

RX300, RX-RDP, RX420(RDP) and LEAF OS User and Configuration Guide (Version 2.1)

NComputing Global, Inc.



WWW.NCOMPUTING.COM

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

Table of contents

1. Introduction.....	1
1.1. Purpose of this book.....	1
1.2. Intended audience.....	1
1.3. Edition history	1
1.3.1. Change log.....	1
First edition (version 1.0).....	1
Second edition (version 2.0)	1
Second edition (version 2.1)	1
1.4. Device firmware versions described in this book.....	1
2. Overview of RX-series thin client devices and LEAF OS.....	2
2.1. About NComputing.....	2
2.2. What is the RX300?	2
2.3. What is the RX-RDP?	2
2.4. What is the RX420(RDP)?	2
2.5. What is the LEAF OS?	3
2.6. What are the differences between the RX300, RX-RDP, and RX420(RDP) thin clients?.....	3
2.7. What is in the product box?	4
2.8. RX300 and RX-RDP mechanical elements and cable connections	5
2.9. RX420(RDP) mechanical elements and cable connections	5
2.10. Available device operation modes	5
2.10.1. vSpace Client operation mode	6
2.10.2. VERDE VDI Client operation mode	6
2.10.3. RDP Client operation mode.....	6
2.10.4. Raspbian Desktop operation mode.....	6
3. Using the RX-series thin client and repurposed PCs with LEAF OS	7
3.1. Common elements of graphical user interface	7
3.2. Main screen GUI in vSpace Client operation mode.....	8
3.2.1. Connecting to automatically detected vSpace server.....	9
3.2.2. Connecting to vSpace server group.....	9
3.2.3. Connecting to vSpace server belonging to vSpace server group	10
3.2.4. Connecting to manually specified vSpace server	11
3.3. Main screen GUI in VERDE Client operation mode	12
3.3.1. Connecting to VERDE VDI desktop	13
3.4. Main screen GUI in RDP Client operation mode	14
3.4.1. Connecting directly to a Remote Desktop Session Host	15
3.4.2. Connecting to a RemoteApp program or desktop	16

3.5. Device GUI in Raspbian Desktop operation mode	18
3.6. Main screen GUI when a VPN connection is enabled	18
3.6.1. Using OpenVPN with configuration file provided by the user	19
3.7. Opening the Setup GUI.....	21
4. Setup GUI.....	22
4.1. General settings.....	23
4.1.1. Selecting the device operation mode	24
4.1.2. Configuring Device Name	24
4.1.3. Configuring device Asset Tag.....	25
4.1.4. Protecting the Setup GUI against unauthorized access	25
4.2. Connections settings in vSpace Client mode.....	25
4.3. Connections settings in VERDE VDI Client mode.....	26
4.4. Connections settings in RDP Client mode	27
4.4.1. Configuring direct connections to RD Session Hosts.....	27
4.4.2. Configuring connections to RD Session Hosts located behind RD Gateway	29
4.4.3. Configuring connections to RemoteApp programs or desktops	31
4.5. Server Groups	33
Adding a vSpace Pro server to Server Group	34
4.6. Kiosk Mode settings	34
4.6.1. Configuring user auto-logon settings	34
4.6.2. Pre-configuring the Domain name for VERDE VDI and RDP connections	35
4.6.3. Configuring legacy application auto-start	36
4.6.4. Configuring RemoteApp program or desktop auto-start.....	37
4.7. Display settings.....	37
4.7.1. RX300 and RX-RDP display settings.....	37
Configuring screen resolution	38
Configuring primary screen position.....	38
Secondary display adapters limitations	39
4.7.2. RX420(RDP) display settings.....	39
Configuring screen resolutions	39
Configuring secondary display position	40
Enabling screen mirroring	40
Configuring screen rotations.....	40
4.7.3. LEAF OS display settings	41
4.7.4. Resetting the display settings to factory defaults.....	41
4.7.5. Configuring the screen saver.....	42
4.7.6. Configuring desktop wallpaper	42
4.8. Peripherals settings	43
4.8.1. Native redirection of peripheral devices.....	44

4.8.2. Generic USB redirection of peripheral devices	44
4.8.3. Customizing peripheral devices redirection.....	45
4.8.4. Native redirection of mass storage devices	46
4.8.5. Generic USB redirection of mass storage devices.....	46
4.8.6. Native redirection of audio devices	47
4.8.7. Generic USB redirection of audio devices	48
4.8.8. Native redirection of printers.....	48
Adding a USB printer for native redirection.....	50
Adding a network printer for native redirection.....	52
Removing printer from native redirection	54
4.8.9. Generic USB redirection of printers	54
Additional considerations for UXP sessions	56
Additional considerations for RDP sessions	61
4.8.10. Generic USB redirection of imaging devices	61
4.8.11. Native redirection of smart card readers	62
Enabling native redirection of smart card readers for UXP sessions	62
Enabling native redirection of smart card readers for RDP sessions	63
4.8.12. Generic USB redirection of smart card readers	63
4.8.13. Native redirection of serial ports	63
4.8.14. Generic USB redirection of serial ports	64
Optimizing the Generic USB redirection of serial ports in vSpace Pro systems.....	65
4.8.15. Generic USB redirection of human interface devices	66
4.8.16. Native redirection of touchscreen displays.....	66
4.8.17. Native redirection of HID DigitalPersona fingerprint readers.....	66
4.8.18. Generic USB redirection of custom devices identified by VID and PID.....	67
Removing USB devices from Custom VID:PID list	68
4.9. Audio settings	68
4.10. Keyboard settings.....	69
4.11. Network settings	70
4.11.1. Configuring the Ethernet interface	70
4.11.2. Configuring enterprise (802.1x) Ethernet settings.....	71
4.11.3. Configuring the Wi-Fi interface	71
4.11.4. Configuring DNS settings.....	72
4.11.5. Configuring Internet Proxy settings.....	72
4.11.6. Configuring VPN connections.....	72
Configuring OpenVPN connection with configuration file provided by the user.....	73
Configuring OpenVPN connection with all settings stored on the device	74
Configuring OpenConnect VPN connection	75
Configuring PPTP VPN connection	77

4.12. Management settings.....	78
4.12.1. Configuring remote device management settings	79
Enabling vSpace Console management	79
Enabling PMC management.....	79
4.12.2. Configuring VNC screen shadowing	80
VNC screen shadowing limitations on RX300 and RX-RDP devices.....	80
4.13. Security settings	82
4.13.1. Installing Certification Authority certificates	83
4.13.2. Installing Client certificates	84
4.13.3. Removing certificates	85
4.14. Support options.....	86
4.14.1. Updating firmware to the latest version available in LAN	86
4.14.2. Updating firmware from specified vSpace Server.....	86
4.14.3. Updating from FTP/HTTP URL	86
4.14.4. Updating from a USB stick.....	86
4.14.5. Collecting troubleshooting information	87
4.14.6. Resetting the device to factory defaults	87
4.15. Date and Time settings.....	87
4.16. Device status information (About)	88
5. Device recovery mode.....	89
5.1. Recovering the thin client partition	89
5.2. Recovering the Raspbian partition.....	89
5.2.1. Resetting the device to factory defaults	89

1. Introduction

1.1. Purpose of this book

The purpose of this book is to provide comprehensive information about the setup and configuration of NComputing RX300, RX-RDP, RX420(RDP) thin client devices (sometimes referred to as RX-series thin clients) and repurposed PCs running NComputing LEAF OS.

1.2. Intended audience

NComputing vSpace Pro administrators, NComputing RX-series thin client and LEAF OS administrators, systems engineers, technical support engineers, help desk personnel.

1.3. Edition history

Book edition	Release date
Version 1.0	July 15, 2019
Version 2.0	April 6, 2020
Version 2.1	May 11, 2020

1.3.1. Change log

First edition (version 1.0)

This was the first edition of this book.

Second edition (version 2.0)

- Updated to cover RX300 3.7.0 and RX-RDP 2.9.1 firmware functionality.
- Added information for the lately released RX420(RDP) devices.
- Added information for the lately released LEAF OS.
- Added the sections missing in the first edition.

Second edition (version 2.1)

- Added sections regarding VPN configuration.
- Added information about redirection of HID DigitalPersona fingerprint readers.

1.4. Device firmware versions described in this book

Information contained in this book corresponds with following RX-series device firmware and LEAF OS versions:

Product	Firmware version
RX300	3.8.1
RX-RDP	2.11.0
RX420(RDP)	1.5.1
LEAF OS	2.1.2

2. Overview of RX-series thin client devices and LEAF OS

2.1. About NComputing

NComputing is a desktop virtualization company with more than 70,000 customers and 20 million daily users in 140 countries. NComputing serves customers large and small, in diverse markets and with varying use cases across education, government, healthcare, among other industry sectors.

With innovative and award-winning technologies, NComputing brings customers an impressively quick ROI with economical, high-performance desktop virtualization solutions.

2.2. What is the RX300?

RX300 is a cloud-ready, Wi-Fi enabled thin client for Windows and Linux, built on the latest Raspberry Pi 3 platform and optimized for vSpace Pro, VERDE VDI, and Microsoft RDS.

Easy deployment and central management of the virtual desktop environment make the RX300 ideal in SMBs and education. The compact RX300 device offers the lowest acquisition cost of NComputing's product families.

RX300 features full-screen, full-motion HD multimedia playback with built-in transparent USB redirection achieving unparalleled peripheral support, and optional access to Linux Raspbian OS managed by the IT admin. Dual Monitor Support allows an added screen for increased productivity (requires additional hardware module).

As an additional option RX300 allows the users to work in Raspbian Linux desktop environment.

2.3. What is the RX-RDP?

The RX-RDP is a cloud-ready, Wi-Fi enabled thin client designed and optimized specifically for Microsoft Remote Desktop Services and NComputing VERDE VDI platform. Powered by Raspberry Pi 3, the RX-RDP provides a rich PC-like experience in an affordable, energy-saving device with a small footprint.

For organizations using Microsoft Windows Server or VDI infrastructure, the RX-RDP provides a simple-to-deploy, centrally-managed, high-performing virtual desktop.

RX-RDP features full-screen, full-motion HD multimedia playback with support for Microsoft RemoteFX and NComputing vCAST Streaming, Wi-Fi connectivity and built-in transparent USB redirection achieving unparalleled peripheral support.

2.4. What is the RX420(RDP)?

The RX420(RDP) is a cloud-ready thin client designed and optimized specifically for Microsoft Remote Desktop Services and our VERDE VDI platform. Powered by the latest Raspberry Pi 4 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.

For organizations using Microsoft Windows Server or VDI infrastructure, the RX420(RDP) provides a simple-to-deploy, centrally-managed, high-performing virtual desktop. RX420(RDP) features native dual display, full-screen, full-motion HD multimedia playback with support for Microsoft RemoteFX and NComputing vCAST Streaming, Wi-Fi connectivity and built-in transparent USB redirection achieving unparalleled peripheral support.

2.5. What is the LEAF OS?

LEAF OS is a solution that eliminates the headaches related to traditional PC management by converting the hardware from a stand-alone personal computer to a server-driven thin client allowing access to current operating systems and applications.

LEAF OS is based on Linux software developed specifically for vSpace Pro Enterprise Edition, creating a secure computing platform that is simple to deploy and manage. With LEAF OS the customers can easily migrate from end-of-life operating systems like Windows 7 and give users powerful desktops that just work.

2.6. What are the differences between the RX300, RX-RDP, and RX420(RDP) thin clients?

RX-RDP is the ideal product to provide the perfect balance of functionality for customers with Microsoft RDS or VERDE VDI infrastructure. RX300 is our flagship product which provides the most compatibility with popular thin client connection modes, including vSpace, VERDE VDI, RDP and Raspbian Linux. RX420(RDP) is RX-RDP's successor built on the Raspberry Pi 4 platform.

RX300, RX-RDP, RX420(RDP) comparison matrix

Product feature	Description	RX300	RX-RDP	RX420(RDP)
Connection Mode	vSpace Pro	✓	N/A	N/A
	vSpace for Linux	✓	N/A	N/A
	VERDE VDI	✓ (UXP and RDP protocol)	✓ (UXP and RDP protocol)	✓ (UXP and RDP protocol)
	Microsoft RDP	✓	✓	✓
	Raspbian Desktop	✓	N/A	N/A
Multimedia Optimization	NComputing vCAST Streaming (UXP protocol)	✓	N/A	N/A
	NComputing vCAST Streaming (RDP protocol)	✓ Separate SuperRDP license required	✓ Separate SuperRDP license required	✓ Separate SuperRDP license required
	Microsoft RemoteFX Support	✓	✓	✓

Product feature	Description	RX300	RX-RDP	RX420(RDP)
Device Management	vSpace Console	✓	N/A	N/A
	PMC Device Management	Optional (AMP subscription required)	Included	Included
User Session Management	vSpace Pro	vSpace Console	N/A	N/A
	vSpace for Linux	vSpace Console	N/A	N/A
	VERDE VDI	VERDE Management Console	VERDE Management Console	VERDE Management Console
	Microsoft RDP	RDS tools	RDS tools	RDS tools
Warranty & Maintenance	Hardware Warranty	1 year	1 year	1 year
	Firmware Maintenance Update	Perpetual Included	1-year included RX-RDP AMP license can be purchased for subsequent software updates	1-year included RX420(RDP) AMP license can be purchased for subsequent software updates

2.7. What is in the product box?



The RX300, RX-RDP and RX420(RDP) product boxes contain the thin client device, a power supply, and a quick start guide.

2.8. RX300 and RX-RDP mechanical elements and cable connections



1. Power in (5.1V micro USB)
2. HDMI video output
3. Audio output
4. Ethernet port
5. 4 USB 2.0 ports for peripheral devices
6. Kensington security lock
7. Sleep/power button

2.9. RX420(RDP) mechanical elements and cable connections



1. Power button with sleep mode for additional power savings
2. 2 USB 3.0 and 2 USB 2.0 ports with full USB redirection support
3. Gigabit Ethernet port
4. Kensington security port
5. Power in (USB-C)
6. Dual micro HDMI video output
7. Audio output

2.10. Available device operation modes

RX300 thin client devices can operate in following modes:

- vSpace Client

- VERDE VDI Client
- RDP Client
- Raspbian Desktop

RX-RDP and RX420(RDP) thin client devices can operate in following modes:

- VERDE VDI Client
- RDP Client

Repurposed PCs running LEAF OS can operate in vSpace Client mode only.

2.10.1. vSpace Client operation mode

The vSpace Client mode allows the RX300 devices to run virtual desktop sessions on vSpace Pro 11.3 LTS and vSpace Pro Enterprise 12 (or newer) systems.

In repurposed PCs running LEAF OS the vSpace Client mode allows connecting to virtual desktop sessions on vSpace Pro Enterprise 12 (or newer) systems.

2.10.2. VERDE VDI Client operation mode

The VERDE VDI Client mode allows the RX300, RX-RDP and RX420(RDP) devices to run virtual desktop sessions on VERDE VDI 8.2.1 (or newer) servers. The NComputing UXP and Microsoft RDP protocols can be used for connecting the virtual desktop sessions.

2.10.3. RDP Client operation mode

The RDP Client mode allows the RX300, RX-RDP and RX420(RDP) devices to connect to Microsoft Remote Desktop Services deployments. Direct connections to virtual desktops hosted on Remote Desktop Session Hosts are supported, as well as connections to RemoteApp desktops and programs hosted on Remote Desktop Session Hosts and Virtualization Hosts brokered by Remote Desktop Web Access and Remote Desktop Connection Broker servers and secured by Remote Desktop Gateway servers.

2.10.4. Raspbian Desktop operation mode







The RX300 thin client devices when switched into Raspbian Desktop mode behave like standard Raspberry Pi devices running the Raspbian operating system.




3. Using the RX-series thin client and repurposed PCs with LEAF OS

After booting up the RX300, RX-RDP, RX420(RDP) and LEAF OS devices present to the user the graphical interface (the GUI) of the main screen. The contents of the main screen and the device behavior depend on the device operation mode selection as well as on some other configuration settings (especially server auto-connect and user auto-logout settings).

3.1. Common elements of graphical user interface

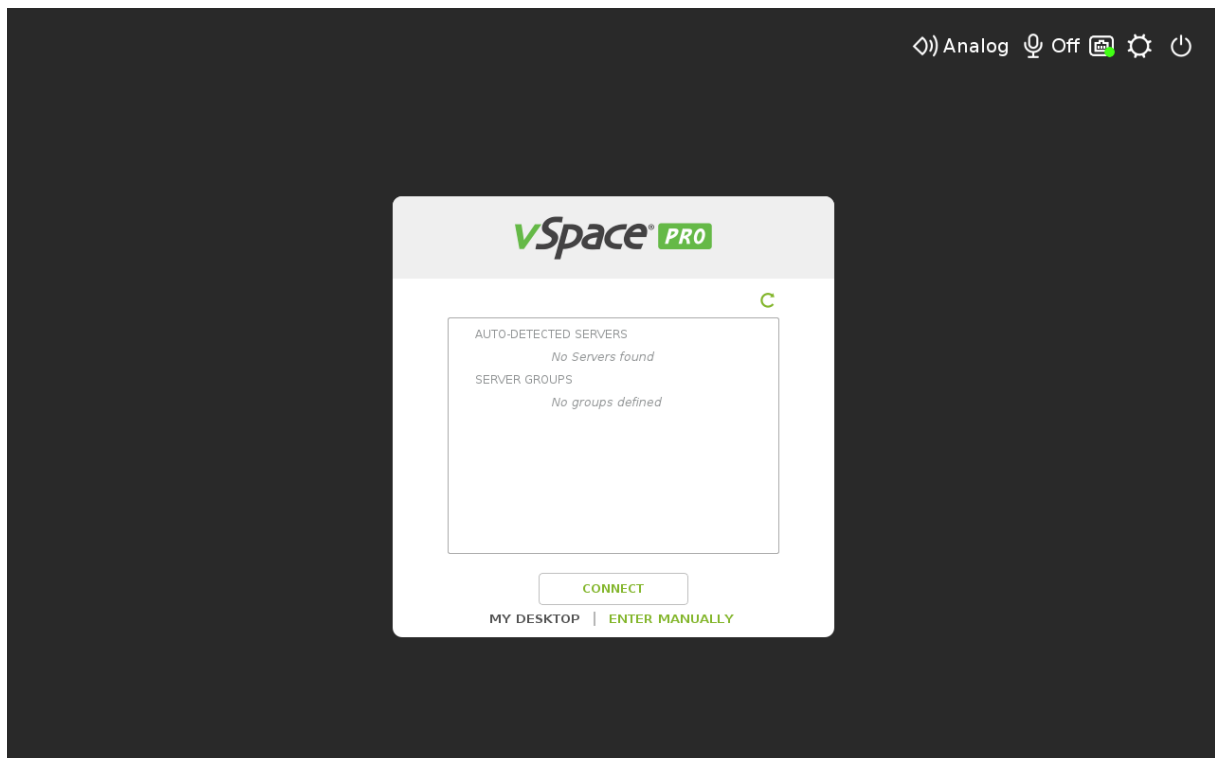
There are some elements appearing in the upper-right corner of the device screen, which do not depend on the operation mode, but are network state indicators or allow execution of some specific actions. These elements are visible when the devices show the main screen GUI, as well as when it shows the Setup GUI.

Icon	Icon meaning	Icon description and possible actions
	Audio output selection	Icon's label indicates the currently selected audio output. When clicked allows selection of audio output.
	Audio input selection	Icon's label indicates the currently selected audio input. When clicked allows selection of audio input.
	Touch screen calibration	When clicked, allows calibration of connected touch screen or interactive whiteboard (smartboard).
	Ethernet status	Hovering the mouse pointer over the icon displays current IP address of the Ethernet interface. <ul style="list-style-type: none">• Absent icon: Ethernet interface is disabled.• Icon with green dot: Successful Ethernet connection.• Icon with yellow dot: Ethernet connected, but no IP address obtained from DHCP.• Icon with red dot: Ethernet interface is enabled, but the cable is disconnected.
	Wi-Fi status	Hovering the mouse pointer over the icon displays current IP address of the Wi-Fi interface, the Wi-Fi network name (SSID) and signal strength. <ul style="list-style-type: none">• Absent icon: Wi-Fi interface is disabled.• Icon with green dot: Successful Wi-Fi connection.• Icon with yellow dot: Connected to Wi-Fi access point, but no IP address obtained from DHCP.• Icon with red dot: Wi-Fi interface is enabled, but there was a problem with Wi-Fi access point association.
	VPN status	Icon's presence indicates an active VPN connection. Hovering the mouse pointer over the icon displays current IP address of the VPN interface.

Icon	Icon meaning	Icon description and possible actions
	VPN or 802.1x Ethernet disconnect	When clicked, disconnects the VPN or 802.1x Ethernet connection.
	Setup GUI	When clicked, opens the Setup GUI.
	Power options	When clicked, allows putting the device into sleep mode, rebooting, or shutting down.

3.2. Main screen GUI in vSpace Client operation mode

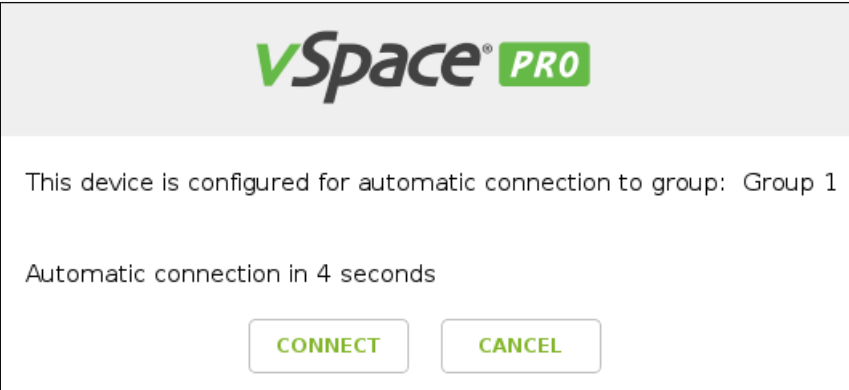
Note: This section only applies to RX300 and LEAF OS devices.



When a device operating in vSpace Client mode is using the factory default settings for the vSpace connection then the main screen GUI consists of following elements:

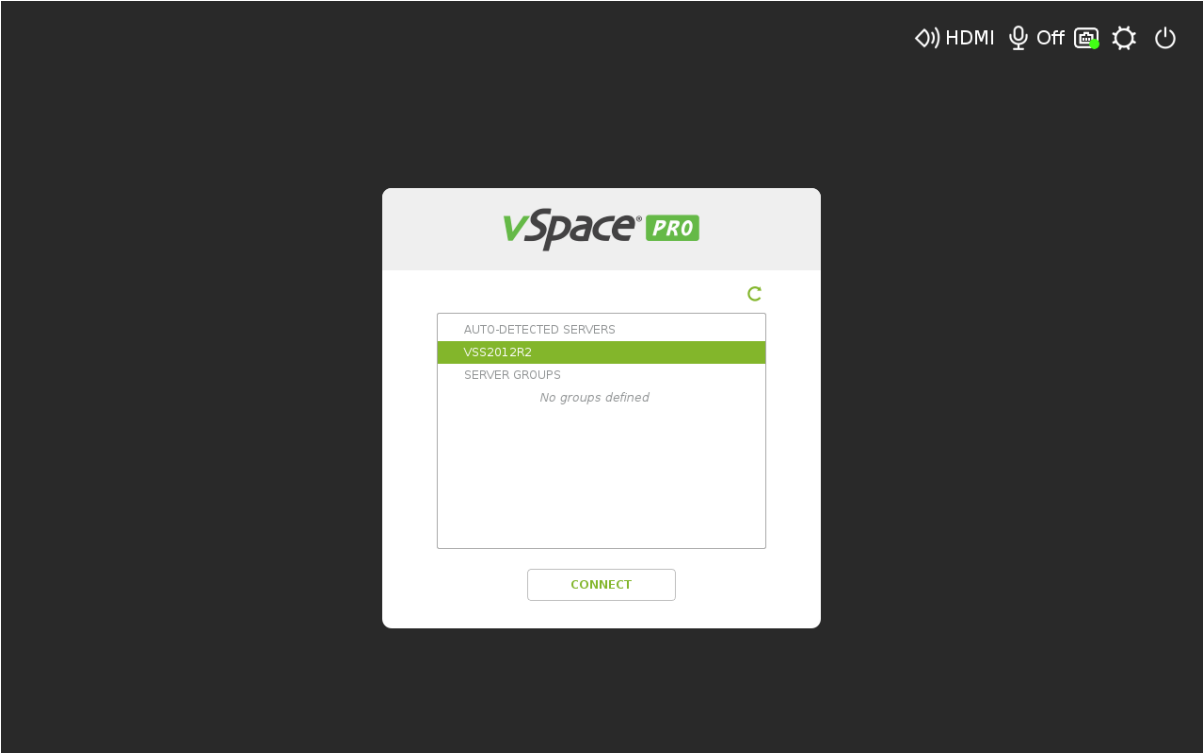
- The list of automatically detected vSpace servers and configured vSpace server groups. RX300 uses the UDP protocol to detect the vSpace servers available in local area network.
- The **C** (Refresh) icon, which allows refreshing the list of automatically detected servers.
- The **[CONNECT]** button for initiating the connection to vSpace server or vSpace server group.
- The optional **MY DESKTOP | ENTER MANUALLY** selector for switching between the list of vSpace servers or groups and an input field to manually enter (or select from the history) the address of vSpace server to connect to.

The RX300 thin client device or LEAF OS can be configured to automatically connect to a vSpace Server or to a vSpace Server Group. In such case the information about the vSpace server or group the device connects to gets displayed instead of the above described main screen:



3.2.1. Connecting to automatically detected vSpace server

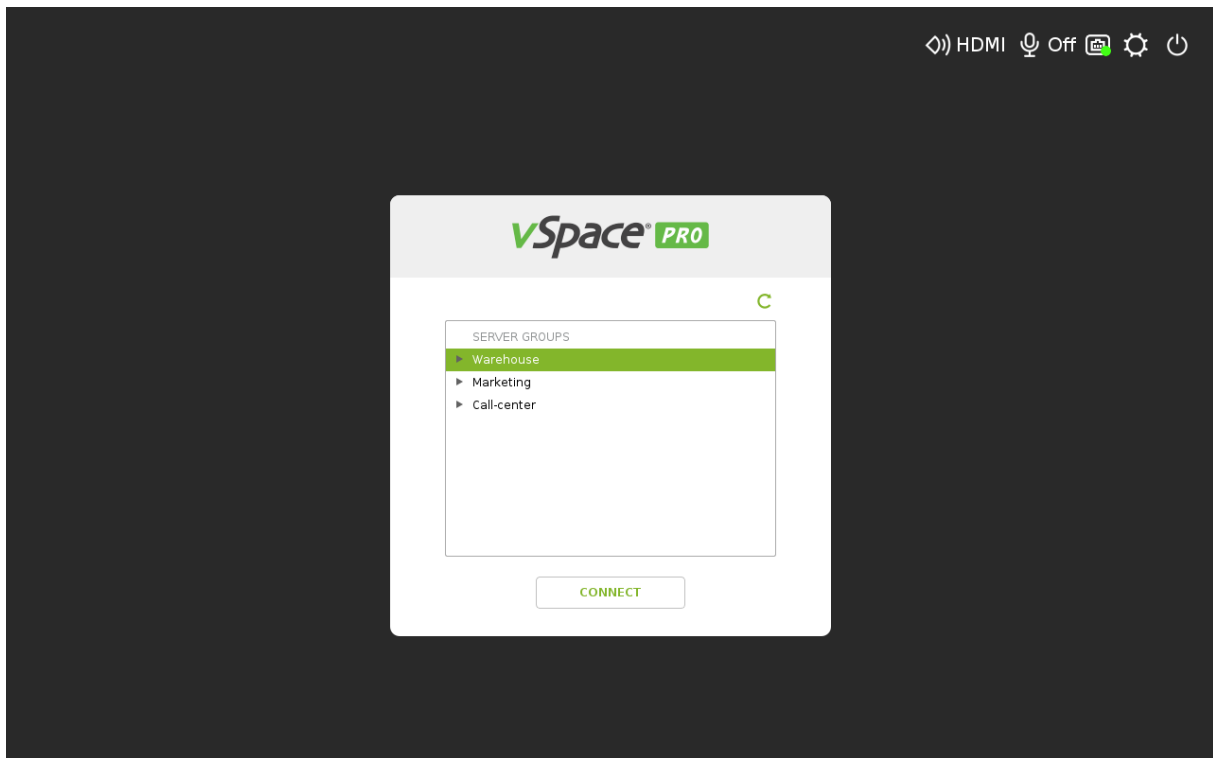
When the device is configured to display the automatically detected vSpace servers, then a server can be selected on the list. The device will try to establish a connection to the selected server after clicking the [CONNECT] button.



