

NComputing RX420(RDP) and RX-RDP+ Firmware version 2.4.5

RELEASE NOTES

April 14, 2021



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

PRODUCT RELEASE NOTES: NCOMPUTING RX420(RDP) AND RX-RDP+ FIRMWARE, VERSION 2.4.5

Product: NComputing RX420(RDP) and RX-RDP+ firmware

Version: 2.4.5

RX420(RDP) device configuration version: 15

RX-RDP+ device configuration version: 11

Supported hardware:

- NComputing RX420(RDP) thin clients
- NComputing RX-RDP+ thin clients

Supported virtual desktop environments:

- Microsoft Windows Virtual Desktop deployments:
 - Fall 2019 release
 - Spring 2020 release
- Microsoft Remote Desktop Services deployments:
 - Microsoft Windows Server systems:
 - Windows Server 2008 R2
 - Windows Server 2012 R2
 - Windows Server Multipoint Server 2012
 - Windows Server 2016
 - Windows Server 2016 (Multipoint Services)
 - Windows Server 2019
 - Microsoft Windows desktop systems:
 - Windows 7
 - Windows 8.1
 - Windows 10
- NComputing VERDE VDI (version 8.2.1 or higher) and VERDE Remote Access (version 8.2.7 or higher)
- NComputing vSpace Pro Enterprise (version 12.3.2 or higher)

Supported device management systems:

- NComputing PMC (version 2.0.6 or higher)
- vSpace Console from vSpace Pro Enterprise Edition

This document contains important information. Please read the entire document to ensure that your deployment process goes smoothly.

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.

Both devices are designed for **Microsoft Windows Virtual Desktop (WVD) & Remote Desktop Services (RDS)**, **VERDE VDI**, **VERDE Remote PC Access**, as well as **vSpace Pro Enterprise**.

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.

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, perfect for use in SMB and SME organizations with Microsoft Windows Server or VDI infrastructure for on-premise and cloud deployment.

Features highlights:

- Native dual display support for RX420(RDP); single display for RX-RDP+
- Multimedia enhancement through Microsoft RemoteFX
- [Microsoft WVD](#), [Microsoft RDS](#), [VERDE VDI](#) & [Remote Access](#), and [vSpace Pro Enterprise](#) desktop virtualization support
- Microsoft WVD client based on official Microsoft Linux client SDK for best functionality and optimized performance
- NComputing vCAST Streaming technology with SuperRDP software (separate license required)
- Broad USB peripheral support
- Integrated [PMC Device Management](#) software
- Flexible deployment through Gigabit Ethernet or built-in 2.4/5GHz Wi-Fi
- Low cost of ownership and low power consumption

ABOUT THIS RELEASE:

2.4.5 is a major RX420(RDP) and RX-RDP+ firmware release which replaces the 1.12.8 and earlier firmware versions with feature enhancements and bug fixes.

Following are the new product features introduced in RX420(RDP) and RX-RDP+ firmware version 2.4.5:

- Greatly enhanced user experience with hardware-accelerated H.264 decoding for RDP 10 and WVD sessions using the AVC444 codec.
- Webcams support (native/functional redirection) for WVD sessions.
- Local printers support (native/functional redirection) for WVD sessions.
- Hardware-accelerated H.264 encoding for redirected webcams to minimize network bandwidth utilization in RDP, WVD, VERDE VDI and vSpace sessions.
- Setting the first printer from the list of printers defined for native redirection as the default printer for RDP sessions, WVD sessions, and Chromium browser.
- Support for troubleshooting information requests from PMC (when managed by the upcoming PMC 2.6).
- Viewer for the system logs in the Support section of Setup GUI.
- Information about device AMP status in the About section of Setup GUI.

Other improvements introduced in RX420(RDP) and RX-RDP+ firmware version 2.4.5:

- Default peripherals redirection settings differentiated on per device operation mode basis.
- Printers defined for native redirection movable up/down the list.
- Chromium web browser updated to version 86.
- Additional password prompt during WVD VM login when the 'fPromptForPassword' registry value is set to 1.
- Cleaning up the username and password fields in RDP and VERDE VDI client modes when the logon page re-appears after turning off the screen saver or waking the device up from sleep mode.
- Device serial number encoded as QR code in the About section of Setup GUI for easier device registration with the mobile NComputing app.
- Device GUI improvements for better user experience (element styles, font sizes, etc.)
- Updated vCAST web streaming components.

The following RX420(RDP) and RX-RDP+ firmware issues have been fixed in version 2.4.5:

- RXFOURRDP-554 - FreeRDP issues in certain display configurations.
- RXFOURRDP-552 - x11vnc server crash when shadowing RDP sessions.
- RXFOURRDP-548 - WVD VM login issue when the 'fPromptForPassword' registry value is set to 1.
- RXFOURRDP-547 - Generic USB redirection (Incentives Pro) not working in VERDE VDI RDP sessions.
- RXFOURRDP-543 - [WVD] Inability to enter national characters composed with 'dead keys'.

- RXFOURRDP-541 - Incorrect vSpace session state sent to vSpace console after disconnecting session.
- RXFOURRDP-535 - Audio control keys not working in vSpace sessions.
- RXFOURRDP-534 - Bad RDP session performance on second screen in AVC444 mode.
- RXFOURRDP-526 - FullHD dual display not working with some Dell and NEC monitor models.
- RXFOURRDP-498 - [WVD] Black resources list window after session logout when user auto-logon was enabled.
- RXFOURRDP-485 - vSpace session disconnect when USB headset will be unplugged during video playback.
- RXFOURRDP-481 - [WVD] Unexpected runtime execution error when audio output is set to HDMI 1.

PREVIOUS RX420(RDP) AND RX-RDP+ FIRMWARE VERSION 1.12.8 RELEASE NOTES

1.12.8 is a major RX420(RDP) and RX-RDP+ firmware release which replaces the 1.10.10 firmware and earlier versions with feature enhancements and bug fixes.

