Dell Hybrid Client version 2310

Administrator's Guide

October 2023
Rev. A00

DELL Technologies

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.

© 2023 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Chapter 1: Introduction 9
Supported platforms 9
Supported management software 9
Supported operating system 10
Salient features of Dell Hybrid Client 10
Other documents you may need 10

Chapter 2: Dell Hybrid Client installation 11
Dell Hybrid Client Bundle Upgrade 11
Dell Hybrid Client Upgrade from version 1.x to 2310 11
Transfer Configurations from Dell Hybrid Client 1.x to 2.x 16
Verify Bundle Upgrade Status 23
ISO Upgrade using Wyse Management Suite 24
Steps to Install Dell Hybrid Client ISO Upgrade 24
Verify ISO Upgrade Status 28
BIOS Upgrade 29
Upgrade BIOS using Wyse Management Suite 29
Upgrade BIOS Manually from BIOS Setup 32

Chapter 3: Registering Dell Hybrid Client to Wyse Management Suite 38
End User License Agreement and First Boot setup Wizard 38
Displays for the following scenarios 38
End User License Agreement 38
Dell Hybrid Client Setup Wizard 39
Configuring Ethernet and Wyse Management Suite registration 41
Configuring Wi-Fi and WMS Registration 44
Do not have Network Connection 48
Register Dell Hybrid Client if Skipped Registration in Setup wizard 49
Registering Dell Hybrid Client by using DHCP option tags 50
Registering Dell Hybrid Client by using DNS SRV record 50
Enrollment Validation 50

Chapter 4: Getting started with Dell Hybrid Client 51
Desktop overview 51
Configure the date and time using Wyse Management Suite 52
Configure the date and time using Device Settings 53
Using the top bar 53
Using the taskbar 54
Applications overview screen 54
Log Out, Suspend, Restart, or Power Off 55
Lock your desktop 55

Chapter 5: Policy settings overview 56
Managing the Dell Hybrid Client policy settings from Wyse Management Suite 56

Viewing system information... 58
Configure the GDM Login Screen power control settings...59
Account Privileges... 59
Configure Account Privilege...59
Customize Account Privileges...60
Single application mode... 60
Configure the custom connection settings...62
Set custom values for registry location...63
Multilanguage support...63
Download and install language add-ons on Dell Hybrid Client...64
Configure the language settings using Wyse Management Suite... 64

Chapter 6: Configuring the VDI environment... 66
Single Sign-On (SSO) to VDI applications... 66
Multifactor authentication for VDI applications...67
Global Session Settings...67
Configure Global Session Settings... 67
Configuring Citrix... 68
Citrix Installation...69
Configure Citrix Broker Connection using Wyse Management Suite...69
Configure Citrix Session Settings...72
Connect to a Citrix session... 74
Desktop Restart for Citrix Session...75
Citrix Configuration Editor... 75
Configuring Anyware... 79
Anyware Installation...79
Configuring Anyware Broker Connection using Wyse Management Suite...79
Configuring Anyware Session Settings from Wyse Management Suite... 84
Configuring Azure Virtual Desktop...89
Configure the Azure Virtual Desktop broker settings... 89
Manage Azure Virtual Desktop connections locally... 90
Connect to an Azure Virtual Desktop session...90
Azure Virtual Desktop limitations... 91
Configuring VMware... 91
VMware Installation... 92
Configure VMware Broker Connection from Wyse Management Suite... 92
Configure VMware Session Settings...95
Connect to a VMware session... 97
VMware connection with DHCP Option Tag...97
Configuring RDP...99
RDP Installation...99
Configuring RDP Broker Settings from Wyse Management Suite ...99
Configuring RDP Session Settings from Wyse Management Suite ... 102
Connect to an RDP session...105
Connect to an RDP session using TS Gateway with WebSocket...105
Configuring Imprivata... 106
Configure the Imprivata as Connection mode ...106
Connect to an Imprivata PIE mode...107
Logging in to a VDI session using a smart card...107
Install a certificate...108

View Installed certificates....108
Unified Communications optimization....109
Zoom plug-in for VDI....109
Multimedia add-on package for VDI....110
Bloomberg keyboard support for VDI....110
Bundle and Addon Naming....110
File Type Association....110
Configure the File Type Association for Citrix....111
Configure the File Type Association for VMware....111
Configure the File Type Association for RDP....112

Chapter 7: Managing user accounts....114
Configure the guest user account settings....114
Configure the local user account settings....115
Configure multiple local user accounts....116
Change local user credentials from Wyse Management Suite....116
Log in as a local user....117
Joining Active Directory....117
Log in as a domain user using Active Directory credentials....118
Direct Domain Login....118
Configuring the direct domain login....118
Banner message on device login screen....119
Log in as a domain user using a smart card....119
Show user list on the Dell Hybrid Client login screen....120
System password....120
Change Admin (System) Password Protection....120
View the System password....121
Device compliant....121
Generate the default System password....121
User Personalization....122
Configure the User Personalization Roaming Settings....122

Chapter 8: Configure VPN settings....125
Configure VPN Settings....125
Configure VPN from Wyse Management Suite....125
Configure VPN from Device Settings....127
Connect to a VPN on Dell Hybrid Client....129
Configure the power profile settings....132
User Data Roaming....132
Configure the User Data Roaming Settings....132
Switch users(Inactivity Action)....134
Block keyboard shortcut keys....135
Configure Keyboard Layout for Login Screen using Wyse Management Suite....135
Simplified Certificate Enrollment Protocol....136
Configure the SCEP settings using Wyse Management Suite....136
Network authentication using IEEE 802.1x....136
Configure the EAP-PEAP MSCHAPv2 user mode authentication....137
Configure the EAP-PEAP MSCHAPv2 machine mode authentication....137
Configure the EAP-TLS user mode authentication....138

Configure the EAP-TLS machine mode authentication....139
Connect to hidden Wi-Fi networks using Wyse Management Suite....139

Chapter 9: User applications....141
Browse the Internet....141
Enable or disable multicontainers for Firefox....141
Enable or disable site isolation for Chrome....142
Enable or disable plugins for Chrome....142
Custom policy configuration for Firefox and Chrome....142
Allow and Deny access to websites....143
Configure the browser shortcut settings....143
Create a desktop shortcut to a browser URL....144
Using Dell File Explorer....144
Create a file....147
Add a folder....147
Open with functionality....147
Save cloud files for offline use....148
Format a USB device....149
Configure a network drive using Wyse Management Suite....149
Access local applications....150
Pin an application to desktop....150
Using the Zoom application....150
Installing third-party applications....151
Install a Dell-signed application....151
Install a custom-signed application....152
Install an unsigned application....153

Chapter 10: Configuring the local device settings....154
Network....154
Network Configuration using Device Settings....155
Network Configuration using Wyse Management Suite....155
Connect to hidden Wi-Fi networks....155
Proxy settings in device settings....156
Proxy in Quick Start Wizard....156
Configuring proxy in device settings....156
Configuring the Display Settings....156
Configure the display personalization settings....157
Configure the region and language settings....158
Configure the power settings....159
Inactive Timeout....160
Change the password....160
Configure the network drive locally....161
Configure the advanced settings....161
Configure the troubleshooting options....162
Access the terminal window....163
Configure SCEP locally....166
Configure the wired and wireless Advanced Network Settings....166
Configure the Dell Client Agent (DCA) settings manually....167

Chapter 11: Configuring the Cloud environment 169
Single Sign-On (SSO) to cloud applications 169
Multifactor authentication for cloud applications 169
File Affiliation 170
Configure the Cloud + Local Mode 170
Configure the VDI Mode 171
Configure the VDI + Local Mode 172
Configure the Cloud + VDI + Local Mode 173
Configure personal accounts for Azure 174
Configure personal accounts for Google Cloud 175
Connect to Microsoft 365 Apps 175
Connect to Google Workspace Apps 176
Create shortcuts for cloud apps 177
Connect to Box cloud drive 178

Chapter 12: Device security 179
Configure the SSH settings 179
Configure the VNC settings 180
Manage USB devices 181
User data encryption using ZFS file system 181
User data cleanup 182
Configure the security profile settings 182
Configuring metadata for Firejail profiles 183

Chapter 13: Dell Hybrid Client troubleshooting 186
Using log files for troubleshooting 186
Request log files using Wyse Management Suite 186
Troubleshooting 186
Export log files using Advanced Settings 187
Export VDI log files 188
Device is unable to register to Wyse Management Suite 188
Enrollment validation is pending 188
Reset the Dell Hybrid Client to factory default settings 188
Reimage using Wyse Management Suite 189

Chapter 14: Security update cadence 190

Chapter 15: Frequently Asked Questions (FAQs) 191
How to configure Single and multiple display settings 193
Configuring Display using Device Settings 193
Configuring Display Settings using Wyse Management Suite 213
How to configure the features using Optional Packages 231
How to Add optional packages 231
How to View the Installed Packages 234
How to Uninstall the Packages 235
How to configure the Peripheral Management settings 237
Configuring Audio using Device Settings 237
Configuring Audio using Wyse Management Suite 239

Configuring Keyboard using Device Settings....240
Configuring a Keyboard using Wyse Management Suite....241
Configuring Mouse using Device Settings....242
Configuring a Mouse using Wyse Management Suite....243
Configuring Printer using Device Settings....244
Configuring Printer using Wyse Management Suite....245
How to prepare and configure the USB bootable drive with the ISO image....249

1

Introduction

Dell Hybrid Client is a desktop solution by Dell that follows the Software-as-a-Service (SaaS) model of software delivery. It provides a hybrid operating environment that enables end users to access virtual, cloud, or local applications and resources seamlessly. It encompasses the cloud and storage aggregation for maintaining security and simplicity.

You must use a management software to configure, operate, and update devices that are powered by Dell Hybrid Client, thereby eliminating the need for IT support to go to the physical devices. You can manage the devices by using Wyse Management Suite Pro. Wyse Management Suite offers process automation and helps lower costs for large deployments of devices that are powered by Dell Hybrid Client. Using secure HTTPS-based communication and Active Directory authentication for role-based administration, Wyse Management Suite keeps your devices up to date.

This guide is intended for administrators and users who use Wyse Management Suite to manage devices powered by Dell Hybrid Client. This guide contains information and detailed system configurations to help you design and manage a Dell Hybrid Client environment using Wyse Management Suite. The target audience for this guide is Enterprise customers with administrator privileges. You must have knowledge about cloud infrastructure, network technologies, and user authentication technologies.

Dell Hybrid Client 2310 supports Full Disk Encryption on Ubuntu 22.04 only for OptiPlex 3000 Thin Client. Full Disk Encryption (FDE) provides extra security to the client by encrypting the entire disk. All the functionalities provided by Dell Hybrid Client non-FDE are also supported in Dell Hybrid Client FDE.

Supported platforms

Dell Hybrid Client 2310 is a software solution that can be deployed on Ubuntu 20.04 and 22.04-based platforms with a minimum memory (RAM) of 8 GB and disk storage of 64 GB or higher capacity.

NOTE: Recommended Storage size is 64 GB and higher capacity, considering the maintenance and security updates.

Ubuntu 20.04 and 22.04-based devices that have Dell Client Agent - Enabler (DCA Enabler) installed can be converted to Dell Hybrid Client version 2310 using Wyse Management Suite. You can also convert from Windows to Dell Hybrid Client using ISO image (OptiPlex 3000 Thin Client, Precision 3260, Latitude 5440, Latitude 3440, OptiPlex 7410 AIO, Latitude 3330, and OptiPlex 5400 AIO).

For information about the supported platforms and configurations for the Dell Hybrid Client deployment and conversion, see the *Dell Hybrid Client Version Conversion Guide* at www.dell.com/support.

- The following platforms are preinstalled with Dell Hybrid Client:
  - OptiPlex 3000 Thin Client
  - Precision 3260
  - Latitude 5440
  - Latitude 3440
  - OptiPlex 7410 AIO

    NOTE: Newly supported platforms have Dell Hybrid Client preinstalled.
- Any platforms that run Dell Hybrid Client 2.0 and 2.5 can be upgraded to Dell Hybrid Client 2310 using Wyse Management Suite (Dell Hybrid Client should have a minimum storage of 64gb).

Supported management software

Table 1. Supported management software

Dell Hybrid Client version	Supported management software
2310.72	Wyse Management Suite Pro Edition 4.1 and later

Supported operating system

Dell Hybrid Client is an application stack based on the Ubuntu operating system.

Table 2. Supported operating system

Dell Hybrid Client version	Base operating system
2310.72	Ubuntu 22.04 (FDE and Non FDE)
2310.72	Ubuntu 20.04

Salient features of Dell Hybrid Client

The following are the salient features of the Dell Hybrid Client:

- **Full Disk Encryption**—Dell Hybrid Client ensures an enhanced security for clients by encrypting their entire disk. It protects unauthorized individuals from recovering or physically transferring any data or the complete disk of the FDE client.
- **Dell File Explorer**—Dell Hybrid Client provides a secure way to access files on local or cloud drives. The application associated to open the files can be a local, VDI or a cloud application.
- **User security**—Dell Hybrid Client provides a high level of user security in which the data of a particular user is encrypted and cannot be viewed by other users. A user's access to Dell Hybrid Client is controlled with specific permissions and data profiles that are managed using Wyse Management Suite.
- **Secure browsing**—Dell Hybrid Client provides a secure endpoint for your browser-based work environment.
- **Direct AD Login**—Dell Hybrid Client allows domain user to authenticate Active Directory without joining the domain.
- **Active Directory authentication**—Dell Hybrid Client supports user authentication with Active Directory—local AD and On-Prem User Sync with Azure AD.

  NOTE: On-Prem User Sync with Azure AD is only available for Cloud-based authentication
- **Single Sign-On (SSO) to applications**—Dell Hybrid Client extends Single Sign-On (SSO) to cloud applications along with VDI applications. You get access to most applications by logging in once.
- **File Affiliation**—Dell Hybrid Client delivers a distinct setting called File Affiliation, in which you can restrict the user's ability to access files with associated applicatons depending on the mode which is configured.
  - **Cloud mode**—In the Cloud mode, the client shows applications that are supported by Cloud services.
  - **Local mode**—In the Local mode, the client shows the local applications that are installed on Dell Hybrid Client.

    NOTE: Not all applications are supported in the Local mode.
  - **VDI mode**—In the VDI mode, the client shows the VDI published applications.

  In the Offline mode, the system shows the files that operate on the cached files. On the same device different modes can be configured for different users using user policy groups.

Other documents you may need

In addition to this guide, you can access the following guides available at www.dell.com/support/manuals.

- The *Dell Hybrid Client v2310 Release Notes* provides information about new features and known issues in each Dell Hybrid Client release.
- The *Dell Hybrid Client Conversion Guide* provides information about how to convert your devices running Windows, or Ubuntu running with DCA-enabler to Dell Hybrid Client.
- The *Dell Hybrid Client v2.5 Security Guide* provides guidelines that help you maximize the security of your devices powered by Dell Hybrid Client.
- The *Dell Wyse Management Suite 4.1 or later Administrator's Guide* provides information about configuration, and maintenance of the devices powered by Dell Hybrid Client by using the Wyse Management Suite console.

2

Dell Hybrid Client installation

Dell Client Agent-Enabler (DCAE) is a client agent for generic client management solutions. Installing DCAE on a generic client allows you to do minimal actions managed by Dell Wyse Management Suite. For more information, see *Dell Hybrid Client Conversion Guide* at www.dell.com/support.

Dell Hybrid Client Bundle Upgrade

Dell Hybrid Client 2310 supports Bundle Upgrade from 1.6.2 version or later. You can upgrade the Dell Hybrid Client version X.X to Y.Y by pushing Y.Y.tar.gz from Wyse Management Suite. The Bundle is compatible with the base operating system version. Once the Bundle is upgraded, you can verify the Dell Hybrid Client version in System Information. If the Bundle is successfully upgraded, you can use the latest Dell Hybrid Client features.

Dell Hybrid Client Upgrade from version 1.x to 2310

Dell Hybrid Client can be upgraded from version 1.x to 2310 from Wyse Management Suite using `DellHybridClient2310.x.XXX.tar.gz` file. You can use the latest features of Dell Hybrid Client.

