client' operation mode, navigate to Settings -> General, select **AVD Client** and click 'Apply' to save.

The screenshot shows the 'General' settings tab for the RX420(RDP) device. On the left is a sidebar menu with options: General, Connections, Kiosk Mode, Display, Peripherals, Audio, Keyboard, Network, Management, Security, Support, Date and Time, and About. The 'General' tab is active. The main content area is titled 'DEVICE OPERATION MODE' and contains several buttons: 'RDP Client', 'WVD Client' (which is highlighted in green), 'VERDE VDI Client', 'vSpace Client', and 'Chromium Browser'. Below these buttons are three input fields: 'DEVICE NAME' (containing 'RX420RDP10000000D9EE83F1'), 'SUBNET TAG' (empty), and 'ASSET TAG' (empty). To the right of these fields is a 'DEVICE PROTECTION' section with a checkbox labeled 'Password protection of device settings' which is currently unchecked. Below this checkbox are two password input fields: 'Enter password' and 'Confirm password', both containing masked characters. At the bottom right of the settings panel are 'APPLY' and 'Cancel' buttons.

STEP (3) CONFIGURE AVD CLIENT SETTINGS

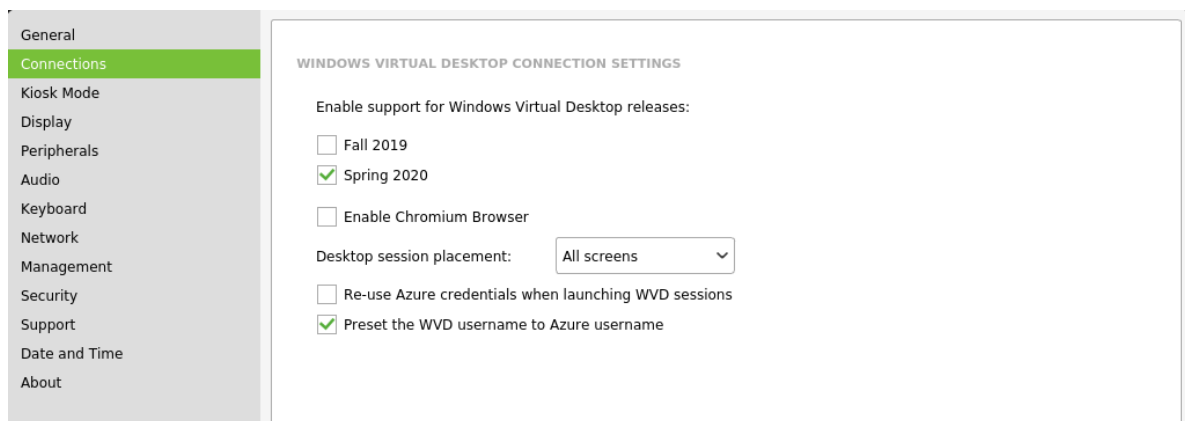
Navigate to **Connections** tab and select your AVD deployment release version(s). RX420(RDP) device supports and can deliver published resources from **Spring 2020**, **Fall 2019**, or both Azure Virtual Desktop releases.

By default, **Spring 2020** deployment is pre-selected. Make your selection and click 'Apply' to save and the corresponding AVD login UI will appear.

Note: For Windows 365 Cloud PC access, use the default 'Spring 2020' checkbox selection.