3.2.2. Connecting to vSpace server group

When any [vSpace Server Groups](#) are defined, then their names will be displayed on the main screen's list. One or many vSpace Pro servers can belong to each server group. Selecting a server group name and clicking the [CONNECT] button causes the device to try connecting to the first server from the group. If this connection will be unsuccessful, the device will fail over to the next server from the

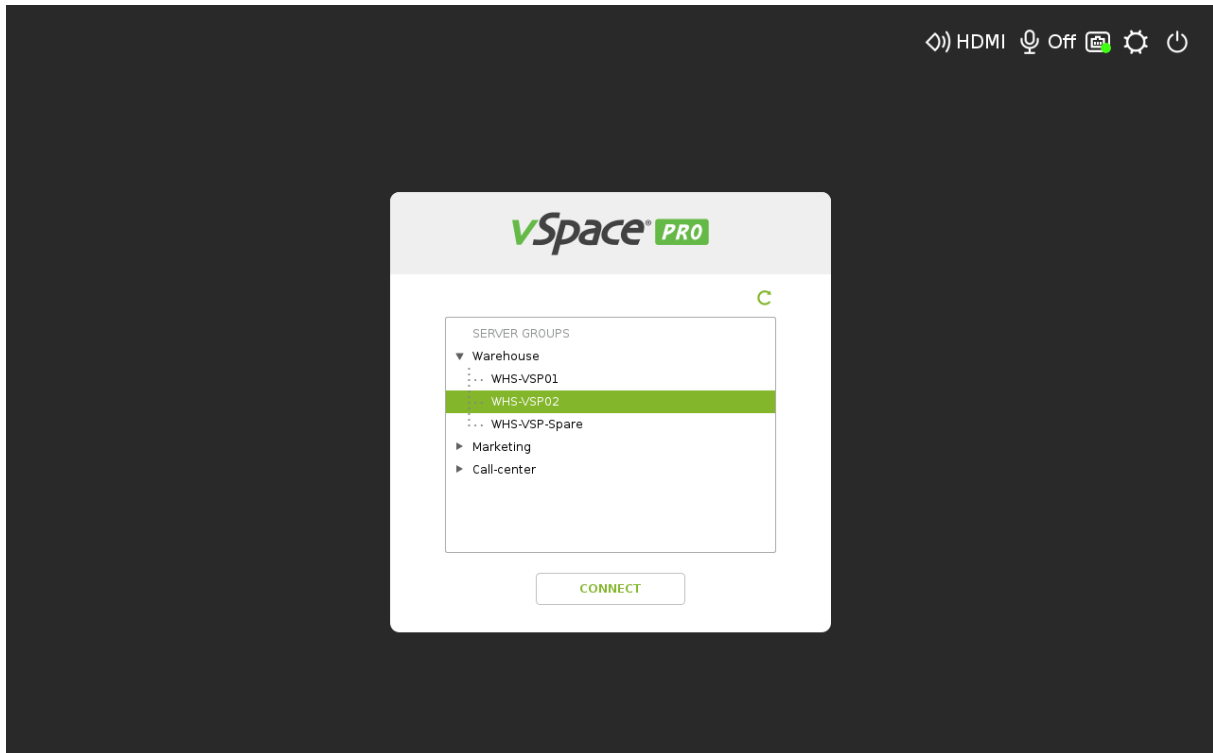
group, and so on, if this connection will be unsuccessful too. Device will repeat this sequence until a connection will be successfully established.



3.2.3. Connecting to vSpace server belonging to vSpace server group

In the case when a connection to a particular vSpace Pro server from a defined vSpace server group needs to be established, the group can be expanded by clicking the ► icon preceding the group

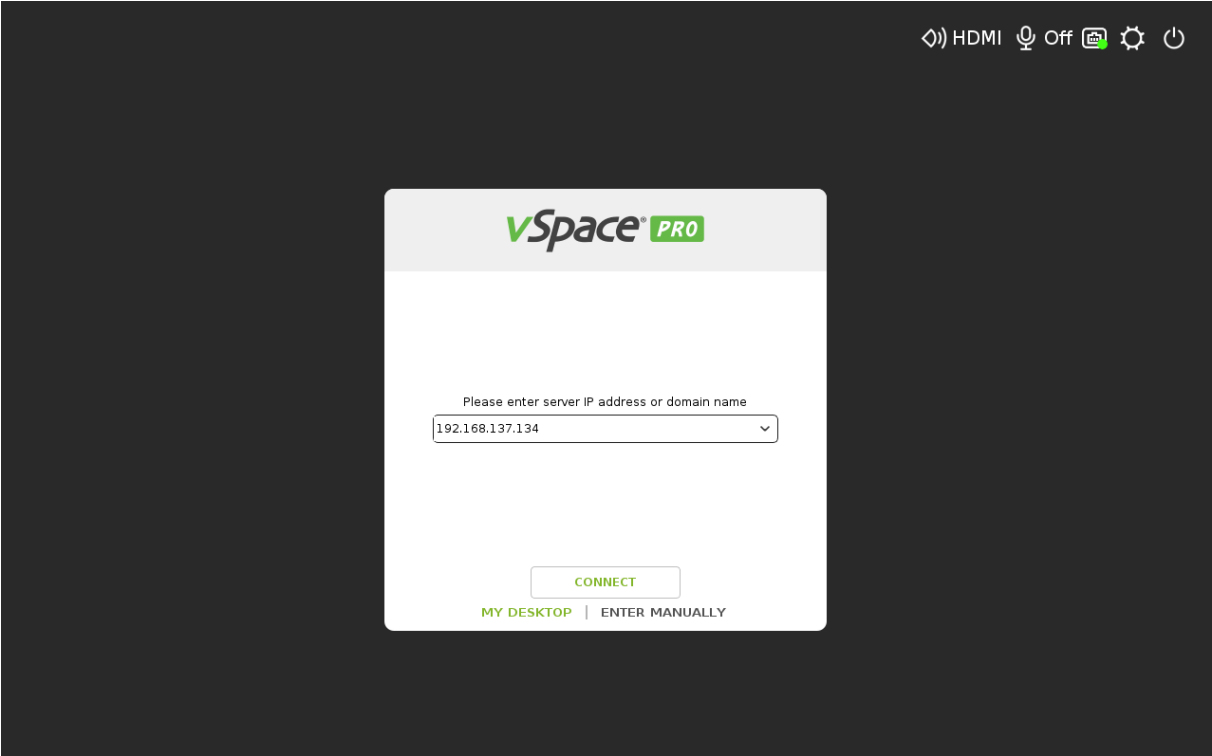
name, and the desired server can be selected. The device will try to establish a connection to the selected server after clicking the **[CONNECT]** button.



3.2.4. Connecting to manually specified vSpace server

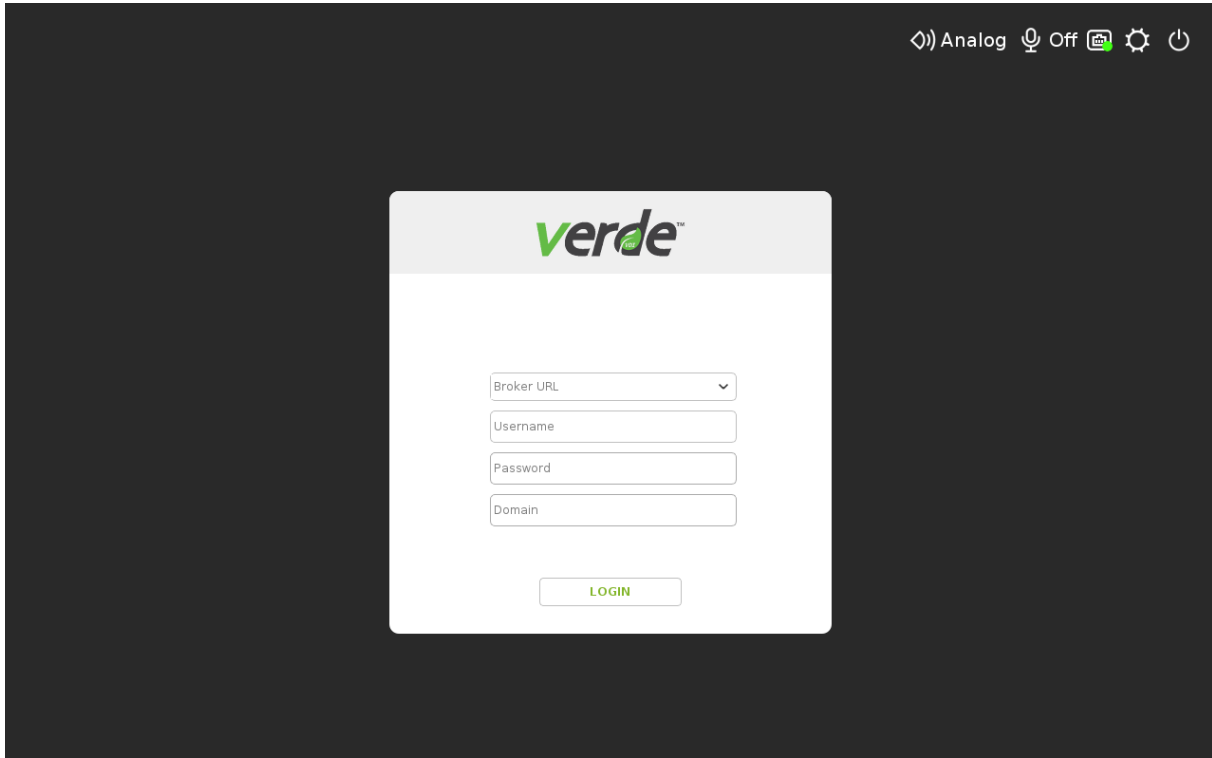
If the device is configured to allow the user to manually enter server address or name (the **Allow manual vSpace Server connections** option is active in [vSpace Client mode connection settings](#)), then the main screen displays the **MY DESKTOP | ENTER MANUALLY** selector. After clicking ENTER MANUALLY, the IP address, hostname, or full-qualified domain name of the desired vSpace Pro server

can be entered. The device will try to establish a connection to the specified server after clicking the [CONNECT] button.



After clicking MY DESKTOP, the main screen will display again the list of automatically detected vSpace Pro servers and the list of defined vSpace server groups.

3.3. Main screen GUI in VERDE Client operation mode



When an RX300, RX-RDP, or RX420(RDP) device operating in VERDE VDI Client mode is using the factory default settings for the VERDE VDI connection then the main screen GUI consists of following elements:

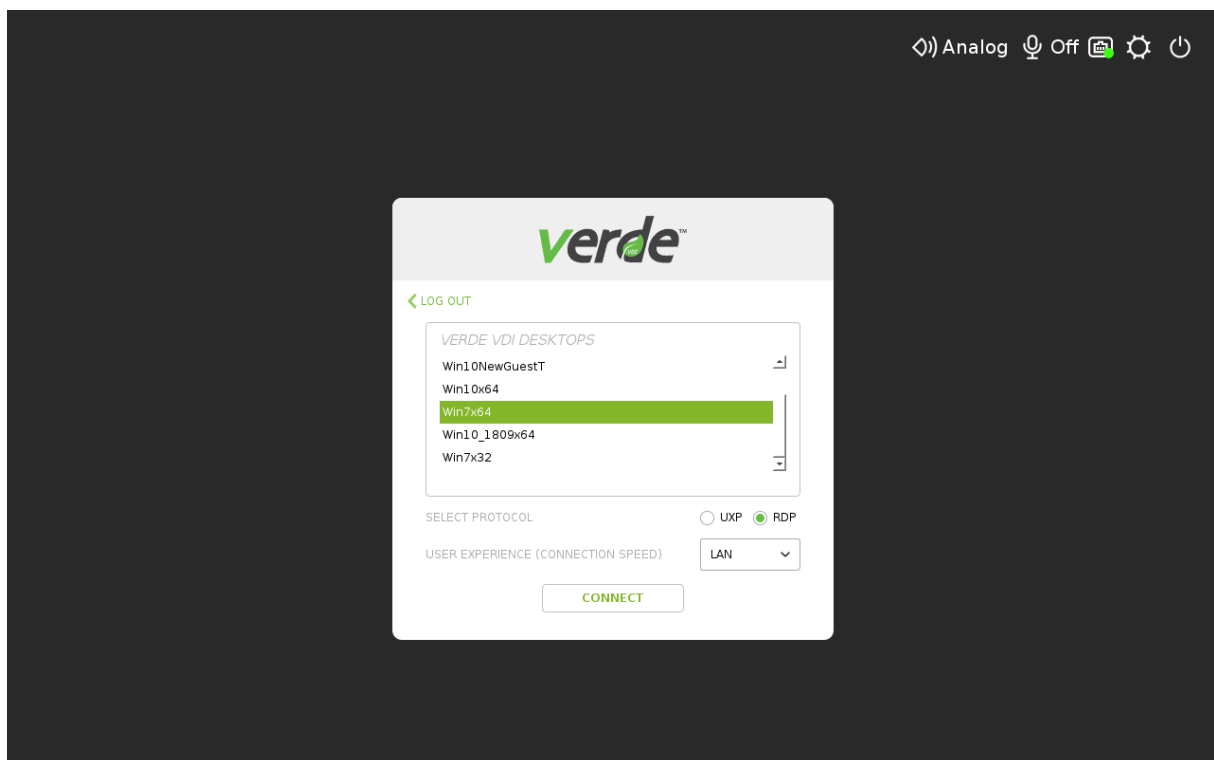
- **Broker URL** – optional input field for custom (manually specified or selected from history) VERDE VDI connection broker URL address.
- **Username, Password, Domain** – user credentials input fields (Username, Password, Domain).
- **[LOGIN]** button for initiating the user authentication process with the specified credentials.

3.3.1. Connecting to VERDE VDI desktop

After successfully authenticating the user the RX-series device operating in VERDE VDI Client mode displays the list of available VERDE desktops. Users have the option to connect using the UXP and RDP protocols. Users can also select the experience settings appropriate for the currently used connection type. The available user experience selections are:

- LAN
- Broadband
- WAN
- Modem

The device will connect to the selected VERDE VDI desktop after clicking the **[CONNECT]** button.



The VERDE VDI desktop session will be started in full-screen mode. Only one VERDE VDI desktop session can be started at the same time.

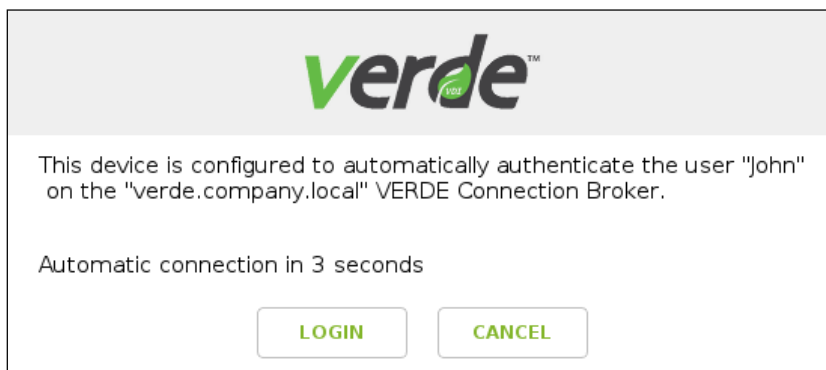
After logging off or disconnecting from the VERDE VDI desktop the device will return to the main screen GUI. The authenticated user can also click the < **LOG OUT** button to return to the main (logon) screen without connecting to any VERDE VDI desktop.

Pre-configuring the Domain name

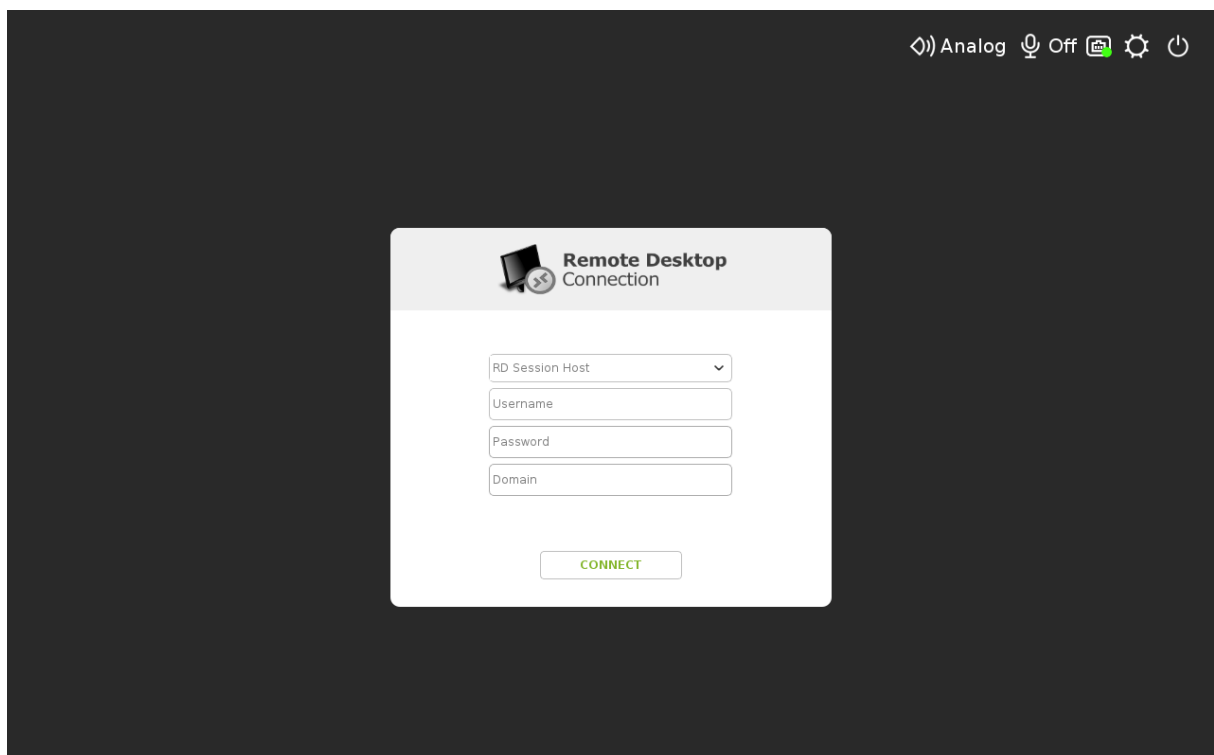
To simplify the logon process and to exempt the users from the necessity to enter the Domain name, the Domain name can be pre-configured. Please refer to the [Pre-configuring the Domain name for VERDE VDI and RDP connections](#) section for more information.

Automatic user logon

The device can be configured to automatically authenticate a predefined user on a specified VERDE VDI Connection Broker (so called Kiosk Mode configuration). In such case the information about the user account used for the automatic logon and the VERDE VDI Connection Broker address used for authentication get displayed instead of the above described main screen:



3.4. Main screen GUI in RDP Client operation mode



When an RX300, RX-RDP or RX420(RDP) device operating in RDP Client mode is using the factory default settings for the RDP connection then the main screen GUI consists of following elements:

- **RD Session Host** – optional input field for custom (manually specified or selected from history) Remote Desktop Session Host address or Remote Desktop Web Access server URL.
- **Username, Password, Domain** – user credentials input fields.
- **[CONNECT]** button for initiating the user authentication process with the specified credentials.

3.4.1. Connecting directly to a Remote Desktop Session Host

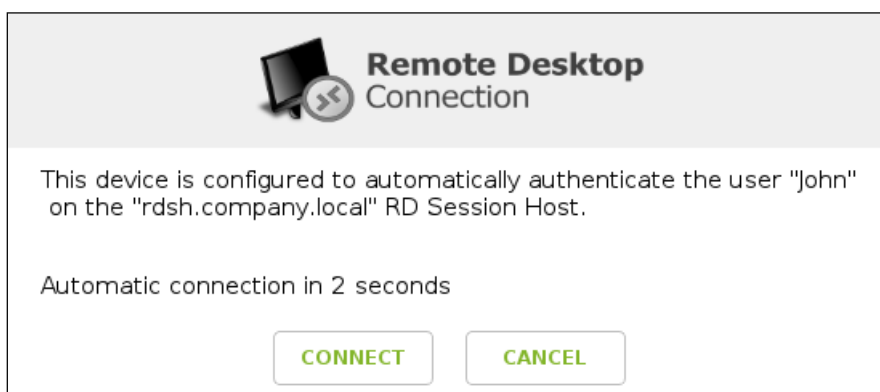
When an RX300 or RX-RDP device operates in RDP Client mode and is configured for a [direct Remote Desktop Session Host connection](#) then immediately after booting up the device shows the Remote Desktop Connection logon box on the main screen. As soon as the user enters valid credentials and clicks the **[CONNECT]** button the device attempts to authenticate the user and, in case of successful authentication, attempts to establish an RDP connection and start a full-screen remote desktop session. When the authentication fails an error message gets displayed. When the user logs off or disconnects the RDP session the device reverts to the main screen with the Remote Desktop Connection logon box.

Pre-configuring the Domain name

To simplify the logon process and to exempt the users from the necessity to enter the Domain name, the Domain name can be pre-configured. Please refer to the [Pre-configuring the Domain name for VERDE VDI and RDP connections](#) section for more information.

Automatic user logon

The device can be configured to automatically authenticate a predefined user on a specified Remote Desktop Session Host and to automatically connect to RD Session Host in case of successful authentication (so called [Kiosk Mode configuration](#)). In such case the information about the user account used for the automatic logon and the Remote Desktop Session Host address gets displayed instead of the above described main screen:



When the user logs off or disconnects the automatically started RDP session the device re-attempts to authenticate the same user using the same RD Session Host and the process repeats.

Refer to [Configuring user auto-logon settings](#) paragraph in Kiosk Mode section for the information about automatic user logon configuration.

3.4.2. Connecting to a RemoteApp program or desktop

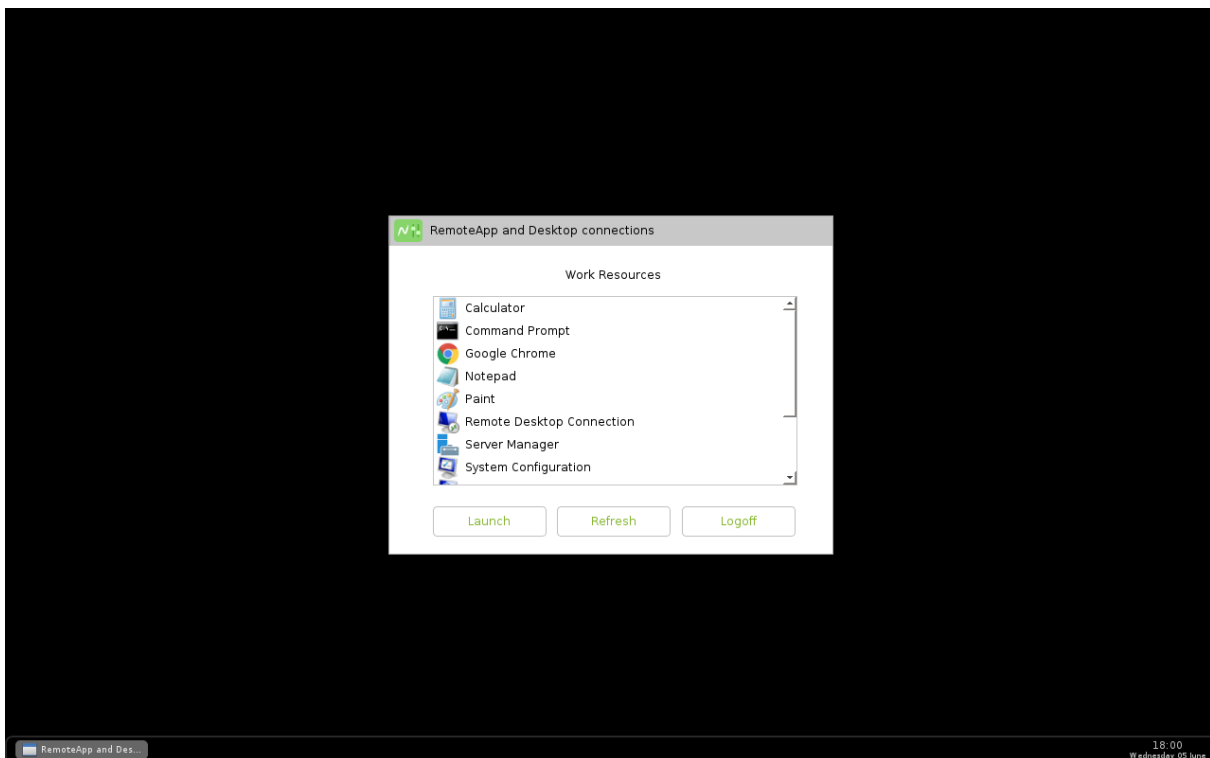
When an RX300 or RX-RDP device operates in RDP Client mode and is configured for a [RemoteApp programs or desktops connection](#) then immediately after booting up the device shows the Remote Desktop Connection logon box on the main screen. As soon as the user enters valid credentials and clicks the **[CONNECT]** button the device attempts to authenticate the user and, in case of successful authentication, enumerates the RemoteApp resources (programs and desktop) which have been published for the authenticated user. When the authentication fails an error message gets displayed.

Pre-configuring the Domain name

To simplify the logon process and to exempt the users from the necessity to enter the Domain name, the Domain name can be pre-configured. Please refer to the [Pre-configuring the Domain name for VERDE VDI and RDP connections](#) section for more information.

Working with RemoteApp programs and desktops

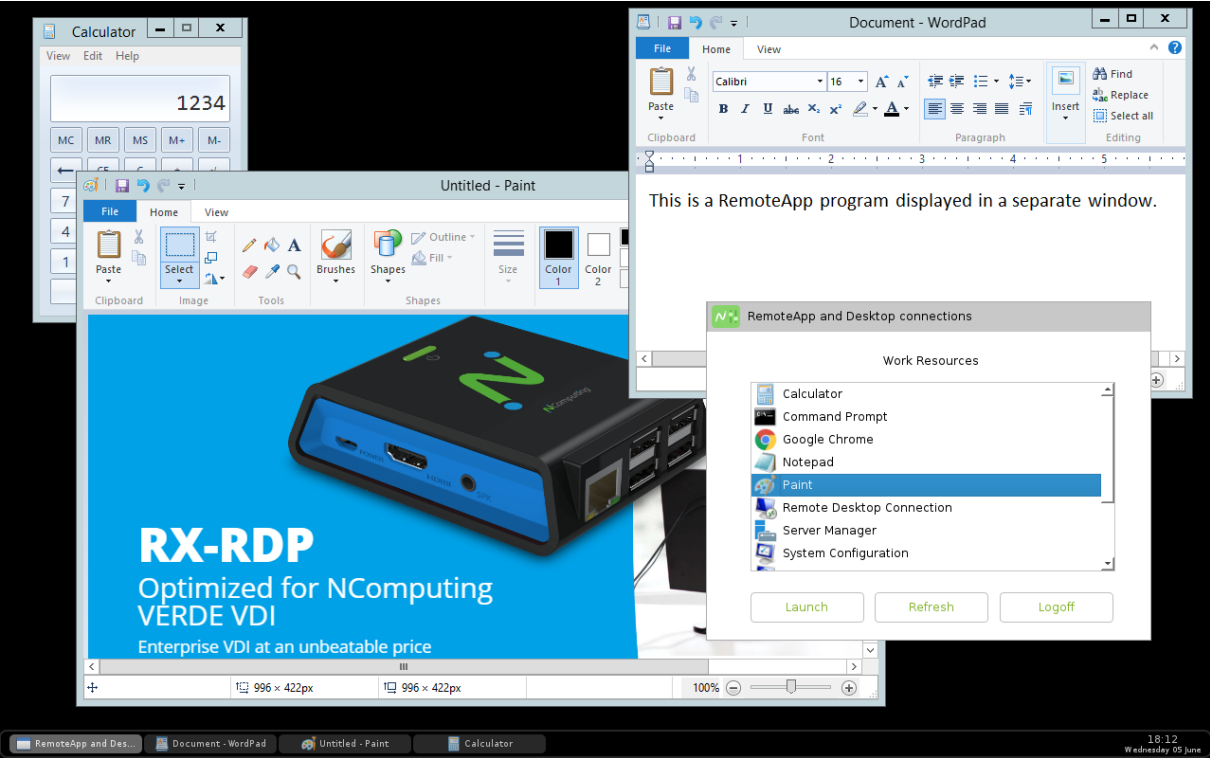
The enumerated RemoteApp programs and desktops are listed for the user in RemoteApp and Desktop Connections window:



The **[Launch]**, **[Refresh]**, and **[Logoff]** buttons allow the user to launch the selected program or desktop, refresh the RemoteApp list, or logoff.

Published RemoteApp desktops will always be launched in full-screen mode. The NComputing SuperRDP extension will be supported and the users can benefit from the vCAST technology included in SuperRDP (additional license fee applies).

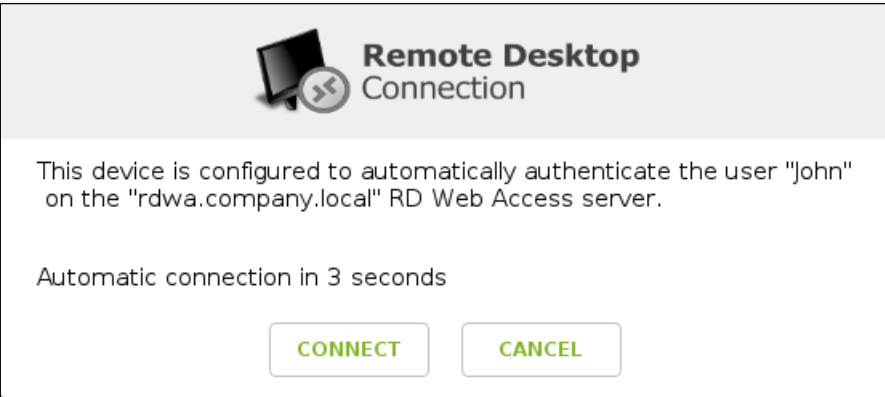
Published RemoteApp programs will be started in separate window, which the user can freely re-arrange on his or her desktop: maximize, minimize, restore, resize, move, etc. Switching between the windows of RemoteApp programs is possible by clicking the window icon on the taskbar, or with the Alt-Tab key combination.



When the user clicks the **[Logoff]** button and confirms the intention to log off the credentials will be invalidated and the possibly running RemoteApp programs will be disconnected. The programs will keep running on their RD Session Host and reconnecting them later will be possible.

Automatic user logon

The device can be configured to automatically authenticate a predefined user on a specified Remote Desktop Web Access server. In such case the information about the user account and the Remote Desktop Web Access server used for authentication gets displayed instead of the above described main screen:



List of published RemoteApp resources will be displayed after automatic user logon.

Refer to [Configuring user auto-logon settings](#) paragraph in Kiosk Mode section for the information about automatic user logon configuration.

