Dell Wyse ThinLinux

Version 2.1 Administrator’s Guide

Notes, cautions, and warnings

ⓘ | **NOTE: A NOTE indicates important information that helps you make better use of your product.**

△ | **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ | **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

© 2018 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

2018 - 11

Rev. A00

Contents

1

Introduction

Wyse ThinLinux from Dell simplifies the user management paradigm with elegant application icons and comes with a single built-in user to enhance user experience along with having the benefits of a single-operating system. ThinLinux software combines the security, flexibility and market-leading usability of enterprise-grade Linux with Dell's thin computing optimizations in management. It is ideal for organizations that want to run server-based, Web-based or local applications including legacy applications without the deployment and security concerns of a nonstandard Linux distribution.

Topics:

- About this guide
- New features
- Supported platforms
- Dell Technical Support

About this guide

This guide is intended for administrators of thin clients running Dell Wyse ThinLinux. It provides information and detailed system configurations to help you design and manage a Dell Wyse ThinLinux environment.

New features

The following are the new features or enhancements delivered in this release:

- Added the USB Manager option to configure USB ports and devices.
- Added support to configure system network proxy settings using INI parameters.
- Added support to configure the Firefox proxy settings using INI parameters.
- Added support to configure system firewall settings using UI and INI parameters.
- Added support to hide the default desktop icons in user mode.
- Added support to download the wallpaper forcibly using INI parameters.
- Added the home button on Settings App.
- Added the Custom Info tab in System Settings.
- Updated Citrix Receiver Client to version 13.10.
- Updated VMware Horizon Client to version 4.8.
- Updated Google Chrome to version 68.0.3.
- Added support to enable or disable the system manual lock.
- Added support for Simple Certificate Enrollment Protocol (SCEP) on HTTPS.
- Added support for device mapping to access devices from a Citrix session.
- Added support to log in to Citrix Server using NetScaler Gateway.
- Added support to enable or disable features of Firefox and Chrome browsers using UI and INI parameters.

Supported platforms

This section provides the information about the supported platforms.

Table 1. Supported platforms

Hardware platform	Memory configuration—eMMC / RAM
Wyse 5070 thin client—Celeron Processor	16 GB / 4 GB
Wyse 5070 thin client—Pentium Processor	16 GB / 4 GB

Dell Technical Support

To access Dell Wyse technical resources, visit www.dell.com/support/contents/us/en/19/article/Product-Support/Dell-Subsidiaries/wyse. For more information, you can submit cases to Dell TechDirect or contact Dell at www.dell.com/support/contents/us/en/04/category/contact-information.

Related documentation and services

Fact sheets containing features of the hardware products are available on the Dell Wyse website. Go to www.dell.com/wyse and select your hardware product to locate and download the fact sheet.

To get support for your Wyse product, check your product Service Tag or serial number.

- For Dell service tagged products, find knowledge base articles and drivers on the Dell Wyse product pages.
- For Non-Dell Service Tagged Products, find all the support needed by accessing the www.dell.com/support/contents/us/en/04/article/Product-Support/Self-support-Knowledgebase/Dell-Subsidiaries/wyse.

Dell Online Community

Dell maintains an online community where users of our products can seek and exchange information about user forums. Visit the Dell Online Community forums at Dell.com/community.

2

Getting started

Use the following information to learn the basics and get started using your thin client:

- Logging in to your thin client device
- Using your ThinLinux desktop
- Configuring thin client settings and connections
- Viewing system information
- BIOS settings

Logging into your thin client device

On your initial configuration, Dell recommends that you connect by using a wired connection by plugging in the network connected Ethernet cable to your thin client.

After you turn on your thin client, you are automatically logged in to the thinuser account. The default password of the thinuser account is **thinuser**. For information about changing the default password, see Managing the account settings.

ⓘ NOTE: **If a GDM login is needed (for example, AD/Domain login, PNAgent login, and so on), the autologin option can be turned off through the GUI or by using the INI parameter.**

Admin mode enables you to perform system administration tasks such as adding or removing connections and setting up specific device settings. To switch to admin mode, click the **Switch to Admin** button on the Settings application screen and enter the default root password in the **Authentication required** window. The default root password is **admin**. For information about changing the default password, see Managing the account settings.

You can press Ctrl + Shift + Alt + F11 to switch to admin mode.

Application overview screen

ThinLinux boots to the application overview screen. This is the default ThinLinux screen that is displayed after you log in to the thin client (without auto-start of any connections or application).

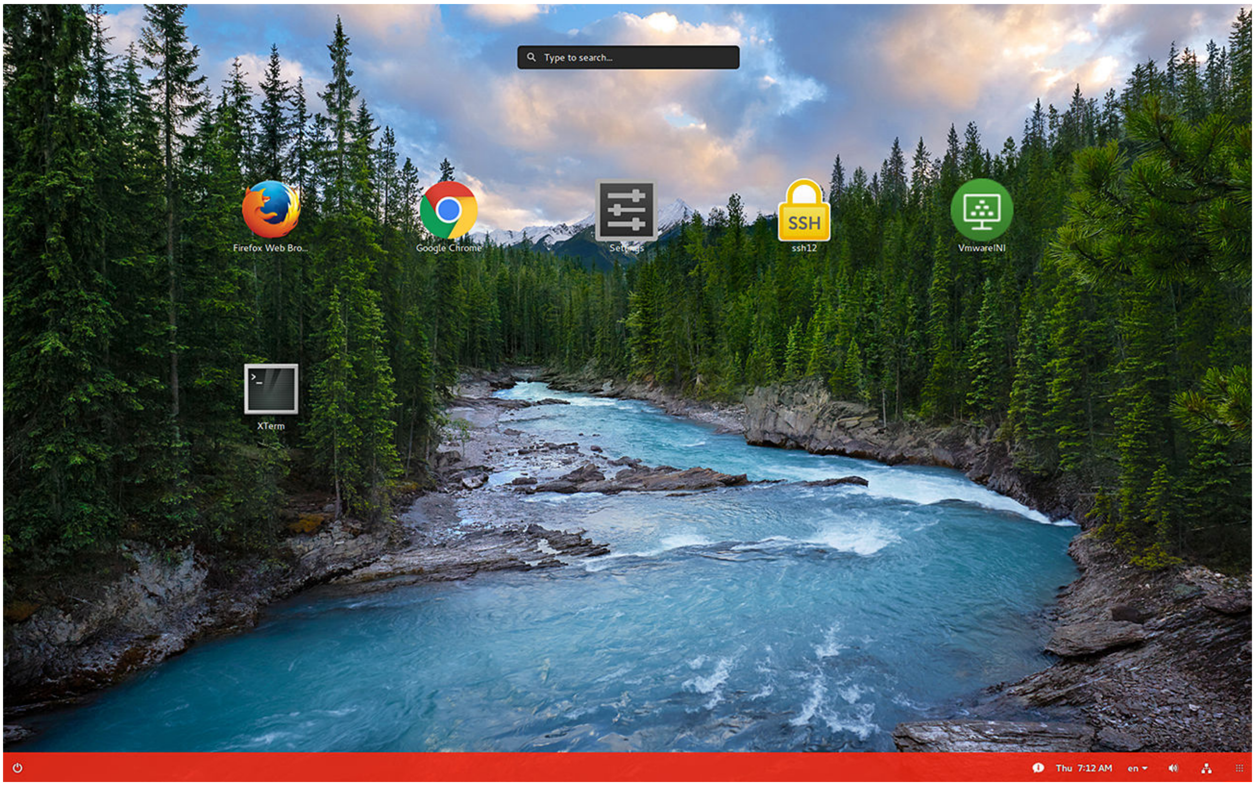


Figure 1. Application overview screen

- **Application Icons**—To access the application icons, click the dots on the lower-right corner of the screen. You can start the application by clicking a particular application icon. If there are more application icons, the icons are displayed on multiple pages.
- **Taskbar**—The taskbar is displayed at the bottom of the Application overview screen (ThinLinux desktop).

The Application overview screen consists of the following screen elements:

- **Search entry**—User can search for applications by typing the application name in the **Search** text box.
- **Multi-displays**—This is only applicable when you want to set up multiple displays. The Application overview screen icons are displayed only on the primary display. On the rest of the connected displays, only background is displayed. For example, if an application is running on the secondary display in the desktop view, a thumb nail of the application is displayed on the secondary display on the Application overview screen.
- **Firefox browser**—Starts the Mozilla Firefox web browser.
- **Chrome browser**—Starts the Google Chrome web browser.
- **Settings App**—The Settings Application is the integrated application for system settings in both user and admin mode. This application icon is displayed in the **Application overview screen** upon system startup in both user and admin mode.
- **XTerm**—XTerm is the standard terminal emulator for the X Window system. Use the terminal emulator window for X to access a text terminal and all its applications such as command line interfaces (CLI) and text user interface applications. It is applicable for admin mode.

Desktop view—This is the desktop view for running applications. The desktop automatically switches to the **Desktop view** mode when you launch any application. The system remains in this desktop view if there is at least one open window. When all the system windows are closed, the system automatically switches back to the Application overview screen.

On multiple displays by default, the primary monitor displays the running applications and the rest of the connected monitors display the background. You can move the application from the primary monitor to the rest of the monitors or from the rest of the monitors to primary monitor. To switch between the desktop screen and Application overview screen, click the **Show Desktop** button.

System lock—To manually lock your thin client, press CTRL + ALT + L or Win + L.

Using the taskbar

Use the taskbar to view the time, configure the volume settings, view system information, view network information, shutdown the thin client, view keyboard settings and switch to desktop screen.

The taskbar consists of quick launch icons and taskbar buttons:

- **Show Desktop** – Click this button to switch between the Desktop view screen and Application Overview Screen.
- **Shutdown** – Use this button to shut down or restart the thin client. If you click this button, the Power Off dialog box is displayed. If you do not select any option in the dialog box, the system will automatically power off in sixty seconds. You can cancel the power off by clicking the Cancel button. You can restart or Power Off the thin client by clicking the respective buttons.

  ⓘ NOTE: **When auto-login is disabled or if the user has switched to the admin mode, a logout button is displayed in the Power Off dialog box and you can log out by clicking this button.**
- **Activities** – The application icon is added to the taskbar whenever a new application is started. Taskbar displays a single icon for a single running application. If multiple instances of the same application are running, multiple icons are displayed in the Taskbar. Hover the mouse pointer over the Taskbar to view the tooltip for application name. The icon of the current running application that is in focus is highlighted in the taskbar.
- **Date and Time** – Use this icon to view the date and time.
- **Volume icon** – Use this option to increase or decrease the speaker volume or mute the speaker.
- **Network icon** – Use this icon to view the Network details.
- **Keyboard icon**– Click this icon to view the available keyboard layout. You can switch between the keyboard layouts using this option.
- **System Information** – Use the System Information screen to view Identity, Network, Packages, and Copyright information. For more information, see Viewing System Information.

Viewing system information

Use the **System Information** UI to view the Identity, Network, Packages, and Copyright information.

To view your system information, click the **System Information** icon on the taskbar.

The **System Information** dialog box displays the following information:

- **Identity tab**—Displays identity information such as:
  - **System**
    - Current User
    - Terminal Name
    - Product Name
    - Platform
    - Build
    - Build Revision
    - OS Version
    - Uptime
  - **Hardware**
    - Processor
    - Processor Speed
    - Total Memory
    - Free Memory

        - Media Size
        - Serial Number
    - **BIOS**
        - BIOS Version
    - **Custom Info**
        - Location
        - Contact
        - Custom 1
        - Custom 2
        - Custom 3

- **Network tab**—Displays network information such as:
    - **Network Device**—**eth0** and **wlan0**
    - **Interface Information**
        - MAC address
        - Network Speed
        - Maximum Transmission Unit (MTU)
    - **IP Information**
        - IP Address
        - IPv6 Address
        - Subnet Mask
        - Gateway
        - Domain
        - Primary DNS
        - Secondary DNS
        - DHCP Server
        - Lease
        - Elapsed
- **Packages tab**—The packages tab displays the add-ons. The add-ons are listed with the attributes—package, version, status and size. The **Original** value in the **Status** column specifies the built-in add-ons in the ThinLinux image.

  Original add-ons are displayed in **Black** color, and the add-ons upgraded from Dell Wyse are displayed in **Green** color.

  The packages can be sorted by Package Name, Version, Status or Size by clicking the respective buttons. By default, only Dell Wyse packages are displayed. To view all packages, click the **Show All Packages** button.
- **Copyright tab**—Displays the software copyright and patent notices.

BIOS settings

This section describes the procedure to invoke UEFI BIOS settings and select boot source for your thin client.

The standard UEFI BIOS features and boot options are as follows:

- Boot from UEFI: Hard Drive, Partition 2 – Boots from the internal eMMC storage.
- Boot from IP4 Realtek PCIe GBE Family Controller – Boots from the network through PXE.
- Boot from IP6 Realtek PCIe GBE Family Controller – Boots from the network through PXE.
- Boot from USB – Boots the USB storage from any of the USB ports (this option gets display if plugin in the Bootable USB devices).

The following are the UEFI BIOS Hot Key functions while booting:

- F12-Key – The key invokes the boot selection menu. It is used to select boot order or to do a BIOS flash update.
- F2-Key – The key invokes the BIOS settings that are protected by a password. The default password is `Fireport`.

3

Configuring thin client settings locally

This chapter contains information to help you set up your thin client hardware, look and feel, and system settings. To configure your thin client settings, click the **Switch to Admin** button to enter into the **Admin mode**. Enter the default password in the displayed window. The default password is **admin**.

Click the **Settings** icon on the Desktop. The **System Settings** page is displayed.

The **System Settings** consists of the following tabs:

- System
- Peripherals
- Network
- Personalization
- Connections
- Security
- Management

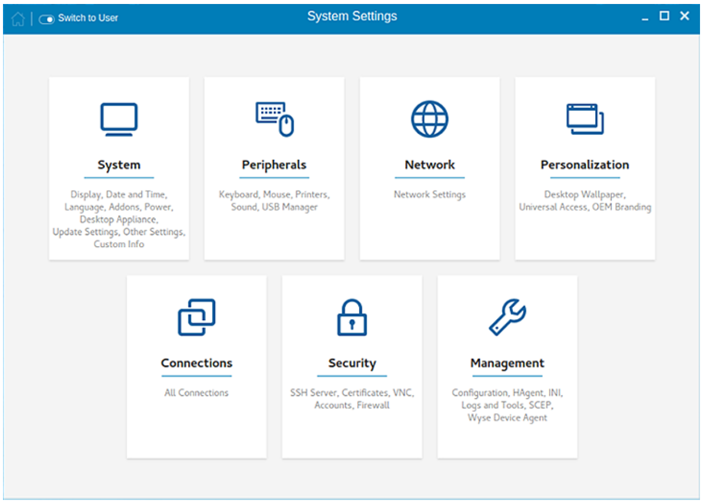

Switch to User
System Settings
System
Display, Date and Time, Language, Addons, Power, Desktop Appliance, Update Settings, Other Settings, Custom Info
Peripherals
Keyboard, Mouse, Printers, Sound, USB Manager
Network
Network Settings
Personalization
Desktop Wallpaper, Universal Access, OEM Branding
Connections
All Connections
Security
SSH Server, Certificates, VNC, Accounts, Firewall
Management
Configuration, HAgent, INI, Logs and Tools, SCEP, Wyse Device Agent

Figure 2. System settings

In ThinLinux 2.1 release, the **Home** button is added in **Settings App**. The **Home** button is disabled on the **Settings App** home page. When you navigate to system settings inside the **Settings App**, the **Home** icon is enabled.

Topics:

- Changing system settings
- Peripherals
- Network
- Personalization

Changing system settings

On the **System Settings** page, click the **System** icon. The following tabs are displayed on the left pane of the **System Settings** page.

- Display
- Date and Time
- Language
- Addons
- Power
- Desktop Appliance
- Update Settings
- Other Settings
- Custom Info

Customizing the display

ⓘ **NOTE: This section is applicable to Wyse 5070 thin client.**

By default, the **Customize your display** screen is available in both user mode and admin mode. Any changes to display preferences are saved and available for the built-in user named **thinuser**. In a **Dual-monitor** configuration, if both monitors are connected, then by default, the monitors are in extended mode. The primary monitor is on the left (monitor 1), and the secondary monitor is on the right (monitor 2). The resolutions of the monitors are auto detected by the system by analyzing the monitor capabilities.

To customize the display, do the following:

1. Click the **Display** tab.

   The **Customize Your Display** page is displayed.

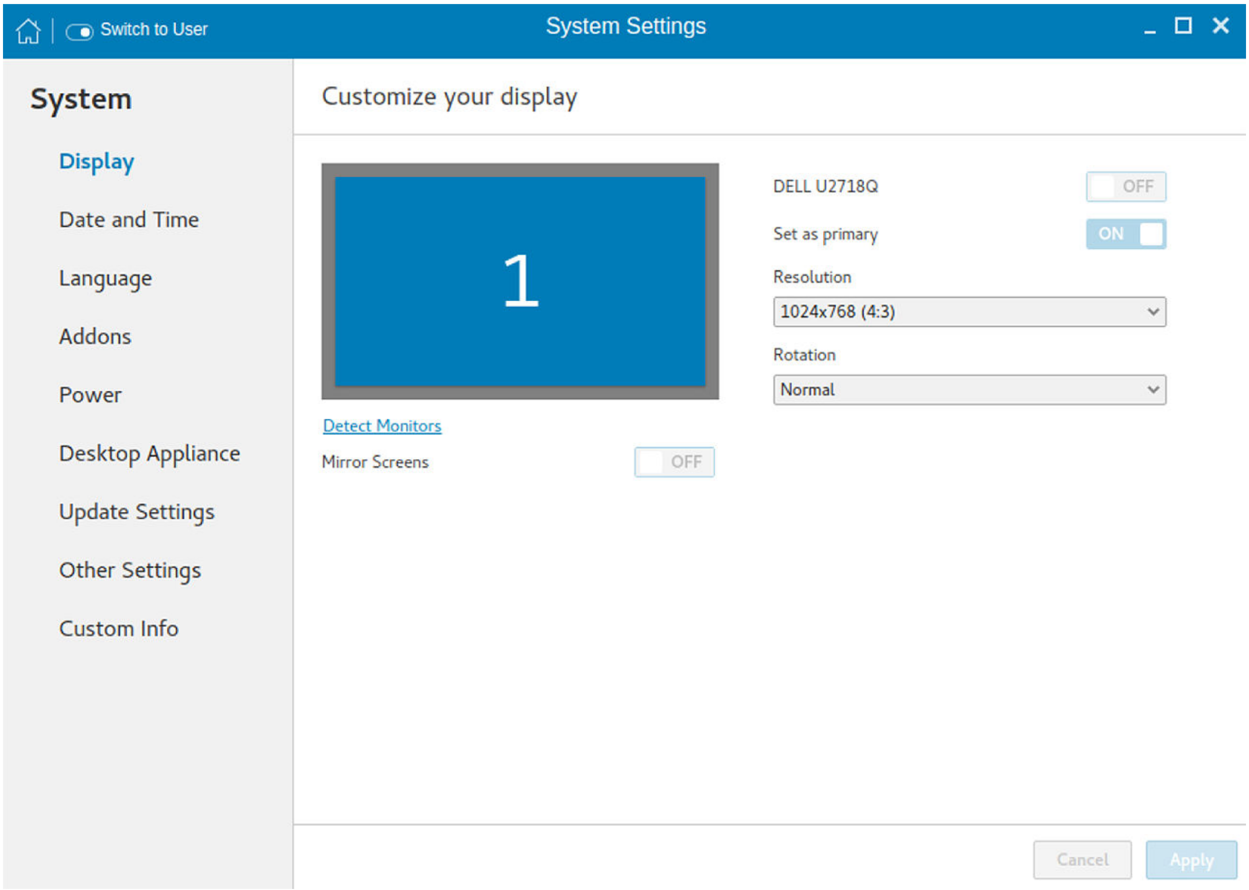


Figure 3. Display settings

2 From the **Resolution** drop-down list, select the preferred resolution.

3 From the **Rotation** drop-down list, select the rotation.

- Normal
- Right
- Left
- Upside-down

4 To enable the screen mirroring for secondary displays in a multi-monitor configuration, click the **ON/OFF** button.

5 To enable the **Set as primary** option, click the **ON/OFF** button. This option allows you to set the selected monitor as primary.

6 To enable the **Monitor On/Off** option, click the **ON/OFF** button. This option allows you to turn off and turn on the preferred monitor in a dual monitor configuration.

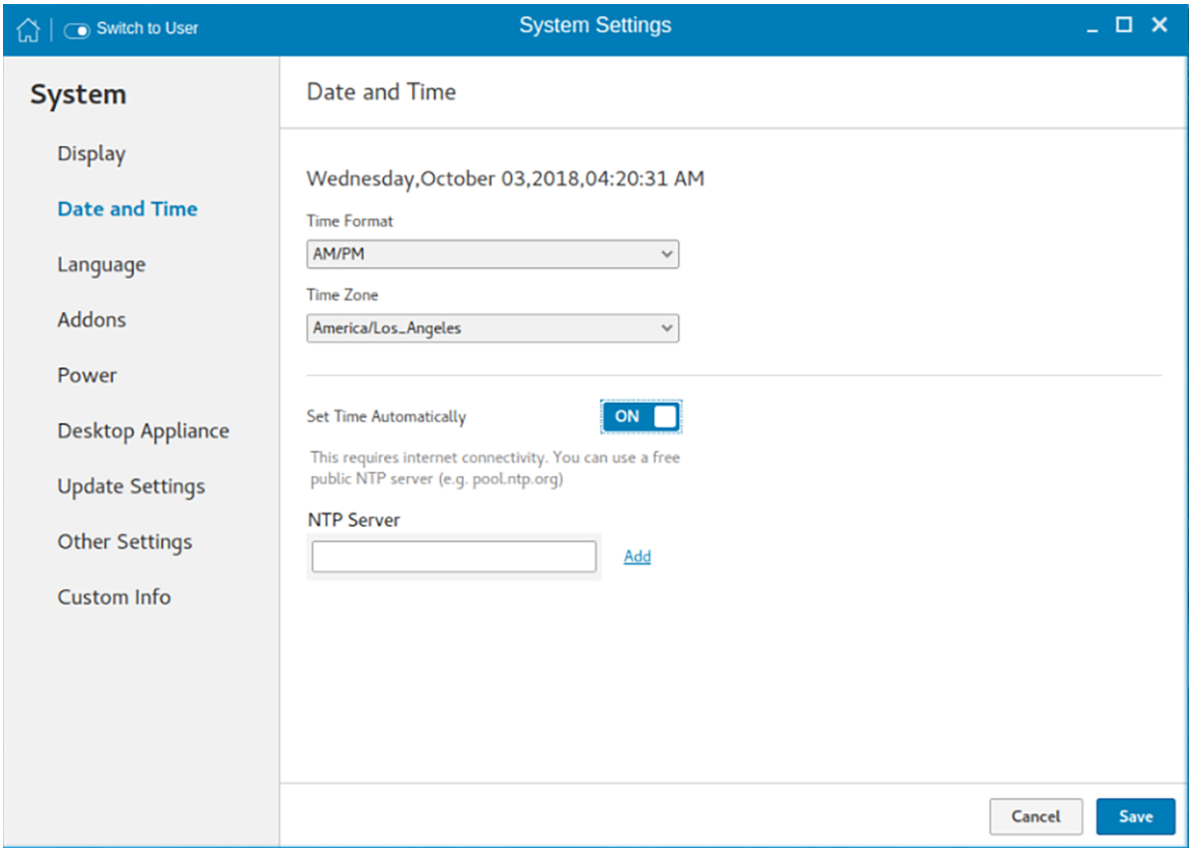
Setting the date and time

1 Click the **Date and Time** tab to set the date and time on your thin client.

The Date and Time screen enables you to set the device's date, time, time zone, and whether or not the device should sync its time with an NTP (Network Time Protocol) server. You can configure the Date and Time either manually or automatically. The date, month and the year along with the time is displayed at the top of the screen.

The **Time Format** can be changed by using the Time Format drop-down list, and the **Time Zone** can be changed by using the Time Zone drop-down list. The default time zone is America/Los_Angeles. Both changes can be performed regardless of the ON or OFF state of the **Set Time Automatically** switch.

ⓘ NOTE: **By default, the Date and Time screen is available only in Admin mode**



Date and Time

Wednesday,October 03,2018,04:20:31 AM

Time Format: AM/PM

Time Zone: America/Los_Angeles

Set Time Automatically: ON

This requires internet connectivity. You can use a free public NTP server (e.g. pool.ntp.org)

NTP Server

Figure 4. Date and time settings

2 To configure the **Date and Time** settings manually when the **Set Time Automatically** switch is in **OFF** position.

   a Click the date field and select the year, month and date.

   Any changes performed in the date field such as, the time format is selected as 24 Hours or an additional AM/PM format, is displayed at the top of screen.

   The time field consists of Hour and Minute drop-down list.

   b Click **Save** to save the changes. Clicking **Save** when **Set Time Automatically** switch is in the OFF state also disables NTP synchronization.

> **NOTE: The Date and Time screen detects whether or not the NTP daemon is activated. By default, the NTP daemon is deactivated. The manual setting time zone/date/time page is displayed, if the NTP daemon is deactivated. Otherwise, the auto setting time zone page is displayed.**

3 To configure the **Date and Time** automatically:

   a Click the **Set Time Automatically** button, to turn on the automatic settings. Note that internet access is required to use this option. Turning on this option activates the NTP daemon and enables the NTP daemon to start syncing the device's time with the specified NTP server.

   b Click the **+** icon to add a new **NTP** server. The **NTP Server IP or FQDN** box is displayed on the page.

   c Enter the NTP Server IP or FQDN Server IP in the **NTP Server IP or FQDN** box. The **+** icon and **x** icons are displayed on the right side of the box, when you start typing the characters in the box.

   - Click the **+** icon to add the specified NTP server/FQDN to the NTP Server list. If a proper NTP server IP is not entered, then a warning message is displayed on the page.
   - Click the **x** icon to clear the IP address you have entered in the box.

   d The **Delete**, **Up arrow** and **Down arrow** icons are displayed next to the NTP Server name when you hover the mouse over a particular NTP server in the NTP Server list.

   - Click the **Delete** icon to delete the specified NTP server from the NTP Server list.
   - Click **Up arrow** and **Down arrow** to change the order of the particular NTP server in the NTP Server list.

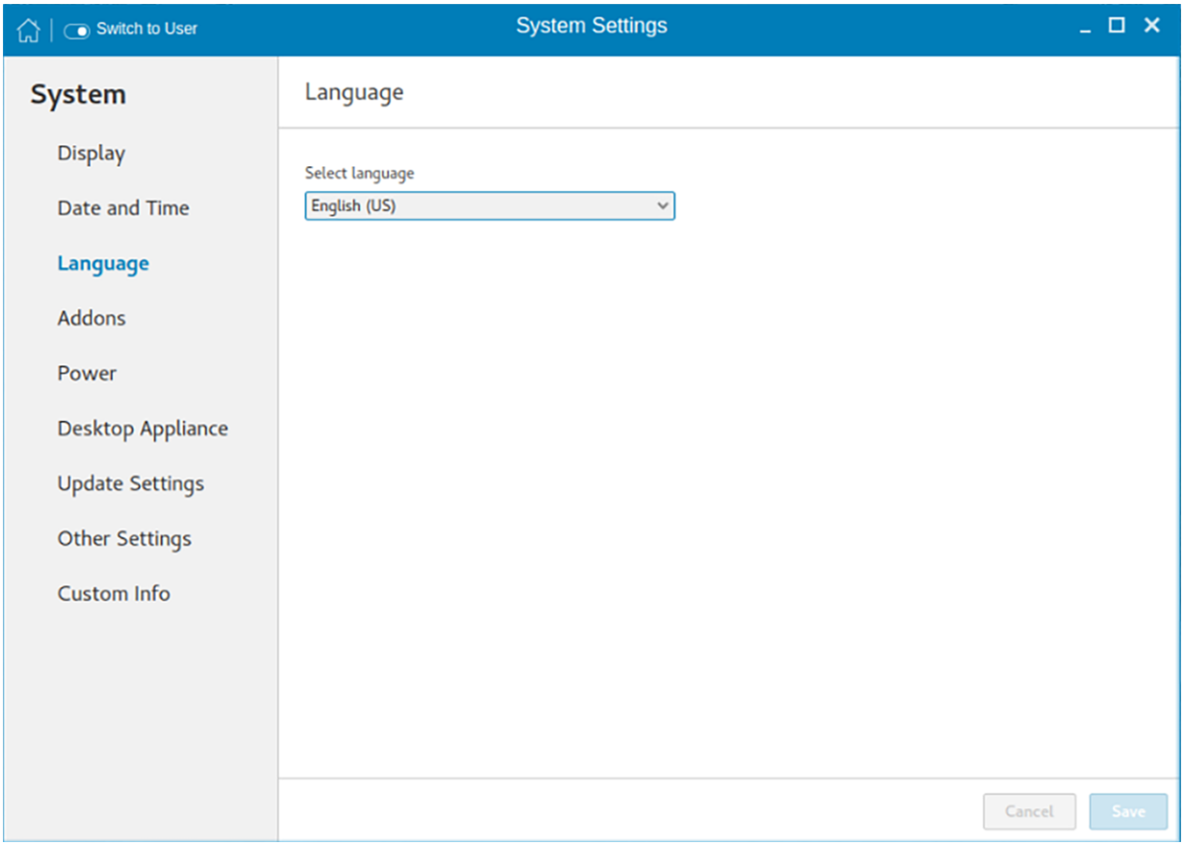
> **NOTE:**
>
> - The **Up arrow** is enabled when the particular NTP server can be moved to the top in the NTP Server list and it is disabled when the particular NTP server is listed at the top of the NTP Server list.
> - Click **Down arrow** to change the order of the particular NTP by moving it down in the list.
> - The **Down arrow** is enabled when the particular NTP server can be moved down in the NTP Server list and it is disabled when the particular NTP server is listed at the bottom of the NTP Server list.

4 Click **Save** to save the changes. Clicking **Save** button when, **Set Time Automatically** is in **ON** position, enables NTP synchronization.

Selecting the language

By default, the **Language** applet is available only in Admin mode. Any changes made through Language applet is saved and continued for the built-in thinuser.

From the **Select Language** drop-down list, select the language of the screen from the list of supported languages and click **Save** to save your settings.



Language

Select language: English (US)

Figure 5. Language settings

Configuring the addons

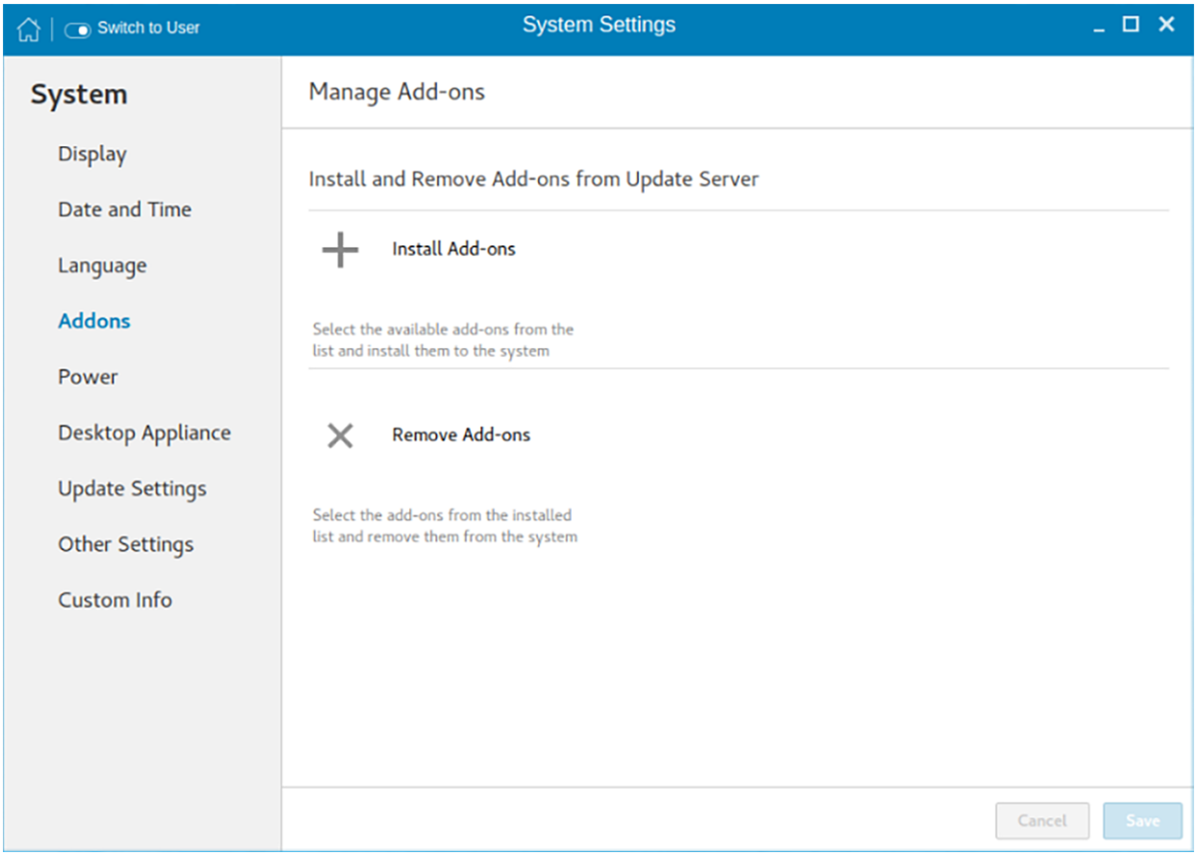
The Add-ons page enables you to install and remove Add-ons from INI server.

As a prerequisite, you must configure the location of add-ons on the **Manager INI Configuration** page. For more information about INI management, see INI Management.

ⓘ NOTE: **The Addons screen is available only in Admin mode.**

1 Click the **+** icon to Install the Add-ons.

A list of available add-ons is displayed.



Switch to User
System Settings
System
Display
Date and Time
Language
Addons
Power
Desktop Appliance
Update Settings
Other Settings
Custom Info
Manage Add-ons
Install and Remove Add-ons from Update Server
Install Add-ons
Select the available add-ons from the list and install them to the system
Remove Add-ons
Select the add-ons from the installed list and remove them from the system
Cancel
Save

Figure 6. Install Add-ons

2 Select the required add-ons and install them to the system. You can select multiple add-ons at a time.

3 Click the **x** icon to remove the Add-ons from the installed add-ons list.

4 Select the add-ons that you want to remove and click **Remove Add-ons**.

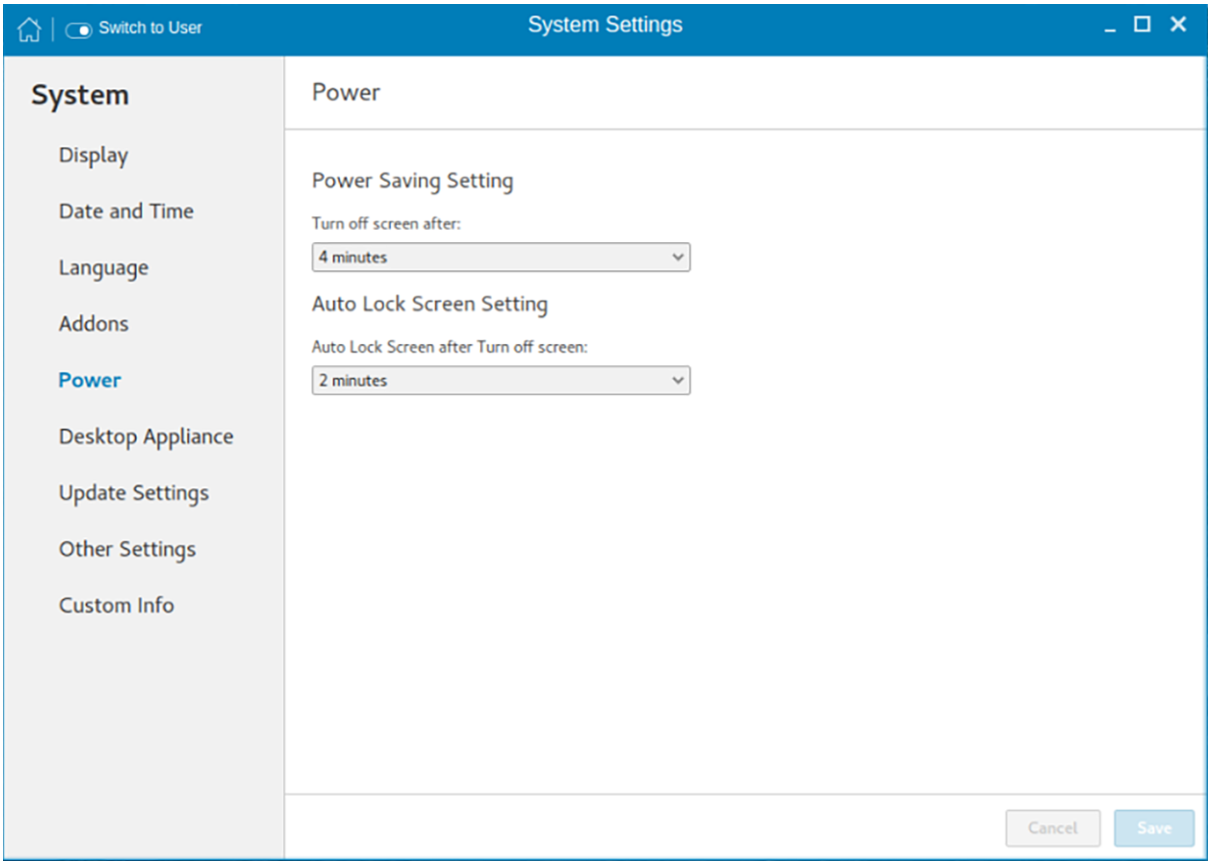
5 Click **Save** to save the changes.

Configuring the power saving setting

The **Power Setting** page enables you to set **Monitor Sleep mode**.

1 From the **Turn off screen after** drop-down menu, select the time in seconds to set the monitor to turn off after the specified idle time.

2 From the **Auto Lock Screen after Turn off screen** drop-down menu, select the time in seconds to set the turned off screen to lock the thin client after the specified idle time.



Power

Power Saving Setting

Turn off screen after: 4 minutes

Auto Lock Screen Setting

Auto Lock Screen after Turn off screen: 2 minutes

Figure 7. Power settings

NOTE: **ThinLinux supports the display turn off, and by default it is set for 4 minutes of idle time to comply with Energy Star category. If you select never option from the drop down list, it corresponds to idle time of 0 minutes.**

Configuring desktop appliance

We can configure Desktop Appliance (Power On to Power Off VDI theme) using GUI, INI and DHCP. For INI configuration, refer the tags description of DesktopAppliance, CitrixConnectionType, PNAgentServer and Storename INI parameters.

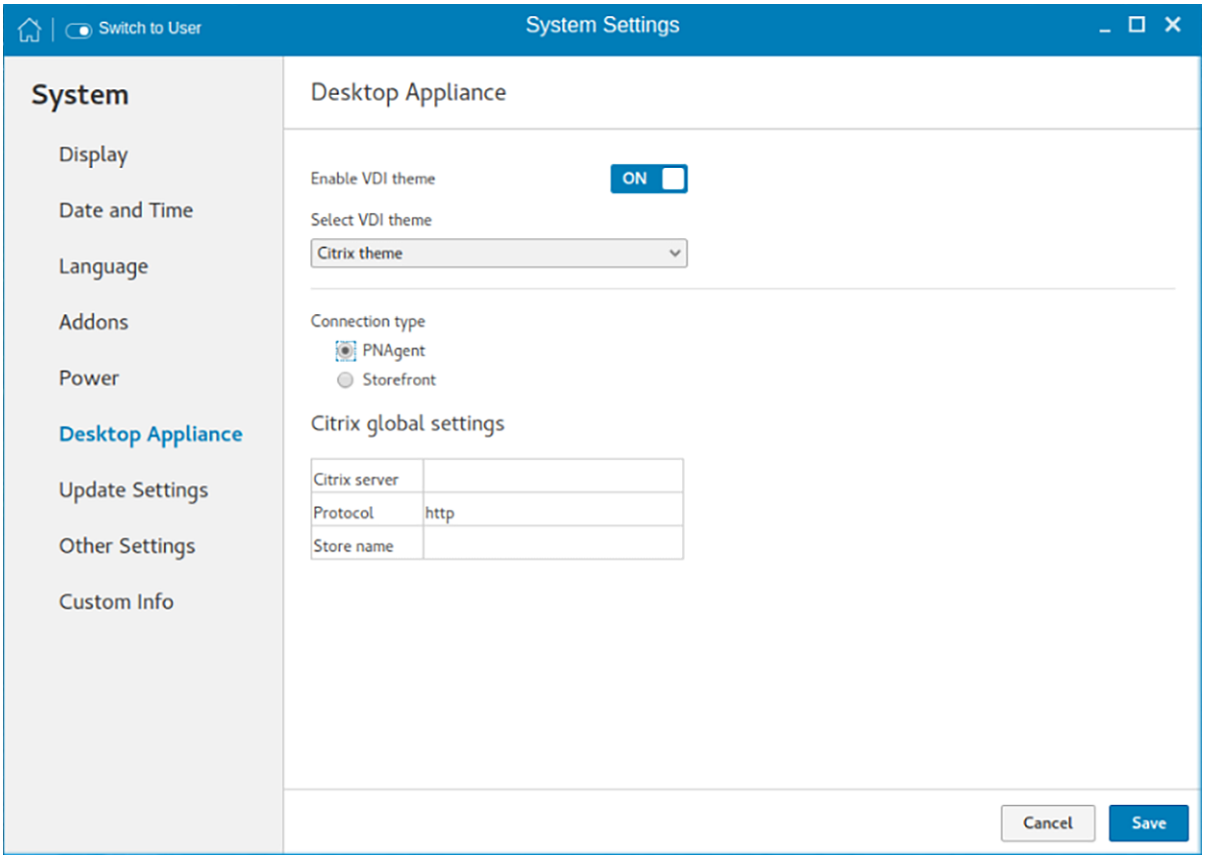
For DHCP configuration,

- 181—Configure Citrix server url—either specify pnagent url xyz.com/citrix/pnagent/config.xml, storefront xyz.com/citrix/store/discovery, or IP/FQDN.
- 203—Type of VDI theme
- 204—Type of Citrix server
- 205—Storename. For more information, see DHCP Option Tags

By default, the **Desktop Appliance** screen is available only in Admin mode. Any changes made through **Desktop Appliance** screen is saved and continued for the built-in thinuser.

1 Click the **ON/OFF** button to enable or disable the **VDI theme** option after you log in to the session.
2 From the drop-down list, select your preferred VDI theme.

NOTE: **Only Citrix theme is supported in this release.**



Desktop Appliance

Enable VDI theme ON

Select VDI theme

Citrix theme

Connection type

● PNAgent

○ Storefront

Citrix global settings

Citrix server	
Protocol	http
Store name	

Figure 8. Desktop appliance settings

3 Select the type of Citrix Server.

Citrix server, Protocol and Storename can be configured from the **Change global settings** page. Go to **All connections** page, select the **Citrix** option and then select the **Change global settings** option to configure the Citrix settings. For more settings for Applications or Desktops, go to All connections page, select Citrix option and then select Change global settings option to configure the Applications or Desktops settings.

4 Click **Save**.

You are prompted to restart the system.

5 Click **OK** to save the changes and restart the system in selected theme.

6 After the system is restarted, a **log on** button is displayed.

a Click the **Log On** button.

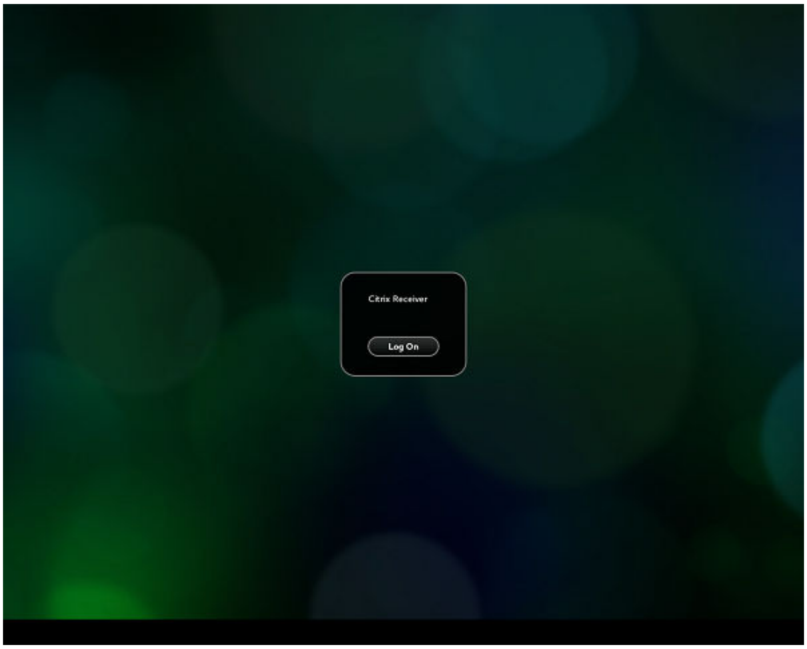


Figure 9. Login screen

You are required to authenticate by entering the following credentials:

- User name
- Password
- Domain

You are logged on to the Citrix receiver.

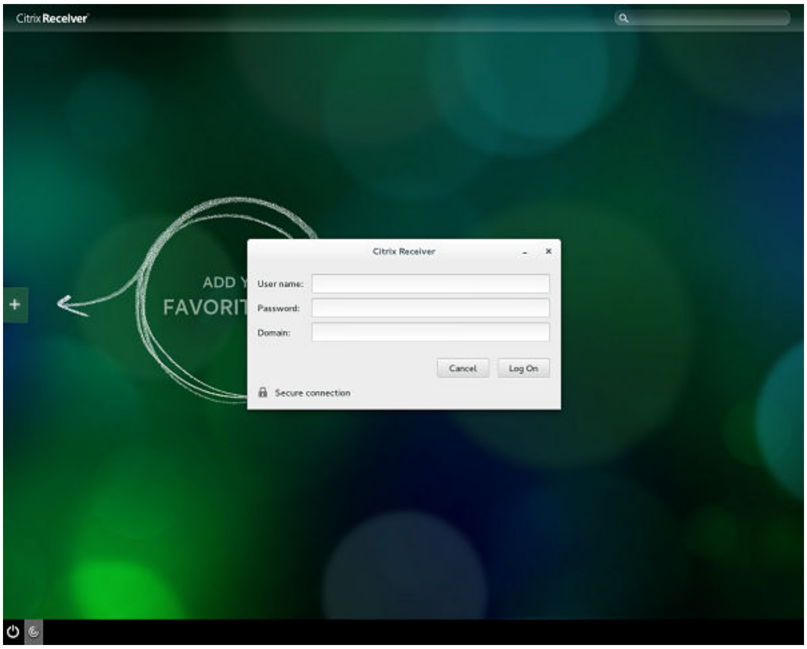


Figure 10. Authentication screen

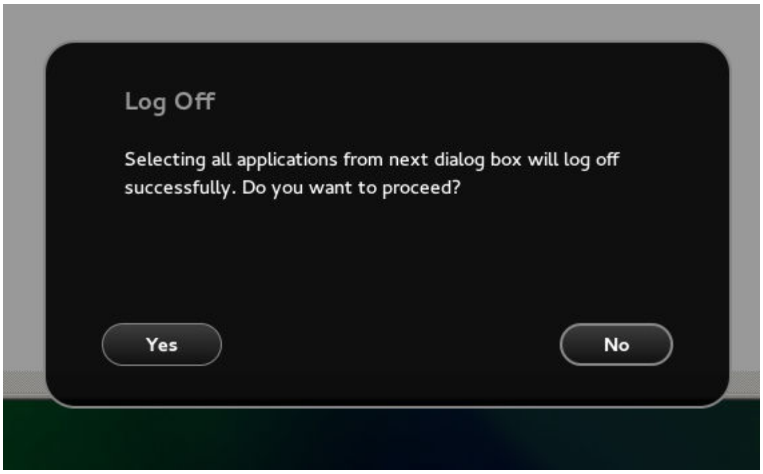
If the logon authentication fails, you are prompted with a screen. Click **try again** to query the server again.