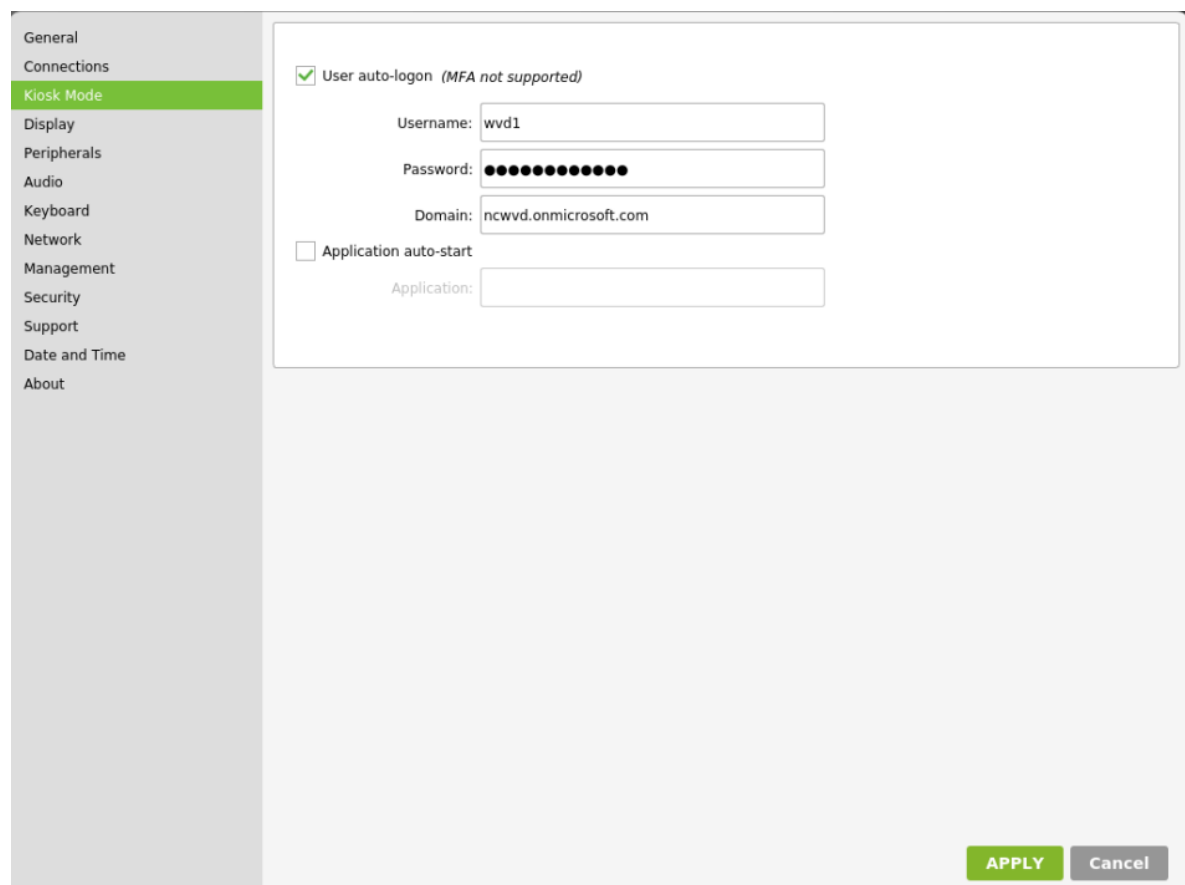
Also by default, the device will re-use the Azure login credentials when launching AVD session. If the user credentials necessary for launching certain AVD RemoteApp program or desktop session are different than the Azure credentials, then the **Re-use Azure credentials when launching AVD sessions** option can be disabled. Please uncheck the default selection and click 'Apply' to save. If only the AVD session password is different than the Azure password, then the **Preset the AVD username to Azure username** option can be

used for user's convenience. The username will be preset in the AVD logon window then and the user will only need to enter the password.



STEP (4) OPTIONAL - SETUP KIOSK MODE

This is an optional step. The **Kiosk Mode** settings allow the user to automatically login to his/her AVD account, and if required, automatically launch a specified Windows application or desktop. The username and domain name need to be specified separately here (instead of user@company.domain) for the automatic user logon. The name of AVD resource to be automatically launched after (manual or automatic) user logon can be specified as **Application** to auto-start. Click 'Apply' to save. Please note that MFA is not supported when 'Kiosk Mode' is enabled.



STEP (5) OPTIONAL - CONFIGURE PERIPHERAL DEVICE SETTINGS

Navigate to **Peripherals** tab to configure the redirection of peripheral devices. By default, the optimum redirection settings are selected for all supported classes of peripheral devices. The best behavior will be achieved when using the native (functional) redirection. For AVD sessions the native redirection is available for mass storage devices, audio devices, printers, webcams, and smart card readers. Administrator can customize the settings and enable or disable redirection for selected classes of peripheral devices.