3.5. Device GUI in Raspbian Desktop operation mode

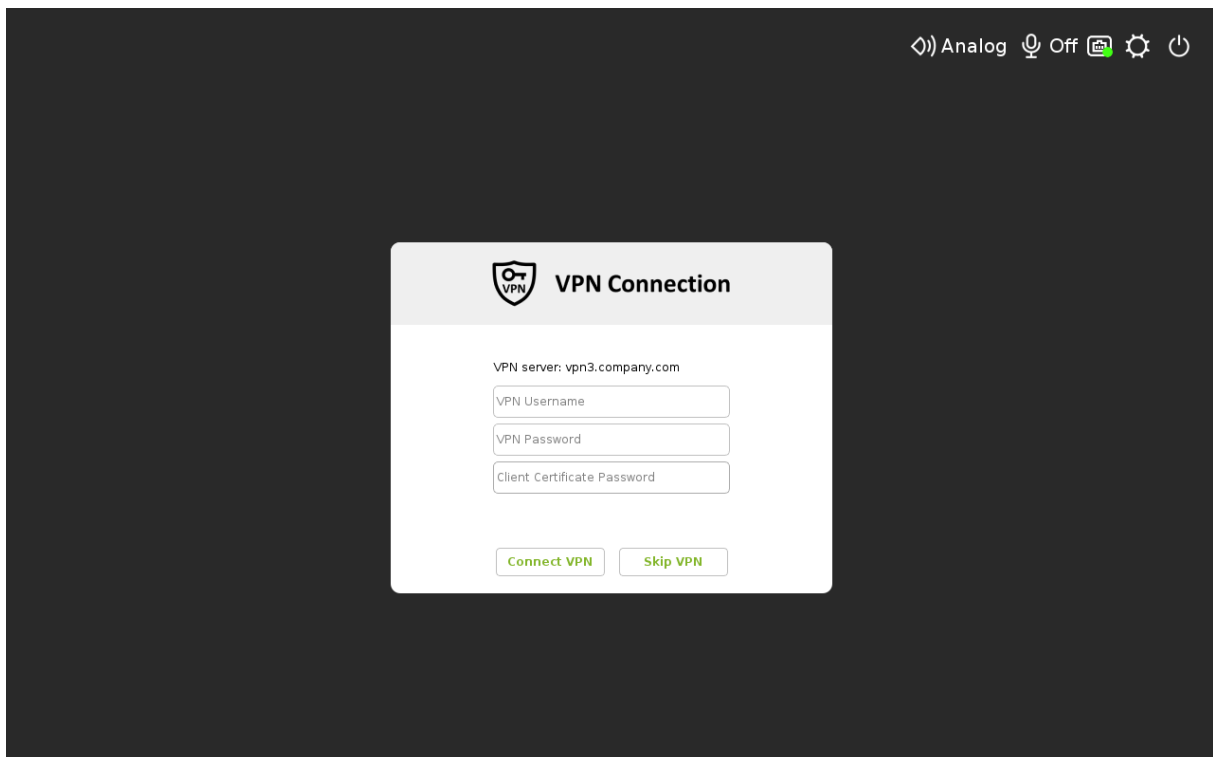
Note: This section only applies to RX300 devices.

When switched into Raspbian Desktop mode the device shows the standard Raspbian (Jessie) desktop environment.

Note: RX300 device switched into Raspbian Desktop mode can't be remotely managed from vSpace Console nor PMC device management system. Turning the device back into thin client mode is only possible by manually clicking the icon intended for this purpose and located on the Raspbian desktop.



3.6. Main screen GUI when a VPN connection is enabled

In all device operations mode described above the main screen GUI can turn into VPN logon screen, when a VPN connection is enabled and the options letting the user to provide the VPN credentials are active.



The input fields which appear on the VPN logon screen depend on the authentication type selected for the VPN connection and can be: the VPN username and the password, the client certificate password, or all the three. The **[Connect VPN]** button initiates the VPN user authentication process and, in case of successful authentication, starts the VPN connection. The **[Skip VPN]** button allows the user to skip the VPN connection and proceed to the main screen appropriate for the selected [device operation mode](#), without trying to establish the VPN connection. The device will only be able

to communicate with servers accessible through the LAN or Wi-Fi connection, if the VPN connection will be skipped.

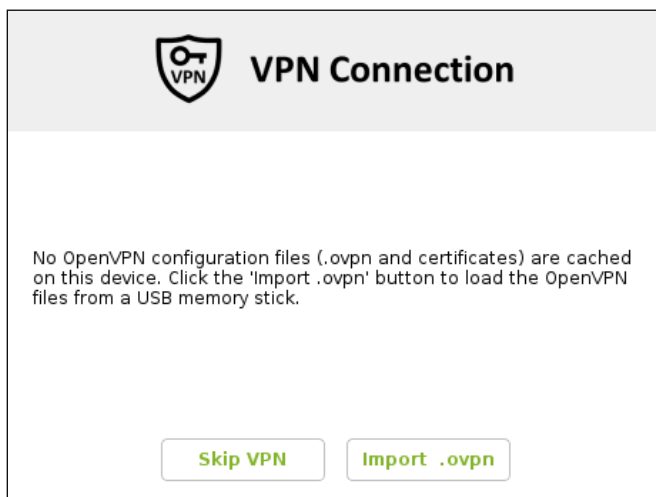
The VPN icon () at the top of the screen indicates successful VPN connection. Hovering the mouse pointer over this icon displays the current IP address of the VPN interface. The exit icon () at the top of the screen allows disconnecting the VPN connection and returning the VPN logon screen.

3.6.1. Using OpenVPN with configuration file provided by the user

The OpenVPN connection can be configured in a way [allowing the user to provide the configuration file](#) on a USB memory stick. The contents of the main screen depend on several factors then:

- on whether the configuration file and associated files are cached on the device, or not,
- on the contents of the cached configuration file (as the authentication method depends on that),
- on whether the VPN credentials are cached on the device, or not.

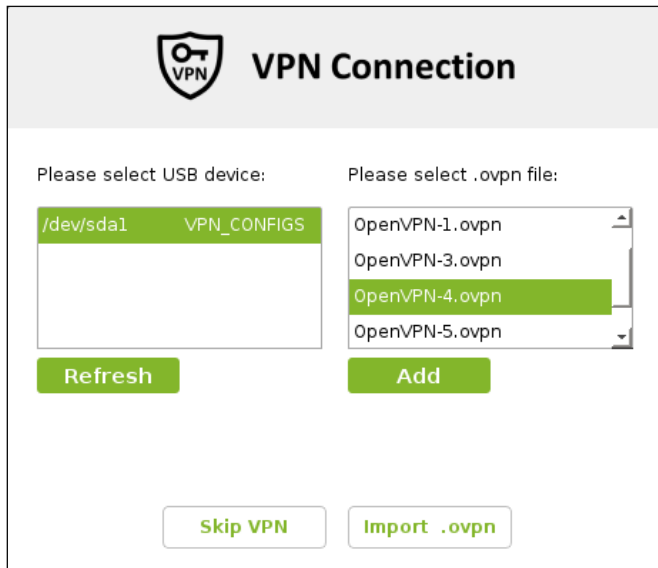
Following VPN logon screen appears on a device with OpenVPN enabled with the option letting the user to provide the configuration file, but without any files cached on the device yet:



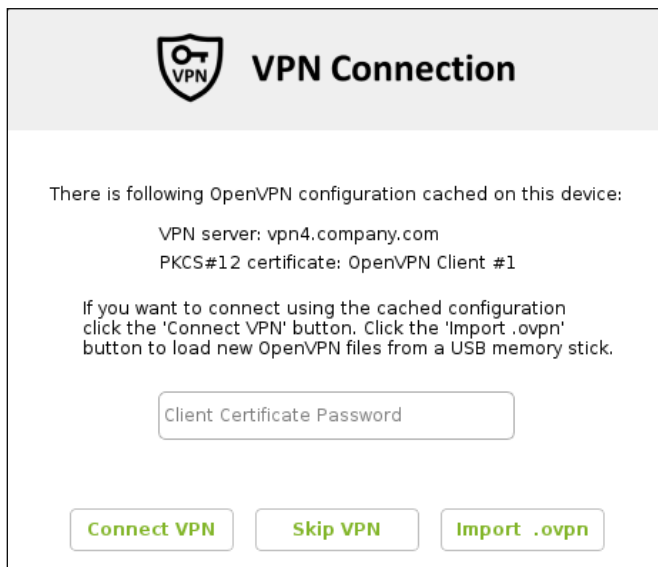
User can always click the **[Skip VPN]** button to immediately proceed to the main screen appropriate for the selected [device operation mode](#), without trying to establish the VPN connection. The device will only be able to communicate with servers accessible through the LAN or Wi-Fi connection, if the VPN connection will be skipped.

To import the OpenVPN configuration file from a USB memory stick the user should click the **[Import .ovpn]** button. The GUI will show a list of connected USB storage devices on the left-hand side.



On the right-hand side there will be the list of OpenVPN configuration files (files with .ovpn extension) found in the root directory of the USB memory stick selected on the left-hand side:




The **[Refresh]** button can be clicked to refresh the lists, if a USB memory stick was connected after clicking the **[Import .ovpn]** button. After selecting the appropriate OpenVPN configuration file, the user must click the **[Add]** button to copy the file(s) to the internal storage of the device. Depending on the contents of the imported OpenVPN configuration file, a VPN logon screen containing the OpenVPN server address and the input fields appropriate for the determined authentication mode will be displayed. If a client certificate requiring a password has been cached on the device, then an information about the certificate subject will appear too. For example:



The **[Connect VPN]** button initiates the VPN user authentication process and, in case of successful authentication, starts the VPN connection. The **[Import .ovpn]** button in this situation can be used to replace the currently cached OpenVPN configuration file with a new one.

The VPN icon () at the top of the screen indicates successful VPN connection. Hovering the mouse pointer over this icon displays the current IP address of the VPN interface. The exit icon () at the top of the screen allows disconnecting the VPN connection and returning the VPN logon screen.

3.7. Opening the Setup GUI

In each device operation mode (excluding the Raspbian Desktop mode) the Setup GUI can be opened by clicking Setup () icon.

If the device is configured to automatically connect to a vSpace server group, to automatically authenticate a user on a VERDE VDI Connection Broker, to automatically authenticate a user and connect to a Remote Desktop Session Host, or to automatically authenticate a user on a Remote Desktop Web Access server, then the connection or authentication attempt must be cancelled or time-out for the Setup icon to appear.

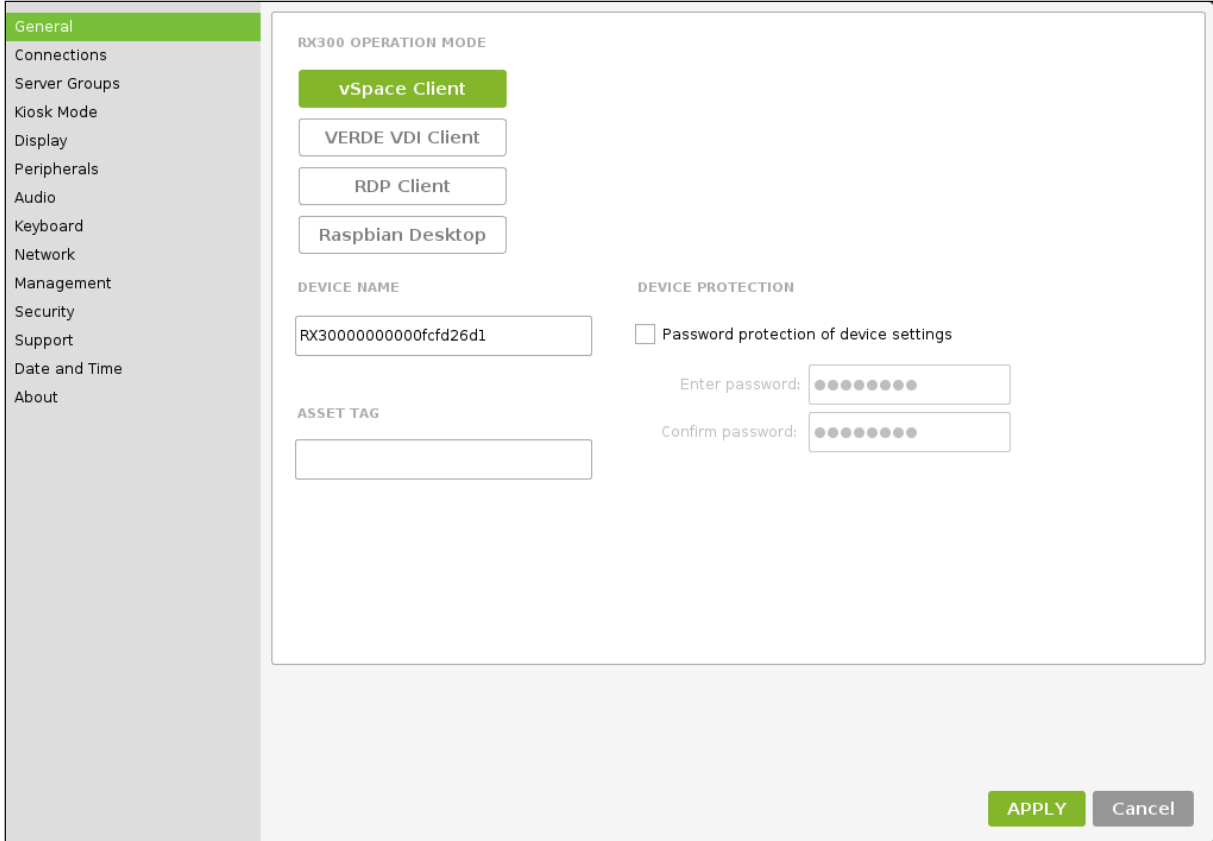
4. Setup GUI

The Setup GUI is divided into following sections:

Section	Description
General	General device settings, including selection of the device operation mode.
Connections	Operation mode specific connection settings.
Server Groups	Configuration of vSpace Server Groups (on RX300 and LEAF OS).
Kiosk Mode	Automatic user logon and application start settings.
Display	Display settings.
Peripherals	Redirection settings for peripheral devices.
Audio	Audio settings.
Keyboard	Keyboard layout selection.
Network	Network settings.
Management	Remote device management settings.
Security	Certificates management.
Support	Firmware update and troubleshooting tools.
Date and Time	Date and time settings.
About	Information about current device state.

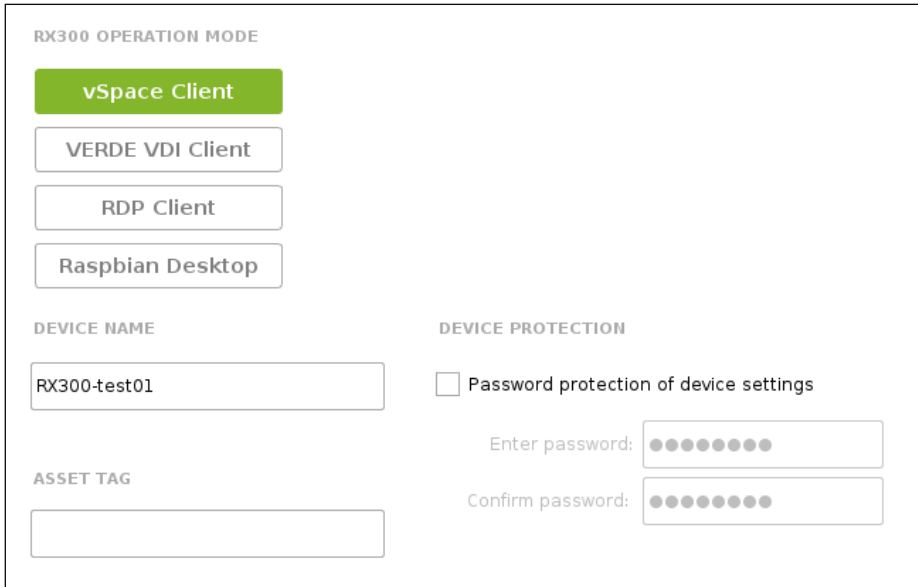
The list of available Setup GUI sections will be displayed in menu form on the left-hand side of the window. The main area of the Setup GUI allows configuring the device settings specific to the selected section. In the bottom-right corner there are the **[APPLY]** and **[Cancel]** buttons. Clicking the

[APPLY] button saves and applies the configuration changes. Clicking the **[Cancel]** button closes the Setup GUI without saving and applying any changes.



4.1. General settings

The General settings section allows selection of device operation mode, configuring a device name, setting a device asset tag, and configuring a password for protecting the Setup GUI against unauthorized access.



4.1.1. Selecting the device operation mode

RX300 thin client devices can be configured to operate in one of the following modes:

- vSpace Client
- VERDE VDI Client
- RDP Client
- Raspbian Desktop

RX-RDP and RX420(RDP) thin client devices can be configured to operate in one of the following modes:

- VERDE VDI Client
- RDP Client

Repurposed PCs running LEAF OS can operate in vSpace Client mode only.

Appropriate button in RX300, RX-RDP or RX420(RDP) **Device Operation Mode** settings group must be clicked to change the operation mode. Depending on the operation mode selected in **General** section different settings become available in the **Connections** section of Setup GUI.

Selecting the **Raspbian Desktop** mode on RX300 device requires device reboot for the change to take effect.

Note: RX300 device switched into **Raspbian Desktop** mode can't be remotely managed from vSpace Console nor from the PMC Device Management system. Turning the device back into thin client mode is only possible by manually clicking the icon intended for this purpose and located on the Raspbian desktop.

4.1.2. Configuring Device Name

The **Device Name** parameter acts as the hostname of the device and will be used when communicating with the DHCP server and device management tools (vSpace Console or PMC Device Management system). The DHCP server and device management tools use the Device Name as one of parameters allowing device identification.

The default Device Name can be changed to a name reflecting the organization's department affiliation, device network- or physical location, device user's role, etc. The specified device name must comply with computer hostname rules: it can only consist of lowercase and uppercase letters, digits, and the hyphen (-) sign. The Device Name must not start with hyphen sign.

The Device Name value will be used as following:

- It will be contained in the DHCP request sent by the device to DHCP server when obtaining an IP address. This allows the DHCP server to register the Device Name in DNS on behalf of the DHCP client device.
- In RDP and UXP sessions in Windows operating systems the Device Name will be available as the value of the %CLIENTNAME% environment variable (please refer to vSpace Pro Administration Guide for additional information regarding necessary vSpace Pro

configuration). Scripts or applications running on the terminal servers can leverage this variable to perform device-specific tasks.

Note: In Windows operating systems the NetBIOS computer names have the maximum length of 15 characters. The %CLIENTNAME% environment variable will accommodate up to 15 characters of Device Name.

- It will be reported to PMC Device Management system. Based on the Device Name PMC can automatically assign the device to a Name Scope within the Subnet the device belongs to.

4.1.3. Configuring device Asset Tag

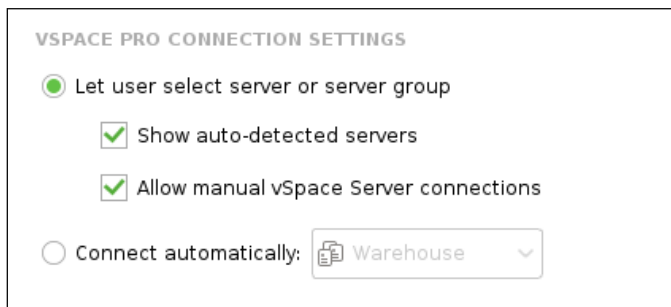
The **Asset Tag** is yet another parameter which the device reports to PMC Device Management system. Based on the Asset Tag value PMC can automatically assign the device to an Asset Tag based device group within the Subnet the device belongs to. An Asset Tag is a string value.

4.1.4. Protecting the Setup GUI against unauthorized access

The Setup GUI can be protected from unauthorized access by selecting the **Password protection of device settings** settings checkbox and specifying a password for administrator. Whenever a user will try to open the Setup GUI on a password-protected device a password prompt will appear and the Setup GUI will only be opened after providing a valid password.

4.2. Connections settings in vSpace Client mode

The RX300 and LEAF OS devices allow connections to vSpace Pro servers. The connections can be initiated by user or started automatically.



The screenshot shows a dialog box titled "VSPACE PRO CONNECTION SETTINGS". It contains four options:

- Let user select server or server group
 - Show auto-detected servers
 - Allow manual vSpace Server connections
- Connect automatically: Warehouse (dropdown menu)

Following are the parameters which can be configured when the device is set to operate in vSpace Client mode:

- **Let user select server or server group** – with this selection the user will initiate the vSpace connection.
- **Show auto-detected servers** – list of servers automatically detected in the local subnet will be presented to the user when this option will be enabled.
- **Allow manual vSpace Server connections** – with this option enabled user will have the ability to manually specify the name or address of target vSpace Pro server.
- **Connect automatically** – with this selection the device will immediately connect to the selected vSpace Pro server or vSpace Server Group after booting up. The combo-box will be populated with the list of automatically detected vSpace Pro servers and defined [vSpace Server Groups](#).

Refer to [Kiosk Mode](#) settings for the information about automatic user logon or application start options.

4.3. Connections settings in VERDE VDI Client mode

When switched into VERDE VDI Client mode the RX300, RX-RDP and RX420(RDP) devices allow connections to VERDE VDI deployments.

The screenshot shows a configuration window titled "VERDE VDI CONNECTION SETTINGS". It contains the following elements:

- A text input field labeled "VERDE Connection Broker:" with the value "verde.company.local".
- A checkbox labeled "Connect automatically:" which is unchecked, followed by a text input field with the placeholder text "Enter desktop name".
- Radio buttons for "Default protocol": "NComputing UXP" (unchecked) and "Microsoft RDP" (checked).
- A checkbox labeled "Allow using custom VERDE Connection Brokers" which is checked.

Following connection parameters can be configured for VERDE VDI Client mode:

- **VERDE Connection Broker** – the address of the VERDE Connection Broker (sometimes referred to as VERDE Connection Server), which authenticates the user, delivers the list of available VERDE VDI desktops and their addresses when the users attempt to connect. This is an obligatory parameter.
- **Connect automatically** – a name of a VERDE VDI desktop can be optionally specified here. This desktop will be started automatically after successful user authentication, when specified.
- **Default protocol** – selection of default presentation protocol for the VERDE VDI remote desktop sessions.
- **Allow using custom VERDE Connection Brokers** – this option will enable the user to specify on the main screen the name or address of a VERDE VDI Connection Broker of own choice. This option controls the appearance of the **Broker URL** combo-box on the VERDE VDI Client's main screen.

Following are the RDP protocol related parameters, which can be additionally configured for the VERDE VDI Client connections:

The screenshot shows a configuration window titled "RDP PROTOCOL SETTINGS". It contains the following elements:

- A text input field labeled "Custom parameters :".
- Four checked checkboxes: "Enable RemoteFX", "Smooth edges of screen fonts", "Show window contents while dragging", and "Show desktop wallpaper".

- **Custom parameters** – this option can be used to specify additional parameters (command-line options) for the FreeRDP client used by the device for establishing VERDE VDI connections with the RDP protocol. When multiple FreeRDP command-line options must be specified then the options should be separated with the semicolon (;) character (without any surrounding whitespaces).
Please refer to FreeRDP client documentation for information about FreeRDP command-line options, which can be passed as custom RDP parameters:
 - <https://github.com/FreeRDP/FreeRDP/wiki/CommandLineInterface>
 - <https://github.com/awakecoding/FreeRDP-Manuals/blob/master/User/FreeRDP-User-Manual.markdown>
- **Enable RemoteFX** – this option can be enabled to improve the user experience, especially when using multimedia applications. With RemoteFX enabled the RDP protocol will internally use codecs which are optimized for multimedia contents.
- **Smooth edges of screen fonts** – this option enables the fonts smoothing (ClearType) inside RDP sessions. It will only have effect when this feature is not disabled on the server side.
- **Show window contents while dragging** – this option controls the behavior of application windows dragging inside the RDP session. When enabled the contents of the windows will be displayed while dragging. This option will only have effect when this feature is not disabled on the server side.
- **Show desktop wallpaper** – this option controls the display of the desktop wallpaper inside RDP sessions. It will only have effect if desktop wallpapers are not disabled on the server side.

4.4. Connections settings in RDP Client mode

When switched into RDP Client mode the RX300, RX-RDP and RX420(RDP) devices allow following types of connections to Remote Desktop Services deployments:

1. Direct connections to Remote Desktop Session Hosts.
2. Connections to Remote Desktop Session Hosts located behind Remote Desktop Gateway.
3. Connections to RemoteApp desktops and programs brokered by Remote Desktop Connection Broker and Remote Desktop Web Access servers. The RemoteApp desktops and programs can be accessed by contacting the Remote Desktop Session Hosts directly or through Remote Desktop Gateway.

4.4.1. Configuring direct connections to RD Session Hosts

Direct (not brokered) connections to Remote Desktop Session Hosts are the simplest possible RDP connections, as it is enough to only have one server, where a role-based installation of the Remote Desktop Session Host role was performed. No other Remote Desktop server roles (like Connection Broker or Web Access) must be deployed for this connection type. The Remote Desktop Session Host does not need to belong to Active Directory domain in this scenario.

Following are the obligatory parameters which must always be configured for a direct Remote Desktop Session Host connection:

- **Remote Desktop Session Host** – an IP address, hostname, or fully-qualified domain name (FQDN) of an RD Session Host must be specified here. This RD Session Host will perform the user authentication. The RDP terminal connection will go to the address returned by the RD Session Host after successful user authentication. In simplest case (with only one RD Session Host in place) this will be the same address, but in general (especially in deployments including Session Host collections consisting of multiple RD Session Hosts) the session can go to another RD Session Host, e.g. to the one, where the user had a disconnected session.
- **Enable RemoteApp and Desktop Connections** – this checkbox must be not selected.

REMOTE DESKTOP CONNECTION SETTINGS

Remote Desktop Session Host:

Custom parameters:

Allow connections to custom Remote Desktop Session Hosts

Enable RemoteFX

Enable RemoteApp and Desktop Connections

Smooth edges of screen fonts

Show window contents while dragging

Show desktop wallpaper

Optional parameters for direct Remote Desktop Session Host connections are:

- **Custom parameters** – this option can be used to specify additional parameters (command-line options) for the FreeRDP client used by the device for establishing RDP connections. When multiple FreeRDP command-line options must be specified then the options should be separated with the semicolon (;) character (without any surrounding whitespaces). Please refer to FreeRDP client documentation for information about FreeRDP command-line options, which can be passed as custom RDP parameters:
 - <https://github.com/FreeRDP/FreeRDP/wiki/CommandLineInterface>
 - <https://github.com/awakecoding/FreeRDP-Manuals/blob/master/User/FreeRDP-User-Manual.markdown>
- **Allow connections to custom Remote Desktop Session Hosts** – this option can be enabled (which is the factory default settings) or disabled. When enabled the RD Session Host input field will be visible on the [main screen](#), allowing the user to manually enter a Remote Desktop Session Host address of own choice. Device will remember the history of up to 10 successful custom RD Session Host connections. The Remote Desktop Session Host address specified in Setup GUI will always appear on the history list. When disabled the user will always be connected only to the RD Session Host with the address specified in the Connections settings. In environments where the users should not be given a chance to connect to custom Remote Desktop Session Hosts it's advisable to have this option disabled.
- **Enable RemoteFX** – this option can be enabled to improve the user experience, especially when using multimedia applications. With RemoteFX enabled the RDP protocol will internally

use codecs which are optimized for multimedia contents. It is advisable to have supported GPUs available in RD Sessions Hosts to accelerate the screen encoding process. Software-based screen encoding when RemoteFX is enabled can cause high CPU load on the server side, especially when multiple users will connect at the same time to the same server.

- **Smooth edges of screen fonts** – this option enables the fonts smoothing (ClearType) inside RDP sessions. It will only have effect when this feature is not disabled on the server side.
- **Show window contents while dragging** – this option controls the behavior of application windows dragging inside the RDP session. When enabled the contents of the windows will be displayed while dragging. This option will only have effect when this feature is not disabled on the server side.
- **Show desktop wallpaper** – this option controls the display of the desktop wallpaper inside RDP sessions. It will only have effect if desktop wallpapers are not disabled on the server side.

4.4.2. Configuring connections to RD Session Hosts located behind RD Gateway

Note: For brokered RDP connections which have to traverse RD Gateway please refer to the [next section](#).

Not brokered connections to Remote Desktop Session Hosts located behind Remote Desktop Gateway servers are supported. Including the Remote Desktop Gateways in RDS deployments improves the security when the Remote Desktop Session Hosts will have to be accessed by users connecting through the Internet. Only one IP address, belonging to the Remote Desktop Gateway server, will have to be exposed to the public Internet then. Multiple Remote Desktop Session Hosts can be located in the secure network behind the Gateway. The Gateway will pass-through the traffic to Remote Desktop Session Hosts only after successfully authenticating the connecting user.

Following are the obligatory parameters which must always be configured for connections to Remote Desktop Session Hosts located behind Remote Desktop Gateway:

- **Remote Desktop Session Host** – a hostname or fully-qualified domain name (FQDN) of target RD Session Host must be specified here. This hostname does not need to be resolvable on the public Internet but must be resolvable on the Gateway machine. An IP address may not work here.
- **Custom parameters** – the '/g:' custom parameter followed by the RD Gateway FQDN must be specified here, e.g. /g:gw.company.com. The credentials entered by the user on the logon screen will be used for the authentication on the Remote Desktop Gateway. The same credentials will then be used for authentication on the target Remote Desktop Session Host.

- **Enable RemoteApp and Desktop Connections** – this checkbox must be not selected.