Following are the new product features introduced in RX420(RDP) and RX-RDP+ firmware version 1.12.8:

- Additional VPN clients:
 - L2TP/IPsec VPN client.
 - IKEv2/IPsec VPN client.
 - SecureGuard VPN client.
 - FortiClient SSL VPN client.
- Notifications about availability of firmware updates.
- Support for Subnet Tags (when managed by the upcoming PMC 2.6).
- Ability to set up a custom boot splash image.
- Support for the shutdown command sent by vSpace Console.

Other improvements introduced in RX420(RDP) and RX-RDP+ firmware version 1.12.8:

- Chromium web browser updated to version 84 (with optimizations for web-based Microsoft Teams and Zoom conferencing).
- OpenConnect VPN client updated to version 8.10.
- Support for more MFA solutions with (optional) additional credentials prompt before launching WVD session.
- Additional primary and secondary screen resolution selections.
- Additional secondary screen position selections (support for vertical dual screen layouts).
- VPN reconnect after plugging in the Ethernet cable.
- NTP date and time update after plugging in the Ethernet cable.
- Updated vSpace Client with support for screen resolutions up to 2560x1440.
- New default NComputing wallpaper.
- Updated vCAST web streaming components.

The following RX420(RDP) and RX-RDP+ firmware issues have been fixed in version 1.12.8:

- RXFOURRDP-467 - [WVD] Black screen after session logout when application auto-start was enabled.
- RXFOURRDP-466 - [WVD] Published resources with "/" in name are not listed.
- RXFOURRDP-463 - Incorrect calculation of MD5 sums for certificate files added manually.
- RXFOURRDP-452 - Blurry text in vSpace Session with 1920x1200 resolution.
- RXFOURRDP-436 - Redirection issue when USB 3.0 mass storage device is plugged into USB 3.0 port in vSpace Client mode.
- RXFOURRDP-421 - [WVD] Using microphone for long time causes out of memory error.
- RXFOURRDP-420 - WVD session crashes occasionally when an application tries to open the microphone.
- RXFOURRDP-415 - Black screen on primary display when resolutions are automatically set to 1920x1080 75Hz in dual display mode.
- RXFOURRDP-414 - After second click on Back button in WVD logon page, empty resources list is shown with authentication error.
- RXFOURRDP-401 - [WVD] Inability to open Setup GUI when device was booted while network was unavailable.
- RXFOURRDP-397 - WVD session freeze when an application tries to open redirected microphone, but no microphone is present.
- RXFOURRDP-367 - vCAST web streaming - frequent flickering in vSpace Client mode.
- RXFOURRDP-345 - RDP session disconnects when VLC player gets closed.

PREVIOUS RX420(RDP) AND RX-RDP+ FIRMWARE VERSION 1.10.10 RELEASE NOTES

Following are the new product features introduced in RX420(RDP) and RX-RDP+ firmware version 1.10.10:

- Microsoft Windows Virtual Desktop client allowing connections to Windows Virtual Desktop deployments hosted in Microsoft Azure cloud.
 - Spring 2020 and Fall 2019 Windows Virtual Desktop releases
 - Multi-Factor-Authentication (MFA) support
 - RemoteApp programs and desktops
 - Regular vs. Kiosk mode auto-login
 - Native dual display with independent screen rotation
 - Peripheral devices:
 - Storage
 - Audio
- Chromium web browser available locally as new device operation mode or as an additional option for WVD Client and RDP Client (with RemoteApp) operation modes.
- Native/functional webcam redirection for RDP, VERDE VDI and vSpace sessions.
- RDP 10 protocol support in RDP Client and VERDE VDI Client modes.

Other improvements introduced in RX420(RDP) and RX-RDP+ firmware version 1.10.10:

- Ability to select Wi-Fi network frequency range (2.4 GHz or 5 GHz) when configuring Wi-Fi connections.
- Improved Ethernet network detection process.
- Support for 2560x1080, 2560x1440 and 2560x1600 automatic screen resolutions with 50 Hz refresh rate.
- Faster GUI initialization after device bootup.

The following RX420(RDP) and RX-RDP+ firmware issues have been fixed in version 1.10.10:

- RXFOURRDP-374 - OpenVPN: Device caches the .ovpn file and user credentials even when not configured to do so.
- RXFOURRDP-373 - Incorrect entry in /boot/cmdline.txt causing sluggish behavior of wireless mice.
- RXFOURRDP-286 - Keys do not autorepeat in VNC shadow.

PREVIOUS RX420(RDP) FIRMWARE VERSION 1.8.0 RELEASE NOTES

Following are the product features introduced in RX420(RDP) firmware version 1.8.0:

- Support for the VERDE Remote Access feature to further enable work-from-home use cases (VERDE 8.2.7 or higher version).
- vSpace Client operation mode for connections to vSpace Pro Enterprise servers (version 12.3.2 or higher).

Other improvements introduced in RX420(RDP) firmware version 1.8.0

- Reduced Wi-Fi settings application time.
- Improved behavior of the Wi-Fi icon.
- Improved system daemons reloading procedure when applying configuration changes.
- Improved RDP sessions stability by disabling audio redirection when "No audio output/input" is at the top of audio priority list.
- Improved dialog box for selecting USB devices identified by custom VID:PID.
- Ctrl-Alt-Arrow Up/Down key combination for local windows switching.
- Improved GUI styling.

The following RX420(RDP) firmware issues have been fixed in version 1.8.0:

- RXFOURRDP-163 - Issue with launching RDP RemoteApp resources.
- RXFOURRDP-160 - GUI does not re-appear after touch screen calibration.
- RXFOURRDP-151 - GUI crash when Ethernet, VPN and PMC were connected and the Ethernet cable was unplugged/plugged.
- RXFOURRDP-139 - OpenVPN: The key file specified as parameter of the tls-auth entry of .ovpn file does not get copied from memory stick.
- RXFOURRDP-111 The English/Korean (한/영) toggle key doesn't work in RDP sessions.

FIRMWARE UPDATE INSTRUCTIONS

The firmware update (including the download of firmware package) can take a few minutes. Please do not turn off your device during this time. Once the firmware update is complete, the device will reboot automatically.