PERIPHERAL DEVICES REDIRECTION SETTINGS

☐ No Redirection ☒ Default ☐ Custom

Most peripheral devices will be redirected to remote server

Select redirection type for device classes:

Mass storage: Native (RDP & WVD)

Audio: Native (UXP, RDP, WVD)

Printers: Native (RDP & WVD)

Video and imaging devices: Native (UXP, RDP, WVD)

Smart card readers: Native (UXP, RDP, WVD)

Serial ports: Native (RDP only)

Human Interface Devices: No redirection

Custom VID:PID

Note: Generic USB redirection will be used for custom VID:PID

☐ Enable HID DigitalPersona fingerprint readers

☐ Enable native redirection for touchscreens

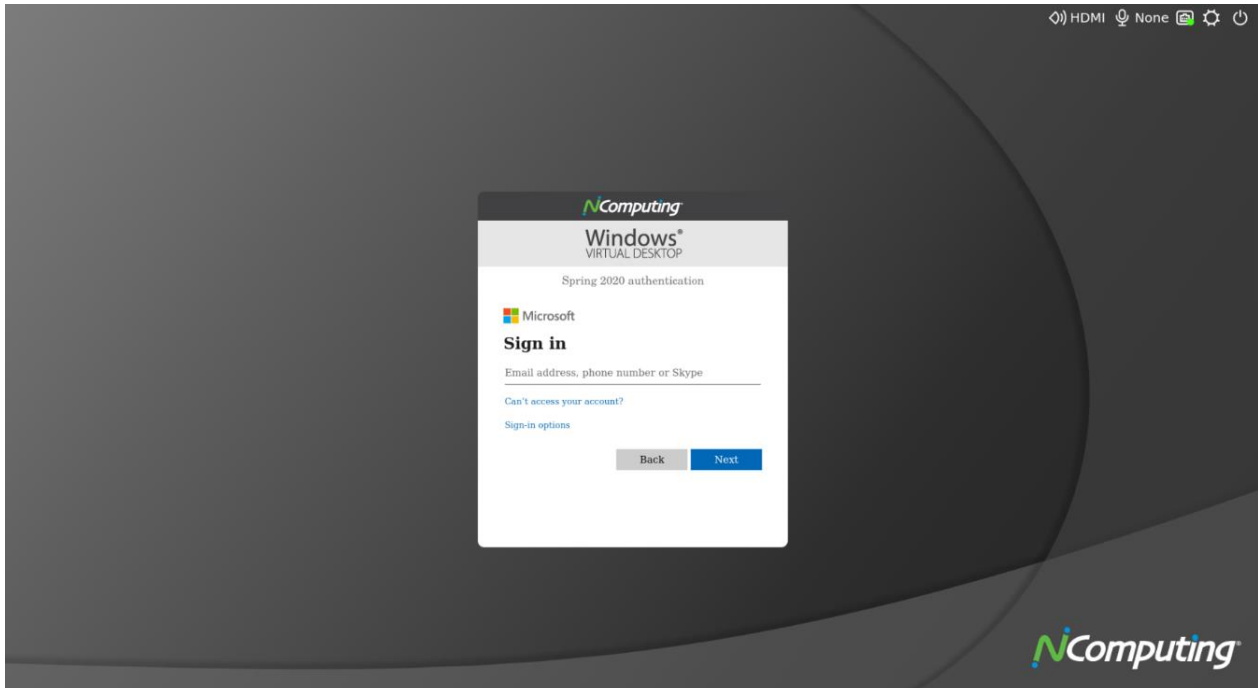
The native redirection of printers requires the printers to be defined locally on the thin client. USB and network (JetDirect) printers are supported. When adding USB printers, a USB printer identification string needs to be specified. It can be also pulled from the USB printer, if it is connected. This 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 AVD virtual 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 AVD session.