REMOTE DESKTOP CONNECTION SETTINGS

Remote Desktop Session Host:

Custom parameters:

Allow connections to custom Remote Desktop Session Hosts

Enable RemoteFX

Enable RemoteApp and Desktop Connections

Smooth edges of screen fonts

Show window contents while dragging

Show desktop wallpaper

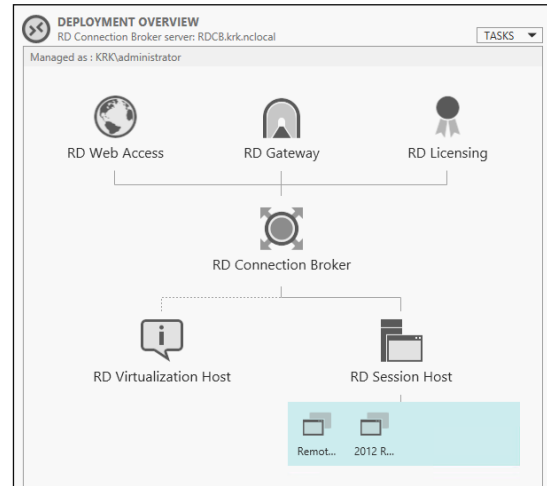
Optional parameters for connections to Remote Desktop Session Hosts located behind RD Gateway are:

- **Custom parameters** – this option can be used to specify FreeRDP parameters (command-line options) other than the '/g:', which is mandatory in this scenario. When multiple FreeRDP command-line options must be specified then the options should be separated with the semicolon (;) character (without any surrounding whitespaces). Please refer to FreeRDP client documentation for information about FreeRDP command-line options, which can be passed as custom RDP parameters:
 - <https://github.com/FreeRDP/FreeRDP/wiki/CommandLineInterface>
 - <https://github.com/awakecoding/FreeRDP-Manuals/blob/master/User/FreeRDP-User-Manual.markdown>
- **Allow connections to custom Remote Desktop Session Hosts** – this option can be enabled (which is the factory default settings) or disabled. When enabled the RD Session Host input field will be visible on the [main screen](#), allowing the user to manually enter a Remote Desktop Session Host address of own choice. Device will remember the history of up to 10 successful custom RD Session Host connections. The Remote Desktop Session Host address specified in Setup GUI will always appear on the history list. When disabled the user will always be connected only to the RD Session Host with the address specified in the Connections settings. In environments where the users should not be given a chance to connect to custom Remote Desktop Session Hosts it's advisable to have this option disabled.
- **Enable RemoteFX** – this option can be enabled to improve the user experience, especially when using multimedia applications. With RemoteFX enabled the RDP protocol will internally use codecs which are optimized for multimedia contents. It is advisable to have supported GPUs available in RD Sessions Hosts to accelerate the screen encoding process. Software-based screen encoding when RemoteFX is enabled can cause high CPU load on the server side, especially when multiple users will connect at the same time to the same server.
- **Smooth edges of screen fonts** – this option enables the fonts smoothing (ClearType) inside RDP sessions. It will only have effect when this feature is not disabled on the server side.

- **Show window contents while dragging** – this option controls the behavior of application windows dragging inside the RDP session. When enabled the contents of the windows will be displayed while dragging. This option will only have effect when this feature is not disabled on the server side.
- **Show desktop wallpaper** – this option controls the display of the desktop wallpaper inside RDP sessions. It will only have effect if desktop wallpapers are not disabled on the server side.

4.4.3. Configuring connections to RemoteApp programs or desktops

Customers having complete Remote Desktop Services deployments in place can benefit from the RemoteApp programs and desktops publishing. RX300, RX-RDP and RX420(RDP) thin client devices in RDP Client mode support connections to published RemoteApp desktops (accessed in the full-screen mode) and programs (accessed in separate windows). The Remote Desktop Services deployments must include servers with the RD Connection Broker and RD Web Access role services installed to allow connections from RX300, RX-RDP and RX420(RDP) thin client devices with RemoteApp and Desktop Connections support enabled. For increased security, when accessing the Remote Desktop Services deployments from the Internet, the deployments can contain an RD Gateway. The client devices will automatically receive the RD Gateway address from the configured RD Web Access server.



Following are the obligatory parameters of a RemoteApp programs or desktops connection:

- **Remote Desktop Web Access URL** – an IP address, hostname, fully-qualified domain name (FQDN), or URL of Remote Desktop Web Access server providing the Remote Desktop Connection feed API must be specified here. This RD Web Access server will (along with other RD deployment components) perform the user authentication and return the list of RemoteApp resources (programs and desktops) published for the authenticated user. The Remote Desktop Web Access server URL can be specified in simplified or complete form. When a simplified URL will be specified in this field the device will expand it to create a complete one, e.g.:

Specified Web Access URL	Expanded (complete) Web Access URL
192.168.50.7	https://192.168.50.7:443/RDweb
rdwa	https://rdwa:443/RDWeb
rdwa.company.local	https://rdwa.company.local:443/RDWeb
rdwa.company.local:444	https://rdwa.company.local:444/RDWeb
https://rdwa.company.local/RDWeb	https://rdwa.company.local:443/RDWeb

- **Enable RemoteApp and Desktop Connections** – this checkbox must be selected.

REMOTE DESKTOP CONNECTION SETTINGS

Remote Desktop Web Access URL:

Custom parameters:

Allow connections to custom Remote Desktop Web Access URLs

Enable RemoteFX

Enable RemoteApp and Desktop Connections

Smooth edges of screen fonts

Show window contents while dragging

Show desktop wallpaper

Optional parameters of RemoteApp programs of desktops connections are:

- **Custom parameters** – this option can be used to specify additional parameters (command-line options) for the FreeRDP client used by the device for establishing RDP connections. When multiple FreeRDP command-line options must be specified then the options should be separated with the semicolon (;) character (without any surrounding whitespaces). Please refer to FreeRDP client documentation for information about FreeRDP command-line options, which can be passed as custom RDP parameters:
 - <https://github.com/FreeRDP/FreeRDP/wiki/CommandLineInterface>
 - <https://github.com/awakecoding/FreeRDP-Manuals/blob/master/User/FreeRDP-User-Manual.markdown>
- **Allow connections to custom Remote Desktop Web Access URLs** – this option can be enabled (which is the factory default settings) or disabled. When enabled the RD Web Access URL input field will be visible on the [main screen](#), allowing the user to manually enter a Remote Desktop Web Access URL of own choice. Device will remember the history of up to 10 successful authentication attempts with custom URL. The Remote Desktop Web Access URL configured in Setup GUI will always appear on the history list. When disabled the user will always be authentication on the RD Web Access server with the URL specified in the Connections settings. In environments where the users should not be given a chance to connect through custom Remote Desktop Web Access URLs it's advisable to have this option disabled.
- **Enable RemoteFX** – this option can be enabled to improve the user experience when accessing published desktops, especially when using multimedia applications. With RemoteFX enabled the RDP protocol will internally use codecs which are optimized for multimedia contents. It is advisable to have supported GPUs available in RD Sessions Hosts to accelerate the screen encoding process. Software-based screen encoding when RemoteFX is enabled can cause high CPU load on the server side, especially when multiple users will connect at the same time to the same server.

- **Smooth edges of screen fonts** – this option enables the fonts smoothing (ClearType) inside RDP sessions. It will only have effect when this feature is not disabled on the server side.
- **Show window contents while dragging** – this option controls the behavior of application windows dragging inside the RDP session. When enabled the contents of the windows will be displayed while dragging. This option will only have effect when this feature is not disabled on the server side.
- **Show desktop wallpaper** – this option controls the display of the desktop wallpaper inside RDP sessions. It will only have effect if desktop wallpapers are not disabled on the server side.

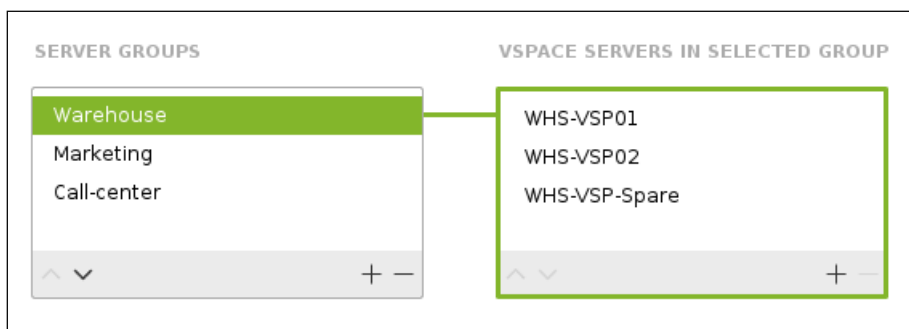
Refer to [Kiosk Mode](#) settings for the information how to configure automatic start of a RemoteApp program or desktop.

4.5. Server Groups

Note: This section only applies to RX300 and LEAF OS devices configured to operate in vSpace Client mode.

When the device operates in vSpace Client mode it allows connections to specific vSpace Pro servers (determined by hostname or IP address) or to groups of vSpace Pro servers. The vSpace Server Groups implement the concept of vSpace Pro servers' failover. The sequence in which the device will attempt to connect to group servers depends on the order of the servers in the group. When connecting to a Server Group the vSpace session will be started on the first vSpace Pro server which accepted the client connection. If no server from the group accepted the connection, then the device will re-start the cycle and will keep trying until a connection will be successfully started on some server.

vSpace Server Groups can be defined in the **Server Groups** section of the Setup GUI. Two lists will be presented: **Server Groups** and **vSpace Servers in selected group**:



The Server Groups list contains the list of defined groups, the other group the list of servers belonging to the group. The [+] and [-] buttons allow adding and removing the groups or servers, accordingly. The [▲] or [▼] buttons allow moving the selected list items up and down.

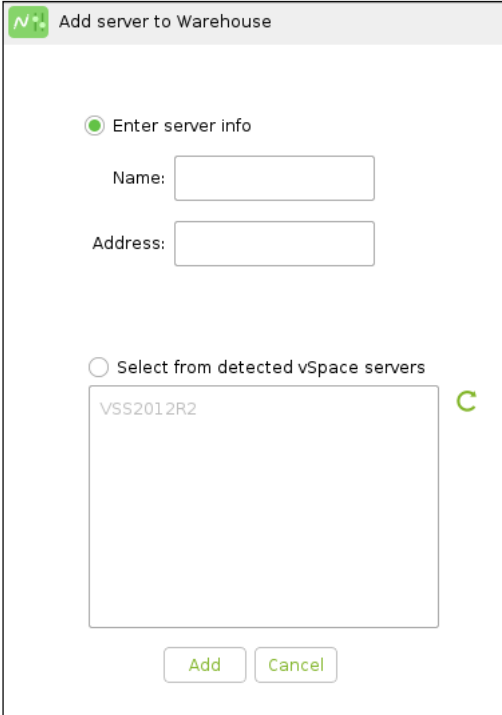
Adding a vSpace Pro server to Server Group

Device firmware allows adding to Server Groups manually specified servers or automatically detected servers.

To add a server manually select the **Enter server info** radio-button. The specified server **Name** will appear on the list and the connection attempt will go to the specified **Address**.

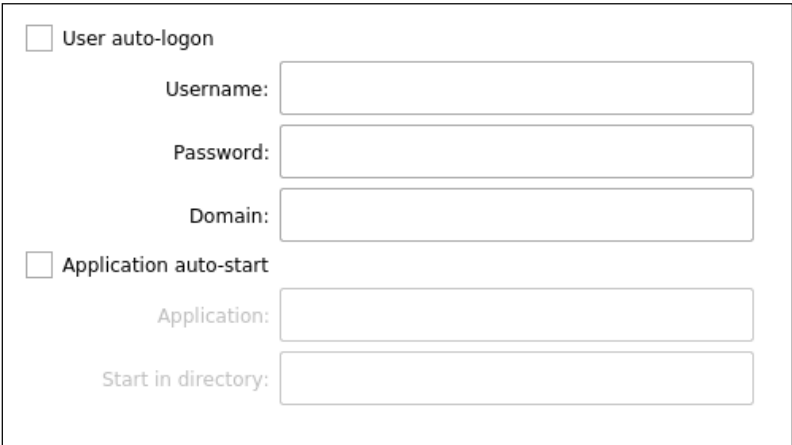
To select an automatically detected vSpace Pro server select the **Select from detected vSpace servers** radio-button. The selected server name will appear on the list and the server's address will be used for client connections.

The **[Add]** button needs to be clicked to add the specified or selected vSpace Pro server to Server Group.



4.6. Kiosk Mode settings

Kiosk Mode settings allow configuration of user auto-logon and application auto-start. Pre-configuration of the Domain name for VERDE VDI and RDP connections can also be done here.



4.6.1. Configuring user auto-logon settings

Automatic user logon can be used for terminal connections in vSpace Client, VERDE VDI Client, and RDP Client operation modes. Following are the parameters necessary to enable automatic logon of a user:

- **User auto-logon** – this checkbox must be selected.
- **Username** – the account name of the user for automatic logon.
- **Password** – user's password.

- **Domain** – for Active Directory-joined systems only – the Active Directory Domain name.

Depending on the device operation mode the following will happen after booting up a device with user auto-logon enabled:

vSpace Client mode – no credentials prompt will appear when a connection to vSpace server will be established. The specified user will be logged on automatically.

VERDE VDI Client mode – no logon box will appear. Device will automatically authenticate the specified user on the configured VERDE connection broker. Depending on VERDE VDI connection settings a list of VERDE VDI desktops will be presented, or the specified virtual desktop will be started automatically.

RDP Client configured for a direct RD Session Host connection – no logon box will appear. Device will automatically authenticate the specified user. An RDP session will be started automatically and the specified user will be logged on.

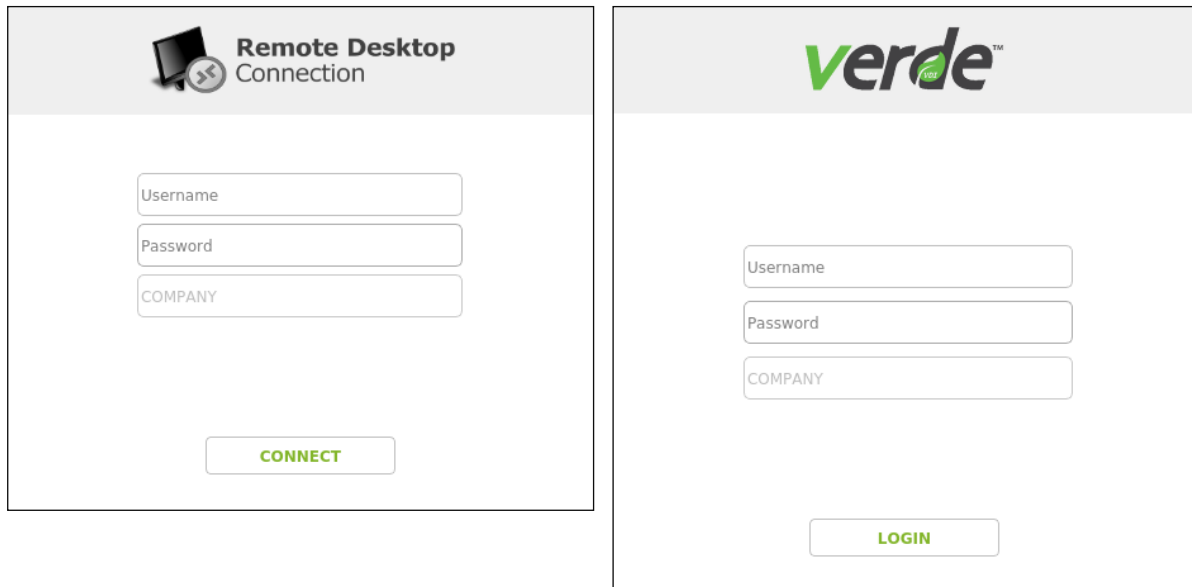
RDP Client with RemoteApp support enabled – no logon box will appear. Device will automatically authenticate the specified user. List of published RemoteApp programs and desktops will be displayed.

4.6.2. Pre-configuring the Domain name for VERDE VDI and RDP connections

The VERDE VDI Client mode and RDP Client mode are device operation modes, where the device immediately after booting up displays the logon box on the main screen. In environments where the VERDE VDI systems or Microsoft Remote Desktop Deployments are integrated with Active Directory the users must provide their Active Directory credentials, including the domain name, during logon. In many cases the users will have their accounts in one specific Active Directory domain. To simplify the logon process and to exempt the users from the necessity to always enter the same domain name, the domain name can be pre-configured.

To pre-configure the Domain name for VERDE VDI and Remote Desktop Connection logon box the desired AD domain name must be entered into the **Domain** field. The **User auto-logon** checkbox does not need to be selected.

The domain name configured that way will be stored in device configuration and will be put into the **Domain** field of VERDE VDI and Remote Desktop Connection logon boxes. In such case the users will have to provide their usernames and passwords only when attempting to authenticate.



The image shows two side-by-side screenshots of login interfaces. The left interface is titled "Remote Desktop Connection" and features three input fields: "Username", "Password", and "COMPANY". Below these fields is a green "CONNECT" button. The right interface is titled "verde" and features three input fields: "Username", "Password", and "COMPANY". Below these fields is a green "LOGIN" button.

Note: With the domain name preconfigured in the way described here the users will still have the ability to enter own domain name. When the username provided will be in the form of DOMAIN\user or user@domain then the user-specified domain name will be used for authentication instead of the preconfigured domain name.

4.6.3. Configuring legacy application auto-start

The application auto-start feature causes the terminal session to only start for the user the specified application, instead of the full desktop. Closing the application terminates the session and logs the user off. This feature can be set up for vSpace, VERDE VDI, and direct RDP connections to RD Session Hosts. Please see the additional note below regarding RDP connections (including RDP connections to VERDE system).

Following parameters must be configured to enable automatic start of an application:

- **Application auto-start** – this checkbox must be selected.
- **Application** – the name of the program to be started. For programs located in system's default search path (which includes C:\Windows, C:\Windows\system32, etc.) it is enough to specify the name of the executable file (e.g. notepad.exe). For other programs the fully qualified path of the executable file must be specified (e.g. C:\Program Files\Software Vendor\Software Package\application.exe).
- **Start in directory** – the default start directory for the application.

Note: The following must be considered when configuring application auto-start for RDP connections: latest versions of Windows operating systems favor RemoteApp program and desktops publishing and do not allow launching applications with program paths specified on the client side. This functionality can be re-enabled by modifying Windows registry:

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

4.6.4. Configuring RemoteApp program or desktop auto-start

When the RX300, RX-RDP or RX420(RDP) device operates in [RDP Client mode with RemoteApp and Desktops support](#) enabled then the device can be configured to automatically start the published RemoteApp resource after successfully authenticating the user.

Following **Kiosk Mode** settings must be configured to enable automatic start of published RemoteApp resource:

- **Application auto-start** – this checkbox must be selected.
- **Application** – the name of the desired RemoteApp program or desktop.
- **Start in directory** – this field should be left empty.

4.7. Display settings

The **Display** section of the Setup GUI allows the configuration of device settings related to displays.

4.7.1. RX300 and RX-RDP display settings

The RX300 and RX-RDP devices support resolutions up to 1920x1200 and only have one HDMI output. These devices can work with primary display and with an optional secondary display. Primary display is the one which is connected directly to the [HDMI output](#) of the device. Secondary display can be connected through a USB-based Secondary Display Adapter (SDA).

Three SDA types are supported:

- **NComputing Raspberry Pi Zero (Pi0) SDA**
Secondary Display Adapters based on Raspberry Pi Zero.



- **DisplayLink SDA**
Secondary Display Adapters based on DisplayLink DL-1x0 and DL-1x5 (e.g. DL-150) chipsets. DisplayLink adapters with following USB vendor ID and product ID (VID:PID) will be recognized and work:

- | | | |
|-------------|-------------|-------------|
| ○ 17e9:0290 | ○ 17e9:0378 | ○ 17e9:037d |
| ○ 17e9:0351 | ○ 17e9:0379 | ○ 17e9:410a |
| ○ 17e9:030b | ○ 17e9:037a | ○ 17e9:430a |
| ○ 17e9:0377 | ○ 17e9:037b | ○ 17e9:4312 |
| | ○ 17e9:037c | |

The RX300 or RX-RDP device must be rebooted to become properly configured after

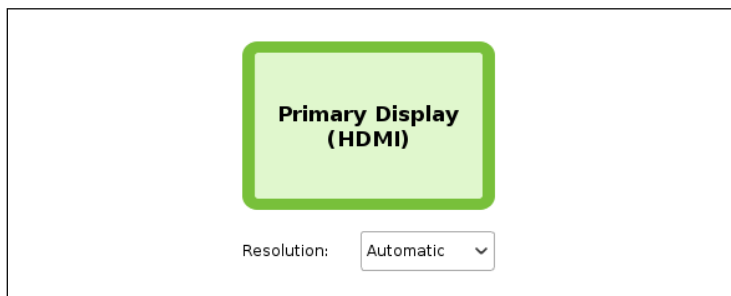
physically connecting or disconnecting any DisplayLink adapter. Hot-plugging the DisplayLink adapters is not supported.

- **NComputing N-series SDA**
Secondary Display Adapters based on SMSC/Microchip UFX6000 chip, previously offered by NComputing for the N-series devices, are supported and can be used to extend the full-screen UXP and RDP desktop sessions. These adapters were offered in two variants: USB-VGA and USB-DVI and both can be used with RX300 and RX-RDP.



Configuring screen resolution

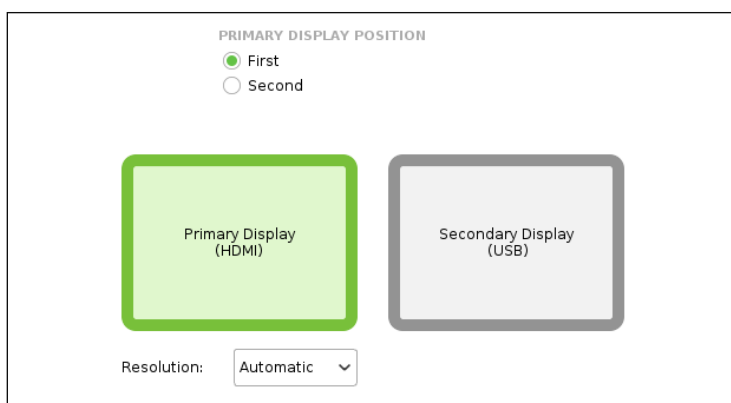
RX300 and RX-RDP devices by default automatically set up the optimal resolution for the primary display. Optimal resolution matches the native resolution of the monitor connected to the HDMI output. This is indicated by the Automatic selection in resolution combo-box. In case when the native resolution was not recognized properly or when it is desirable to set a specific resolution, the resolution for the primary display can be selected in the Display section of Setup GUI:



There is no option to select a specific the resolution for the secondary display. Secondary display will always work with the optimal (automatically detected) resolution.

Configuring primary screen position

When connection of the secondary display will be detected then the position of the primary display can be selected. Primary display is usually the one on which the credentials prompt appears.



- **First** – means that the primary display will be on the left-hand side.

- **Second** – means that the primary display will be on the right-hand side.

Secondary display adapters limitations

The Secondary Display Adapters are mainly purposed to allow desktop extension in full-screen UXP (vSpace Client, VERDE VDI Client) and RDP (RDP Client, VERDE VDI Client) desktop sessions. Certain limitations apply to different scenarios as listed in the following table:

Scenario	Desktop extension to:		
	Pi0 SDA	DisplayLink SDA	N-series SDA
Local device GUI	Not supported	Supported	Not supported
vSpace Client, UXP session	Supported	Not supported	Supported
VERDE VDI Client, UXP session	Supported	Not supported	Supported
VERDE VDI Client, RDP session	Supported	Supported	Supported
RDP Client, full-screen desktop session	Supported	Supported	Supported
RDP Client, RemoteApp program session	Not supported	Supported	Not supported

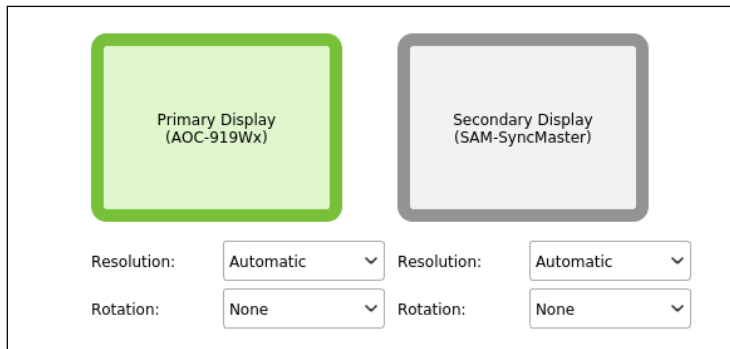
4.7.2. RX420(RDP) display settings

The RX420(RDP) devices support resolutions up to 4K (3840x2160) and have two [micro HDMI outputs](#). These devices can work with one display only or with two displays connected at the same time. Primary display is the one which is connected to the micro HDMI output located closer to the USB-C power port. Secondary display is the one which is connected to the micro HDMI output located closer to the 3.5mm audio output. Both RX420(RDP) displays can be rotated in clockwise and counterclockwise directions. In single display scenarios the primary display should be connected. In dual display scenarios the device desktop can be extended to the secondary display, or the secondary display can be configured to mirror the primary.

Configuring screen resolutions

RX420(RDP) devices by default automatically set up optimal resolutions for both displays. Optimal resolution matches the native resolution of the monitor connected to the micro HDMI output. This is indicated by the Automatic selection in resolution combo-box. In case when the native resolution

was not recognized properly or when it is desirable to set a specific resolution, the resolutions of both displays can be selected with the **Resolution** combo-boxes:



Note: When both displays will be configured (explicitly or automatically) to run at 4K resolutions then the refresh rate of both displays will be 30Hz only. 4K resolution with 60Hz refresh rate on one display can be used as long as the resolution of the other display is not higher than 1920x1080 (which will work with 60Hz refresh rate then too). This reconfiguration requires device reboot.

Configuring secondary display position

The secondary display can be located on the right (which is the default setting) or on the left of the primary display. The **Right** and **Left** radio buttons can be used for selecting the secondary display position.

Enabling screen mirroring

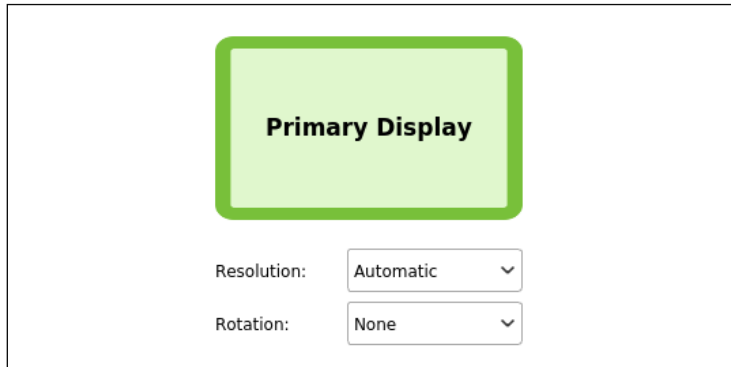
In dual display scenarios the device desktop can be extended to the secondary display (which is the default setting) or the secondary display can be configured to mirror the primary. To enable screen mirroring the **Mirror Display** checkbox must be selected. Secondary display will use the same resolution and rotation settings as the primary when display mirroring will be enabled.

Configuring screen rotations

RX420(RDP) displays can be rotated in clockwise and counterclockwise directions. The **Rotation** combo-boxes can be used for selecting the rotation direction of both displays.

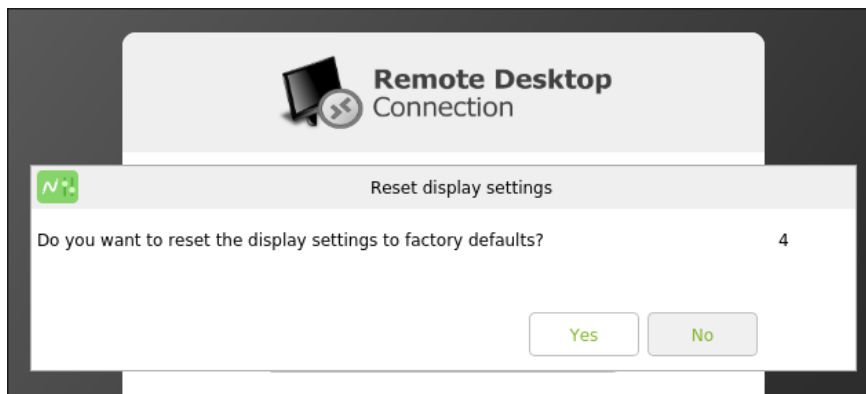
4.7.3. LEAF OS display settings

Repurposed PCs running LEAF OS can only work with single display, which acts as primary display. Screen resolution and rotation of the display can be configured. Resolutions up to 4K (3840x2160) are supported as well as clockwise and counterclockwise rotations.



4.7.4. Resetting the display settings to factory defaults

In case when the device was previously connected to different monitor and configured with a specific resolution, which is not supported by the currently connected monitor (a message like 'Signal out of range' appears on the screen), then the device can be reset to factory display settings. This can be done by pressing the SHIFT-CTRL-F1 key combination, when the device shows the main screen or the Setup GUI.



If the user will not cancel the process within 5 seconds, then the display settings will be reset, and the device GUI will be restarted. This will allow the user to regain the control over the device.

RX300 and RX-RDP factory default display settings are following:

- **Primary display position:** First
- **Primary display resolution:** Automatic

RX420(RDP) factory default display settings are following:

- **Secondary display position:** Right
- **Primary display resolution:** Automatic
- **Primary display rotation:** None
- **Secondary display resolution:** Automatic
- **Secondary display rotation:** None

- **Display mirroring:** Disabled

LEAF OS factory default display settings are following:

- **Resolution:** Automatic
- **Rotation:** None

4.7.5. Configuring the screen saver

The RX-series and LEAF OS devices are equipped with a screen saver, which gets triggered after a period of user’s inactivity. By default, the screen saver is turned off. The inactivity **Timeout** can be selected between 3 minutes and 2 hours. The selectable screen saver **Actions** are:

- **Turn the screens off** – the terminal sessions will keep running on the device.
- **Disconnect sessions and turn the screens off** – the terminal sessions will be disconnected, then the screens will be turned off.

SCREEN SAVER

Timeout: 5 minutes Action: Turn the screens off

4.7.6. Configuring desktop wallpaper

The RX-series firmware as well as LEAF OS allow configuring a custom desktop wallpaper which, for example, can contain organization’s branding elements. Picture files in JPG and PNG formats with resolutions up to 4096x2160 can be used as desktop wallpapers.