- **Updating the firmware locally**

The device firmware can be updated manually from the Setup GUI with a firmware update package uploaded to an FTP or a web server or from a locally connected USB memory stick:

- For FTP or web server (URL):
 - Upload the 'rx4x0-rdp-2.4.5.upd' firmware update package file into your FTP or web server.
 - On the RX420(RDP) and RX-RDP+ device open the Setup GUI and go to the 'Support' section.
 - Enter the FTP or HTTP URL of the firmware update package and click the 'Update' button.
 - Alternatively, user can use the following NComputing's web URL to download and install this version of firmware directly to the RX420(RDP) and RX-RDP+ device:

<http://firmware.ncomputing.com/RX420/rx4x0-rdp-2.4.5.upd>

- For a locally connected USB memory stick:
 - Download the 'rx4x0-rdp-2.4.5.upd' and save it to a USB memory stick.
 - Insert the USB stick to RX420(RDP) or RX-RDP+.
 - On the RX420(RDP) or RX-RDP+ device, open the Setup GUI and go to the 'Support' section.
 - Select 'Update from the USB memory stick' radio-button, select the firmware update file displayed in the pop-up, and click the 'Update button'.

Once the device finishes downloading the firmware update package, the firmware update process will start and will take a while (around half a minute). The process should not be interrupted. Firmware update will end with a device reboot.

- **Updating firmware from PMC**

The device firmware can be updated from supported version of PMC. 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-2.4.5.upd' file.
- Click the 'Upload file' button to upload the firmware package.

- In PMC 2.0.6:
 - Open the Menu, go to 'Device Management > Firmware Updates'.
 - Select the 'rx4x0-rdp-2.4.5.upd' firmware package.
 - Select the device group.
 - Select the devices which should receive the firmware update.
- In PMC 2.5:
 - Open the Menu, go to 'Devices'.
 - Select the devices which should receive the firmware update.
 - Execute the 'Update Firmware' task of the Devices list.
 - Select the 'rx4x0-rdp-2.4.5.upd' 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. For remote devices the process can be followed by observing the Audit Events log on Dashboard. The firmware update process will take a while and should not be interrupted. Firmware update will end with a device reboot.

ADDITIONAL NOTES

- **Authentication methods supported by the VPN clients added in 1.12.5 and newer firmware:**
 - L2TP/IPsec VPN - pre-shared key, username, password.
 - IKEv2/IPsec VPN client - client certificate with password.
 - SecureGuard VPN client - username and password.
 - FortiClient SSL VPN client - username and password.
- **Setting up a custom boot splash image**
Only image files in PNG format are supported.
- **Managing the RX420(RDP) and RX-RDP+ devices from PMC**
Each RX420(RDP) and RX-RDP+ device comes with a perpetual license of PMC software and first-year complimentary software maintenance update (AMP for RDP) license. After the first-year complimentary device [AMP for RDP](#) has expired, the device will not be able to receive and apply firmware updates. An extended device [AMP for RDP](#) licenses must be purchased and allocated to each RX420(RDP) and RX-RDP+ device to allow firmware updates via local or remote (via PMC).
- **Managing the RX420(RDP) and RX-RDP+ devices with 2.4.5 firmware from PMC**
The 2.4.5 firmware uses version 15 of the device configuration when installed on RX420(RDP) and version 11 when installed on RX-RDP+. To be able to manage the RX420(RDP) and RX-RDP+ devices running firmware using these configuration versions, a set of schema files describing these configuration versions must be uploaded to PMC. Without that PMC will only

be able to show the devices on the device list and schedule firmware updates, but will not allow editing the device (or device profile) settings.

Follow the below steps to upload to PMC the schema files for RX420(RDP) configuration version 15 and RX-RDP+ configuration version 11:

- Logon to PMC as a user with administrative privileges, open the Menu, go to 'Administration > Device Configurations'.
- Click the 'Choose file' button and select the PCU file containing the new schema files.
- Click the 'Upload file' button to upload the schema files.

After completing the above steps, PMC will become fully able to manage the RX420(RDP) devices running firmware using configuration version 15 and RX-RDP+ devices running firmware using configuration version 11 (e.g. the 1.12.5, 1.12.7, 1.12.8 and 2.4.5 firmware).

- **PMC server auto-discovery**

To automate the PMC server discovery the DHCP option 207 can be used. This DHCP option should provide a string value containing the URL in form of 'https://<PMC_address>', like: 'https://pmc.company.local', or: 'https://192.168.10.12'.

- **RD Session Host and WVD virtual machine configuration for best user experience**

The RDP and WVD clients integrated in RX420(RDP) and RX-RDP+ devices support the use of H.264/AVC encoding (Advanced Video Codec) in RDP and WVD sessions. Using AVC ensures the best WVD user experience. To take advantage of this H.264/AVC graphics mode, 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 graphics mode for Remote Desktop Connections'.

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).

- **RD Session Host and WVD virtual machine configuration for webcam redirection**

The RDP and WVD 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

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).

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 RDP or WVD session.

- **RD Session Host and WVD virtual machine configuration for printers redirection**

The RDP and WVD 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 RD Session Host or WVD 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

The above mentioned Group Policy settings can be deployed through Active Directory Group Policy Objects or, in simplest case, they can be configured on the local machine with Local Group Policy Editor (gpedit.msc).

- **RD Session Host and WVD virtual machine configuration for smart cards redirection**

The RDP and WVD clients integrated in RX420(RDP) and RX-RDP+ devices support the native (functional) redirection of smart cards (smart card readers). CCID-compliant, ReinerSCT and ACS smart card readers are supported. Refer to [Appendix A](#) 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

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).

- **WVD Client connection configuration**

The RX420(RDP) and RX-RDP+ firmware supports connections to Microsoft Windows Virtual Desktop deployments hosted in Microsoft Azure cloud. When the 'WVD Client' will be selected as device operation mode under General settings, then, under Connections settings, the WVD release version matching customer's deployment(s) should be selected. The 'Spring 2020' WVD release will be selected by default. The 'Fall 2019' release can be enabled additionally, or instead of 'Spring 2020'. The user will be asked for credentials and the authentication will be performed separately for each enabled WVD release. This will even happen when both customer's WVD deployments are based on the same Azure Active Directory.