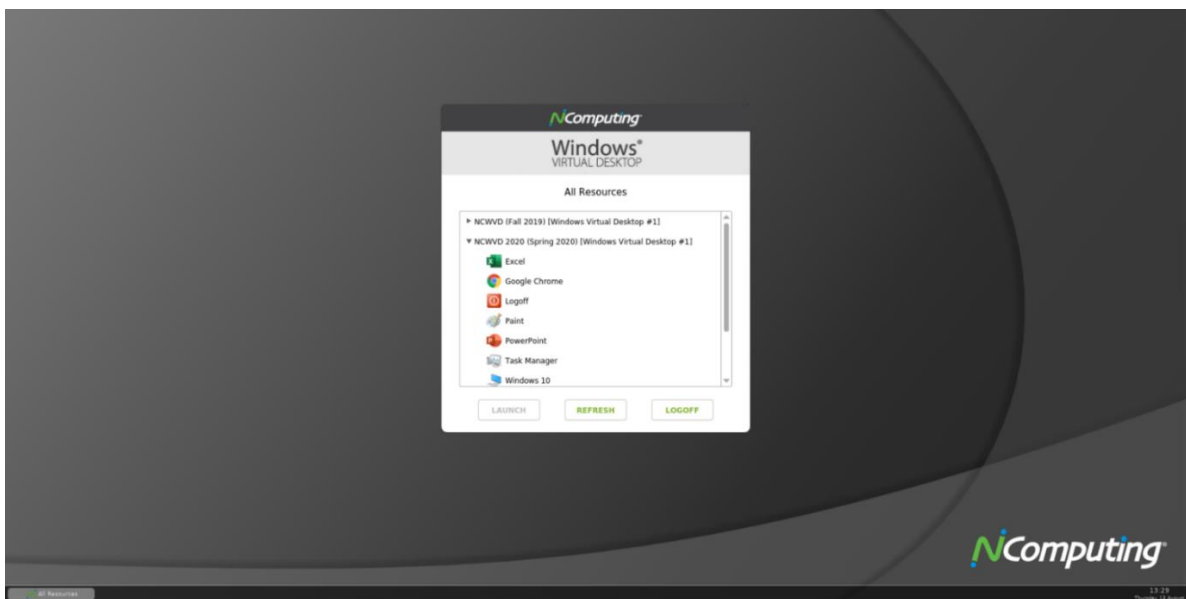
STEP (6) LOGIN TO AVD OR WINDOWS 365 ACCOUNT

If you did not setup 'Kiosk Mode' in step 4, you will need to manually enter your AVD or Windows 365 credentials in the 'AVD Client' login page. Multifactor Authentication (MFA) is also supported (e.g., SMS passcode, authenticator app).