The wallpaper file to be added to the device must be uploaded to a web or FTP server and be accessible through HTTP, HTTPS, or FTP protocol. The URL of the wallpaper file must be specified after clicking the **[Add]** button:

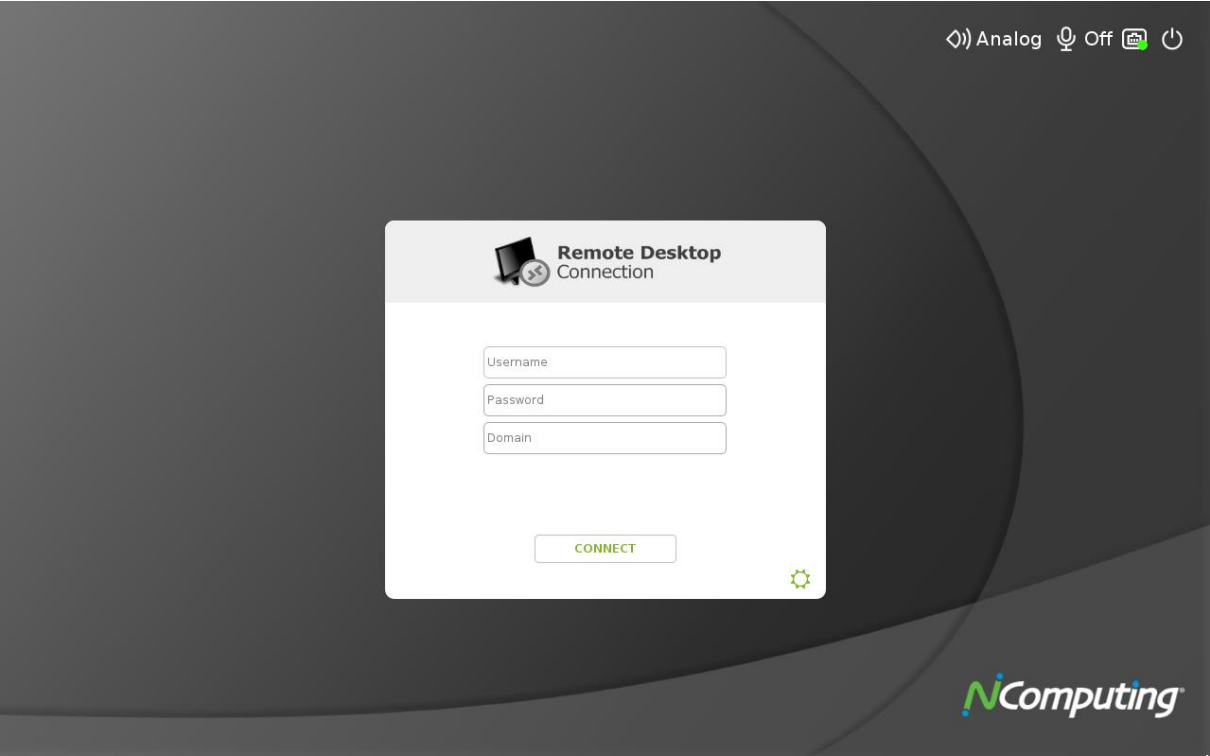
Adding Desktop Wallpaper

Wallpaper file (jpg/png) URL:

http://resources.company.local/wallpapers/wallpaper1.jpg

Add Cancel

The downloaded wallpaper will be set as background image for the main screen, Setup GUI, and RemoteApp desktop.

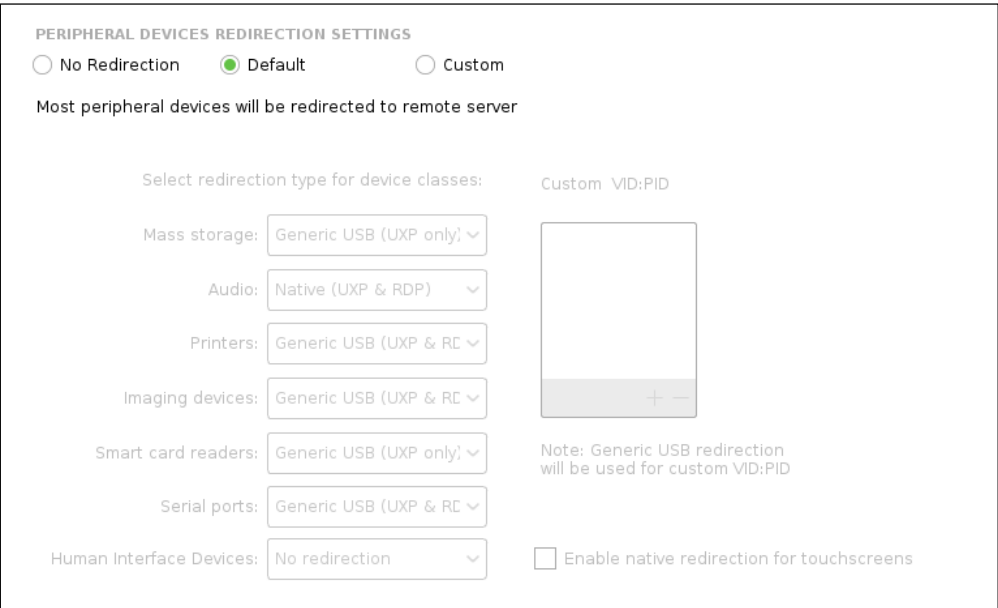


Removing the desktop wallpaper

To reset the desktop wallpaper to the default gray one the **[Reset]** button located in the **Desktop Wallpaper** settings group of Display settings can be used.

4.8. Peripherals settings

The **Peripherals** section of the Setup GUI allows granular control of what peripheral device classes will be redirected to terminal sessions and what redirection type will be used.



There are three general redirection policies selectable, with preconfigured settings for different device classes:

- **No redirection** – no peripheral devices other than system keyboard and mouse will be redirected.
- **Default** – preferred redirection settings for the thin client device model will be used.
- **Custom** – devices will be redirected or blocked according to granular selections.

Two redirection types (methods) are possible: **Native** redirection and **Generic USB** redirection. The availability of the redirection methods varies between device classes and terminal session protocols.

4.8.1. Native redirection of peripheral devices

Native redirection, also referred to as ‘functional redirection’, leverages a dedicated virtual channel in terminal protocol to allow device specific communication between the application accessing the peripheral device running in terminal session and the software components responsible for device handling on the client side. Native redirection usually provides optimized (e.g. ensuring best performance) support for the peripheral device class. The peripheral devices redirected in native way not always appear in the Device Manager inside user session. Some kind of support for the devices redirected in the native way must be present on the client side. The necessary software components are built into the RX300, RX-RDP and RX420(RDP) firmware for the device classes where the native redirection is possible. The necessary components are also present in LEAF OS. Because of that requirement (and sometimes because of lack of necessary API) not all peripheral device classes are redirectable with the native redirection.

4.8.2. Generic USB redirection of peripheral devices

Generic USB redirection, in contrast to native redirection, does not require any special device support on the client side. With the generic USB redirection, the low-level USB communication between the virtual USB hub created on the server side and the USB device physically connected to the thin client gets redirected. The USB peripheral device connected to thin client’s USB port gets detected by a virtual USB host controller or hub assigned to the user’s terminal session on the server side. The Windows device driver software necessary for using the connected peripheral device must be installed on the terminal server hosting the user session. The peripheral device forwarded with generic USB redirection always appears in the Device Manger inside user’s terminal session. If the terminal server hosting the user sessions is a multi-user system, then it must be able to appropriately handle (filter) the USB devices redirected in the generic way. If that fails then it can happen that the redirected device will interact with the Console session, not with user’s terminal session.

Note: In Windows Server 2019, Windows Server 2016 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 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 peripheral devices in RDP sessions running on operating systems mentioned in this note this group policy setting must be explicitly disabled. In Windows Server 2012 R2, Windows Server 2012, Windows 8 and

Windows 8.1 the Remote Desktop Services by default allow 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.

Note: In Windows Server 2008 R2 and Windows 7 the redirection of supported plug and play devices is allowed by default too, but these legacy operating systems need to additionally run as virtual machines on a Hyper-V host with the RemoteFX feature enabled for the Generic USB redirection in RDP sessions. Using Generic USB redirection in RDP sessions on Windows Server 2008 R2 or Windows 7 installed on physical machines is not possible.

4.8.3. Customizing peripheral devices redirection

When the **Custom** radio-button will be selected as the general redirection policy, then the following redirection type selections are available for different USB device classes:

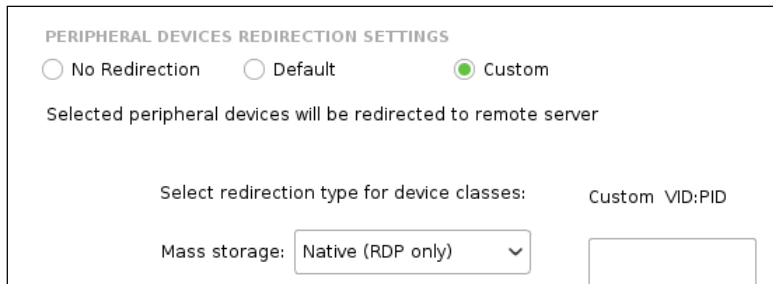
Device class	USB class ID	Available redirection types for UXP connections	Available redirection types for RDP connections
Mass storage	08	Generic USB	Native
Audio	01	Generic USB, Native	Generic USB, Native
Printers	07	Generic USB	Generic USB, Native
Imaging devices	06 0E	Generic USB	Generic USB
Smart card readers	0B	Generic USB, Native	Native
Serial ports	02	Generic USB	Generic USB, Native
Human Interface Devices	03	Generic USB	Generic USB
Touch screens	-	Native	Native

Default redirection types on RX-series and LEAF OS devices:

Device class	USB class ID	RX300	RX-RDP and RX420(RDP)	LEAF OS
Mass storage	08	Generic USB	Native	Generic USB
Audio	01	Native	Native	Native
Printers	07	Generic USB	Generic USB	Generic USB
Imaging devices	06 0E	Generic USB	Generic USB	Generic USB
Smart card readers	0B	Generic USB	Native	Generic USB
Serial ports	02	Generic USB	Native	Generic USB
Human Interface Devices	03	No redirection	No redirection	No redirection
Touch screens	-	No redirection	No redirection	No redirection

4.8.4. Native redirection of mass storage devices

Native redirection can be used to redirect **Mass storage** devices into RDP (RDP Client mode and VERDE VDI Client mode with RDP protocol) sessions only.



PERIPHERAL DEVICES REDIRECTION SETTINGS

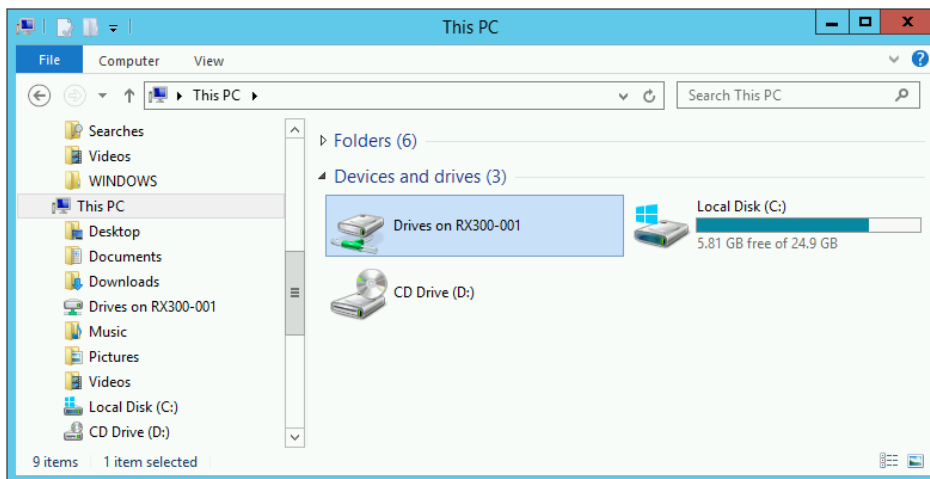
No Redirection Default Custom

Selected peripheral devices will be redirected to remote server

Select redirection type for device classes: Custom VID:PID

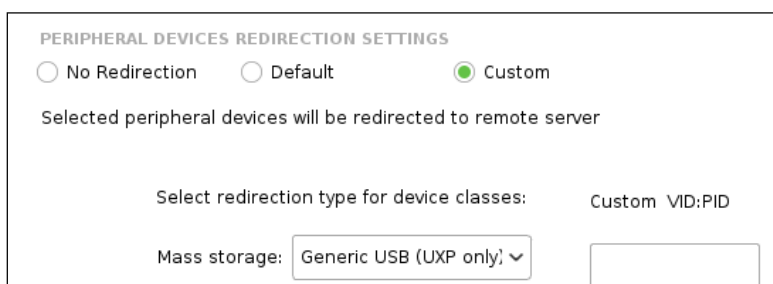
Mass storage: Native (RDP only) []

The FAT32 and NTFS file systems are supported on the USB mass storage devices. The RX-series or LEAF OS device mounts the USB mass storage device locally prior to redirection. What actually gets redirected is the local folder where the USB mass storage device was mounted. The redirected mass storage devices appear in RDP sessions as folders in the 'Drives' share of the thin client device:



4.8.5. Generic USB redirection of mass storage devices

Generic USB redirection can be used to redirect **Mass storage** devices into UXP sessions only. This applies to vSpace Client mode on RX300 or LEAF OS and to VERDE VDI Client mode with UXP protocol on RX300, RX-RDP or RX420(RDP).



PERIPHERAL DEVICES REDIRECTION SETTINGS

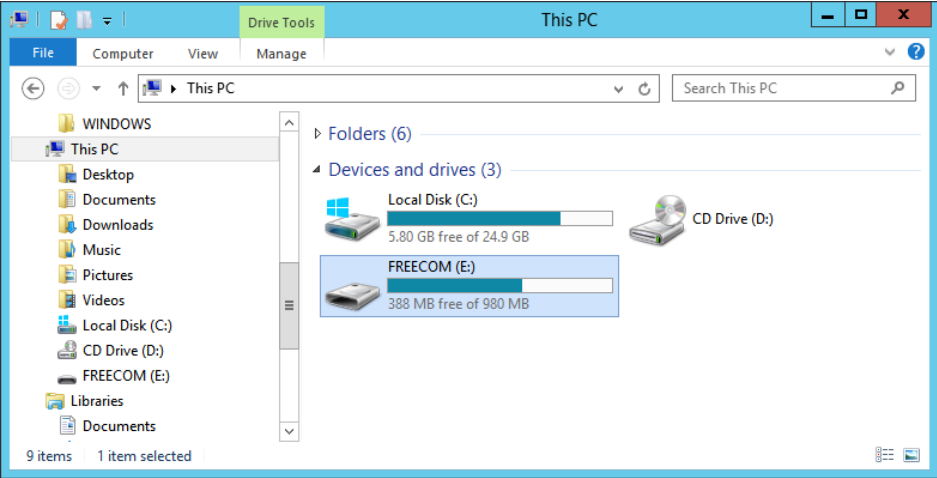
No Redirection Default Custom

Selected peripheral devices will be redirected to remote server

Select redirection type for device classes: Custom VID:PID

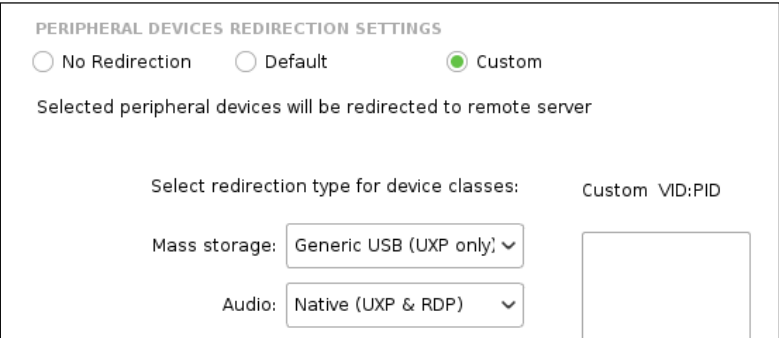
Mass storage: Generic USB (UXP only) []

All file system types supported by Windows OS should be supported with Generic USB redirection of mass storage devices. The redirected USB mass storage devices appear in UXP session as ordinary disk drives with a drive letter assigned:



4.8.6. Native redirection of audio devices

Native redirection is the default **Audio** redirection method for both protocols: UXP and RDP.



The names of Playback and Recording devices, which will appear in the terminal session, depend on the terminal server type and protocol used.

Terminal session protocol	Playback device name	Recording device name
UXP	Speakers NComputing virtual audio device	Microphone NComputing virtual audio device
RDP	Remote Audio	Remote Audio

What actual audio output (playback) and input (recording) device will be used depends on the configuration of device [audio settings](#) in the **Peripherals** section of Setup GUI.

During native redirection the properties of the audio devices usually get set to some system-specific values. E.g. for vSpace sessions the sampling rate for the playback device will be set to 22050 Hz by default, the resolution to 16-bit, stereo. Connecting a device supporting a higher sampling rate will be not beneficial, as the system will use own settings anyway. To fully use the capabilities of higher-end audio devices the **Generic USB** redirection should be used.

4.8.7. Generic USB redirection of audio devices

The **Generic USB** redirection of **Audio** devices is possible with both protocols: UXP and RDP.

PERIPHERAL DEVICES REDIRECTION SETTINGS

No Redirection Default Custom

Selected peripheral devices will be redirected to remote server

Select redirection type for device classes: Custom VID:PID

Mass storage: Generic USB (UXP only) ▼

Audio: Generic USB (UXP & RC) ▼

The audio devices redirected in the generic way appear in terminal session with their standard name and all capabilities of the devices can be used. This includes higher sampling rates and additional elements of the device, like control buttons.

Note: What needs to be considered when planning to use the **Generic USB** redirection for audio devices is that this redirection method requires transmission of big amounts of raw audio data, what, especially when using higher sampling rates, can cause very high network traffic. If there will be not enough network bandwidth available between the terminal server and the thin client device, or when any of the communicating parties will be unable to process the data on time, the interruptions in reproduced or recorded sound are to be expected.

Note: [Additional requirements](#) and [limitations](#) apply when using the Generic USB redirection with RDP protocol.

4.8.8. Native redirection of printers

Native redirection of printers is supported in RDP (RDP Client mode) connections only and can be used with USB and network printers. When native redirection of printers is selected then a printing subsystem will be started inside RX300, RX-RDP or RX420(RDP) device. The role of this printing subsystem is to spool the print jobs received from remote terminal servers and to send the spooled print jobs to configured local printers. The RDP client, when making a connection to a Remote Desktop Session Host, informs the host what Windows printer driver should be used for the redirected printer. The redirection will succeed only when the necessary driver is installed on the session host. This is because the local printing subsystem running in RX-series devices has no print job formatting capabilities. It must receive a print job already formatted on the server side by appropriate Windows printer driver.

The list of Windows printer drivers installed on a Windows machine can be obtained with following command:

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

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

Driver_name,driver_type,driver_architecture

For example:

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

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

For native redirection of client printers, the type 3 (Type 3 - User Mode) drivers for Windows x64 architecture should be selected. Type 4 drivers are known to cause issues with native redirection of client printers.

The list of printers created in terminal session can be obtained with following command:

```
wmic /NameSpace:\\Root\CIMV2 path Win32_Printer GET Caption,Comment,DriverName,PortName,
PrintProcessor /value
```

For the USB printers forwarded with the Native redirection method the PortName property will be like TS001. This indicates that the printer uses a 'terminal server' printer port, which redirects the print jobs to a terminal server client. This is the expected behavior.

For example:

```
C:\>wmic /NameSpace:\\Root\CIMV2 path Win32_Printer GET Caption,Comment,DriverName,PortName,
PrintProcessor /value
```

```
Caption=HP5520_network (redirected 2)
Comment=
DriverName=HP Deskjet 5520 series
PortName=TS001
PrintProcessor=winprint
```

```
Caption=Microsoft XPS Document Writer
Comment=
DriverName=Microsoft XPS Document Writer v4
PortName=PORTPROMPT:
PrintProcessor=winprint
```

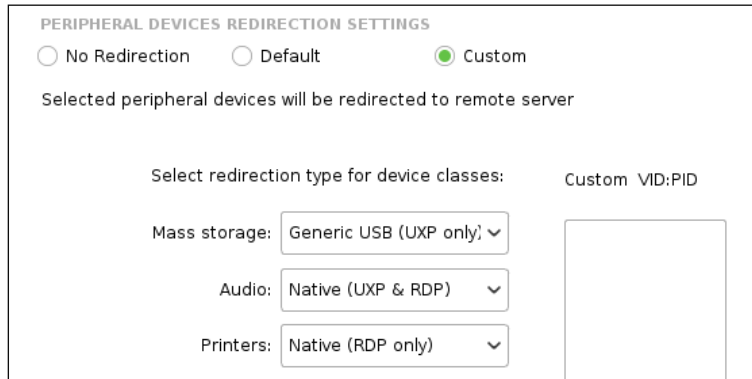
PortName like USB001 (which is not the expected behavior when trying to use the Native redirection) will indicate that the listed printer is a printer created locally on the Remote Desktop Session Host, or a printer forwarded with the Generic USB redirection method, instead of the Native method.

Cheapest GDI printers should be avoided when planning native redirection of printers. More advanced printers understanding the PCL, PostScript, and/or some other high-level page description languages are advisable and should work.

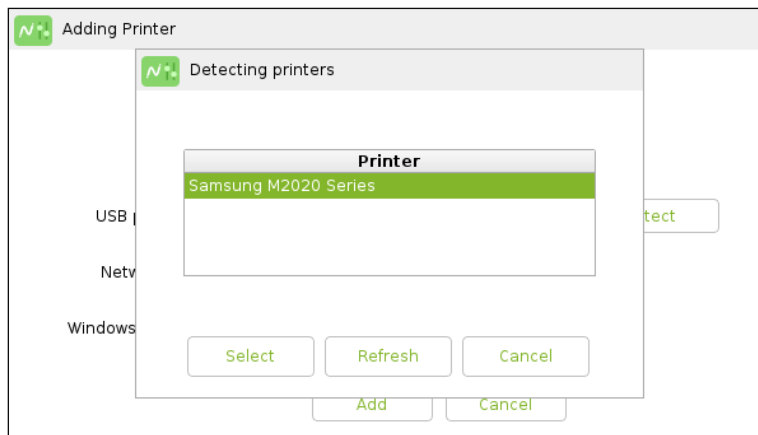
Adding a USB printer for native redirection

Follow the below steps to add a USB printer for the native redirection:

1. In the **Peripheral device redirection settings** settings group in the **Peripherals** section of Setup GUI select the **Custom** general redirection policy radio-button.
2. For the Printers class select the **Native (RDP only)** redirection type.



3. In the **Printers for native redirection** settings group click the [+] button.
4. Specify a printer **Name**. The name must not exceed 127 characters, must start with a letter and can only contain letters, digits, and the underscore (_) character.
5. Select **USB** as printer **Type**.
6. Provide a **USB printer identification** string. The **USB printer identification** string can be obtained from the connected USB printer by clicking the **[Detect]** button and selecting one from the list.



Clicking the **[Select]** button in the **Detecting printer** window copies the selected printer identification string into the **USB printer identification** and **Windows printer driver name** fields of the **Adding Printer** dialog window.

Adding Printer

Name: Samsung_M2020

Type: USB

USB printer identification: Samsung M2020 Series Detect

Network printer address:

Windows printer driver name: Samsung M2020 Series

Add Cancel

The **USB printer identification** information will be used to match the physically connected USB printers with the configured **Windows printer drivers**. This matching is necessary when multiple different USB printers are configured, will be connected, and must be redirected. When only one USB printer will be connected and redirected then the **USB printer identification** information does not need to be provided. Note that this is a new feature of the RX-series [firmware versions described in this book](#).

Even though the **Windows printer driver name** can be set automatically when detecting a printer there is no general rule saying that the Windows printer driver name is always the same as the identification string reported by the printer. In many cases the name of the Windows printer driver to be used for the redirected printer will have to be specified manually. This driver must be installed on the terminal server and will be used for rendering the print jobs forwarded to thin client device for local printing.

Adding Printer

Name: Samsung_M2020

Type: USB

USB printer identification: Samsung M2020 Series Detect

Network printer address:

Windows printer driver name: Samsung Universal Print Driver

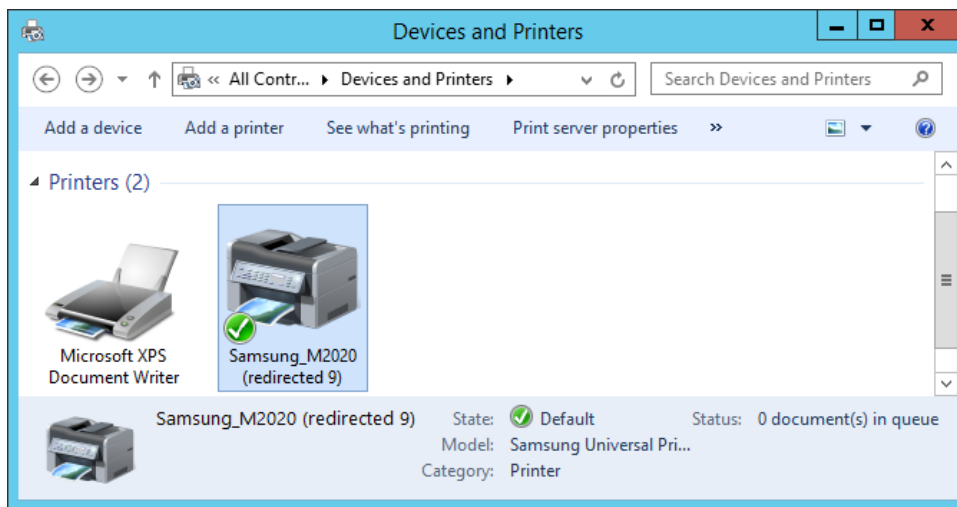
Add Cancel

7. Click the **[Add]** button.

The added printer will appear on the list and will be redirected to RDP sessions in RDP Client mode:

PRINTERS FOR NATIVE REDIRECTION			
Name	Type	Address/Identification	Windows printer driver name
Samsung_M...	USB	Samsung M2020 Series	Samsung Universal Print Driver 3

The Remote Desktop Session Host will create a session printer with the specified name and Windows driver:

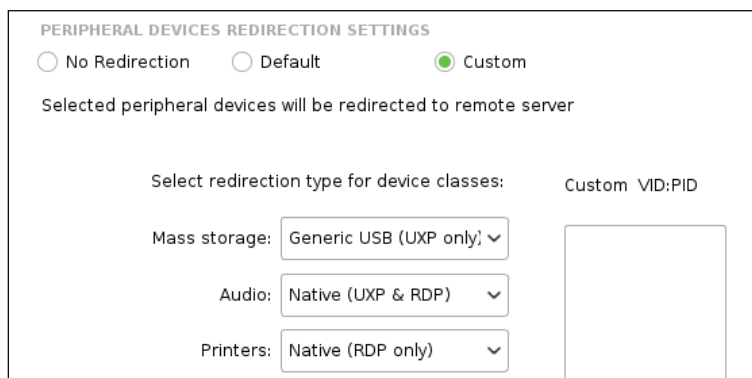


Adding a network printer for native redirection

Network printers supporting the JetDirect protocol (also referred to as RAW or AppSocket protocols) can be used with native redirection.

Follow the below steps to add a network printer for the native redirection:

1. In the **Peripheral device redirection settings** settings group in the **Peripherals** section of Setup GUI select the **Custom** general redirection policy radio-button.
2. For the **Printers** class select the **Native (RDP only)** redirection type.



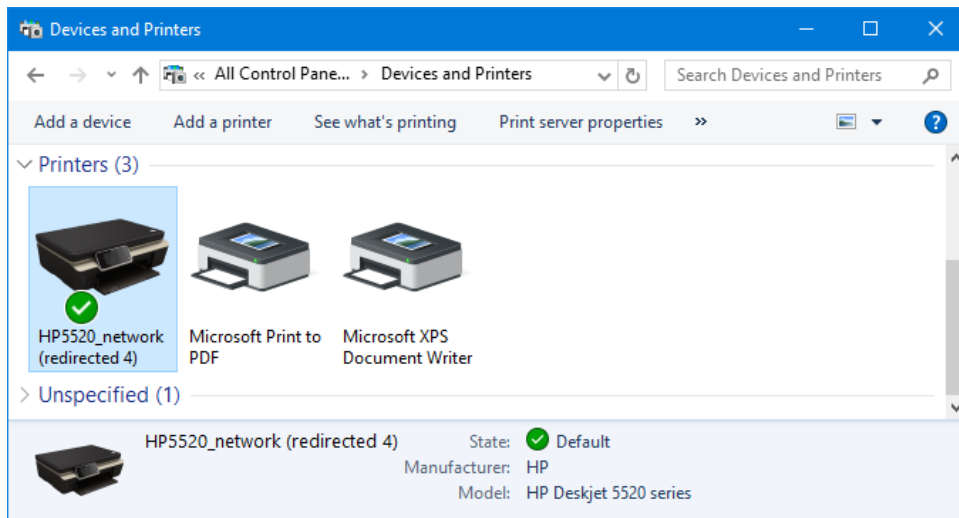
3. In the **Printers for native redirection** settings group click the [+] button.
4. Specify a printer **Name**. The name must not exceed 127 characters, must start with a letter and can only contain letters, digits, and the underscore (_) character.
5. Select **Network (JetDirect)** as printer **Type**.
6. Provide a **Network printer address**. This can be an IP address, hostname, or FQDN of the network printer.
7. Specify a **Windows printer driver name**. This driver must be installed on the terminal server and will be used for rendering the print jobs forwarded to thin client device for local printing.

8. Click the **[Add]** button.

The added printer will appear on the list and will be redirected to RDP sessions in RDP Client mode:

PRINTERS FOR NATIVE REDIRECTION			
Name	Type	Address/Identification	Windows printer driver name
HP5520_net...	Network (Jet...	10.0.0.106	HP Deskjet 5520 series
			+ -

The Remote Desktop Session Host will create a session printer with the specified name and Windows driver:

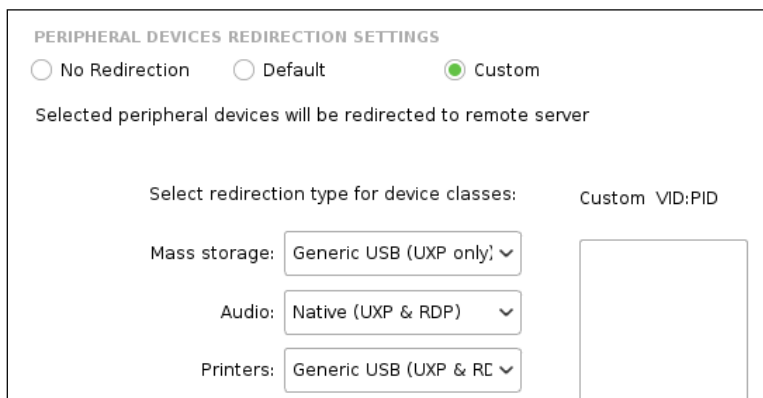


Removing printer from native redirection

To remove a printer from the list of printers configured for native redirection select the printer on the list and click the [-] button. Click the [OK] button to confirm the removal when asked.