- **Accessing published WVD resources**

After logging into the WVD account, user will be presented with a list of WVD published resources, based on either 'Spring 2020' or 'Fall 2019' releases. The resource listing can be expanded or collapsed by clicking at the top-level category. Double-clicking on any RemoteApp or desktop icon allows launching the resource. The taskbar at the bottom of the screen can be used to manage multiple opened applications.

- **WVD Client connection in Kiosk Mode**

The 'Kiosk Mode' settings allow the user to automatically login to his/her WVD account, and if required, automatically launch a particular Windows application or desktop. The 'Domain' field allows preconfiguration of the Azure Active Directory domain name. Preconfiguring a domain name will simplify users logon, as the users will only need to provide their names, without the '@domainname...' suffix. Please note that multifactor authentication (MFA) is not supported when 'Kiosk Mode' is enabled.

- **RDP Client connection configuration**

The RX420(RDP) and RX-RDP+ firmware supports RemoteApp and Desktop Connections. The parameters necessary for the RDP Client connection are different depending on the RemoteApp support being enabled or not.

- RemoteApp and Desktop Connections not enabled: The RDP Client connects directly to specified Remote Desktop Session Host.
- RemoteApp and Desktop Connections enabled: The RDP Client first communicates with the specified Remote Desktop Web Access server (which cooperates with Remote Desktop Connection Broker; both must exist in the RDS deployment). The Remote Desktop Web Access server URL must be specified in RDP Client connection configuration. This URL can be entered in simplified or full form, e.g.:
 - 192.168.50.7 - will be expanded to:
https://192.168.50.7/RDweb
 - rdwa - will be expanded to: https://rdwa/RDWeb
 - rdwa.company.local - will be expanded to:
https://rdwa.company.local/RDWeb
 - https://rdwa.company.local/RDWeb - will be used as is.

- **Using custom parameters for RDP connections**

The RX420(RDP) and RX-RDP+ firmware allows specifying custom parameters for RDP connections. Please refer to FreeRDP documentation

(<https://github.com/FreeRDP/FreeRDP/wiki/CommandLineInterface>) for the information about supported parameters. If multiple custom parameters must be specified then they should be separated by the “;” (semicolon) character.

- **vCAST support in RDP sessions**

Support for vCAST Web Streaming and vCAST VLC Media Streaming in RDP sessions started from RX420(RDP) and RX-RDP+ devices require installation of the NComputing SuperRDP Server Pack software on the Remote Desktop machine. The ‘Enable RDP 10’ decoding option must be disabled in the device’s setting (under ‘Connections’ tab). The NComputing SuperRDP server pack is available through your reseller (SKU: SuperRDP-PREM-VC-P).

- **vCAST limitations**

The vCAST Web Streaming and vCAST Media Streaming technologies require the client device to use optimized (hardware-accelerated) display drawing to work properly. Such optimized drawing methods are only available when the terminal session runs in full-screen desktop mode. For that reason vCAST is not supported in published RemoteApp programs. RemoteApp desktop sessions run in full-screen mode and support vCAST.

Note: For vCAST support in RDP sessions, the SuperRDP software must be installed on the remote machine.

The vCAST Media Streaming technology can only offload to the client device H.264-encoded media contents. For other formats the VLC player needs to have the ‘Windows GDI’ video output selected under Video output settings.

- **Connecting to vSpace Pro Enterprise servers**

vSpace Client connections from RX420(RDP) and RX-RDP+ devices are only supported on latest vSpace Pro Enterprise (12.3.2 or newer) servers. vSpace Pro 11 LTS servers will not accept connections from RX420(RDP) and RX-RDP+ devices.

Unlike the vSpace Clients contained in the NComputing RX300 thin client devices, the vSpace Clients from the RX420(RDP) and RX-RDP+ firmware do not contain any embedded vSpace Client connection licenses. Appropriate vSpace Client connection licenses need to be purchased and added to the vSpace Pro Enterprise deployments to allow uninterrupted vSpace Client connections from RX420(RDP) and RX-RDP+ devices. Without the necessary licenses, the vSpace sessions will run in trial mode and will be disconnected after 10 minutes.

vSpace Pro Client Connection License ordering SKUs:

- 1 year (vSpacePro-SW-1A)
- 3 years (vSpacePro-SW-3A)
- 5 years (vSpacePro-SW-5A)

- **Connecting to VERDE VDI or VERDE Remote Access**

Two license types are supported. Both are concurrent connection models:

- VERDE-WFH-1A-10 (VERDE VDI Suite - Remote Access 10-seat license, annual subscription)

- This license type allows Remote Access connections to PCs through the VERDE Connection Broker and is the most affordable option.
 - VERDE8-CCU-1A (VERDE VDI Suite -1-seat license, annual subscription)
 - This license type allows Remote Access connections to PCs through the VERDE Connection Broker and supports connections to VDI sessions hosted by VERDE Servers.
- **Touchscreen support**

Touchscreen monitors are only supported when only one (primary) display is connected.
- **Server CPU load in RDP 8 sessions with RemoteFX enabled**

Enabling the RemoteFX feature for Remote Desktop connections greatly improves user experience by providing very good GUI performance. This is thanks to optimized algorithms used to encode the areas of the session screen which contain dynamically changing contents (like videos or animations). Ideally the screen encoding on the server side should be accelerated by supported graphics cards. Leveraging server CPUs for RemoteFX screen encoding can cause high load and effectively limit the per-server user density.
- **Kiosk mode application auto-start**

Latest versions of Windows operating systems favor RemoteApp publishing and do not allow launching applications with executable program paths specified on the client side. This functionality can be re-enabled by modifying the Windows registry:

Registry key: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\TSAppAllowList
 Registry value: REG_DWORD fDisabledAllowList
 Registry value data: 1

Registry key: HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server
 Registry value: REG_DWORD HonorLegacySettings
 Registry value data: 1

Published RemoteApp program or desktop will be automatically started when program or desktop name will be specified as 'Application' in Kiosk Mode configuration. RX420(RDP) and RX-RDP+ device must be configured in 'RDP Client' mode with RemoteApp support enabled in Connection settings for this feature to work.
- **Native (functional) redirection of printers in RDP and WVD sessions**

Following are the topics to consider when planning to use the native/functional redirection of printers in RDP sessions:

 - Locally connected USB printers and network printers supporting the JetDirect protocol (also known as RAW or AppSocket) can be used with native redirection.
 - Low-cost GDI printers should be avoided, as they may not work properly. More advanced printers understanding the PCL, PostScript, and/or other high-level page description languages are advisable and should work.