The following image displays Dell Hybrid Client with DHC-1.X 20.04 image which has configured addons like Citrix Workspace, VMware Horizon Client, and AVD Client.

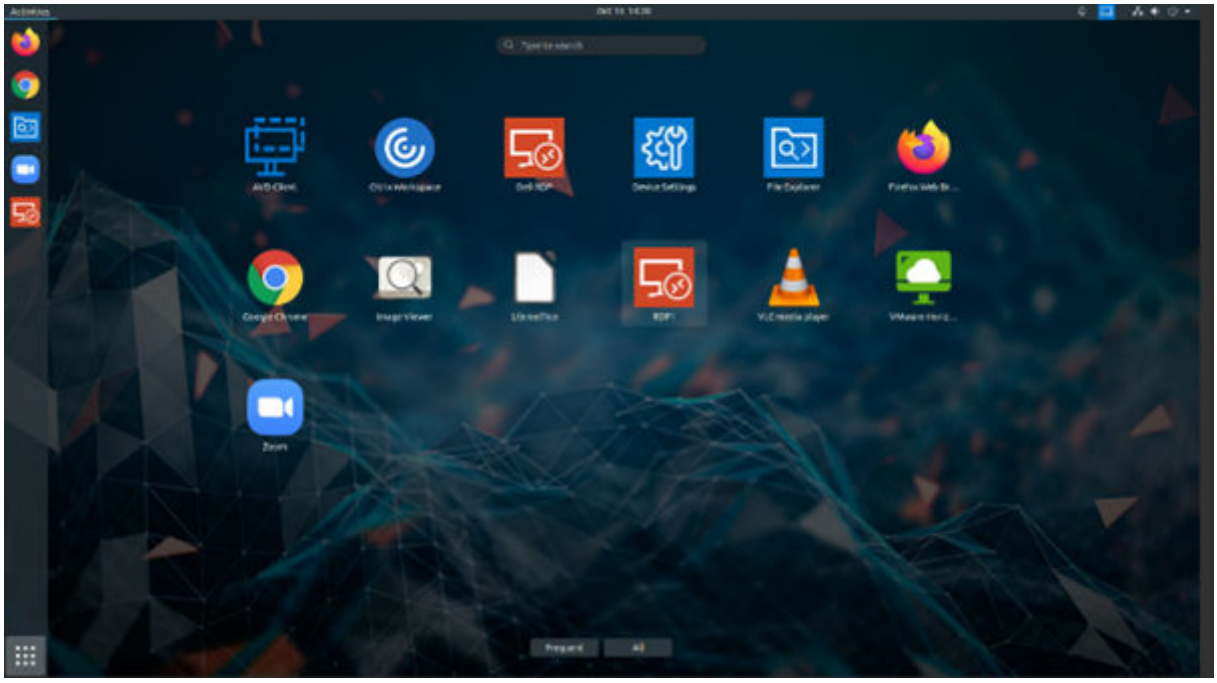


Figure 1. Dell Hybrid Client

The following are the steps to Bundle Upgrade from Wyse Management Suite.

1. Download and Save **2310_xxx.tar.gz file** in Local Repository.

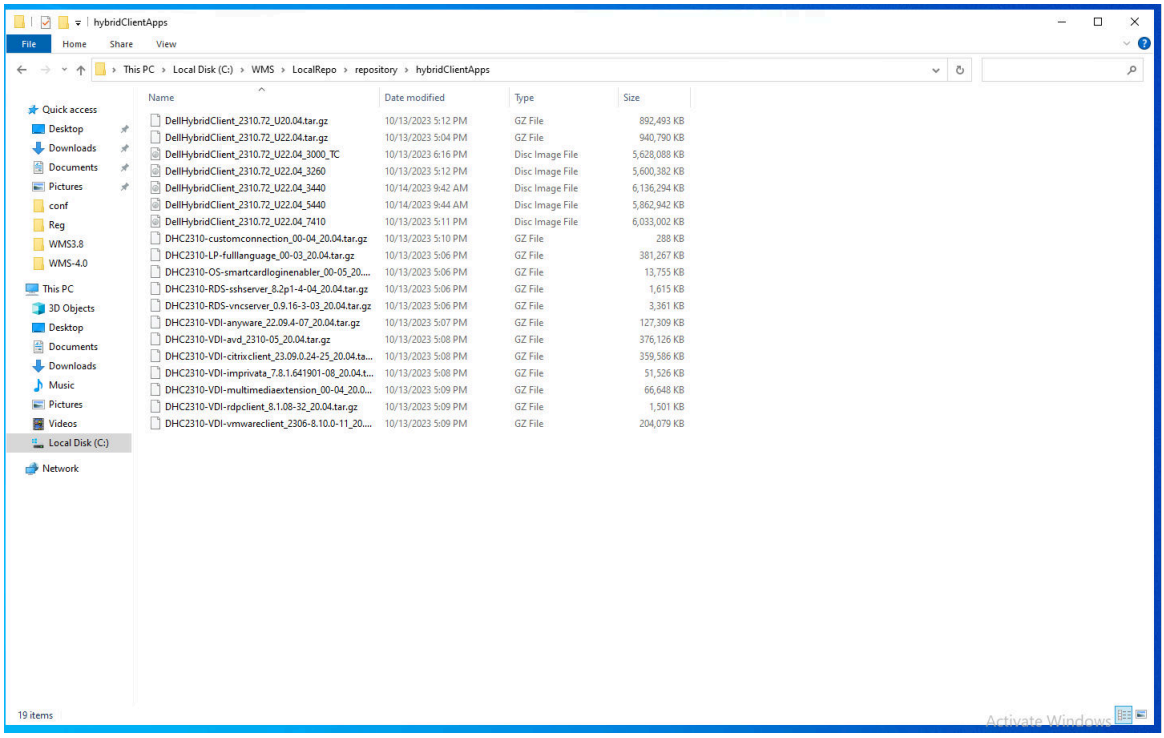


Figure 2. Local Repository

2. After you save **2310_xxx.tar.gz** file in the Local Repository, you can view it in the Wyse Management Suite App Inventory.

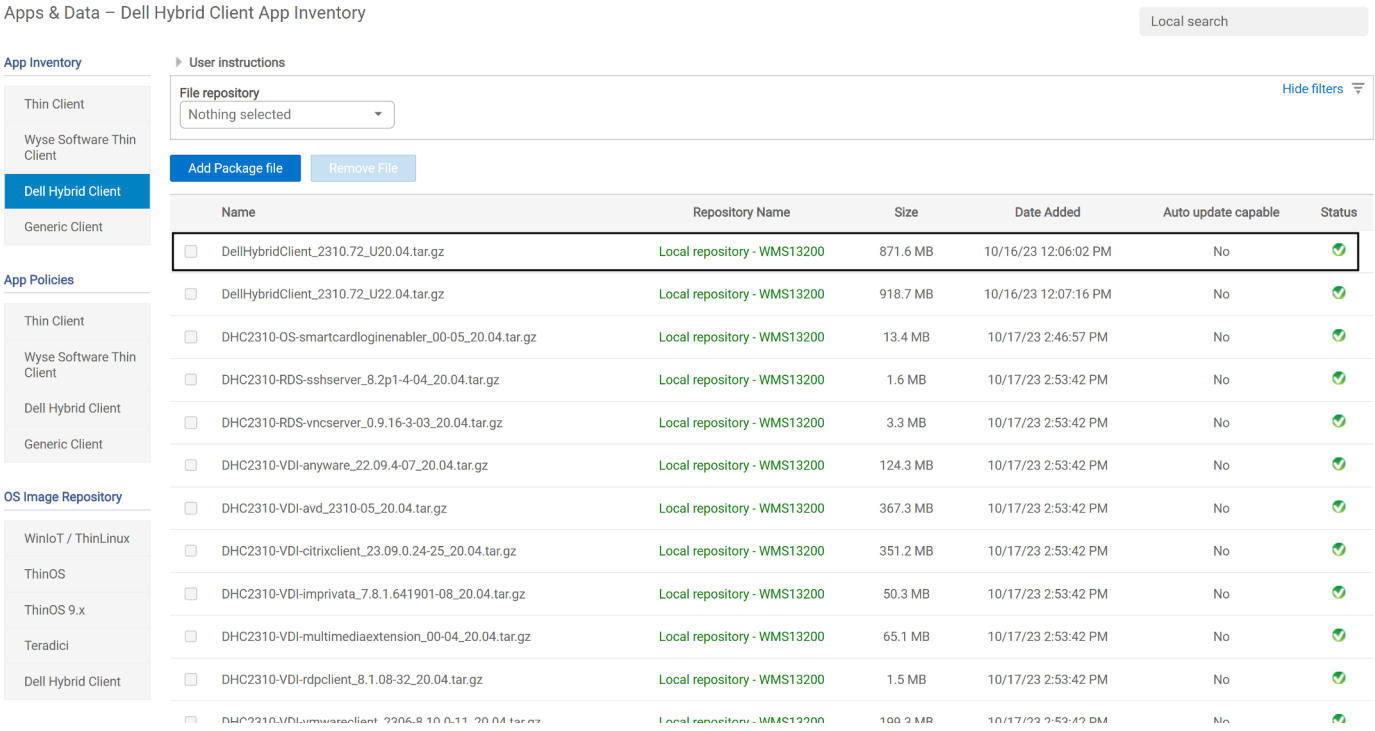


Figure 3. Wyse Management Suite App Inventory

NOTE: For Cloud WMS, by default the 2310 Bundle is available in the cloud repository.

3. Go to **Apps & Data** > **App Policies**.
4. Click **Dell Hybrid Client**.

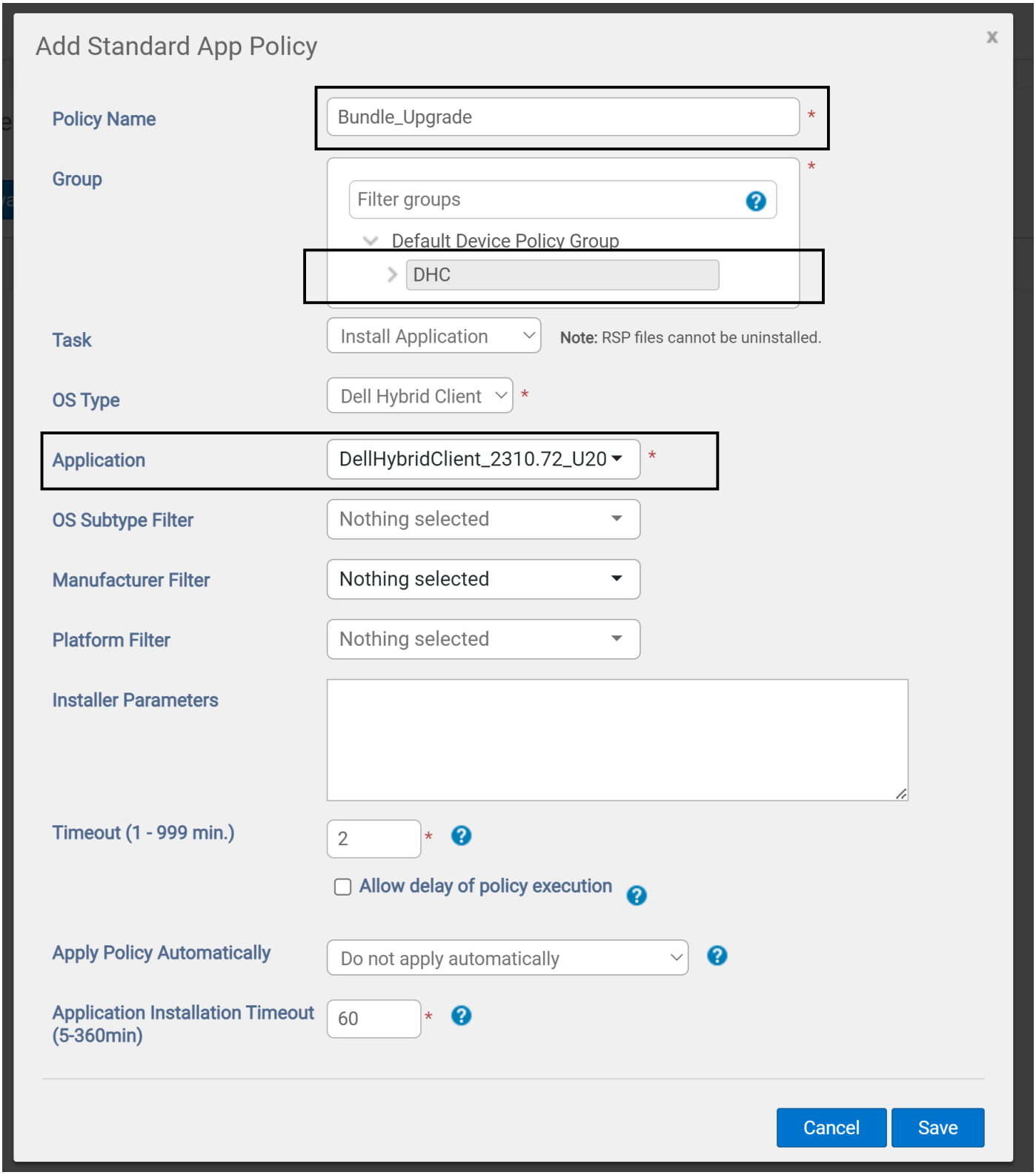


Figure 4. Add Standard App Policy

5. Enter the **Policy Name**.
6. Select your **Group**.
7. Select **DellHybridClient_xx_xx.tar.gz** in **Application**.
8. Select **OS Subtype filter** and **Platform Filter**. This is an optional step.
9. Click the **Save** button.

   An **Alert** prompt is displayed to Schedule time for bundle upgrade.