4.8.9. Generic USB redirection of printers

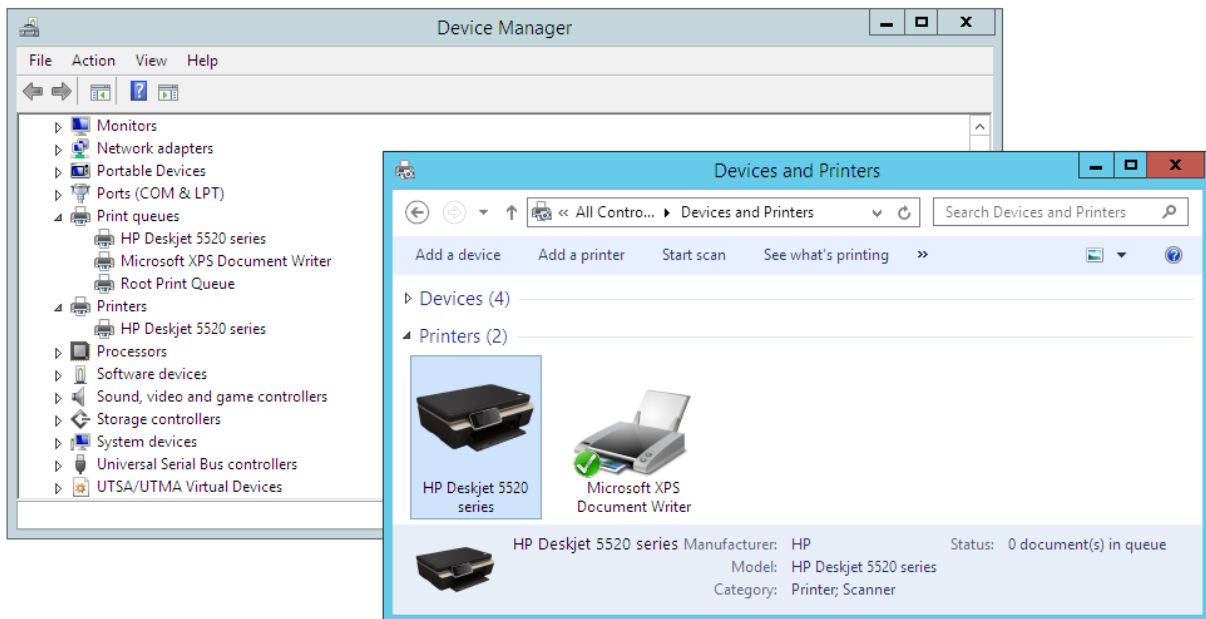
The **Generic USB** redirection of **Printers** is possible with both protocols: UXP and RDP.



The Generic USB redirection allows redirection of multi-function (MFD, MFP, all-in-one) devices which, besides the printer, also offer a document scanner, memory card reader, and/or other functionalities.

When the generic USB redirection will be used for printers then the low-level USB communication between the virtual USB hub created on the server side and the USB printer physically connected to the RX-series client or LEAF OS device will be redirected. The USB printer will be detected by a virtual USB host controller or hub assigned to the user's terminal session on the server side. The Windows USB printer driver necessary for the redirected printer must be installed on the terminal server hosting the user session.

The USB printer forwarded with generic USB redirection will appear in the Device Manager inside user's session.



The list of Windows printer drivers installed on a Windows machine can be obtained with following command:

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

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

Driver_name,driver_type,driver_architecture

For example:

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

```
Name  
Microsoft XPS Document Writer v4,4,Windows x64  
ZDesigner ZT230-200dpi ZPL,3,Windows x64  
Microsoft Shared Fax Driver,3,Windows x64  
HP Deskjet 5520 series,3,Windows x64
```

The list of printers created in terminal session can be obtained with following command:

```
wmic /Namespace:\\Root\CIMV2 path Win32_Printer GET Caption,Comment,DriverName,PortName,  
PrintProcessor /value
```

For the USB printers forwarded with the Generic USB redirection method the PortName property will be like USB001.

For example:

```
C:\>wmic /NameSpace:\\Root\CIMV2 path Win32_Printer GET Caption,Comment,DriverName,PortName,PrintProcessor /value
```

```
Caption=HP Deskjet 5520 series  
Comment=  
DriverName=HP Deskjet 5520 series  
PortName=USB001  
PrintProcessor=winprint
```

```
Caption=Microsoft XPS Document Writer  
Comment=  
DriverName=Microsoft XPS Document Writer v4  
PortName=PORTPROMPT:  
PrintProcessor=winprint
```

Additional considerations for UXP sessions

The vSpace Pro software contains the **Printer Management** feature, which improves the behavior of printers forwarded with the Generic USB redirection method.

Redirected printers' behavior without enabling the Printer Management

Printers physically connected to NComputing thin clients will be redirected to vSpace Pro server, but the underlying Windows operating system will be treating them in the same way as printers directly connected to the USB ports of vSpace Pro server host machine. This standard behavior includes creating printer object with standard name (hardcoded in printer driver) and standard user access control list (ACL). Standard ACL for printer objects includes the Allow Print permission for the Everyone user group.

The above results with following disadvantages:

- All system users, no matter from what clients they are connected, can see all client printers and also print on them.
- In environments with multiple thin-clients with locally connected printers each user can see dozens of printers redirected from different thin-clients.
- In case of multiple printers of the same model the system is creating the printers with the same name and adding the Copy 1, Copy 2, ... suffixes to differentiate the printers. User can potentially get a different copy of the printer assigned to his session every day.
- Printers from disconnected or logged off NComputing thin-client sessions are still visible as offline printers.
- Administrators and support personnel do not have any easy way to determine which printer belongs to what user or thin client.

Redirected printers' behavior with Printer Management enabled

The vSpace Pro server's Printer Management feature allows the following:

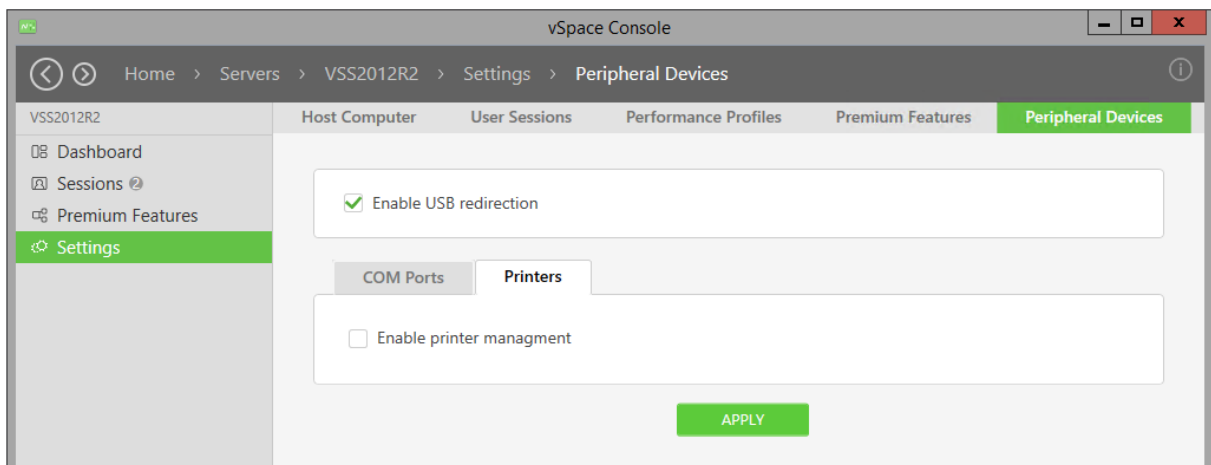
- Configuring the right user access control lists on the redirected NComputing thin-client printer objects to make sure that only the user running the session on the thin-client where

the printer is physically connected will be able to see and use the printer. Printers connected to other users' clients are not visible and not accessible.

- Dynamically changing printer names to reflect the session ID, name of the logged-on user and the device name of the thin-client device. This allows the administrators and support personnel to quickly and easily identify the printers.
- Mapping printer driver names. Users can see shorter and more friendly names for some printers.
- Automatically removing the offline printers.
- Using configurable rules for printer renaming, removal and becoming the default one.

Printer Management settings in vSpace Console

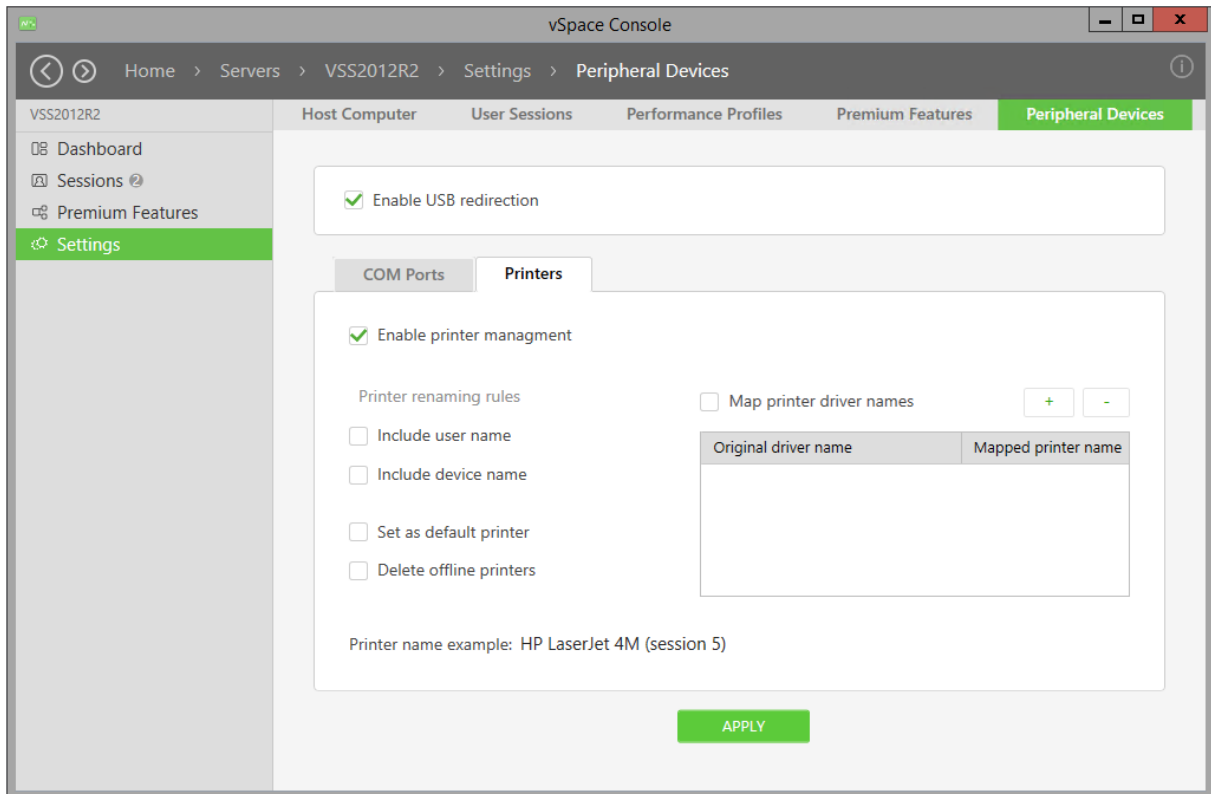
The Printer Management settings are available in vSpace Console for each vSpace Pro server on the 'Home > Servers > *ServerName* > Settings > Peripheral Devices' page. The Printer Management functionality depends on the **USB Redirection** feature, so the USB Redirection must be enabled for the Printer Management features to become available:



Enabling Printer Management

Printer Management is disabled by default. With Printer Management disabled vSpace Pro handles the printers in the standard, described above. To enable Printer Management the **Enable printer**

management checkbox must be selected. Otherwise the Printer Management settings will have no effect.



Configuring printer renaming rules

Printers handled by Printer Management will always be renamed to include the ID of the vSpace Pro session to which the printer belongs. For example, if the ID of a user session where an HP LaserJet 4M printer is connected is 5, then the new printer name will become 'HP LaserJet 4M (session 5)'. Following settings can be configured to additionally include user and device name when renaming the printer:

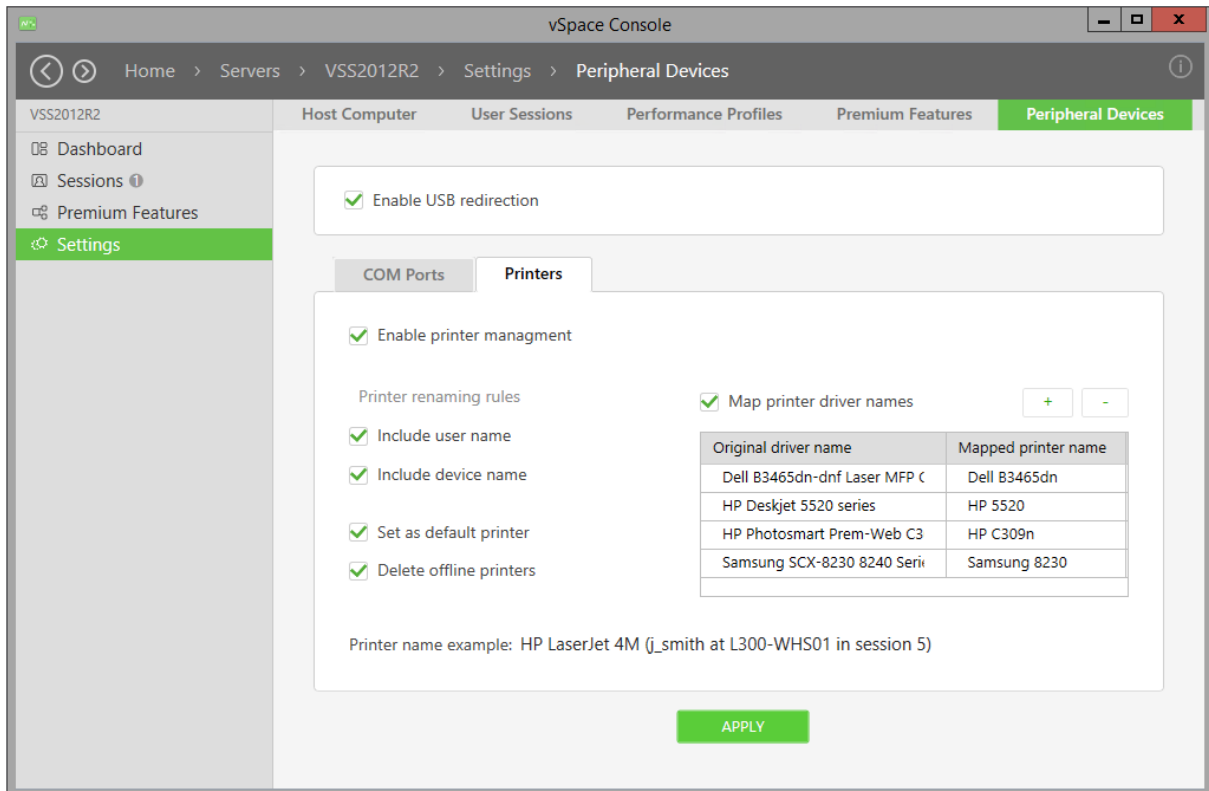
Setting	Function
Include user name	The user name will be additionally included in new printer name. Printer name will become for example: 'HP LaserJet 4M (j_smith in session 5)'.
Include device name	The thin-client's device name will be additionally included in new printer name. Printer name will become for example: 'HP LaserJet 4M (from RX300-WHS01 in session 5)'.

When both checkboxes will be selected then the user name and device name will be included in new printer name, which will be like: 'HP LaserJet 4M (j_smith at RX300-WHS01 in session 5)'.

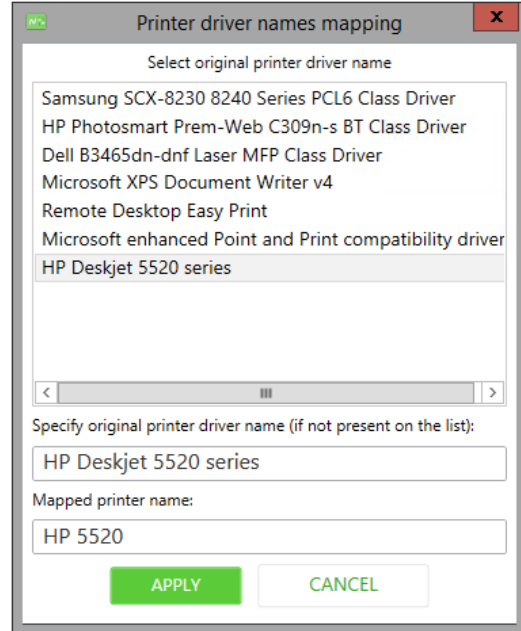
Configuring printer driver mappings

The original names of some printers created by Windows are long and sometimes contain redundant details. Printer driver mappings can be used to let the system use shorter or more user-friendly printer names for USB printers redirected from NComputing thin clients. To enable printer driver

mapping the **Map printer driver names** check-box must be selected. The [+] and [-] buttons located above the mapping list allow adding and removing printer driver mappings:



When adding a printer driver mapping the original driver name list shows all printer drivers installed on the managed vSpace Server. Windows uses this name when creating a new printer. When printer driver mapping will be enabled the vSpace Server, instead of using the original name, will rename the printer using the name specified as 'Mapped printer name'. For printer drivers not present on the list the original driver name can be specified manually.



Other printer management options

There are two other Printer Management options, which can be additionally configured:

Setting	Function
Set as default printer	With this option enabled the printer redirected from NComputing thin client will automatically become the default printer in the user session.

Setting	Function
Delete offline printers	Enabling this option lets system remove the printer when it will become offline. With this option enabled the printers will be automatically deleted when the NComputing thin-client user will log off or disconnect the session.

Printer Management example

Here is a real-life example of what Printer Management can do:

User session ID: 2

User name: demo1

Device name: L350-test

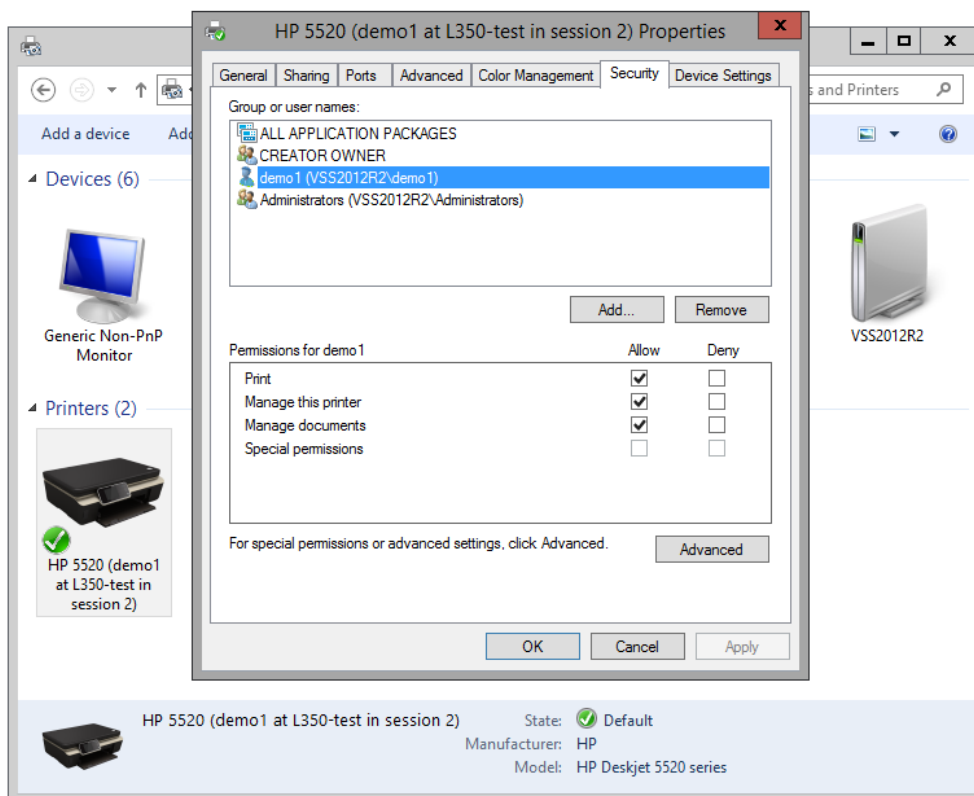
Include user name: enabled

Include device name: enabled

Printer driver name mapping: enabled

Mapping for the 'HP Deskjet 5520 series' printer driver: HP 5520

With all the above-mentioned options set the access control list of a sample printer may become like the following:



The 'demo1' user logged on from the L350-test thin-client, not the Everyone group, has the Print permission on this printer. Members of the Administrators group will always see and will be able to manage all printers. The printer has been renamed to 'HP 5520 (demo1 at L350-test in session 2)' according to configured printer renaming rules and printer driver name mapping settings.

Additional considerations for RDP sessions

For proper operation of the USB printers forwarded to Remote Desktop Session Hosts with the Generic USB redirection method and with the RDP protocol the SuperRDP Server Pack software must be installed on the host machine.

Note: [Additional requirements](#) and [limitations](#) apply when using the Generic USB redirection with RDP protocol.

4.8.10. Generic USB redirection of imaging devices

Generic USB redirection is the only method available to redirect the **Imaging devices** in RDP and UXP protocols. The **Imaging devices** device class includes (among others) the web cameras and document scanners.

PERIPHERAL DEVICES REDIRECTION SETTINGS

No Redirection Default Custom

Selected peripheral devices will be redirected to remote server

Select redirection type for device classes: Custom VID:PID

Mass storage: Generic USB (UXP only) ▼

Audio: Native (UXP & RDP) ▼

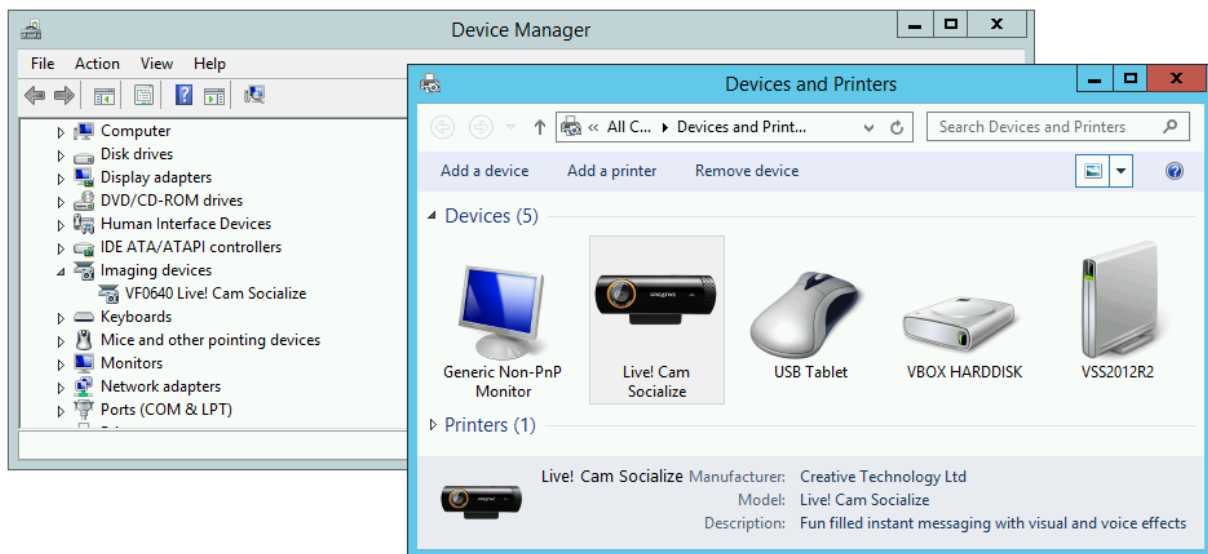
Printers: Generic USB (UXP & RC) ▼

Imaging devices: Generic USB (UXP & RC) ▼

+

Note: Although the document scanners fit into the Imaging devices category and the Generic USB redirection is currently the only available redirection method for them, they are known to be one of the most challenging devices to redirect. NComputing cannot guarantee that the document scanners forwarded with the Generic USB redirection will work properly. This especially applies to RDP sessions.

The redirected imaging device will appear in terminal session with its standard name. The device will be visible in Device Manager.



What needs to be considered is the fact that the redirected device (especially web cameras) produce big amounts of raw video data. In network bandwidth constrained environments, the possibility of some video frame drops must be considered.

Note: [Additional requirements](#) and [limitations](#) apply when using the Generic USB redirection with RDP protocol.

4.8.11. Native redirection of smart card readers

The RX-series firmware and LEAF OS contain the PC/SC daemon and a set of smart card reader drivers which allow the native (functional) redirection. CCID-compliant smart card readers and numerous ACS (Advanced Card Systems, Ltd.) smart card readers are supported with native redirection. Any number of thin clients can start the terminal sessions with native smart card reader redirection enabled. Please refer to RX300 or RX-RDP firmware Release Notes for full list of supported smart card reader models.

Enabling native redirection of smart card readers for UXP sessions

The **Native (UXP and RDP)** redirection type must be selected for the **Smart card readers** device class in **Peripheral devices redirection settings** settings group in the **Peripherals** section of Setup GUI to enable the native redirection of smart card readers for UXP sessions (in vSpace Client and VERDE VDI Client operation modes). Smart card support must be enabled on vSpace Pro server for the native redirection of smart card readers to work. Refer to vSpace Pro documentation for the information how to configure vSpace Server for the redirection of smart cards.

The 'certutil -scinfo' command can be used inside the UXP session to verify the operability of the redirected smart card reader and the smart card inserted into the reader. With well working redirection it will ask for card's PIN and display the certificate stored on the card.

Enabling native redirection of smart card readers for RDP sessions

The **Native (UXP and RDP)** redirection type must be selected for the **Smart card readers** device class in **Peripheral devices redirection settings** settings group in the **Peripherals** section of Setup GUI to enable the native redirection of smart card readers for RDP sessions (in RDP Client and VERDE VDI Client operation modes).

The 'certutil -scinfo' command can be used inside the RDP session to verify the operability of the redirected smart card reader and the smart card inserted into the reader. With well working redirection it will ask for card's PIN and display the certificate stored on the card.

4.8.12. Generic USB redirection of smart card readers

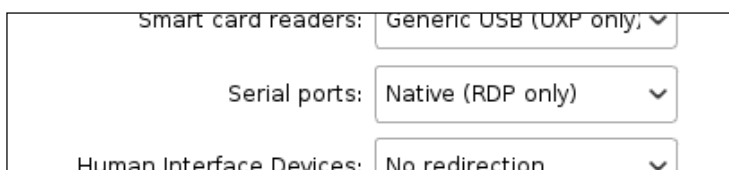
Generic USB redirection for smart card readers can be used with UXP sessions only (in vSpace Client and VERDE VDI Client operation modes). Unlike the native redirection of the smart card readers the generic USB redirection does not rely on the PC/SC daemon nor on any local smart card reader drivers. Smart card readers which are not supported with native redirection because of lacking firmware-side driver can work with generic USB redirection, although the total number of UXP sessions on one vSpace Server with that type of smart card reader redirection is limited to 10 only.

Smart card support must be enabled on vSpace Server for the generic USB redirection of smart card readers to work. Refer to vSpace Pro documentation for the information how to configure vSpace Server for the redirection of smart cards.

The 'certutil -scinfo' command can be used inside the UXP session to verify the operability of the redirected smart card reader and the smart card inserted into the reader. With well working redirection it will ask for card's PIN and display the certificate stored on the card.

4.8.13. Native redirection of serial ports

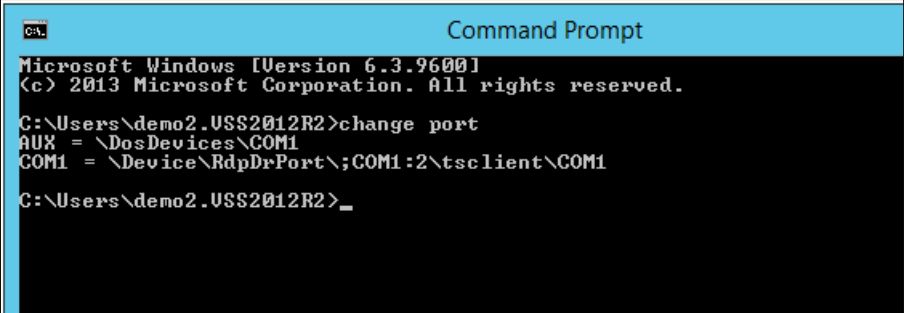
Native redirection of **Serial ports** is supported in RDP connections only.



The screenshot shows a settings window with three rows of dropdown menus. The first row is labeled 'Smart card readers:' and has a dropdown menu set to 'Generic USB (UXP only)'. The second row is labeled 'Serial ports:' and has a dropdown menu set to 'Native (RDP only)'. The third row is labeled 'Human Interface Devices:' and has a dropdown menu set to 'No redirection'.

The RX300, RX-RDP, RX420(RDP) firmware and LEAF OS contain drivers for numerous USB-to-serial adapters, including adapters based on the popular Prolific PL2303, FTDI, CH341 chips, among many others. The device firmware creates a local serial port which the RDP client redirects then in the functional way.