- Functional redirection of printers requires the installation of appropriate Windows printer driver on the remote machine running the RDP session. The literally spelled name of the Windows printer driver must be entered in the 'Windows printer driver name' when adding a printer for native redirection.
- The 'Windows printer driver name' often matches the 'USB printer identification' string obtained from the USB printer during the detection process, but this is not a general rule. For some USB printers the 'Windows printer driver name' automatically populated when detecting the printer will have to be edited to match the real name of the Windows printer driver installed on the remote server.
- The 'type 3' drivers for Windows x64 architecture should be selected for installation. 'Type 4' drivers are known to cause issues with functional redirection of printers.
- The list of Windows printer drivers installed on a Windows machine (with the information about class and architecture) can be obtained with the following command executed in Command Prompt:

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

- **Native (functional) redirection of webcams in RDP and WVD sessions**

Native redirection of webcams is only supported in RDP and WVD sessions only if the Remote Desktop Session Host is a Windows Server 2019 or a Windows 10 machine. Each user, under Privacy settings, needs to allow the applications to access the redirected camera.

- **Native (functional) redirection of webcams in UXP sessions**

vSpace Pro Enterprise 12.4 is necessary for the native webcam redirection functionality. Each user, under Privacy settings, needs to allow the applications to access the redirected camera.

- **Native (functional) redirection of smart card readers in RDP, WVD and UXP sessions**

Functional redirection of smart card readers leverages the PC/SC daemon and smart card reader drives embedded in the device firmware. Please refer to [Appendix A](#) for the list of smart card reader drivers contained in RX420(RDP) and RX-RDP+ firmware.

- **Generic USB redirection of peripheral devices in RDP sessions on Windows Server 2016/2019 and Windows 10**

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 the above mentioned 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 in Remote Desktop sessions running on operating systems mentioned in this note this policy must be explicitly disabled. 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.

ADDITIONAL RESOURCES

- **RX420(RDP) and RX-RDP+ User Configuration Guide:**

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

<https://ncomputing.box.com/shared/static/310pp20tfhh4aqc6x4nj14sxxh52q360.pdf>

- **PMC Device Management Quick Start Guide:**

NComputing PMC is a device management system designed and developed to remotely manage NComputing access devices.

Please refer to the PMC 2.5 Quick Start Guide:

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

CONTACTING NCOMPUTING TECHNICAL SUPPORT

- Visit the NComputing Knowledge Base at <http://kb.ncomputing.com/> for more information, guides, and walkthroughs.
- To request Technical Support, please visit the NComputing Support page at <http://www.ncomputing.com/support/overview>.

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 2021 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.

APPENDIX A - LIST OF AVAILABLE SMART CARD READERS DRIVERS

Drivers for following smart card readers are present in the firmware and the following readers should work:

Readers supported by the Reiner SCT cyberJack driver:

- REINER SCT cyberJack pp_a
- REINER SCT cyberJack ecom_a
- REINER SCT cyberJack pp_a2
- REINER SCT cyberJack RFID standard
- REINER SCT cyberJack RFID komfort
- REINER SCT cyberJack compact
- REINER SCT cyberJack go / go plus
- REINER SCT cyberJack wave

Readers supported by the ACS driver:

- ACS ACR32 ICC Reader
- ACS ACR3201 ICC Reader
- ACS ACR33U-A1 3SAM ICC Reader
- ACS ACR33U-A2 3SAM ICC Reader
- ACS ACR33U-A3 3SAM ICC Reader
- ACS ACR33U 4SAM ICC Reader
- ACS ACR38U-CCID
- ACS ACR3801
- ACS ACR39U ICC Reader
- ACS ACR39K ICC Reader
- ACS ACR39T ICC Reader
- ACS ACR39F ICC Reader
- ACS ACR39U ID1 Card Reader
- ACS ACR39U-SAM ICC Reader
- ACS ACR3901 ICC Reader
- ACS ACR83U
- ACS ACR85 PINPad Reader
- ACS ACR88U
- ACS ACR89 ICC Reader
- ACS ACR89 Dual Reader
- ACS ACR89 FP Reader
- ACS ACR100 ICC Reader
- ACS ACR101 ICC Reader
- ACS ACR102 ICC Reader
- ACS ACR122U
- ACS ACR1222 1SAM PICC Reader
- ACS ACR1222 1SAM Dual Reader
- ACS ACR1222 Dual Reader
- ACS ACR1222 1SAM PICC Reader
- ACS ACR1222 3S PICC Reader
- ACS ACR123 3S Reader
- ACS ACR123 PICC Reader
- ACS ACR123US_BL
- ACS ACR125 nPA plus
- ACS ACR1251 1S CL Reader
- ACS ACR1251 CL Reader
- ACS ACR122U
- ACS ACR1251U-C Smart Card Reader
- ACS ACR1251U-C Smart Card Reader