10. Click **Yes** in the **Alert** prompt.

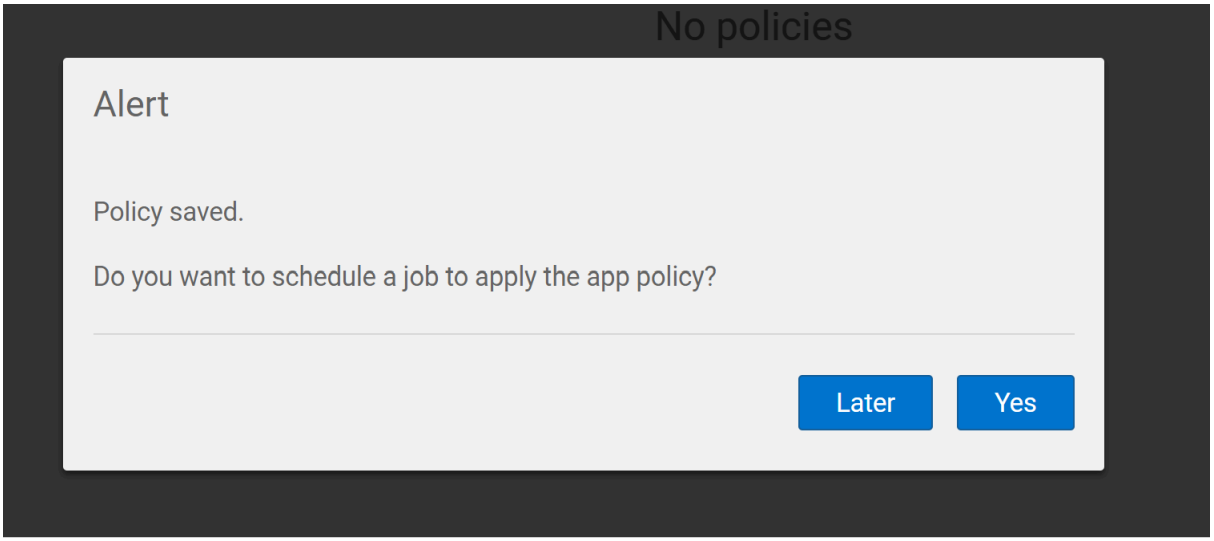


Figure 5. Alert

11. Select **Run** in **App Policy Job** and click **Preview**.

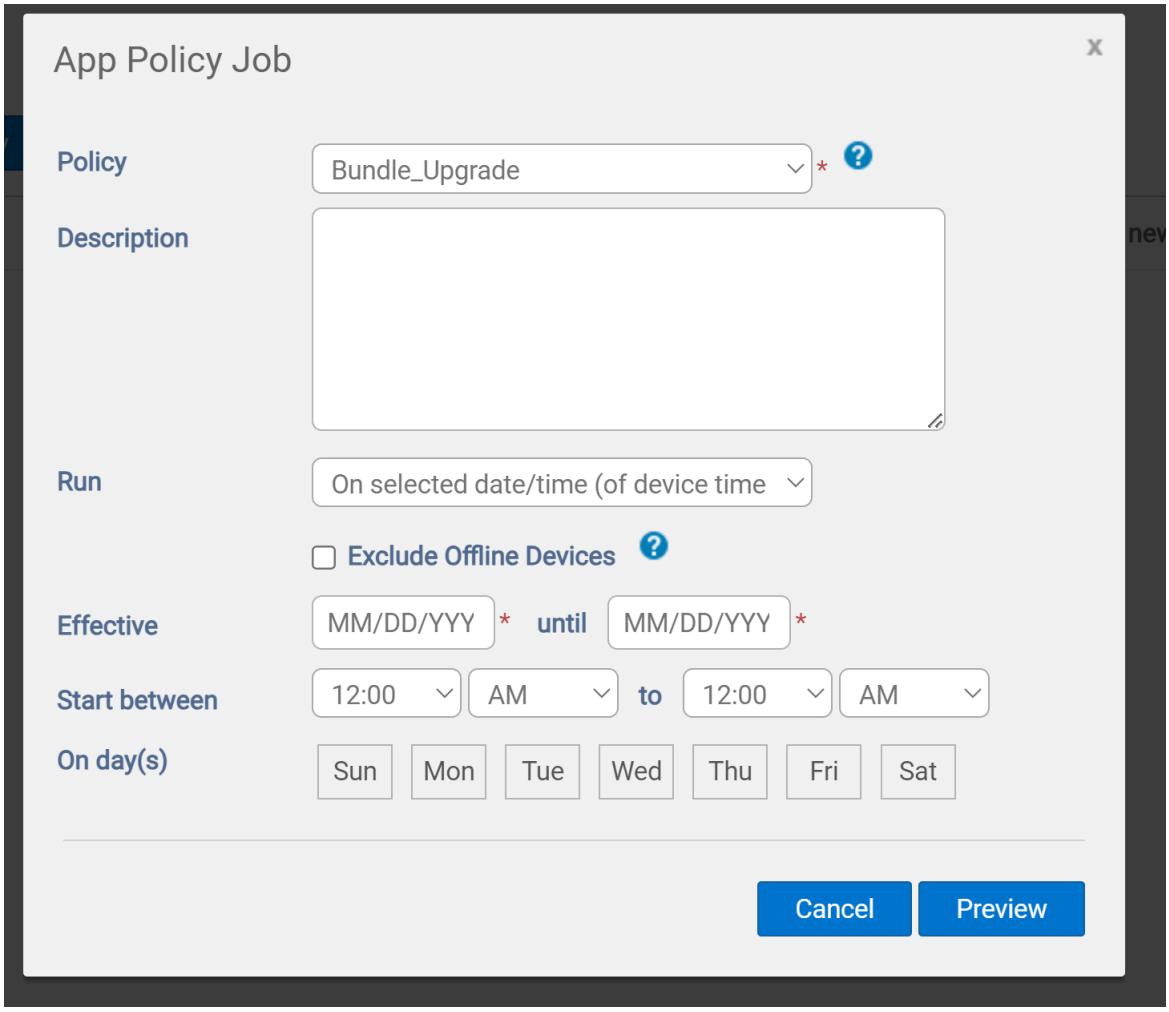


Figure 6. App Policy Job

12. Click **Schedule** in **App Policy Job**.

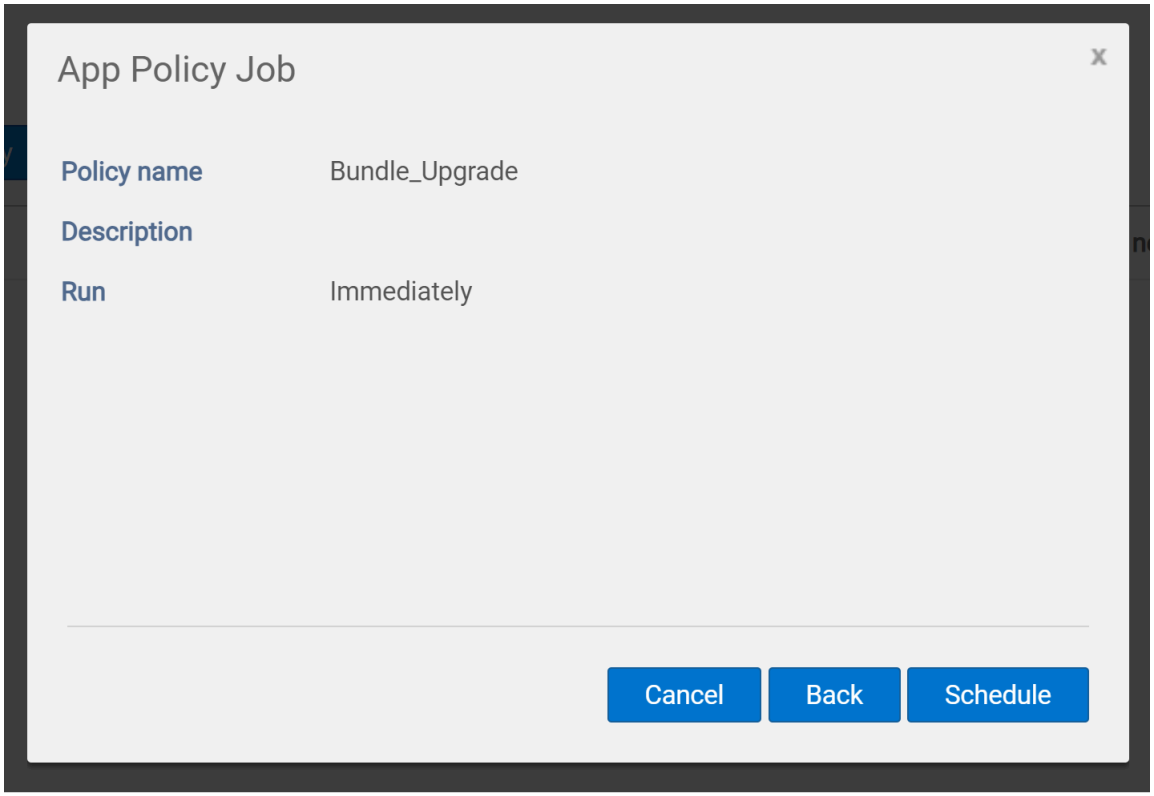


Figure 7. App Policy Job

A notification message is displayed on the client schedule time.

13. Click the **Update Now** button.

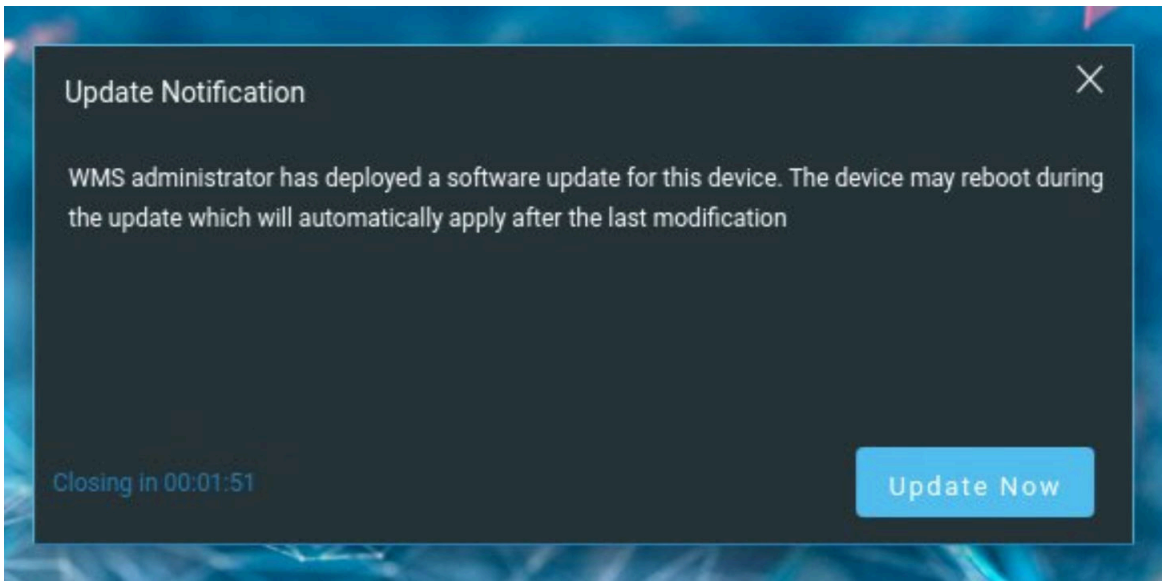


Figure 8. Update Notification

14. The **Lock screen notification** is displayed on the client.

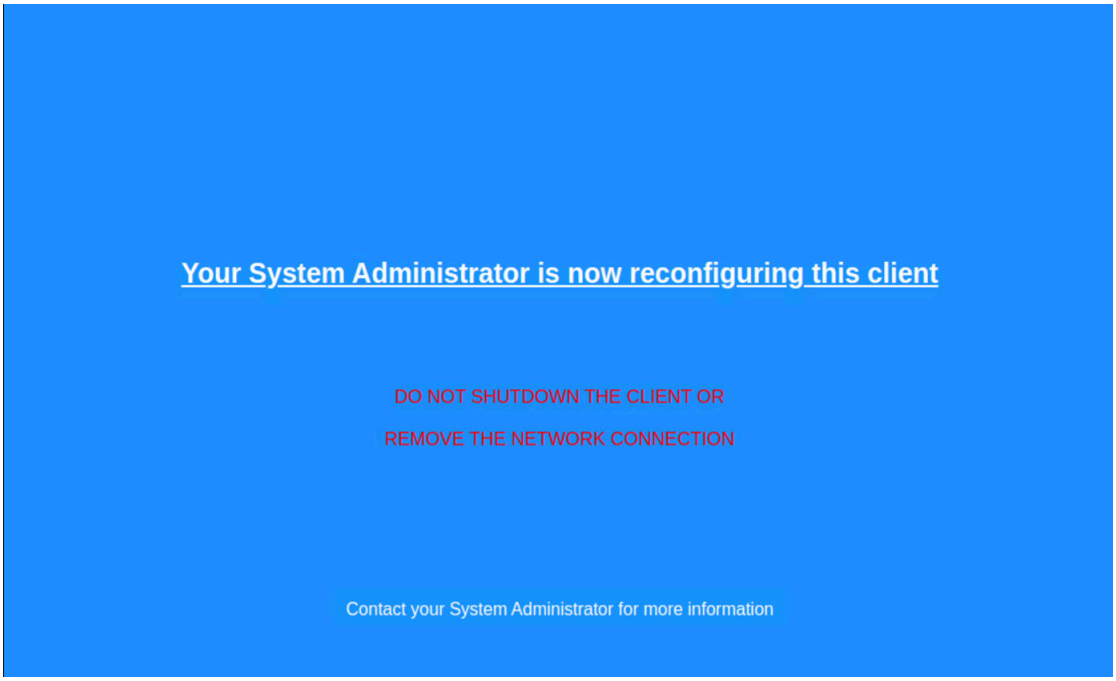


Figure 9. Lock Screen Notification

15. The update process takes around **15 to 20** minutes, after that the device restarts. Once installation is completed, the device redirects you to the **login** screen.

NOTE: Once the upgrade is completed, all the existing addons along with its configurations if pushed are available. You can use all the configured things till the device is moved to a new group or any configuration that is applied from **Dell Hybrid Client 2.X**.

NOTE: After you upgrade from Dell Hybrid Client version 2.x to 2310, all previously installed Dell Hybrid Client 2.x addons are available, you can install Dell Hybrid Client version 2310 optional add-on packages.

NOTE: After you upgrade from Dell Hybrid Client version 1.6.x, 1.8 to 2310, all previously installed Dell Hybrid Client 1.6 addons including VDI clients are removed. You must install Dell Hybrid Client version 2310 optional addon packages. For configuring a remote repository for the cloud, see the **Wyse Management Suite 4.x Administrator's Guide** at support.dell.com.

Transfer Configurations from Dell Hybrid Client 1.x to 2.x

About this task

Dell Hybrid Client 2.x schema is available in Wyse Management Suite 4.0 or later. If administrator pushes configuration from Dell Hybrid Client 2.x, then the Dell Hybrid Client 1.x available on the device is set to default. You must push the same configuration from Dell Hybrid Client 2.x.

Steps

1. Log in to **Wyse Management Suite** > **Groups & Configs** and do where the device is registered.
2. Go to **Edit Policies** and select **Dell Hybrid Client 2.x**.

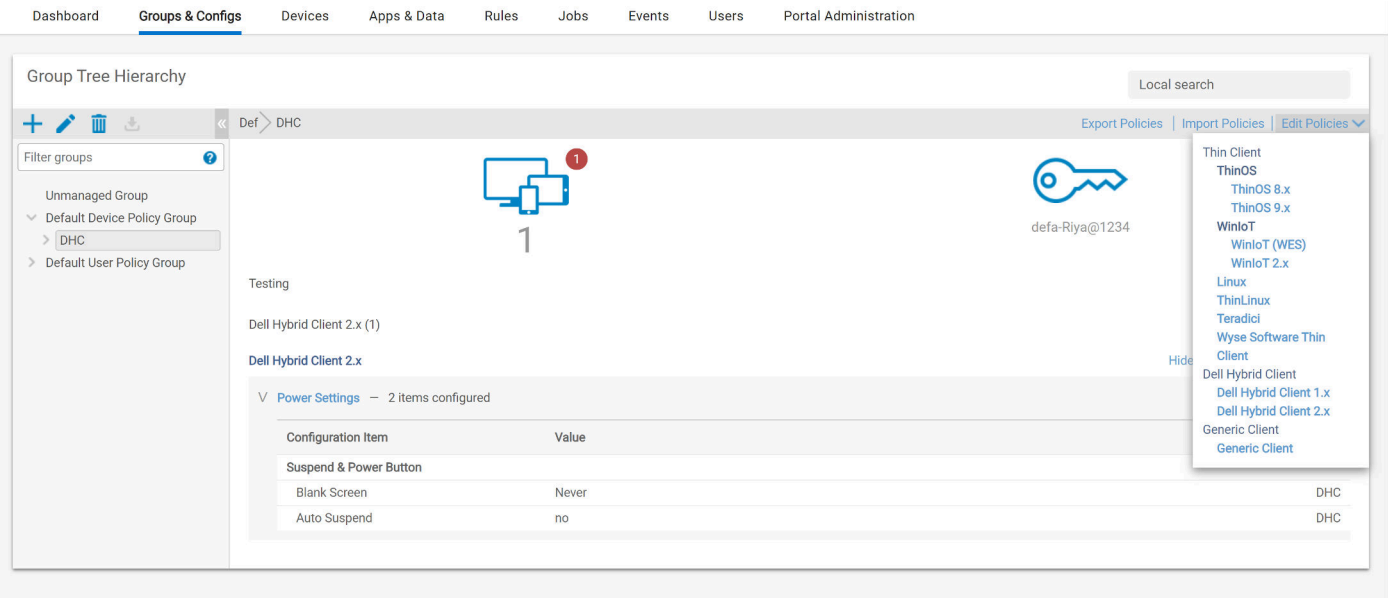


Figure 10. Wyse Management Suite

3. Reconfigure Dell Hybrid Client 2.x configurations same as Dell Hybrid Client 1.x configurations based on your requirement.
4. **Save & Publish** the configuration.

NOTE: If you want to use 2310 features, then you must push configuration only from Dell Hybrid Client 2.x.

Dell Hybrid Client Upgrade from 2.0, 2.5 to 2310

Dell Hybrid Client can be upgraded from 2.0, 2.5 to 2310 from Wyse Management Suite using `DellHybridClient2.y_xxx.tar.gz` file, so you can use latest features of Dell Hybrid Client.

The following image displays Dell Hybrid Client image which has configured addons like Citrix Workspace, VMware Horizon Client, and AVD Client.