The 'change port' command can be used inside the RDP session to verify whether the serial port has been redirected properly. Command output similar to the below will confirm a successful redirection:



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\demo2.USS2012R2>change port
AUX = \DosDevices\COM1
COM1 = \Device\RdpDrPort\;COM1:2\tsc\client\COM1
C:\Users\demo2.USS2012R2>_
```

The serial port redirected with Native redirection will not appear in Device Manager of the terminal server machine.

4.8.14. Generic USB redirection of serial ports

Generic USB redirection of Serial ports is supported in UXP and RDP sessions.



Note: In RDP sessions the Generic USB redirection should only be used when the applications fail to communicate with the serial device through the serial port redirected in Native way.

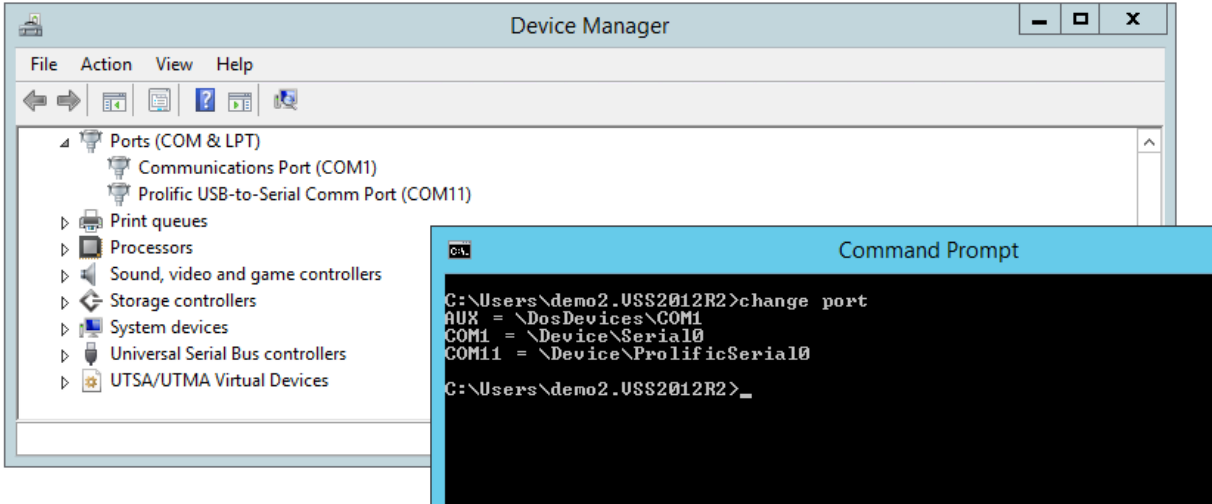
When the Generic USB redirection will be used for the serial ports then the low-level USB communication between the USB-to-serial adapter and virtual USB hub assigned to the user session on the terminal server machine will be sent over the terminal connection.

Some USB-to-serial adapters (e.g. the Prolific PL2303-based one used to illustrate examples contained in this book) appear on the USB bus as Vendor Specific Class devices. The RX-series firmware is unable to recognize such USB-to-serial adapters as serial ports. To enable the Generic USB redirection of such adapters their VID and PID numbers need to be [added to the Custom VID:PID list](#).



The USB-to-serial adapter redirected with Generic USB redirection will appear in Device Manager of the terminal server machine. The 'change port' command can also be used inside the UXP or RDP

session to verify whether the serial port has been redirected properly. Command output similar to the below will confirm a successful redirection:

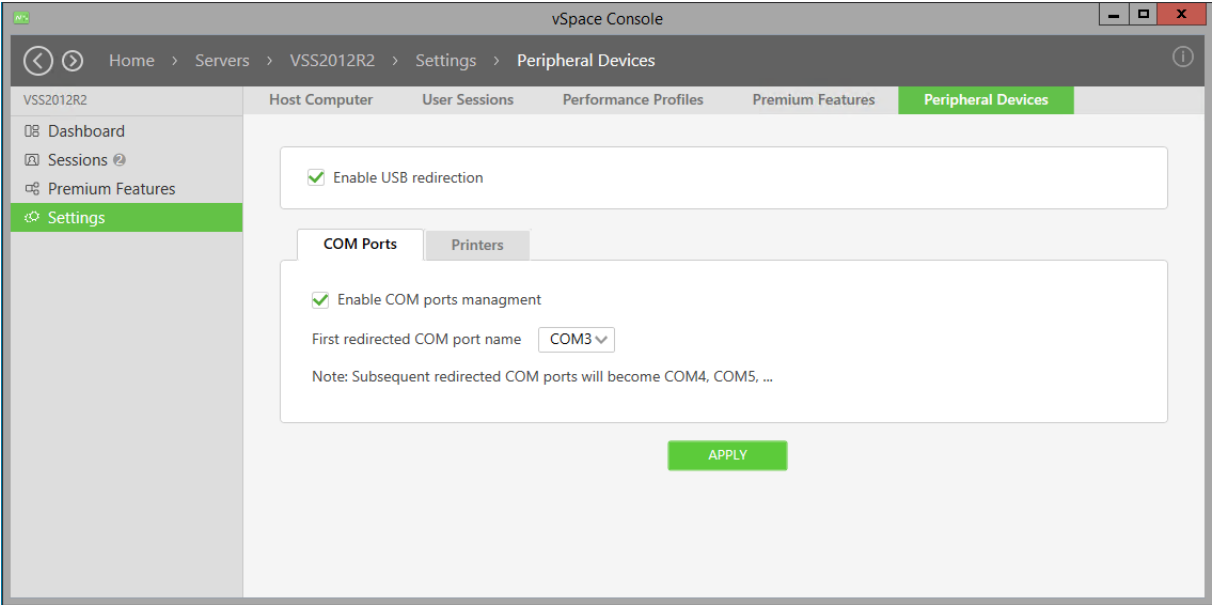


Note: [Additional requirements](#) and [limitations](#) apply when using the RDP protocol.

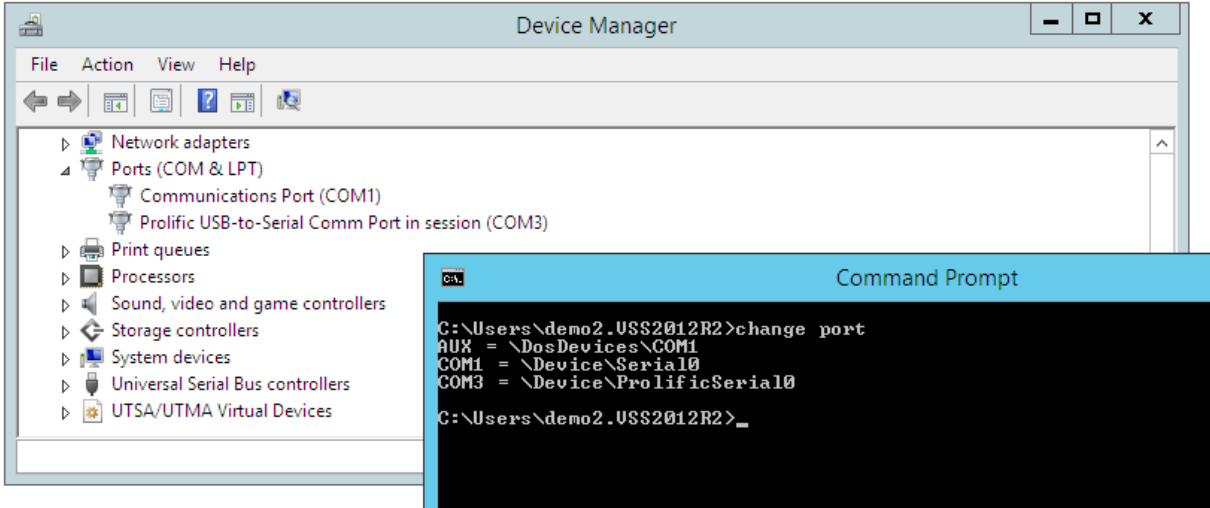
Optimizing the Generic USB redirection of serial ports in vSpace Pro systems

The drawback of the Generic USB redirection is the fact that the Windows OS can create the redirected serial ports using unpredictable numbers (COM9, COM11, ...) The same user connecting from the same device can get during subsequent logon differently numbered serial ports. Users connecting to same multiuser terminal server machine will surely get differently numbered serial ports. This can constitute a serious administrative challenge and make the configuration of application software installed on the terminal server difficult. The vSpace Pro system contains the 'COM port management' feature which allows mitigating the above described issue.

The number used for the first redirected COM port can be selected in vSpace Console, under 'Servers > Server > Settings > Peripheral Devices':



With this feature enabled the serial ports redirected from vSpace Client devices will be created starting with the selected number (e.g. COM3). All users of the vSpace Pro server (even connected concurrently) will get the redirected serial ports with the selected name. This will greatly simplify the configuration of the application software which will need to access the serial device, as the same system-wide settings can be used for all users.



4.8.15. Generic USB redirection of human interface devices

In current RX300, RX-RDP and RX420(RDP) firmware versions it is advisable to not use the generic USB redirection for human interface devices, as it can cause unintentional redirection of the thin client’s system keyboard and mouse too, which in turn will cause inability to use the keyboard and mouse after starting the terminal session. If a human interface device other than keyboard and mouse really needs to be redirected, the custom USB device redirection should be used, as described in next sections.

4.8.16. Native redirection of touchscreen displays

Although the touchscreen displays (which also includes multitouch screens and interactive whiteboards/smartboards) are usually Human Interface Devices (HID devices) there is no general **Native** selection for the whole **Human Interface Devices** class. This is because HID is a very wide class and developing a universal native redirection method covering all HID devices is technically impossible. For that reason, a dedicated checkbox has been added for controlling the native redirection of the (multi)touch screen monitors: **Enable native redirection for touchscreens**. This checkbox must be selected to enable native redirection of touchscreens. This method works with both supported protocols: UXP (vSpace Client mode, VERDE VDI Client mode) and RDP (RDP Client mode, VERDE VDI Client mode).



4.8.17. Native redirection of HID DigitalPersona fingerprint readers

Note: This feature is not available on LEAF OS.

Native redirection of HID DigitalPersona fingerprint readers can be enabled by selecting the **Enable HID DigitalPersona fingerprint readers** checkbox:

Human Interface Devices: <input type="text" value="No redirection"/>	<input checked="" type="checkbox"/> Enable HID DigitalPersona fingerprint readers
	<input type="checkbox"/> Enable native redirection for touchscreens

This method works with both supported protocols: UXP (vSpace Client mode, VERDE VDI Client mode) and RDP (RDP Client mode, VERDE VDI Client mode). vSpace Pro Enterprise version 12.3.6 (or newer) or latest guest tools in a VM controlled by VERDE VDI and accessed with the UXP protocol are required for the native redirection of HID DigitalPersona fingerprint readers to work in UXP sessions.

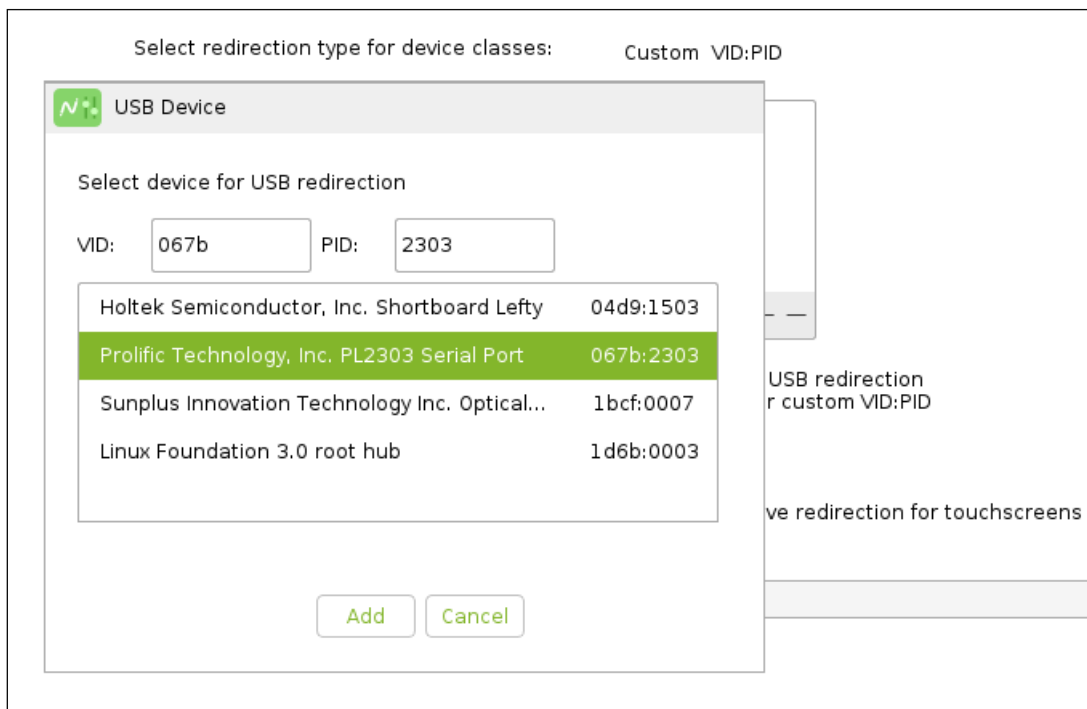
All USB fingerprint readers of HID DigitalPersona (identified by 05BA USB vendor ID) and Upek (identified by 147E USB vendor ID) should work. The HID DigitalPersona U.are.U 4500 fingerprint reader (VID:PID = 05BA:000A) has been tested and confirmed to work in all supported desktop virtualization environments.

Note: The VID:PID pair of the connected HID DigitalPersona fingerprint reader must not be added to **Custom VID:PID** list for the native redirection to work properly.

4.8.18. Generic USB redirection of custom devices identified by VID and PID

Some USB devices appear on the USB bus as so-called Vendor Specific Class devices (with 255 or 0xFF USB device or interface class code). Neither the RX-series firmware nor LEAF OS can properly categorize such devices as printers, smart card readers, audio, etc. To enable the Generic USB redirection for such devices the Vendor ID (VID) and Product ID (PID) numbers identifying the USB device need to be added to the **Custom VID:PID** list.

To add a USB device to the **Custom VID:PID** list click the [+] button located under the list and then specify the VID and PID values (as not prefixed hexadecimal numbers) or select the device from list of currently connected USB devices and press the [Add] button:



Note: Only generic USB redirection will be used for custom VID:PID devices. Generic USB redirection and Native redirection of peripheral devices are mutually exclusive! If the Native redirection method is selected for some USB device, then its VID and PID values must not be added to the **Custom VID:PID** list. Adding a USB device to **Custom VID:PID** list will most likely prevent the Native redirection!

Note: [Additional requirements](#) and [limitations](#) apply when using the Generic USB redirection with RDP protocol.

Removing USB devices from Custom VID:PID list

To remove a USB device from the list of custom devices configured for Generic USB redirection select the device on the list and click the [-] button.

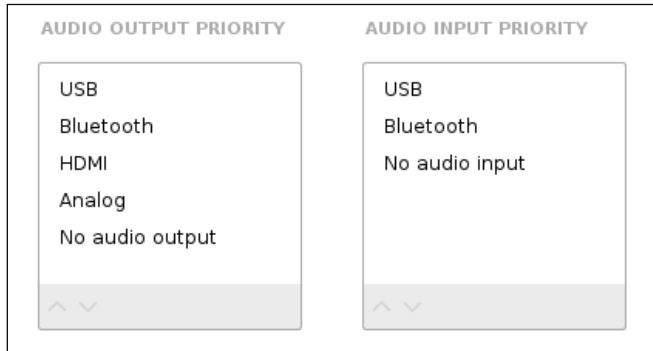
4.9. Audio settings

The settings which are configurable in the **Audio** section of the Setup GUI determine the physical audio device which will be used for the native redirection of audio into terminal sessions using the native method. Please refer to [Native redirection of audio devices](#) section for more information.

The RX300, RX-RDP and RX420(RDP) thin client device can play the sound through the built-in analog audio output. When the connected HDMI monitor is equipped with speakers then the HDMI interface can be used as audio output. Also, an external USB audio device can be used as audio output.

The RX-series devices do not have any built-in audio input. Using an external USB audio device is currently the only available audio input option.

The **Audio** Setup GUI section allows configuration of the order in which the firmware looks for audio output and input devices. The first device found will be used as audio output or input accordingly.



Note: Despite of the fact that the Bluetooth selections are available on the audio output and input priority lists the current RX30 and RX-RDP firmware does not support the Bluetooth audio devices.

With the default **Audio output priority**, the device firmware will select the USB audio device as audio output when a USB audio device will be detected. Otherwise an HDMI audio output will be used if an audio-capable HDMI monitor will be detected. Otherwise the built-in analog audio output will be used.

With the default **Audio input priority**, the device firmware will select the USB audio device as audio input when a USB audio device will be detected. In case of USB audio device absence, no audio input will be used.

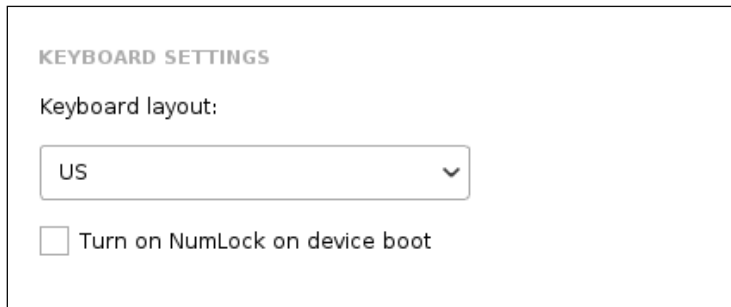
The enumeration of audio devices and the application of the audio output and input priority rules happens at the device boot as well as whenever a new (USB or HDMI) audio device will be detected. The administrator can change the output and input priority order by selecting an item on the list and clicking the [**▲**] or [**▼**] buttons located below the lists. E.g. to force the selection of the (always available) analog audio output, the **Analog** item should be moved to the top of the list. To disable audio output the **No audio output** item should be moved to the top of the list.

The **Show audio selection icons on the toolbar** checkbox controls the appearance of the speaker and microphone icons in the upper-right corner of the screen. These icons allow the user without administrative permissions to override the automatic audio device selection (which is based on the priority rules) and to select an audio output or input device of own choice.

4.10. Keyboard settings

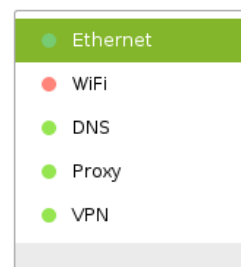
The keyboard layout settings configurable in the **Keyboard** section of the Setup GUI are only relevant for RDP sessions (in RDP Client and VERDE VDI Client modes). In vSpace sessions the default keyboard layout of the vSpace server will always be used. The RDP client component communicates the selected **Keyboard layout** to the remote terminal server and the servers configures that layout for user session.

The **Turn on NumLock on device boot** controls the initial state of the NumLock key when the device boots up.



4.11. Network settings

The **Network** section of Setup GUI allow the configuration of network settings. The parameters of the Ethernet and Wi-Fi interfaces, DNS, and Internet Proxy settings, as well as VPN settings, can be configured. The network settings sub-category can be selected through the sub-categories list located on the left-hand side.



4.11.1. Configuring the Ethernet interface

By default, the Ethernet interface is enabled and configured to obtain the IP parameters from a DHCP server.

Following Ethernet interface parameters are configurable:

- **Enable Ethernet interface** – enables the interface when the checkbox is selected and disables it otherwise.
- **IP Configuration** – **DHCP** or **Static**. With **DHCP** selected the IP address, network mask, the address of default gateway, the addresses of DNS servers, as well as the default DNS domain search suffix will be obtained from a DHCP server. This selection also allows automatic discovery of the [PMC address](#). With **Static** selected the above parameters can be specified manually.
- **Address** – the static IP address.
- **Network mask** – the static network mask.
- **Default gateway** – the static default gateway.

Hovering the mouse pointer over the Ethernet icon located in the upper-right corner of the screen displays current IP address of the Ethernet interface. The state of this icon provides additional information for the Ethernet interface:

- Absent icon – Ethernet interface is disabled.
- Icon with green dot – Successful Ethernet connection.
- Icon with yellow dot – Ethernet connected, but no IP address obtained from DHCP.
- Icon with red dot – Ethernet interface is enabled, but the cable is disconnected.

4.11.2. Configuring enterprise (802.1x) Ethernet settings

(Documentation to be provided)

4.11.3. Configuring the Wi-Fi interface

By default, the Wi-Fi interface is disabled on RX300 and RX-RDP devices. Following Wi-Fi parameters can be configured:

- **Enable Wi-Fi interface** – enables the interface when the checkbox is selected and disables it otherwise.
- **Network name (SSID)** – the Service Set Identifier (the name) of the Wi-Fi network. The name can be selected from the list when the Wi-Fi network broadcasts its SSID.
- **Hidden SSID** – selecting this checkbox allows manual specification of the **Network name (SSID)** for networks not broadcasting it.
- **IP configuration** – **DHCP** or **Static**. With **DHCP** selected the IP address, network mask, the address of default gateway, the addresses of DNS servers, as well as the default DNS domain search suffix will be obtained from a DHCP server. With **Static** selected the above parameters can be specified manually.
- **Address** – the static IP address.
- **Network mask** – the static network mask.
- **Default gateway** – the static default gateway.

The **[Edit WiFi]** button allows configuration of Wi-Fi network security settings.

- **Open** – the network is open and does not use any security nor encryption.
- **Personal** – must be selected when the network uses Personal security. The network's pre-shared **Password** needs to be provided to connect to the Wi-Fi network. The Wi-Fi Protected Access (WPA) type and encryption type will be detected automatically.
- **Enterprise (802.1x)** – needs to be selected to connect to an Enterprise Wi-Fi network.

Following Enterprise Wi-Fi settings can be configured:

- **Advanced security** – the Wi-Fi Protected Access (WPA) type selection: Auto, WPA, WPA2.
- **Encryption** – the Wi-Fi encryption to be used: Auto, TKIP, CCMP/AES.
- **Authentication method** – the user/client authentication method to be used: PEAP, TTLS, TLS.
- **User name** – the name of the Wi-Fi network user for PEAP, TTLS, or TLS authentication methods.
- **User password** – the Wi-Fi network user password for PEAP or TTLS authentication methods.
- **CA certificate** – the [Certification Authority certificate](#) to be used for verification of the certificate of the Access Point and/or client certificate.
- **Client certificate** – the [Client \(PKCS #12\) certificate](#) of the Wi-Fi device or user.
- **Private key password** – the password for accessing the private key of the client certificate.

Hovering the mouse pointer over the icon displays current IP address of the Wi-Fi interface, the Wi-Fi network name (SSID) and signal strength.

- Absent icon – Wi-Fi interface is disabled.

- Icon with green dot – Successful Wi-Fi connection.
- Icon with yellow dot – Connected to Wi-Fi access point, but no IP address obtained from DHCP.
- Icon with red dot – Wi-Fi interface is enabled, but there was a problem with Wi-Fi access point association.

4.11.4. Configuring DNS settings

By default, the addresses of DNS servers and the DNS domain name search suffix will be obtained automatically from a DHCP server. The DNS parameters can also be specified manually:

- **DNS configuration** – **DHCP** or **Static**. With **DHCP** the DNS parameters will be obtained automatically. **Static** allows manual specification of the parameters.
- **DNS Server 1** – the IP address of first DNS server.
- **DNS Server 2** – the IP address of second (optional) DNS server.
- **Domain name** – the DNS domain name search suffix.

Note: The DNS configuration can only be obtained from a DHCP server when at least one network interface (Ethernet or Wi-Fi) is configured to obtain its parameters from a DHCP server too. When both network interfaces use static (manual) configuration also the **DNS configuration** must be set to **Static** and the DNS parameters must be specified manually.

4.11.5. Configuring Internet Proxy settings

In some restricted network environments direct access to the Internet is blocked and the network devices must go through a proxy server to access the Internet. The RX-series devices need to communicate with the Internet when using the vCAST Web Streaming technology in vSpace (UXP) sessions or in RDP sessions on RD Session Hosts with the NComputing SuperRDP Server Pack extension software installed. Also, the PMC device management server or the web or FTP server hosting the device firmware can be placed in the Internet. The RX-series devices connected to restricted networks can use an Internet Proxy in the above-mentioned scenarios.

Following Internet Proxy settings can be configured:

- **Proxy settings** – **No proxy** or **Use proxy**. **No proxy** (which is the default setting) should be selected when unrestricted (direct) Internet access is possible. **Use proxy** must be selected when Internet connections must go through a proxy server.
- **Address** – the address of the proxy server. Can be specified as a hostname, FQDN, or IP address.
- **Port** – the port number of the proxy server.
- **User name** – name of the proxy user when the proxy server requires user authentication.
- **Password** – proxy user's password.

Note: The specified Internet proxy will be used for HTTP, HTTPS, and FTP connections.

4.11.6. Configuring VPN connections

The RX300, RX-RDP, RX420(RDP) and LEAF OS devices support OpenVPN, OpenConnect (which allows connections to Cisco AnyConnect VPN) and Point-to-Point Tunneling Protocol (PPTP) VPN

connections. To enable a VPN connection the **Enable VPN connection** checkbox must be selected. The desired **VPN type** must be selected in the combo-box. All VPN types can be configured in a way allowing the device to automatically establish the VPN connection (with the VPN credentials stored in device configuration) after booting up and connecting to Ethernet or Wi-Fi network. The devices can also be configured to establish the VPN connections with credentials provided by the user on the VPN logon screen. The OpenVPN connections can additionally be configured in a way allowing the user to provide the configuration file on a USB memory stick.

Configuring OpenVPN connection with configuration file provided by the user

The OpenVPN connection can be configured to let the user provide the configuration file (an .ovpn file) on a USB memory stick. The provided configuration file must be located in the root directory of a FAT-, NTFS-, ext3- or ext4-formatted USB stick. If the configuration (.ovpn) file refers to any other files, like client certificates, Certification Authority certificates, or private keys, then all those files must be copied to the root directory of the USB memory stick too. All files must be available as separate files. Compressed archives (ZIP, RAR, 7z, etc.), containing all files, are not supported.

OpenVPN connections using the user-provided configuration files can use following authentication methods:

- username and password,
- client certificate password,
- private key password,
- and combinations of them.

Following settings must be configured to enable OpenVPN and allow the user to provide the OpenVPN configuration file:

- **Enable VPN Connection** – this checkbox must be selected.
- **VPN type** – OpenVPN must be selected.
- **Let user provide the .ovpn and certificate files** – this checkbox must be selected.

The screenshot shows a configuration window with the following elements:

- Enable VPN connection
- VPN type: OpenVPN (dropdown menu)
- OpenVPN settings
 - Let user provide .ovpn and certificate files
 - Cache the .ovpn and certificate files
 - Cache the client certificate password and/or user credentials

For OpenVPN connections, for which the users will provide the configuration files, the following optional settings can be configured:

- **Cache the .ovpn and certificate files** – when selected, the device will copy from the USB memory stick to internal storage the user-provided .ovpn file and its associated certificate and/or key files, if necessary. This will allow reestablishing the VPN connection without the necessity to provide the memory stick with the files again.
- **Cache the client certificate password and/or user credentials** – when selected, the device will store the credentials provided by the user on the VPN logon screen and will automatically establish the VPN connection after reboot, without asking the user for any

credentials. This option can only be used when the **Cache the .ovpn and certificate files** option is selected too.

Note: Enabling the above options opens the VPN connection to anybody who will have physical access to the device, thus keeping them disabled increases the security of the VPN connection.

Configuring OpenVPN connection with all settings stored on the device

Preconfigured OpenVPN connections support VPN authentication with:

- username and password,
- client (PKCS #12) certificate (with password),
- username, user password and client (PKCS #12) certificate with password.

Following settings can be used to preconfigure an OpenVPN connection:

- **Enable VPN Connection** – this checkbox must be selected.
- **VPN type** – OpenVPN must be selected.
- **Let user provide the .ovpn and certificate files** – this checkbox must not be selected.
- **VPN server address** – the fully qualified domain name or IP address of the OpenVPN server.
- **Credentials type** – selection of authentication method. Depending on this selection the appropriate input fields will appear on the VPN logon screen. Possible selections:
 - Username and password
 - Client certificate
 - Username, password and client certificate

The screenshot displays the OpenVPN configuration interface. At the top, the 'Enable VPN connection' checkbox is checked. Below it, the 'VPN type' is set to 'OpenVPN'. Under the 'OpenVPN settings' section, four checkboxes are present: 'Let user provide .ovpn and certificate files', 'Let user provide VPN username and password', 'Let user provide VPN client certificate password', and 'Re-use VPN credentials for terminal sessions', all of which are unchecked. The 'VPN server address' is 'vpn2.company.com'. The 'Credentials type' is 'Username, password and client'. The 'User name' is 'VPNuser'. The 'User password' field is masked with dots. The 'CA certificate' is 'company.local Root CA'. The 'Client certificate' is 'OpenVPN Client #1'. The 'Client certificate password' field is also masked with dots. An 'Advanced Options' button is located at the bottom right of the configuration area.

- **Let user provide VPN username and password** – when selected, the device will display a VPN logon screen with username and password fields. When not selected, the username and password from device configuration will be used for VPN authentication.
- **Let user provide VPN client certificate password** – when selected, the device will display a VPN logon screen with prompt for client certificate password. When not selected, the client certificate password from device configuration will be used.
- **Re-use VPN credentials for terminal sessions** – when selected, the device will automatically attempt to authenticate the user (and possibly establish a terminal session) in the remote desktop environment depending on the selection of [device operation mode](#). The VPN logon

screen will additionally contain the **Domain** field when this option will be enabled. The username and password (without Domain) provided on the VPN logon screen will be used for VPN authentication. After successfully establishing the VPN connection the device will re-use the provided username and password combined with the specified of [preconfigured Domain name](#) to authenticate the user in the remote desktop environment and possibly start a terminal session for the user, if some kind of terminal session auto-start is configured.