- ACS ACR1251K Dual Reader
- ACS ACR1251 1S Dual Reader
- ACS ACR1251 Reader
- ACS ACR1251 CL Reader
- ACS ACR1252 1S CL Reader
- ACS ACR1252 CL Reader
- ACS ACR1252 USB FW_Upgrade v100
- ACS ACR1252U BADANAMU MAGIC READER
- ACS ACR1252IMP 1S CL Reader
- ACS ACR1255U-J1 PICC Reader
- ACS ACR1256U PICC Reader
- ACS ACR1261 1S Dual Reader
- ACS ACR1261 CL Reader
- ACS ACR128U
- ACS ACR1281 1S Dual Reader
- ACS ACR1281 CL Reader
- ACS ACR1281 Dual Reader
- ACS ACR1281 PICC Reader
- ACS ACR1281 Dual Reader
- ACS ACR1281 PICC Reader
- ACS ACR1281 Dual Reader
- ACS ACR1281 2S CL Reader
- ACS ACR1281 1S PICC Reader
- ACS ACR1281U-K PICC Reader
- ACS ACR1281U-K Dual Reader
- ACS ACR1281U-K 1S Dual Reader
- ACS ACR1281U-K 4S Dual Reader
- ACS ACR1283 4S CL Reader
- ACS ACR1283 CL Reader
- ACS ACR1283U FW Upgrade
- ACS ACR1311 PICC Reader
- ACS AET62 PICC Reader
- ACS AET62 1SAM PICC Reader
- ACS AET65 ICC Reader
- ACS AMR220 Reader
- ACS APG8201
- ACS APG8201-B2
- ACS APG8201Z
- ACS APG8201Z
- ACS CryptoMate64
- ACS CryptoMate (T1)
- ACS CryptoMate (T2)
- ACS ACR38U
- ACS ACR38U-SAM
- ACS AET65 1SAM ICC Reader
- ACS CryptoMate
- IRIS SCR21U

CCID-compliant readers:

- Access IS ePassport Reader
- Access IS NFC Smart Module
- ACS ACR 38U-CCID
- ACS ACR101 ICC Reader
- ACS ACR122U PICC Interface
- ACS ACR1251 Dual Reader
- ACS ACR1252 Dual Reader

- ACS ACR1255U-J1
- ACS ACR3901U ICC Reader
- ACS ACR39U ICC Reader
- ACS APG8201 PINhandy 1
- ACS APG8201 USB Reader
- ACS CryptoMate (T2)
- ACS CryptoMate64
- ActivCard ActivCard USB Reader V2
- ActivIdentity Activkey_Sim
- ActivIdentity USB Reader V3
- AK910 CKey
- AK910 IDONE
- Aktiv Co., ProgramPark Rutoken Magistra
- Aktiv PINPad Ex
- Aktiv PINPad In
- Aktiv Rutoken ECP
- Aktiv Rutoken lite
- Aktiv Rutoken PINPad 2
- Aladdin R.D. JaCarta
- Aladdin R.D. JaCarta Flash
- Aladdin R.D. JaCarta LT
- Aladdin R.D. JaCarta U2F (JC602)
- Aladdin R.D. JCR-770
- Aladdin R.D. JC-WebPass (JC600)
- Alcor Micro AU9520
- Alcor Micro AU9522
- Alcor Micro AU9560
- ANCUUD CCID USB Reader & RNG
- appidkey GmbH ID100L-USB-SC-Reader
- appidkey GmbH ID50 -USB
- appidkey GmbH ID60-USB
- ASK-RFID CPL108
- Athena ASE IIIe
- Athena ASEDrive IIIe Combo Bio PIV
- Athena ASEDrive IIIe KB
- Athena ASEDrive IIIe KB Bio PIV
- Athena IDProtect Flash
- Athena IDProtect Key v2
- ATMEL AT90SCR050
- ATMEL AT90SCR100
- ATMEL AT91SC192192CT-USB ICCD reader
- ATMEL AT91SO CCID Smart Card Reader
- ATMEL AT98SC032CT-USB
- ATMEL VaultIC420 Smart Object
- ATMEL VaultIC440
- ATMEL VaultIC460
- Avtor SC Reader 371
- Avtor SecureToken
- Axalto Reflex USB v3
- BIFIT iBank2Key
- BIFIT iToken
- BIFIT USB-Token iBank2key
- Bit4id CKey4
- Bit4id cryptokey
- Bit4id Digital DNA Key
- Bit4id iAM

- Bit4id miniLector
- Bit4id miniLector-s
- Bit4id tokenME FIPS v3
- BLUTRONICS BLUDRIVE II CCID
- Broadcom Corp 5880
- C3PO KBR36
- C3PO LTC31 v2
- C3PO LTC32
- C3PO LTC36
- C3PO LTC3x USB
- C3PO TLTC2USB
- CASTLES EZCCID Smart Card Reader
- CCB eSafeLD
- charismathics plug'n'crypt CCID token
- Cherry GmbH SmartBoard XX1X
- Cherry GmbH SmartBoard XX33
- Cherry GmbH SmartBoard XX44
- Cherry GmbH SmartTerminal ST-1275
- Cherry GmbH SmartTerminal ST-2xxx
- Cherry GmbH SmartTerminal XX1X
- Cherry GmbH SmartTerminal XX44
- Cherry KC 1000 SC
- Cherry KC 1000 SC Z
- Cherry KC 1000 SC/DI
- Cherry KC 1000 SC/DI Z
- Cherry Smart Card Reader USB
- Cherry Smartcard Keyboard G87-1xx44
- Cherry SmartTerminal XX44
- Cherry TC 1300
- Chicony HP USB Smartcard CCID Keyboard JP
- Chicony HP USB Smartcard CCID Keyboard KR
- Chicony USB Smart Card Keyboard
- COVADIS ALYA
- COVADIS Auriga
- COVADIS VEGA-ALPHA
- Dell Dell Smart Card Reader Keyboard
- Dell keyboard SK-3106
- DUALi DE-620 Combi
- DUALi DRAGON NFC READER
- eID_R6 001 X8
- Elatec TWN4 SmartCard NFC
- Elatec TWN4/B1.06/CPF3.05/S1SC1.32/P (Beta 3)
- ESMART Token GOST
- Eutron Card Reader
- Eutron Cryptoidentity CCID
- Eutron Digipass 860
- Eutron Smart Pocket
- Feitian 502-CL
- Feitian bR301
- Feitian bR500
- Feitian eJAVA Token
- Feitian ePass2003
- FEITIAN iR301
- Feitian R502
- Feitian SCR301
- Feitian Technologies FT SCR310