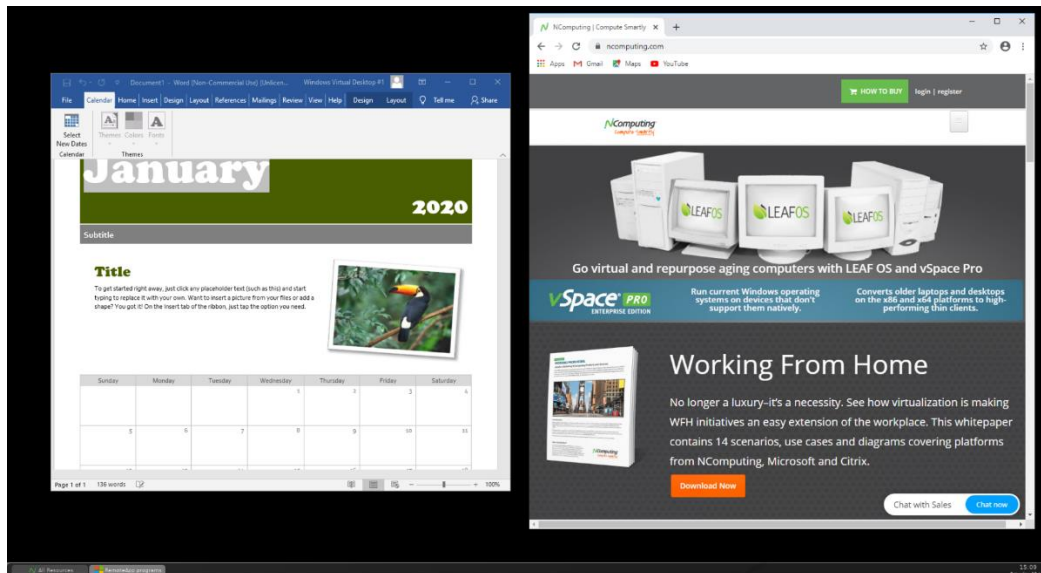


STEP (7) ACCESS AVD OR WINDOWS 365 PUBLISHED RESOURCES

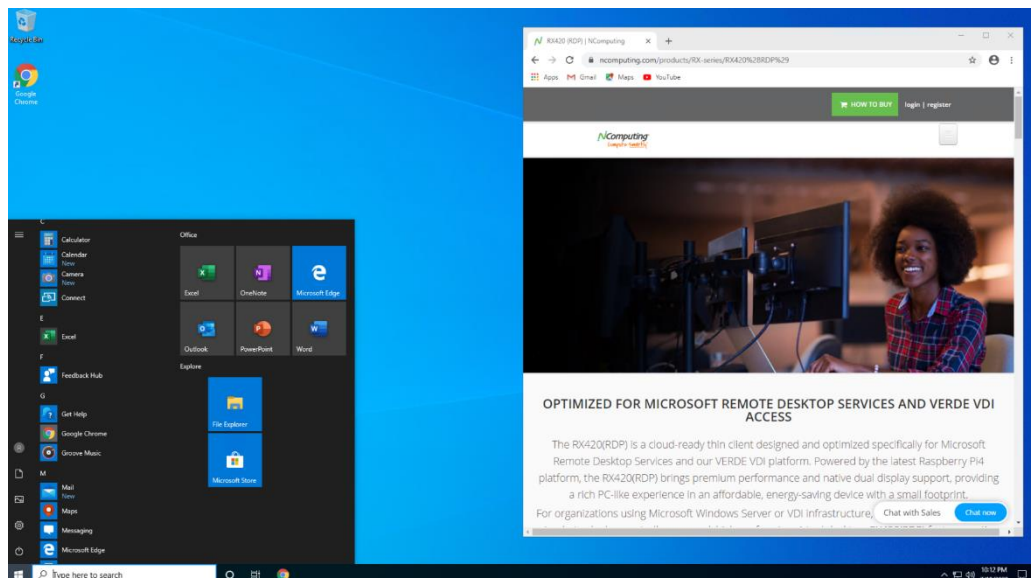
- After you login to the AVD or Windows 365 account, you will be presented with a list of AVD published resources, based on either Spring 2020 or Fall 2019 releases.
- You can expand or collapse the resource listing by clicking at the top-level category.
- Double-click on any RemoteApp or desktop icon to launch the resource.
- Use the integrated taskbar to manage multiple opened applications.