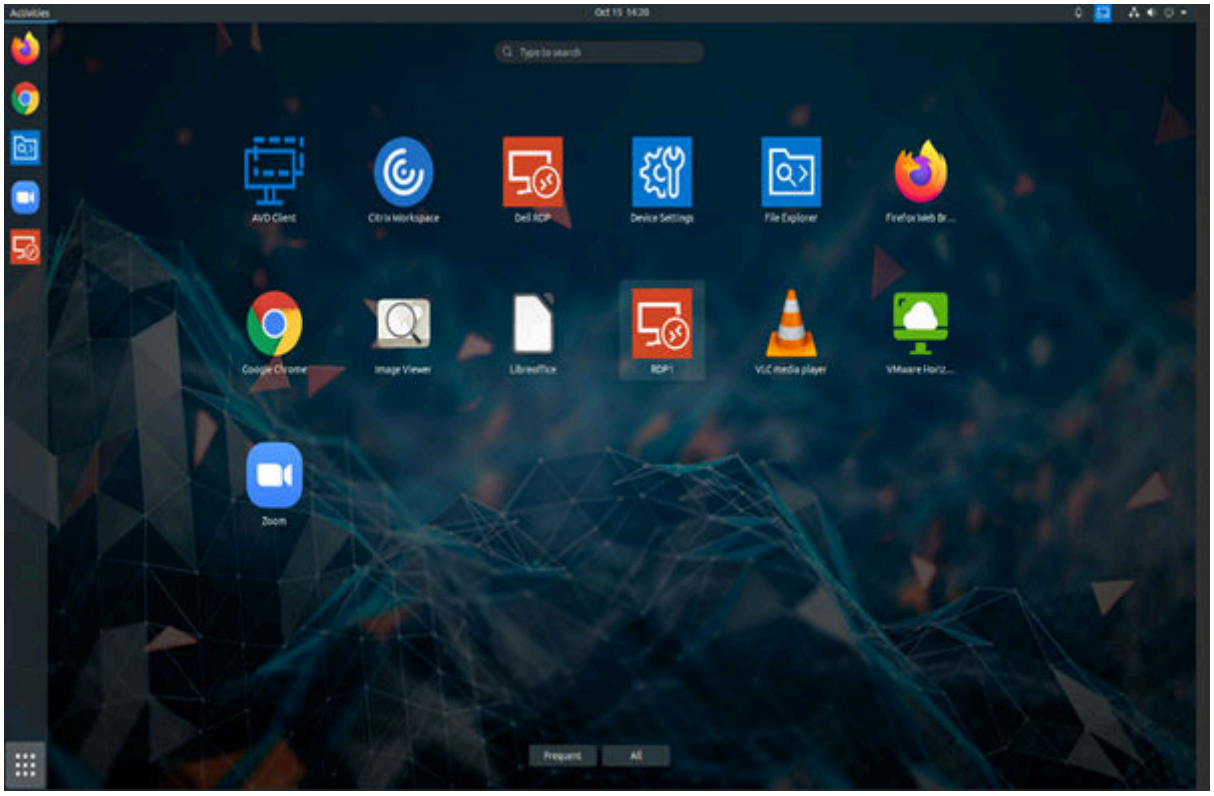


Figure 11. Dell Hybrid Client

The following are the steps to Bundle Upgrade from Wyse Management Suite

1. Download and Save `2.y_xxx.tar.gz` file in Local Repository.

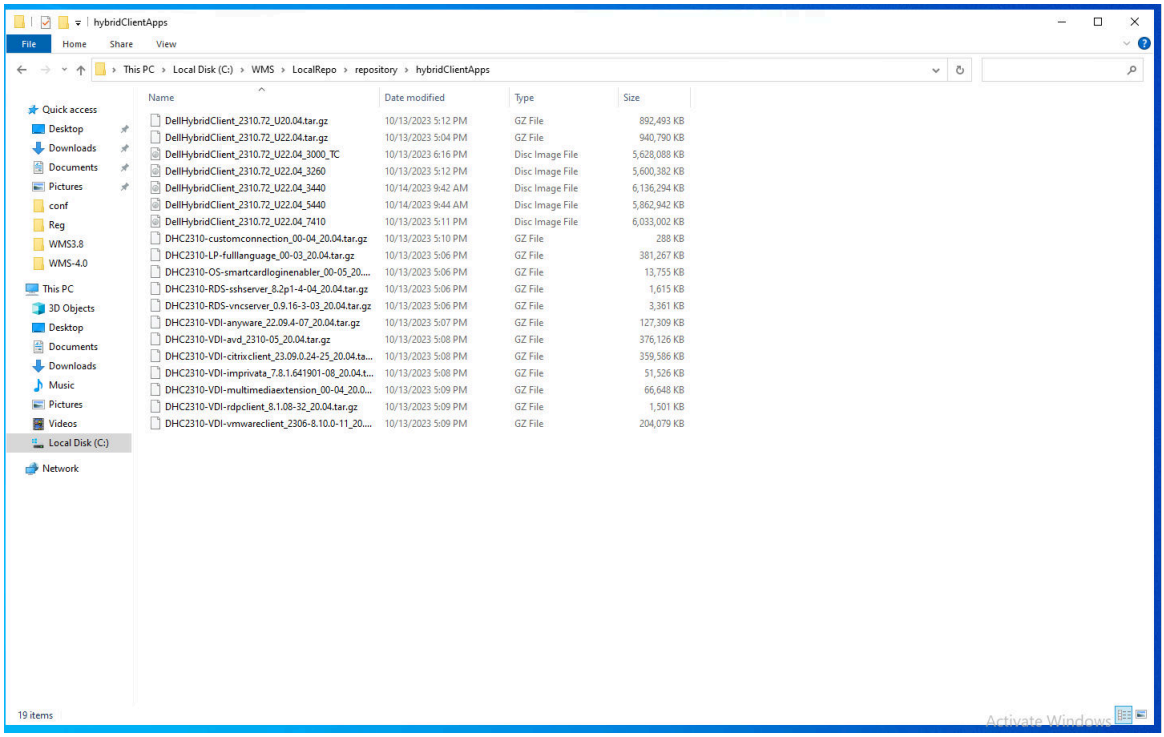


Figure 12. Local Repository

2. After you save `2.y_xxx.tar.gz` in Local Repository, you can view it in the Wyse Management Suite App Inventory.

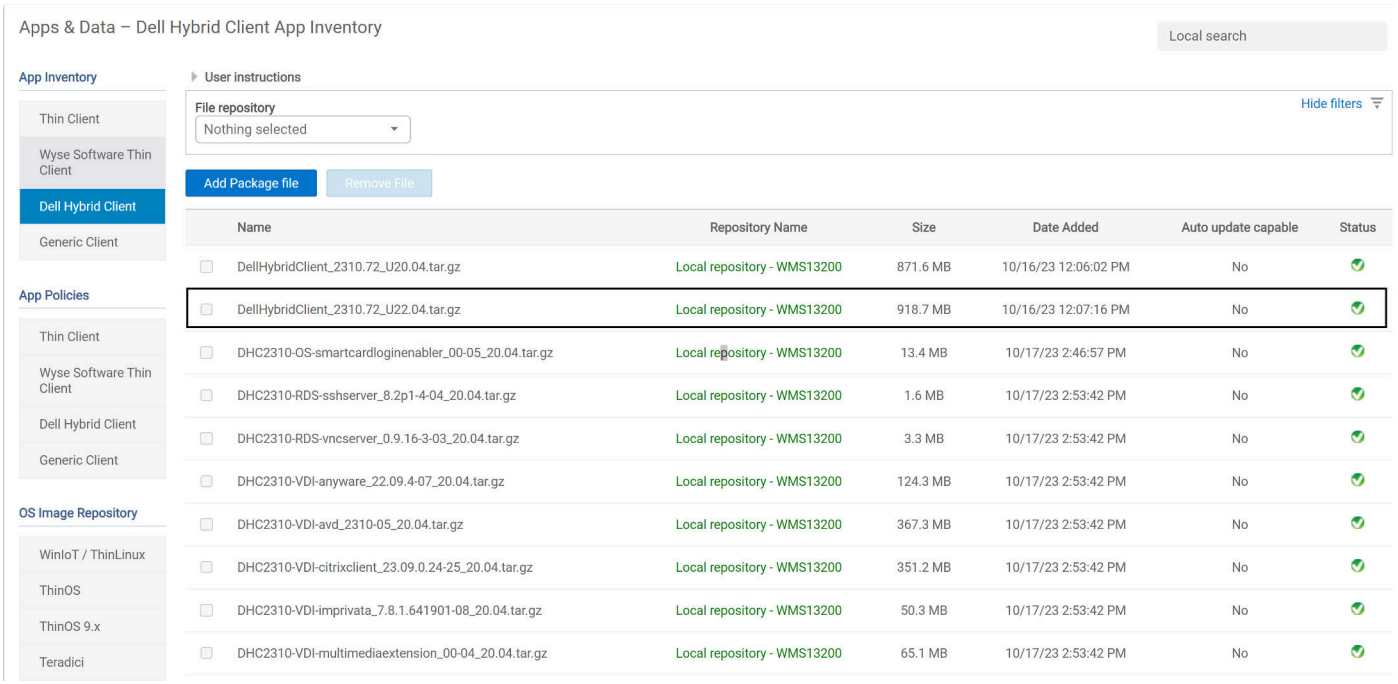


Figure 13. Wyse Management Suite App Inventory

NOTE: For Cloud WMS, by default the 2.y Bundle is available in the cloud repository.

3. Go to **Apps & Data** > **App Policies**.
4. Click **Dell Hybrid Client**.

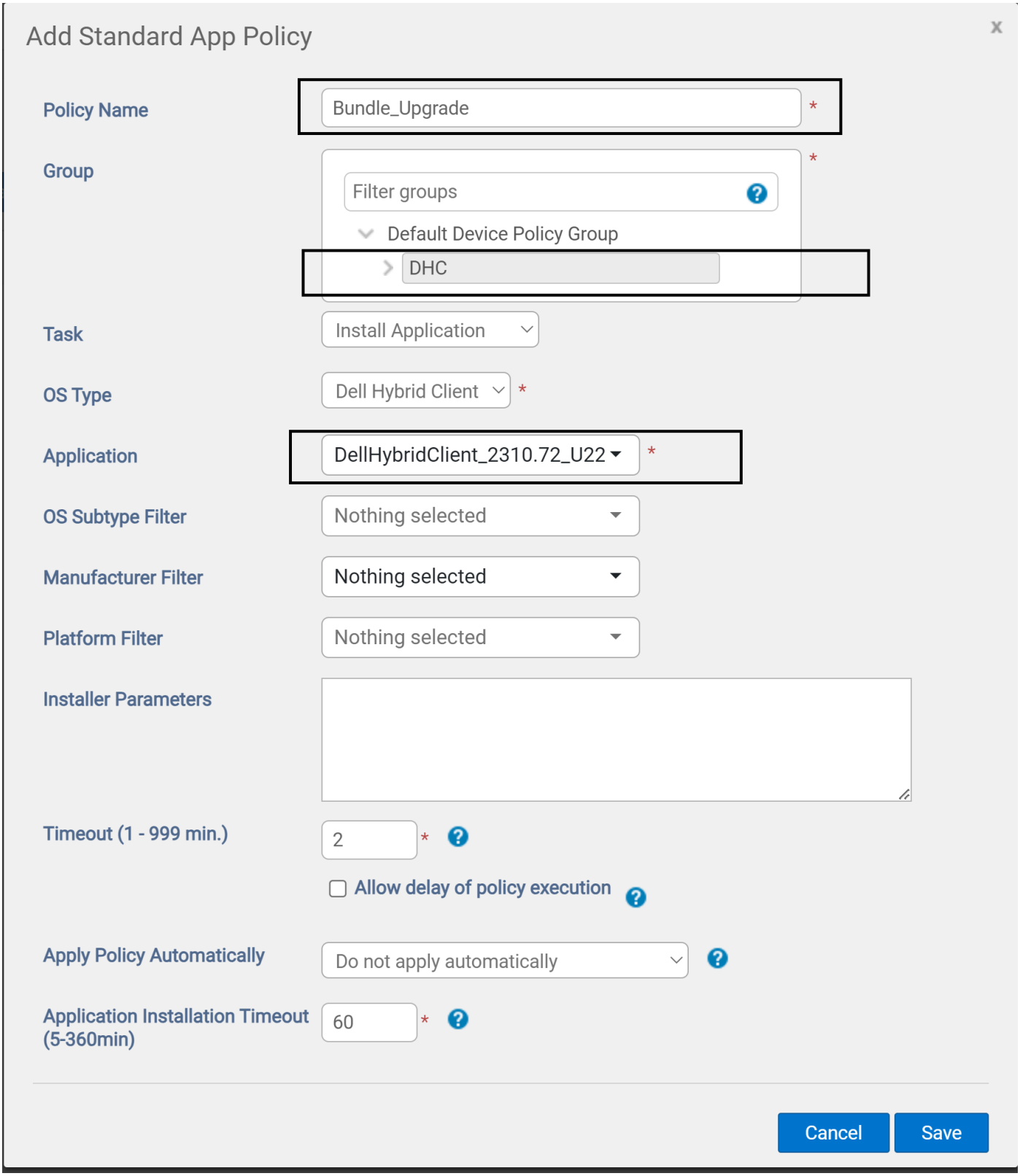


Figure 14. Add Standard App Policy

5. Enter the **Policy Name**.
6. Select your **Group**.
7. Select **DellHybridClient_xx_xx.tar.gz** in **Application**.
8. Select **OS Subtype filter** and **Platform Filter**. This is an optional step.
9. Click the **Save** button.

An Alert prompt is displayed to **Schedule time** for bundle upgrade.