- Feitian VR504 VHBR Contactless & Contact Card Reader
- Free Software Initiative of Japan GnuK
- FT CCID
- FT CCID KB
- FT ePass2003Auto
- FT U2F CCID
- FT U2F CCID KB
- Fujitsu Siemens Computers SmartCard Keyboard USB 2A
- Fujitsu Siemens Computers SmartCard USB 2A
- Fujitsu Smartcard Reader D323
- FujitsuTechnologySolutions GmbH Keyboard KB100 SCR
- FujitsuTechnologySolutions GmbH Keyboard KB100 SCR eSIG
- FujitsuTechnologySolutions GmbH Smartcard Keyboard G87-914x
- FujitsuTechnologySolutions GmbH SmartCase KB SCR eSIG
- GEMALTO CT1100
- Gemalto EZIO CB+
- Gemalto Ezio Shield
- Gemalto Ezio Shield Branch Reader
- Gemalto Ezio Shield Secure Channel
- Gemalto Gem e-Seal Pro USB Token
- Gemalto GemCore SIM Pro Smart Card Reader
- Gemalto GemPC Express
- Gemalto Gemplus USB SmartCard Reader 433-Swap
- Gemalto Hybrid Smartcard Reader
- Gemalto IDBridge K3000
- Gemalto PC Twin Reader
- Gemalto PDT
- Gemalto Prox Dual USB PC Link Reader
- Gemalto Prox SU USB PC LinkReader
- Gemalto SA .NET Dual
- Gemalto Smart Enterprise Guardian Secure USB Device
- Gemalto USB GemPCPinpad SmartCard Reader
- Gemalto USB Shell Token V2
- Gemplus GemCore POS Pro Smart Card Reader
- Generic MultiCard Device
- Generic Smart Card Reader Interface
- Generic USB Smart Card Reader
- Generic USB2.0-CRW
- German Privacy Foundation Crypto Stick v1.2
- Giesecke & Devrient GmbH Star Sign Card Token 350 (ICCD)
- Giesecke & Devrient GmbH Star Sign Card Token 550 (ICCD)
- Giesecke & Devrient GmbH StarSign Crypto USB Token
- Giesecke & Devrient GmbH StarSign CUT S
- GIS Ltd SmartMouse USB
- GoldKey Security PIV Token
- HDZB uKeyCI800-K18
- Hewlett Packard HP USB Smartcard CCID Keyboard
- Hewlett Packard MFP Smart Card Reader
- Hewlett-Packard Company HP USB CCID Smartcard Keyboard
- Hewlett-Packard Company HP USB Smart Card Keyboard
- Hewlett-Packard HP It4112 Gobi 4G Module
- HID Global OMNIKEY 3x21 Smart Card Reader
- HID Global OMNIKEY 5022 Smart Card Reader
- HID Global OMNIKEY 5122 Dual
- HID Global OMNIKEY 5122 Smartcard Reader
- HID Global OMNIKEY 5422 Smartcard Reader

- HID Global OMNIKEY 6121 Smart Card Reader
- HID Global veriCLASS Reader
- HID OMNIKEY 5025-CL
- HID OMNIKEY 5127 CK
- HID OMNIKEY 5326 DFR
- HID OMNIKEY 5427 CK
- Hitachi, Ltd. Hitachi Biometric Reader
- Hitachi, Ltd. Hitachi Portable Biometric Reader
- id3 Semiconductors CL1356A_HID
- id3 Semiconductors CL1356T
- Identiv @MAXX ID-1 Smart Card Reader
- Identiv @MAXX Light2 token
- Identiv CLOUD 2980 F Smart Card Reader
- Identiv SCR3500 A Contact Reader
- Identiv SCR3500 B Contact Reader
- Identiv SCR35xx USB Smart Card Reader
- Identiv uTrust 2900 R Smart Card Reader
- Identiv uTrust 2910 R Smart Card Reader
- Identiv uTrust 2910 R Taglio SC Reader
- Identiv uTrust 3512 SAM slot Token
- Identiv uTrust 3522 embd SE RFID Token
- Identiv uTrust 3700 F CL Reader
- Identiv uTrust 3701 F CL Reader
- Identiv uTrust 4701 F Dual Interface Reader
- Identive CLOUD 2700 F Smart Card Reader
- Identive CLOUD 2700 R Smart Card Reader
- Identive CLOUD 4000 F DTC
- Identive CLOUD 4500 F Dual Interface Reader
- Identive CLOUD 4510 F Contactless + SAM Reader
- Identive SCT3522CC token
- Identive Technologies Multi-ISO HF Reader - USB
- IID AT90S064 CCID READER
- IIT E.Key Almaz-1C
- IIT E.Key Crystal-1
- InfoThink IT-102MU Reader
- INGENICO Leo
- Ingenico WITEO USB Smart Card Reader
- Inside Secure AT90SCR050
- Inside Secure AT90SCR100
- Inside Secure AT90SCR200
- INSIDE Secure VaultIC 405 Smart Object
- Inside Secure VaultIC 420 Smart Object
- Inside Secure VaultIC 440 Smart Object
- INSIDE Secure VaultIC 441 Smart Object
- Inside Secure VaultIC 460 Smart Object
- IonIDe Smartcard Reader
- KACST HSID Reader
- KACST HSID Reader Dual Storage
- KACST HSID Reader Single Storage
- Kapsch TrafficCom USB SAM reader
- KEBTechnology KONA USB SmartCard
- Kingtrust Multi-Reader
- KOBIL EMV CAP - SecOVID Reader III
- KOBIL KAAAN Advanced
- KOBIL KAAAN Base
- KOBIL KAAAN SIM III