ⓘ **NOTE: You can break kiosk mode and enter into admin mode at any point of time by using the shortcut key. The shortcut key is <Control><Alt><Shift>F11.**

b After the successful login, you can add the required applications or desktops from the left **+** button.

c Click the application or desktop to start it. You are prompted with an error if there as an error message.

d You can logout at any point of time by clicking the power icon on task bar. Depending on whether any application is opened, you are prompted with an error message.



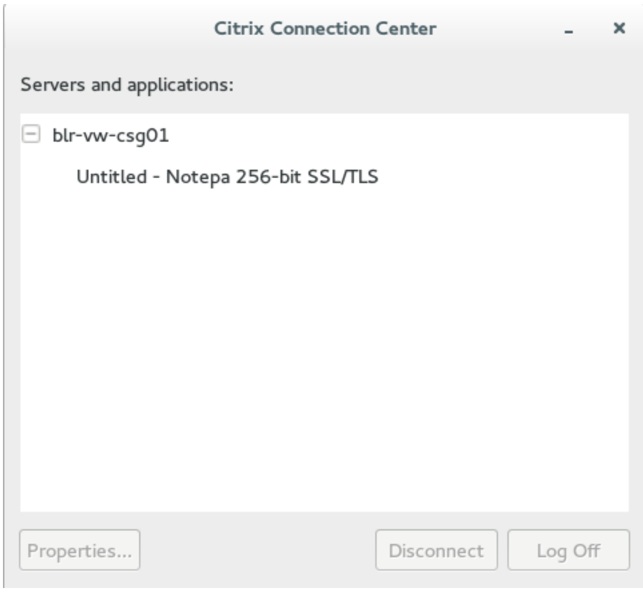
Log Off

Selecting all applications from next dialog box will log off successfully. Do you want to proceed?

Figure 11. Log Off screen

e If any applications are running, connection center window is displayed, select each application and either log off or disconnect. Following which click the cross to close the control center and logoff completely.

ⓘ **NOTE: If you do not follow above procedure to log off, you may see sessions active and running behind the displayed log on button.**



Citrix Connection Center

Servers and applications:

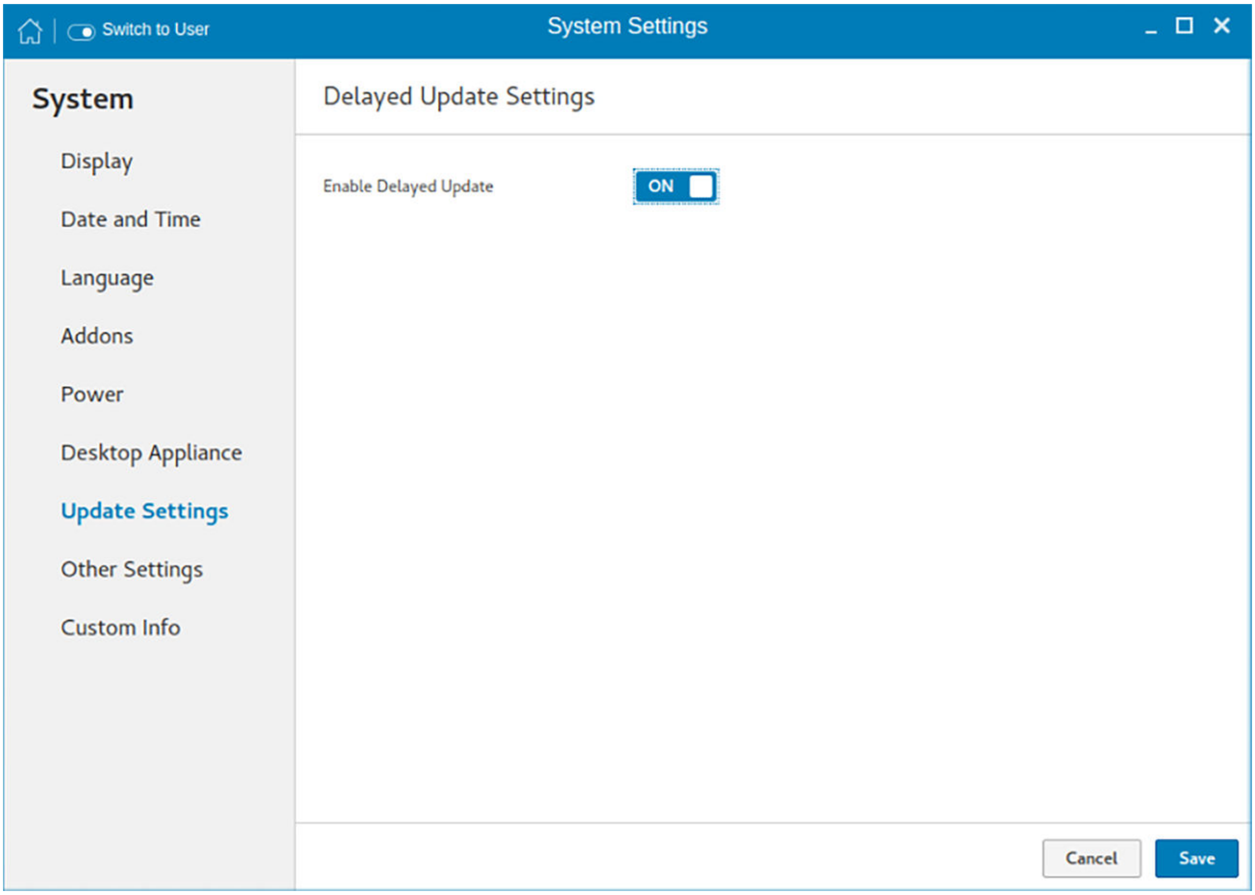
blr-vw-csg01

Untitled - Notepa 256-bit SSL/TLS

Figure 12. Citrix connection center

Delayed update settings

By default, the delayed update option is enabled. You must provide the File Server credentials using INI parameters to start the Merlin image upgrade process. For more information, see the latest *Dell Wyse ThinLinux INI Reference Guide* on www.dell.com/support.



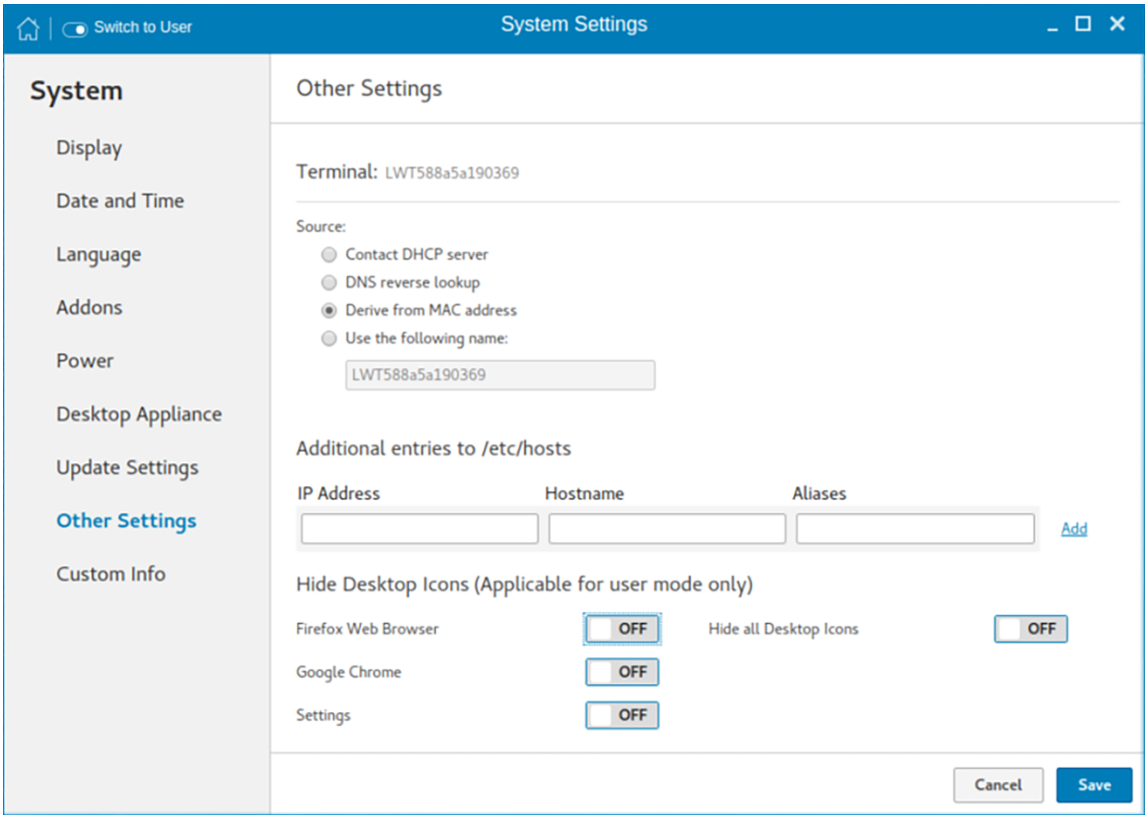
Delayed Update Settings

Enable Delayed Update ON

Figure 13. Delayed update

Other settings

The **Other Settings** page enables you to enter the hostname of the thin client to add or delete the additional entries to the /ect/hosts file in the device. Any changes that are made through **Other Settings** screen are saved and preserved over reboots for the built-in thinuser. The **Other Settings** screen is available only in admin mode.



Other Settings

Terminal: LWT588a5a190369

Source:

○ Contact DHCP server
○ DNS reverse lookup
● Derive from MAC address
○ Use the following name:

LWT588a5a190369

Additional entries to /etc/hosts

IP Address	Hostname	Aliases

Hide Desktop Icons (Applicable for user mode only)

Firefox Web Browser: OFF

Hide all Desktop Icons: OFF

Google Chrome: OFF

Settings: OFF

Figure 14. Other settings

To configure the other settings, do the following:

1 In the **Source** section, configure one of the following options:

- **Contact DHCP server**—If you set the hostname of the thin client by selecting the DHCP server option, the hostname is set to the standard **host-name** tag received from the DHCP server. If the DHCP server does not provide the **host-name** tag, the device retains the previously set hostname.
- **DNS reverse lookup**—If you select **DNS reverse lookup** option to enter the hostname of the thin client, a reverse DNS lookup operation is performed using the existing IPv4 address of the thin client, and the hostname is set to the received value.

  NOTE: The previous hostname is retained if the device cannot perform a successful reverse DNS lookup operation due to reasons such as, network connection is not established, DNS servers are not established or are invalid, and the IP address is not in the DNS server's list.
- **Derive from MAC address**—Select the **Derive from MAC address** option to specify the **host name** of the thin client. You can specify the hostname by using the MAC address. The Ethernet of the thin client interfaces with the MAC address. It creates the hostname by extracting the MAC address from its field separators, such as, (:) and the MAC address is prefixed with the string LWT. For example, a device with MAC address of 00:80:64:c1:8b:14 has MAC derived hostname as LWT008064c18b14. If you want to use the manually named device as a seed device for Merlin image pulling, you must be cautious in specifying the hostname manually. The changed hostname is pushed to other devices and these devices use the same hostname. Only through device factory reset, you can recover the default value by using MAC address.
- **Use the following name**—This option enables you to enter your preferred hostname. When you log in to the session, the screen displays the previous hostname in the box and in the Terminal option.

  NOTE: The hostname entered is not authenticated if the string entered has a white space. The first part of the string up to the first white space is used to set the hostname of the devices. All white spaces at the beginning of the string are ignored, and the maximum hostname string size is 64.

2 In the **Additional entries to /etc/hosts** section, you can set the device name and update the entries on the **/etc/hosts** file. This option enables you to add to the preset default data, and update or delete the existing entries. To configure this option, do the following:

a Enter the **IP address**, **host name**,and **Aliases** in the respective fields.

b Click the **Add** option, and update the default data.

3 In the **Hide Desktop icons** section, configure any of the following options:

ⓘ **NOTE: These options are applicable for user mode only.**

- **Firefox Web Browser**—Click the **ON/OFF** button to enable or disable this option. If you enable this option, the Mozilla Firefox web browser icon is not displayed on the desktop.
- **Google Chrome**—Click the **ON/OFF** button to enable or disable this option. If you enable this option, the Google Chrome web browser icon is not displayed on the desktop.
- **Settings**—Click the **ON/OFF** button to enable or disable this option. If you enable this option, the Settings app icon is not displayed on the desktop.

  If the **Settings** app is hidden, and if you log into the thin client with user credentials, then you cannot open the **Settings** app or switch to the admin mode. You can restore the **Settings** app using one of the following methods:

  – Use INI parameters.

  – Log in to the thin client with admin credentials and enable the **Settings** option.

  – Perform a factory reset or factory recovery.
- **Hide all Desktop icons**—Click the **ON/OFF** button to enable or disable this option. If you enable this option, the created connection icons are not displayed on the desktop.

4 Click **Save**.

Setting the custom information

The **Custom Info** page enables you to set the device details.

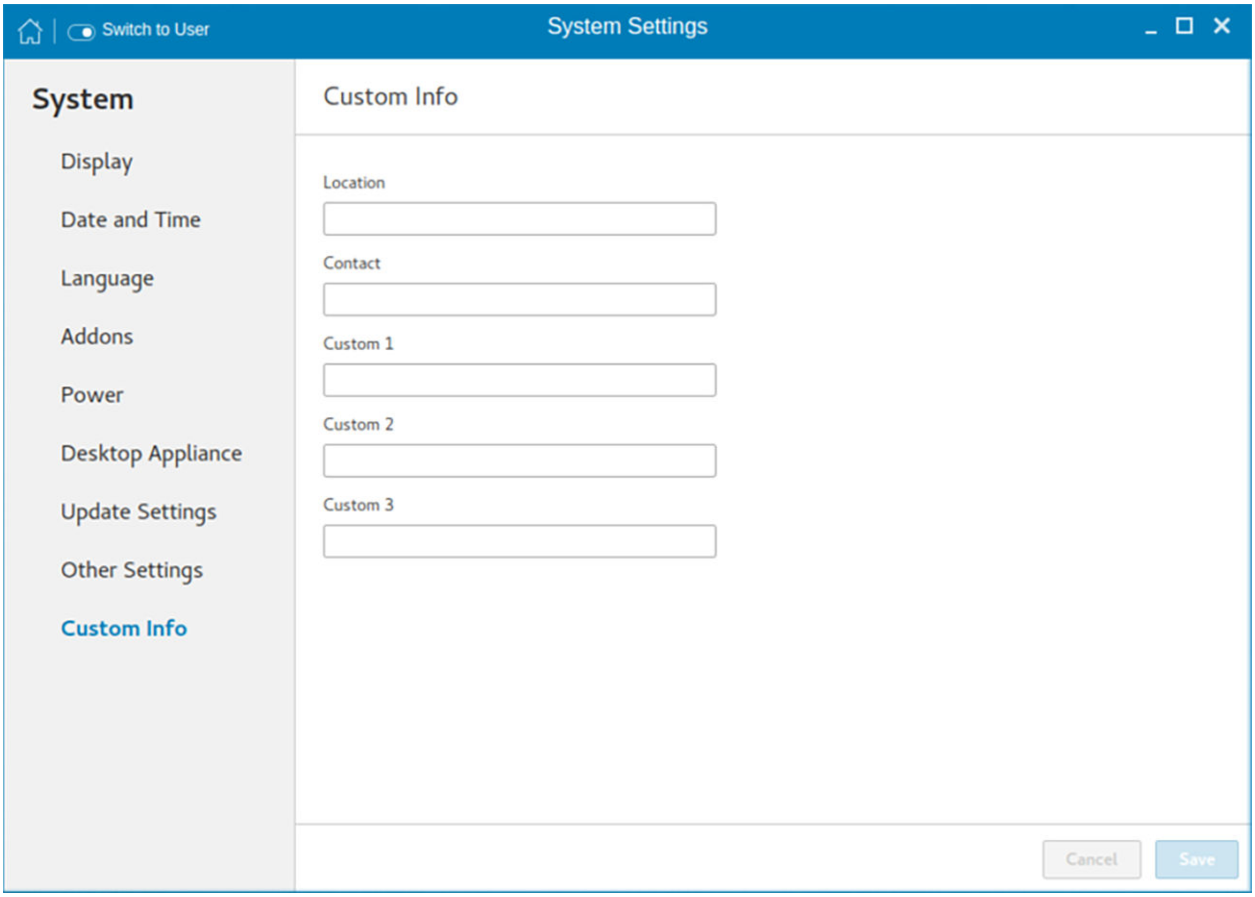


Figure 15. Custom Information

To set the custom details for your thin client, do the following:

1 In the **Location** field, enter the device location.

2 In the **Contact** field, enter the contact details of the concerned authority.

3 In the **Custom 1**, **Custom 2** and **Custom 3** fields, enter the custom values pertaining to your device.

4 Click **Save**.

Peripherals

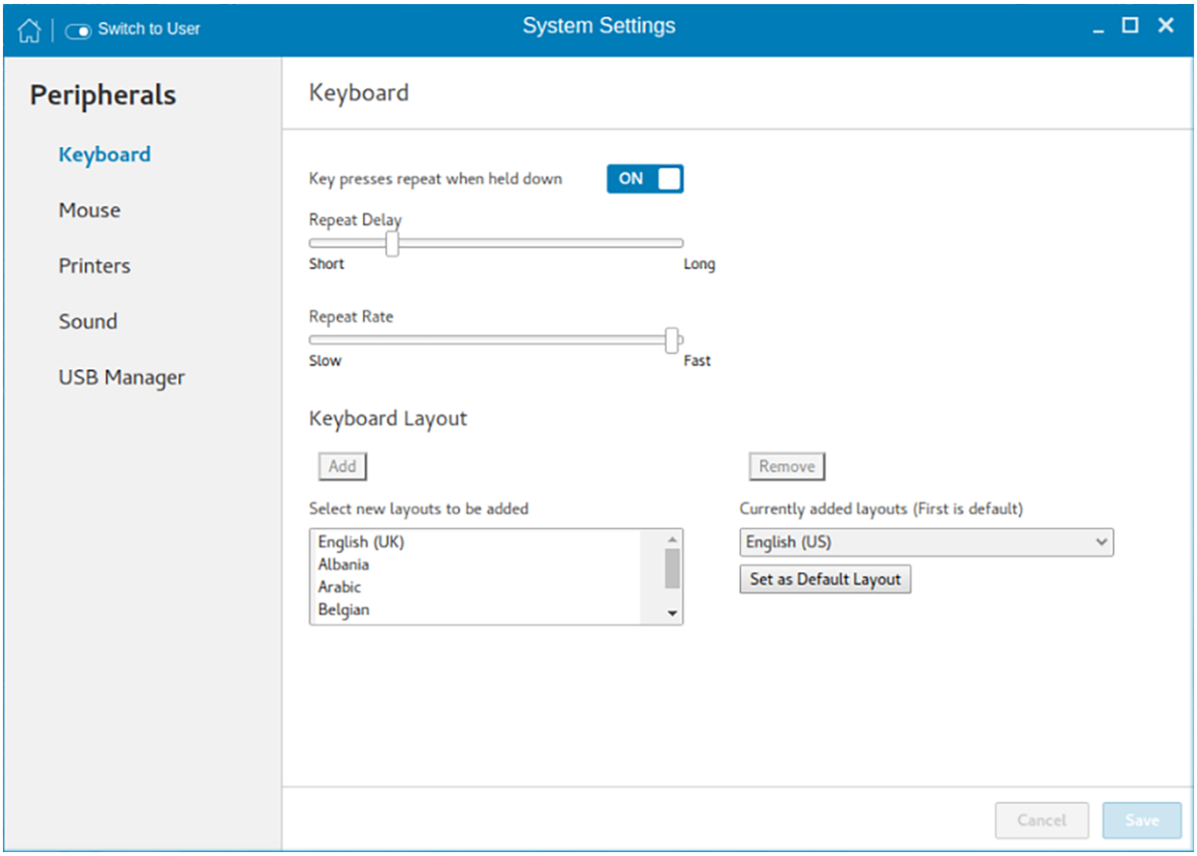
On the **System Settings** page, click the **Peripherals** icon. The following tabs are displayed on the left pane of the System Settings page.

- Keyboard
- Mouse
- Printers
- Sound
- USB Manager

Setting the keyboard preferences

The **Keyboard** setting page enables you to set the Keyboard preferences and make the Keyboard layout.

NOTE: By default, the Keyboard screen is available in both User mode and Admin mode. Any changes made through Keyboard preferences screen is saved and preserved over reboots for the built-in thinuser



Key presses repeat when held down ON

Repeat Delay: Short — Long

Repeat Rate: Slow — Fast

Keyboard Layout

Select new layouts to be added: English (UK), Albania, Arabic, Belgian

Currently added layouts (First is default): English (US)

Figure 16. Keyboard preferences

1 Click the **ON/OFF** button to disable or enable the **Key presses repeat when held down** option after you log in to the session.

2 Move the slider to the left to decrease the repeated delay time of the pointer or move the slider to the right to increase the repeated delay time of the pointer.

3 Move the slider to the left to decrease the repeat rate of the pointer or move the slider to the right to increase the repeat rate of the pointer.

4 In the **keyboard layout** box, select the layout you want to use and click **Add** to include the preferred layout in the **currently added layouts** list.

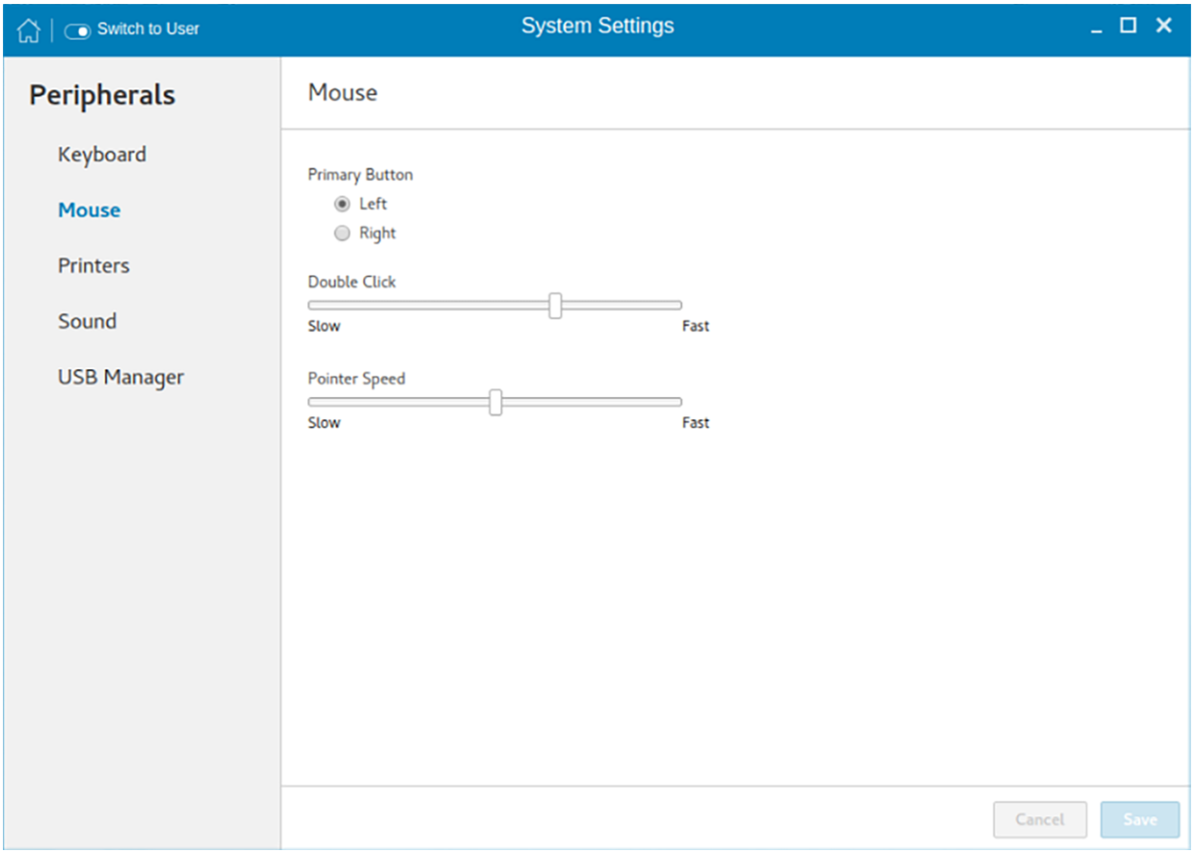
5 Select the preferred keyboard layout from the currently added layouts list, and click **Set as Default Layout** button to set the default layout.

ⓘ NOTE: **The default keyboard layout is listed on the top of the currently added layout list.**

6 Click **Save** to save your changes.

Setting the mouse preferences

By default, the **Mouse** screen is available in both User mode and Admin mode. Any changes made through the Mouse preferences screen is saved and preserved over reboots for the built-in thinuser.



Primary Button
● Left
○ Right

Double Click
Slow Fast

Pointer Speed
Slow Fast

Figure 17. Mouse settings

The Mouse settings page enables you to set the mouse preferences.

1 Click **Right** or **Left** to set the primary button of the mouse.

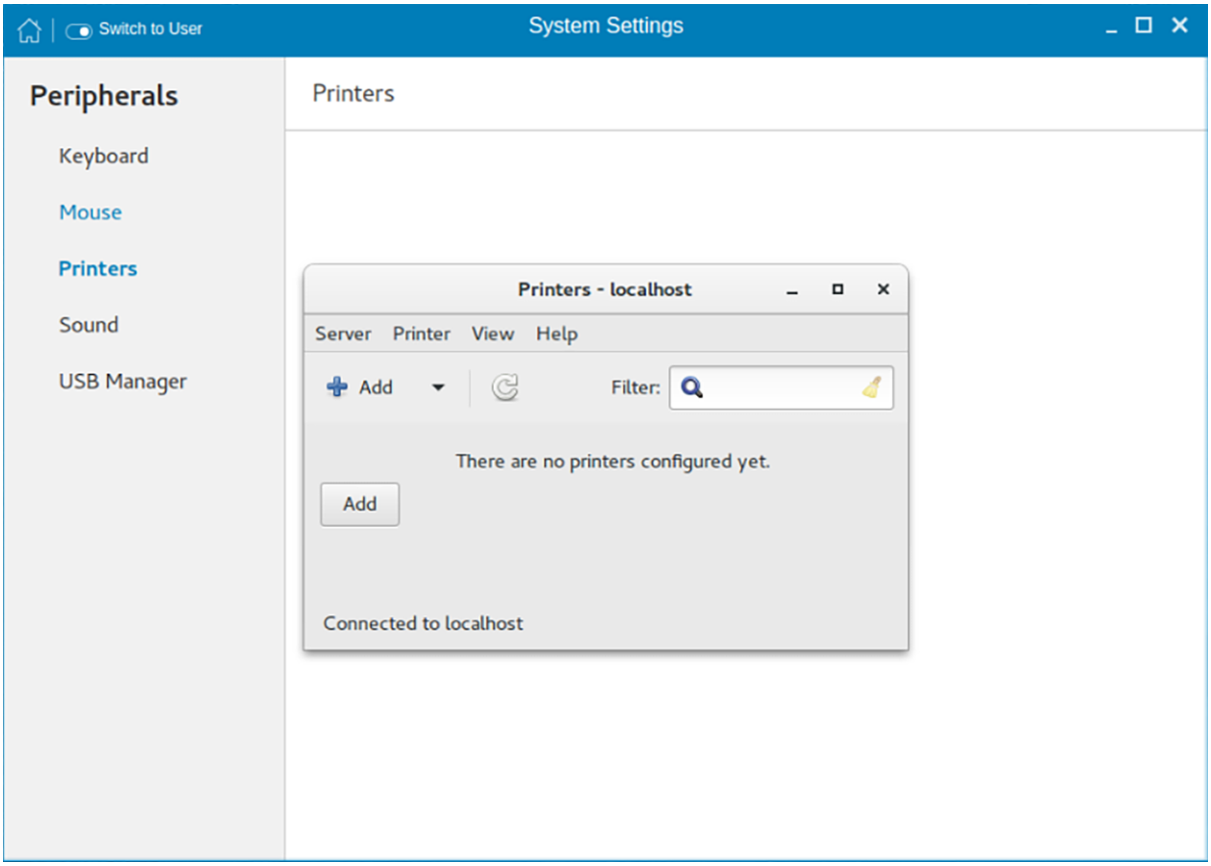
2 Move the slider to the left to increase the speed of the pointer when double-clicked or move the slider to the right to decrease the length of double-clicked.

3 Move the slider to the left to increase the speed of the mouse pointer or move the slider to the right to decrease the speed of the mouse pointer.

4 Click **Save** to save your changes.

Configuring the printer settings

By default, the **Printers** screen is available only in Admin mode.



There are no printers configured yet.

Connected to localhost

Figure 18. Printers - localhost

1 Click the printer icon.

The **Printers - localhost** dialog box is displayed.

2 Click the **Add** button to include a new printer.

The **New Printer** window is displayed. You can configure the printer type based on your preference.

> ⓘ NOTE: **If a USB printer is connected, then it is displayed by default. The printer is not found if wrong address is provided or the USB is not attached.**

3 Select a device type from the following options:

- **LPT Port**—Select this option if your printer is attached to the thin client through an LPT port, and enter valid values.
- **Serial Port**—Select this option if your printer is attached to the thin client through a serial port, and enter valid values.
- **Enter URL**—Select this option to enter URL for a local printer, and enter valid values.
- **Network Printer**—Select this option if you are using a network printer. Use any one of the options for configure your network printer:
  - **Windows Printer via SAMBA**
  - **Internet Printing Protocol (ipps)**
  - **LPD/LPR Host or Printer**
  - **Internet Printing Protocol (https)**
  - **Internet Printing Protocol (ipp14)**
  - **Internet Printing Protocol (ipp)**
  - **AppSocket/HP Jet Direct**

Enter valid values to search for your printer host on network.

4 After you configure the printer based on your preference, click **Forward**.

The thin client searches for the available printer drivers.

5 Select a printer driver, and click **Forward**. You can select the printer driver from database or search for a printer driver to download. You can also browse to the location where you have saved the PostScript Printer Description (PPD) files, and select the appropriate file.

6 Specify the **Printer Name**, **Description**, and **Location**.

7 Click **Apply**.

The printer is listed on the screen.

> ⓘ **NOTE: You can click Print Test Page to test the printer.**

8 Right-click the printer icon, and click **Properties**.

9 Configure the following tabs based on your printing preference:

- **Settings**—Use this tab to configure the location, device URL, model, and printer state.
- **Policies**—Use this tab to configure the printer state, error policy, operation policy, starting banner, and ending banner.
- **Access Control**—Use this tab to set the printing privileges to users.
- **Printer Options**—Use this tab to configure the general printer settings, such as media size.
- **Job Options**—Use this tab to specify the default job options for the printer.
- **Ink/Toner Levels**—Use this tab to view the marker levels and status messages of the printer.

10 Click **OK**.

The thin client is ready to print.

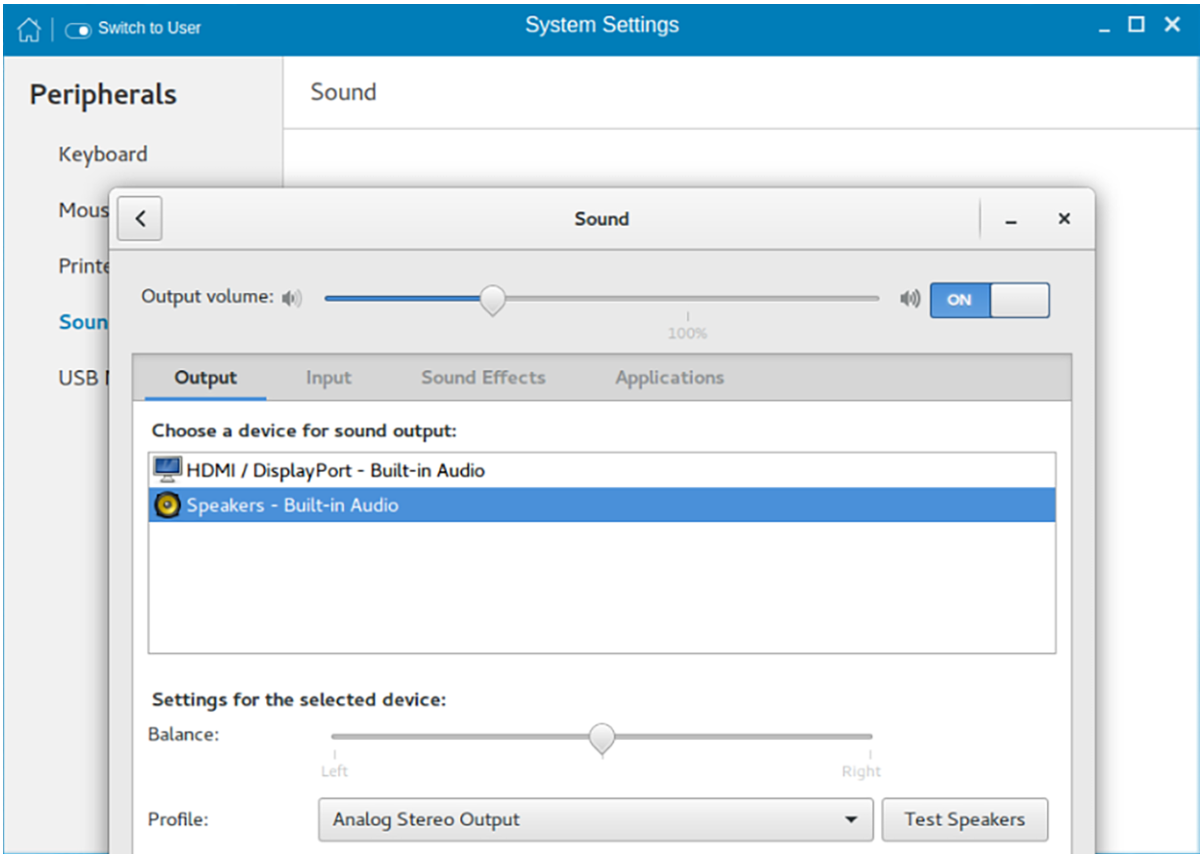
Configuring the sound settings

By default, the sound screen is available in both user mode and admin mode. Any changes to the sound settings are saved and available for the built-in user named **thinuser**.

To configure the sound settings, do the following:

1 Move the **Output volume** slider to adjust the output or speaker volume. Click the **ON/OFF** button to enable or disable the output volume.

2 Click the **Output** tab, and do the following:



Speakers - Built-in Audio

Profile: Analog Stereo Output

Figure 19. Sound output

a From the output devices list, select a device for sound output. The default audio output is the Analog Output.
b Based on the channels available for the selected output device and profile, move the **Balance** slider to adjust the sound balance.
c From the drop-down list, select an audio profile.
d Click **Test Speakers**. A dialog box is displayed. You can test the speaker by playing sample wave files.

3 Click the **Input** tab, and do the following:

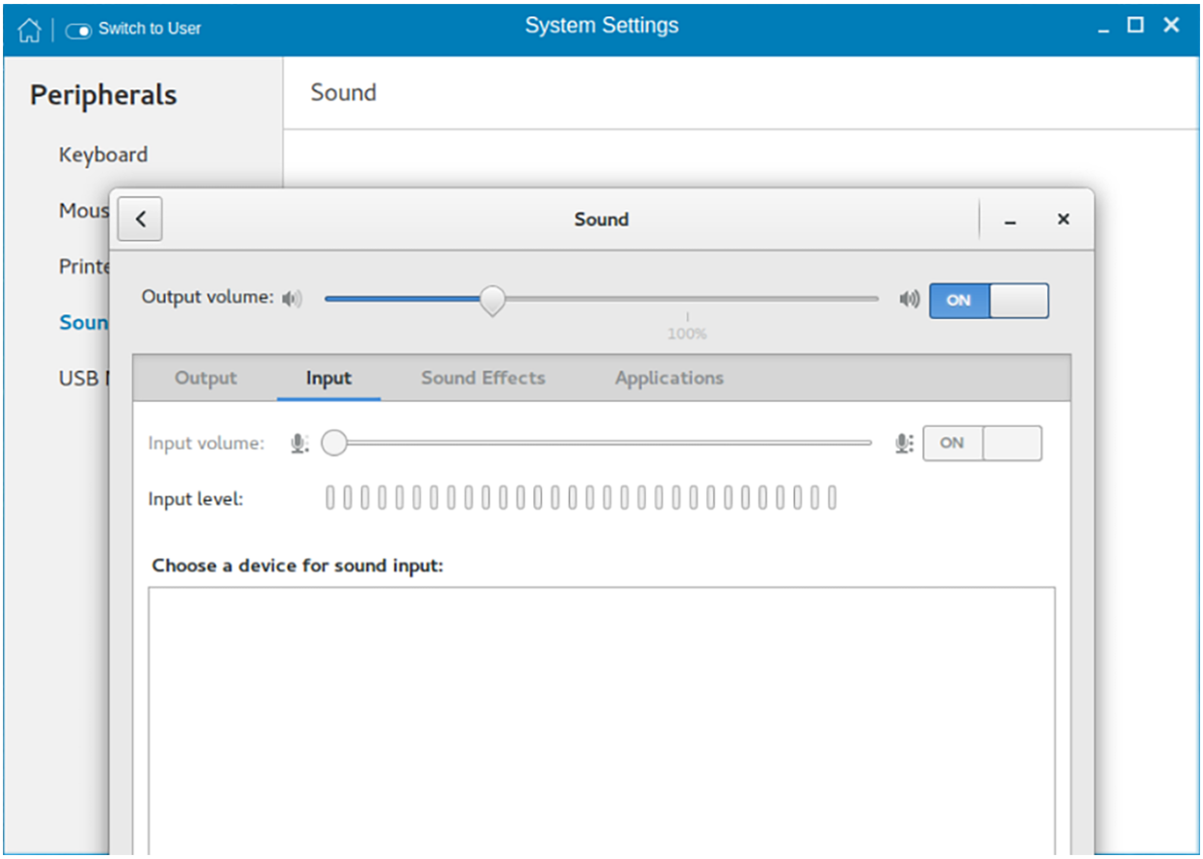


Figure 20. Sound input

a From the input devices list, select a device for sound input. The default audio input is the Analog Input.

b Move the **Input Volume** slider to adjust the input or Mic volume. Click the **ON/OFF** button to enable or disable the input volume.

The **Input level** bar displays the input volume peak level.

4 Click the **Sound Effects** tab, and do the following:

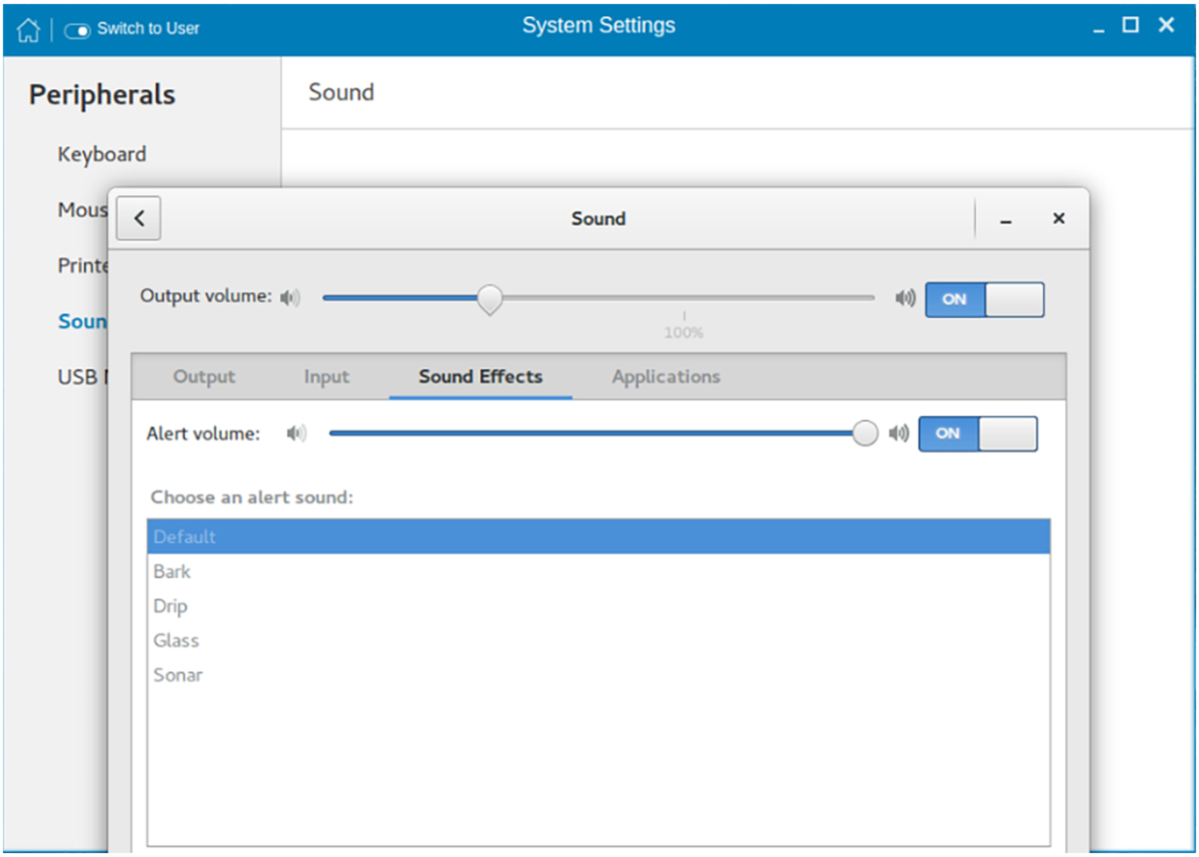
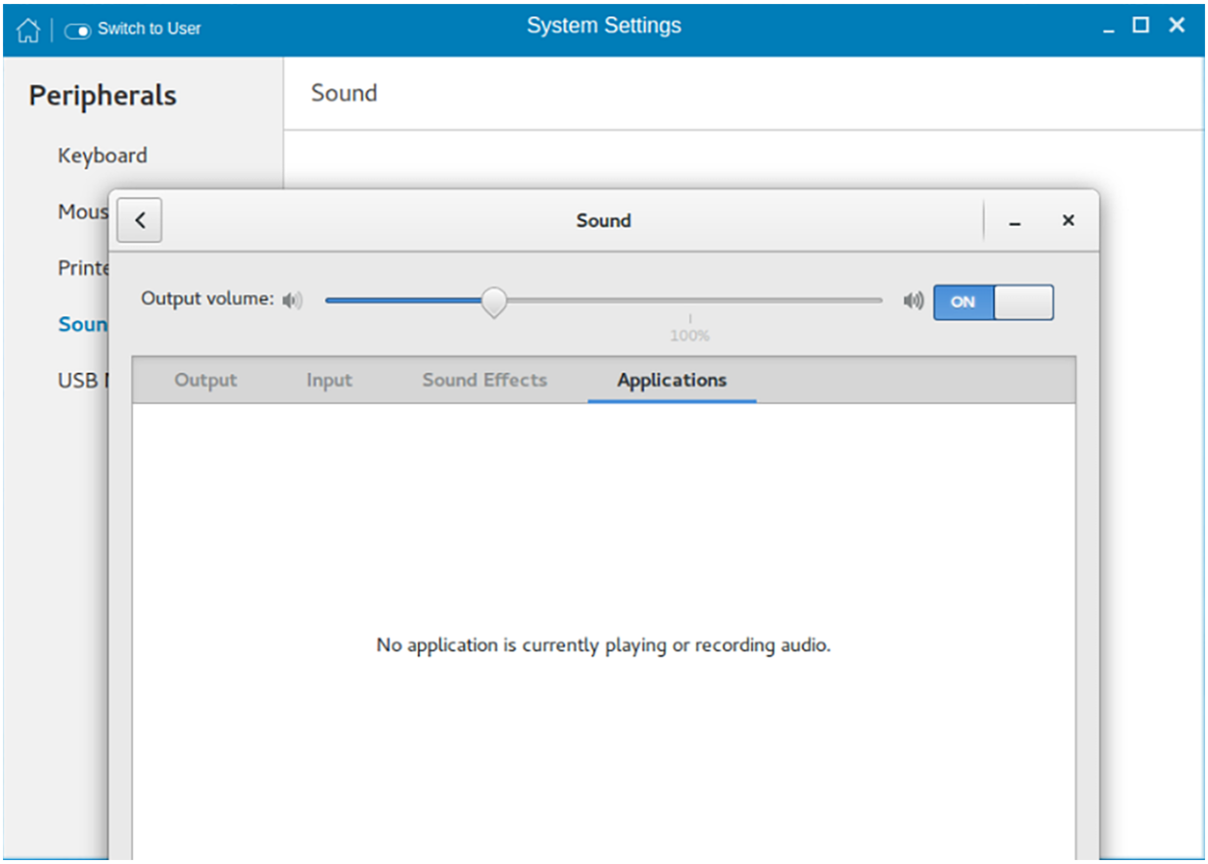


Figure 21. Sound effects

a From the alert sound list, select an alert sound theme.

b Move the **Alert Volume** slider to adjust the volume level of alert sounds. Click the **ON/OFF** button to enable or disable the alert volume.

5 Click the **Applications** tab to view all the applications that are currently playing a sound file, or recording audio.



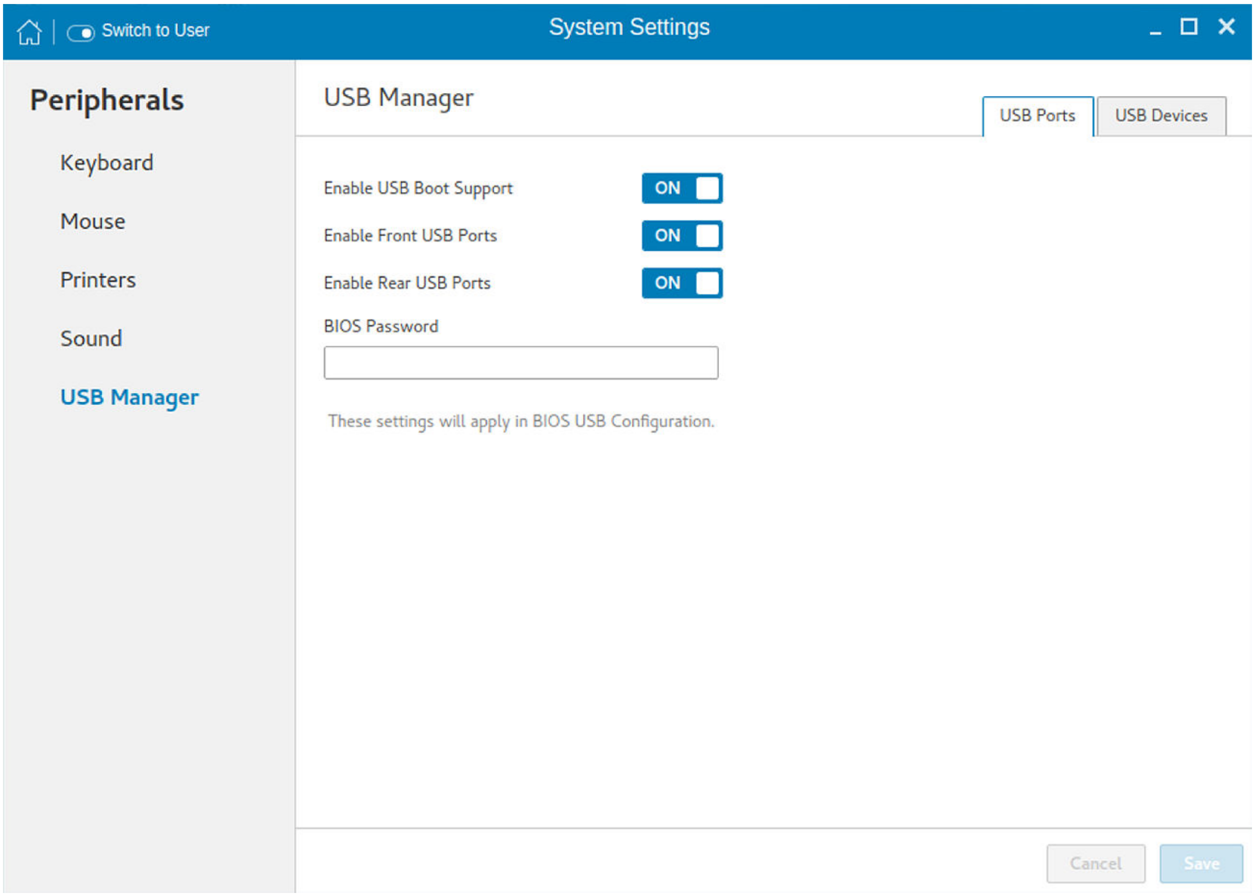
No application is currently playing or recording audio.