10. Click **Yes** in the **Alert** prompt.

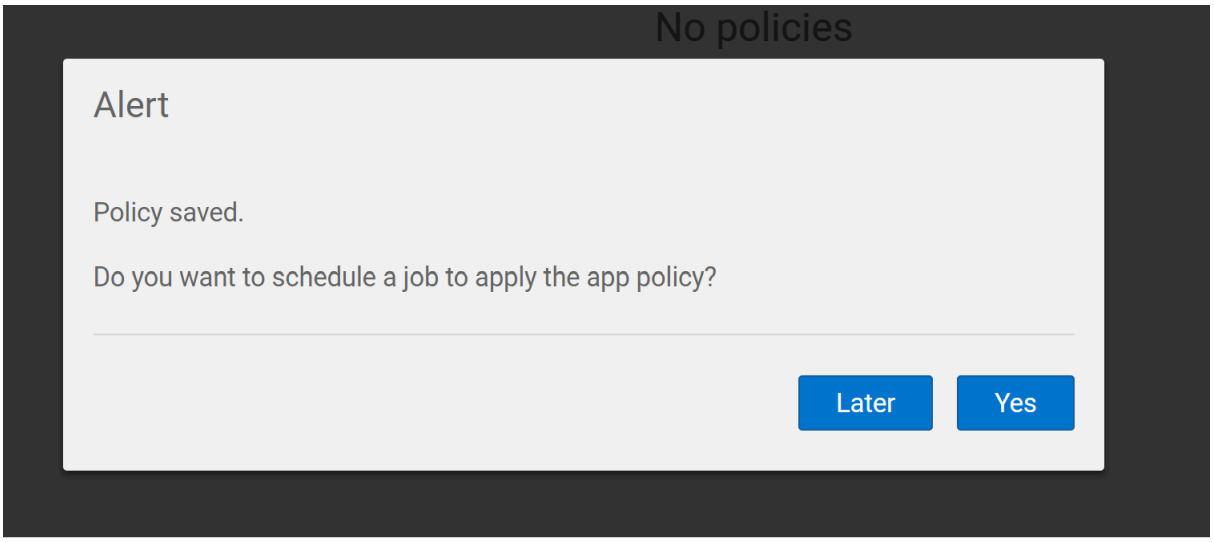


Figure 15. Alert

11. Select **Run** in **App Policy Job** and click **Preview**.

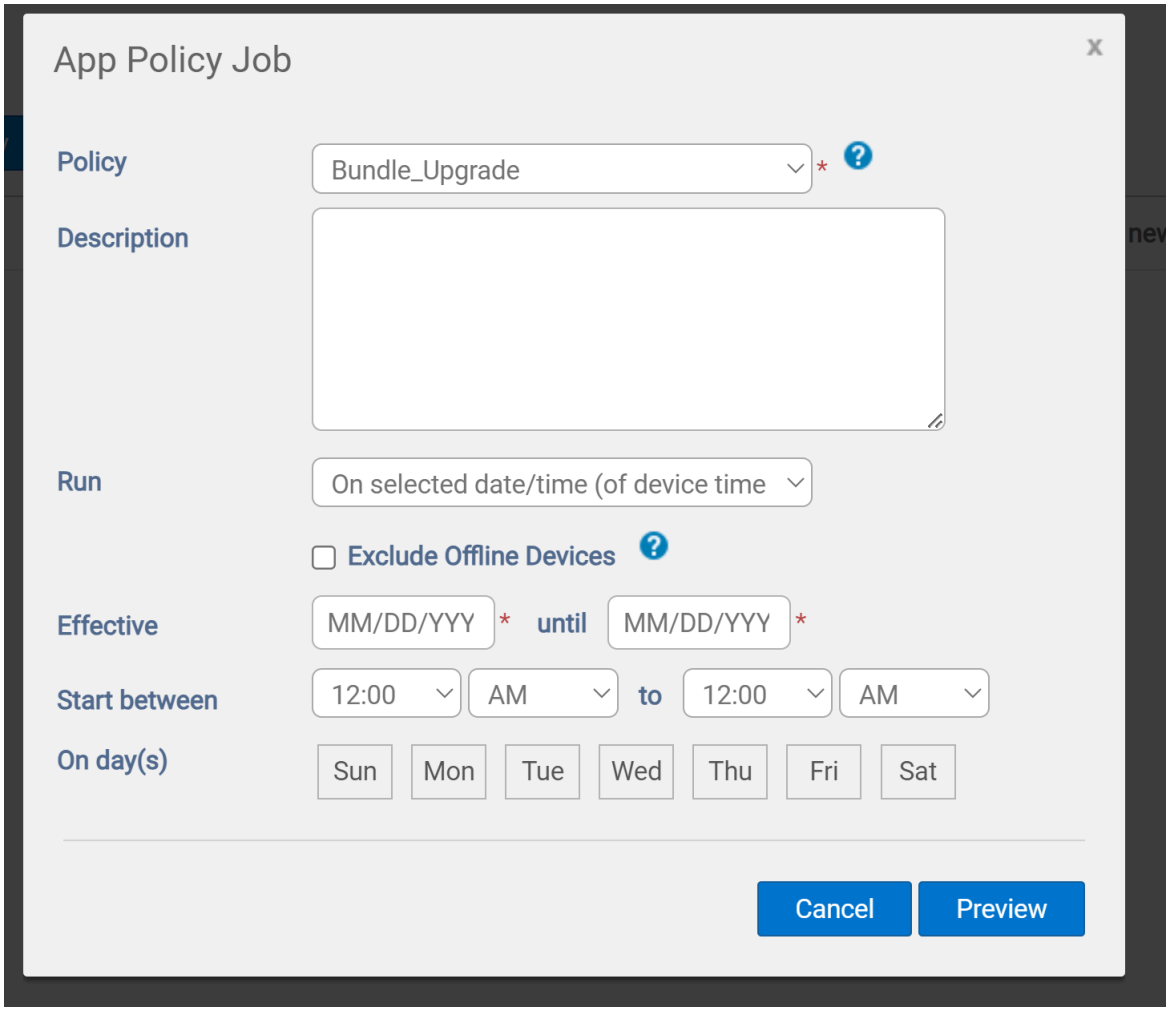


Figure 16. App Policy Job

12. Click **Schedule** in **App Policy Job**.

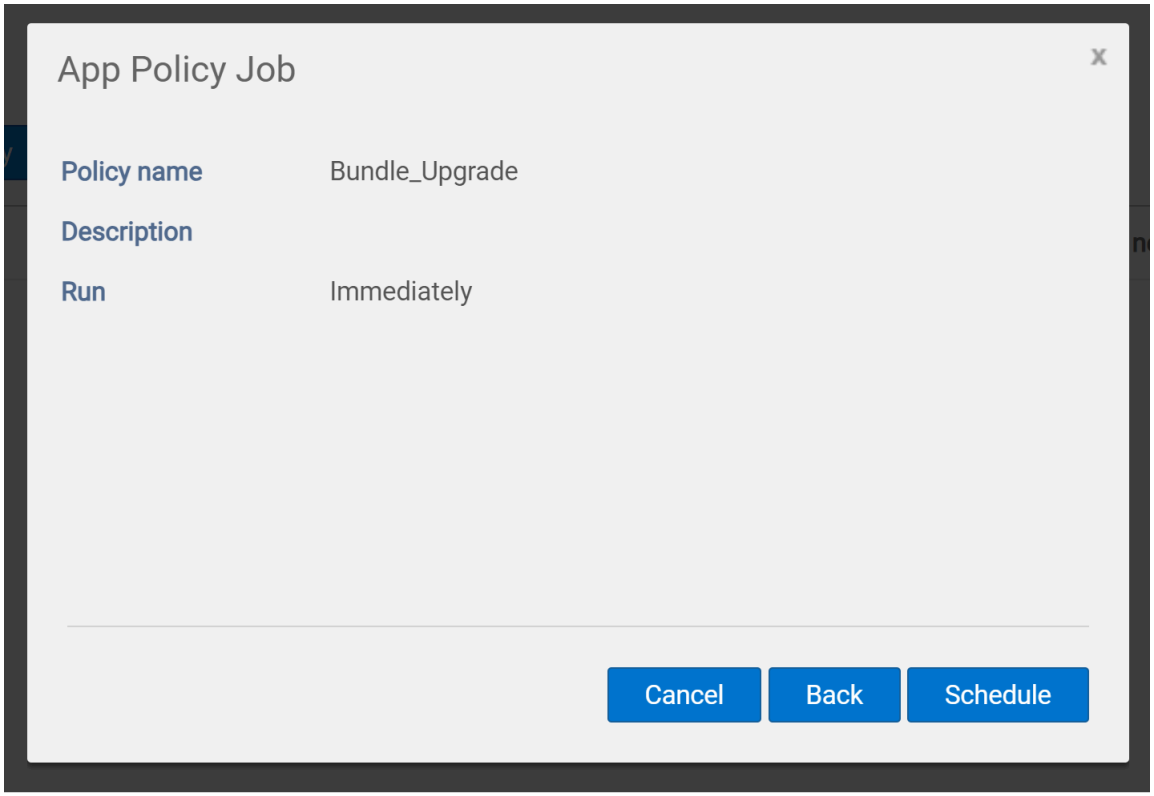


Figure 17. App Policy Job

A notification message is displayed on the client schedule time.

13. Click the **Update** button.

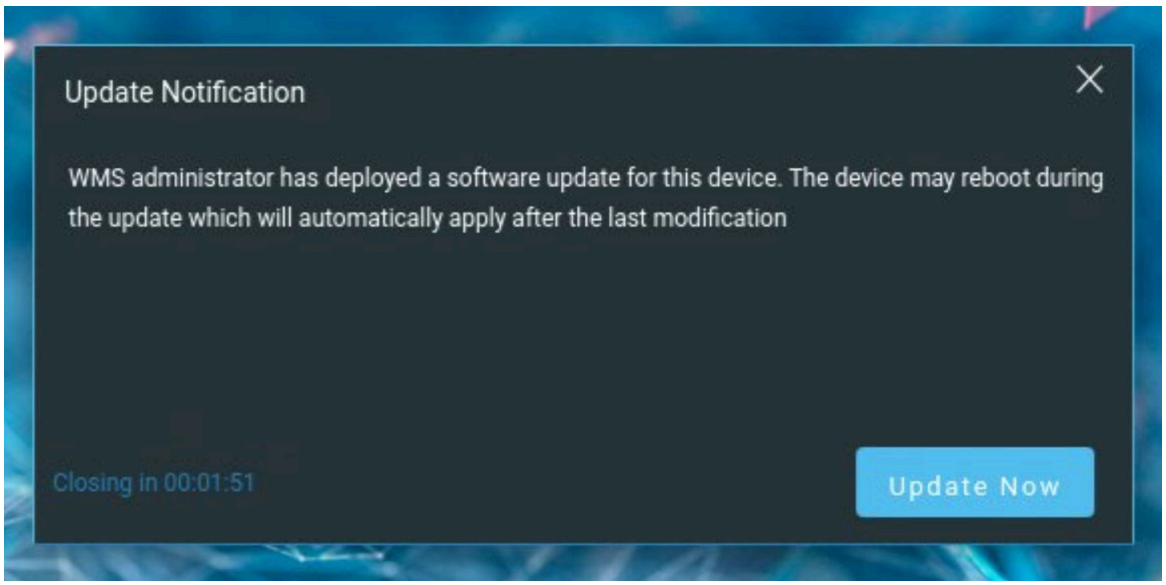


Figure 18. Update Notification

The **Lock screen notification** is displayed on the client.

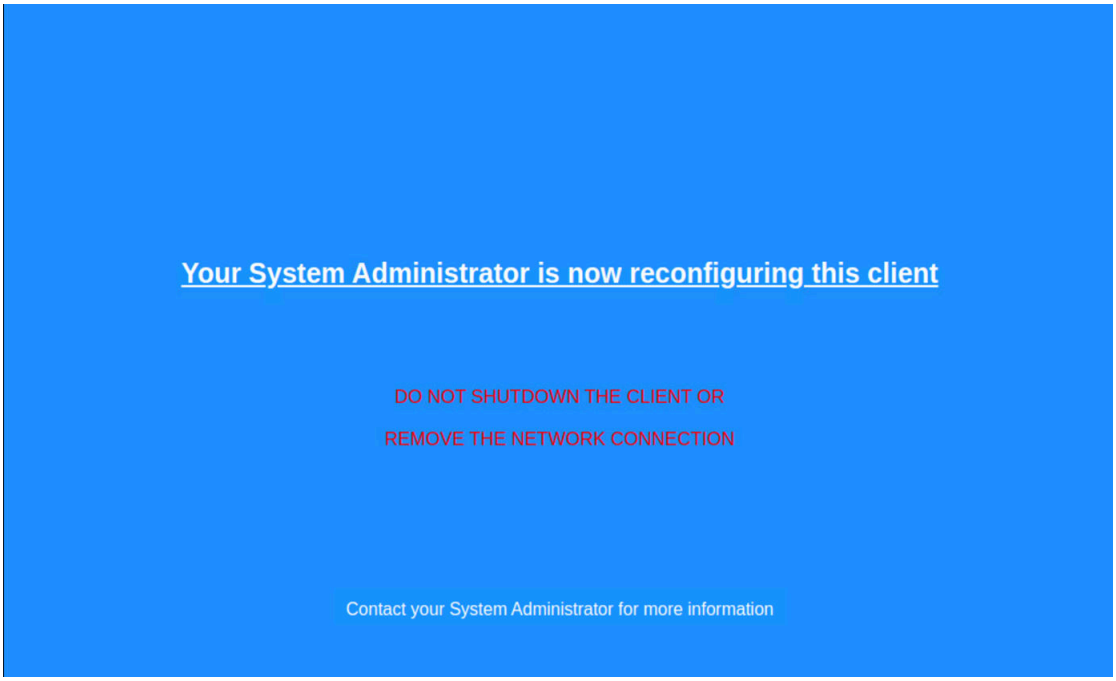


Figure 19. Lock Screen Notification

The update process takes around **15 to 20** minutes, after that the device restarts. Once installation is completed, the device redirects you to the **login** screen.

Verify Bundle Upgrade Status

You can verify the Bundle Upgrade status in System Information.

After the Bundle Upgrade is completed, the device redirects you to the **login screen**.

1. Log in into the device.
2. Click **System Information** on the **Top Bar**.
3. Go to the **About** tab and check **DHC Version**.

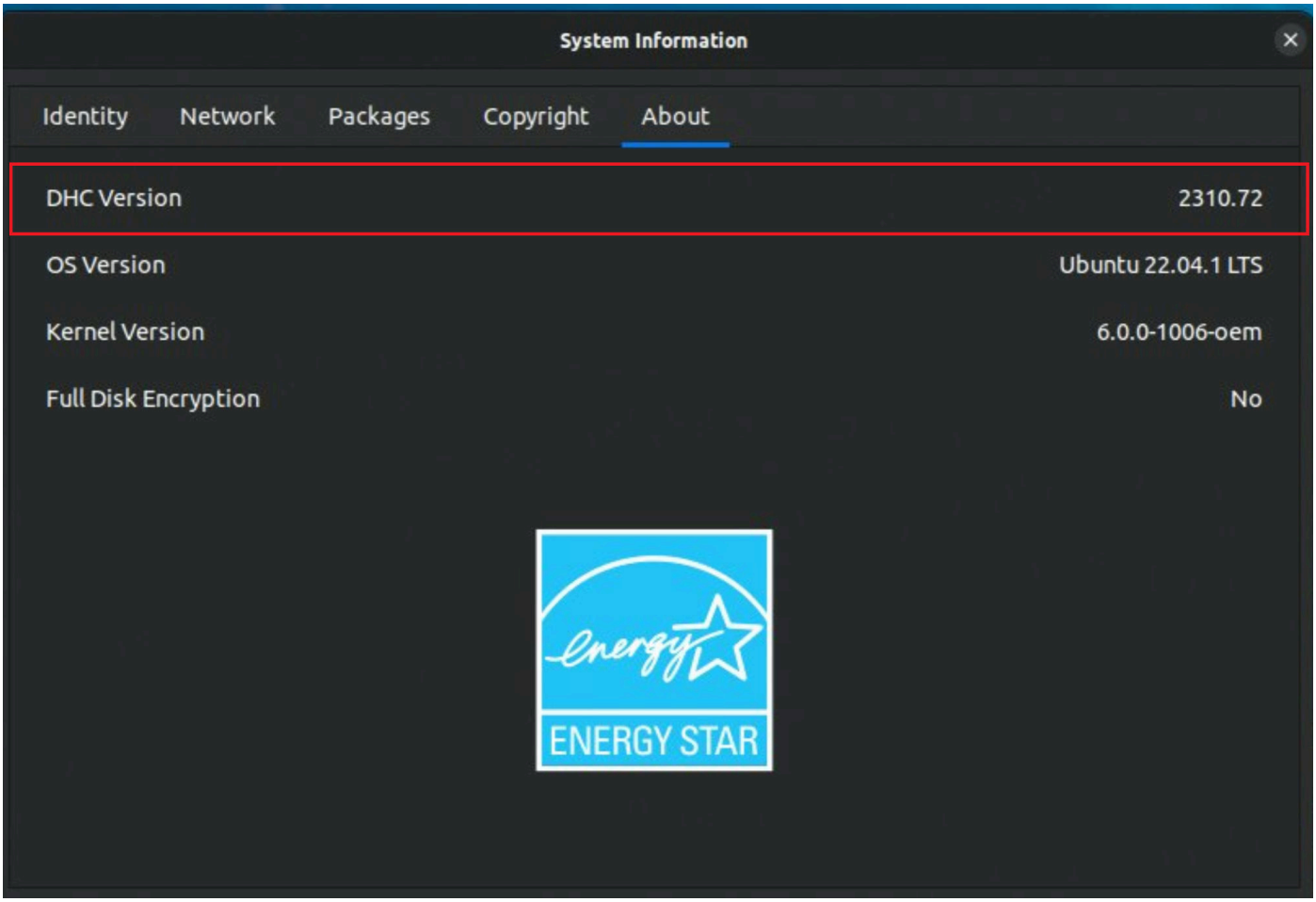


Figure 20. System Information

ISO Upgrade using Wyse Management Suite

Dell Hybrid Client supports ISO installation from Wyse Management Suite. Dell Hybrid Client can be upgraded to the latest version. You can upgrade Dell Hybrid Client including the underlying Base OS for Ubuntu from one version to another. For example, Ubuntu 20.04 + DHC 1.8 to Ubuntu 22.04 + DHC 2.5 or DHC 2310 using the ISO provided for the specific platforms.

NOTE: ISO upgrade from Generic client must install version 1.8.02 from dl.dell.com/FOLDER10424683M/1/DCA_Enabler_1.8.0-2.zip.