- KOBIL Systems IDToken
- KOBIL Systems mIDentity 4smart
- KOBIL Systems mIDentity 4smart AES
- KOBIL Systems mIDentity fullsize
- KOBIL Systems mIDentity fullsize AES
- KOBIL Systems mIDentity M
- KOBIL Systems mIDentity visual
- KOBIL Systems mIDentity XL
- KOBIL Systems Smart Token
- KRONEGGER Micro Core Platform
- KRONEGGER NFC blue Reader Platform
- Ledger Nano S
- Lenovo Integrated Smart Card Reader
- Lenovo USB Smartcard Keyboard
- Liteon HP SC Keyboard - Apollo (Liteon)
- Liteon HP SC Keyboard - Apollo JP (Liteon)
- Liteon HP SC Keyboard - Apollo KR (Liteon)
- Macally NFC CCID eNetPad
- mCore SCard-Reader
- Microchip SEC1110
- Microchip SEC1210
- MK Technology KeyPass S1
- Morpho MSO1350 Fingerprint Sensor & SmartCard Reader
- Morpho MSO350/MSO351 Fingerprint Sensor & SmartCard Reader
- MSI StarReader SMART
- MYSMART MySMART PAD V2.0
- Neowave Weneo
- Nitrokey Nitrokey HSM
- Nitrokey Nitrokey Pro
- Nitrokey Nitrokey Start
- Nitrokey Nitrokey Storage
- NTT Communications Corp. SCR3310-NTTCom USB SmartCard Reader
- NXP Pegoda 2 N
- NXP PR533
- O2 Micro Oz776
- OBERTHUR TECHNOLOGIES ID-ONE TOKEN SLIM v2
- OCS ID-One Cosmo Card USB Smart Chip Device
- OMNIKEY 5421
- OMNIKEY 6321 CLi USB
- OMNIKEY AG 3121 USB
- OMNIKEY AG 6121 USB mobile
- OMNIKEY AG CardMan 3121
- OMNIKEY AG CardMan 3621
- OMNIKEY AG CardMan 3821
- OMNIKEY AG CardMan 5121
- OMNIKEY AG CardMan 5125
- OMNIKEY AG CardMan 6121
- OMNIKEY AG Smart Card Reader
- OMNIKEY CardMan 1021
- OMNIKEY CardMan 4321
- OMNIKEY CardMan 5321
- Panasonic Panasonic USB Smart Card Reader 7A-Smart
- Philips Semiconductors JCOP41V221
- Philips Semiconductors SmartMX Sample
- PIVKey T800
- Planeta RC700-NFC CCID

- Precise Biometrics Precise 200 MC
- Precise Biometrics Precise 250 MC
- Precise Biometrics Sense MC
- Raritan D2CIM-DVUSB VM/CCID
- Regula RFID Reader
- REINER SCT cyberJack go
- REINER SCT cyberJack one
- REINER SCT cyberJack RFID basis
- REINER SCT cyberJack RFID standard
- REINER SCT tanJack Bluetooth
- Rocketek RT-SCR1
- RSA RSA SecurID (R) Authenticator
- SafeNet eToken 5100
- SafeNet eToken 5300
- SafeNet eToken 7300
- SafeTech SafeTouch
- SAFETRUST SABRE SCR
- SchlumbergerSema SchlumbergerSema Cyberflex Access
- SCM Microsystems Inc. HP USB Smartcard Reader
- SCM Microsystems Inc. SCL010 Contactless Reader
- SCM Microsystems Inc. SCL01x Contactless Reader
- SCM Microsystems Inc. SCR 331
- SCM Microsystems Inc. SCR 3310
- SCM Microsystems Inc. SCR 3311
- SCM Microsystems Inc. SCR 331-DI
- SCM Microsystems Inc. SCR 335
- SCM Microsystems Inc. SCR 355
- SCM Microsystems Inc. SCR3310 USB Smart Card Reader
- SCM Microsystems Inc. SCR331-DI USB Smart Card Reader
- SCM Microsystems Inc. SCR3320 - Smart Card Reader
- SCM Microsystems Inc. SCR3340 - ExpressCard54 Smart Card Reader
- SCM Microsystems Inc. SCR33x USB Smart Card Reader
- SCM Microsystems Inc. SDI010 Smart Card Reader
- SCM Microsystems Inc. SDI011 Contactless Reader
- SCM Microsystems Inc. SPR 532
- Secure Device Solutions DOMINO-Key TWIN
- SecuTech SecuTech Token
- Sitecom Sitecom USB simcard reader MD-010
- Softforum Co., Ltd XecureHSM
- SpringCard CrazyWriter
- SpringCard CSB6 Basic
- SpringCard CSB6 Secure
- SpringCard CSB6 Ultimate
- SpringCard EasyFinger Standard
- SpringCard EasyFinger Ultimate
- SpringCard H512 Series
- SpringCard H663 Series
- SpringCard NFC'Roll
- SpringCard Prox'N'Roll
- Spyrus Inc PocketVault P-3X
- SYNRIX STD200
- Teridian Semiconductors TSC12xxFV.09
- THRC Smart Card Reader
- THURSBY SOFTWARE TSS-PK1
- TianYu CCID Key TianYu CCID SmartKey
- Tianyu Smart Card Reader

- Todos Argos Mini II
- Todos CX00
- ubisys 13.56MHz RFID (CCID)
- udea MILKO V1.
- Unicept GmbH AirID USB
- Unicept GmbH AirID USB Dongle
- Validy TokenA sl vt
- VASCO DIGIPASS 870
- VASCO DIGIPASS 875
- VASCO DIGIPASS 920
- VASCO DIGIPASS KEY 101
- VASCO DIGIPASS KEY 200
- VASCO DIGIPASS KEY 202
- VASCO DIGIPASS KEY 860
- VASCO DP855
- VASCO DP865
- VASCO DP905v1.1
- Verisign Secure Storage Token
- Verisign Secure Token
- VMware Virtual USB CCID
- WatchCNPC USB CCID Key
- Watchdata USB Key
- Watchdata W5181
- Winbond CCID SmartCard Controller
- XIRING Leo v2
- XIRING MyLeo
- XIRING XI-SIGN USB V2
- Yubico Yubikey 4 CCID
- Yubico Yubikey 4 OTP+CCID
- Yubico Yubikey 4 OTP+U2F+CCID
- Yubico Yubikey 4 U2F+CCID
- Yubico Yubikey NEO CCID
- Yubico Yubikey NEO OTP+CCID
- Yubico Yubikey NEO OTP+U2F+CCID
- Yubico Yubikey NEO U2F+CCID