Figure 22. Applications

Managing the USB ports and devices

The **USB Manager** page enables you to configure and manage the USB ports and devices that are connected to your thin client. To configure the USB port and device settings, do the following:

1 In the **USB Ports** tab, configure any of the following options:



USB Manager

Enable USB Boot Support ON

Enable Front USB Ports ON

Enable Rear USB Ports ON

BIOS Password

These settings will apply in BIOS USB Configuration.

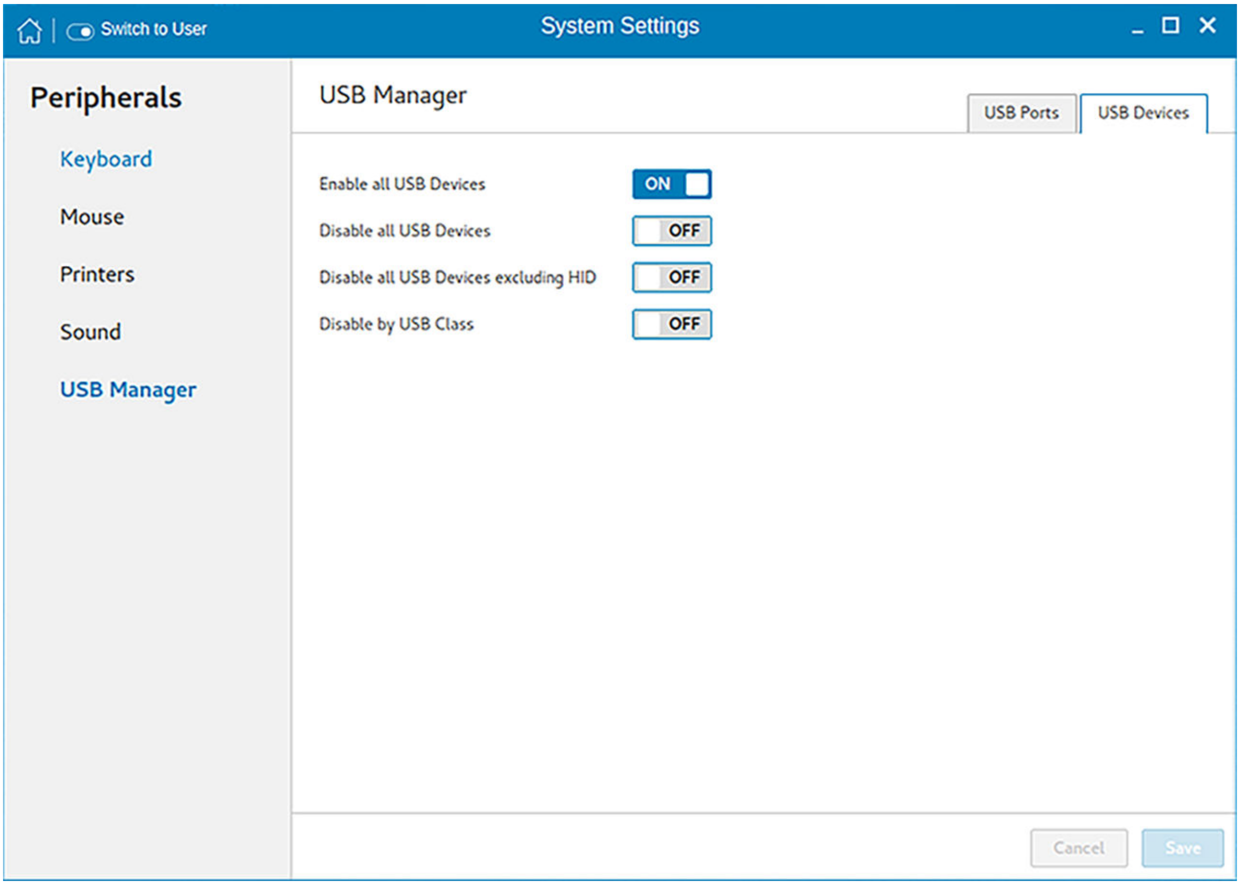
Figure 23. USB Manager

- **Enable USB Boot Support**—Click the **ON/OFF** button to enable or disable the USB boot setup. If this option is enabled, you can use a USB storage device to boot the operating system.
- **Enable Front USB Ports**—Click the **ON/OFF** button to enable or disable the front USB port(s). If the USB port is disabled, the operating system cannot detect the device that is attached to this port.
- **Enable Rear USB Ports**—Click the **ON/OFF** button to enable or disable the rear USB port(s). If the USB port is disabled, the operating system cannot detect the device that is attached to this port.
- **BIOS Password**—Enter the BIOS password.

  > **NOTE: If BIOS is configured to use the admin password and if the BIOS password is not set, any changes to the USB port settings are not saved after rebooting the thin client.**

2 In the **USB Devices** tab, configure any of the following options:

- **Enable all USB Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system detects all USB devices connected to the thin client.



USB Manager

Enable all USB Devices ON

Disable all USB Devices OFF

Disable all USB Devices excluding HID OFF

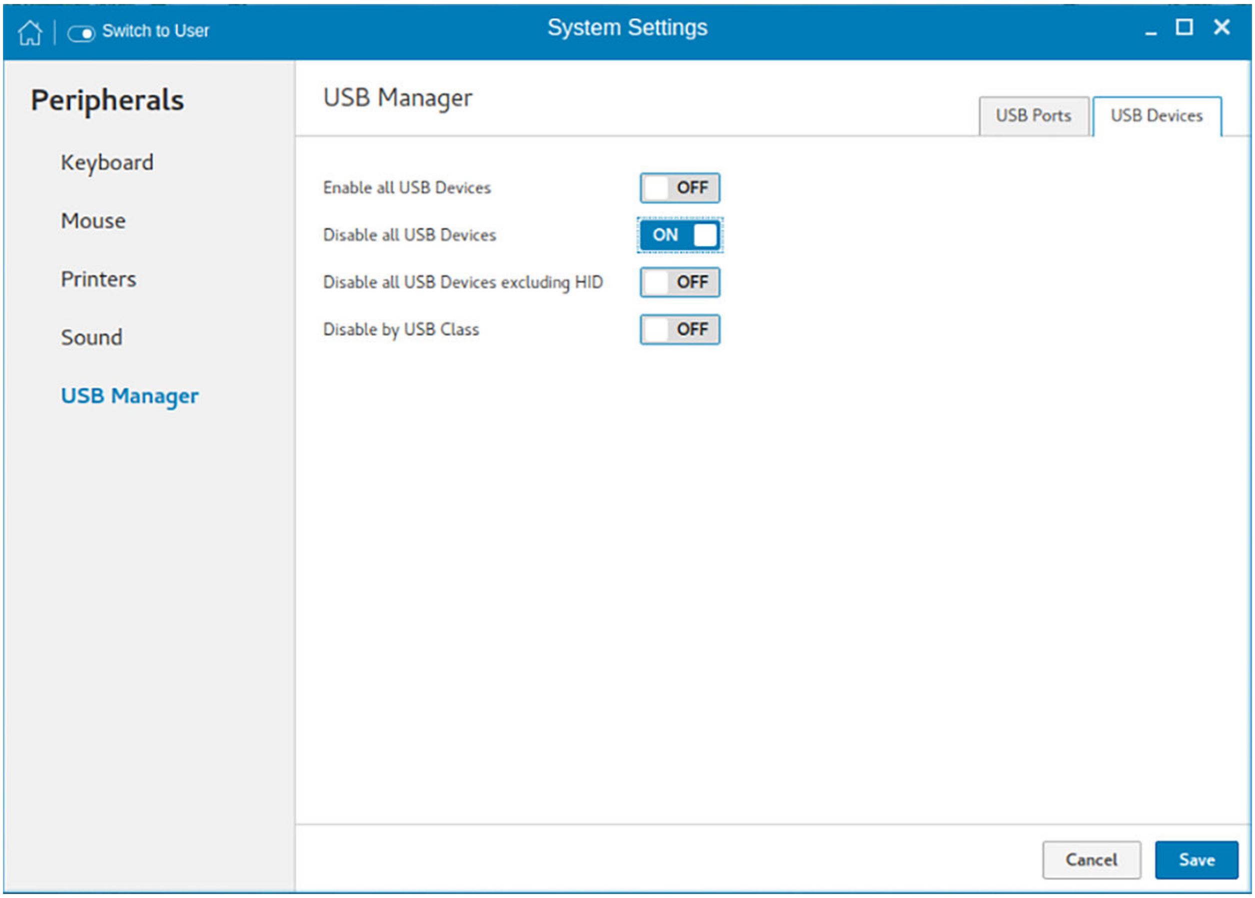
Disable by USB Class OFF

Figure 24. Enable all USB devices

If this option is disabled, you must enable one of the following options:

- **Disable all USB Devices**
- **Disable all USB Devices excluding HID**
- **Disable by USB Class**

- **Disable all USB Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system does not detect USB devices connected to the thin client.



Enable all USB Devices OFF

Disable all USB Devices ON

Disable all USB Devices excluding HID OFF

Disable by USB Class OFF

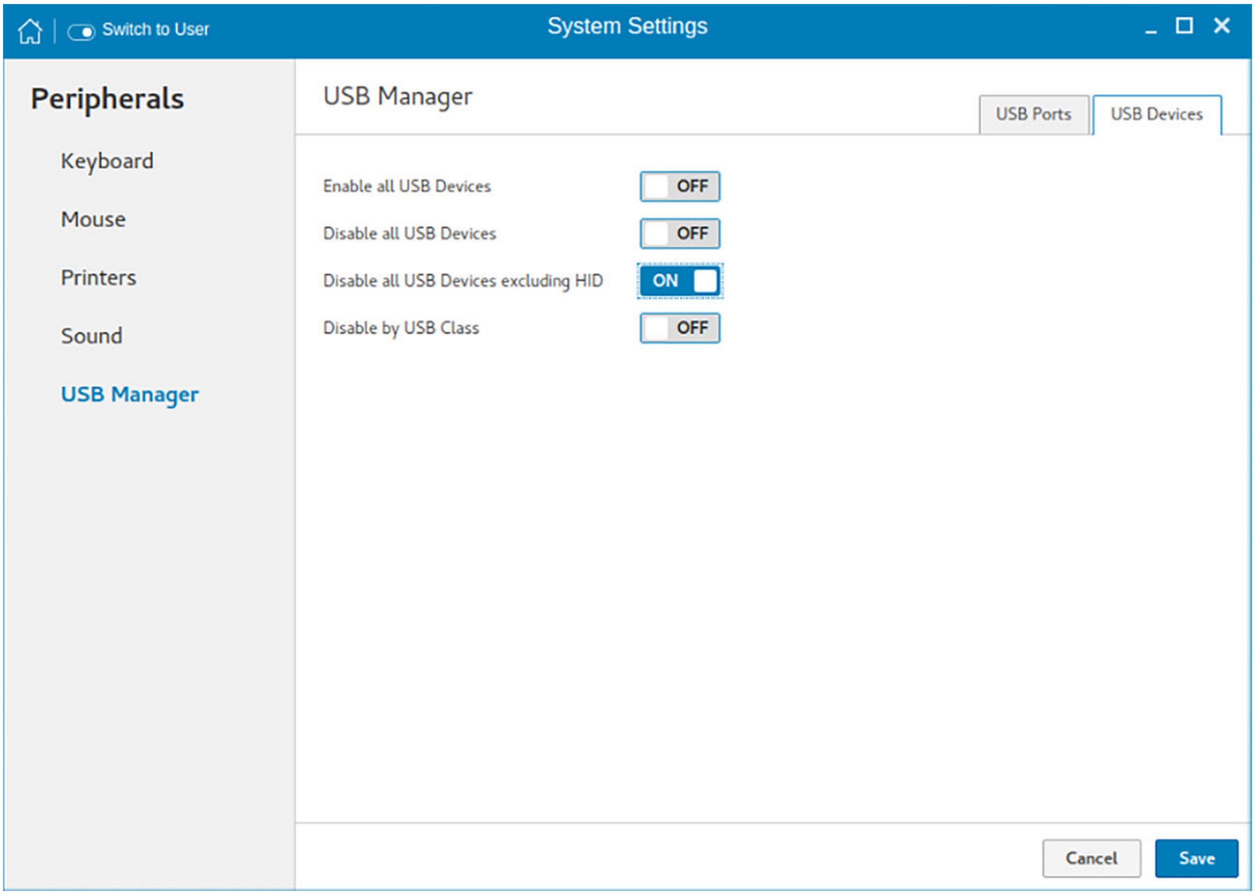
Figure 25. Disable all USB devices

If this option is disabled, you must enable one of the following options:

- **Enable all USB Devices**
- **Disable all USB Devices excluding HID**
- **Disable by USB Class**

> NOTE:
>
> If the **Disable all USB Devices** option is enabled, all USB devices including keyboard and mouse are disabled. You cannot reset the settings or use the G-key option.

- **Disable all USB Devices excluding HID**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system detects only Human Interface Devices (HID) such as keyboard and mouse.



Enable all USB Devices OFF

Disable all USB Devices OFF

Disable all USB Devices excluding HID ON

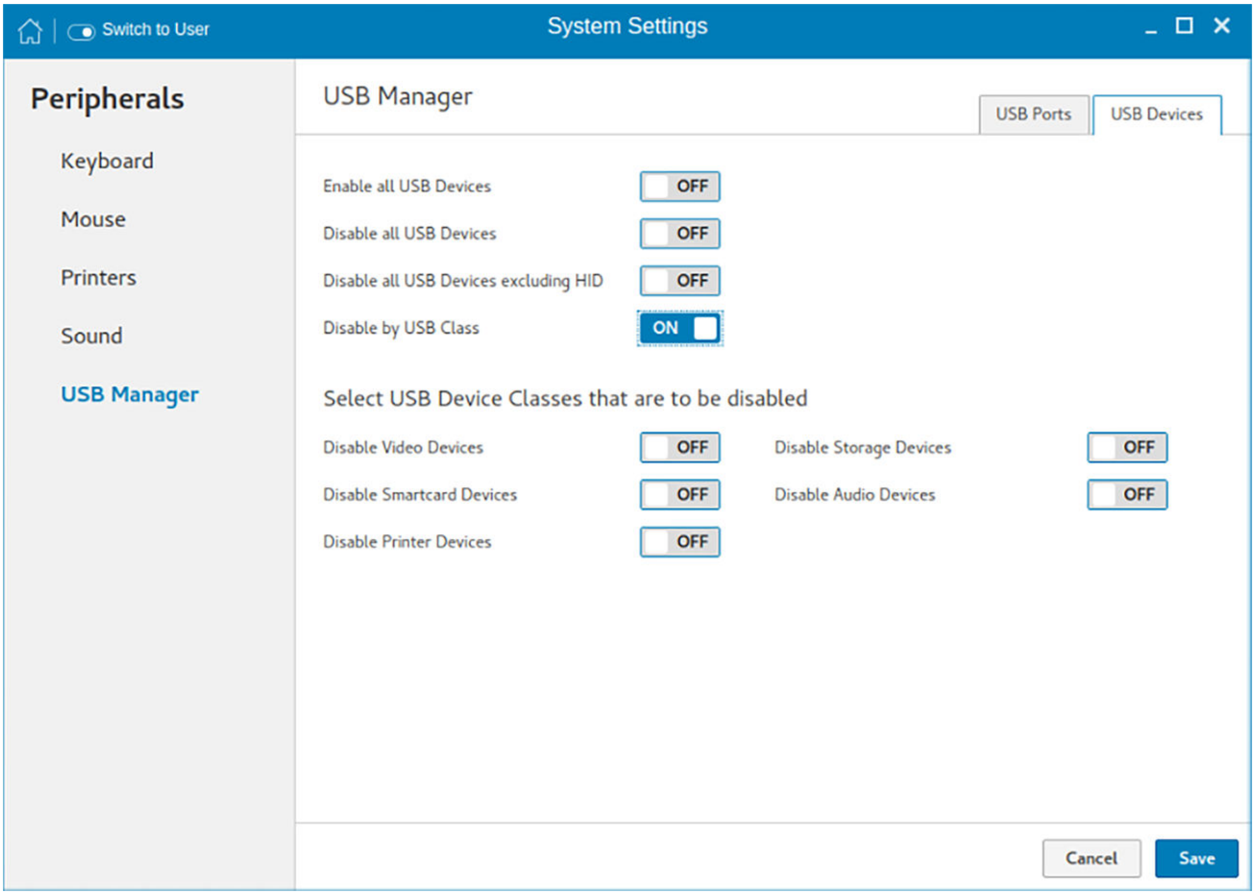
Disable by USB Class OFF

Figure 26. Disable all USB Devices excluding HID

If this option is disabled, you must enable one of the following options:

- **Enable all USB Devices**
- **Disable all USB Devices**
- **Disable by USB Class**

- **Disable by USB Class**—Click the **ON/OFF** button to enable or disable this option.



USB Manager

Enable all USB Devices OFF

Disable all USB Devices OFF

Disable all USB Devices excluding HID OFF

Disable by USB Class ON

Select USB Device Classes that are to be disabled

Disable Video Devices OFF

Disable Storage Devices OFF

Disable Smartcard Devices OFF

Disable Audio Devices OFF

Disable Printer Devices OFF

Figure 27. Disable by USB Class

If this option is enabled, you must configure any of the following options:

- **Disable Video Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system does not detect the video devices connected to the thin client.
- **Disable Storage Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system does not detect the storage devices connected to the thin client.
- **Disable Smartcard Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system does not detect the smart card devices connected to the thin client.
- **Disable Audio Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system does not detect the audio devices connected to the thin client.
- **Disable Printer Devices**—Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the operating system does not detect the printers connected to the thin client.

3 Click **Save** to save the settings.

Network

On the **System Settings** page, click the **Network** tab to view the **Network Settings** page.

1 Click the **Network** icon.

2 The **Network settings** page is displayed. In the left-pane, the following tabs are available for you to configure.

- Wi-Fi
- Wired
- Network proxy

Configuring the wi-fi settings

To configure the Wi-Fi settings, perform the following steps:

1 In the left-pane, click **Wi-Fi** tab.

2 Click the **ON/OFF** button to enable or disable the Wi-Fi option. The list of wireless SSID is displayed if broadcast is enabled.

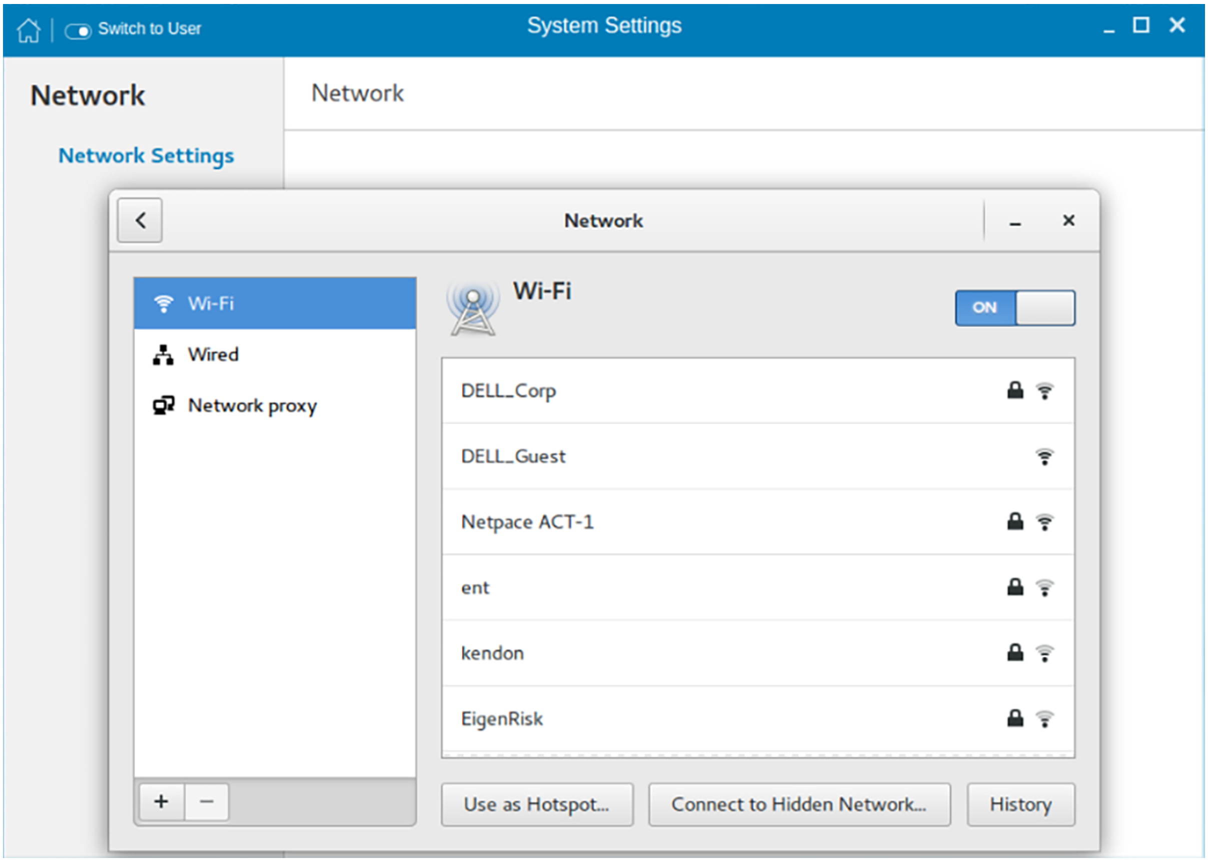
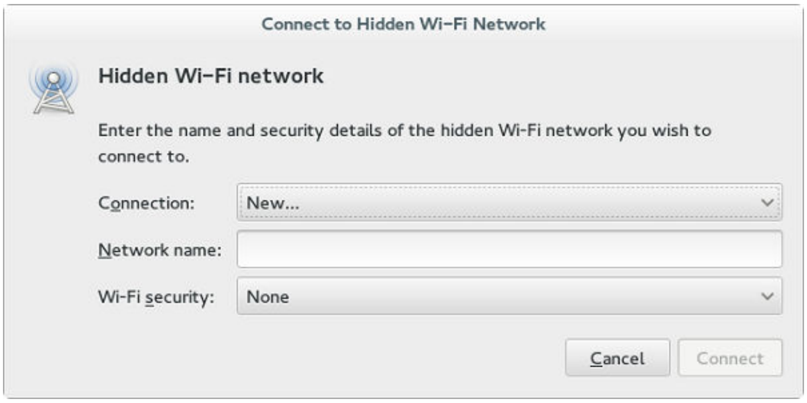


Figure 28. Wi-Fi Settings

3 To connect to Wi-Fi connection, select the preferred wireless SSID from the list displayed.

4 Click the **Connect to Hidden Wi-Fi Network** button. The Connect to Hidden Wi-Fi Network window is displayed.


Connect to Hidden Wi-Fi Network

Hidden Wi-Fi network

Enter the name and security details of the hidden Wi-Fi network you wish to connect to.

Connection: New...

Network name:

Wi-Fi security: None

Figure 29. Hidden Wi-Fi Network

5 Enter the name and security details of the hidden network that you want to connect to.

Table 2. Hidden network

Parameter	Description
Connection	From the drop-down list, select the type of connection.
Network name	Enter the preferred network name.
Wi-Fi security	From the drop-down list, select the security type.

6 On the **Network** page, click the **History** button to view the previous Wi-Fi connections and details.

Configuring wired network connection settings

To configure the wired connection settings, perform the following steps:

1 Click the **Wired** tab. The following attributes are displayed if the network cable is connected to your thin client and wired connection is established.
- IPv4 Address
- IPv6 Address
- Hardware Address
- Default Route
- DNS

ⓘ NOTE: **After the network is disconnected, only hardware address and last used information are displayed.**

2 On the lower-right corner of the page, click the **Settings** icon to configure the Wired Network connections.
   a In the **Details** tab, the following attributes are displayed.
      - Link Speed
      - IPv4 Address
      - IPv6 Address
      - Hardware Address
      - Default Route
      - DNS

3 Click the **Security** tab to configure the 802.1x security settings.
   a Click the **ON** button to enable the 802.1x Security for your network connection.
   b From the **Authentication** drop-down list, select the type of authentication you want to set for your network connection. The available options are:
      - TLS

- Protected EAP (PEAP)

You must configure TLS and PEAP using the INI parameters only. Options that you configure using the INI parameters are populated on the UI screen. For more information about the usage of INI parameters, see Dell Wyse ThinLinux INI Reference Guide.

> ⓘ **NOTE: You cannot configure the 802.1x authentication settings using the GUI options.**

4 Click the **Identity** tab and configure the following settings:

> ⓘ **NOTE: Only Administrators are allowed to authenticate these settings by entering the admin password in the root privilege authentication dialog box after a particular setting is changed or configured.**

a **Name**—Specifies the default name of the wired connection. If you want to set your preferred name for the connection, enter the name and then click **Apply**.

b **MAC Address**—Specifies the MAC address of the network connection.

c **Cloned Address**—Specifies the IP address that is cloned by the router.

d **Maximum transmission unit (MTU)**—Specifies the size (in bytes) of the largest protocol data unit that the protocol layer can pass onwards.

e **Firewall Zone**—Specifies the security level of the connection.

f **Connect automatically**— Select this check box to automatically connect to the network after you plug-in the network wire.

g **Make available to other users**— Select this check box if you want to allow other users to configure these settings.

5 Click the **IPv4** tab and do the following:

a Enable the **IPv4** button to configure the IPv4 settings.

b From the **Addresses** drop-down menu, select the type of IPv4 configuration. The available options are:

- Automatic (DHCP)
- Manual
- Link-Local Only

c If **Automatic (DHCP)** option is selected, you must configure the following options.

Table 3. Automatic (DHCP)

Parameter	Description
DNS	Enable the **Automatic** button, if you want the thin client to automatically fetch the DNS Server.
Server	Specifies the IP address of the DNS Server. Click the **+** icon to add a new DNS server to the list.
Routes	Enable the **Automatic** button to turn on the automatic IPv4 routing.
Address	Specifies the Router IP address.
Netmask	Specifies the Netmask. Netmask is used to divide an IP address into subnets and specify the network's available hosts.
Gateway	Specifies the IP address of the default Gateway.
Metric	Specifies the Metric value for the network connection.
Use this connection only for resources on its network	Select this check box, if you want to allow the wired connection only for resources on its network.

d If **Manual option** is selected, you must specify the IP address, Netmask IP and Gateway IP along with the parameters mentioned in the Automatic (DHCP) table.

   e. If **Link-Local Only** option is selected, the DNS and Routes options are disabled. This is applicable only for communications within the host link or the host domain.

6. Click the **IPv6** tab and do the following:
   a. Enable the **IPv6** button to configure the IPv6 settings.
   b. From the **Addresses** drop-down menu, select the type of IPv6 configuration. The available options are:
      - Automatic
      - Automatic, DHCP only
      - Manual
      - Link-Local Only

      The IPv6 configuration is similar to configuring the IPv4 Settings. For IPv4 configuration, see the IPv4 settings in this section.
7. Click the **Reset** tab and do the following:
   a. Click **Reset** to reset the settings for your network connection, including passwords. However, the previous network is displayed as a preferred network.
   b. Click **Forget** to remove all details relating to this network that you do not want to automatically connect to.
8. Click **Apply** to save your configured settings.

ⓘ NOTE: **Click the Add Profile tab to add a new network profile. On the right pane, you must configure the following options:**

- Security
- Identity
- IPv4
- IPv6

The configuration of all these tabs are similar to **Wired Network connections configurations** described in this section.

Configuring the network proxy settings

To configure the Network proxy settings, complete the following task:

1. Click the **Network proxy** tab.
2. From the Proxy drop-down menu, select the type of Proxy method you want to deploy. The available Proxy methods are:
   - None
   - Manual
   - Automatic
3. If **Manual proxy** method is selected, you must configure the following options:
   a. Enter the **HTTP Proxy** port details for your network connection.
   b. Enter the **HTTPS Proxy** port details for your network connection.
   c. Enter the **FTP Proxy** port details for your network connection.
   d. Enter the **SOCKS host** port details for your network connection.
   e. Use the **Ignore Hosts** option to set up proxy to ignore all local addresses.
4. If **Automatic proxy** method is selected, you must type the configuration URL address in the field.

   ⓘ NOTE: **Web Proxy Autodiscovery is used when a Configuration URL is not provided. Dell does not recommend this option for untrusted public networks.**

Adding a network connection

ⓘ NOTE: **Adding additional wired Ethernet connections is allowed but the added interface is not used in any of the ThinLinux features.**

To add a new network connection, complete the following tasks:

1. On the lower-left corner of the page, click the **+** icon.

   The **Add Network Connection** dialog box is displayed. The following options are listed for you to configure.

   - VPN
   - Bond
   - Team
   - Bridge
   - VLAN
2. Click **VPN** to add a VPN network connection. You must import a file from the stored location to configure the VPN settings.
3. Click **Bond** to add and configure the Bond network connection for your thin client.
   a. Click the **General tab**, and configure the following options:
      - Select any of the following check boxes based on your requirement:
        – Automatically connect to this network when it is available.
        – All users may connect to this network.
        – Automatically connect to VPN when using this connection.
      - From the drop-down menu, select the firewall zone.

   b. Click the **Bond** tab, and configure the following options:
      1. Type a name for your network interface.
      2. The number of bonded connections that are set up are listed here. To add a new bond connection, click the **Add** button and select the type of connection you want to create. The available options are Ethernet, InfiniBand, Bond, Bridge, Team, and VLAN.
      3. Select the type of Network Mode from the drop-down list. The available options are:
         - Round-robin
         - Active Backup
         - XOR
         - Broadcast
         - 802.3ad
         - Adaptive transmit load balancing
         - Adaptive load balancing
      4. **Link Monitoring** — Select the type of link monitoring from the drop-down list. The available options are:
         - MII (recommended)
         - ARP
      5. Enter the time in ms for the link up delay duration.
      6. Enter the time in ms for the link down delay duration.

   c. Click the **IPv4 Settings** tab, and do the following:
      1. From the drop-down list select the following method for IPv4 authentication.
         - If **Automatic (DHCP)** method is selected, you must configure the following options:
           1. Additional DNS Servers — Type the IP addresses of domain name users that are used to resolve host names. Use commas to separate multiple domain name server addresses.
           2. Additional Search Domains — Type the IP addresses of domains used when resolving host names. Use commas to separate multiple domains.
           3. DHCP client ID — Enter the ID for the DHCP client. This client identifier allows the network administrator to customize your computer's configuration.
           4. Require IPv4 addressing for this connection to complete — The IPv4 address is required to complete the connection. If the IPv4 address is not available, then the connection is not configured.

5 Click the **Routes** button to edit IPv4 routes for Bond connection.

    a Click **Add** to add an IP address. After an IP is added, Netmask, Gateway and Metric specific to that IP are displayed.

    b Select the check box if you want to ignore the automatically obtained routes.

    c Select this check box if you want to use your connection only for resources on that particular network.

- If **Automatic (DHCP) addresses only** method is selected, you must configure the following options:

    1 DNS Servers — Type the IP addresses of domain name users that are used to resolve host names. Use commas to separate multiple domain name server addresses.

    2 Search domains — Type the IP addresses of domains that are used when resolving host names. Use commas to separate multiple domains.

    3 DHCP client ID — Enter the ID for the DHCP client. This client identifier allows you to customize your computer's configuration.

    ⓘ NOTE: **The other settings remain same as described in automatic (DHCP) method for IPv4 authentication.**

- If **Manual** method is selected, you must configure the following options:

    1 Click **Add** to add an IP address. After an IP is added, Netmask, Gateway specific to that IP are displayed.

    2 DNS Servers — Type the IP addresses of domain name users that are used to resolve host names. Use commas to separate multiple domain name server addresses.

    3 Search domains — Type the IP addresses of domains used when resolving host names. Use commas to separate multiple domains.

    ⓘ NOTE: **The DHCP client ID option and Ignore automatically obtained routes check boxes are disabled.**

    The other settings remains the same as described in automatic (DHCP) method for IPv4 authentication.

- If **Link-Local Only** method is selected, the DNS Servers, Search domains, DHCP client ID, and Routes options are disabled. You can select the **Require IPv4 addressing for this connection to complete** check box to allow the connection to complete. The IPv4 address is required to complete the connection. If the IPv4 address is not available, then the connection is not configured.
- If **Shared to other computers** method is selected, the DNS Servers, Search domains, DHCP client ID, and Routes options are disabled. You can select the **Require IPv4 addressing for this connection to complete** check box to allow the connection to complete. The IPv4 address is required to complete the connection. If the IPv4 address is not available, then the connection is not configured.
- If **Disabled** option is selected, IPv4 is not available for this connection.

d Click the **IPv6 Settings** tab. From the drop-down list, select the following method type for IPv4 authentication. The available options are:

- Ignore
- Automatic
- Automatic, addresses only
- Manual
- Link-Local Only

ⓘ NOTE: **The settings are same as configuring the IPv4 settings tab described in this section.**

4 Click **Team** to add and configure the team network connection for your thin client.

a Click the **Team** tab, and configure the following options:

1 Interface name—Type the name of your network interface.

2 MTU—Specifies the size (in bytes) of the largest protocol data unit that the protocol layer can pass onwards.

3 Teamed connections—Lists the number of team connections that are configured. To add a new team connection, click **Add** and select the type of connection you want to create. The available options are Ethernet, Bond, Bridge, Team, and VLAN.

        4. JSON config— If you have already added a new team connection, you can enter a custom JSON configuration string in the text box or import a configuration file.
    b. To configure the **General** tab, **IPv4 Settings** tab, and **IPv6 Settings** tab for team connection, see the configuration details for Bond connection in this section.
5. Click **Bridge** to add and configure the bridge network connection for your thin client.
    a. Click the **Bridge** tab, and configure the following options:
        1. Interface name — Type the name for your network interface.
        2. Bridged connections — The number of bonded connections that are set up are listed here. To add a new bond connection, click the Add button and select the type of connection you want to create. The available options are Ethernet, Wi-Fi, and VLAN.
        3. Aging time — Enter the Aging time duration in seconds.
        4. Enable IGMP snooping—Select this check box to monitor Internet Group Management Protocol (IGMP) communications among devices.
        5. Enable STP — Select this check box to enable the Spanning Tree Protocol (STP) for your connection.
        6. Priority — Enter the priority value.
        7. Forward delay — Enter the forward delay duration in seconds.
        8. Hello time — Enter the hello time duration in seconds.
        9. Max age — Enter the value for the maximum age.
    b. To configure the **General** tab, **IPv4 Settings** tab, and **IPv6 Settings** tab for Bridge connection, see the configuration details for Bond connection in this section.
6. Click **VLAN** to add and configure the VLAN network connection for your thin client.
    a. Click the **VLAN** tab, and configure the following options:
        1. Parent interface — Type the name for your parent interface.
        2. VLAN ID — Enter the value for the VLAN id.
        3. VLAN interface name — Type the name for your VLAN interface.
        4. Cloned MAC address — Type the cloned MAC address.
        5. MTU —Specifies the size (in bytes) of the largest protocol data unit that the protocol layer can pass onwards.
        6. Flags—Select the Reorder headers, Generic VLAN Registration Protocol (GVRP), Loose binding, and Multiple VLAN Registration Protocol (MVRP) check boxes to enable the respective functions for your VLAN connection.
    b. To configure the **General** tab, **IPv4 Settings** tab, and **IPv6 Settings** tab for VLAN connection, see the configuration details for Bond connection in this section.
7. Click **Save** to save your settings.

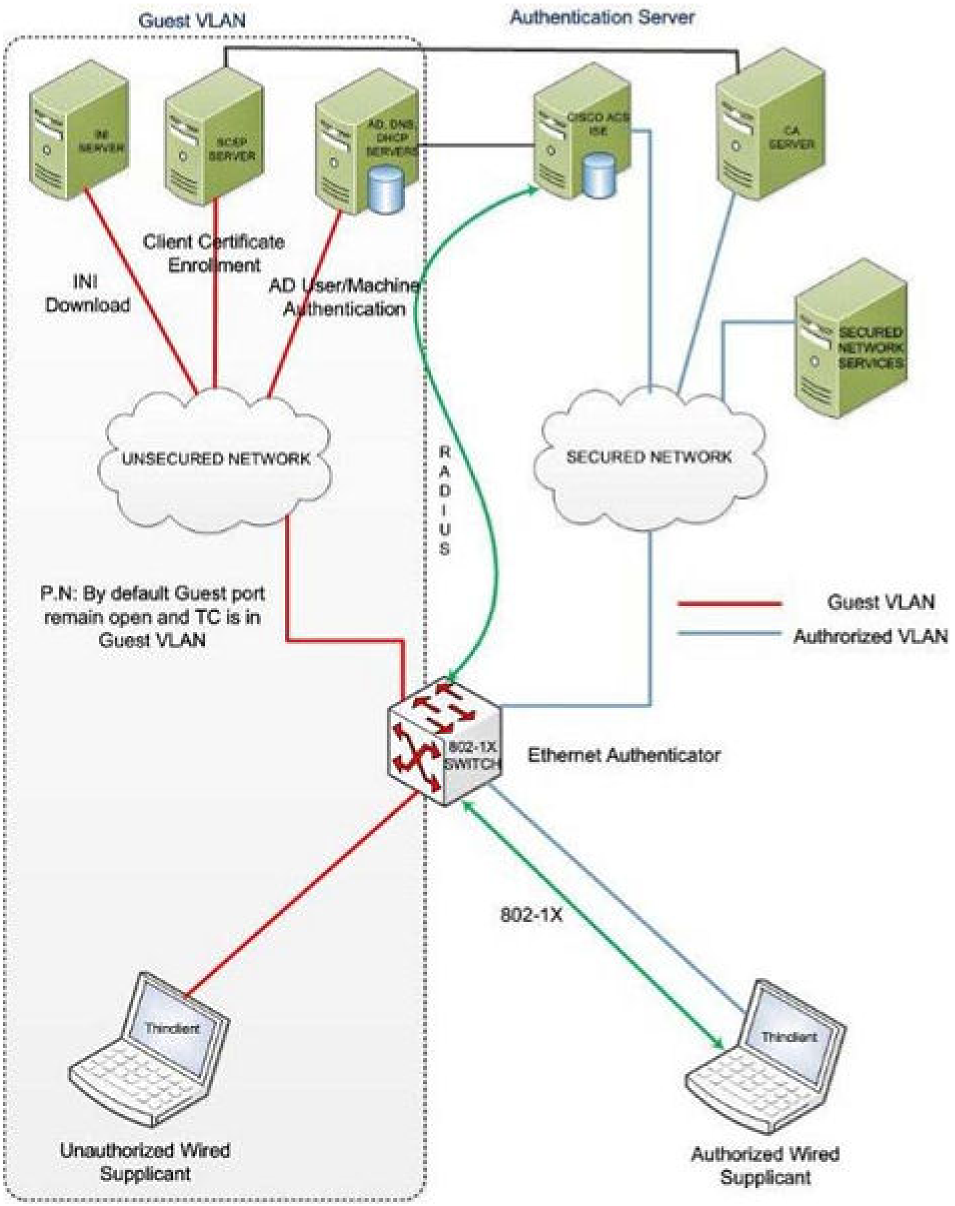
802.1x configuration

To configure the network connections:

NOTE: Currently, 802.1x configuration by using the Enable802 INI parameter is supported only for Wired connections and supported authentications are EAP-PEAP (MSCHAPv2) and EAP-TLS using SCEP.

- Supported seamless 802.1x authentication works with Linux thin clients by using Active Directory domain user credentials for EAP-MSCHAPv2 authentication, see EAP PEAP MSCHAPv2 Authentication Workflow.
- EAP-TLS is certificate-based authentication which uses SCEP for certificate enrollment, see EAP TLS Authentication Workflow.

The following diagram depicts communication between the components in an 802.1x Linux thin client solution.



NOTE: EAP-TLS security requires client side and server side certificates for mutual authentication. Every user and client, including the authentication server that participates in EAP-TLS, must have at least the following two certificates:

- Client certificate signed by the certificate authority (CA).
- Copy of the CA root certificate.

IMPORTANT: Dell recommends you to set INI values for all the 802.1x parameters because these parameters are part of the persistent registry which will remain across the reboot and if any parameter is not set, it will take the previously set value, which may show inconsistent behaviors.

EAP-PEAP MSCHAPv2 authentication workflow

When a Linux thin client is initially connected to the network, the thin client obtains Guest VLAN resources by default, that is TC should be able to reach INI server to fetch the INI configurations required for 802.1x configuration.

Pre-requisites for EAP-PEAP (MSCHAPv2) 802.1x authentication:

- Make sure that the INI file has the configurations for 802.1x, Active Directory server, and Domain and Import certs. If you are pushing a CA certificate by using the Dell Wyse Device Manager (WDM), the Imports Certs INI is not required, but you must be sure that the CA certificate name is correct in the 802.1x INI parameter. For more information, see *Dell Wyse ThinLinux INI Guide*.
- If you are using CA certificate for 802.1x authentication, then use the ImportCerts INI parameter to import CA certificates into the device. Ignoring CA certificate is considered as the default option, if the CA certificate name is not included in the 802–1x INI configuration.
- Domain List INI parameter is required to display the available domains on the GDM login screen.

EAP-PEAP (MSCHAPv2) 802.1x authentication can be configured in two different modes:

- User Authentication
- Machine Authentication

EAP-PEAP MSCHAPv2 user authentication

To authenticate 802.1x by using an Active Directory username account:

1. Turn on your thin client device.

   After the INI is downloaded to the thin client, you can access the domain that is configured in the INI from the domain drop-down list on the GDM Login screen.
2. On the GDM login screen, select the domain, and then enter the user domain credentials.
3. Click **Log in**.

   The 802-1 authentication automatically starts.

   > NOTE: **The GDM Authentication module performs the Network Manager configuration required for 802.1x PEAP (MSCHAPv2) authentication by using the credentials entered and 802.1x configurations from INI. Then, it reinitializes the network to do a direct 802.1x authentication with the switch.**

   - If **log in** is successful, then the thin client gets IP address from the protected VLAN and you can start the local thin client session (GNOME session). You can also start RDP, ICA, PCOIP sessions using the same domain credentials provided in the GDM login. These credentials will be preexisting in the connection manager, and you need not renter the same again.

     > NOTE:
     > – If you set Is802DirectEnabled=yes, the direct authentication is enabled which will trigger the 802.1x authentication from the GDM login screen. In this case the ActiveDirectoryServer parameter is not required.
     > – If you set Is802DirectEnabled=no, the 802.1x authentication is triggered after the user logs in to the thin client. In this case you need to include the ActiveDirectoryServer parameter in the INI.

   - If **log in** is unsuccessful, the 802.1x authentication fails and the thin client remains in the Guest VLAN.
4. When you log out or restart the device, thin client will again move to Guest VLAN by sending an EAPOL logoff to switch and disabling the 802.1x configuration at Network Connections applet.

The following is an example of the INI configuration for EAP-PEAP (MSCHAPv2) 802.1x User authentication.

For **AD and Domain settings**

```
DomainList=npac.local DisableDomain=no
```

For **Imports Certficates**

```
ImportCerts=no
```

For **802.1x Configuration**

```
Enable802=yes Authentication=PEAP InnerAuthentication=MSCHAPv2 PromptPassword=no AuthMode=User
Is802DirectEnabled=yes CACertificate=SCEP PeapVersion=Auto
```

EAP-PEAP MSCHAPv2 machine authentication

To enable EAP-PEAP (MSCHAPv2) machine authentication:

- Your machine must have an account created in the Active Directory database with Hostname as the username field.
- Set the same password for all machine/host name accounts to be created.
- The INI parameter should contain a **MachinePassword** Field that can be used for authentication.

To authenticate 802.1x using Machine name (Host name):

1. Turn on your thin client device.

   Once the INI is downloaded to the thin client and all the 802.1x parameters for machine PEAP authentication are retrieved from the INI server, the authentication starts in the background.

   The Authentication module performs the Network Manager configuration required for 802.1x PEAP MSCHAPv2 authentication by using the host name and password from INI and 802.1x configurations from INI.

   - If 802.1x authentication is successful, then thin client gets IP Address from protected VLAN.
   - If 802.1x authentication fails due to any wrong 802.1x configuration, then thin client remains in the Guest VLAN.
2. When you restart your thin client, the device moves to Guest VLAN by sending an EAPOL logoff to switch and disabling the 802.1x configuration at Network Connections applet.

The following is an example of the INI configuration for EAP-PEAP (MSCHAPv2) 802.1x machine authentication:

For **AD and Domain settings**

```
DomainList=npac.local DisableDomain=no
```

For **Imports Certificates**

```
ImportCerts=yes Certs=npac-ca-cert.cer
```

For **802.1x Configuration**

```
Enable802=yes Authentication=PEAP InnerAuthentication=MSCHAPv2 PeapVersion=Auto
PromptPassword=no CACertificate=npac-ca-cert.cer Authmode=Machine MachinePassword=tangocharlie
```

EAP TLS authentication workflow

When a Linux thin client is initially connected to the network, it should be able to obtain the Guest VLAN resources by default. It should be able to reach AD, DNS, SCEP and the INI server to fetch the INI configurations required for Active Directory Domain User Authentication, 802.1x, SCEP, and so on.

EAP-TLS 802.1x authentication can be configured in INI in two different modes:

- Machine Authentication.
- User Authentication.

EAP TLS – Machine authentication

The following steps are involved with 802.1x authentication:

- When the thin client restarts, it remains in the Guest VLAN and downloads the INI configuration from the INI server.

- The INI file must have the configurations for 802.1x EAP-TLS with AuthMode set for Machine Authentication and SCEP.
- After the INI is downloaded to the thin client, SCEP client enrolls the client certificate with Machine hostname and Domain configured in the INI.
- 802.1x EAP-TLS machine authentication will then begin and the thin client will move to an Authorized VLAN

> ⓘ **NOTE:**
>
> You can view the network progress icon on the taskbar.

- If 802.1x authentication fails due to any wrong 802.1x configuration, the thin client will automatically fall back to the Guest VLAN, with a notification message **Failed to connect to trusted network. Please contact your system administrator**, in the right pane of the GNOME panel. The user receives the same notification in the case of an expired CA certificate.
- When a user restarts the device, the thin client will again move to the Guest VLAN by sending an EAPOL logoff to switch and disable the 802.1x configuration at the Network Connections applet.

This is an example of the INI configuration for 802.1x TLS Machine authentication.

```
Enable802=yes Authentication=TLS PromptPassword=no CACertificate=scep UserCertificate=scep
PrivateKey=scep PrivateKeyPassword=ZG90MXg= AuthMode=Machine
```

EAP TLS User authentication

To authenticate 802.1x:

1. Turn on your thin client device.

   When the thin client restarts, the thin client remains in the Guest VLAN and downloads the ini configuration from the INI server.
2. After the INI is downloaded to the thin client, you can access the domain that is configured in the INI from the domain drop-down list on the GDM Login screen.
3. On the GDM login screen, select the domain, and then enter the user domain credentials.

   Domain User authentication is performed against the AD server mentioned in the INI configuration.
4. Click **Log in**.
   - If domain user login is successful, then the user certificate will be enrolled via SCEP, and 802.1x authentication will begin and you can see the network progress icon on the taskbar and the thin client will move to Authorized VLAN.
   - If 802.1x authentication fails due to any wrong 802.1x configuration or if the CA certificate has expired, the thin client will automatically fall back to Guest VLAN, and a notification message **Failed to connect to trusted network. Please contact your system administrator** is displayed in the right corner of GNOME panel.
   - When you log out or restart the thin client, the thin client as suggested above to Guest VLAN by sending an EAPOL logoff to switch and disabling the 802.1x configuration at the Network Connections applet.