Example: launching multiple AVD RemoteApp programs



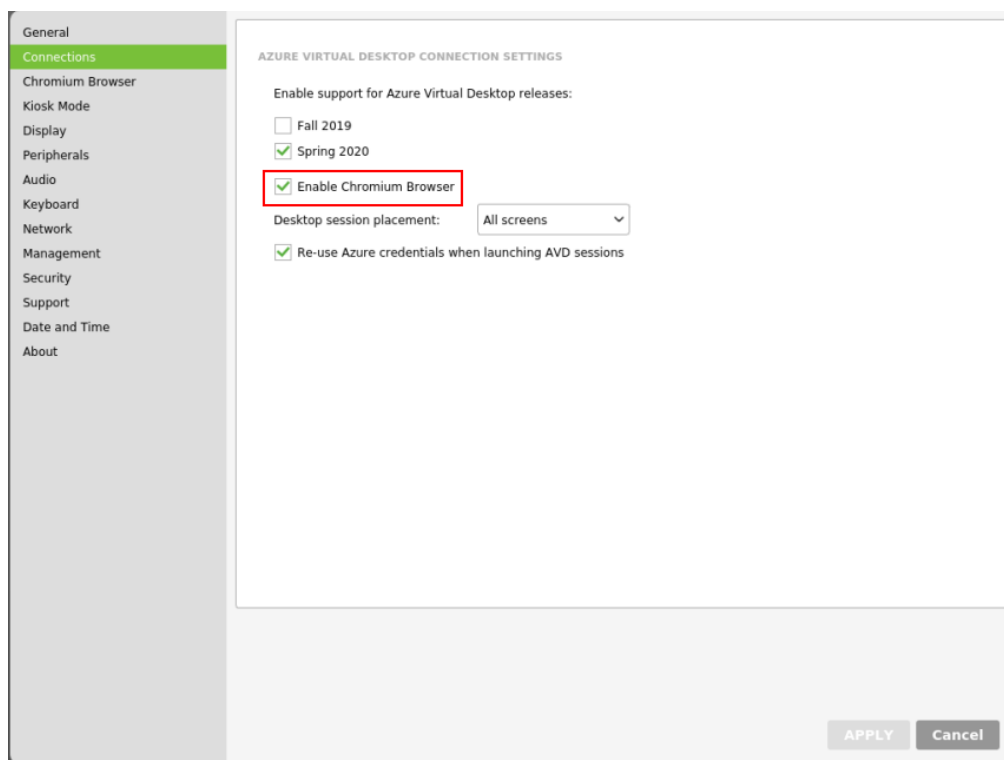
Example: launching full-screen AVD Remote Desktop



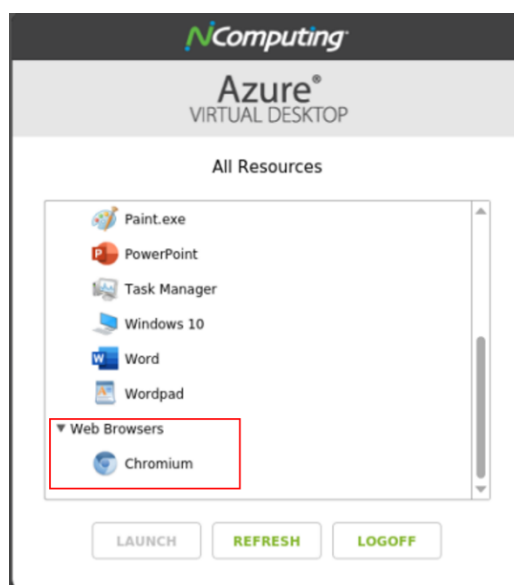
STEP (8) ACCESS LOCAL CHROMIUM BROWSER IN AVD SESSION

RX420(RDP) and RX-RDP+ thin clients allow users to multi-task between AVD sessions and the built-in local Chromium browser, providing added flexibility for direct access of web content and web apps without going through desktop virtualization.

- To enable local Chromium browser in AVD session, the admin first needs to 'Enable Chromium Browser' in the AVD 'Connections' setting menu.



- Once the end-user logs in to his/her AVD session, he/she will see the “Chromium” web browser listing among the AVD all resources listing.



STEP (9) TIPS: MULTI-TASKING IN AVD OR WINDOWS 365 SESSION

- From the AVD or Windows 365 session, the user can launch multiple RemoteApps or RemoteDesktops. If the user launches RemoteDesktop, it will be displayed in full-screen by default. The user can switch from full-screen desktop to ‘windowed’ desktop display to allow for multi-tasking. To switch from full-screen AVD desktop to ‘windowed’ AVD desktop, use the **Ctrl+Alt+Enter** combo key.