Note: The **Re-use VPN credentials for terminal sessions** option is only meaningful when the **Let user provide VPN username and password** checkbox is selected.

- **User name** – the name of the VPN user. This setting is only meaningful when the **Let user provide VPN username and password** checkbox is not selected.
- **User password** – the password of the VPN user. This setting is only meaningful when the **Let user provide VPN username and password** checkbox is not selected.
- **CA certificate** – selection of an [uploaded Certification Authority certificate](#) used for verification of the certificate of the VPN server and/or of the client certificate.
- **Client certificate** – selection of an [uploaded Client \(PKCS #12\) certificate](#) used during VPN authentication.
- **Client certificate password** – password for the private key contained in the selected **Client certificate**.

Following advanced OpenVPN settings can be configured after clicking the **[Advanced Options]** button:

- **Protocol** – selection of the protocol to be used for the communication with the OpenVPN server. TCP or UDP.
- **Port** – number of the UDP or TCP port used for the communication with the OpenVPN server. Default value: 1194.
- **Authentication** – selection of the authentication algorithm. Possible selections: SHA1, SHA128, SHA256, SHA512, MD5, NONE.
- **Cipher** – selection of the cipher to be used for encryption of the OpenVPN communication. Possible selections: BF-CBC, AES-128-CBC, AES-256-CBC, NONE.
- **Custom parameters** – additional command line parameters, which will be passed to the OpenVPN client. If multiple parameters need to be passed, then they must be separated with the semicolon (;) character (without any whitespaces besides the semicolon). Please refer to OpenVPN documentation for the list of available command line parameters:
<https://openvpn.net/community-resources/reference-manual-for-openvpn-2-3/>

Configuring OpenConnect VPN connection

The OpenConnect VPN connection can be configured to allow RX300, RX-RDP, RX420(RDP) or LEAF OS users to connect to Cisco AnyConnect (or compatible) VPN servers.

OpenConnect connections support VPN authentication with:

- username and password,
- client (PKCS #12) certificate with password,
- username, password and client (PKCS #12) certificate with password.

Note: The **Authentication group**, supplementing the username- and password-based authentication (required by some Cisco AnyConnect VPN servers), can be specified under **Advanced Options**, when necessary.

Following settings can be used to configure an OpenConnect VPN connection:

- **Enable VPN Connection** – this checkbox must be selected.
- **VPN type** – OpenConnect must be selected.
- **VPN server address** – the fully qualified domain name or IP address of the VPN server supported by the OpenConnect VPN client (e.g. Cisco AnyConnect VPN).
- **Credentials type** – selection of authentication method. Depending on this selection the appropriate input fields will appear on the VPN logon screen. Possible selections:
 - Username and password
 - Client certificate
 - Username, password and client certificate

- **Let user provide VPN username and password** – when selected, the device will display a VPN logon screen with username and password fields. When not selected, the username and password from device configuration will be used for VPN authentication.
- **Let user provide VPN client certificate password** – when selected, the device will display a VPN logon screen with prompt for client certificate password. When not selected, the client certificate password from device configuration will be used.
- **Re-use VPN credentials for terminal sessions** – when selected, the device will automatically attempt to authenticate the user (and possibly establish a terminal session) in the remote desktop environment depending on the selection of [device operation mode](#). The VPN logon screen will additionally contain the **Domain** field when this option will be enabled. The username and password (without Domain) provided on the VPN logon screen will be used for VPN authentication. After successfully establishing the VPN connection the device will re-use the provided username and password combined with the specified of [preconfigured Domain name](#) to authenticate the user in the remote desktop environment and possibly start a terminal session for the user, if some kind of terminal session auto-start is configured.

Note: The **Re-use VPN credentials for terminal sessions** option is only meaningful when the **Let user provide VPN username and password** checkbox is selected.

- **User name** – the name of the VPN user. This setting is only meaningful when the **Let user provide VPN username and password** checkbox is not selected.
- **User password** – the password of the VPN user. This setting is only meaningful when the **Let user provide VPN username and password** checkbox is not selected.
- **CA certificate** – selection of an [uploaded Certification Authority certificate](#) used for verification of the certificate of the VPN server and/or of the client certificate.
- **Client certificate** – selection of an [uploaded Client \(PKCS #12\) certificate](#) used during VPN authentication.
- **Client certificate password** – password for the private key contained in the selected **Client certificate**.

Following advanced OpenConnect settings can be configured after clicking the **[Advanced Options]** button:

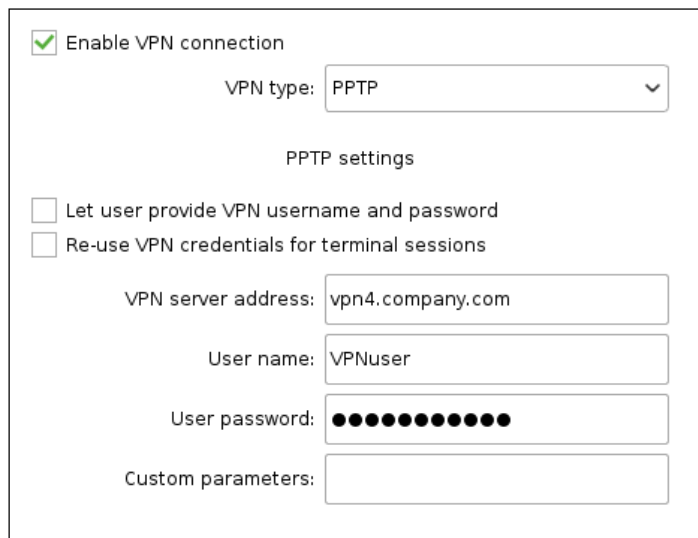
- **Server fingerprint** – fingerprint of the VPN server certificate. This optional parameter allows connections to VPN servers presenting an untrusted SSL certificate. The fingerprint needs to be specified as a string consisting of hexadecimal numbers, without any separators like colon (:) or dash (-). E.g.: 67D961FB719FFC8425635431F9A547BA62D4851D.
- **Authentication group** – the name of the authentication group required by some Cisco AnyConnect VPN servers.
- **Custom parameters** – additional command line parameters, which will be passed to the OpenConnect VPN client. If multiple parameters need to be passed, then they must be separated with the semicolon (;) character (without any whitespaces besides the semicolon). Please refer to OpenConnect VPN client documentation for the list of available command line parameters: <https://www.infradead.org/openconnect/manual.html>.

Configuring PPTP VPN connection

The RX-series and LEAF OS devices allow VPN connections based on the legacy but still used Point-to-point-Tunneling Protocol (PPTP). The PPTP VPN connections can be used with username- and password-based authentication only.

Following settings can be used to configure a PPTP VPN connection:

- **Enable VPN Connection** – this checkbox must be selected.
- **VPN type** – OpenConnect must be selected.
- **VPN server address** – the fully qualified domain name or IP address of the VPN server supported by the OpenConnect VPN client (e.g. Cisco AnyConnect VPN).
- **Let user provide VPN username and password** – when selected, the device will display a VPN logon screen with username and password fields. When not selected, the username and password from device configuration will be used for VPN authentication.



The screenshot shows a configuration window for a PPTP VPN connection. At the top, there is a checked checkbox labeled 'Enable VPN connection'. Below it, 'VPN type' is set to 'PPTP' in a dropdown menu. Under the heading 'PPTP settings', there are two unchecked checkboxes: 'Let user provide VPN username and password' and 'Re-use VPN credentials for terminal sessions'. Below these are four input fields: 'VPN server address' containing 'vpn4.company.com', 'User name' containing 'VPNuser', 'User password' which is masked with 12 dots, and an empty 'Custom parameters' field.

- **Re-use VPN credentials for terminal sessions** – when selected, the device will automatically attempt to authenticate the user (and possibly establish a terminal session) in the remote desktop environment depending on the selection of [device operation mode](#). The VPN logon screen will additionally contain the **Domain** field when this option will be enabled. The username and password (without Domain) provided on the VPN logon screen will be used for VPN authentication. After successfully establishing the VPN connection the device will re-use the provided username and password combined with the specified of [preconfigured Domain name](#) to authenticate the user in the remote desktop environment and possibly start a terminal session for the user, if some kind of terminal session auto-start is configured.
Note: The **Re-use VPN credentials for terminal sessions** option is only meaningful when the **Let user provide VPN username and password** checkbox is selected.
- **User name** – the name of the VPN user. This setting is only meaningful when the **Let user provide VPN username and password** checkbox is not selected.
- **User password** – the password of the VPN user. This setting is only meaningful when the **Let user provide VPN username and password** checkbox is not selected.
- **Custom parameters** – additional command line parameters, which will be passed to the PPTP VPN client. If multiple parameters need to be passed, then they must be separated with the semicolon (;) character (without any whitespaces besides the semicolon). Please refer to PPTP VPN client documentation for the list of available command line parameters: <https://manpages.debian.org/stretch/pptp-linux/pptp.8.en.html>.

4.12. Management settings

The **Management** Setup GUI section allows configuration of remote device management options. An administrator can remotely configure the RX300, RX-RDP, RX420(RDP), or LEAF OS device settings using vSpace Console or the PMC device management system. It is also possible to remotely shadow the device GUI and control it in that way.

4.12.1. Configuring remote device management settings

The availability of remote device management options depends on the configured [operation mode](#) of the device:

Operation mode	vSpace Console management	PMC management
vSpace Client	Possible	Possible
VERDE VDI Client	Impossible	Possible
RDP Client	Impossible	Possible
Raspbian Desktop (RX300 only)	Impossible	Impossible

Enabling vSpace Console management

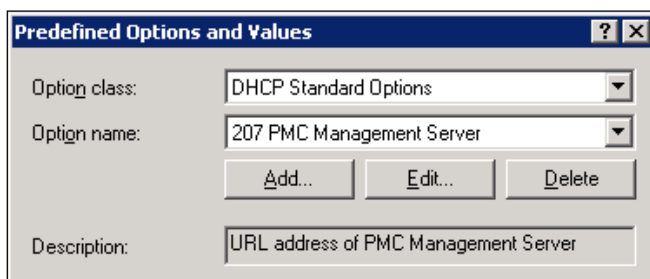
To enable device management from vSpace Console the **Enable vSpace Console management** checkbox needs to be selected.

Note: The vSpace Console can only manage a subset of RX300 and LEAF OS settings, mainly settings which are directly related to vSpace connections.

Enabling PMC management

To enable device management from the PMC device management system the **Enable PMC management** checkbox needs to be selected.

The RX300, RX-RDP, RX420(RDP) and LEAF OS devices can automatically discover the URL address of the PMC server when the **Automatically discover PMC address** radio-button is selected. 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>', where <PMC_address> must be replaced with the proper FQDN, hostname, or IP address of the PMC virtual appliance.



The address of PMC appliance can also be specified manually by selecting the **Use following PMC address** radio-button:

REMOTE DEVICE MANAGEMENT SETTINGS

Enable vSpace Console management

Enable PMC management

Automatically discover PMC address

Use following PMC address:

The PMC server URL can be specified in simplified or complete form. When a simplified URL will be specified then the device will expand it to create a complete one, e.g.:

Specified PMC URL	Expanded (complete) PMC URL
pmc	https://pmc:443
pmc.company.local	https://pmc.company.local:443
192.168.15.50	https://192.168.15.50:443
https://pmc.company.local	https://pmc.company.local:443
https://51.43.123.87:8443	https://51.43.123.87:8443

The same expansion rules apply to PMC URLs obtained through DHCP option 207.

4.12.2. Configuring VNC screen shadowing

Following settings can be used to configure VNC screen shadowing:

- **Enable VNC screen shadowing** – this is the general switch enabling or disabling this feature.
- **VNC screen shadowing mode** – **Full control** or **View only** can be selected. With **Full control** the shadower can interact with the device GUI. With **View only** only screen viewing will be possible.
- **Ask for user’s acceptance** – with this option enabled the user will be informed that someone is going to shadow the screen and the user will have the options to accept or reject the request.
- **Enable screen shadowing password** – this option allows setting up an additional password, which the shadower will have to provide to be able to view the screen or control the device.
- **VNC password** – is the password which will have to be specified by the shadower when the **Enable screen shadowing password** option is enabled.

VNC screen shadowing limitations on RX300 and RX-RDP devices

The VNC screen shadowing feature is mainly purposed to remotely view and control the local device GUI. When the RX300 or RX-RDP device is running a terminal session, some limitations apply, and the screen shadowing might end-up with a black screen being displayed in VNC viewer application. This happens because of the optimized (hardware-accelerated) display drawing methods used in some

scenarios. The display data bypasses the traditional frame buffer then and can't be shadowed with VNC.

Scenario	Primary screen shadowing	Secondary screen shadowing
Local device GUI, no SDA connected	Possible	N/A
Local device GUI, Pi0 SDA connected	Possible	N/A
Local device GUI, DisplayLink SDA connected	Possible	Possible
Local device GUI, N-series SDA connected	Possible	N/A
vSpace (UXP) session, no SDA connected	Impossible	N/A
vSpace (UXP) session, Pi0 SDA connected	Impossible	Impossible
vSpace (UXP) session, DisplayLink SDA connected	Impossible	N/A
vSpace (UXP) session, N-series SDA connected	Impossible	Impossible
RDP full-screen desktop session, no SDA connected	Impossible	N/A
RDP full-screen desktop session, Pi0 SDA connected	Impossible	Impossible
RDP full-screen desktop session, DisplayLink SDA connected	Possible	Possible
RDP full-screen desktop session, N-series SDA connected	Impossible	Impossible
RDP RemoteApp application session, no SDA connected	Possible	N/A
RDP RemoteApp application session, Pi0 SDA connected	Possible	N/A
RDP RemoteApp application session, DisplayLink SDA connected	Possible	Possible
RDP RemoteApp application session, N-series SDA connected	Possible	N/A

N/A – not applicable.

The above limitations do not apply to RX420(RDP) devices. Screens of these devices can always be shadowed with VNC.

4.13. Security settings

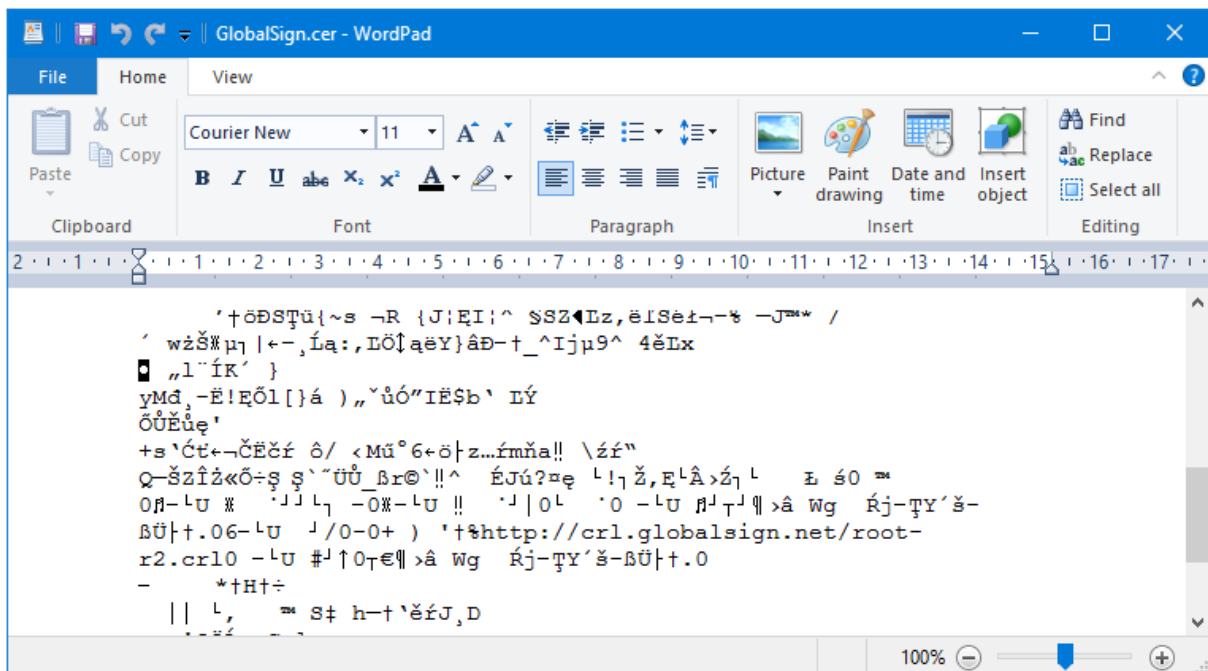
The **Security** settings allow the management of Certification Authority and Client (personal) certificates, which are necessary when setting up Enterprise (802.1x) Wi-Fi network connections.

Supported certificate file formats:

Certificate type	Supported certificate file format	Typical certificate file name extensions	Expected file name extension
Certification Authority (root or intermediate)	Base64-encoded X.509 (PEM)	.cer, .crt, .pem	.pem
Client	PKCS #12	.pfx, .p12	.p12

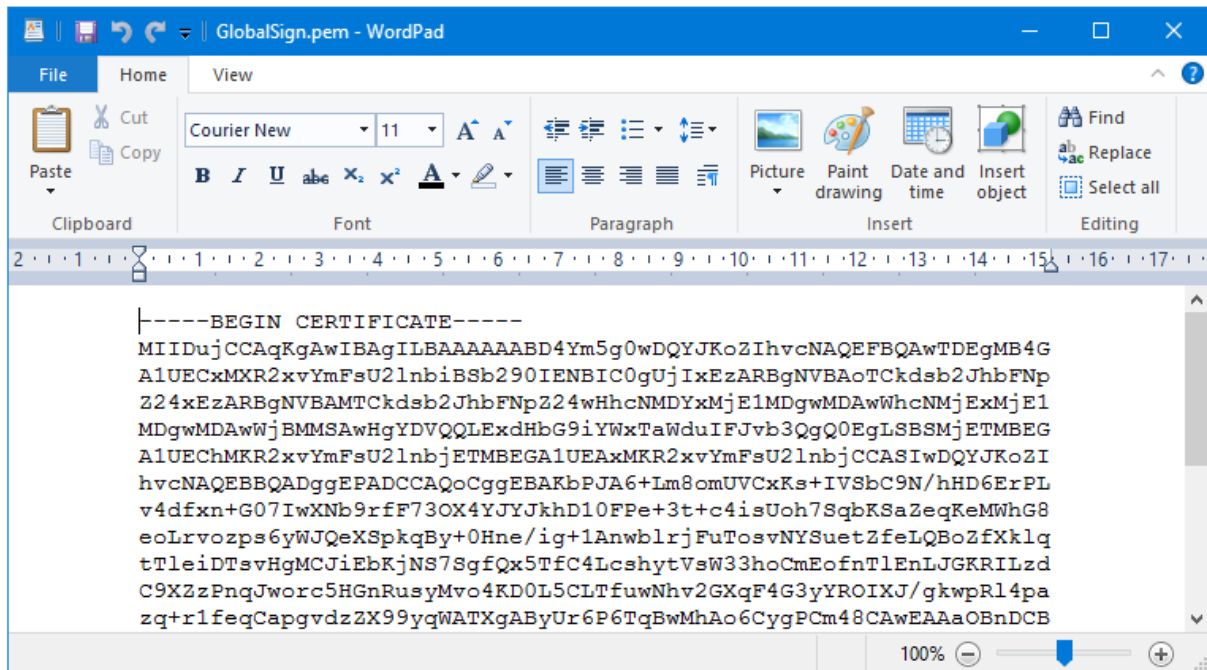
The file name extension of Certification Authority certificate file (like .cer, .crt, .pem, ...) actually says nothing about the real internal format of the certificate file. Microsoft Windows uses the .cer file name extension for the Base64-encoded X.509 (PEM) certificates as well as for the binary encoded X.509 (DER) certificate files. Real certificate file format can be quickly determined by opening the certificate file in a text editor, like WordPad.

If the file will contain random binary characters, then the file is in unsupported binary (DER) format:



If the file will contain nicely formatted ASCII characters only, will start with '-----BEGIN CERTIFICATE-----' header and end with '-----END CERTIFICATE-----' footer, then the file is in

PEM format and can be added as Certification Authority (root or intermediate CA) certificate to RX300 or RX-RDP thin client device:



Certificate files can be easily converted from DER to PEM format by opening them in Microsoft Windows, clicking the **[Copy to file]** button on the **Details** tab, and selecting the **Base-64 encoded X.509** format in next step.

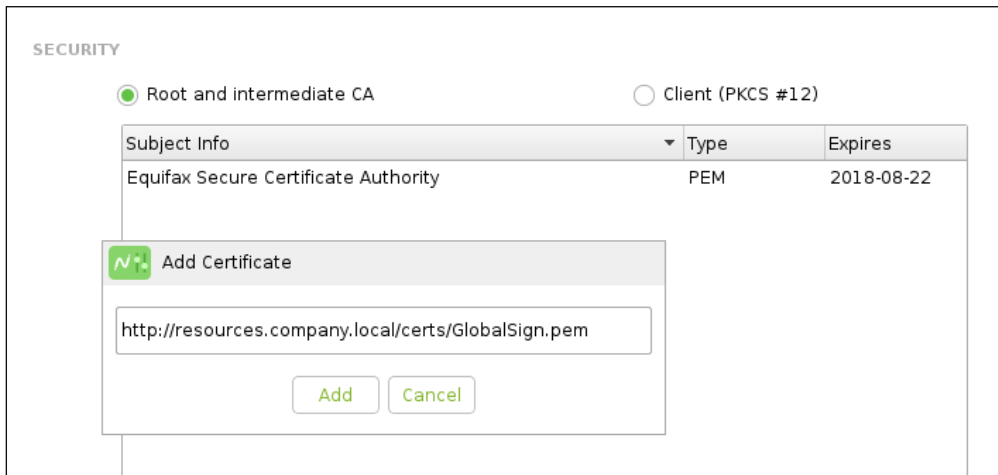
The certificate files to be added to the device must be uploaded to a web or FTP server and be accessible through HTTP, HTTPS, or FTP protocol.

4.13.1. Installing Certification Authority certificates

Follow the below steps to add a Certification Authority (root or intermediate CA) certificate:

1. Make sure that the CA certificate file uploaded to your web or FTP server is in PEM format has the .pem extension. Convert the file from DER to PEM format if necessary and change the file name extension to .pem if it is .cer or .crt.
2. In the Security section of Setup GUI select the **Root and intermediate CA** radio-button.
3. Click the **[+]** button located below the list of installed certificates.

4. In the **Add Certificate** dialog box enter the certificate file URL and click the **[Add]** button.



If a valid certificate file URL was specified, the device will confirm a successful certificate download.

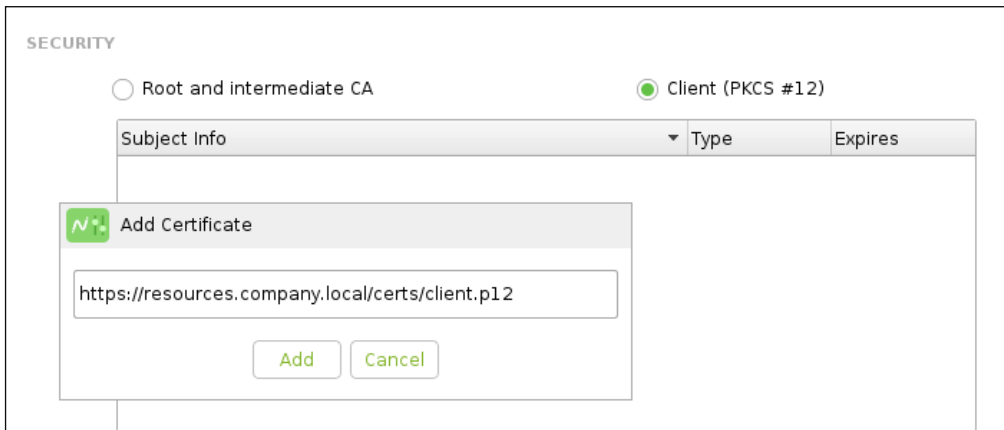
4.13.2. Installing Client certificates

Client (PKCS #12) certificates can be used for securing enterprise (802.1x) [Wi-Fi](#) and [Ethernet](#) connections, as well as [VPN connections](#).

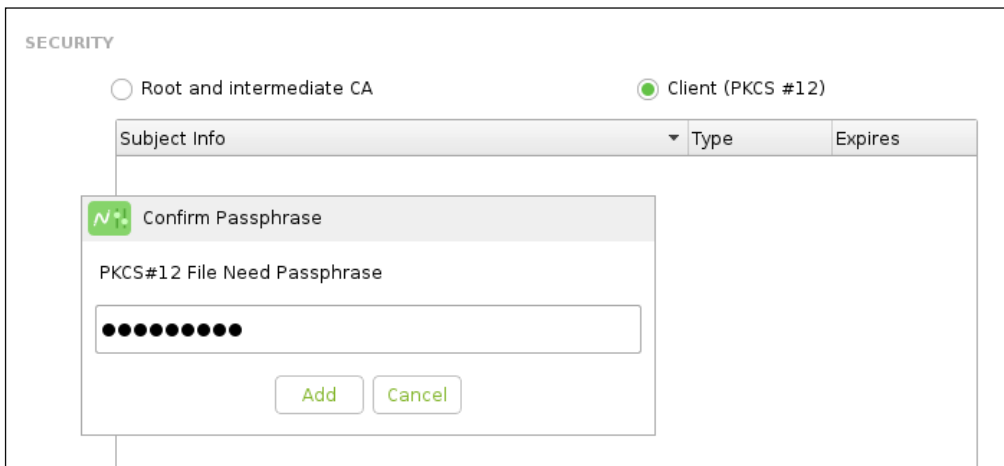
Follow the below steps to add a Client (PKCS #12) certificate:

1. Make sure that the certificate file uploaded to your web or FTP server has the .p12 extension. Change the file name extension to .p12 if it is .pfx.
2. In the Security section of Setup GUI select the **Client (PKCS #12)** radio button.
3. Click the **[+]** button located below the list of installed certificates.

4. In the **Add Certificate** dialog box enter the certificate file URL and click the **[Add]** button.



5. If a valid certificate URL was specified, the device will ask for certificate password. This password is required to open the certificate file and read from it the certificate details.



If correct certificate password was specified, the device will confirm a successful certificate download.

4.13.3. Removing certificates

To remove a certificate, select a certificate type (CA or Client), select the certificate to be removed on the list, and click the **[-]** button located below the list.

4.14. Support options

The **Support** section of Setup GUI contains firmware update and troubleshooting tools. The availability of firmware update tools depends on the selection of [device operation mode](#).

Operation mode	Availability of firmware update method			
	Update to the latest version available in LAN	Update from FTP/HTTP URL	Update from vSpace Server	Update from USB stick
vSpace Client (RX300 only)	Available	Available	Available	Available
VERDE VDI Client	Unavailable	Available	Unavailable	Available
RDP Client	Unavailable	Available	Unavailable	Available

4.14.1. Updating firmware to the latest version available in LAN

The **Update to the latest version available in LAN** option uses the UDP protocol to find in the local network a vSpace Server offering the newest RX300 firmware. The 'Multiuser Boot Server for Miniterm' service running in each vSpace Server handles the request and provides the firmware file.

4.14.2. Updating firmware from specified vSpace Server

The **Update from vSpace Server** option can be used to download a specific firmware file from specified vSpace Server. As in previous case the 'Multiuser Boot Server for Miniterm' service running in each vSpace Server handles the request and provides the firmware file. By default, the 'Multiuser Boot Server for Miniterm' service stores the firmware files in 'C:\Program Files\NComputing\vSpace Server Software\Bootsrv' folder of the vSpace Server. The RX300 **Firmware file** name is like 'rx300-3.6.0.upd'. The **vSpace Server** can be specified as a hostname, FQDN, or IP address.

4.14.3. Updating from FTP/HTTP URL

The **Update from FTP/HTTP URL** firmware update method is available in all device operation modes. The necessary firmware file needs to be uploaded to an FTP or web server before using this method and the file URL must be specified as **FTP/HTTP URL** parameter. The HTTPS protocol can be used too. If the web or FTP server requires user authentication, then the username and password can be provided through the dedicated input fields. These fields should be left empty for anonymous FTP or web server download.

4.14.4. Updating from a USB stick

The **Update from USB stick** firmware update method is available in all device operation modes. The firmware update package (.upd file) needs to be copied to the root directory of a USB stick formatted with FAT32, NTFS, ext3, or ext4 filesystem. The device will display two tables. First table will contain the list of connected USB mass storage devices, the second the list of firmware update package files found. The **[REFRESH]** button can be clicked to refresh the lists if a new USB stick was connected after selecting the USB-stick-based firmware update method.

The selected firmware update package will be installed after clicking the **[UPDATE]** button.

Device	Partition label or ID
/dev/sdb1	LINUX

REFRESH

Update package file name
rx300-3.7.0.upd

4.14.5. Collecting troubleshooting information

In case when NComputing Technical Support will have to be contacted to resolve any kind of technical issue with an RX-series device or LEAF OS system the troubleshooting logs should be collected on the affected device and provided to NComputing support representative. When preparing the troubleshooting file, the device will capture its current configuration, collect numerous logs, and use internal tools to obtain additional information about the current state of the device.

The logs should be collected with all related peripheral devices still connected, after reproducing the issue in terminal session, and before rebooting the device. The troubleshooting file will be saved then to a connected USB mass storage device.

Device	Filesystem	Partition label or ID
/dev/sda	vfat	FREECOM

COLLECT CANCEL

The troubleshooting logs collection process will be started after selecting a storage device and clicking the **[COLLECT]** button.

4.14.6. Resetting the device to factory defaults

The device can be reset to factory default settings by clicking the **[FACTORY RESET]** button in the **Troubleshooting** box of the **Support** section of Setup GUI.

4.15. Date and Time settings

The **Date and Time** setting allow the device to obtain the current date and time, which will be used by the system clock displayed on the task bar when the device operates as RDP Client with RemoteApp support enabled. The date and time will also be used when validating SSL certificates during Enterprise Wi-Fi connections.

Following settings are configurable:

- **Timezone** – the time zone where the device is located.
- **Set date and time automatically** – when enabled the date and time will be synchronized with the NTP server specified as **Time server**. When not enabled the administrator will have an option to set the date and time manually. As the RX300 and RX-RDP devices do not contain any battery-powered real-time clock the manually set date and time will get lost whenever the device will be rebooted.
- **Time server** – the NTP server to synchronize the date and time with.

4.16. Device status information (About)

The **About** section of the Setup GUI displays general information about the device and its current state, like the device model, its serial number, firmware version, the version of the device configuration, contained version of the RDP client, the IP and MAC addresses of Ethernet and Wi-Fi interfaces, as well as PMC connection status (including the current PMC server URL, when known).

5. Device recovery mode

5.1. Recovering the thin client partition

(Documentation to be provided)

5.2. Recovering the Raspbian partition

(Documentation to be provided)

5.2.1. Resetting the device to factory defaults

(Documentation to be provided)