This is an example of the INI configuration for 802.1x TLS User authentication.

```
Enable802=yes Authentication=TLS PromptPassword=no CACertificate=scep UserCertificate=scep
PrivateKey=scep PrivateKeyPassword=ZG90MXg= AuthMode=User
```

Personalization

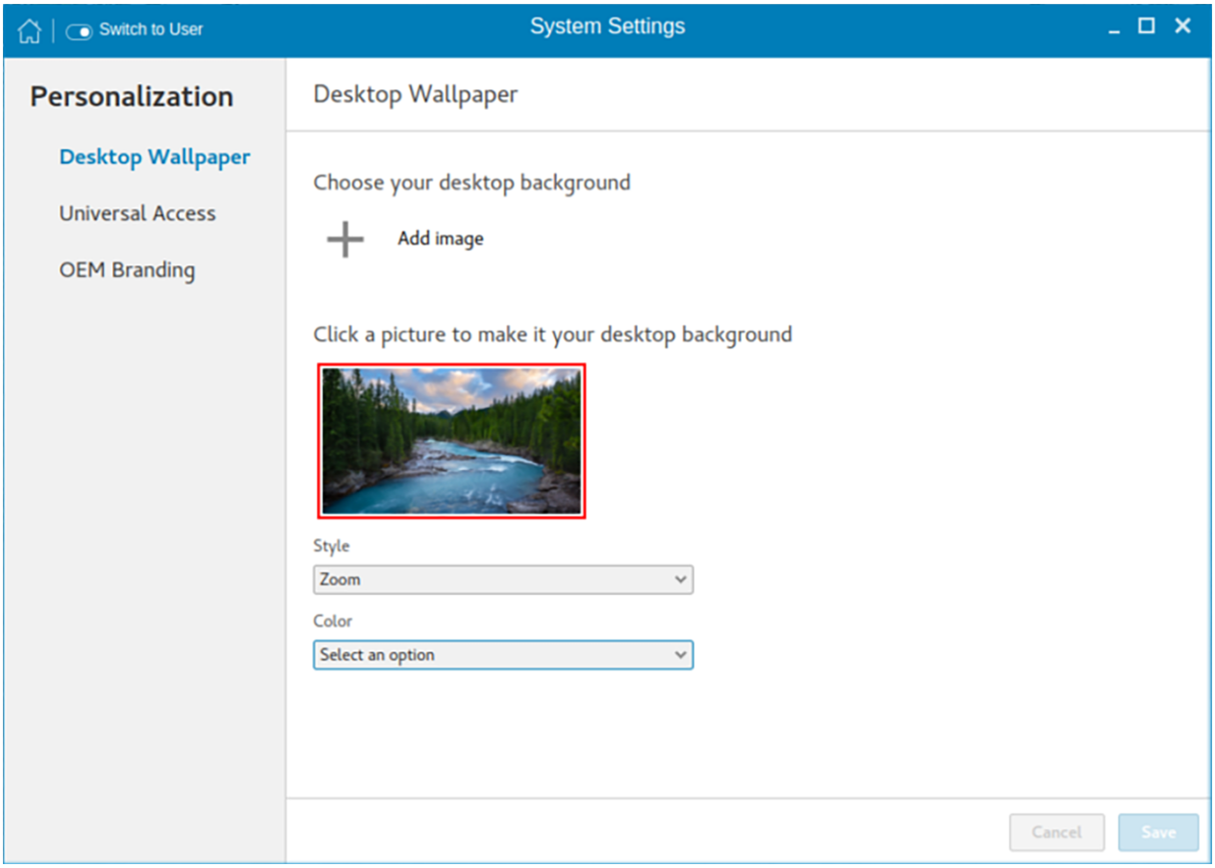
You can customize your desktop settings such as color, background in addition to enable various option that helps to improve the look and feel of the screen. Some of the important parameters such as display settings, audio settings, typing settings and pointer settings can be personalized.

On the **System Settings** page, click **Personalization** icon. The following tabs are listed on the left pane of the **System Settings** page.

- Desktop Wallpaper
- Universal Access
- OEM Branding

Setting the desktop wallpaper

Use this page to set the desktop wallpaper for your desktop.



Style: Zoom

Color: Select an option

Figure 30. Desktop wallpaper

1. Click **Add image** to load a desktop wallpaper from the USB drive.

   The wallpapers are listed on the screen.
2. Select a wallpaper for your desktop.
3. From the **Style** drop-down list, select a fit option.
4. From the **Color** drop-down list, select a color for your desktop.

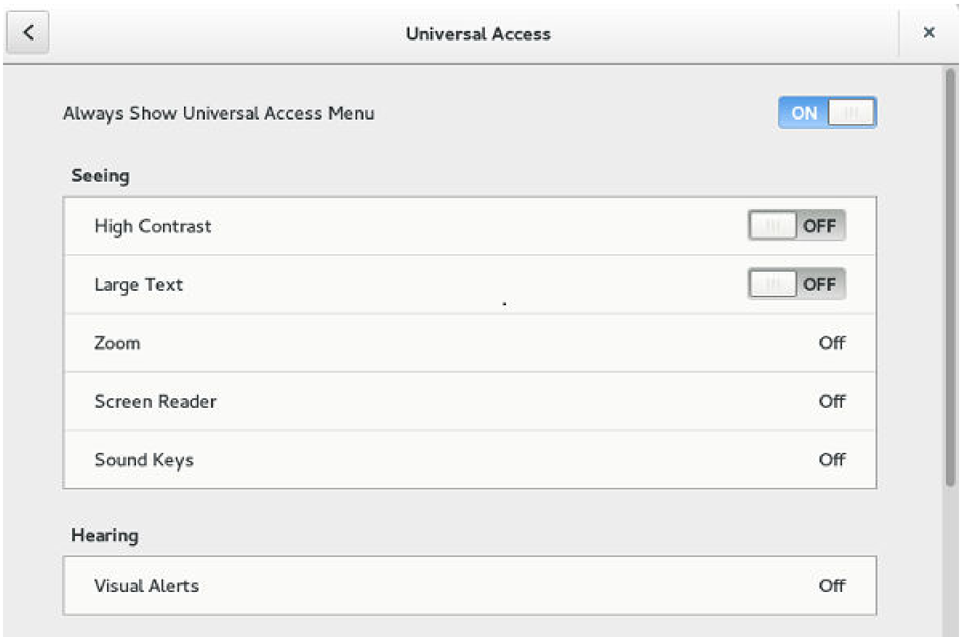
Use the desktop INI parameters to download a wallpaper to the thin client forcibly. For more information, see the *Dell Wyse ThinLinux INI Reference Guide* at www.dell.com/support.

Configuring universal access

The Universal Access page allows you to configure the display settings, audio settings, typing settings and pointer settings. The **Universal Access Menu** allows you to improve the look and feel of the desktop.

1. Click the desktop icon on the **Universal access** page.
2. Click the **ON/OFF** button to enable or disable the option. If enabled, the Universal Access menu can be viewed always.
3. Configure the following options:
   - Seeing

- Hearing
- Typing
- Pointing and Clicking



Universal Access

Always Show Universal Access Menu ON

Seeing

High Contrast OFF

Large Text OFF

Zoom Off

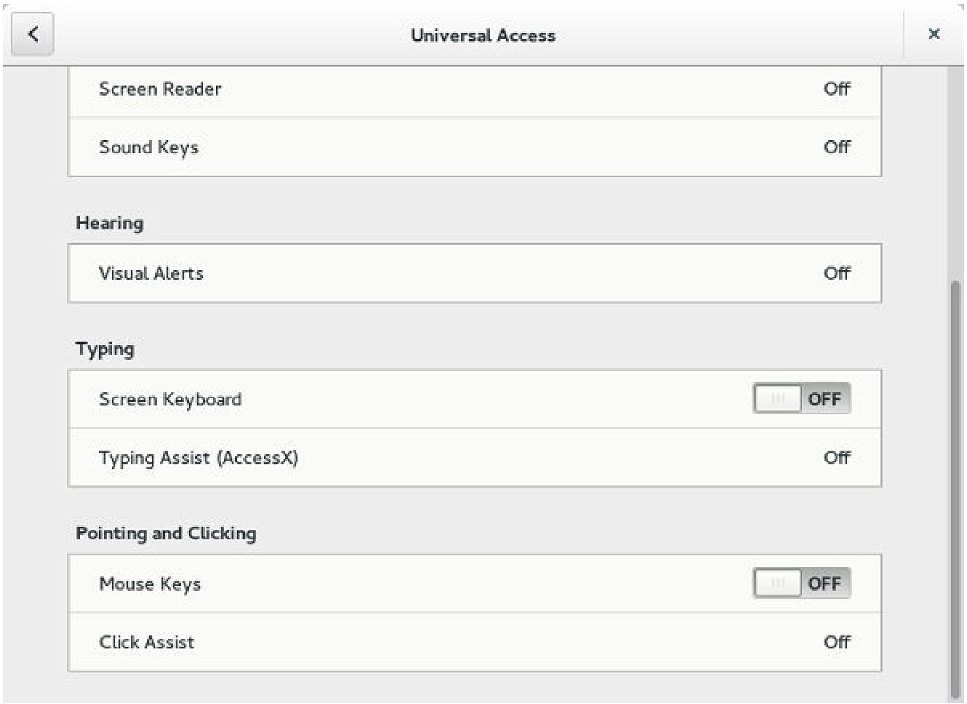
Screen Reader Off

Sound Keys Off

Hearing

Visual Alerts Off

Figure 31. Universal access



Universal Access

Screen Reader Off

Sound Keys Off

Hearing

Visual Alerts Off

Typing

Screen Keyboard OFF

Typing Assist (AccessX) Off

Pointing and Clicking

Mouse Keys OFF

Click Assist Off

Figure 32. Universal access

Seeing

The **Seeing** tab enables you to configure the display settings.

1. Click the **ON/OFF** button to enable or disable the High contrast option. If enabled, the contrast is increased and you can see the difference instantly.
2. Click the **ON/OFF** button to enable or disable the Large text option. If enabled, the text size is increased and you can see the difference instantly.
3. Click the **ON/OFF** button to enable or disable the zoom option. If enabled, the screen is zoomed in and you can control the screen by using the mouse.
   a. Click the **Magnifier** tab to configure the following settings:

      Table 4. Magnifier

Parameter	Description
Magnification	Click **+** to increase the magnification value and click **—** to decrease the magnification value.
Magnifier Position	Select the Magnifier Position. • If you select **Follow mouse cursor**, the other option is disabled. • If you select **Screen part**, select the screen resolution from the drop-down list.

   b. Click **Crosshairs** tab to configure the following settings:
      - Move the slider to the right to increase the **Thickness** and **Length** of the crosshairs.
      - Click the **Color** tab, and select the preferred color.

   c. Click **Color Effects** tab to configure the following settings:
      - Click the **ON/OFF** button to enable or disable the White on Black option.
      - Move the slider to the right to increase the **Brightness**, **Contrast** and **Color**

   d. Click **Close**.
4. Click the **ON/OFF** button to enable or disable the Screen Reader option. If enabled, the screen reader reads the displayed text as you move the text.
5. Click the **ON/OFF** button to enable or disable the Sound Keys option. If enabled the beep sound when number lock or caps lock is clicked is turned ON.

Hearing

This section allows you to configure the Audio alerts by providing an visual indication.

1. Click **Visual Alerts** to configure the visual effects.
2. Click the **ON/OFF** button to enable or disable the option.
3. Select the preferred options in Visual Alerts.
4. Click the **Test flash** tab to have a flash on the screen.
5. Click **Close**.

Typing

This section allows you to configure the typing settings:

1. Click the **ON/OFF** button to disable or enable the keyboard display on the screen.
2. Click the **Typing Assist (AccessX)** to configure the keyboard setting.

    a Click the **ON/OFF** button to enable the features using keyboard.
    b Click the **ON/OFF** button to enable or disable the Sticky Keys option.
    c Click the **ON/OFF** button to enable the long keypress and set the delay using Slow Keys option.

      There is a delay between the action and the result when a key is pressed.
    d Click the **ON/OFF** button to enable or disable the Bounce Keys option.

      This option is used to avoid using the fast duplicate keypress and set the delay.
3 Click **Close**.

Pointing and clicking

This section allows you to configure the Mouse settings.

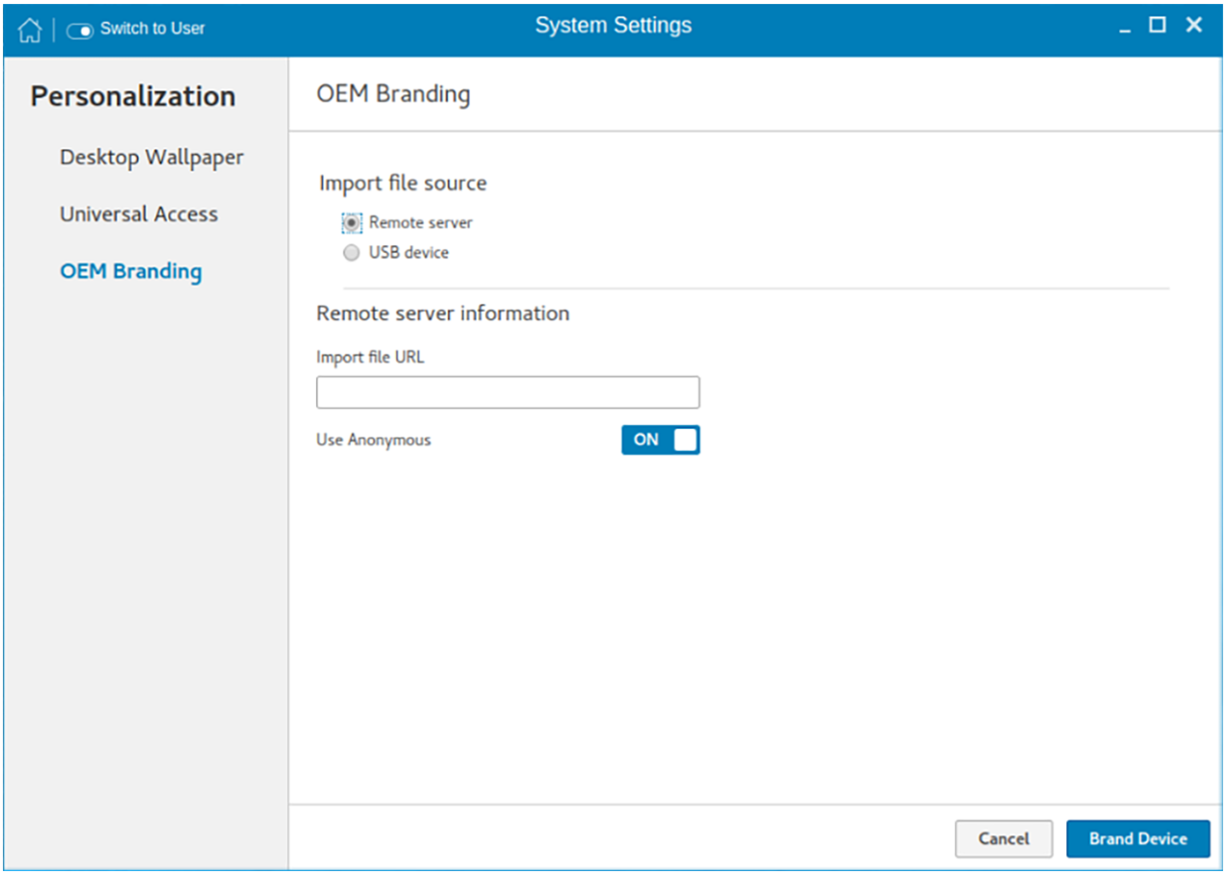
1 Click the **ON/OFF** button to enable or disable the Mouse Keys option.
2 Click the **Click Assist** tab to configure the settings.

Original Equipment Manufacturer branding

Original Equipment Manufacturer (OEM) branding page allows you to customize the manufacturer information for your ThinLinux client. You can customize the Bootsplash screen, Desktop wallpaper, Browser home page, and Product name in the **System Information** tab.

To set your OEM branding, do the following:

1 Import the OEM branding file to the thin client using any one of the following options:
    - **Remote server**—Select this option, and enter a valid server URL. To access the remote server, use the anonymous login option or enter the valid login credentials.



OEM Branding

Import file source

● Remote server

○ USB device

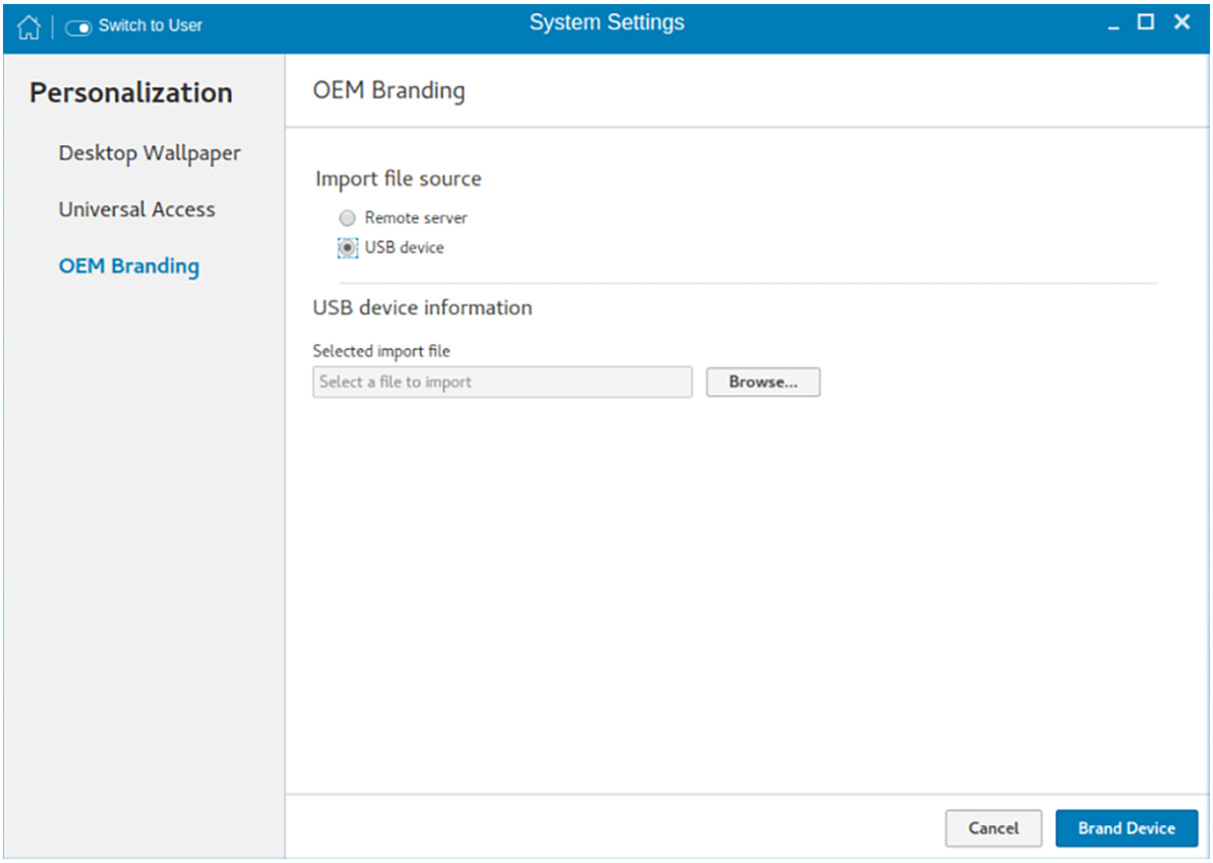
Remote server information

Import file URL

Use Anonymous ON

Figure 33. OEM branding - Remote server

- **USB device**—Select this option, and navigate to browse the file from the USB drive.



OEM Branding

Import file source

○ Remote server
● USB device

USB device information

Selected import file: Select a file to import

Figure 34. OEM branding - USB device

2 Click **Brand Device**.

The thin client restarts, and the device branding is customized based on your requirement.

Configuring Connections locally

On the **System Settings** page, click the **Connections** icon. The Connections page contains the following tabs:

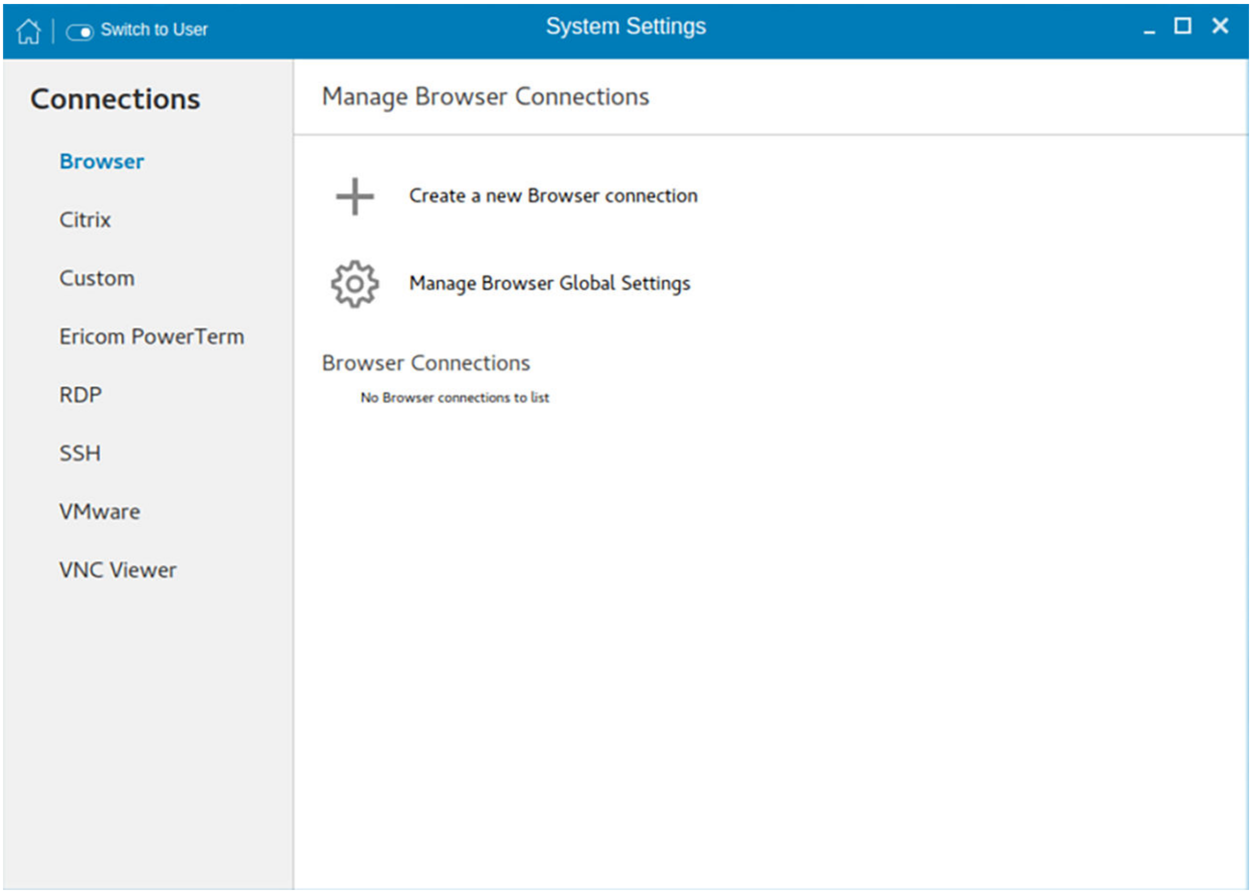
- Browser
- Citrix
- Custom
- Ericom PowerTerm
- RDP
- SSH
- VMware
- VNC Viewer

ⓘ **NOTE: The description names for all the connections can not be edited once you create the connection.**

Topics:

Configuring and managing the browser connections

The **Browser Connections** page enables you to create and manage Firefox browser connections for your thin client.



Manage Browser Connections

Browser Connections

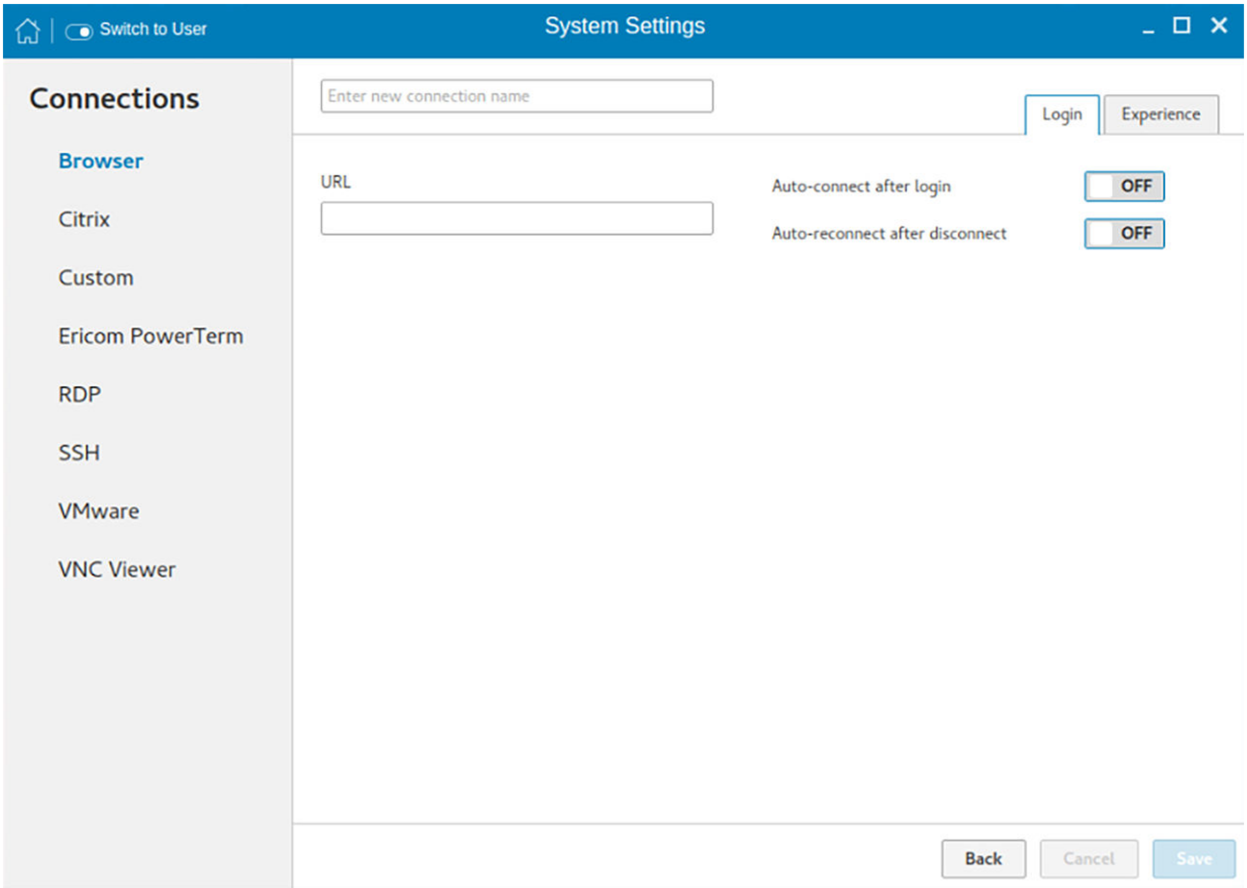
No Browser connections to list

Figure 35. Manage Browser Connections

To create a new browser connection:

1 Click the **+** icon to add a new browser connection.

The **Browser connection** page is displayed.



URL

Auto-connect after login OFF

Auto-reconnect after disconnect OFF

Figure 36. Browser connection login settings

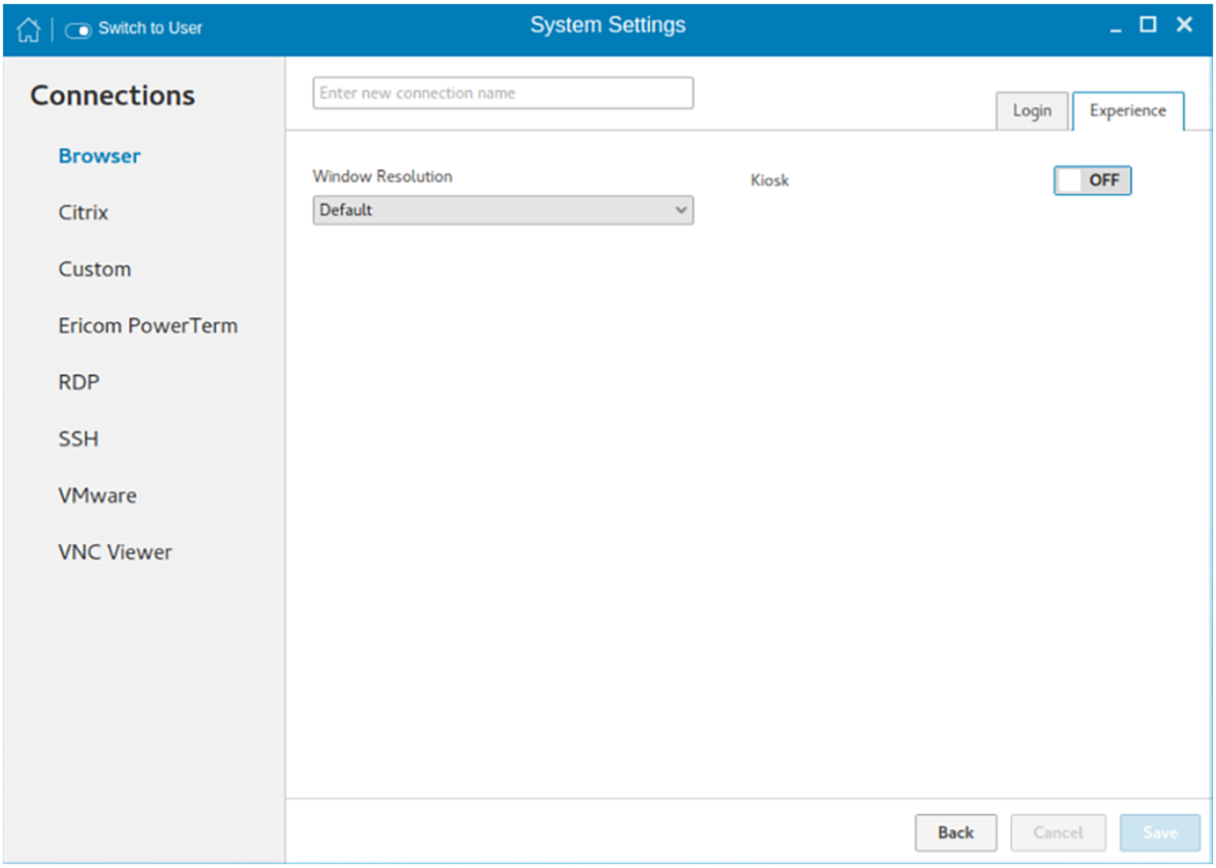
2 In the **Login** tab, enter the URL address of the browser connection you want to connect to.

3 Enter the name of the Browser connection for which you have specified the URL address.

4 Click the **ON/OFF** button to enable or disable the auto-connect option after you log in to the session.

5 Click the **ON/OFF** button to enable or disable the auto-reconnect option after you disconnect from the session. If the **Auto-reconnect** option is enabled, you can enter the **Delay duration (in seconds)** to reconnect to the session. The default value is 30 seconds.

6 Click the **Experience** tab to set the window resolution and Kiosk mode.



Window Resolution: Default

Kiosk: OFF

Figure 37. Browser connection experience settings

a From the drop-down list, select the window resolution you want to set for your Browser window.

b Click the **Kiosk** button to enable the Kiosk mode for your browser.

ⓘ NOTE: **When the Kiosk is Enabled, you cannot change window resolution.**

7 Click **Save** to save the changes.

The browser connection created by you is displayed in the Browser Connections list.

To manage a **Browser** connection:

1 Hover the mouse over a particular browser connection name. The Edit, Remove, and Connect options are displayed next to the browser connection name.

2 Click **Edit** to edit the URL address and other settings of the browser connection.

3 Click **Remove** to remove the browser connection from the list.

4 Click **Connect** to connect to the URL address you have specified for your browser connection. The webpage opens on your default browser.

Managing browser global settings

The **Manage Browser Global Settings** page enables you to configure browser settings for Mozilla Firefox and Google Chrome.

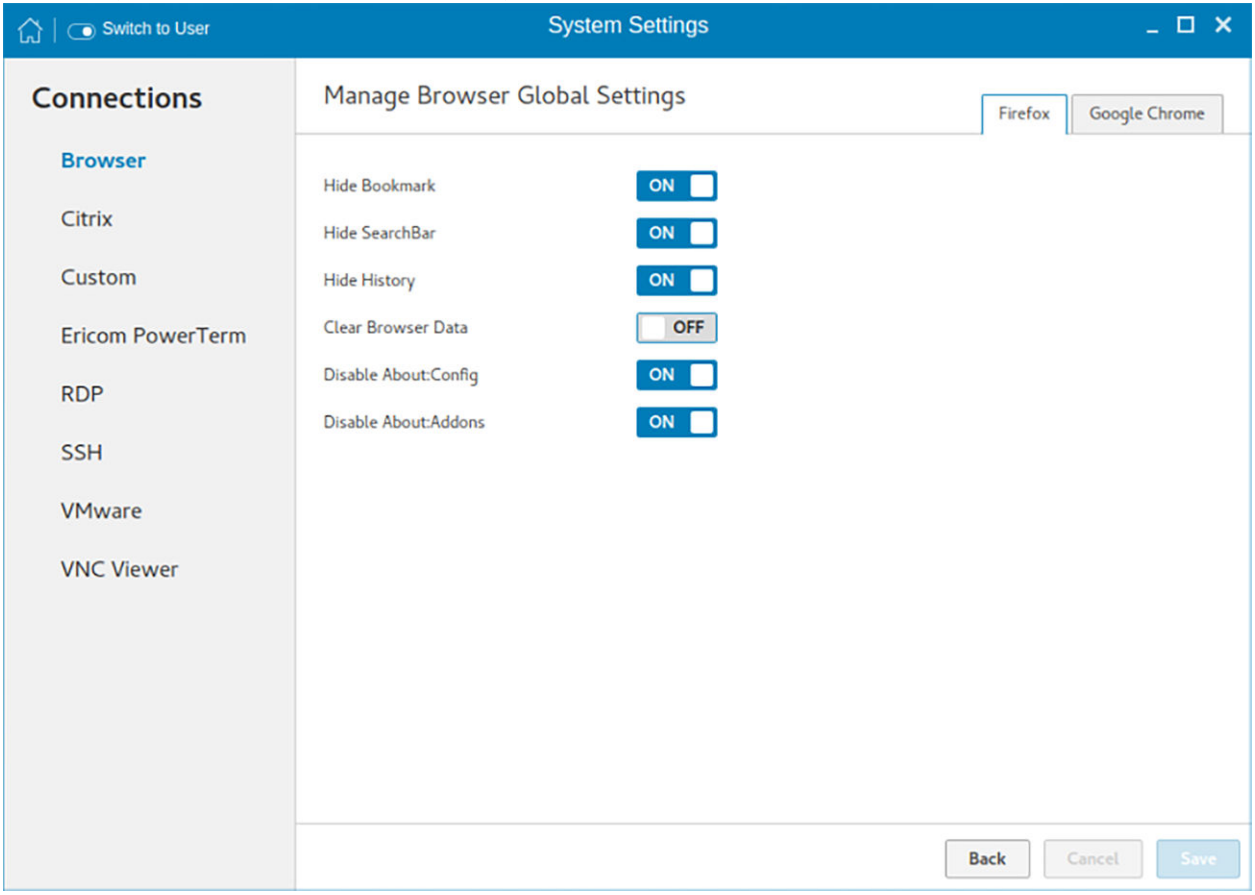
To configure the browser global settings, do the following:

1 Click the **Manage Browser Global Settings** icon.

The **Manage Browser Global Settings** page is displayed.

2 Configure your browser settings based on the requirement.

- If you are using **Firefox**, configure any of the following options:



Hide Bookmark ON

Hide SearchBar ON

Hide History ON

Clear Browser Data OFF

Disable About:Config ON

Disable About:Addons ON

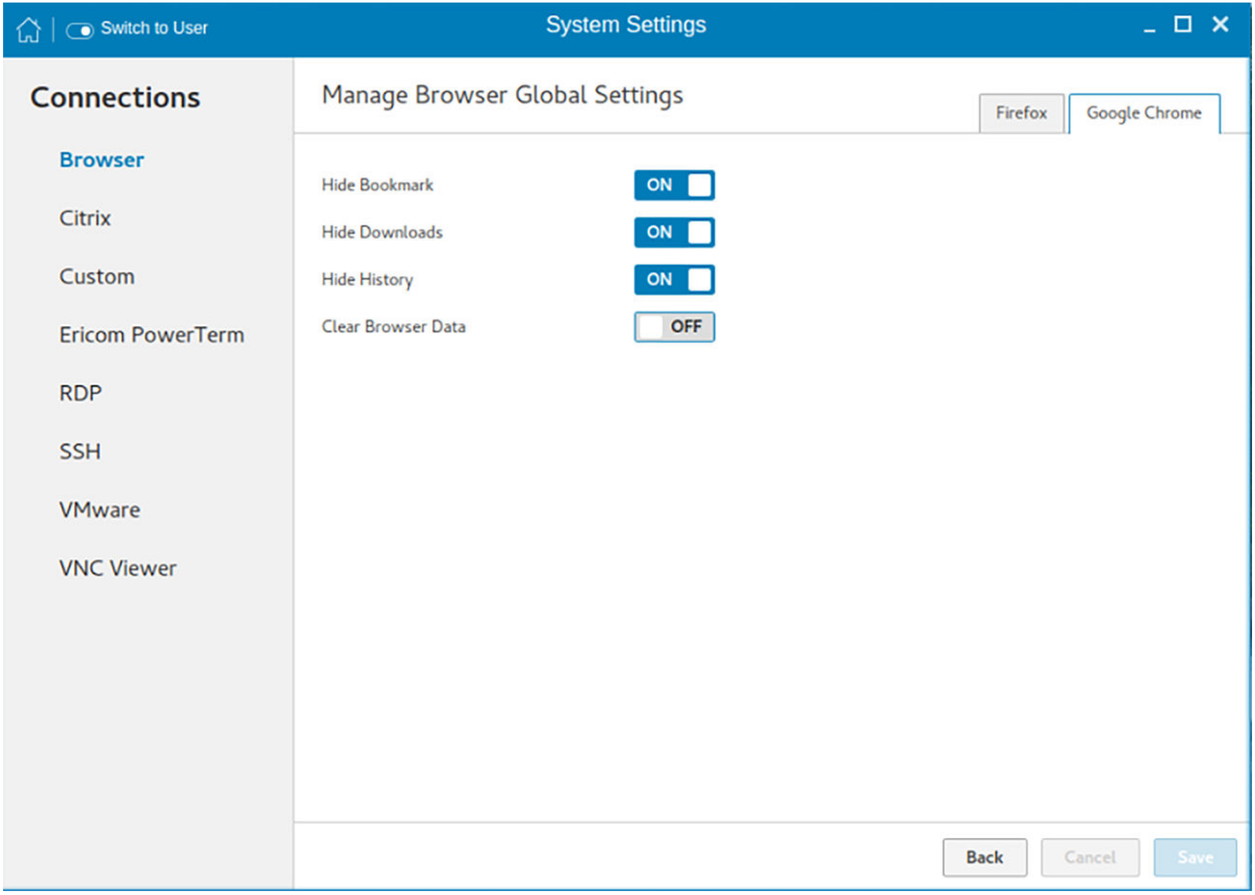
Figure 38. Firefox settings

Table 5. Mozilla Firefox settings

Parameter	Description
Hide Bookmark	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the bookmark bar is not displayed on the web page. By default, this option is enabled.
Hide Searchbar	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the search bar is not displayed on the web page. By default, this option is enabled.
Hide History	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the browser history is not displayed on the web page. By default, this option is enabled.
Clear Browser Data	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the browser data is removed. By default, this option is disabled.
Disable About:Config	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the Configuration Editor is disabled and you cannot configure the Firefox preferences.

Parameter	Description
	By default, this option is enabled.
Disable About:Add-ons	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the Add-ons Manager tab is disabled and you cannot configure the add-ons. By default, this option is enabled.

- If you are using **Google Chrome**, configure any of the following options:



Hide Bookmark	ON
Hide Downloads	ON
Hide History	ON
Clear Browser Data	OFF

Figure 39. Google Chrome

Table 6. Google Chrome settings

Parameter	Description
Hide Bookmark	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the bookmark bar is not displayed on the web page. By default, this option is enabled.
Hide Downloads	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the downloads are not displayed on the web page. By default, this option is enabled.
Hide History	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the browser history is not displayed on the web page. By default, this option is enabled.

Parameter	Description
Clear Browser Data	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the browser data is removed. By default, this option is disabled.

3 Click **Save** to save the settings.

Configuring and managing Citrix connections

The **Citrix Connections** page enables you to create and manage Citrix connections both locally and globally.

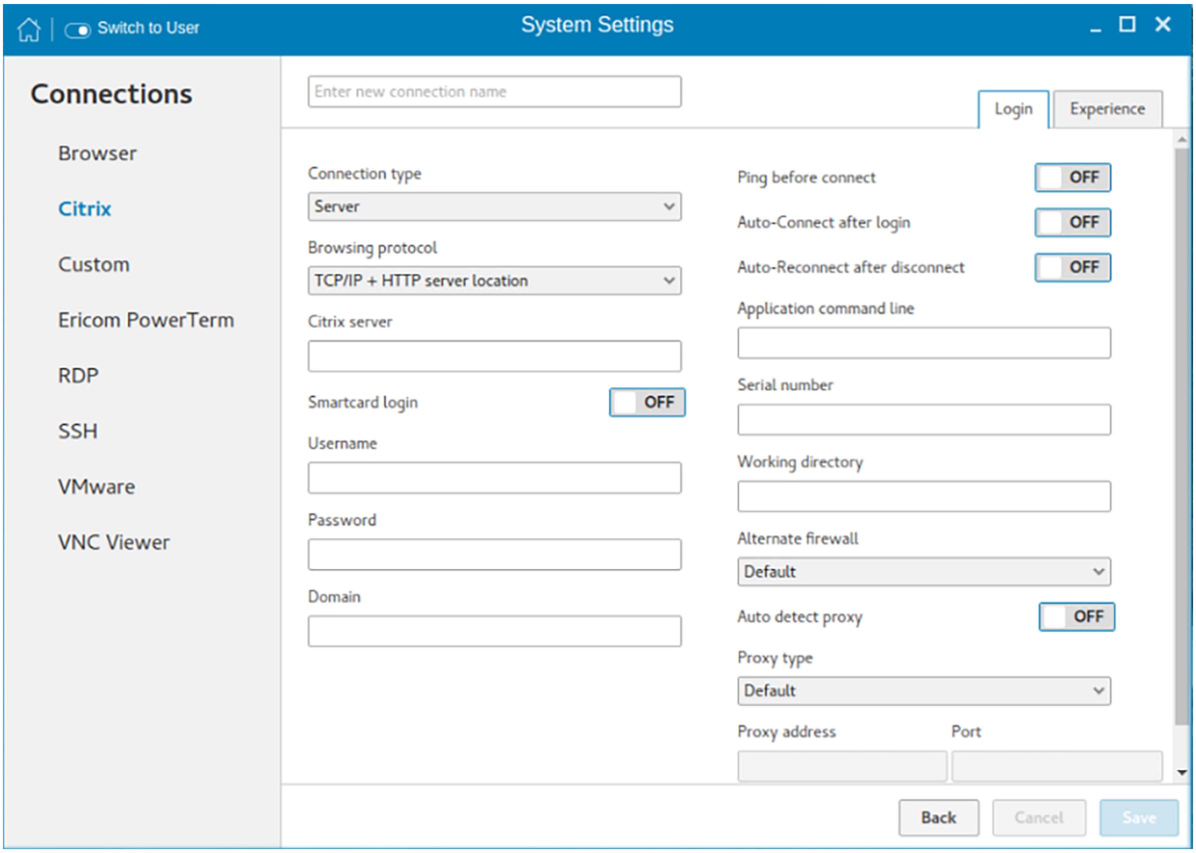
To configure the local **Citrix** settings:

1. Click the **+** icon to add a new **Citrix Connection**.

   The **Citrix Connections** page is displayed.
2. Enter the name of the **Citrix connection** for which you will specify the Server URL address.
3. From the **Connection Type** drop-down list, select any of the following connection type. For more information, see Configuring the server connection type
   - Server
   - Published Application
   - Storefront
4. Click **Save** to save the changes.

Configuring the server connection type

If **Server** is selected as the Connection type, the following options must be configured in the **Login** tab.



Connection type: Server

Browsing protocol: TCP/IP + HTTP server location

Citrix server

Smartcard login: OFF

Username

Password

Domain

Ping before connect: OFF

Auto-Connect after login: OFF

Auto-Reconnect after disconnect: OFF

Application command line

Serial number

Working directory

Alternate firewall: Default

Auto detect proxy: OFF

Proxy type: Default

Proxy address

Port

Figure 40. Citrix connection login settings

Table 7. Server

Parameter	Description
Browsing Protocol	From the drop-down list, select your preferred **Browsing Protocol**.
Citrix Server	Enter the specific **Citrix Server**.
Username	Enter the **Username** of the server.
Password	Enter the **Password** of the server.
Domain	Enter the preferred **Domain** for the server connection.
Ping before connect	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is checked before connecting to a session.
Auto-Connect after login	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically established after you log in to your thin client.

Parameter	Description
Auto-Reconnect after disconnect	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically established after you disconnect from the session.
When disconnect, reconnect	Select the time duration in seconds to delay the reconnection attempt after a disconnection occurs.
Smartcard login	Click the **ON** button to enable smart card login to the thin client. The User Name, Password, and Domain are not required. ⓘ NOTE: **Smart Card Login is applicable only for Server and Storefront Connections**
Smartcard type	This field is enabled when you select **Smart Card Login**. Select the type of smart card you are using from the drop-down list.
Application command line	Enter the **command line** for the program on the server.
Serial number	Enter the **serial number** for environments that require the thin client license serial number.
Working directory	Enter the **working directory** for the program. ⓘ NOTE: Working Directory is applicable only for Server Connections.

Click the **Show advance settings** to view and configure the advanced options for your Citrix server connection.

ⓘ NOTE:

The advanced options are available only for server connections.