Fullscreen mode



Ctrl+Alt+Enter

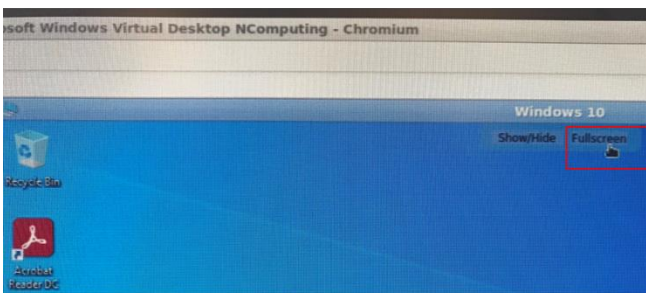


Windowed mode



- To switch from 'windowed' AVD RemoteDesktop to full-screen mode, click on the 'Full screen' icon at the top-center of the desktop.

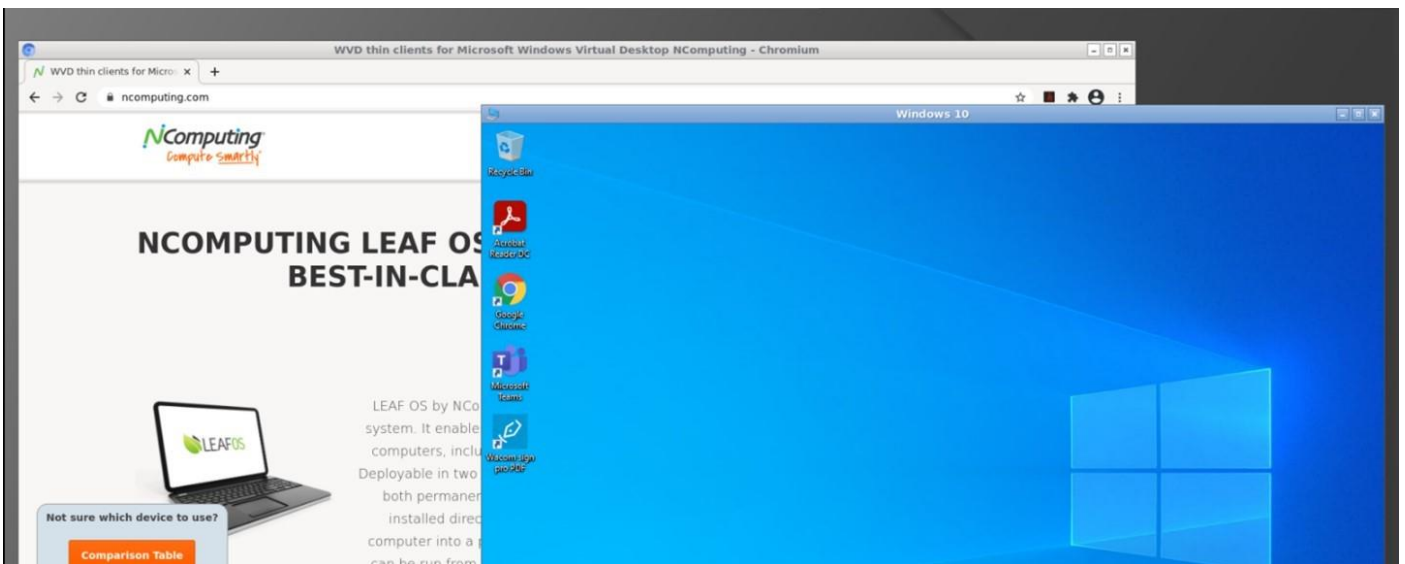
Windowed mode



Click on
'Full screen' icon



- Once the RemoteDesktop is in 'windowed' display mode, the user would be able to multi-task with local 'Chromium' browser (e.g. access side-by-side, minimize, maximize and move windows).



Additional resources:

RX420(RDP)/RX-RDP+ User Configuration Guide:

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

<https://ncomputing.box.com/shared/static/310pp20tfhh4aqc6x4nj14sxxch52q360.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 for 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.
- Remote device shadow support (over LAN or WAN)
- Ability to edit configuration of selected devices and to push configurations to multiple devices (through device profiles).
- Ability to securely shadow all managed 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.

CONTACTING TECHNICAL SUPPORT AND ADDITIONAL RESOURCES

For Microsoft AVD or Windows 365 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.