Table 3. ISO Upgrade from 20.04 to 22.04

Ubuntu 20.04	Ubuntu 20.04 +DCAE (Generic)	Ubuntu 22.04 +DCAE (Generic)
Using App Policies push the DHC 2310 22.04 ISO push from WMS	Using App Policies push the DHC 2310 22.04 ISO push from WMS	Using App Policies push the DHC 2310 22.04 ISO push from WMS

Steps to Install Dell Hybrid Client ISO Upgrade

This section provides the procedure for installing Dell Hybrid Client ISO Upgrade.

About this task

If you have Dell Hybrid Client version 1.8 (20.04) with all addons like Citrix, VMware, Anyware, Dell RDP, and all configurations are pushed.

Steps

1. Copy **DellHybridClient_2310_U22.04_XXX_XXXX.ISO** file to **WMS Repository**.

   For more information about creating a remote Repository, see **Wyse Management Suite 4.1 Administrator's Guide** at support.dell.com.

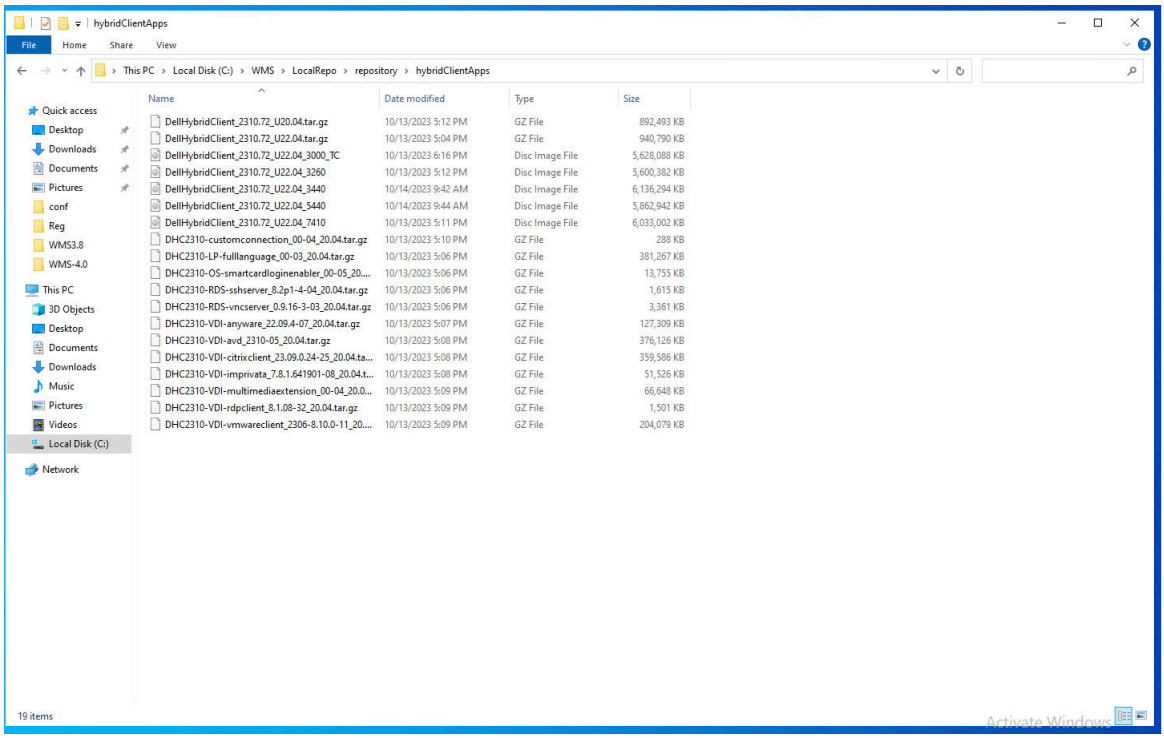


Figure 21. WMS Repository

☐	DellHybridClient_2310.72_U22.04_3440.iso	Local repository - WMS13200	5,992.5 MB	10/17/23 3:11:03 PM	No	✓
☐	DellHybridClient_2310.72_U22.04_5440.iso	Local repository - WMS13200	5,725.5 MB	10/17/23 3:25:31 PM	No	✓
☐	DellHybridClient_2310.72_U22.04_7410.iso	Local repository - WMS13200	5,891.6 MB	10/17/23 3:25:31 PM	No	✓
☐	DellHybridClient_2310.72_U22.04_3000_TC.iso	Local repository - WMS13200	5,496.2 MB	10/17/23 3:25:31 PM	No	✓
☐	DellHybridClient_2310.72_U22.04_3260.iso	Local repository - WMS13200	5,469.1 MB	10/17/23 3:25:31 PM	No	✓

Figure 22. Wyse Management Suite

2. Log in to Wyse Management Suite.
3. Go to **Apps & Data** > **Apps Policies** > **Dell Hybrid Client** > **Add Policy**.
4. Create the App Policy as shown in the below image.

   For more information about creating a remote Repository, see **Wyse Management Suite 4.1 Administrator's Guide** at support.dell.com.

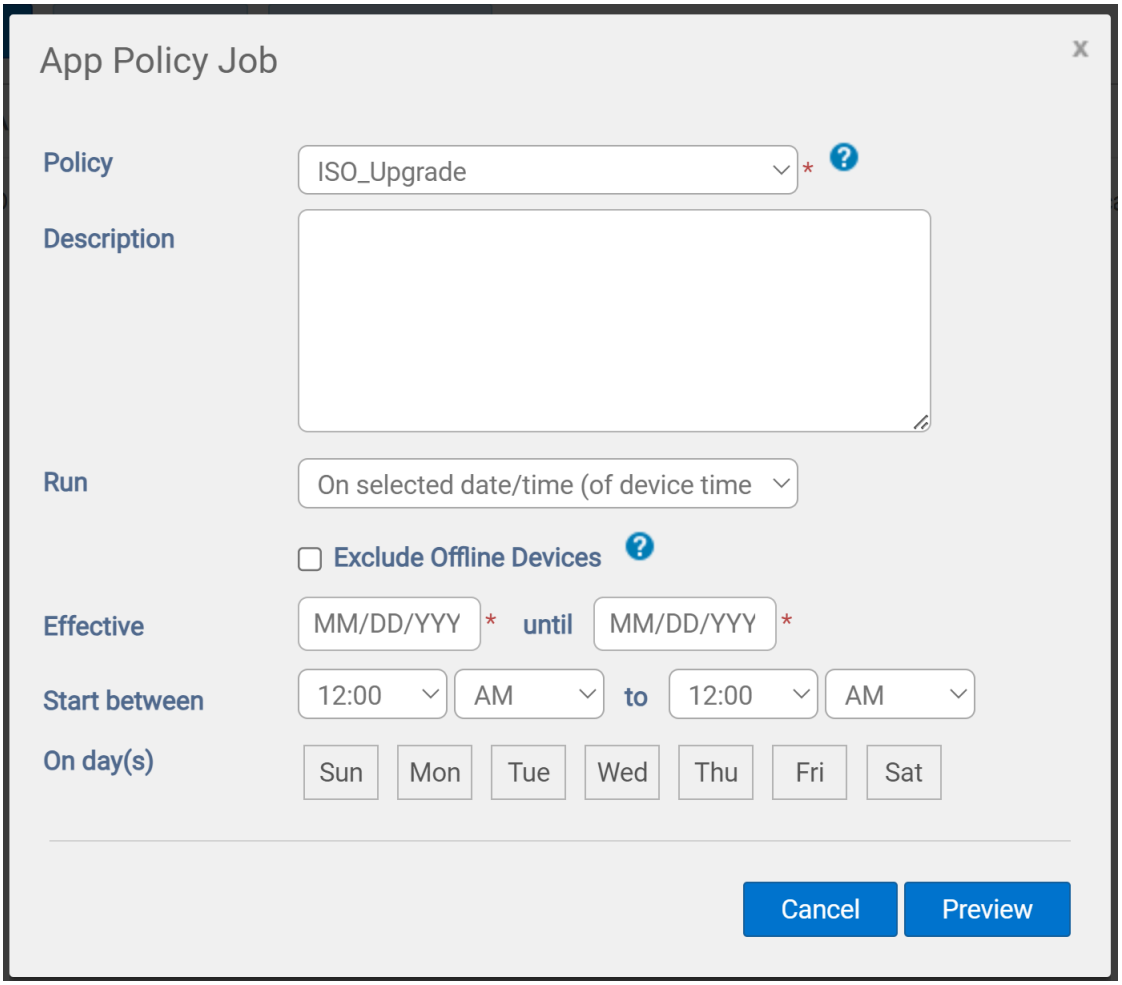


Figure 23. App Policy Job

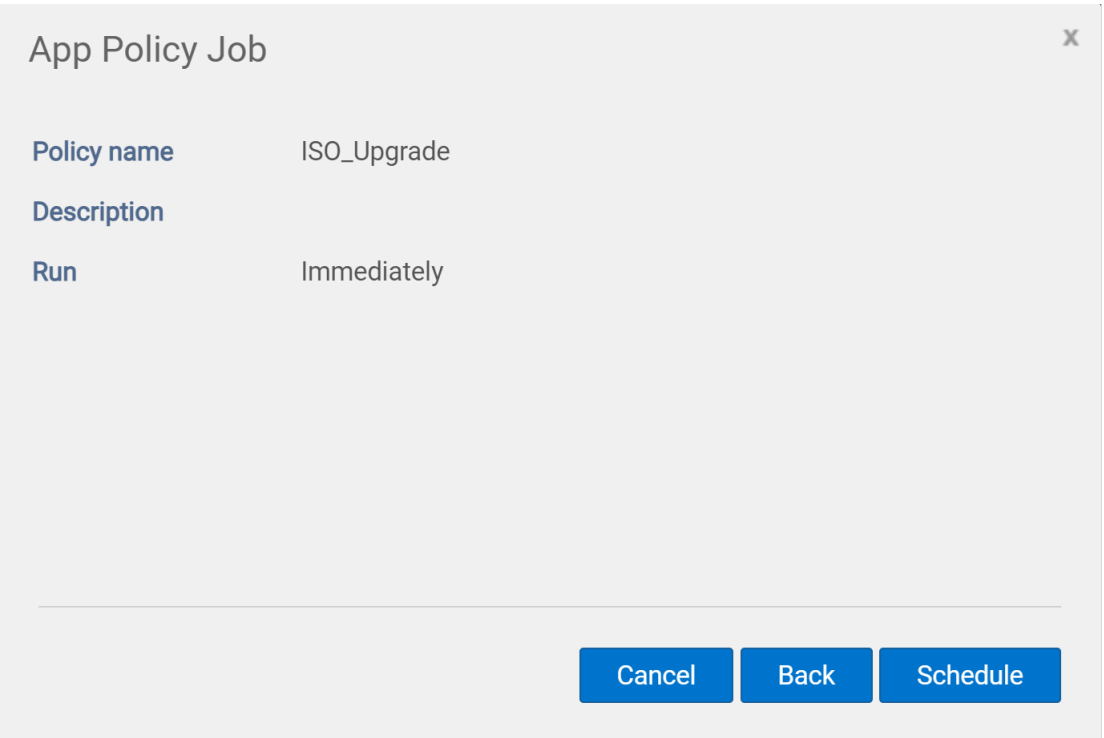


Figure 24. App Policy Job

5. Click **Update Now** when an Update notification is displayed on the device.

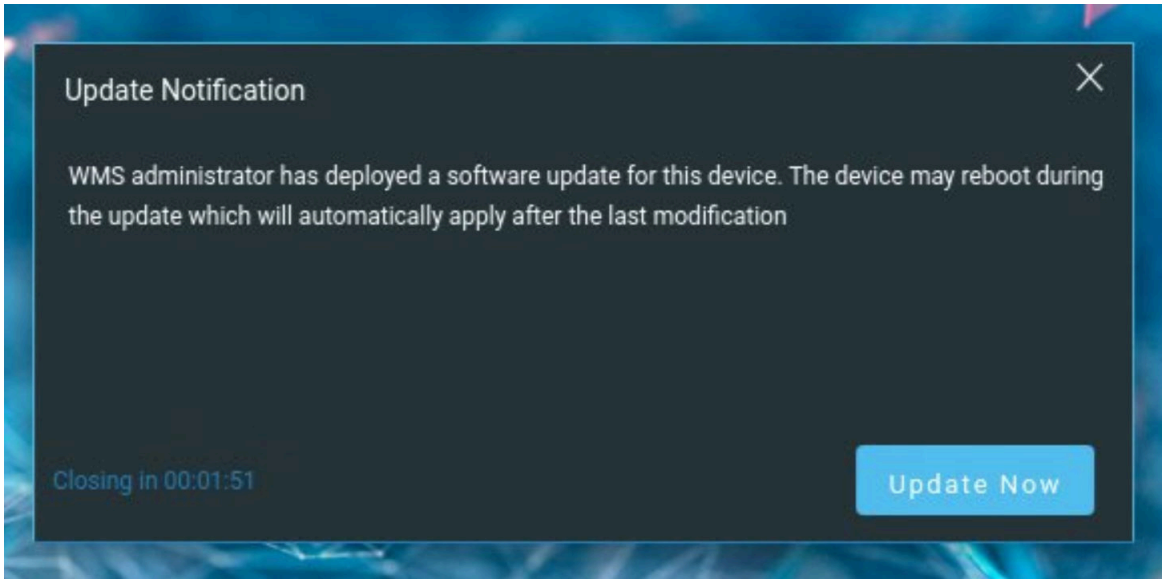


Figure 25. Update Notification

The update process takes around **15 to 20** minutes, after that the device restarts. Once installation is completed, the device redirects you to the **login** screen.

After the upgrade is completed, all the existing addons along with its configuration and User Data is removed.

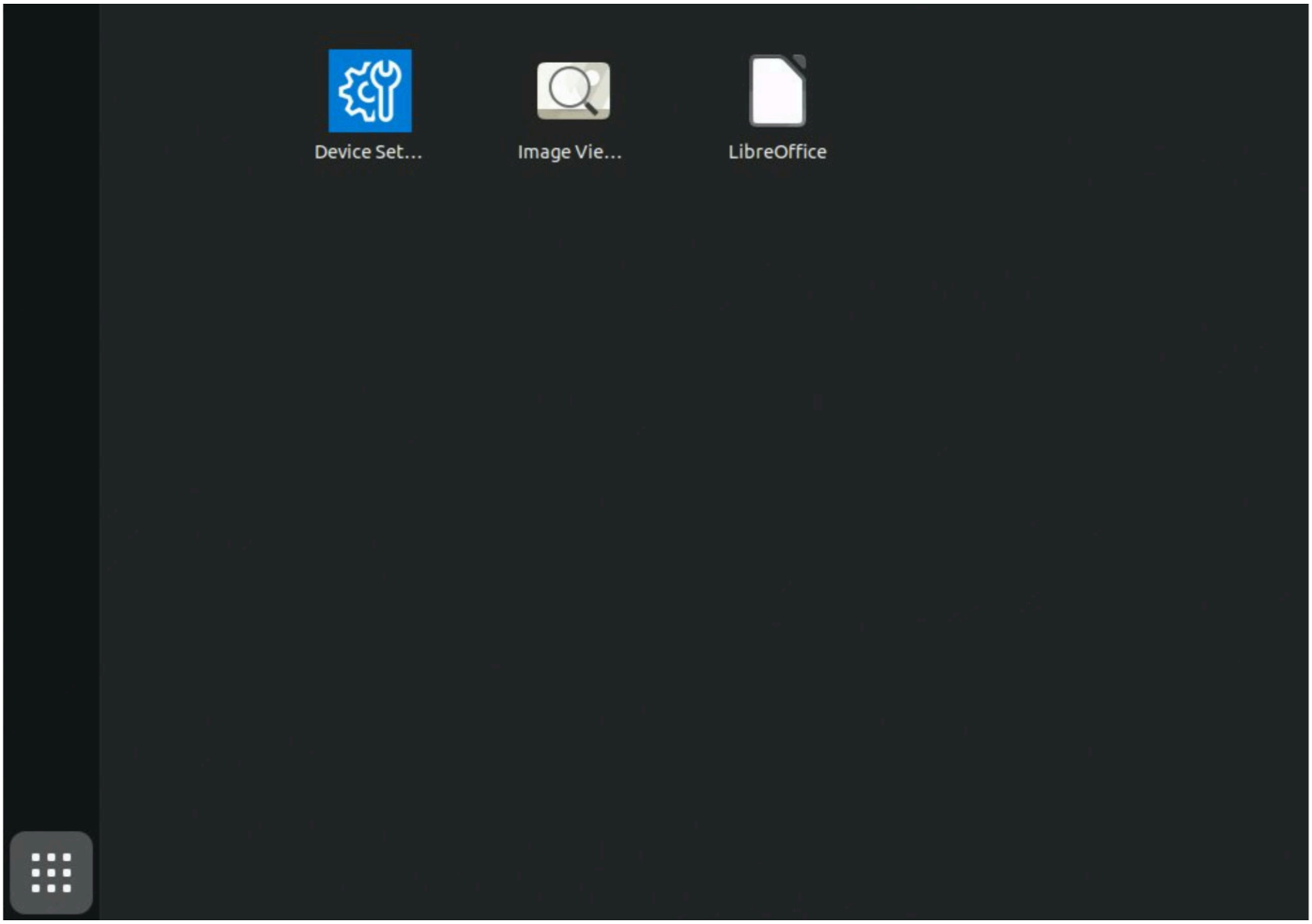


Figure 26. Show Application

You can log in as a guest or configured user.