Table 8. Advanced options

Parameter	Description
Alternate Firewall	From the drop-down list, Select **Yes** to use an alternate address for firewalls.
Auto-detect proxy	Click the **ON** button to automatically detect the proxy type. Click the **OFF** button to manually enter the proxy type.
Proxy type	From the drop-down list, Select a proxy type.
Proxy Address	From the drop-down list, Select a proxy address. ⓘ NOTE: **If you select Secure (HTTPS) or SOCKS as the Proxy Type, you must enter the Proxy Address and Port.**

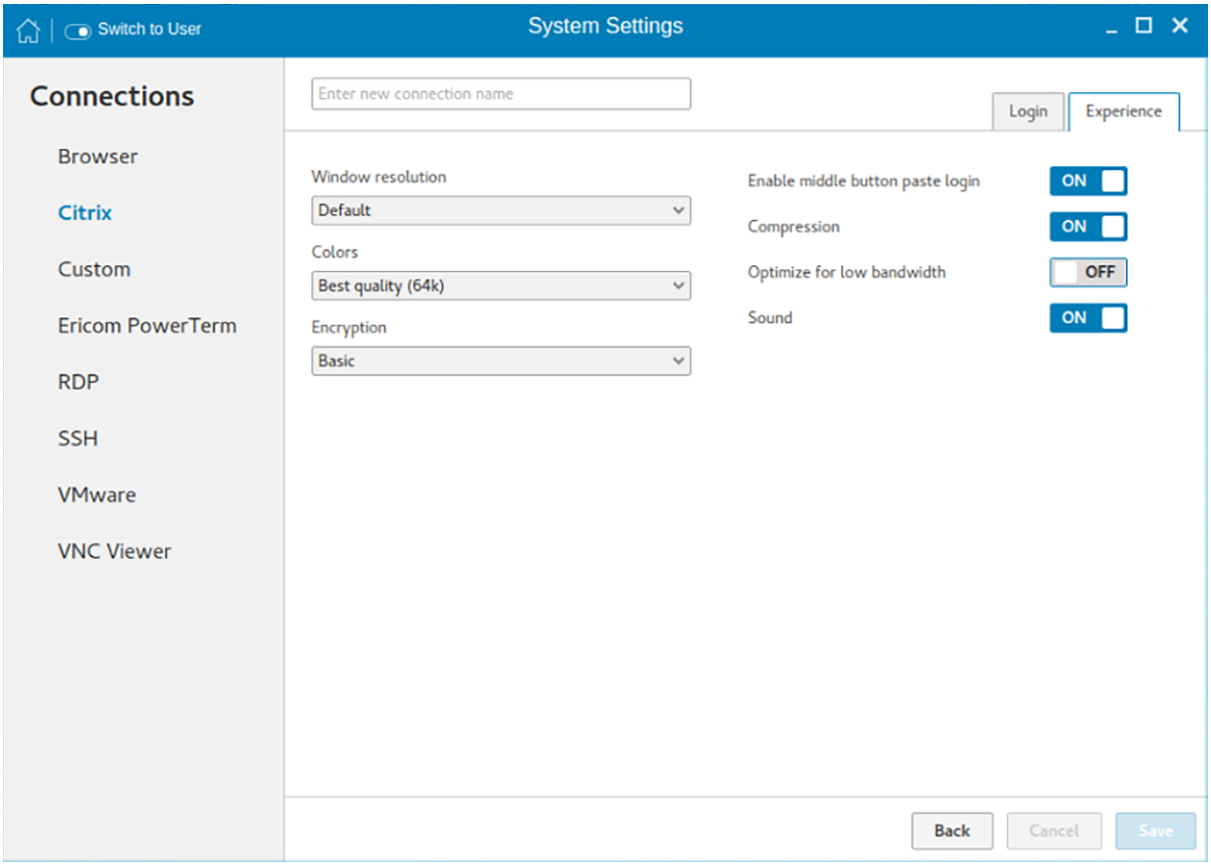
If **Published Application** or **Storefront** is selected as the **Connection Type**, the following options must be configured in addition to the options listed for **Server Connections** Table.

Store Name—Enter your preferred store name. Multiple store names are not supported.

NOTE:

- **SmartCard** Login option is not available for Published applications.
- The Storefront option is applicable only for **Citrix XenDesktop 7.0** and later versions. Select this option to specify the name of a Store Front server to display the applications available in that sever.
- **Smart card type** option is not applicable for Server connections.

The following options must be configured in the **Experience** tab.



System Settings

Enter new connection name

Window resolution: Default

Colors: Best quality (64k)

Encryption: Basic

Enable middle button paste login: ON

Compression: ON

Optimize for low bandwidth: OFF

Sound: ON

Figure 41. Citrix connection experience settings

Table 9. Experience

Parameter	Description
Windows resolution	Select the Windows resolution that you want to use on your monitor. The available resolutions are: Default 640 X 480 800 X 600 1024 X 768 1280 X 1024 1600 X 1200

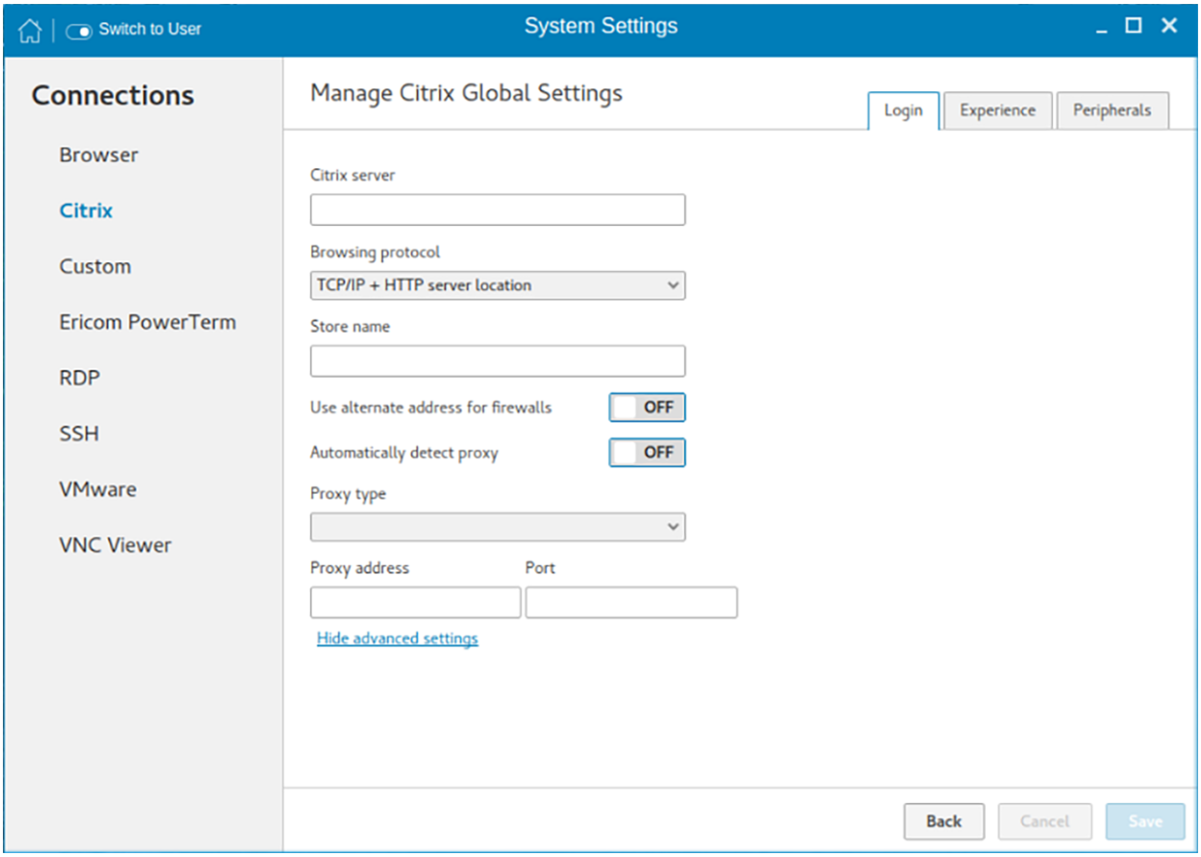
Parameter	Description
	Full Screen
Colors	Specifies the number of colors to display for each pixel. Select the session color mode to get the faster display performance on your monitor. The available options are: 256 Best quality (64k) 16 million
Encryption	Specifies the connection security level. Select the preferred option. Basic RC5 (128 bit-login only) RC5 (40-bit) RC5 (56-bit) RC5 (128-bit) ⓘ **NOTE:** • The highest level is 128-bit security and the lowest level is Basic. • Only Basic, and RC5 128-bit support Citrix XenDesktop 7.15. RC5 40-bit, and RC5 56-bit support Citrix XenDesktop 7.15 and earlier versions. RC5 40-bit and RC5-56 bit support has been deprecated since XenDesktop 7.9.
Enable middle button paste login	Click the **ON/OFF** button to enable or disable this option. If enabled, you can use the mouse middle click to paste content into your text documents.
Compression	Click the **ON/OFF** button to enable or disable this option.
Optimize for low bandwidth	Click the **ON/OFF** button to enable or disable this option.
Sound	Click the **ON/OFF** button to enable or disable this option.

Configuring Global Citrix settings

When you log out and log in, you are prompted for credentials to log in to a Citrix session for the selected domain. When you successfully log in, all the applications and desktops on the remote session are listed on the local desktop.

1. Click **Manage Citrix Global Settings**.

   The **Manage Citrix Global Settings** page is displayed.
2. On the **Login** tab, configure the following options to enable Citrix PAM login and enable the PAM login using the slider, in the Managing PAM login page. The Domain details also need to be provided on the Managing PAM login page.



Citrix server:

Browsing protocol: TCP/IP + HTTP server location

Store name:

Use alternate address for firewalls: OFF

Automatically detect proxy: OFF

Proxy type:

Proxy address:

Port:

Figure 42. Citrix global login settings

a Enter the Citrix server.

b From the drop-down list, select the required browsing protocol. The available options are:

- TCP/IP + HTTP server location
- TCP/IP
- SSL/TLS + HTTPS server location

c Enter the store name.

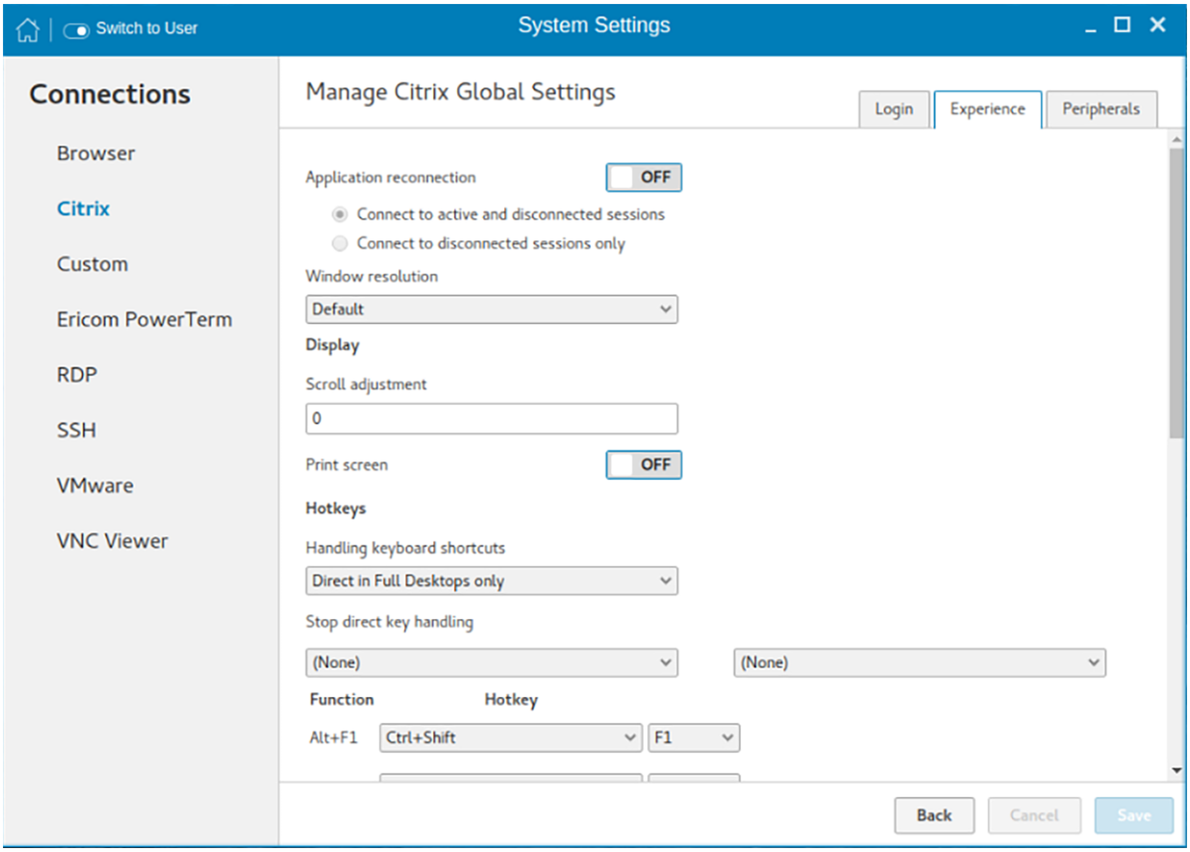
d Click **Show Advance Settings** to view and configure the advanced options.

1 Click the **ON/OFF** button to enable or disable the Use Alternate address for firewall option. If enabled, an alternate address can be used for firewall configuration.

2 Click the **ON** button to automatically detect the proxy type or click the **OFF** button to manually enter the proxy type.

3 From the drop-down list, select a proxy type

3 On the **Experience** tab, configure the following options.



Manage Citrix Global Settings

Application reconnection: OFF

● Connect to active and disconnected sessions

○ Connect to disconnected sessions only

Window resolution: Default

Display

Scroll adjustment: 0

Print screen: OFF

Hotkeys

Handling keyboard shortcuts: Direct in Full Desktops only

Stop direct key handling: (None) (None)

Function	Hotkey	
Alt+F1	Ctrl+Shift	F1

Figure 43. Citrix global experience settings

a Click the **ON/OFF** button to enable or disable the Application Reconnection option. If enabled, the connection is automatically re-established after you disconnect from the session.

b Select the Windows resolution you can use to get the best display on your monitor.

c If you come across over-scrolling when using certain published applications, increase the adjustment by 100 until the display improves.

> NOTE: **The maximum scroll adjustment is 1000.**

d Click the **ON/OFF** button to enable or disable the PrintScreen option. Select the option to use the Print Screen key to capture an image of the desktop to the Clipboard.

e Use this section to map hotkeys on the thin client.

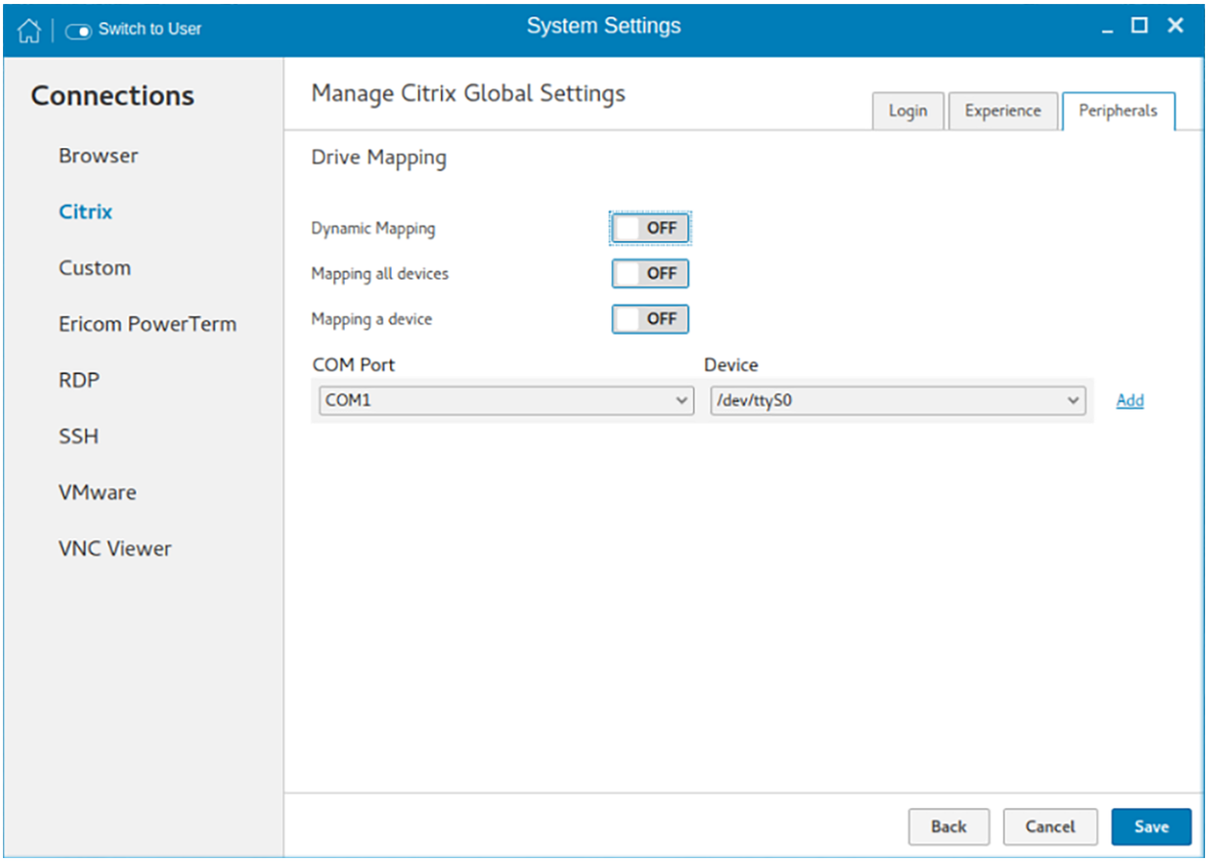
From the drop-down list, select the preferred keyboard shortcuts.

- If you select **Direct** option for handling keyboard shortcuts, then from the drop-down list, Select the direct key to handle keyboard shortcuts.
- If you select **Direct in Full Desktops only** or **Translated** option for handling keyboard shortcuts, then complete the following steps:

  a Click the **Hotkeys** tab to map hotkeys on the thin client.

  b Select a **Hotkey** option using the Hotkey lists for each **function** you want.

4 Click the **Peripherals** tab, and configure the following options:



Manage Citrix Global Settings

Drive Mapping

Dynamic Mapping OFF

Mapping all devices OFF

Mapping a device OFF

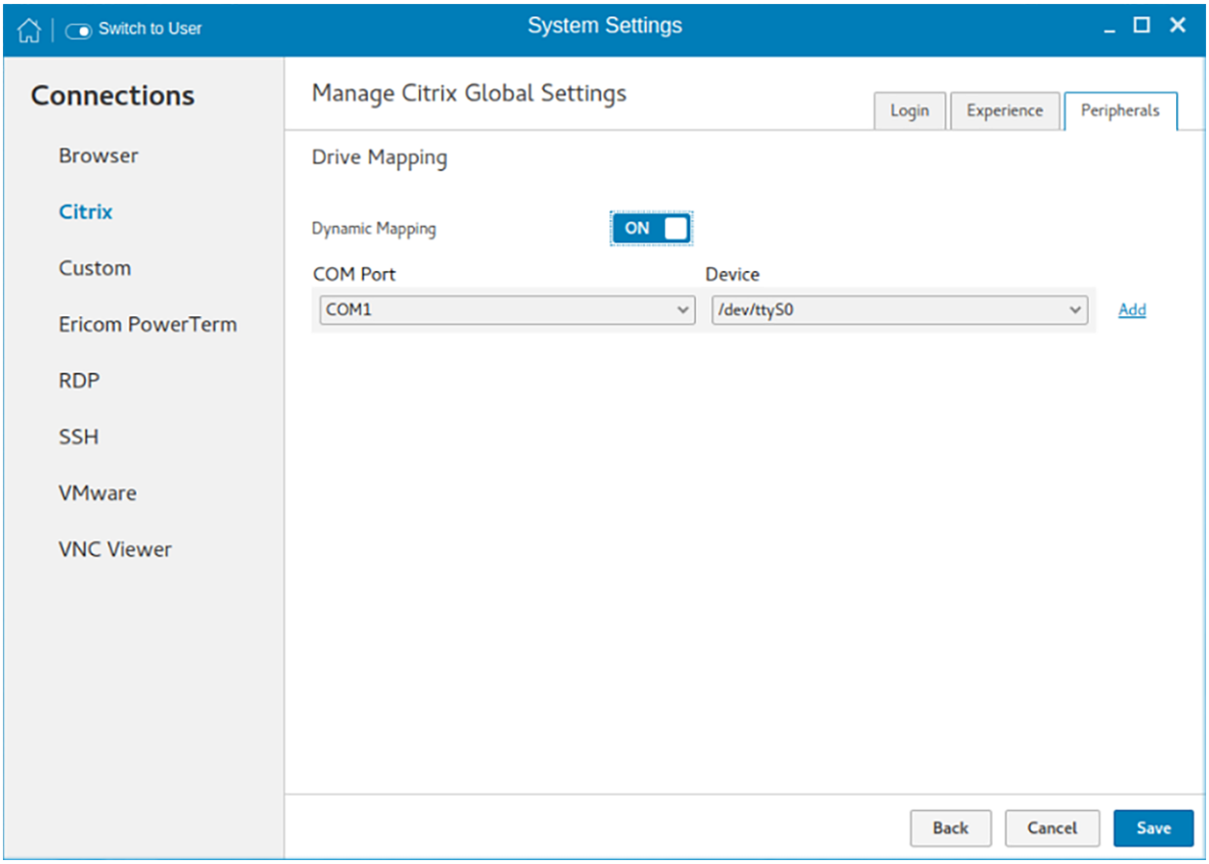
COM Port: COM1

Device: /dev/ttyS0

Figure 44. Drive mapping

a **Drive Mapping**:

- **Dynamic Mapping**—Dynamic client drive mapping enables virtual desktops to access mass storage devices, such as USB flash drives, configured on the endpoint. The virtual (not local) desktop is responsible for controlling USB drives and displaying them in the user interface. When a USB drive is connected to an endpoint, it is automatically mounted and freely accessible. USB drives accessed using dynamic client drive mapping are treated as network drives. For this reason, you cannot check, reformat, or perform other local operations on them.

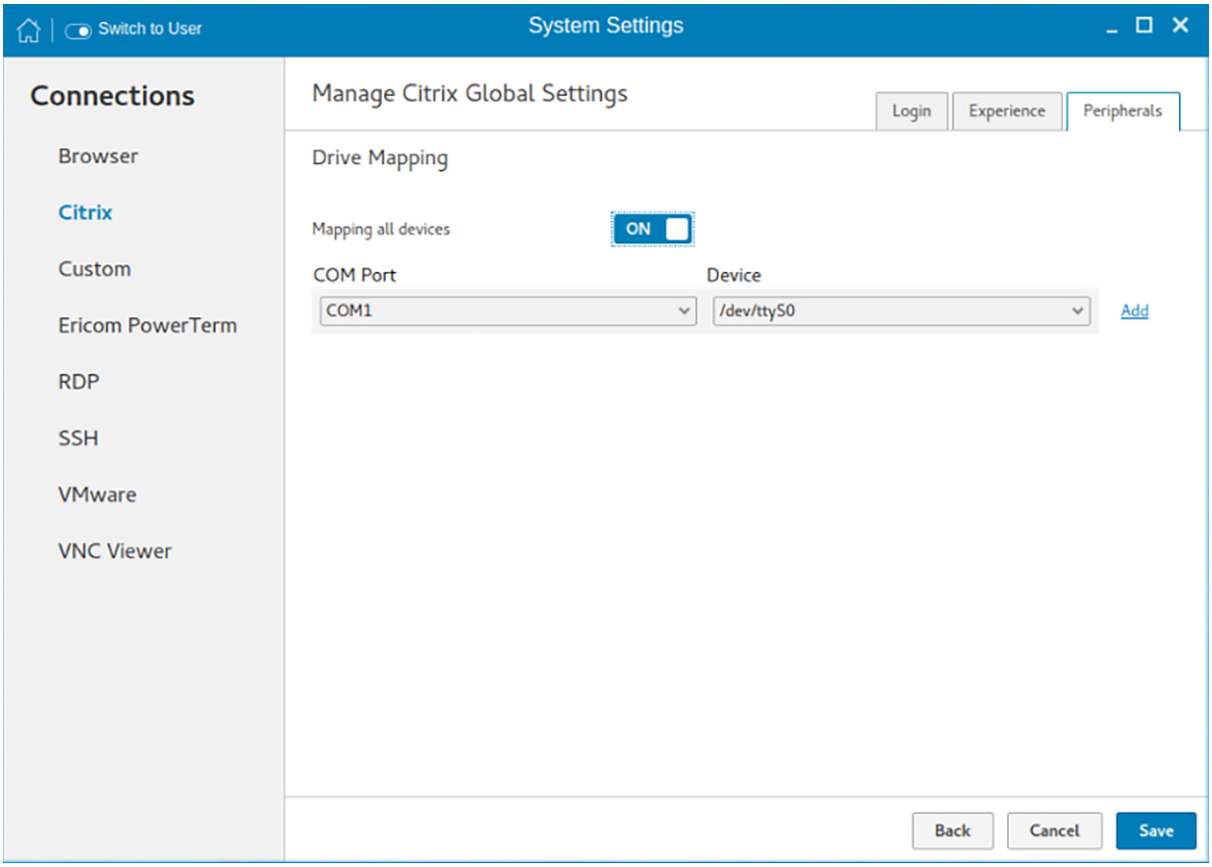


Dynamic Mapping ON

COM Port	Device
COM1	/dev/ttyS0

Figure 45. Dynamic mapping

- **Mapping all devices**—This option is same as Dynamic mapping but the you will be given an option to select the drive letter and read-write permissions for the drives. When this option is enabled all the usb storage devices which are mounted on /run/media/ will be mapped to the Citrix session. You are provided the option to choose the drive letter and read or write permissions for the drives which have been mounted on to the thin client. The device name value remains constant as /run/media/.



Manage Citrix Global Settings

Drive Mapping

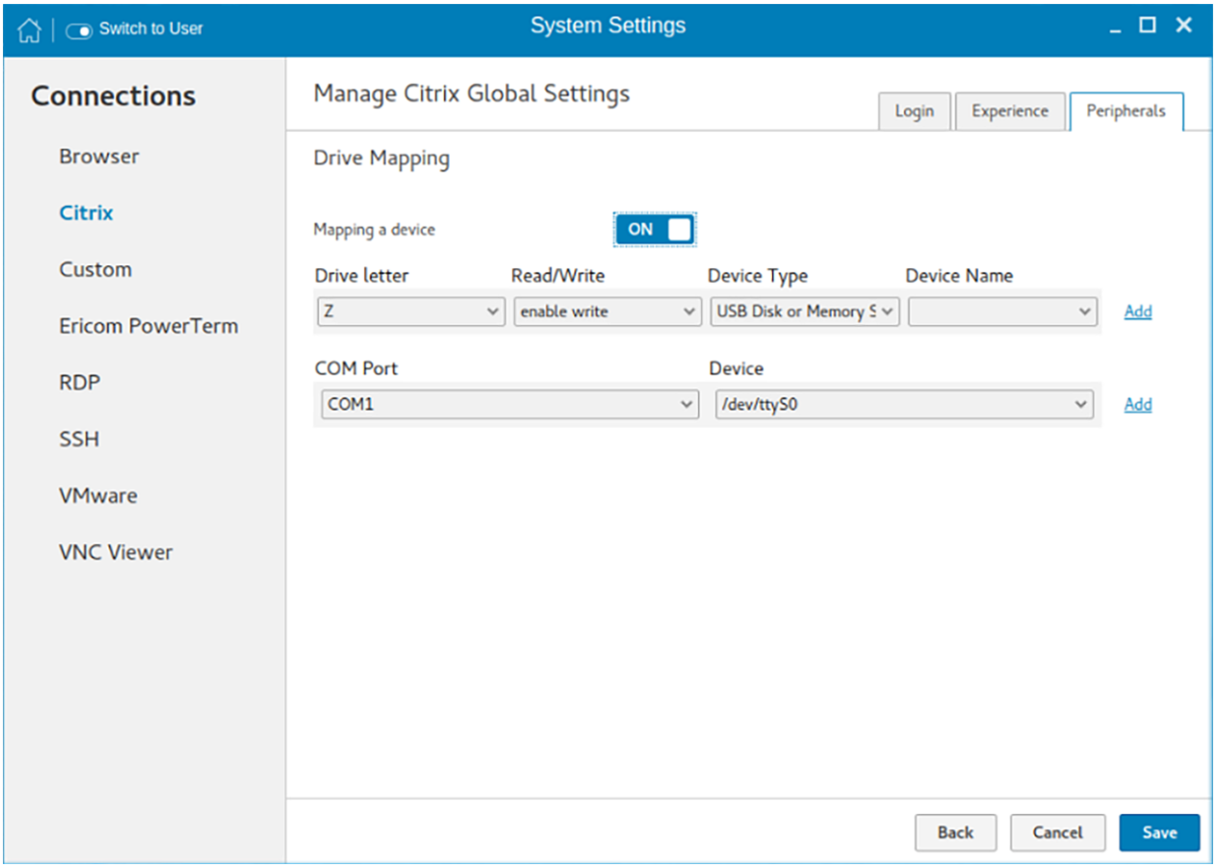
Mapping all devices: ON

COM Port: COM1

Device: /dev/ttyS0

Figure 46. Mapping all devices

- **Mapping a single device**—Unlike the previous two options, this option enables you to select an individual device that should be redirected to the session. The device name lists all the devices that has been successfully mounted on to the thin client. You will be able to select a drive letter and read-write permission for individual drives that redirect to the session.



Manage Citrix Global Settings

Drive Mapping

Mapping a device: ON

Drive letter	Read/Write	Device Type	Device Name
Z	enable write	USB Disk or Memory S	

COM Port	Device
COM1	/dev/ttyS0

Figure 47. Mapping a device

To add a COM port, complete the following task:

a Click **Add**.
b From the **COM Port** list, select a COM port—1 to 4.
c Select a device from the device list.

To delete a COM port, click the **X** icon next to the COM port that you want to delete.

5 Click **Save** to save the changes.

Managing PAM login

1 Click **PAM Login**.

The **Manage PAM Login Settings** page is displayed. The PAM login page displays the settings that are used for PNAgent server connection. It allows you to enable or disable the PAM login, and to enter the domain for PNAgent server.

2 Click the **ON/OFF** button to enable Citrix PAM login option.

3 Click the **ON/OFF** button to enable or disable the Show All Apps option.

4 Enable the **Enable Citrix PAM login** option to enter the Citrix server domain.

The **Citrix Global Settings** table provides you the information about Citrix server, protocol, and Store Name and you are restricted from editing the content.

5 Click **Save** to save the changes.

Citrix ICA Client RTME

Starting from HDX RealTime Media Engine (RTME) 2.3, Citrix supports 64–bit Linux operating systems. Hence, there is no need to install any optional 32-bit add-ons as it is now packaged along with base image. This feature is enabled by default.

Features of RTME

The following are the features of RTME (Real Time Media Engine):

- Improved audio and video quality:
  - Support for H.264 Scalable Video Coding (SVC): SVC handles the transmission of video over varied network and device environments. The sending system includes different levels for the information transmitted such as frames per second, image size, and quality granularity. The receiving device selects the required information from the transmission and optimizes the experience on those devices.
  - SILK audio codec: Delivers higher audio quality across a wide range of network environments, including the public Internet and mobile networks.
  - Improved audio and video quality over lossy connections: By enabling the forward error correction (FEC), we provide higher-quality content over lossy connections.
- Support for 64-bit architecture: Linux 64-bit operating systems are now supported for the Real-Time Media Engine.
- Endpoint identification for location services:
  - Enhanced 9-1-1 (E9-1-1) and E999, E100, and so on: An international emergency dispatch feature that associates a 911 (or an international emergency) call with a specific location information. This information includes street address and the floor number for office buildings. Responders are directed to the correct emergency location. For more information, see Technet.microsoft.com/en-us/library/dn951423.aspx.
  - Support for Quality of Experience (QoE) reporting: Use Quality of Experience data to keep a record of the quality of your users' audio and video calls, including:
    - Number of network packets lost
    - Background noise
    - Amount of jitter (differences in packet delay)
    - Names of devices used for a call
    - Names of devices used for a call
    - ICE Warning flags
    - Endpoint statistics
  - Skype for Business users can communicate with Skype users.
  - Flexible upgrades: Simplified backward compatibility for upgrading from version 2.0.x
  - Fallback mode control: You can disable fallback mode or limit fallback control to server-side media processing for audio only (no video), which reduces CPU impact.
  - Administrator control of system notification balloons: You can enable or disable the system notification balloons the Optimization Pack displays.
  - The Real-Time Optimization Pack About page: The following information can be viewed in the About page:
    - Status of Real-Time Optimization Pack
    - Skype for Business version number
    - Operating systems on which the Real-Time Connector and Real-Time Media Engine are running

      ⓘ **NOTE: In the fallback mode, the version and operating system fields for Real-Time Connector and Real-Time Media Engine display the same values because the Real-Time Optimization Pack uses the Real-Time Media Engine within the Real-Time connector.**
  - Localization: Real-Time Media Engine installers for Linux 64-bit OS are localized and available in German, French, Spanish, Japanese, and Simplified Chinese.
  - Skype for Business 2016: The current Skype for Business 2016 client does not support Real-Time Optimization pack.

Configuring and managing the custom connections

The **Custom Connections** page enables you to create and manage the Custom connection based on shell commands. The main Custom page has options to create a Custom connection.
To configure the **Custom Settings**, complete the following task:

1 Click the **+** icon to add a new Custom Connection.

The **Custom Connections** page is displayed.

2 Enter the name of the Custom connection.

3 The following options must be configured in the **Login** tab.

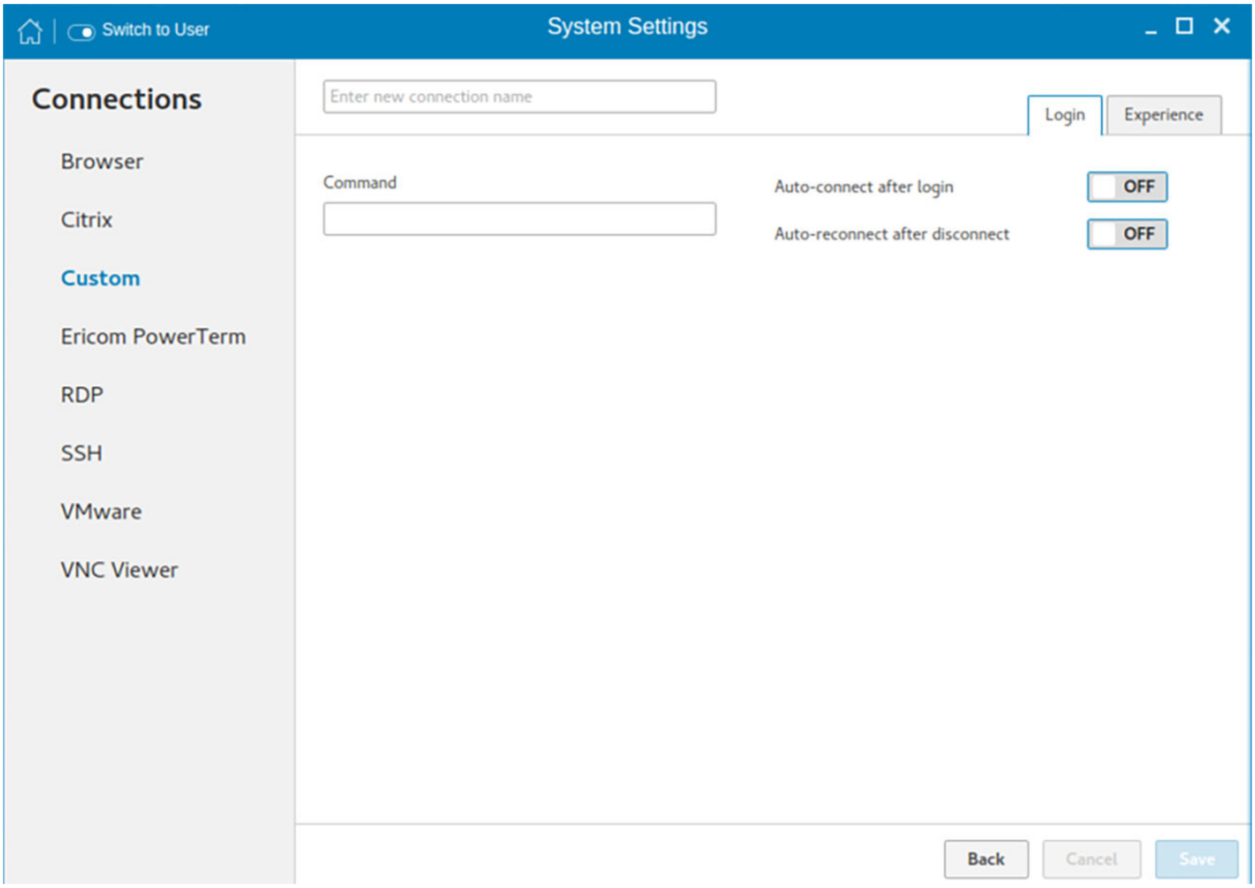


Figure 48. Custom connection login settings

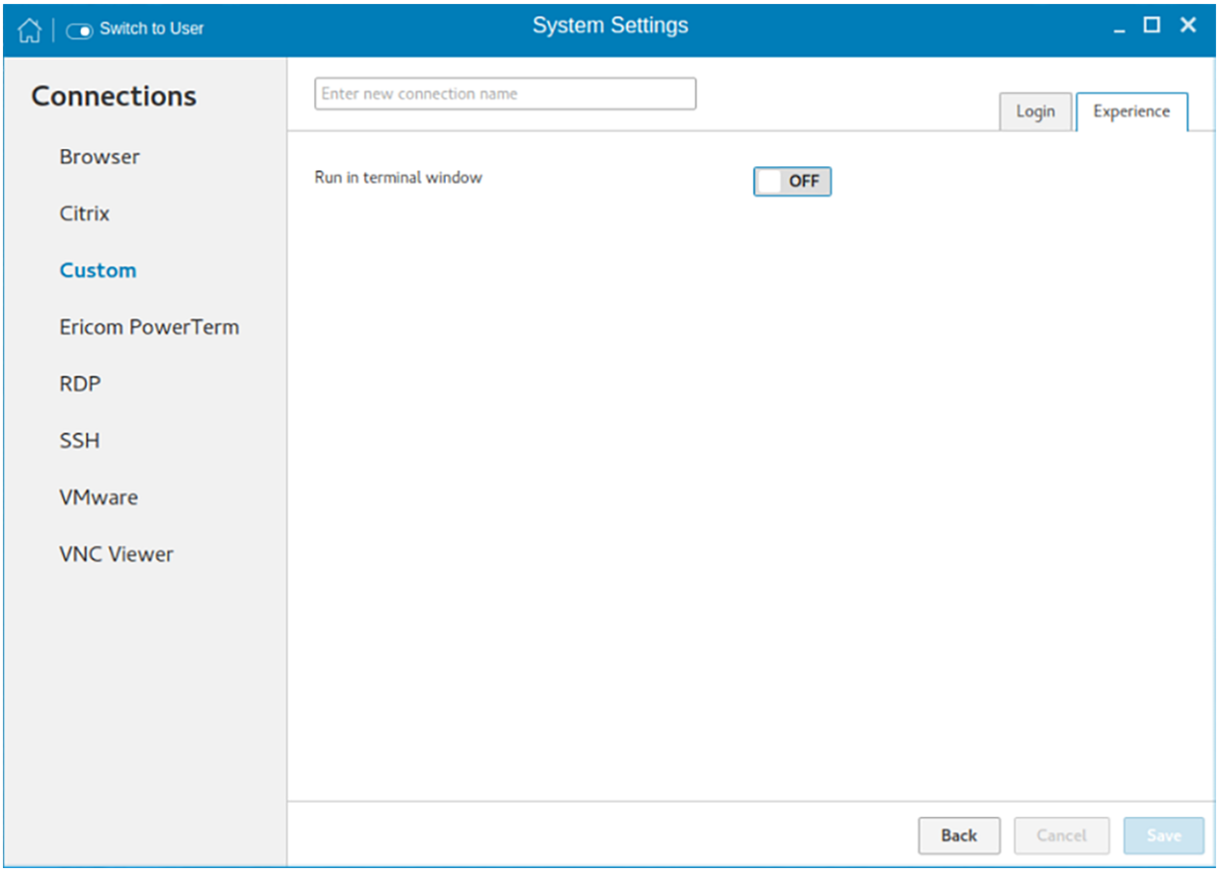
a Enter the shell command. The shell command is performed when you click the connection icon on the desktop.

b Click the **ON/OFF** button to enable or disable the Auto-connect after login option. If enabled, the connection is automatically connected after you log in to your thin client.

c Click the **ON/OFF** button to enable or disable the Auto-reconnect after disconnected option. If enabled, the connection is automatically re-connected after you disconnect from the session.

d Select the time duration in seconds to delay the reconnection attempt after a disconnection occurs.

4 The following options must be configured in the **Experience** tab.



Run in terminal window OFF

Figure 49. Custom connection experience settings

a Click the **ON/OFF** button to enable or disable the Run in terminal window option.

5 Click **Save** to save the changes.

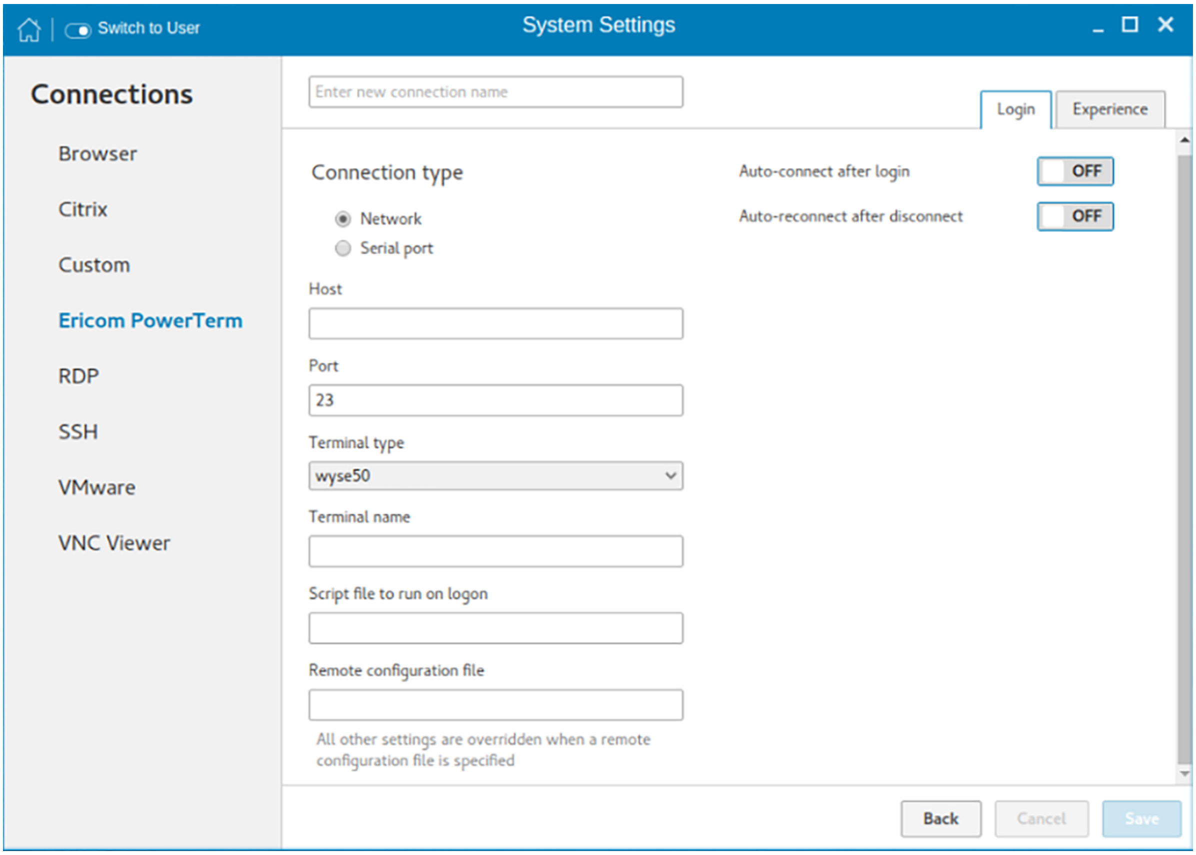
Configuring and managing the Ericom PowerTerm connections

The Ericom PowerTerm connections page enables you to create and manage the Ericom PowerTerm connections.
To configure the Ericom PowerTerm Connection Settings, complete the following task:

1 Click the + icon to add a new Ericom PowerTerm Connection. The Ericom PowerTerm Connections page is displayed.

2 Enter the name of the Ericom PowerTerm connection.

3 The following options must be configured in the **Login** tab .



Enter new connection name

Connection type

● Network

○ Serial port

Host

Port: 23

Terminal type: wyse50

Terminal name

Script file to run on logon

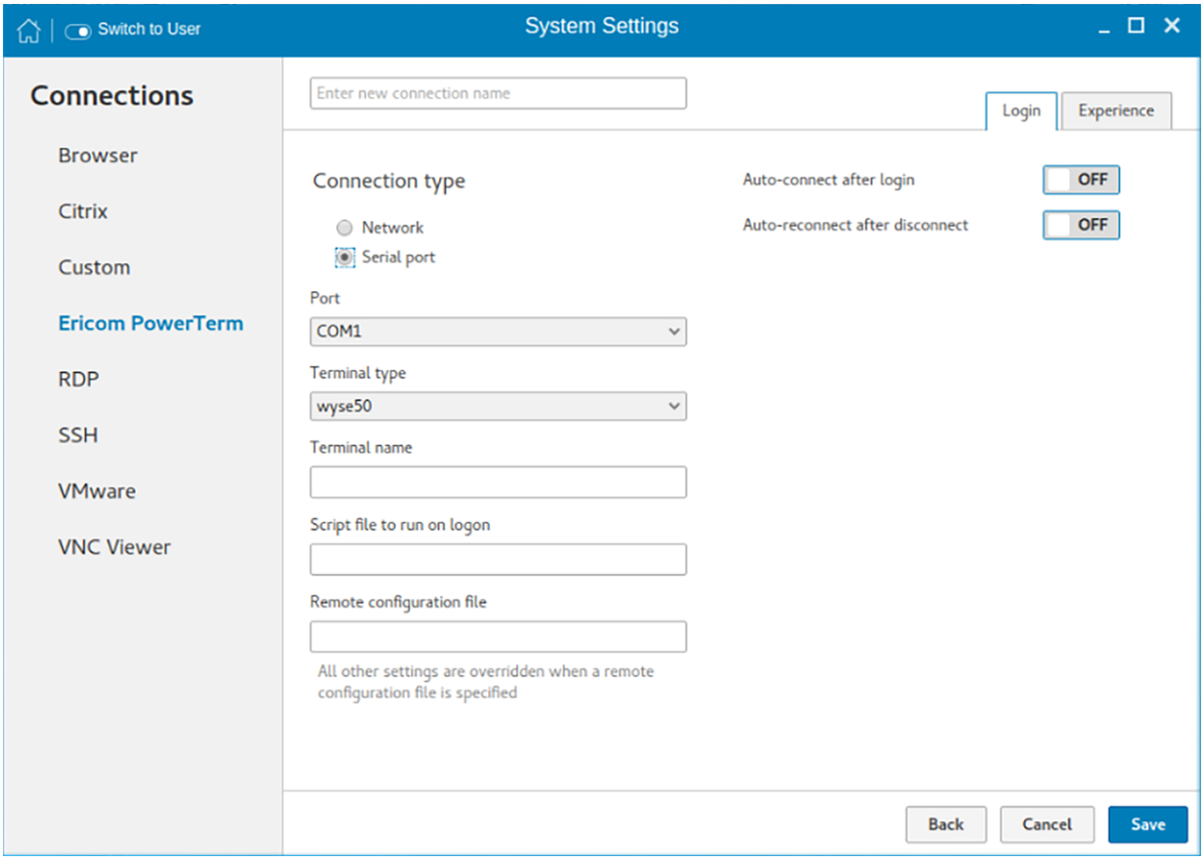
Remote configuration file

All other settings are overridden when a remote configuration file is specified

Auto-connect after login: OFF

Auto-reconnect after disconnect: OFF

Figure 50. Ericom PowerTerm login settings



Connection type

○ Network
● Serial port

Port: COM1

Terminal type: wyse50

Terminal name

Script file to run on logon

Remote configuration file

All other settings are overridden when a remote configuration file is specified

Auto-connect after login: OFF

Auto-reconnect after disconnect: OFF

Figure 51. Ericom PowerTerm login settings

Table 10. Ericom PowerTerm login settings

Parameter	Description
Connection type	On the **Connection Type** page, click the Network or Serial Port radio button depending upon the requirement. By default, the Network option is selected. Serial Port radio button is disabled if the application does not detect any active serial ports.
Host	Enter the Ericom server host’s IP or FQDN address in the **Host** field. This field is hidden, if the connection is through Serial Port.
Port	Specify the port number used to connect the Ericom server in the **Port** field. This is available if the connection is through the network. In case of Serial Port, this field displays as **COM** port and the available serial ports are listed in the drop-down list.
Terminal type	Select the terminal type to be emulated from the drop-down list in the **Terminal Type** field.
Terminal name	Type the name of the Ericom PowerTerm terminal window in the **Terminal Name** field
Script file to run on logon	Specify the path of the script file (if any) to be executed in the remote system in the **Script file to run on Logon** field.

Parameter	Description
Remote configuration file	Specify the location of the remote configuration files in the **Remote configuration file** field.
Auto-connect after login	a Click the ON/OFF button to enable or disable the Auto-connect after login option. If enabled, the connection is automatically connected after you log in to your thin client. b Click the ON/OFF button to enable or disable the Auto-reconnect after disconnected option. If enabled, the connection is automatically re-connected after you disconnect from the session. c Select the time duration in seconds to delay the reconnection attempt after a disconnection occurs.

4 The following options must be configured in the Experience tab.

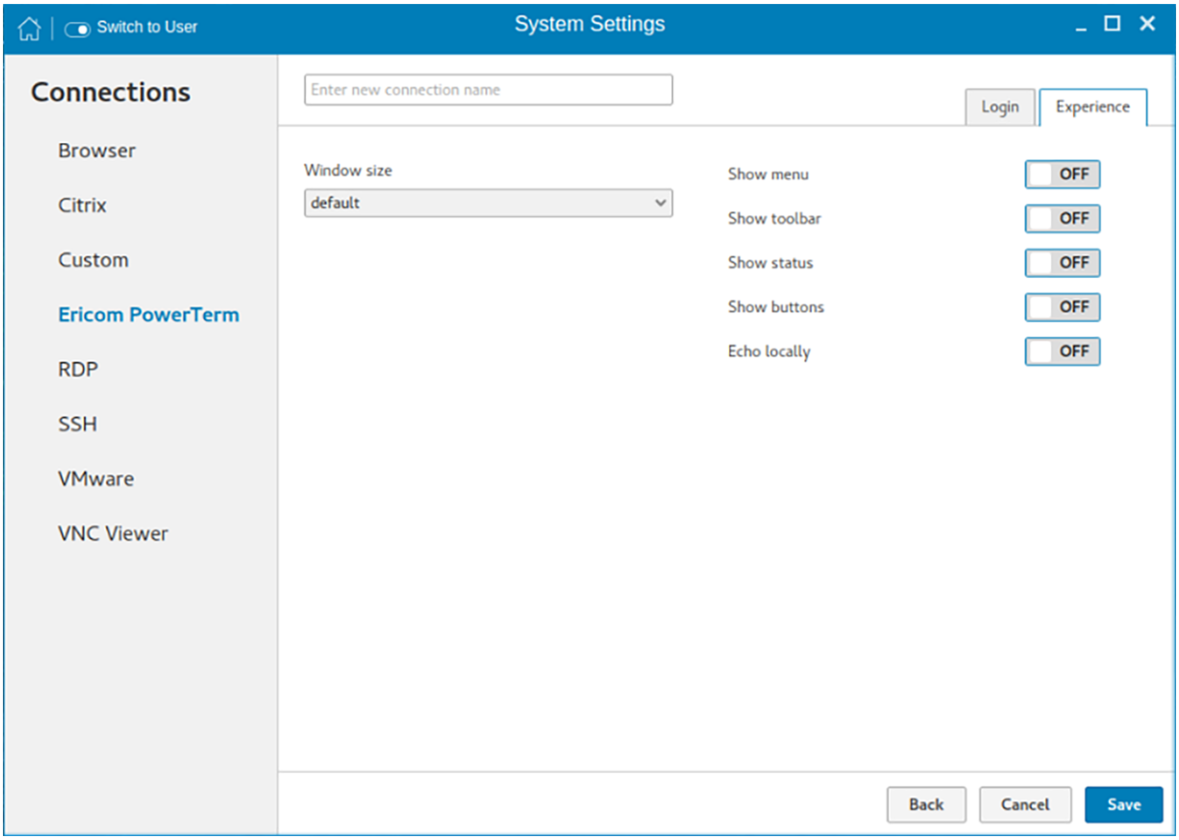
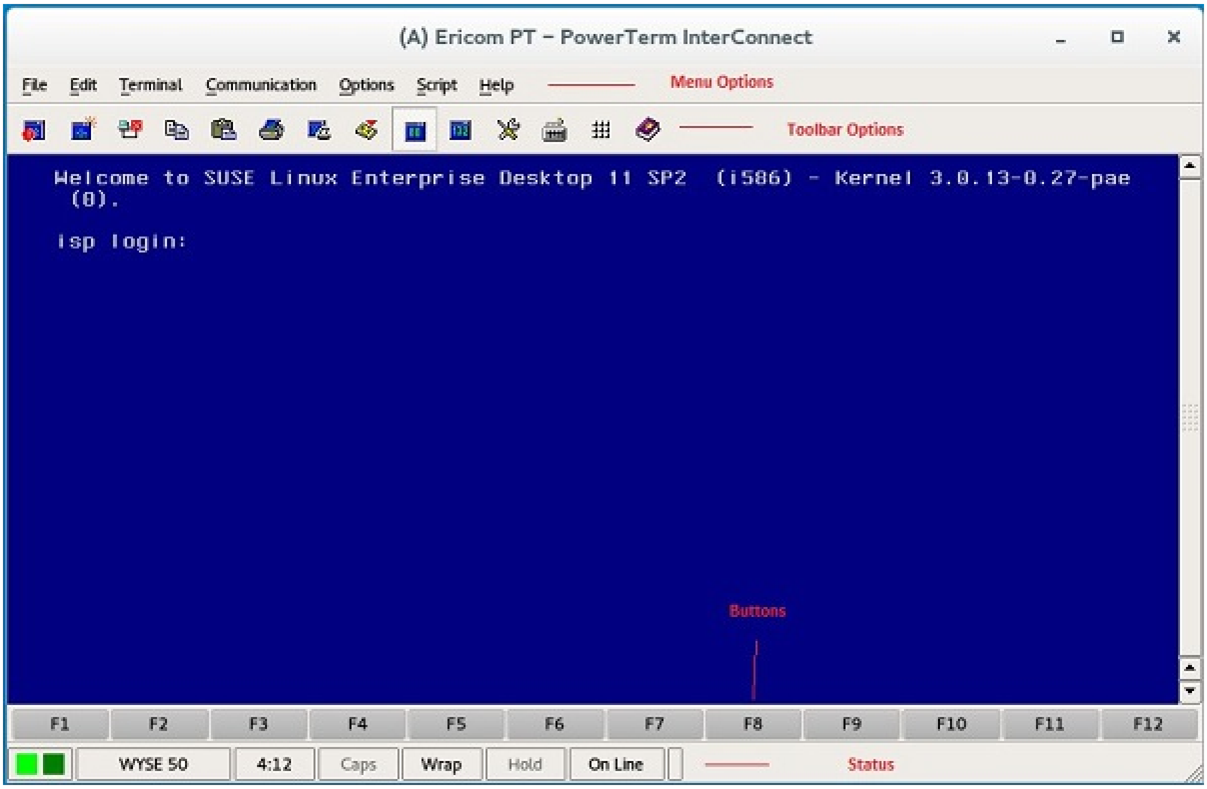


Figure 52. Ericom PowerTerm experience settings

Table 11. Ericom PowerTerm Experience Settings

Parameter	Description
Window size	Select the desired terminal window size from the drop-down list in the **Window Size** field.
Show menu	Click the ON/OFF button to enable or disable this option. It enables the top menu option on the Ericom PowerTerm window.
Show toolbar	Click the ON/OFF button to enable or disable this option. It enables the toolbar option on the Ericom PowerTerm window.

Parameter	Description
Show status	Click the ON/OFF button to enable or disable this option. It enables the status bar on the Ericom PowerTerm window.
Show buttons	Click the ON/OFF button to enable or disable this option. It enables the soft buttons on the Ericom PowerTerm window.
Echo locally	When the connection is configured through Serial Port then additional option **Echo locally** option will be available on the **Experience** tab. If this option is set to ON, it will set the local echo option of the generated Ericom PowerTerm terminal window.



```
Welcome to SUSE Linux Enterprise Desktop 11 SP2  (i586) - Kernel 3.0.13-0.27-pae
 (0).

isp login:
```

Figure 53. Ericom PT — PowerTerm Interconnect

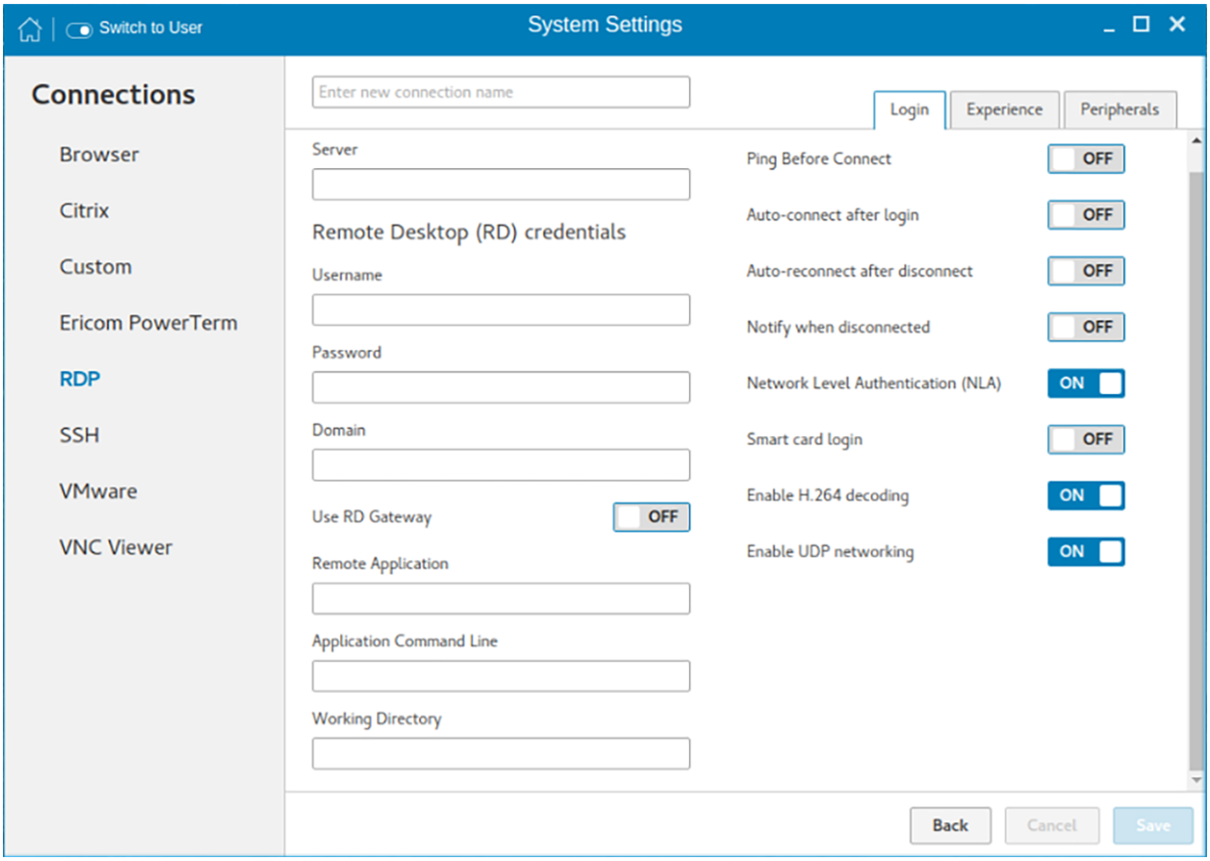
Configuring and managing RDP connections

The **RDP connections** page enables you to create and manage the RDP connection. The main RDP page has options to create an RDP connection and modify existing connections.

To configure the RDP settings, complete the following tasks:

1. Click the **+** icon to add a new RDP Connection.

   The **RDP Connections** page is displayed.
2. Enter the name of the RDP connection.
3. Configure the following tasks in the **Login** tab:



Server

Remote Desktop (RD) credentials

Username

Password

Domain

Use RD Gateway OFF

Remote Application

Application Command Line

Working Directory

Ping Before Connect OFF

Auto-connect after login OFF

Auto-reconnect after disconnect OFF

Notify when disconnected OFF

Network Level Authentication (NLA) ON

Smart card login OFF

Enable H.264 decoding ON

Enable UDP networking ON

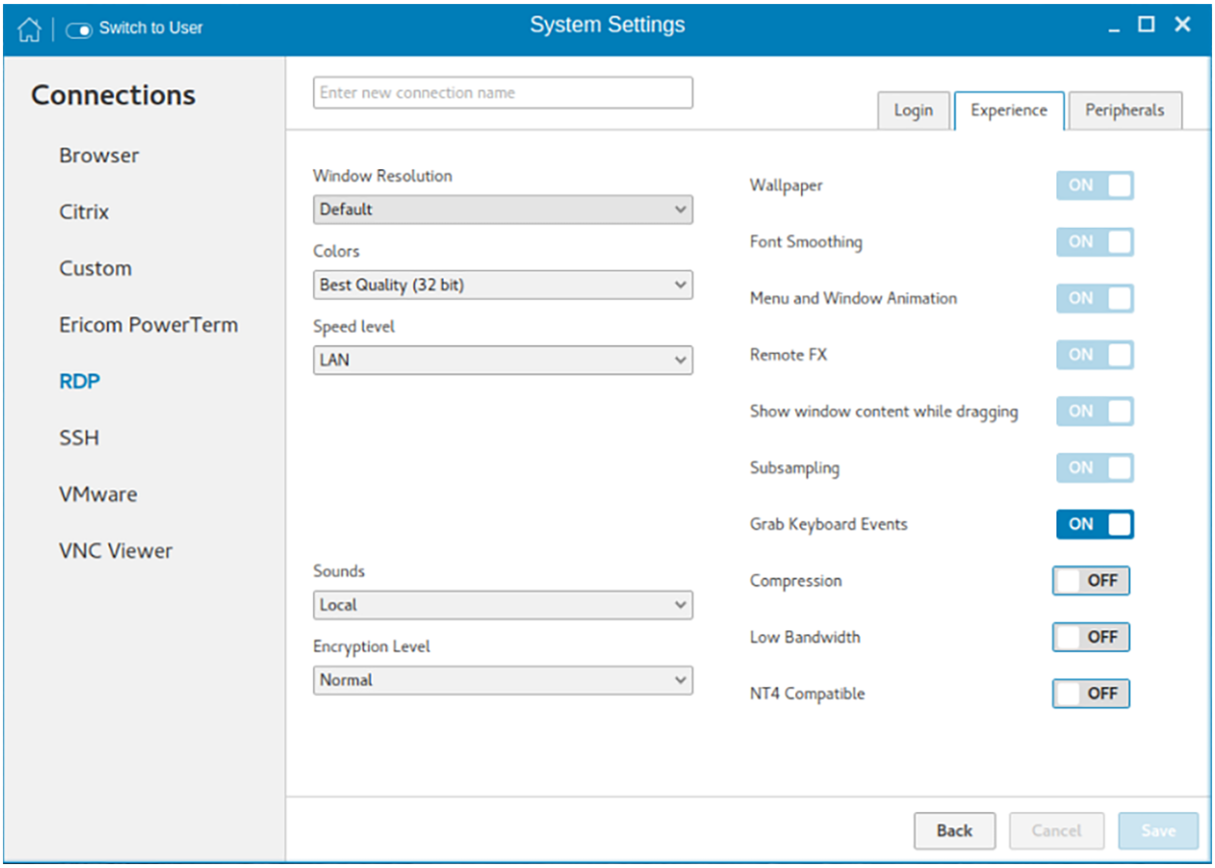
Figure 54. RDP login settings

Table 12. RDP login settings

Parameter	Description
Server	Enter the **IP address** or **FQDN** of the RDP server to which you want to establish a connection.
Username	Enter the **Username** to log in to the RDP Server.
Password	Enter the **Password** to log in to the RDP Server.
Domain	Enter the **Domain** to log in to the RDP Server.
Use RD Gateway	Select to enable and configure an RD Gateway to connect to your remote computers, if required by your network administrator and then do one of the following: • To configure the RD Server, and then Use Remote Desktop Credentials for RD Gateway—Enter the RD Server IP address or URL of the Remote Desktop Gateway server, and then select the Use Remote Desktop credentials for RD Gateway check box, if the server credentials are the same credentials as your RDP host remote computer credentials. • To configure the RD Server, and then Manually enter RD User Name, RD Password, RD Domain—Enter the RD Server IP address or URL of the Remote Desktop Gateway server. Clear the Use Remote Desktop credentials for RD Gateway check box and then manually enter the Username, Password, and Domain of the RD Gateway server, if required.

Parameter	Description
	ⓘ NOTE: **An RD Gateway server is a type of gateway that enables authorized users to connect to remote computers on a corporate network from any computer with an Internet connection. An RD Gateway server enables Remote Desktop connections to a corporate network from the Internet without having to set up virtual private network (VPN) connections. Ask your network administrator whether you need to specify an RD Gateway server.**
Remote Application	Enter the **Remote Application** name.
Application Command Line	Enter the **command line** for the program on the server.
Working Directory	Enter the **Working Directory** for the program. ⓘ NOTE: **Working Directory is applicable only for Server Connections.**
Ping Before Connect	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is checked before connecting to a session.
Auto-Connect after login	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically established after you log in to your thin client.
Auto-reconnect after disconnect	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically re-established after you disconnect from the session. If the Auto-reconnect option is enabled, you must enter the Delay duration (in seconds) when you reconnect to the session. The default time duration is 30 seconds.
Notify when disconnected	Click the **ON/OFF** button to enable or disable this option. It notifies when the connection is disconnected.
Network Level Authentication (NLA)	Click the **ON/OFF** button to enable or disable this option. Enable the Network Level Authentication (NLA), if NLA is enabled on your remote computer. Your remote computer requires NLA user authentication before you establish a full Remote Desktop connection and the login screen is displayed.
Smart card login	Click the **ON/OFF** button to enable smart card login to the thin client. The User Name, Password, and Domain are not required.
Enable H.264 decoding	Click the **ON/OFF** button to enable or disable this option. Enable this option to allow H.264 decoding in Microsoft RDP Client. The RDP client uses H.264 decoding, provided the agent supports H.264 software encoding. If the agent does not support H.264 software encoding, the RDP client uses JPG/PNG decoding. Disable this option if you want to use JPG/PNG decoding.
Enable UDP networking	Click the **ON/OFF** button to enable or disable this option. Enable this option to allow UDP networking in Microsoft RDP Client. The RDP client uses UDP networking, provided UDP connectivity is available. If the UDP networking is blocked, the RDP client uses TCP networking. Disable this option to use TCP networking.

4 The following options can be configured in the **Experience** tab.



Window Resolution: Default

Colors: Best Quality (32 bit)

Speed level: LAN

Sounds: Local

Encryption Level: Normal

Wallpaper: ON

Font Smoothing: ON

Menu and Window Animation: ON

Remote FX: ON

Show window content while dragging: ON

Subsampling: ON

Grab Keyboard Events: ON

Compression: OFF

Low Bandwidth: OFF

NT4 Compatible: OFF

Figure 55. RDP experience settings

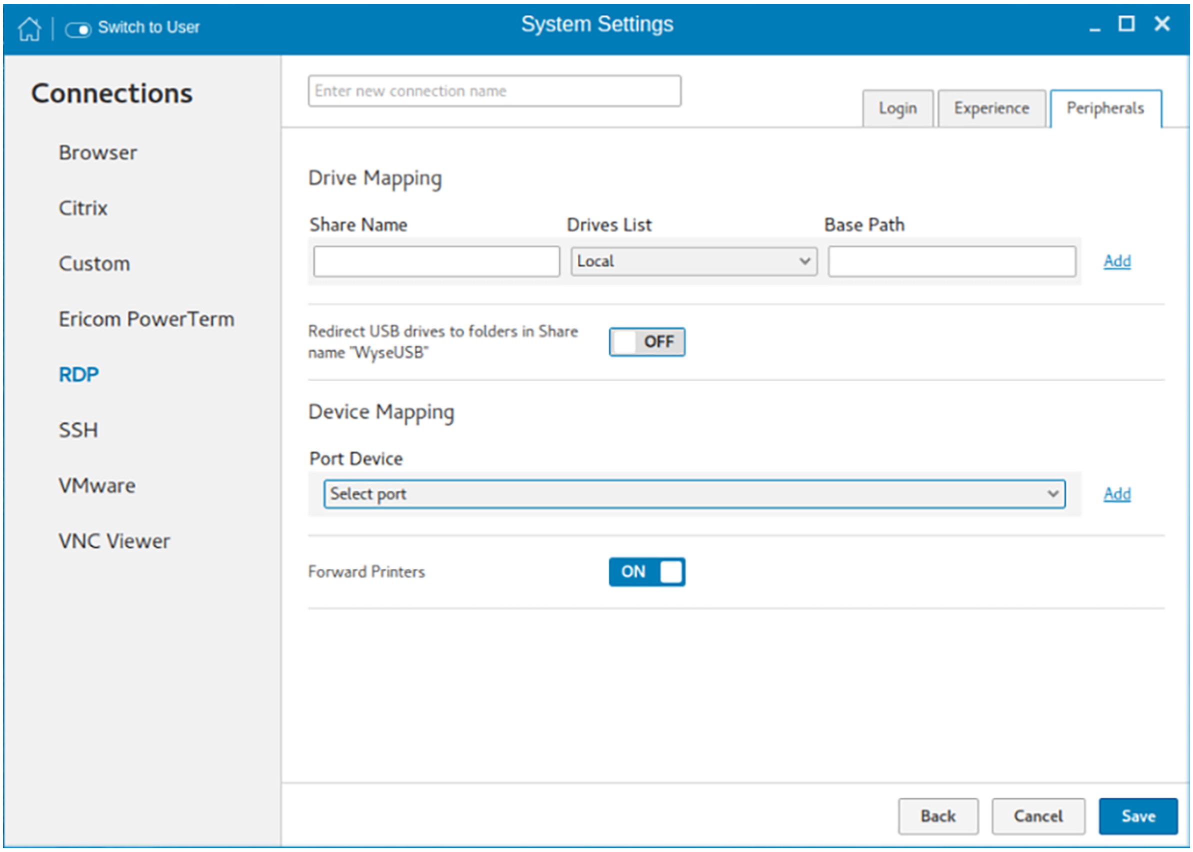
Table 13. RDP Experience Settings

Parameter	Description
Window Resolution	Select the Windows resolution you can use to get the best display on your monitor. The available options are: Default 640 X 480 800 X 600 1024 X 768 1280 X 1024 1600 X 1200 Full Screen
Colors	Specifies the number of colors to display for each pixel. Select the session color mode to get the faster display performance on your monitor. The available options are: High Color (15-bit)

Parameter	Description
	High Color (16-bit) True Color (24-bit) Best Quality (32-bit)
Speed Level	Select a speed level to describe the network connection. • Modem • Broadband • LAN • Custom
Sounds	Select the relevant option from the drop-down list. You can choose to redirect the audio on the remote session to the local device, or not allow the audio to play on the remote session on the local device, or leave the audio playing on the remote session. • Off • Local • Remote
Encryption Level	Select an encryption level, either Normal or None. For servers with data encryption settings, you must select Normal for the encryption level.
Wallpaper	Click the **ON/OFF** button to enable or disable this option.
Font Smoothing	Click the **ON/OFF** button to enable or disable this option.
Menu and Window Animation	Click the **ON/OFF** button to enable or disable this option.
Remote FX	Click the **ON/OFF** button to enable or disable this option.
Show window content while dragging	Click the **ON/OFF** button to enable or disable this option. This option shows the window content when the user drags the window on screen.
Subsampling	Click the **ON/OFF** button to enable or disable this option. It enables color space conversion required for Chroma subsampling. Chroma Subsampling is the practice of encoding/compressing images for a higher transmission experience.
Grab Keyboard Events	Click the **ON/OFF** button to enable or disable this option. It enables all keyboard events within the connection window to be sent to the connection’s applications.
Compression	Click the **ON/OFF** button to enable or disable this option.
Low Bandwidth	Click the **ON/OFF** button to enable or disable this option. If enabled, following options are automatically disabled: Wallpaper Font Smoothing

Parameter	Description
	Menu and Window Animation Remote FX—This feature will be supported in next release. Show window content while dragging Subsampling Enables low-bandwidth optimization.
NT4 Compatible	Click the **ON/OFF** button to enable or disable this option.

5 Configure the following tasks in the **Peripherals** tab.



Drive Mapping

Share Name | Drives List: Local | Base Path

Redirect USB drives to folders in Share name "WyseUSB": OFF

Device Mapping

Port Device: Select port

Forward Printers: ON

Figure 56. RDP peripherals settings

- **Drive Mapping**: Drive mapping tab is used to share map names on the server to USB mass storage devices attached to the thin client, and to view and manage the list of current server share names including the drive information mapped on the thin client.

a Enter the share name.

b The list includes the available drives.

c The Base path is an entry to a directory within the drive.

d Click the **ON/OFF** button to enable or disable the Redirect all USB drives to folders in Share named ‘WyseUSB’ option. If enabled, it redirects all USB drives to folders in Share name **WyseUSB**. You can redirect all your USB drives such as USB Floppy, USB CDROM, USB Disk or Memory stick, and local or mounted disk to the folders in share name **WyseUSB** and if this is enabled **Individual Drive Mapping** is disabled.

- **Device Mapping**: Device mapping tab is used to map devices to ports on the thin client, and to view and manage the list of current devices that are mapped on the thin client.

a Select your preferred port devices.

b Click the **ON/OFF** button to enable or disable the **Forward Printers** option.

6 Click **Save** to save the changes.

Configuring and managing the SSH connections

The **SSH connections** page enables you to create and manage the SSH connections. The main SSH connections page has options to create an SSH connection.
To configure the SSH connection, complete the following task:

1 Click the **+** icon to add a new SSH Connection.

The **SSH Connections** page is displayed.

2 Enter the name of the SSH connection.

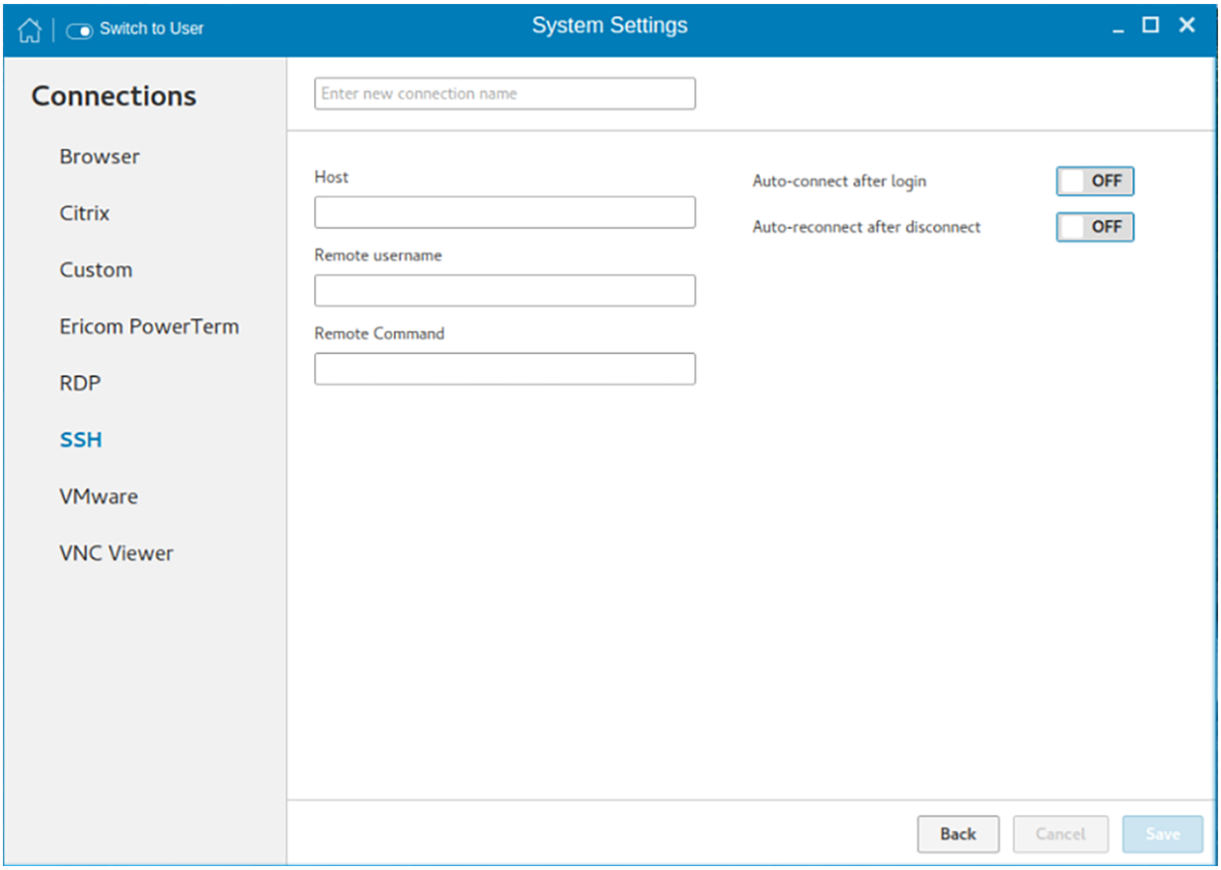


Figure 57. SSH connection settings

3 Enter the IP address or FQDN of the SSH server that you want to connect.

4 Enter the Username to log in to the remote SSH Server.

5 Enter the command to run the program.

6 Click the **ON/OFF** button to enable or disable the Auto-connect after login option. If enabled, the connection is automatically connected after you log in to your thin client.

7 Click the **ON/OFF** button to enable or disable the Auto-reconnect after disconnected option. If enabled, the connection is automatically re-connected after you disconnect from the session.

8 Select the time duration in seconds to delay the reconnection attempt after a disconnection occurs.

9 Click **Save** to save the changes.

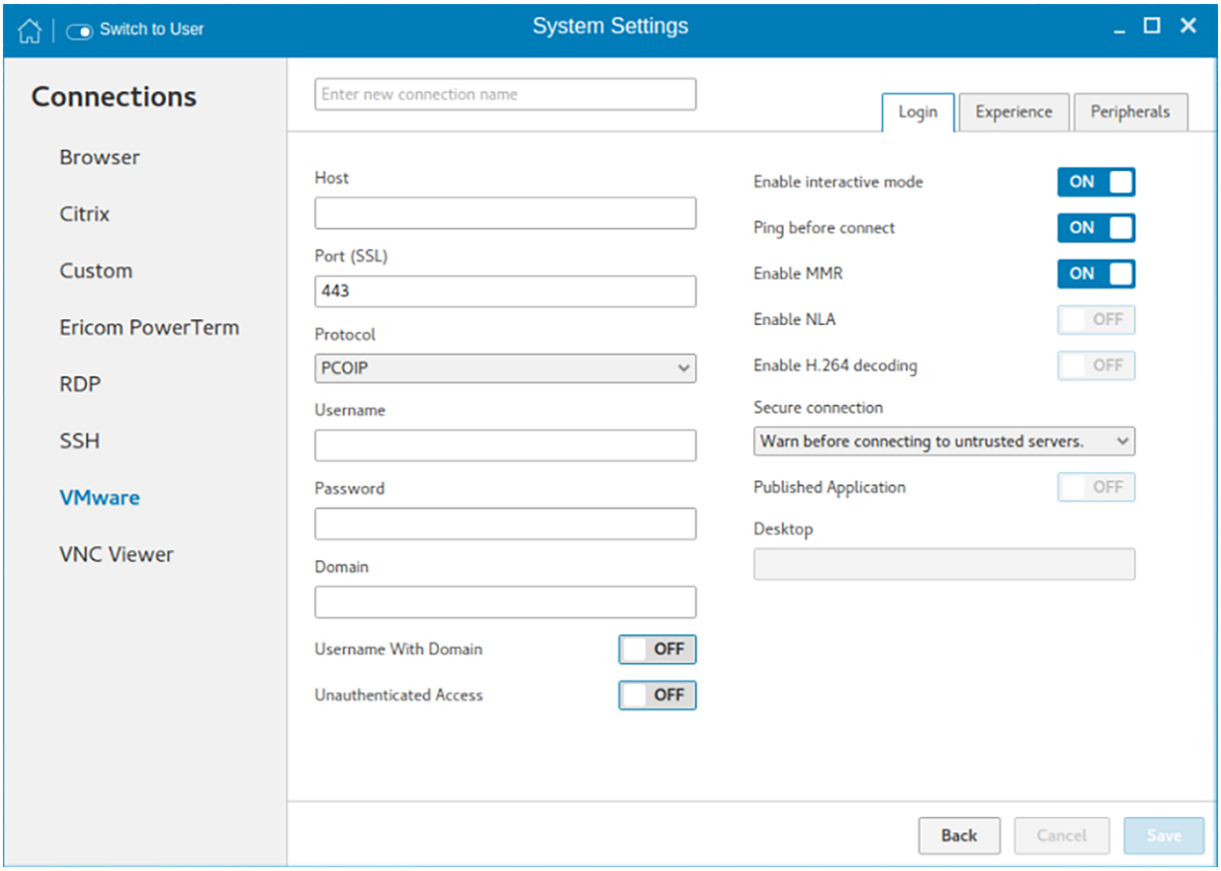
Configuring and managing VMware connections

The **VMware connections** page enables you to create and manage the View client 3.5 connections.

To configure the VMware settings, complete the following task:

1. Click the **+** icon to add a new VMware Connection.

   The **VMware Connections** page is displayed.
2. Enter the name of the **VMware connection**.
3. Configure the following options in the **Login** tab.



Enter new connection name

Host

Port (SSL): 443

Protocol: PCOIP

Username

Password

Domain

Username With Domain: OFF

Unauthenticated Access: OFF

Enable interactive mode: ON

Ping before connect: ON

Enable MMR: ON

Enable NLA: OFF

Enable H.264 decoding: OFF

Secure connection: Warn before connecting to untrusted servers.

Published Application: OFF

Desktop

Figure 58. VMware connection login settings

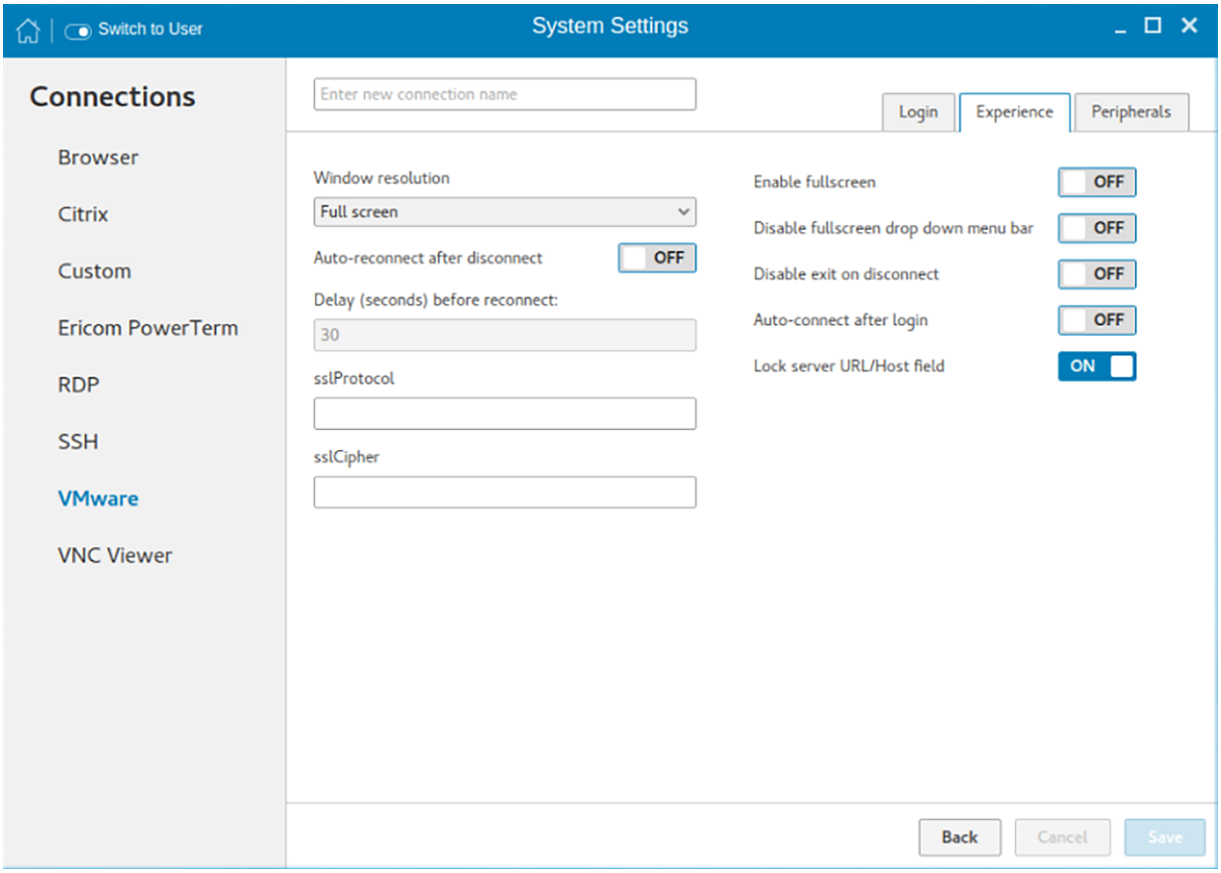
Table 14. Login

Parameter	Description
Host	Enter the host name or **IP address** or **FQDN** of the Horizon of the VMware View Server.
Port	Enter the port number of the host.
Protocol	From the drop-down list, select the specific protocol. The available options are: • PCOIP • RDP

Parameter	Description
	• Blast
Username	Enter the User ID that is used to log in to the remote Horizon server.
Password	Enter the password that is used to log in to the remote Horizon server.
Domain	Enter the Domain name. It is used to log in the remote Horizon server.
Username with Domain	Click the **ON/OFF** button to enable or disable this option. If enabled, specify the domain along with user name.
Unauthenticated Access	Click the **ON/OFF** button to enable or disable this option. If enabled, specify the unauthenticated access username. Password and domain credentials are not required.
Enable interactive mode	Click the **ON/OFF** button to enable or disable this option. If enabled, then after a successful connection to the server, it displays all the published application and desktop icons. You can start the applications or desktop sessions based on your choice If disabled, then the Published Applications option is enabled in the Login tab, and selecting that option enables you to directly start the application or desktop that you specify.
Ping before connect	Click the **ON/OFF** button to enable or disable this option. If enabled, it pings the connection is checked in server IP/FQDN before connecting to a session.
Enable MMR	Click the **ON/OFF** button to enable or disable the multimedia redirection (MMR) feature. If enabled, the multimedia stream is processed on the thin client using a virtual channel.
Enable NLA	This option is available to configure when you select the protocol as RDP. Click the **ON/OFF** button to enable or disable this option. Enable the Network Level Authentication (NLA), if NLA is enabled on your remote computer. Your remote computer requires NLA user authentication before you establish a full Remote Desktop connection and the login screen is displayed.
Enable H.264 decoding	Click the **ON/OFF** button to enable or disable this option. Select this option to allow H.264 decoding in Horizon Client. When this option is selected (the default setting), Horizon Client uses H.264 decoding, if the agent supports H.264 software encoding. If the agent does not support H.264 software encoding, Horizon Client uses JPG/PNG decoding. Deselect this option to always use JPG/PNG decoding. This option is applicable only for VMware Blast protocol and RDP protocol.
Secure connection	Click the Secure Preferences tab and select any of the options that determine how the client should proceed when it cannot verify that your connection to the server is secure.
Published Application	Click the **ON/OFF** button to enable or disable this option. If enabled, specify the Published Application name.

Parameter	Description
	If disabled, specify the Published desktop name.
Desktop	If interactive mode is disabled, you can specify Published desktop name.
Application	If interactive mode is disabled, you can specify Published application name.

4 The following options must be configured in the **Experience** tab.



Enter new connection name

Window resolution: Full screen

Auto-reconnect after disconnect: OFF

Delay (seconds) before reconnect: 30

sslProtocol

sslCipher

Enable fullscreen: OFF

Disable fullscreen drop down menu bar: OFF

Disable exit on disconnect: OFF

Auto-connect after login: OFF

Lock server URL/Host field: ON

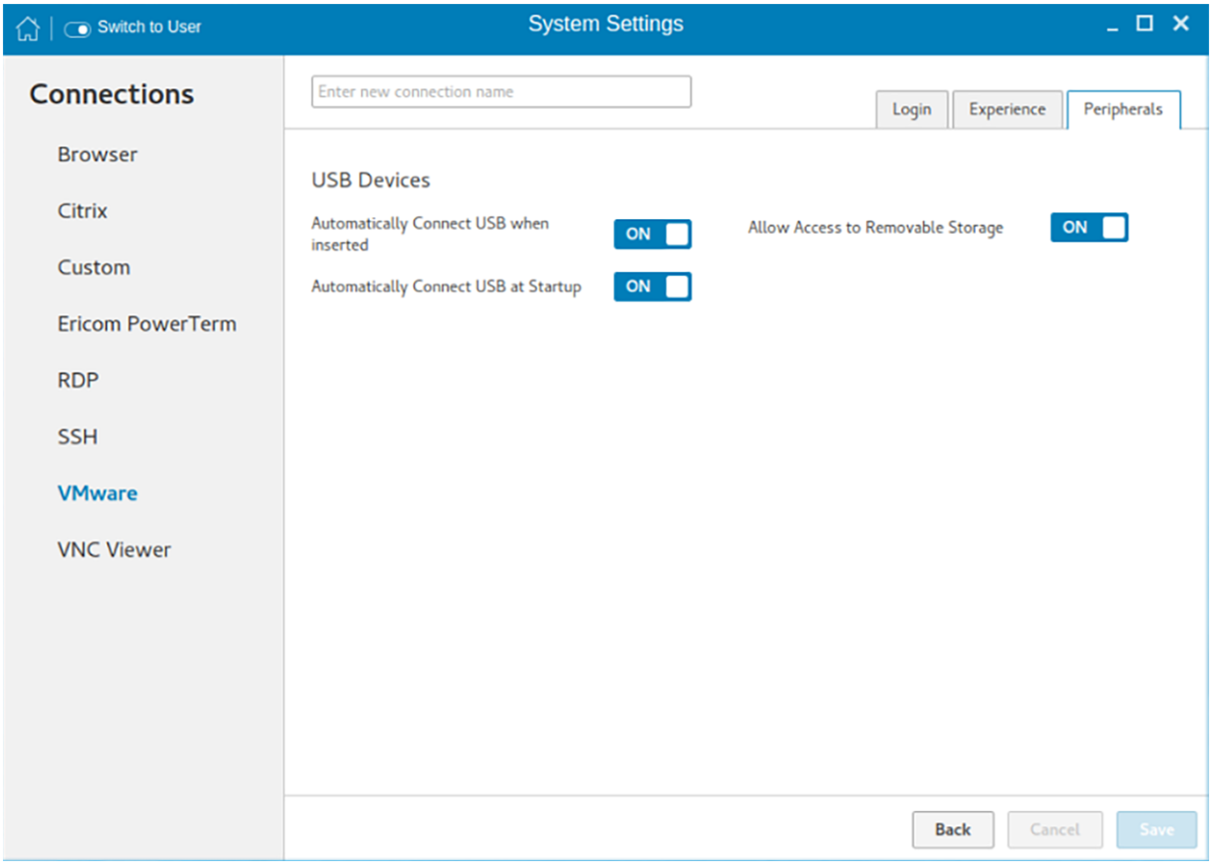
Figure 59. VMware connection experience settings

Table 15. Experience

Parameter	Description
Windows resolution	Select the Windows resolution that you want to get the best display on your monitor. The available resolutions are: Use All Monitors Full Screen Large Screen Small Screen 1024 X 768

Parameter	Description
	800 X 600 640 X 480
Auto-Reconnect after disconnect	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically re-established after you disconnect from the session.
Delay (seconds) before reconnect	Select the time duration in seconds to delay the reconnection attempt after a disconnection occurs.
sslProtocol	Use the SSL protocol to securely connect to a web server over the insecure internet.
sslCipher	Use the SSL Cipher suite to secure your SSL connection.
Enable fullscreen	Click the **ON/OFF** button to enable or disable this option. Select this option to view the remote session in full screen mode in all the monitors.
Disable fullscreeen drop down menu bar	Click the **ON/OFF** button to enable or disable this option. Select this option to disable the drop-down menu bar in the full screen mode.
Disable exit on the disconnect	Click the **ON/OFF** button to enable or disable this option. Select this option if you do not want the Horizon server to retry connecting if there is a connection error. You can typically select this option if you use kiosk mode.
Auto-connect after login	Click the **ON/OFF** button to enable or disable this option. Select this option to reconnect automatically after a disconnection occurs.
Lock server URL/Host field	Click the **ON/OFF** button to enable or disable this option.

5 Configure the following options in the **Peripherals** tab:



USB Devices

Automatically Connect USB when inserted: ON

Allow Access to Removable Storage: ON

Automatically Connect USB at Startup: ON

Figure 60. VMware connection peripherals settings

Table 16. Peripherals

Parameter	Description
Automatically Connect USB when inserted	Click the **ON/OFF** button to enable or disable this option. Select this option if you want to automatically connect your USB key to the thin client after you plug-in the USB key.
Automatically Connect USB at Startup	Click the **ON/OFF** button to enable or disable this option. Select this option if you want to automatically connect your USB key to the thin client when you start the system.
Allow Access to Removable Storage	Click the **ON/OFF** button to enable or disable this option. Select this option if you want to permit access to use removable storage devices.

6 Click **Save** to save the settings.

Configuring and managing the VNC viewer connections

The **VNC Viewer connections** page enables you to create and manage the VNC connections. The main VNC connections page has options to create a VNC connection.

To configure the VNC Viewer Settings, complete the following task:

1. Click the **+** icon to add a new VNC connection. The **VNC Viewer Connections** page is displayed.
2. Enter the name of the VNC connection.
3. The following options must be configured in the **Login** tab.