Verify ISO Upgrade Status

You can verify the ISO Upgrade status in System Information.

Once the ISO is completed, the device redirects you to the **login screen**.

1. Log in into the device.
2. Click **System Information** on the **Top Bar**.
3. Go to the **About** tab and check **DHC Version**. The following image displays the installed **DHC Version**.

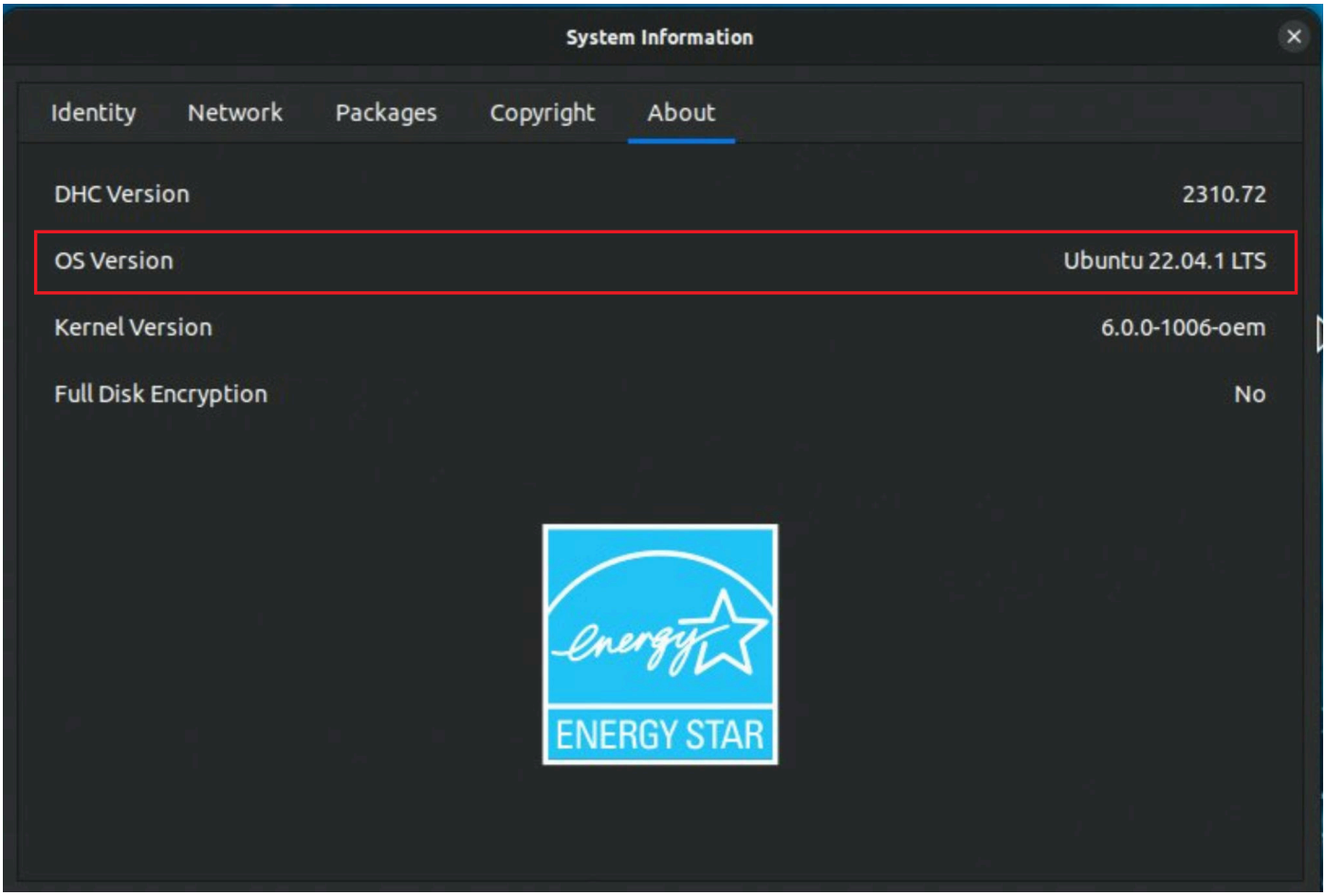


Figure 27. System Information

BIOS Upgrade

You can upgrade BIOS using Wyse Management Suite or manually from the BIOS Setup or command line.

Upgrade BIOS using Wyse Management Suite

You can use Wyse Management Suite to upgrade BIOS.

Prerequisites

- Register your device to Wyse Management Suite and create a group.
- Follow the below steps to download the relevant BIOS file:
  1. Go to the Linux Vendor Firmware Service (LVFS) website at www.fwupd.org.
  2. In the **search for firmware...** search box, enter the device model.
  3. Click your device from the search results to find the latest BIOS file with *.cab* extension.

Steps

1. Log in to Wyse Management Suite using your administrator credentials.
2. Copy the downloaded .cab file to the Wyse Management Suite file repository.

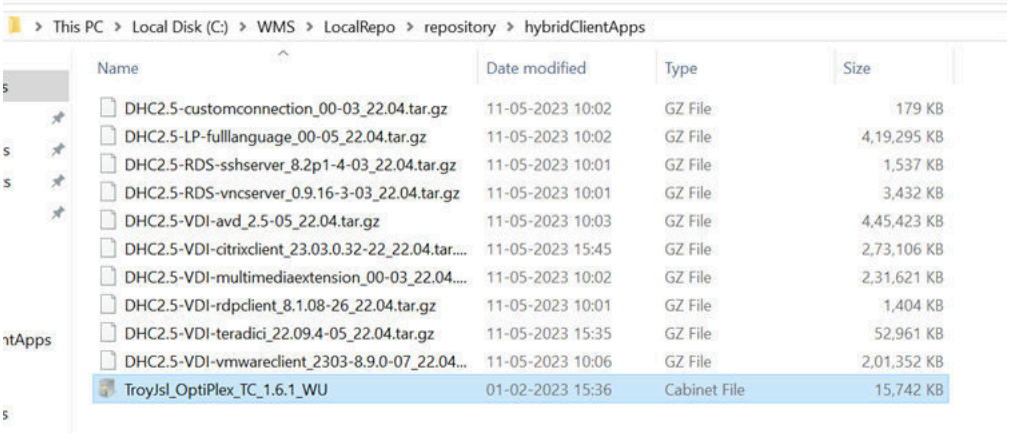


Figure 28. Wyse Management Suite file repository

For example, `C:\WMS\LocalRepo\repository\hybridClientApps` for on premises.

3. In the **Apps & Data tab**, under **App Policies**, click **Dell Hybrid Client**.
4. Click **Add Policy**.

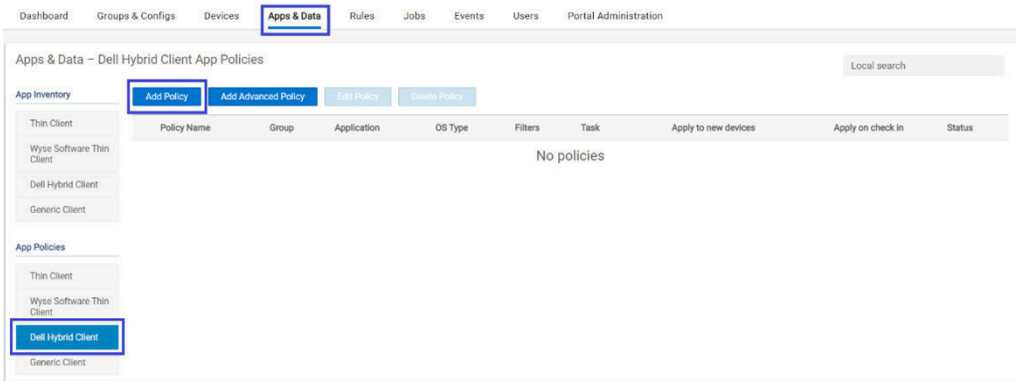


Figure 29. Dell Hybrid Client App Policies

5. Enter the **Policy Name**, select **Group Name**, **Task**, and **OS Type**.
6. From the **Application** drop-down list, select the BIOS file.

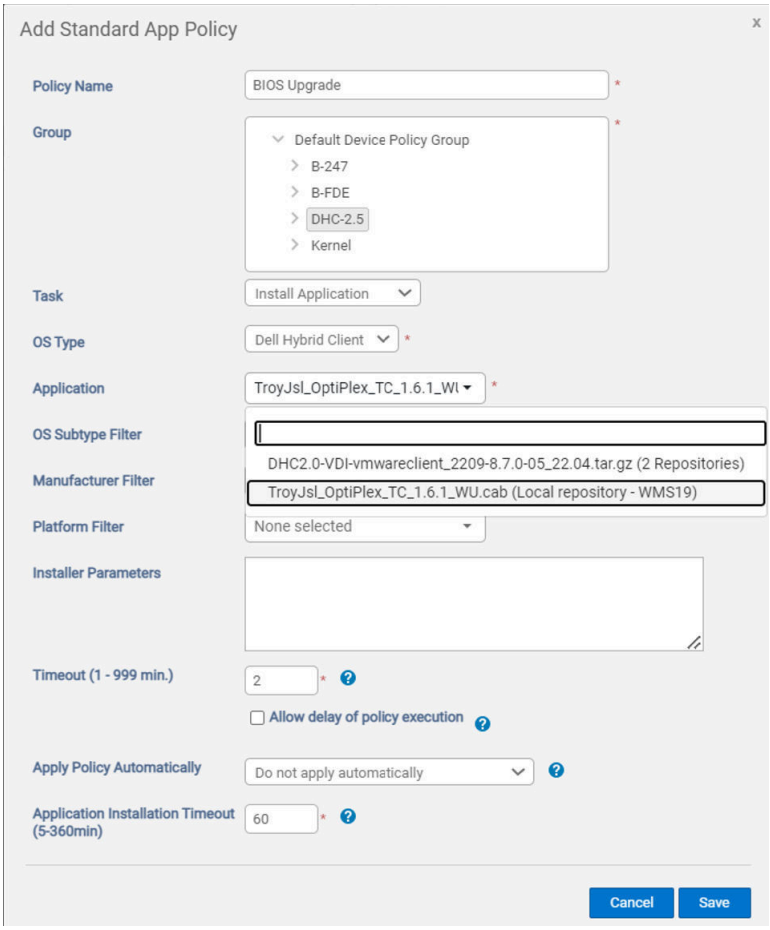


Figure 30. Add Standard App Policy

7. Click **Save**.
8. Schedule the created App policy job to the applicable device or device group.
   On the device, the **Update Now** message is displayed.

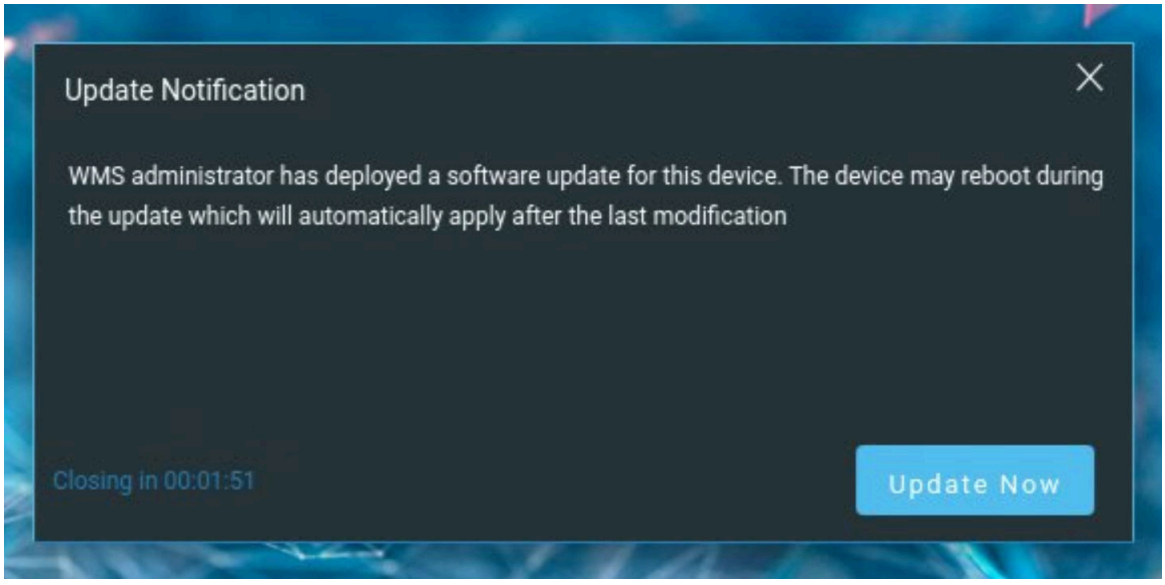


Figure 31. Update Notification

9. Click **Update Now**.
   After the BIOS is downloaded successfully, the device restarts and updates the BIOS automatically.

Upgrade BIOS Manually from BIOS Setup

You can use BIOS Update or BIOS Flash Update - Remote to upgrade BIOS manually from BIOS Setup.

BIOS Update

You can use BIOS Update to upgrade BIOS manually.

Prerequisites

1. Download the latest BIOS from the Dell Support page.
2. BIOS file (.exe) is downloaded and you can copy the file to a pen drive.

Steps

1. Connect the pen drive to the device.
2. Reboot the device and go to **Boot menu** by pressing **F12** in post screen.
3. Click **BIOS UPDATE**.

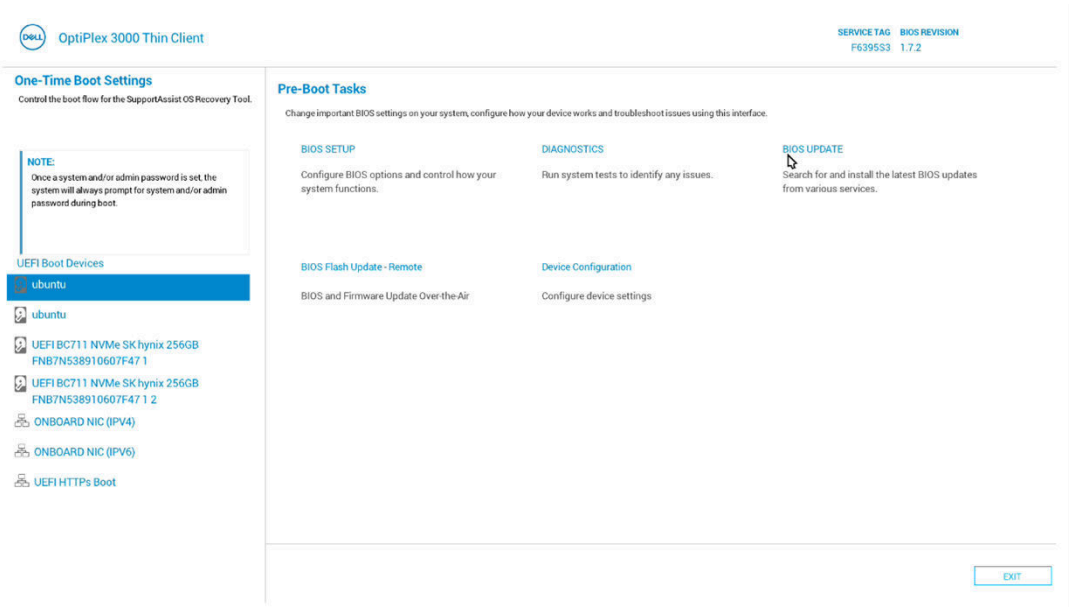


Figure 32. Pre-Boot Tasks

4. In the Flash BIOS page, click **Flash from file**.
5. Select a BIOS file from the Pen drive in the File Explorer window and click **Submit**.