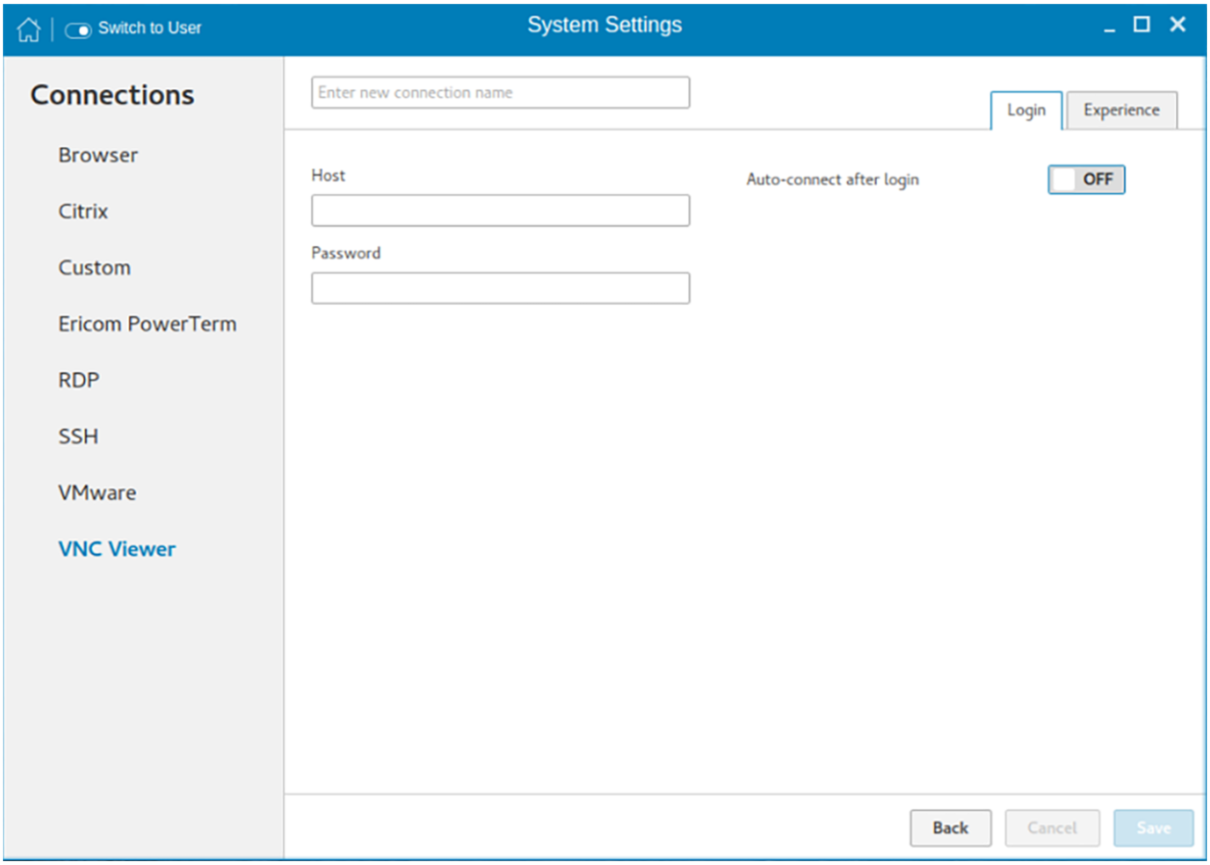
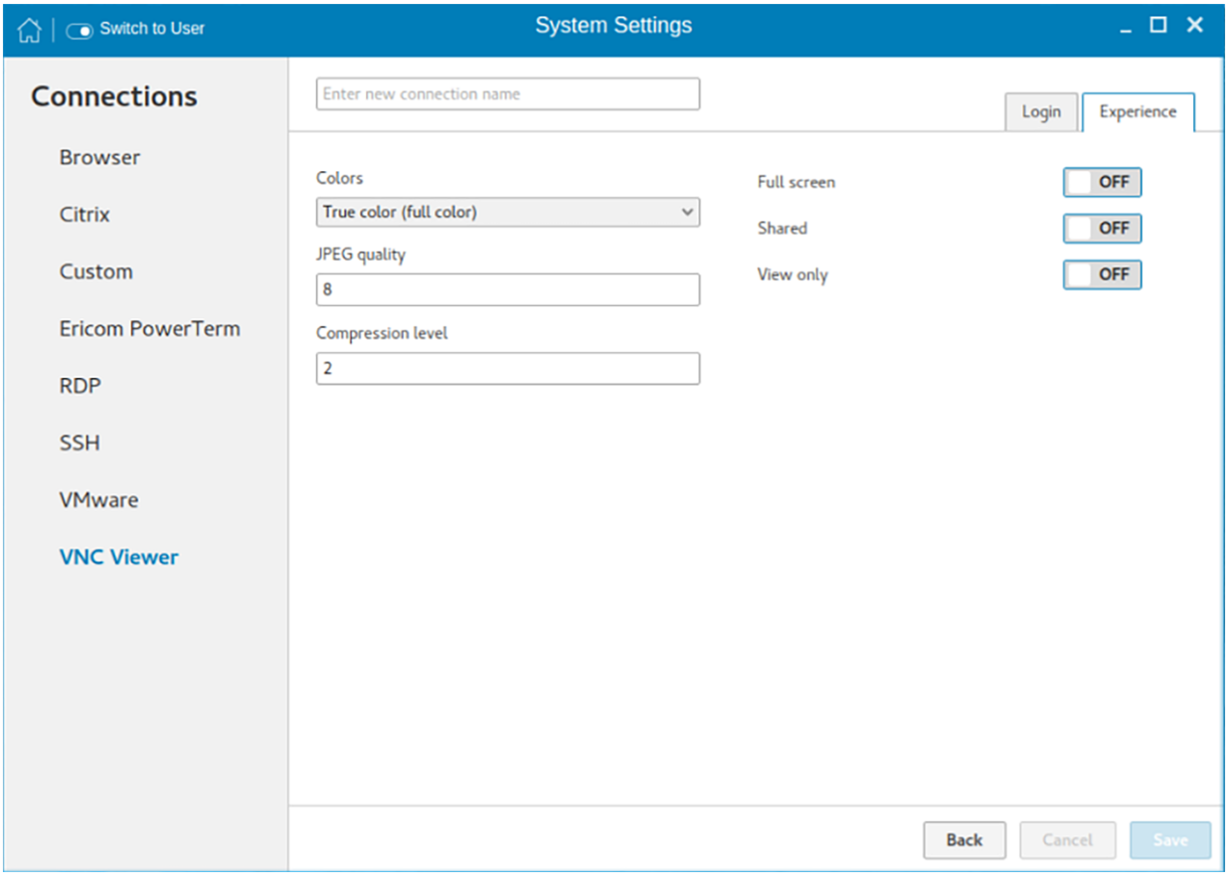


Figure 61. VNC viewer login settings

Table 17. VNC viewer login settings

Parameter	Description
Host	Enter the IP address or FQDN of the VNC server which you want to connect.
Password	Enter the password to log in to the remote VNC Server.
Auto-connect after login	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is automatically connected after you log in to your thin client.

4. The following options must be configured in the **Experience** tab.



Colors: True color (full color)

JPEG quality: 8

Compression level: 2

Full screen: OFF

Shared: OFF

View only: OFF

Figure 62. VNC viewer experience settings

Table 18. VNC viewer experience settings

Parameter	Description
Colors	Specifies the number of colors to display for each pixel. Select the session color mode to get the faster display performance on your monitor. The available options are:\ • True color (full color) • 8 colors (very low) • 64 colors (low) • 256 colors(medium)
JPEG quality	From the drop-down list, select the preferred value. The range for JPEG quality is 0-9, with 0 being poor quality and 9 being the best quality.
Compression level	From the drop-down list, select the preferred value. The range for compression level is 1–6. The 1 value explains the fast quality and 6 value explains the best quality.
Full screen	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is started in the full screen mode. It is not in the kiosk mode, click the standard VNC viewer f8 key to exit the full screen mode.

Parameter	Description
Shared	Click the **ON/OFF** button to enable or disable this option. If enabled, the connected desktop is in share mode.
View only	Click the **ON/OFF** button to enable or disable this option. If enabled, the connection is in view-only mode. Mouse and keyboard input to the remote machine is disabled.

5 Click **Save** to save the changes.

5

Security settings

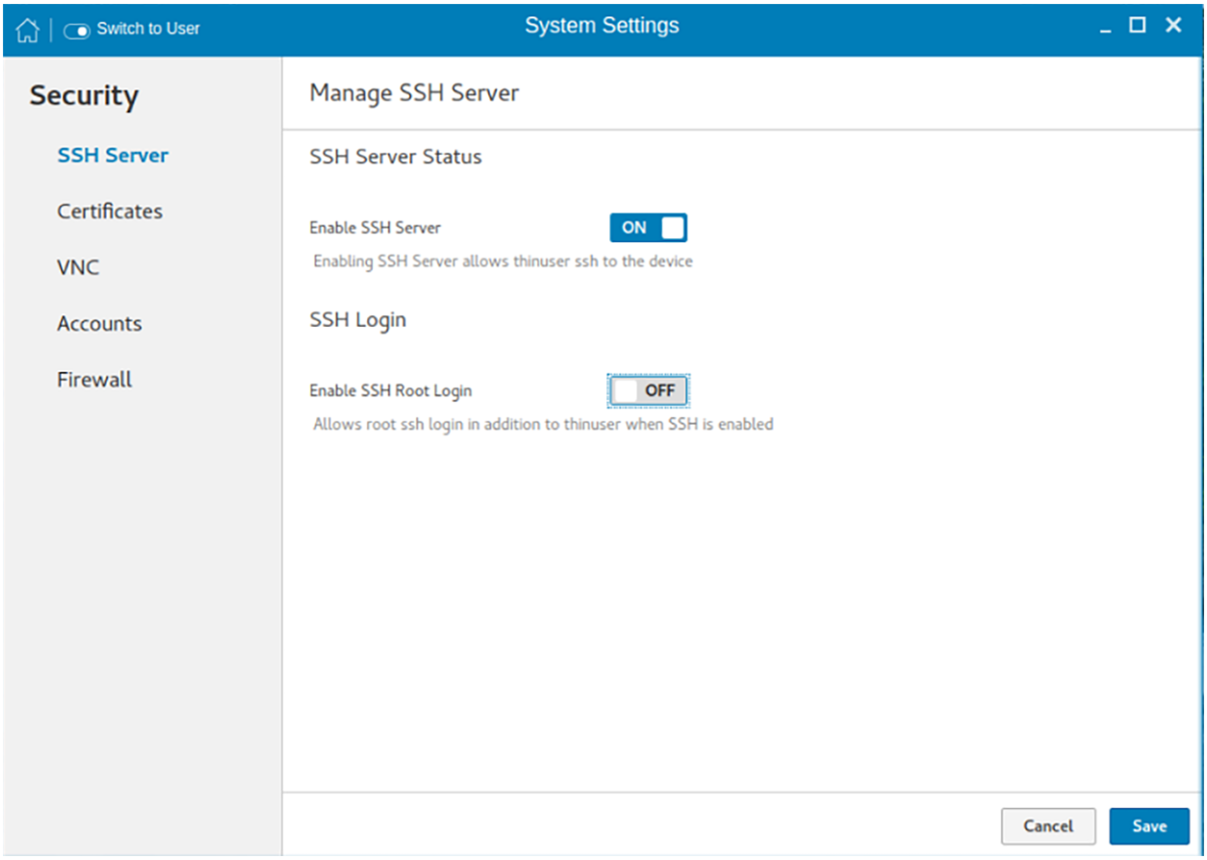
On the **System Settings** page, click the **Security** icon. The following tabs are listed on the left pane of the System Settings page.

- SSH Server
- Certificates
- VNC
- Accounts
- Firewall

Topics:

Managing SSH server preferences

By default, **SSH Server** is disabled on the thin client. The Managing the SSH server screen is available only in Admin mode. It enables to configure the SSH server on the thin client.



Manage SSH Server

SSH Server Status

Enable SSH Server ON

Enabling SSH Server allows thinuser ssh to the device

SSH Login

Enable SSH Root Login OFF

Allows root ssh login in addition to thinuser when SSH is enabled

Figure 63. Manage SSH

Configure the following options:

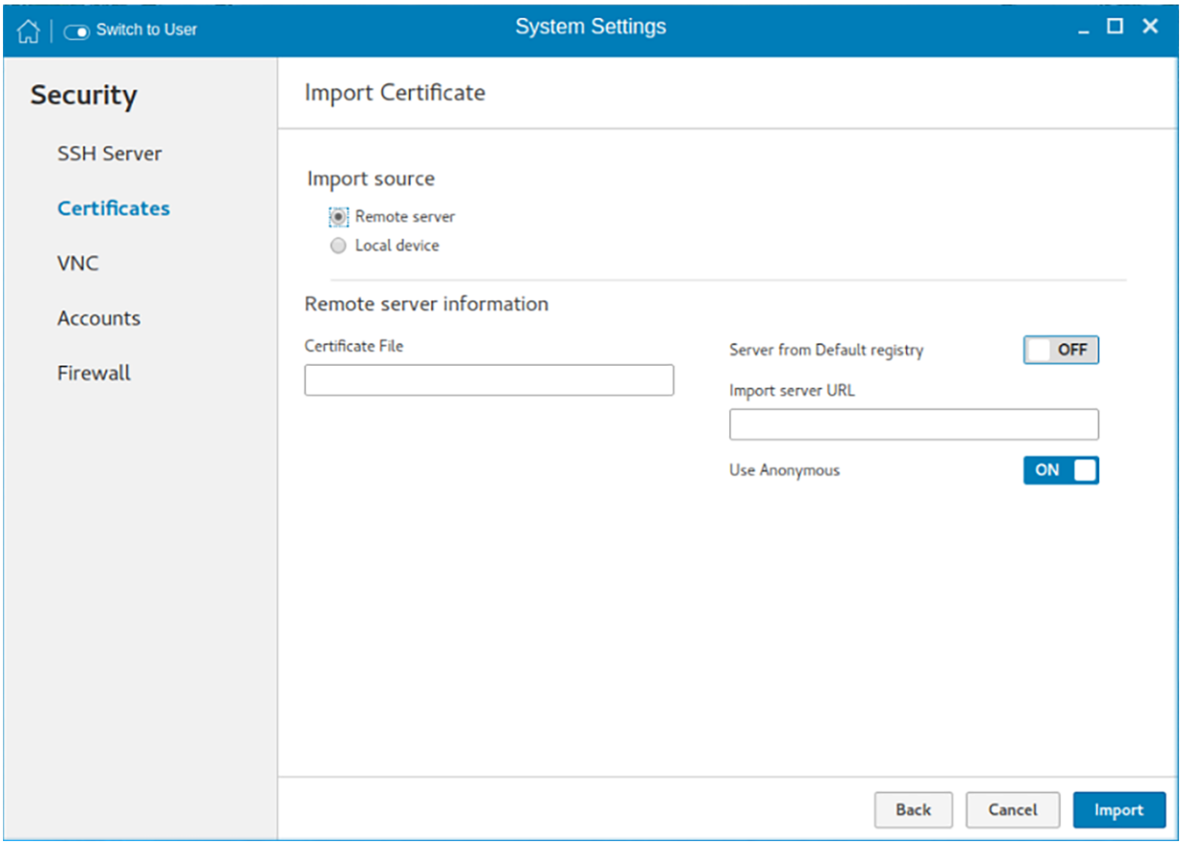
1. Click the **ON/OFF** button to enable the **Enable SSH** option. If enabled, the SSH server starts working.
2. Click the **ON/OFF** button to enable or disable the **Enable SSH Root Login** option. When the **Enable SSH** option is enabled, the **Enable SSH Root Login** option is not enabled automatically.
3. Click **Save** to save the changes.

Managing the certificates

1. Click the **+** icon to import a new certificate.

   The **Import Certificate** page is displayed.
2. Select the preferred **Import Source** option.
   - Remote Server
   - Local Devices

   a. **Remote server**



Import Certificate

Import source

● Remote server

○ Local device

Remote server information

Certificate File

Server from Default registry: OFF

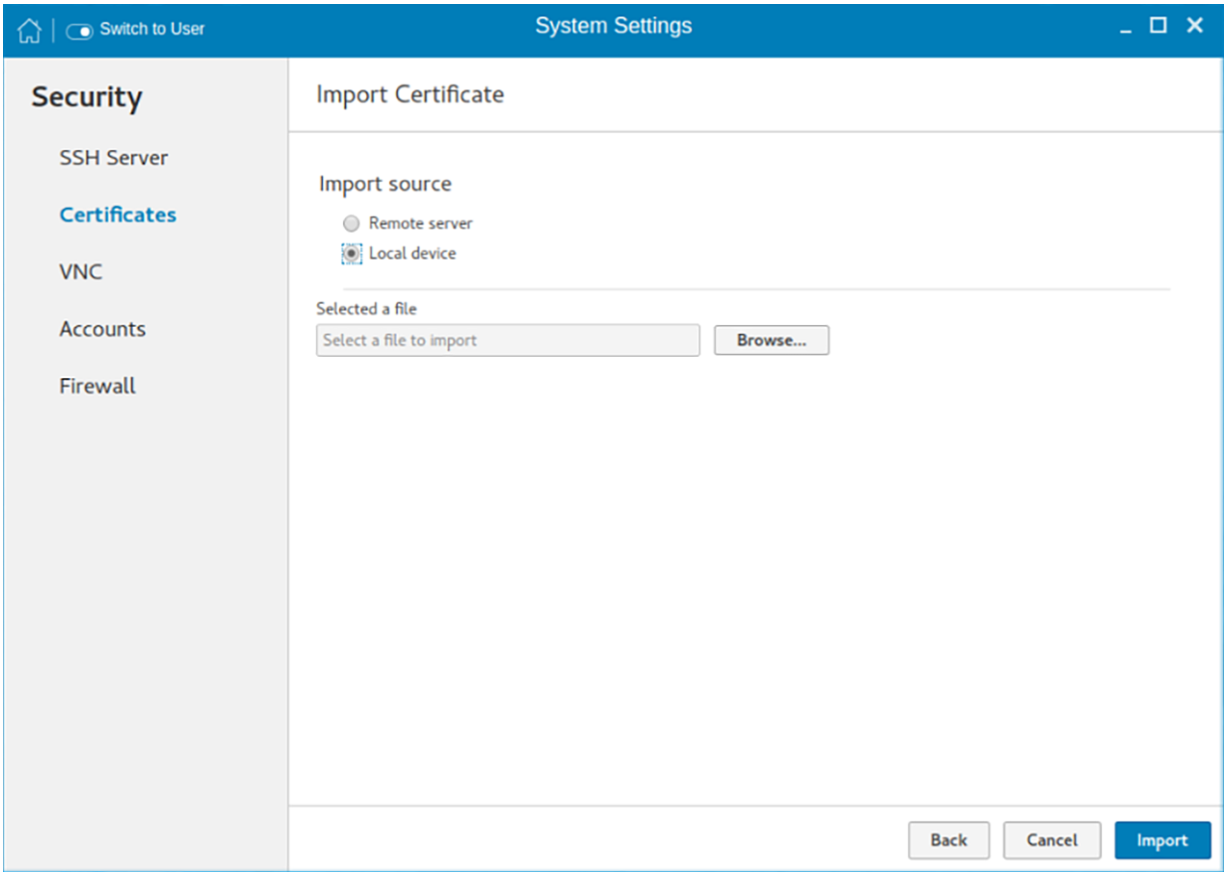
Import server URL

Use Anonymous: ON

Figure 64. Import certificates remote server

1. If you select **Remote server** option, the remote server information is displayed.
   a. Enter the **Importing server URL**. The supported protocols are ftp, http, and https.
   b. Browse the required **Certificate File**.
   c. Click the **ON/OFF** button to enable or disable the **Sever from default registry** option.
2. **User Anonymous**: Click the **ON/OFF** button to enable or disable this option. If disabled, enter the Username and password required for the server.

b **Local Devices**



Import Certificate

Import source

○ Remote server

● Local device

Selected a file

Select a file to import

Figure 65. Import certificates local device

1. Click the **Browse** tab and navigate to the certificate that you want to use.
2. Click **OK**.

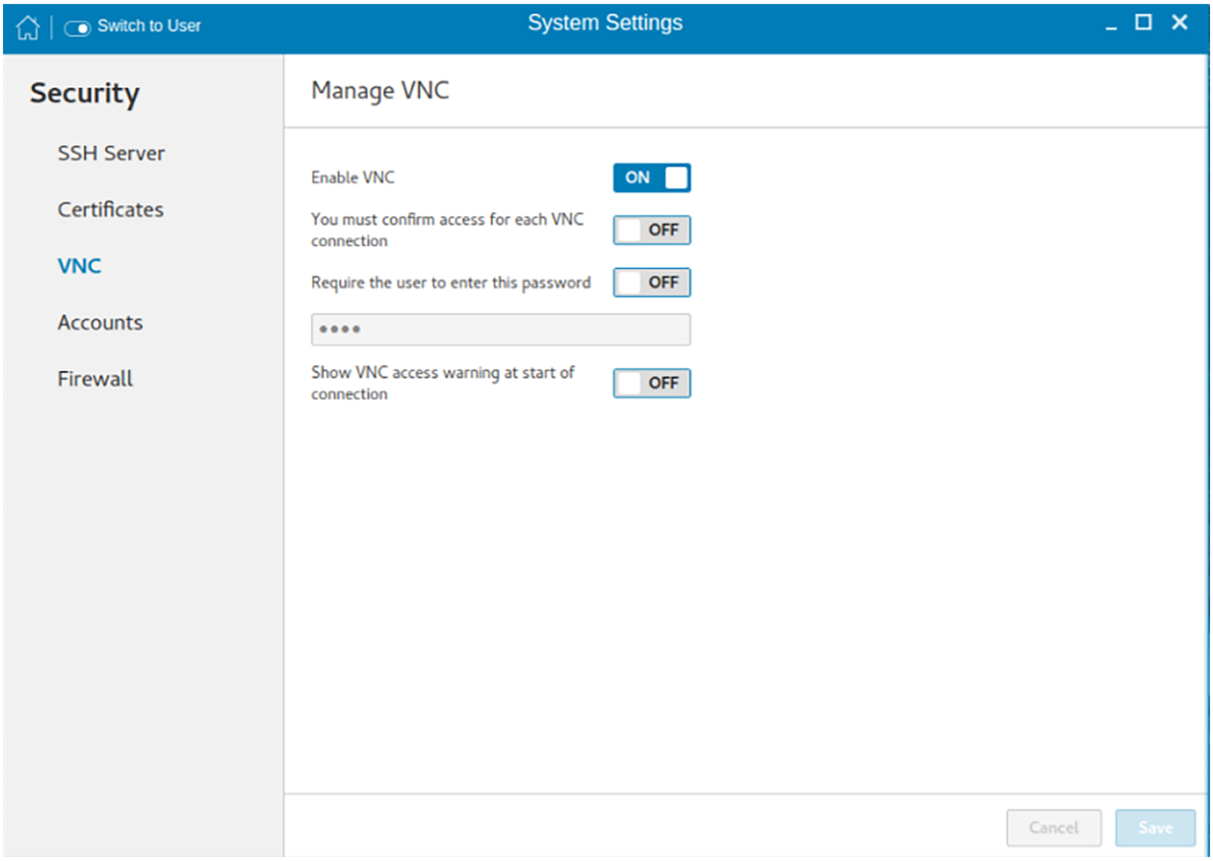
c Click **Import** to import the certificates.

The installed certificates are shown as, Filename: certificate name.

d To remove a certificate, move the cursor over it and click **Remove**.

Setting VNC server preferences

Use the VNC server page to configure the VNC server preferences.



Manage VNC

Enable VNC ON

You must confirm access for each VNC connection OFF

Require the user to enter this password OFF

••••

Show VNC access warning at start of connection OFF

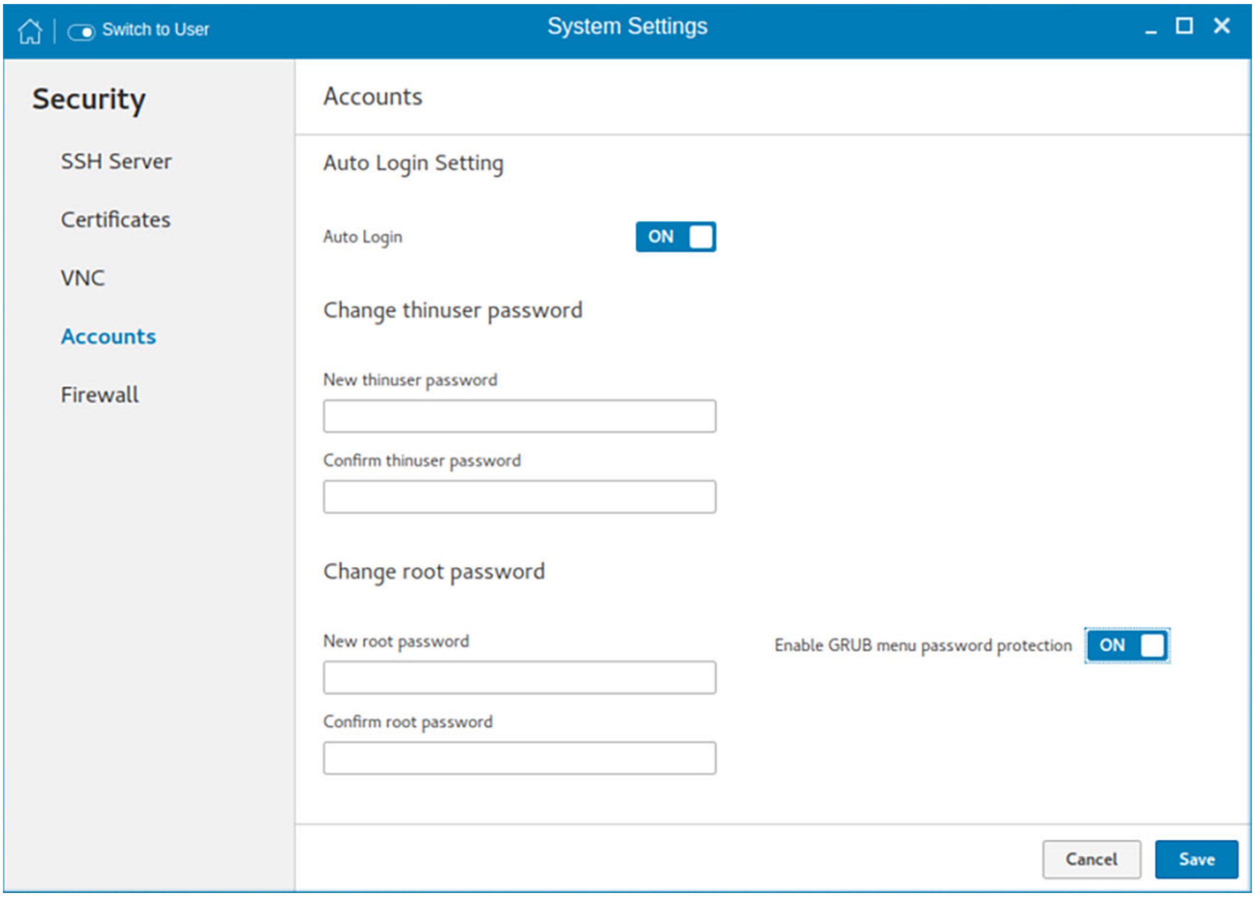
Figure 66. VNC server preferences

To configure the VNC server preferences:

1 Click the **ON/OFF** button to enable or disable the Enable VNC option.
2 Click the **ON/OFF** button to enable or disable the confirmation for accessing each VNC connection option.
3 Click the **ON/OFF** button to enable or disable the Require the user to enter this password option. If enabled, you can enter the password. Maximum length is 8 characters.
4 Click the **ON/OFF** button to enable or disable the option to show the VNC access warning at start of the connection.
5 Click **Save** to save the changes.

Managing the accounts settings

The accounts management page is available in the admin mode only.



Accounts

Auto Login Setting

Auto Login ON

Change thinuser password

New thinuser password

Confirm thinuser password

Change root password

New root password

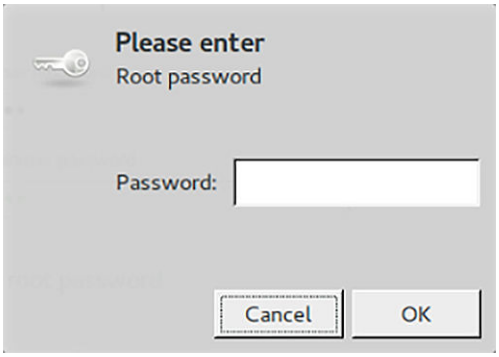
Enable GRUB menu password protection ON

Confirm root password

Figure 67. Accounts settings

To manage the account settings, configure the following options:

1 **Auto Login**—Click the **ON/OFF** button to enable or disable the Auto Login option. If you enable this option, the thin client is automatically logged in without any user intervention.
2 **Change thinuser password**—Use this option if you want to change the thinuser password.
3 **Change root password**—Use this option if you want to change the root password.
4 **Enable GRUB menu password protection**—Click the **ON/OFF** button to enable or disable the GRUB menu password protection. If this option is enabled, you can set the password for the GRUB boot menu to restrict access to specific operations.
5 Click **Save**.
6 When prompted, enter the root password, and click **OK**.



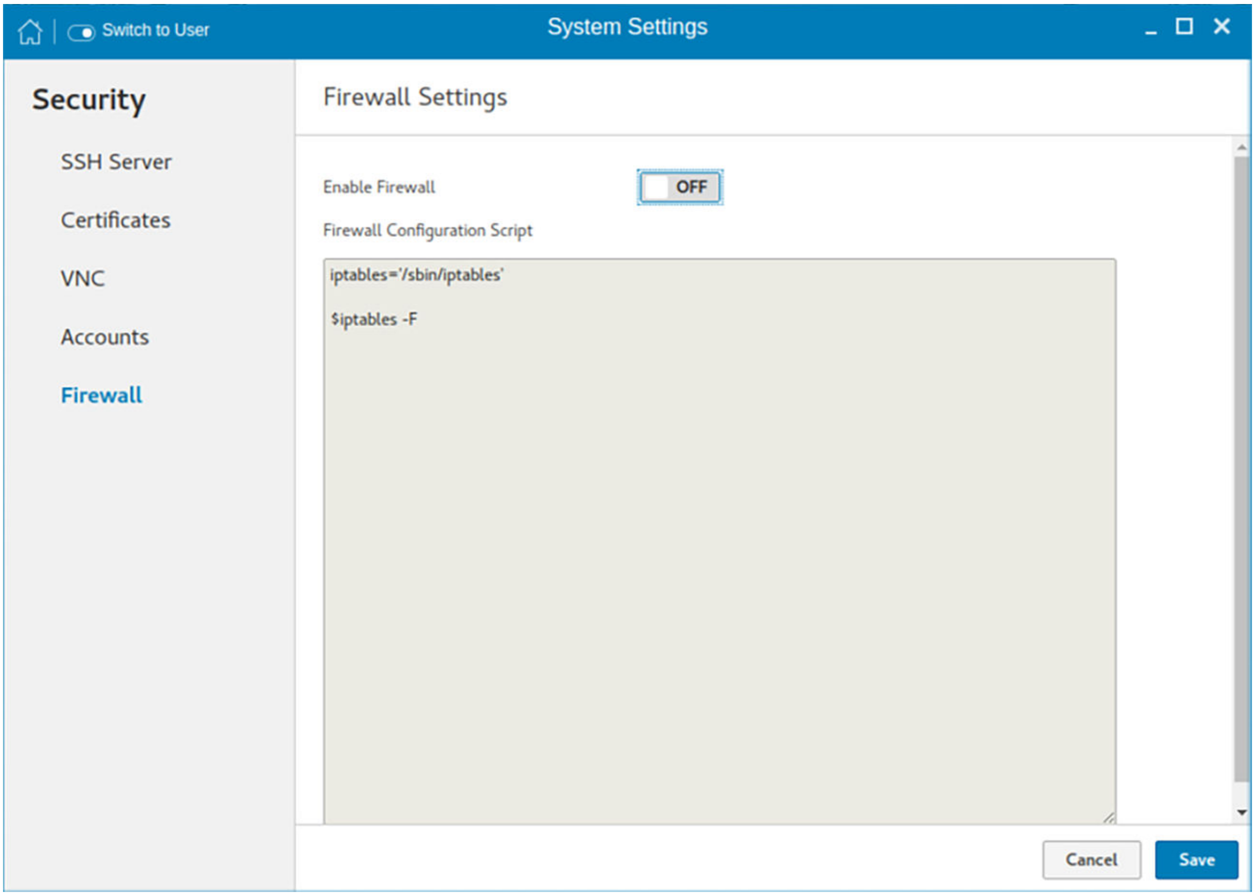
Please enter
Root password

Password:

Figure 68. Root password

Configuring the firewall settings

Use the firewall settings page to configure firewall settings.



Enable Firewall OFF

Firewall Configuration Script

```
iptables='/sbin/iptables'

$iptables -F
```

Figure 69. Firewall settings

To configure the firewall settings on your thin client, do the following:

1. To enable firewall, click the **ON/OFF** button.
2. Type the firewall configuration script in the text box.

   For example, the following `iptables` commands can be used to disable ping from the thin client or to the thin client:

   ```
   /sbin/iptables -A OUTPUT -p icmp --icmp-type 8 -j DROP
   /sbin/iptables -A INPUT -p icmp --icmp-type 8 -j DROP
   ```
3. Click **Save**.
4. When prompted, click **Restart**.

   The changes are applied after the system reboot.

6

Additional management configurations

On the **System Settings** page, click the **Management** icon. The following tabs are listed on the left pane of the **System Settings** page.

- Configuration
- HAgent
- INI
- Logs and Tools
- SCEP
- Wyse Device Agent

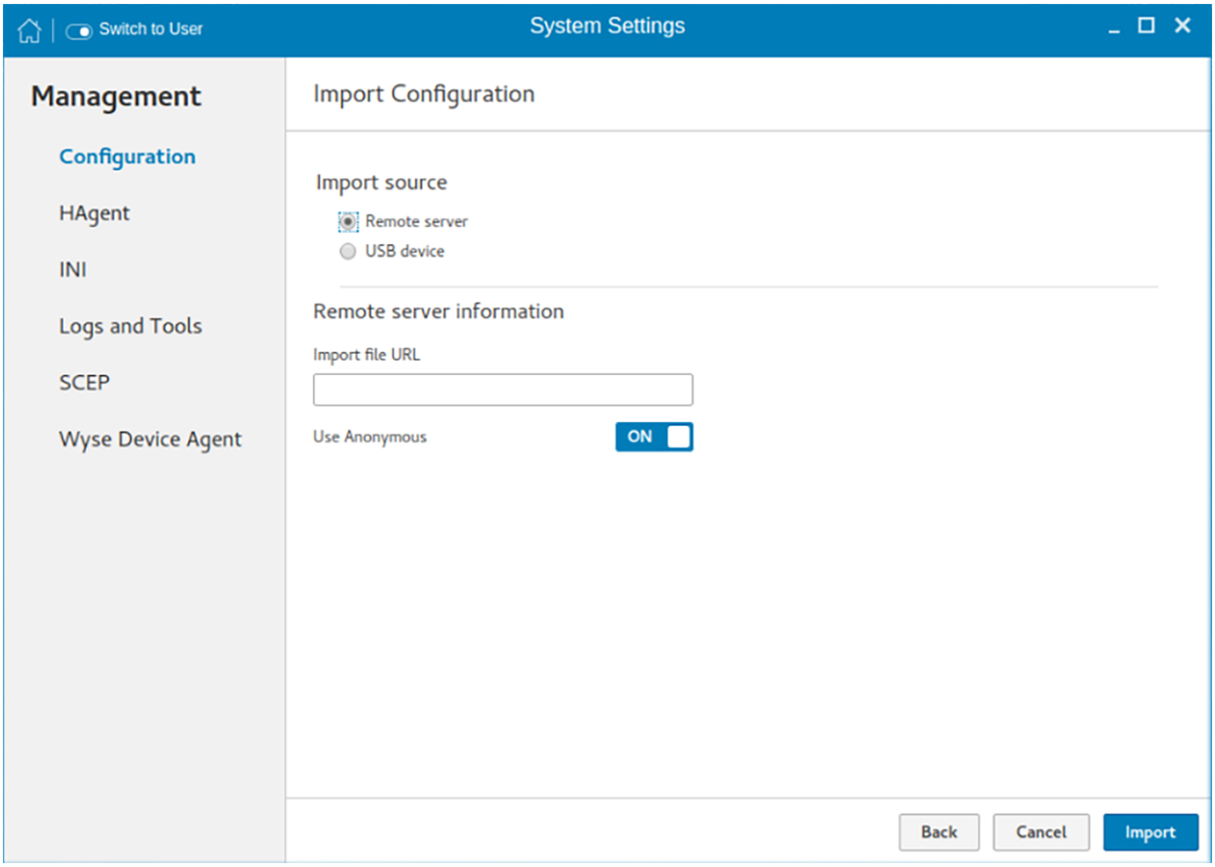
Topics:

Configuration management

You can manage the device configuration stored locally. Use import and export options to deploy the configuration to the other devices.

1. Click the **+** icon to import device configuration from provided configuration file. The **Import Device** configuration page is displayed and you are prompted to restart the system.
2. Select the preferred **Import Source** option.
   - Remote Server
   - USB Device

   a **Remote server**



Import Configuration

Import source

● Remote server
○ USB device

Remote server information

Import file URL

Use Anonymous ON

Figure 70. Import configuration - Remote server

1 If you select **Remote server** option, the remote server information is displayed. Enter the **Importing file URL**. The supported URLs are ftp, http, and https.

2 Click the **ON/OFF** button to enable or disable the Use Anonymous option. If disable, enter the Username and password required for the server.

3 Click **Import** to import the configuration.

b **USB Device**

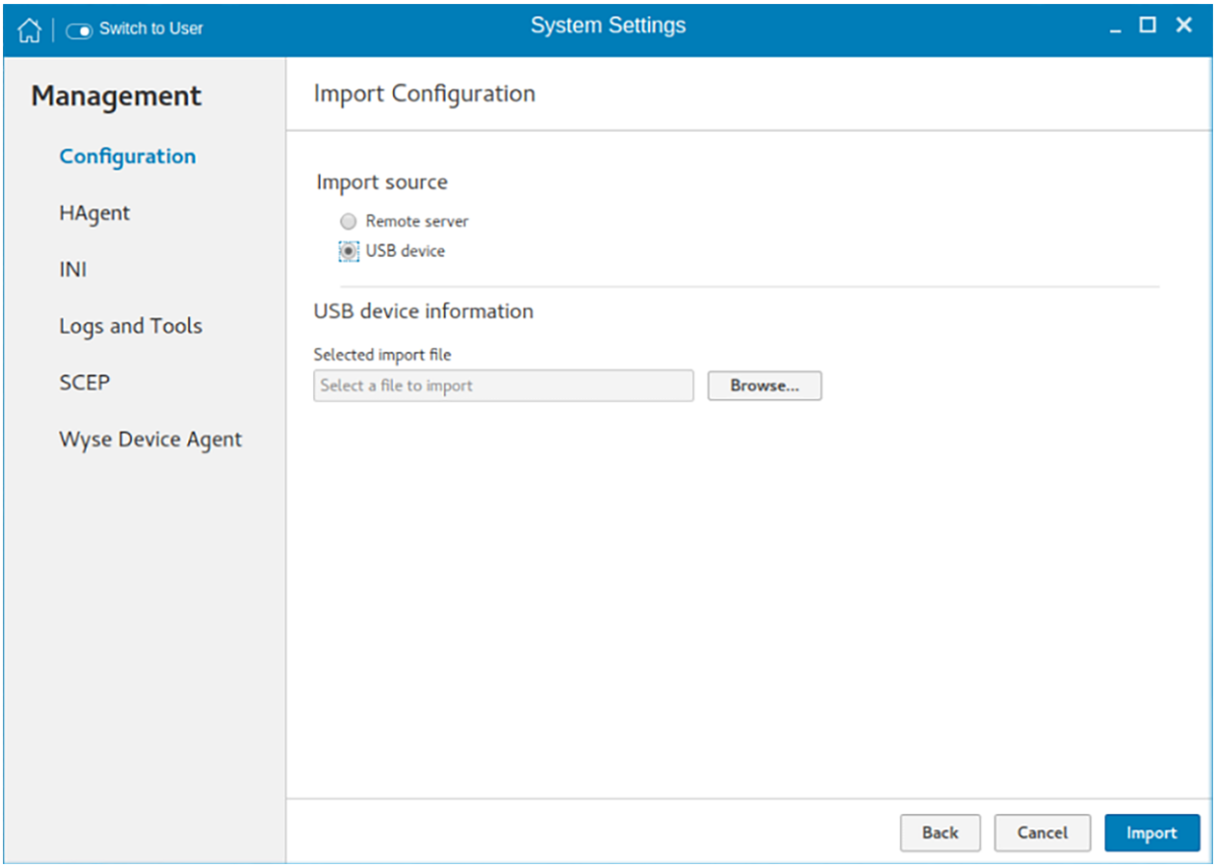


Figure 71. Import configuration - USB device

1. Click the **Browse** tab.

   > NOTE: **You must insert the USB device to import the files.**

2. Click **Import** to import the configuration.

3 Click the icon to Export device configuration to a configuration file. The **Export device configuration** page is displayed.

4 Select the preferred **Export Destination** option.

- Remote Server
- USB Device

a **Remote server**

1. If you select **Remote server** option, the remote server information is displayed. Enter the Configuration file, and export server URL. The supported URLs are ftp, http, and https.
2. Click the **ON/OFF** button to enable or disable the Use Anonymous option. If disable, enter the Username and password required for the server.
3. Click **Export** to export the configuration.

b **USB Device**

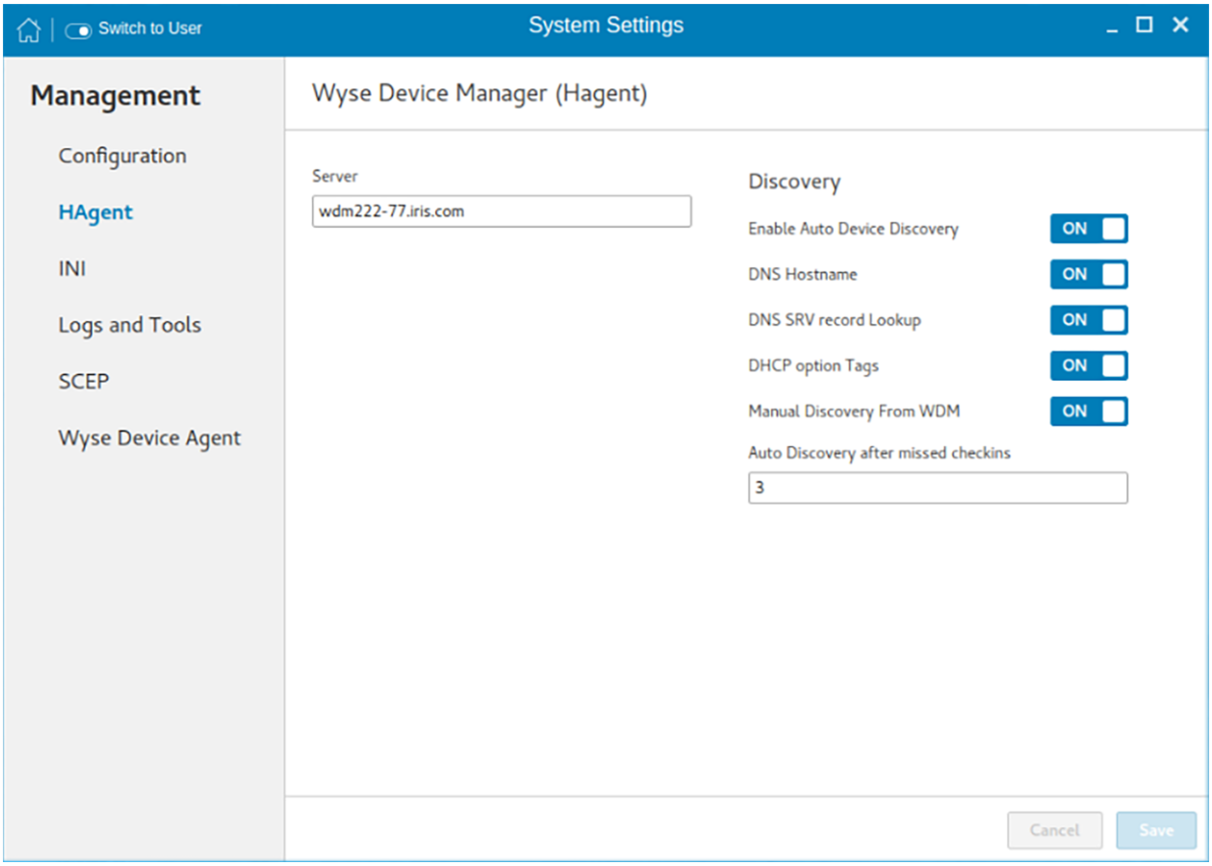
1. Click the **Browse** tab. Use the folders and command buttons to find and specify the export path and file you want to use.
2. Click **OK**.

5 Click the icon to **Reset to factory defaults**.

A warning message is displayed. If you click **OK**, the system is automatically restarted. Resetting to factory defaults affects only configuration, it will not uninstall or reinstall add-ons that are different than the factory image.

HAgent

WDM is a device management solution which helps you to manage cloud clients securely from remote infrastructure. WDM management solution involves both server and client components where client software also known as **HAgent** should be installed on each thin client device for management through WDM.



Server: wdm222-77.iris.com

Enable Auto Device Discovery: ON

DNS Hostname: ON

DNS SRV record Lookup: ON

DHCP option Tags: ON

Manual Discovery From WDM: ON

Auto Discovery after missed checkins: 3

Figure 72. Wyse Device Manager - HAgent

1 Enter the **Wyse Device Manager Server** name in input box.

2 The following options can be configured. This is an admin only configuration in the thin client.

Table 19. Wyse Device Manager Server

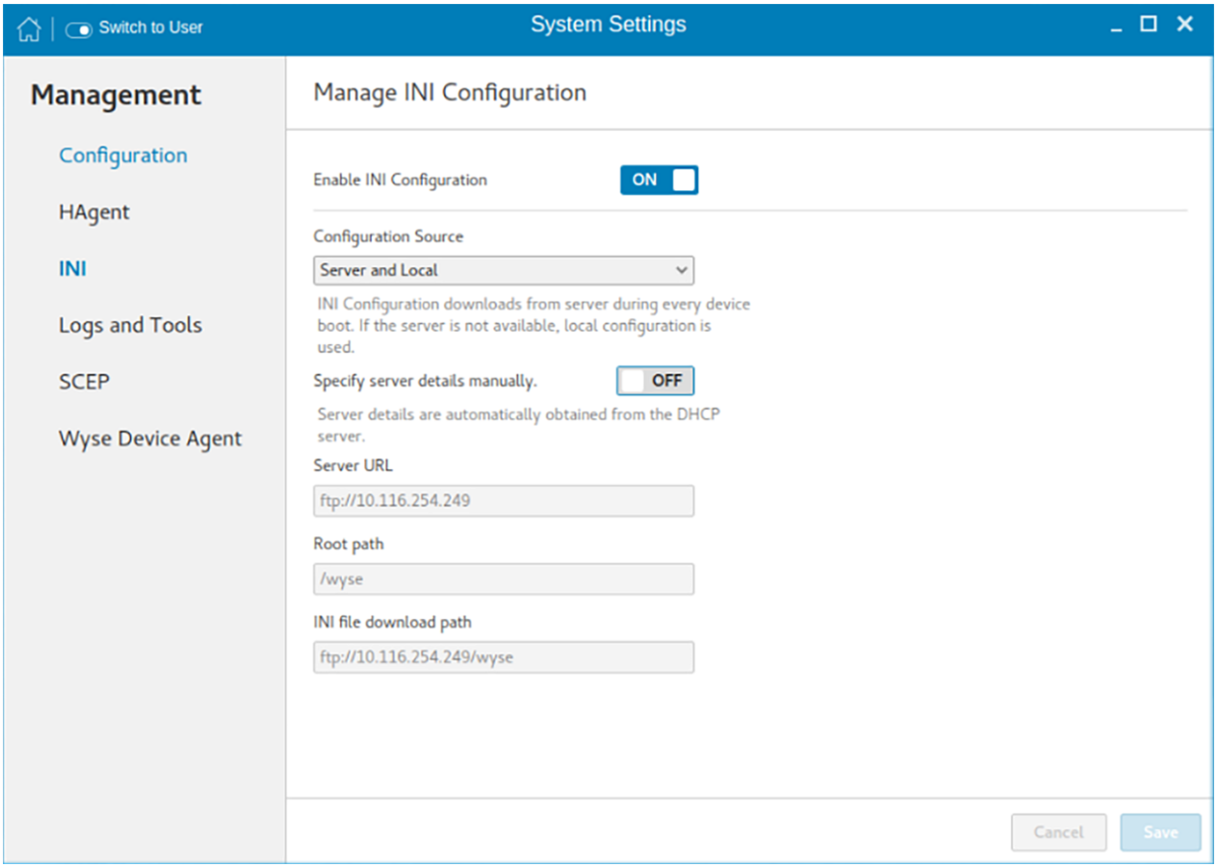
Parameter	Description
Enable Auto Device Discovery	Click the **ON/OFF** button to enable or disable this option. This option enables or disables the discovery of Thin Clients by DNS Hostname , DNS SRV record Lookup , DHCP option Tags.
DNS Hostname	Click the **ON/OFF** button to enable or disable this option. This option will take effect if **Enable Auto Device Discovery** is in OFF state. When this option is in ON state, then the clients are discoverable using DNS Host name.
DNS SRV record Lookup	Click the **ON/OFF** button to enable or disable this option. Auto Device Discovery is in OFF state. When this option is in ON state, then the clients are discoverable using DNS SRV record lookup.

Parameter	Description
DHCP option Tags	Click the **ON/OFF** button to enable or disable this option. This option will take effect if **Enable Auto Device Discovery** is in OFF state. When this option is in ON state, then the clients are discoverable using DHCP options Tags.
Manual Discovery From WDM	Click the **ON/OFF** button to enable or disable this option. If this option is enabled, the WDM server will be able to discover the client through manual discovery.
Auto Discovery after missed checkins	Enter the **Auto Discovery after missed checkins**. The allowable number of missed check-in attempts before going for auto discovery of Wyse Device Manager.

3 Click **Save** to save the changes.

INI management

On the **Manage INI Configuration** page, complete the following task:



Enable INI Configuration: ON

Configuration Source: Server and Local

INI Configuration downloads from server during every device boot. If the server is not available, local configuration is used.

Specify server details manually: OFF

Server details are automatically obtained from the DHCP server.

Server URL: ftp://10.116.254.249

Root path: /wyse

INI file download path: ftp://10.116.254.249/wyse

Figure 73. Manage INI configuration

1 Click the **ON/OFF** button to enable or disable the Enable INI Configuration option. By enabling INI Configuration you can manage this device by configuration files stored on the server or locally.

2 From the drop-down list, select your preferred configuration source.

- Select the Local only source as configuration source. The INI configuration is stored locally on the device.
- Select the Server only source as configuration source, and do the following:

1. Click the **ON/OFF** button to enable or disable the specify server details manually option.
2. If enabled, enter the server URL, username, and password for the secure server.

- Select the Server and Local option as the configuration source, and do the following:
  1. Click the **ON/OFF** button to enable or disable the server and Local option. The INI configuration downloads from the server during every restart of your thin client and if the server is not available, local configuration is used.
  2. If enabled, enter the Server URL, username and password for the secure server.

3 Click **Save** to save the changes.

Logs and Tools

The Logs and Tools section provides the tools for troubleshooting and diagnostics purpose. By default, the **Logs and Tools** screen is available only in admin mode.

1 Click the **Logs** tab to view and export system logs.

The Logs tab shows a list of system logs from where you can select a particular log file to view the contents and search text within the content.

2 Check the check box shown on the left side of Log file name to select log files and click the **Export** button to export logs into a USB drive or remote file server.

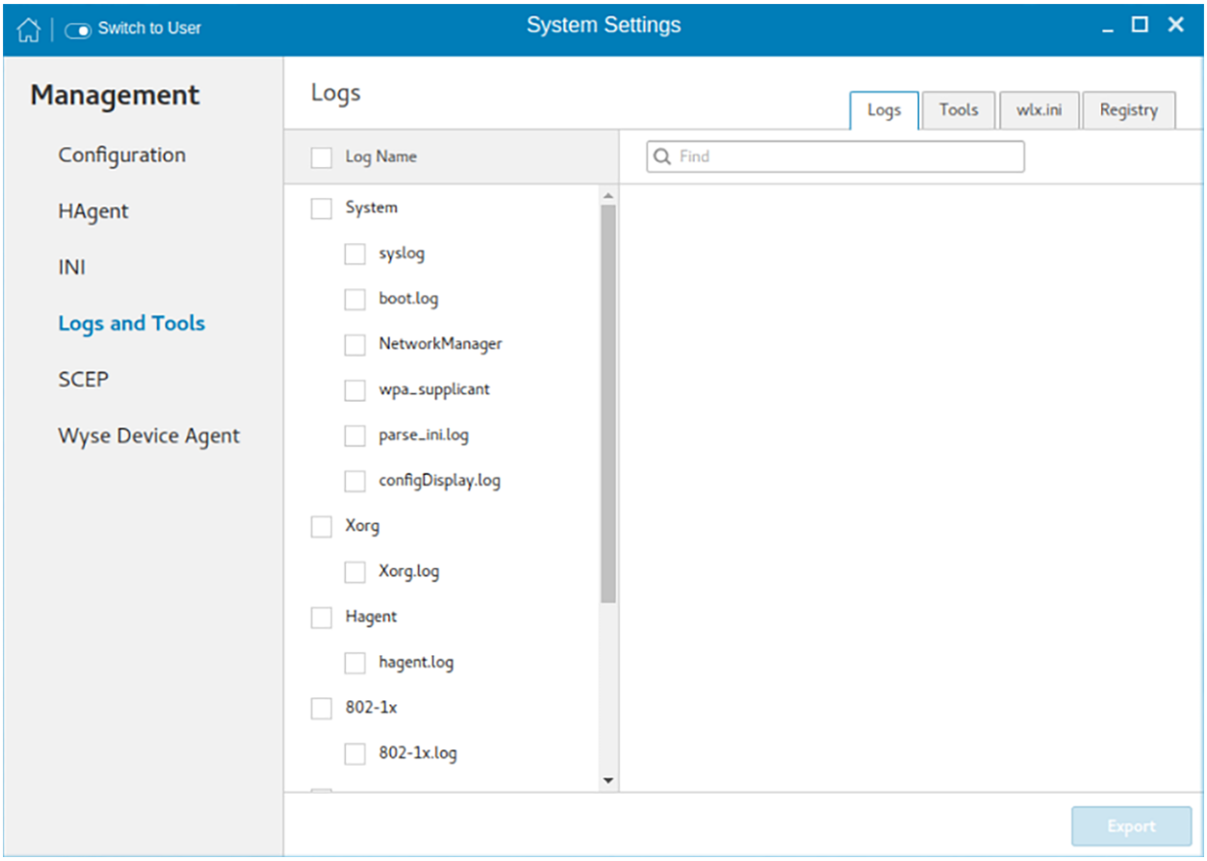


Figure 74. Logs

You can choose one of the following options to export logs:

- If you select the Remote server option, do the following:
  1. Enter remote file server URL in **Export server URL** input box.

2 Enter your credentials if **Use anonymous** switch button is not enabled.

- If you select the USB Drive option, do the following:
  1 Click the Browse tab. The File browser dialog box is displayed. Select a directory from listed USB drive.
  2 Click **Export** to export the logs.

Table 20. Logs

Log name	Description
syslog	Contains a record of events of the ThinLinux operating system. Some of the events include system errors, warnings, system changes, and so on.
boot.log	Contains a record of events related to system boot.
NetworkManager	Contains a record of events related to network settings.
wpa_supplicant	Contains a record of events related to network authentication.
parse_ini.log	Contains a record of events related to parsing an INI file.
configDisplay.log	Contains a record of events related to display configurations.
Xorg.log	Contains a record of events related to the Xorg server.
hagent.log	Contains a record of events related to HAgent for Wyse Device Manager (WDM).
802-1x.log	Contains a record of events related to 802-1.x authentication.
SCEP-client.txt	Contains a record of events related to Simple Certificate Enrollment Protocol.
wda.log	Contains a record of events related to Wyse Device Agent (WDA).
cached_update.log	Contains a record of events related to Merlin imaging using file server.

3 Click the **Tools** tab to configure the following:

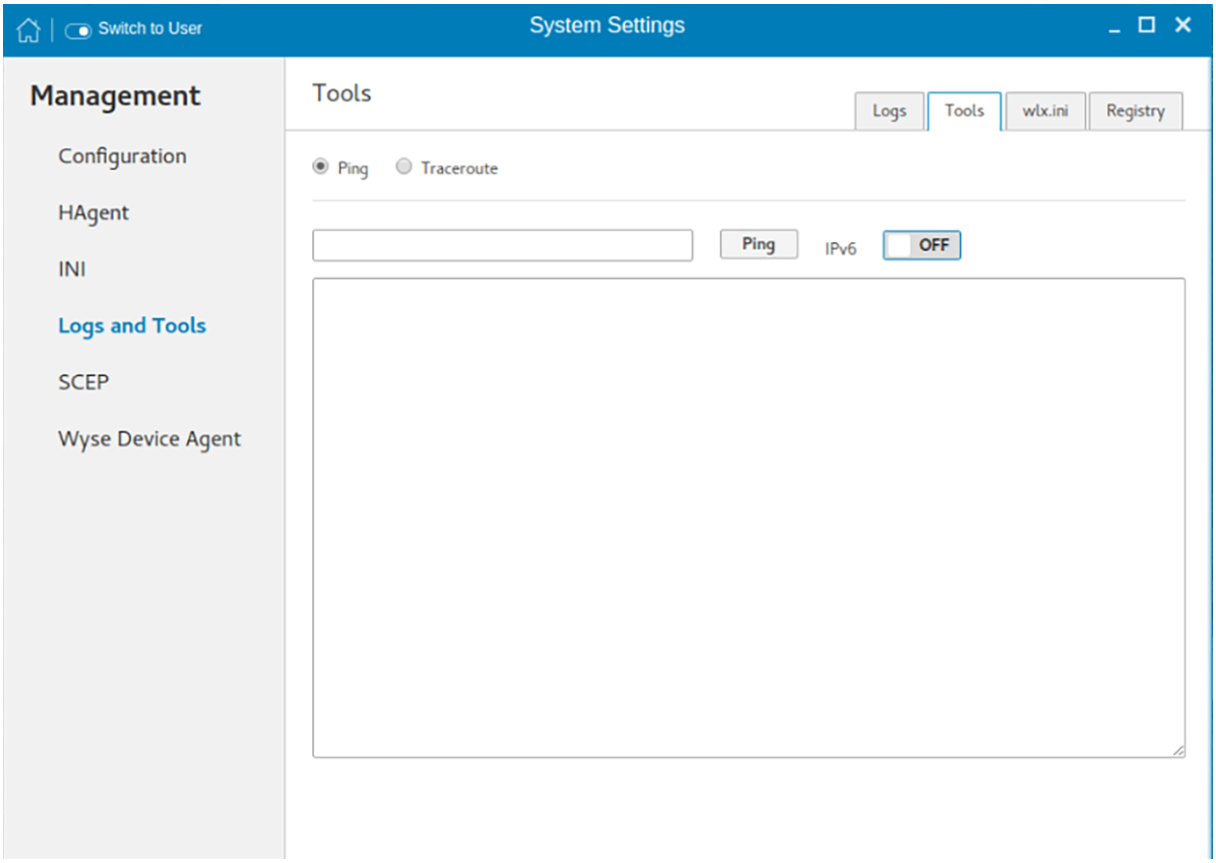


Figure 75. Tools

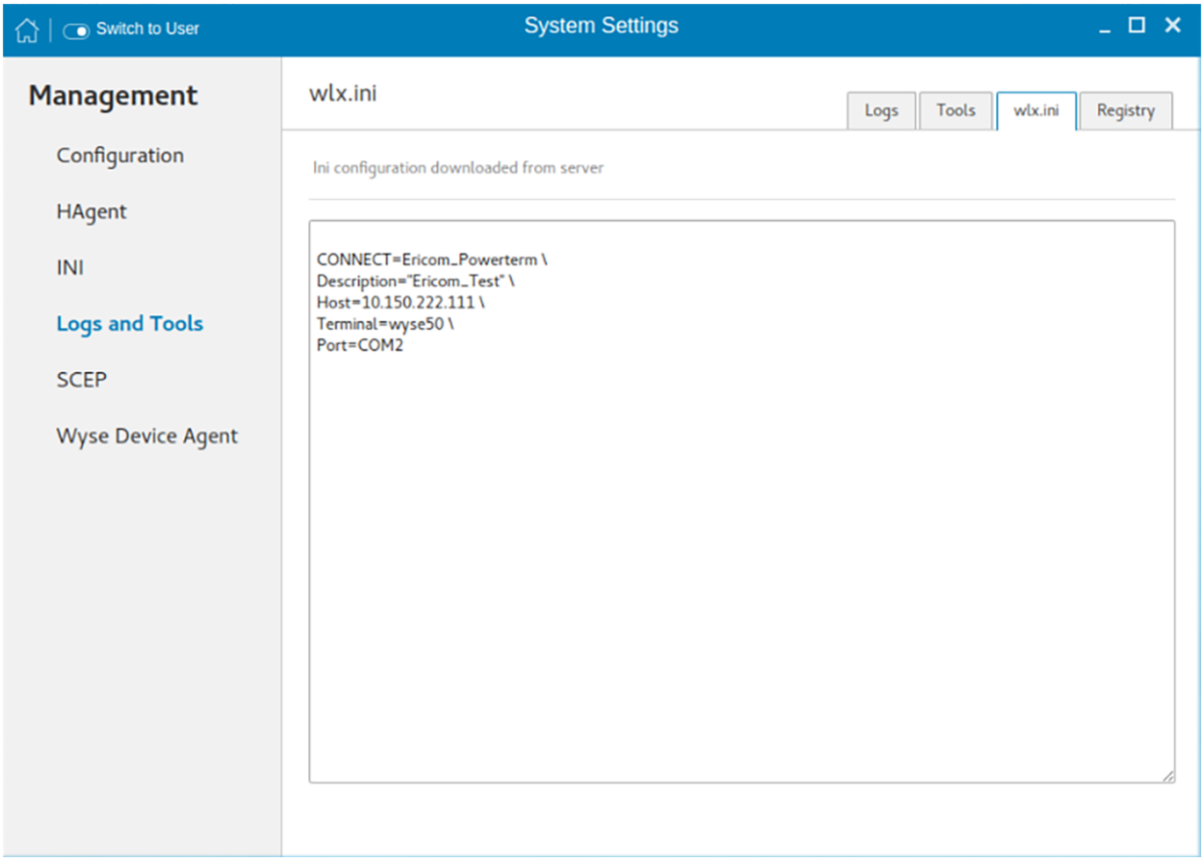
a Enter or select a destination from the drop-down list and click **Ping**.

b Enter or select a destination from the drop down list and click **Traceroute**.

The output of ping or traceroute appears in the text area.

c Click the **ON/OFF** button to enable or disable ping or traceroute for an IPv6 address.

4 Click the **Wlx.ini** tab to view the contents of wlx.ini file downloaded from INI server:



```
CONNECT=Ericom_Powerterm \
Description="Ericom_Test" \
Host=10.150.222.111 \
Terminal=wyse50 \
Port=COM2
```

Figure 76. wlx.ini

5 Click the **Registry** tab to view contents of device registry. You can navigate through different types of registry by choosing appropriate ones from the **Registry** drop-down list.

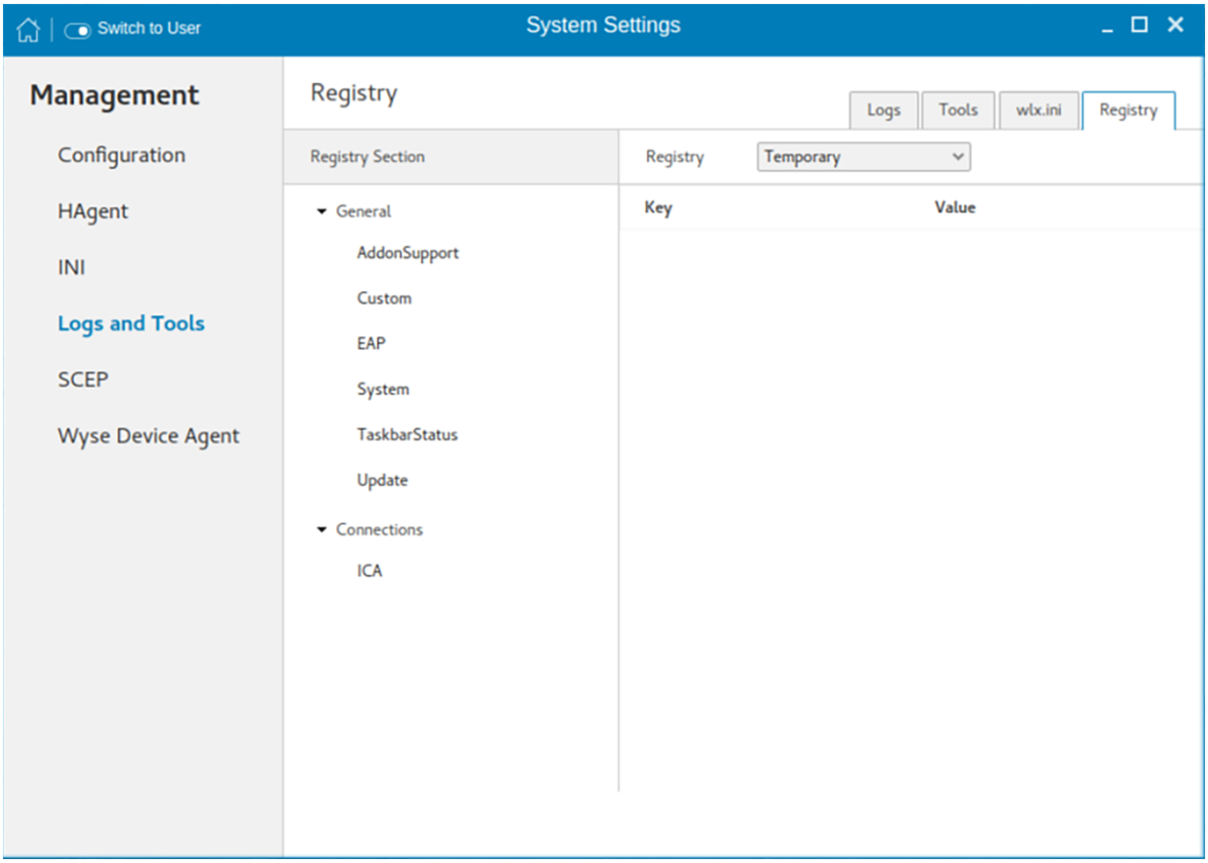


Figure 77. Registry

The available options are:

- **Temporary**—To view contents of temporary registry
- **Save**—To view contents of save registry
- **Permanent**—To view contents of permanent registry

Select the **Registry** option from the drop-down list and the contents of the device registry selected by you are displayed.

SCEP configuration management

The Simple Certificate Enrollment Protocol (SCEP) is a protocol that allows you to securely issue certificates to network devices in a scalable manner. Within an enterprise domain, it enables network devices that do not run with domain credentials to enroll for certificates from a Certification Authority (CA).

1 Click the **+** button to add a new certificate.

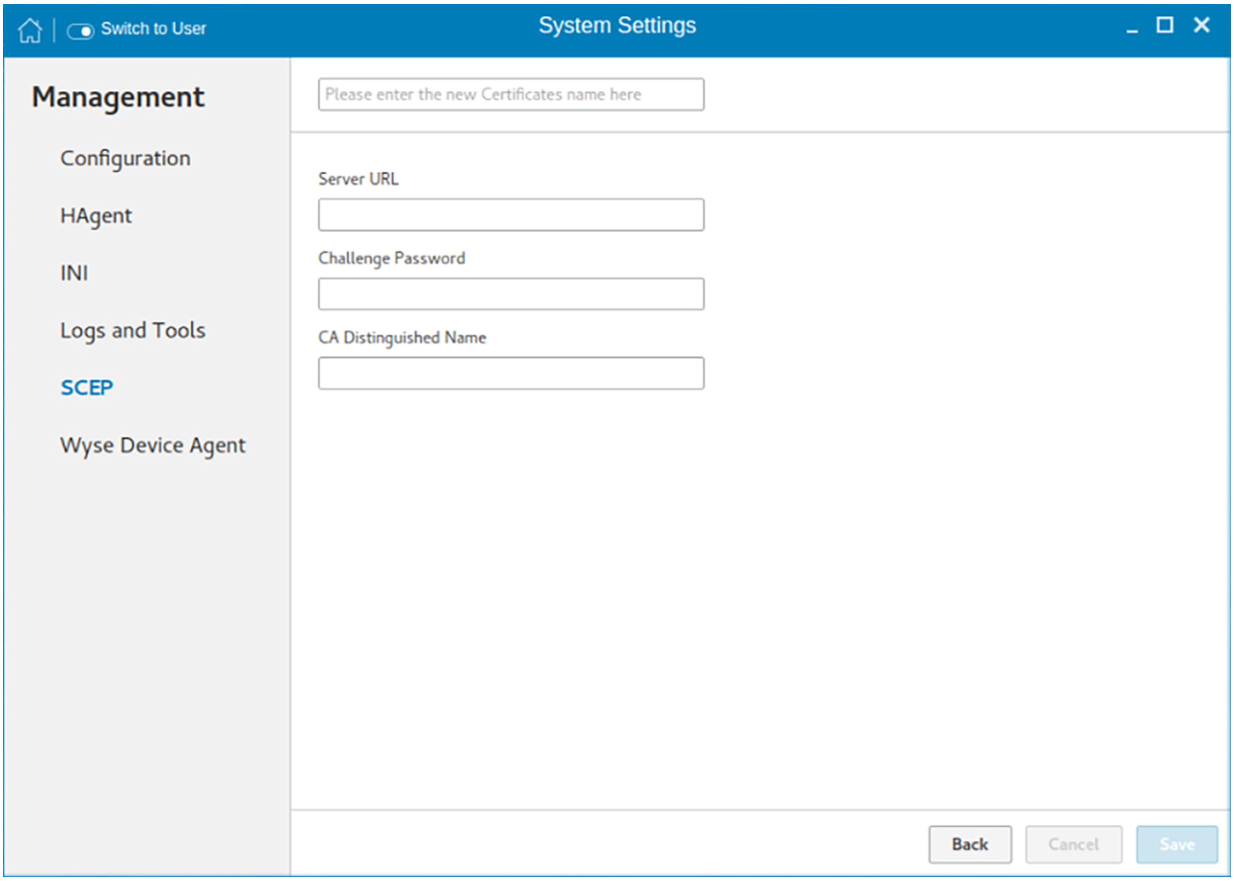


Figure 78. SCEP configuration

2 Enter the **Certificate name**, **Server URL**, **Challenge password**, and **CA Distinguished name**.

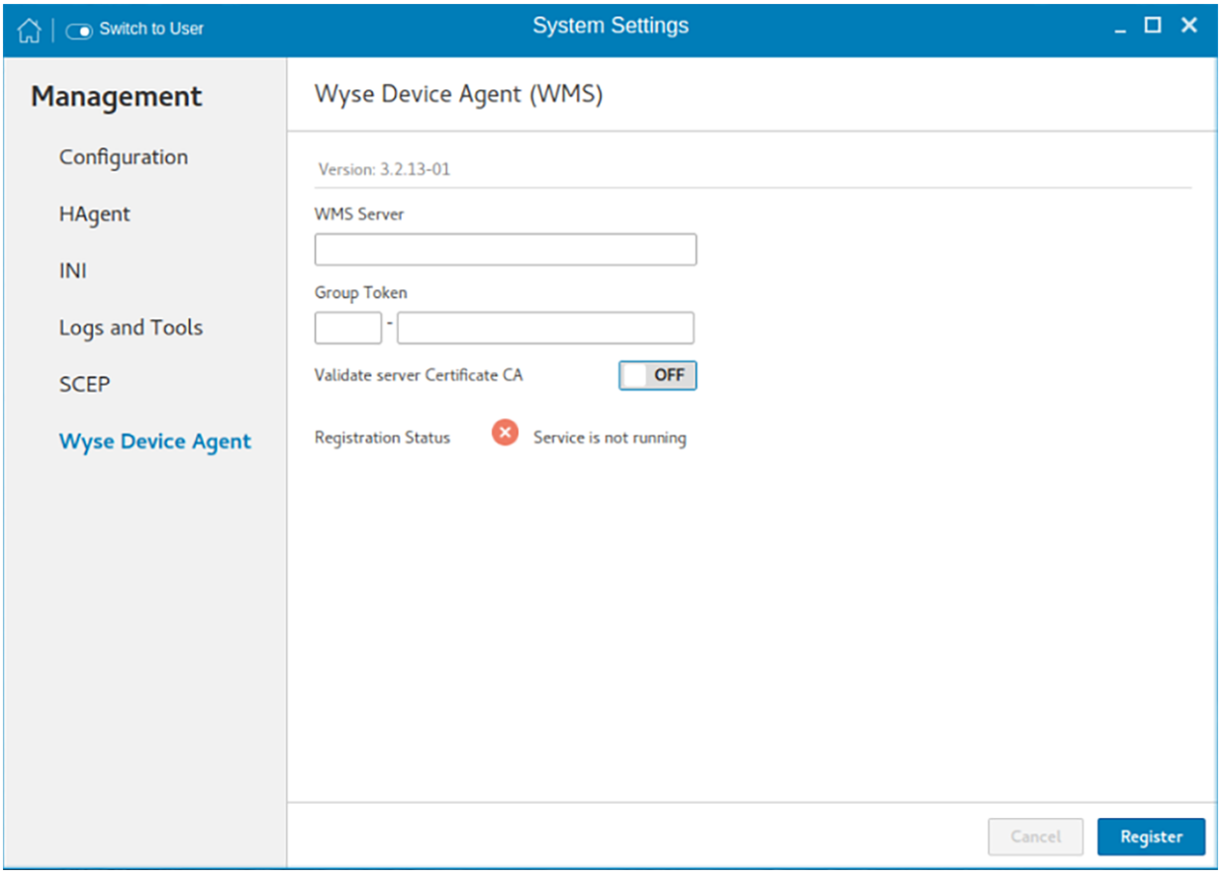
> NOTE: **The server URL can be either an http or https link.**

3 Click **Save** to save the changes.

4 Select the certificate and click **Enroll**.

Wyse Device Agent

Wyse Device Agent (WDA) on the ThinLinux device supports only the features of Wyse Management Suite. Wyse Device Agent is for configuring the client settings and registering a ThinLinux device into Wyse Management Suite. This is available only for admin user.
If the device is not registered to a Wyse Management Suite server, the **Wyse Device Agent** screen shows the registration status as **Not Registered**.



Version: 3.2.13-01

Validate server Certificate CA OFF

Registration Status ✕ Service is not running

Figure 79. Wyse Device Agent

1. In the **WMS Server** input box, enter the URL of Wyse Management Suite server.
2. In the **Group Token** input boxes, enter your group registration key to manage your ThinLinux device. This is a unique key for registering your thin client device. Thin clients can be directly registered to Groups directly and must have a Group Registration Key enabled to perform this action.
3. Click the **ON/OFF** button to enable or disable the Validate server certificate option. Enable this option to perform server certificate validation for all device-to-server communication.
4. Do one of the following options:
   - Click **Register** to register your thin client on the Wyse Management Suite server. When your thin client is successfully registered, the status is shown as **Registered** with green color icon next to the **Registration Status** label. The caption of the **Register** button changes to **Unregister**.
   - Click **Unregister**, if you want to remove your thin client from the Wyse Management Suite. If Unregister fails, a dialog box for the **Force Unregister confirmation** is displayed. Click **Yes** to forcefully unregister your device which is managed by Wyse Management Suite. When you perform Register or Unregister or Force Unregister from the Agent screen, the applet should not be closed until Registration Status. After successful registration, you can access the Wyse Management Suite console where you can view and manage Device Asset Details, Real-Time commands, and the Troubleshooting information of your registered thin client.

Directing the thin client to Wyse Management Suite server:

To direct your thin client to the Wyse Management Suite server, you must provide the Wyse Management Suite/MQTT server details and the Group registration key. These details are discovered by Wyse Device Agent using any of the following ways:

- **Using DNS SRV record**—You can register devices with the Wyse Management Suite server if DNS SRV record fields are set with valid values. For more information about registering devices by using DNS SRV record, see the Wyse Management Suite Administrator's Guide.
- **Using DHCP scope options**—You can obtain the Wyse Management Suite/MQTT server details and Group Registration Key by querying the DHCP server with following option tags:
  - 199 – Scope option for Group Token (type = String, value = Wyse Management Suite-group-key).

  - 165 – Scope option for the Wyse Management Suite server.
  - 166 – Scope option for MQTT server—Optional.
  - 167 – Scope option for CA Validation—Optional.
- **Using INI parameter**—You can use the following INI parameters to direct the thin client to the Wyse Management Suite server:

  ```
  CCMEnable={yes,no} CCMServer=<Wyse Management Suite Server URL>
  GroupRegistrationKey=<tenant code-group code>
  ```

  > **NOTE: When INI discovery method is used for registering the device, if you want to unregister the device, you must delete the INI parameters and restart the device first and then unregister the device. Else you have to perform the unregister process twice. For more information, see Dell Wyse ThinLinux INI Reference Guide.**

- **Using the Wyse Device Agent screen**—You can use the Wyse Device Agent screen to register devices with the Wyse Management Suite server. To configure the Wyse Device Agent, follow the steps 1–4 in this section.

7

Viewing XTerm

XTerm is the standard terminal emulator for the Xterm Window System. Use the terminal emulator window for X to access a text terminal and all its applications such as command line interface (CLI) and text user interface applications.

ⓘ | **NOTE: By default, XTerm is available only in Admin mode.**

To use the Xterm option:

1. On the **Application overview** screen, click Xterm.

   The terminal emulator window is displayed.
2. Type help and press Enter to display a verbose message describing XTerm options.

8

Imaging solutions

ThinLinux Imaging is supported through Dell Wyse Management Suite and Dell Wyse USB Imaging Tool. For more information about the Merlin image installation using Dell Wyse USB Imaging Tool, see the latest *Dell Wyse USB Imaging Tool User's Guide* at www.downloads.dell.com/wyse.

Topics:

Merlin Imaging from file server

To create and use merlin.rsp and imaging files to perform Merlin imaging on device from File Server, complete the following task:

1. Extract and copy Merlin image rsp and contents on any File Server location, for example, `2.1.x_5070_merlin.rsp` and `commandsXml.xml, efi, mbr, recovery`.
2. Rename the RSP file which is available in Merlin Image folder, for example, from `2.1.x_5070_merlin.rsp` to `merlin.rsp`.
3. Copy `merlin.rsp` and other imaging files to the $PLATFORM sub-directory on the FTP location. Place the image at the correct `<PLATFORM>` subfolder. This is because the Merlin imaging is platform dependent.
4. Provide this path as value for `MerlinUpdate.URL` parameter in INI file, and if needed provide credentials for FTP server using `MerlinUpdate.Username` and `MerlinUpdate.Password` parameters and restart the thin client. For example, if the device model is Wyse 5070 thin client, copy the image and rsp file under ftp://<IP>/<directory>/5070/ folder, but mention URL as ftp://<IP>/<directory>/. The Macro $PLATFORM is automatically appended.

   ⓘ **NOTE: Merlin imaging through File Server works only when you provide URL using INI parameters; if you provide the same values on the Update Settings page, the imaging does not work.**

   After restart, Merlin image is downloaded through Delayed Update. A notification is displayed after Merlin image ready. The Merlin imaging takes place after restart. Merlin image is not downloaded, if Delayed Update is disabled.

Limitations

- If the image version on thin client and Merlin image version on FTP server are the same, then imaging does not take place.
- Downgrading is always allowed for Merlin image. There is no force imaging for Merlin.
- Changes are not preserved after Merlin imaging.

Upgrade ThinLinux 2.0 to 2.1 on Wyse 3040 thin client

Use Wyse Management Suite version 1.2 or later to upgrade the ThinLinux build version 2.0.19 to 2.1.

To upgrade ThinLinux by using Wyse Management Suite for Wyse 3040 thin client:

1. Go to www.dell.com/support.
2. Click **Product Support**, enter the **Service Tag** of your thin client, and then press Enter.

   ⓘ **NOTE: If you do not have Service Tag, manually browse for your thin client model.**

3. Click **Drivers and downloads**.
4. From the **Operating system** drop-down list, select **ThinLinux**.
5. Scroll down the page, and do the following:
   - Download the wda3040_3.0.10-01_amd64.deb, wda_3.2.13-01_amd64.tar, and merlin-nonpxe_3.7.7-00.05_amd64.deb add-ons.
   - Download the latest ThinLinux version 2.1 image file (2.1.0.00_3040_merlin_16GB.exe).
6. On the thin client, go to **Settings** > **Management** > **Wyse Device Agent**.
7. Register the device to the Wyse Management Suite server.
8. Log in to the Wyse Management Suite console.
9. Create and deploy app policy for wda3040_3.0.10-01_amd64.deb, wda_3.2.13-01_amd64.tar, and merlin-nonpxe_3.7.7-00.05_amd64.deb add-ons.
10. Reboot the thin client.
11. Log in to the Wyse Management Suite server.
12. Copy the downloaded image (2.1.0.00_3040_merlin_16GB.exe file) to <drive C>/wms/localrepo/repository/osimages/zipped/.
13. Log in to the Wyse Management Suite console.
14. Go to **Apps & Data** > **OS Image repository** > **WES/ThinLinux** and verify that the ThinLinux image is available.
15. Go to **Apps & Data** > **OS Image policies (WES/ThinLinux)** and click **Add Policy**.
16. Update the required fields, and click **Save**.
17. Schedule the job.
18. Click **Update now** on the client to update the image.

Upgrade ThinLinux 2.0 to 2.1 on Wyse 5070 thin client

Use Wyse Management Suite version 1.2 or later to upgrade the ThinLinux build version 2.0.27 to 2.1

To upgrade ThinLinux by using Wyse Management Suite for Wyse 5070 thin client:

1. Go to www.dell.com/support.
2. Click **Product Support**, enter the **Service Tag** of your thin client, and then press Enter.

   ⓘ **NOTE: If you do not have Service Tag, manually browse for your thin client model.**
3. Click **Drivers and downloads**.
4. From the **Operating system** drop-down list, select **ThinLinux**.
5. Scroll down the page, and download the latest ThinLinux version 2.1 image file (2.1.0.00_5070_merlin_16GB.exe).
6. On the thin client, go to **Settings** > **Management** > **Wyse Device Agent**.
7. Register the device to the Wyse Management Suite server.
8. Log in to the Wyse Management Suite server.
9. Copy the downloaded image (2.1.0.00_5070_merlin_16GB.exe file) to <drive C>/wms/localrepo/repository/osimages/zipped/.
10. Log in to the Wyse Management Suite console.
11. Go to **Apps & Data** > **OS Image repository** > **WES/ThinLinux** and verify that the ThinLinux image is available.
12. Go to **Apps & Data** > **OS Image policies (WES/ThinLinux)** and click **Add Policy**.
13. Update the required fields, and click **Save**.
14. Schedule the job.
15. Click **Update now** on the client to update the image.

Upgrade ThinLinux 1.0.4 to 2.1 on Wyse 3040 thin client

Use Wyse Management Suite version 1.2 or later to upgrade the ThinLinux build version 1.0.4 to 2.1

To upgrade ThinLinux by using Wyse Management Suite:

1 Go to www.dell.com/support.
2 Click **Product Support**, enter the **Service Tag** of your thin client, and then press Enter.

 NOTE: If you do not have Service Tag, manually browse for your thin client model.

3 Click **Drivers and downloads**.
4 From the **Operating system** drop-down list, select **ThinLinux**.
5 Scroll down the page, and do the following:
   - Download the Platform_util-1.0.26-0.3.x86_64.rpm, wda-2.1.23-00.01.x86_64.rpm, and merlin_nonpxe-3.7.7-00.05.x86_64.rpm add-ons.
   - Download the latest ThinLinux version 2.1 image file (2.1.0.00_3040_merlin_16GB.exe).
6 On the thin client, go to **Settings** > **Management** > **Wyse Device Agent**.
7 Register the device to the Wyse Management Suite server.
8 Log in to the Wyse Management Suite console.
9 Create and deploy app policy for Platform_util-1.0.26-0.3.x86_64.rpm, wda-2.1.23-00.01.x86_64.rpm, and merlin_nonpxe-3.7.7-00.05.x86_64.rpm.
10 Reboot the thin client.
11 Log in to the Wyse Management Suite server.
12 Copy the downloaded image (2.1.0.00_3040_merlin_16GB.exe file) to <drive C>/wms/localrepo/repository/osimages/zipped/.
13 Log in to the Wyse Management Suite console.
14 Go to **Apps & Data** > **OS Image repository** > **WES/ThinLinux** and verify that the ThinLinux image is available.
15 Go to **Apps & Data** > **OS Image policies (WES/ThinLinux)** and click **Add Policy**.
16 Update the required fields, and click **Save**.
17 Schedule the job.
18 Click **Update now** on the client to update the image.

Upgrade ThinLinux 1.0.4 to 2.1 on Wyse 3040 thin client

Use Wyse Management Suite version 1.2 or later to upgrade the ThinLinux build version 1.0.4 to 2.1

To upgrade ThinLinux by using Wyse Management Suite:

1 Go to www.dell.com/support.
2 Click **Product Support**, enter the **Service Tag** of your thin client, and then press Enter.

 NOTE: If you do not have Service Tag, manually browse for your thin client model.

3 Click **Drivers and downloads**.
4 From the **Operating system** drop-down list, select **ThinLinux**.
5 Scroll down the page, and do the following:
   - Download the Platform_util-1.0.26-0.3.x86_64.rpm, wda-2.1.23-00.01.x86_64.rpm, and merlin_nonpxe-3.7.7-00.05.x86_64.rpm add-ons.
   - Download the latest ThinLinux version 2.1 image file (2.1.0.00_3040_merlin_16GB.exe).
6 On the thin client, go to **Settings** > **Management** > **Wyse Device Agent**.
7 Register the device to the Wyse Management Suite server.
8 Log in to the Wyse Management Suite console.
9 Create and deploy app policy for Platform_util-1.0.26-0.3.x86_64.rpm, wda-2.1.23-00.01.x86_64.rpm, and merlin_nonpxe-3.7.7-00.05.x86_64.rpm.
10 Reboot the thin client.
11 Log in to the Wyse Management Suite server.
12 Copy the downloaded image (2.1.0.00_3040_merlin_16GB.exe file) to <drive C>/wms/localrepo/repository/osimages/zipped/.

13 Log in to the Wyse Management Suite console.

14 Go to **Apps & Data** > **OS Image repository** > **WES/ThinLinux** and verify that the ThinLinux image is available.

15 Go to **Apps & Data** > **OS Image policies (WES/ThinLinux)** and click **Add Policy**.

16 Update the required fields, and click **Save**.

17 Schedule the job.

18 Click **Update now** on the client to update the image.

Password encoding

By default, base-64 encoding is enabled for all passwords when you use INI parameters. If you want to use AES encoding, then generate an AES encoding password by using the WyseINIkeyCrypt.exe tool.

ThinLinux supports the following two password encoding methods for all the passwords in **Connections and Global** settings that are used in the INI parameters:

- Base64 password encoding, see Base64 passcode encoding.
- AES password encoding, see AES password encoding.

Copy the generated encoded password and place it in the INI file where the password field is mapped.

ⓘ | NOTE: **Non-English characters are not supported for AES password encoding.**

Topics:

Base64 passwords encoding

By default, all passwords in the INI file are base-64 encoded. To generate a base-64 encoded password, do the following:

1. Log in to the thin client.
2. Open **xterm**. This is a standard terminal emulator for the X Window System.
3. Enter `regencode` followed by a password in plain text.

   For example, to encode the string **password**, enter `$ regencode password`. The encoded output is `cGFzc3dvcmQ=`.

   You can also use the **WyseINIKeyCrypt** tool to generate encoded passwords.

AES password encoding

All passwords that are related to connections and users in the INI file can be AES encoded. For AES encoding support, add `PasswordEncryptionCode=2` parameter in the INI file.

To generate AES encoded password, do the following:

1. Log in to the thin client.
2. Copy the WyseINIKeyCrypt.exe on any Windows machine.
3. Double-click the .exe file.
   The **Dell Wyse Password Encoder** window is displayed.
4. Enter the plain text password in the **Password to encode** edit box.
5. Click **Encrypt** to generate the AES encoded password.

A

Central configuration—Automating updates and configurations

This appendix describes how to set up your environment to provide your thin clients running Dell Wyse ThinLinux with automatic updates and configurations.

ⓘ **NOTE: Dell thin clients do not require device management software. They are configured to obtain their IP address, as well as the location of firmware and configuration instructions, from a DHCP server. However, you can use WDM or the Dell Wyse USB Firmware Tool for a more hands-on management of client configurations and updates.**

Topics:

How INI files are deployed

INI files that are created and maintained by the network administrator, determine how the thin client is configured and updated. The thin client accesses INI files from the server during the initialization process. Typically, INI files are accessed through FTP, HTTP, and HTTPS; if no protocol is specified, the default is anonymous FTP.

ⓘ **IMPORTANT: The INI file processing hierarchy is as follows:**

- **Scenario 1** — MAC.ini exists. The MAC.ini file is processed and if the Include=WLX.ini statement is included, then the WLX.ini file is processed.
- **Scenario 2** — WLX.ini exists. The WLX.ini file is processed.
- **Scenario 3** — No ini files exist. Local configuration is applied.

INI files are employed as follows:

- **wlx.ini** — This is the global INI file. One wlx.ini file is available to all users. It contains global parameters for all thin clients accessing the server. If the operating system cannot find wlx.ini, it defaults to wnos.ini.
- **MAC.ini** — This file can be used for device-specific configuration. If the thin client locates this INI file that is stored in the same directory as wlx.ini, wlx.ini is not accessed, unless you use the include=wlx.ini parameter.

ⓘ **NOTE:**

The placement of the include=wlx.ini parameter within the MAC.ini file dictates which value takes priority for a same specific parameter that is contained in both the wlx.ini file and the MAC.ini file but is defined differently that is different values for the same parameter.

For example, if the wlx.ini file has parameterA=valueB, and the MAC.ini file has the same parameterA=valueC, then:

- If the include=wlx.ini parameter is included in the MAC.ini file before the parameterA=valueC statement, then the wlx.ini parameterA=valueB is discarded and parameterA=valueC from the MAC.ini file is the final value used.
- If the include=wlx.ini parameter is included in the MAC.ini file after the parameterA=valueC statement, then the MAC.ini parameterA=valueC is discarded and parameterA=valueB from the wlx.ini file is the final value used.

When a thin client is initialized, it accesses the global wlx.ini file. For detailed information on constructing and using INI files, see *Dell Wyse ThinLinux INI Reference Guide*.

ⓘ **NOTE:**
If both PNAgent and a user profile are being used, the username must be defined in the Windows domain that is used. Also the password must be the same for the domain and the profile.

Setting up the automatic configurations and updates

For a Dell thin client running Dell Wyse ThinLinux to successfully access INI files and update itself from a server, you must set up the server with the correct folder structure where the INI files and other update files are located, direct the thin client to the server, and then reboot or start the thin client.

After DHCP and servers are configured and available, the thin client checks at each restart to see whether or not any add-ons or INI parameters are available on a predefined server.

ⓘ **NOTE: DCHP Option #161 specifies the server URL, DCHP Option #162 specifies the root path to the server.**

This involves two tasks:

1. Preparing the Root Directory and Folder Structure on the Server
2. Directing the Thin Client to the Server

Preparing the root directory and folder structure on the server

To prepare the root directory and folder structure on the server:

1. Set up the following folder structure on your server under the C:/inetpub/ftproot folder for FTP or C:/inetpub/wwwroot folder for HTTP or HTTPS and place your INI files and other necessary files inside the structure as noted.
2. This list describes the folder structure, starting with the root directory.

Table 21. Root directory

Parameter	Description
/wyse/	The root directory. It stores the wlx2 folder and the add-ons folder.
/wyse/wlx2	The main INI configuration folder. It stores the following: • wlx.ini file or MAC.ini file • bitmap folder • certs folder • ini folder
/wyse/wlx2/bitmap	The folder where you can place custom images you plan to use.
/wyse/wlx2/certs	The folder where you can place the CA certificates that can be imported to a thin client. ⓘ **NOTE: To import the certificates to the thin clients, use the Certs and ImportCerts INI parameters.**
/wyse/addons	The folder where you can place the add-ons you want to use. It also stores the directory file and the .deb packages available to be installed on the thin client. The directory file should list all available add-ons. The directory file is required in the add-ons folder to guarantee that add-ons are properly located.

Be sure to create/activate the two required MIME Types— **.ini** and **.**,under IIS on a per site basis to enable downloading. Also be sure your Web server can identify the file types used by Dell thin clients.

3 On your IIS server, use the **File Types** menu to add a New Type.

4 In the **File Type** dialog box, Use the following details :

   a **To create/activate the .ini MIME Type**—Enter the Associated extension **.ini** and Content type (MIME) **text/plain**.

   b Click **OK** to apply the settings.

   c **To create/activate the . MIME Type**—Enter the Associated extension **.** and Content type (MIME) **text/plain**.

   d Click **OK** to apply the settings.

Directing the thin client to the server

After you set up the folder structure and populate it with the correct files, Dell recommends that you use DHCP to direct the thin client to the location of the server.

To direct the thin client to the server:

Using DHCP—When using DHCP to direct the thin client to the location of the server, information about the server and root directory is obtained from the following DHCP options:

a **161**—The server.

b **162**—Root path to the server-ftp/http/https.

- If no root path is defined, /wyse is assumed
- If a root path is defined, the additional path will be appended to the URL supplied by option 161.

c **184**—Server username to the server specified in option 161. This is optional.

d **185**—Server password to the server specified in option 161. This is optional.

> ⓘ **IMPORTANT:**
>
> Check-in for firmware updates is done early in the boot process. For that reason, changes in DHCP information may not be propagated to a unit until a full boot is completed. However, you can avoid this by forcing a renewing of the DHCP lease, which makes sure that the unit has the latest file-server location before the next firmware check.
>
> Simply, right-click the **Network Manager** icon, click **Enable Networking** to disable it, right-click the **Wireless Manager** icon, and then click Enable **Networking** to enable it again and the DHCP lease is renewed.

After you start your thin client, the device will look in the defined root path for the latest available image and update if necessary. Additionally, it will check the directory file in the add-ons folder to see if any updates for installed add-ons are defined. Add-ons that exist in the addons folder but are not listed in the directory file, will be ignored during update check-in.

DHCP options tags

Use the guidelines shown in the Table when creating and adding the DHCP options.

Table 22. DHCP options tags

Option	Description	Notes
1	Client identifier	Always sent.
2	Time Offset	Optional.
3	Router	Optional but recommended. It is not required unless the thin client must interact with servers on a different subnet.
6	Domain Name Server (DNS)	Optional but recommended.
12	Host Name/Terminal Name	Optional string. The host name or terminal name to be set.
15	Domain Name	Optional but recommended. See Option 6.
28	Broadcast Address	Optional.
44	WINS servers IP Address	Optional.
51	Lease Time	Optional but recommended.
52	Option Overload	Optional.
53	DHCP Message Type	Recommended.
54	DHCP Server IP Address	Recommended.
55	Parameter Request List	Sent by appliance.
57	Maximum DHCP Message Size	Optional — always sent by thin client.
58	T1 (renew) Time	Optional but recommended.
59	T2 (rebind) Time	Optional but recommended.
61	Client identifier	Always sent.
161	Server (ftp/http/https)	Optional string. If this is an IP address or resolvable host name, the protocol is assumed to be FTP; however, it may be the leading portion of a URL that specifies another protocol. If using the URL form, it should not include a trailing slash, for example, http://server.example.com or ftp://192.168.0.1.
162	Root path to the server (ftp/ http/https)	Optional string. The relative directory starting from the root directory must be given. For example, on an FTP server, the full directory may be **C:/Inetpub/ftproot/wyse**, where wyse is the directory that contains the firmware. In this example, the

Option	Description	Notes
		correct string value for this DHCP option is **/wyse.** On a Linux server, an FTP user-based directory might be **/home/test/wyse**. In this example, if the FTP user is test, then the FTP root path is **/wyse**and not the full path (/home/test/wyse). This value should use URL path notation. **NOTE: URL path notation-Start with a forward slash, /, and use a forward slash as folder separators.**
165	Wyse Management Suite server	Recommended.
166	MQTT server	Optional string.
167	CA Validation	Optional string.
181	Citrix Server FQDN/IP	Optional string. IP address or FQDN of the Citrix Server which will be used by Citrix PAM Login and Desktop Appliance Mode.
182	Wyse Admin List	Optional string. DHCP equivalent of the DomainList ini file parameter.
184	Server Username	Optional string. Username to use when authenticating to the server specified in Option.
185	Server Password	Optional string. Password to use when authenticating to the server specified in Option.
186	WDM IP Address	Optional binary IP address of the WDM server. This option can specify up to one WDM server.
191	XenDesktop DDC URL	Optional string. For more information.
194	WDM FQDN	Optional FQDN of the WDM server. This option can specify up to one WDM server.
199	Wyse Management Suite Group Token	Recommended.
203	Type of VDI theme	Type of VDI theme used by Desktop Appliance mode. The possible values are Citrix/none. None will disable Desktop Appliance mode.
204	Type of Citrix server	pnagent/storefront
205	Citrix server storename	Optional, storename configured on Citrix server. Applicable only for Citrix storefront server.

C

Data recovery imaging

Use the operating system reinstall option to restore the system to its original factory settings. During the process, the device uses the hard drive partition for data recovery imaging.

To perform data recovery imaging:

1. Restart the thin client.

   The thin client boots up and Dell logo is displayed for a short time.
2. During this period, keep pressing the Esc key.

   The GRUB menu is displayed.
3. Select **Reinstall operating system** and press Enter.
4. Enter the username as `root`, and the root password to start the recovery imaging process.