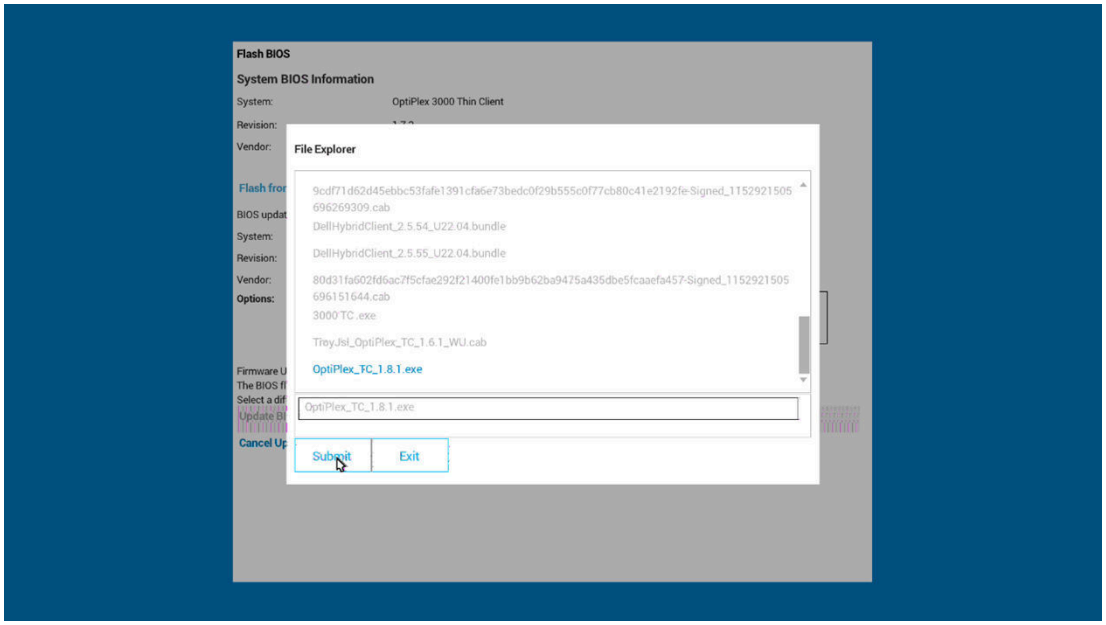


Figure 33. File Explorer

6. Click **Update BIOS**.

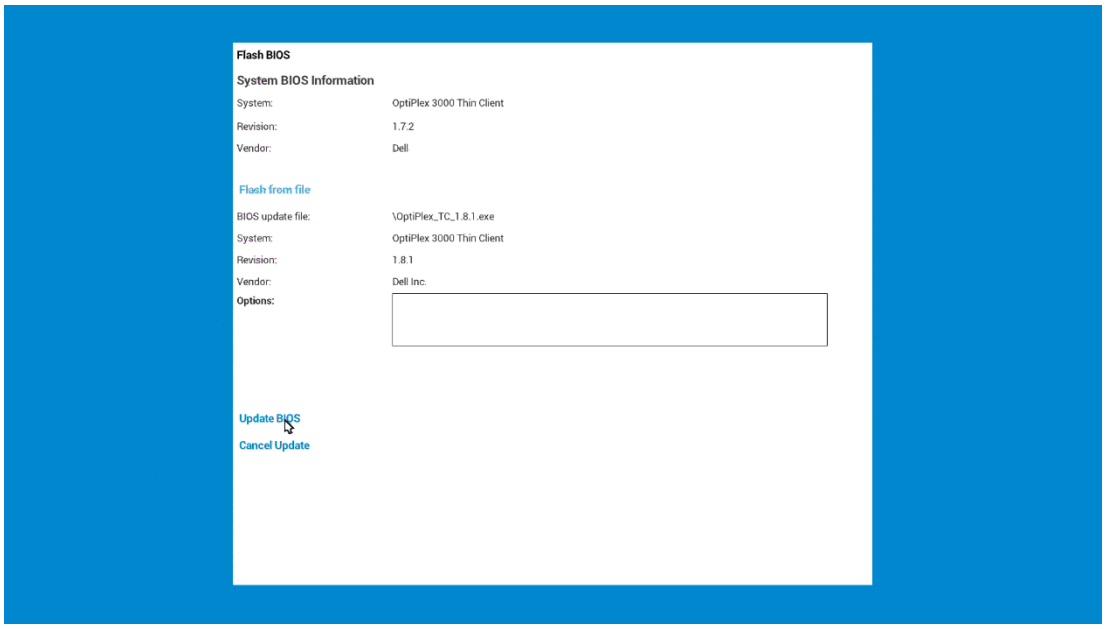


Figure 34. Flash BIOS

BIOS Flash Update - Remote

You can use BIOS Flash Update - Remote to upgrade BIOS manually.

Prerequisites

- The device must be connected to the network.

Steps

1. Reboot the device and go to **BOOT Manager** by pressing **F12** in post screen.

2. Click **BIOS Flash Update - Remote**.

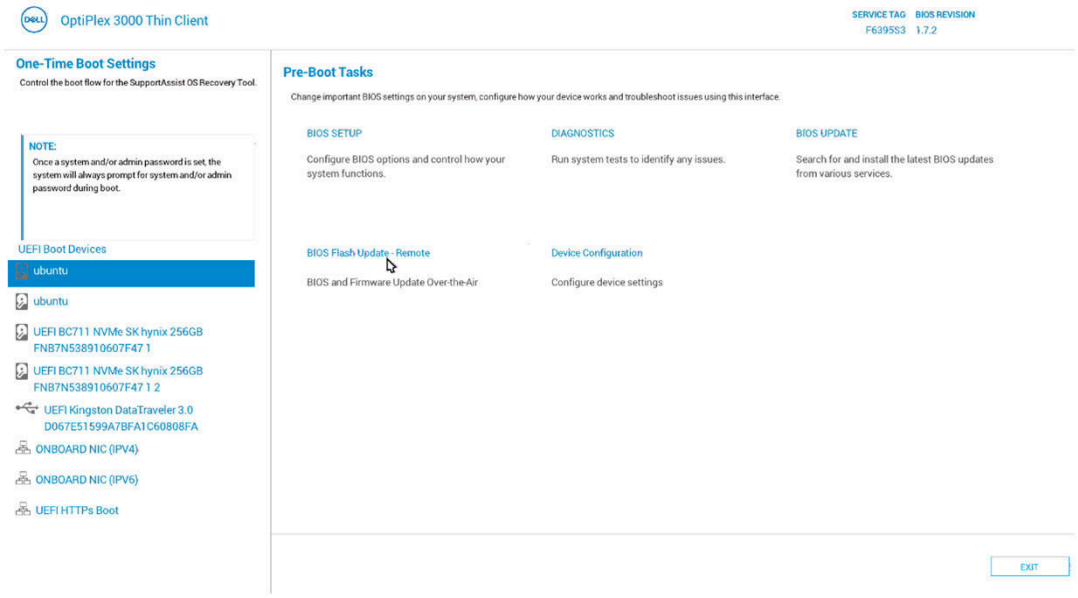


Figure 35. Pre-Boot Tasks

3. Once the connection check is done, then click **Update BIOS**.
The device checks the latest BIOS available and downloads the BIOS automatically.

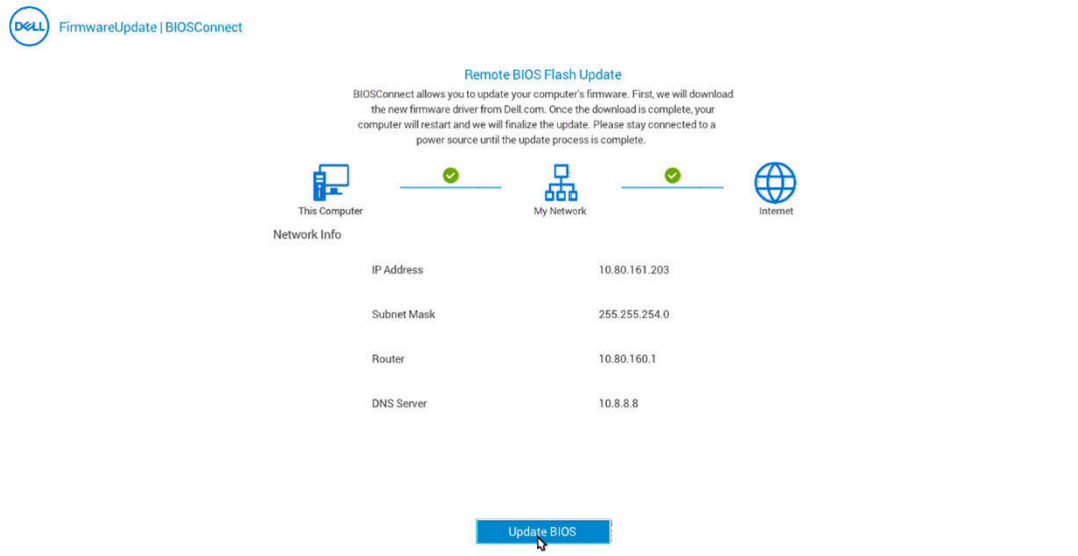


Figure 36. Remote BIOS Flash Update

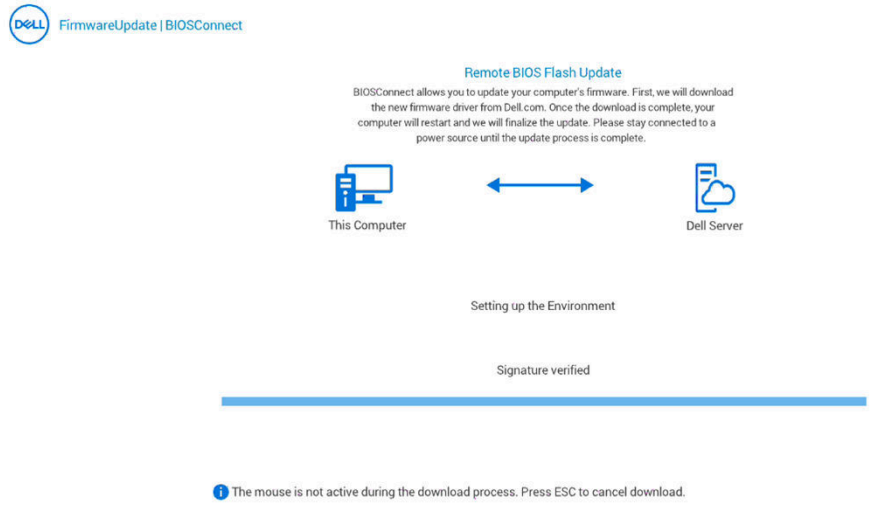


Figure 37. Remote BIOS Flash Update

4. The **latest BIOS** version available message is displayed, Click **Yes** to update the BIOS.

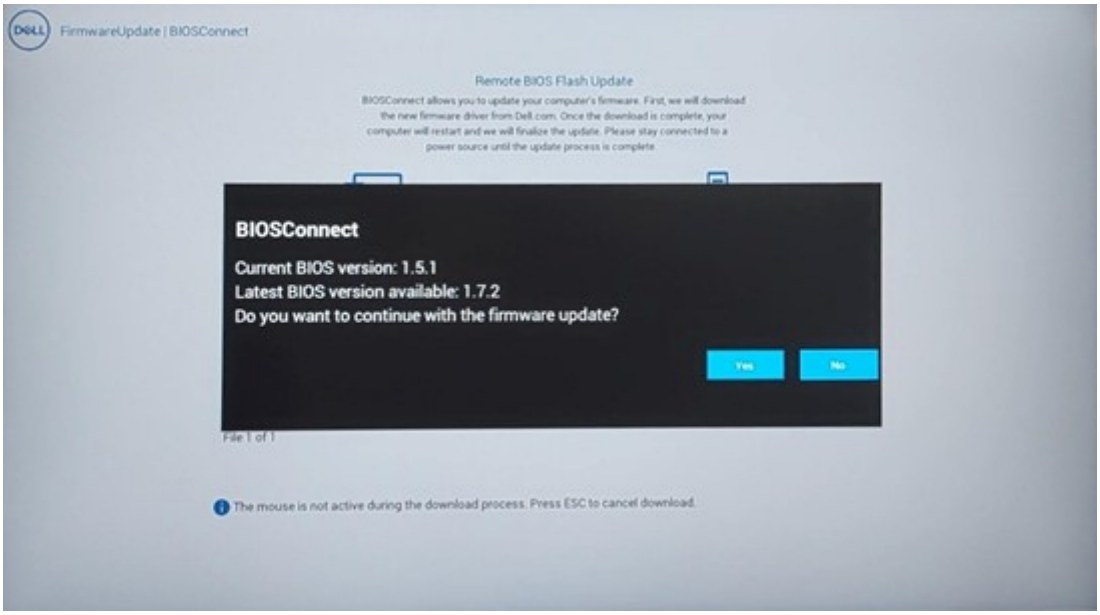


Figure 38. BIOSConnect

The device restarts after downloading the BIOS and starts updating the BIOS or firmware.

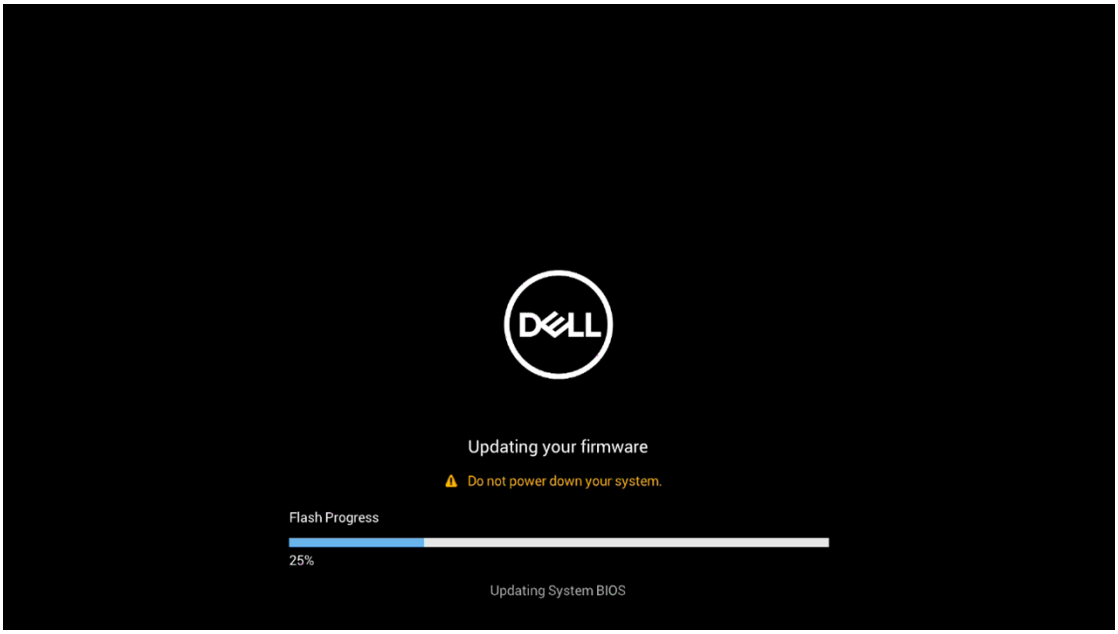


Figure 39. Updating System BIOS

Upgrade BIOS manually from command line

You can use command line to upgrade BIOS manually.

Steps

1. Download the **BIOS file (.cab)** from service provider website.
2. Open the terminal and go to BIOS file location and run below commands with root user privileges.
   fwupdmgr install filename.cab

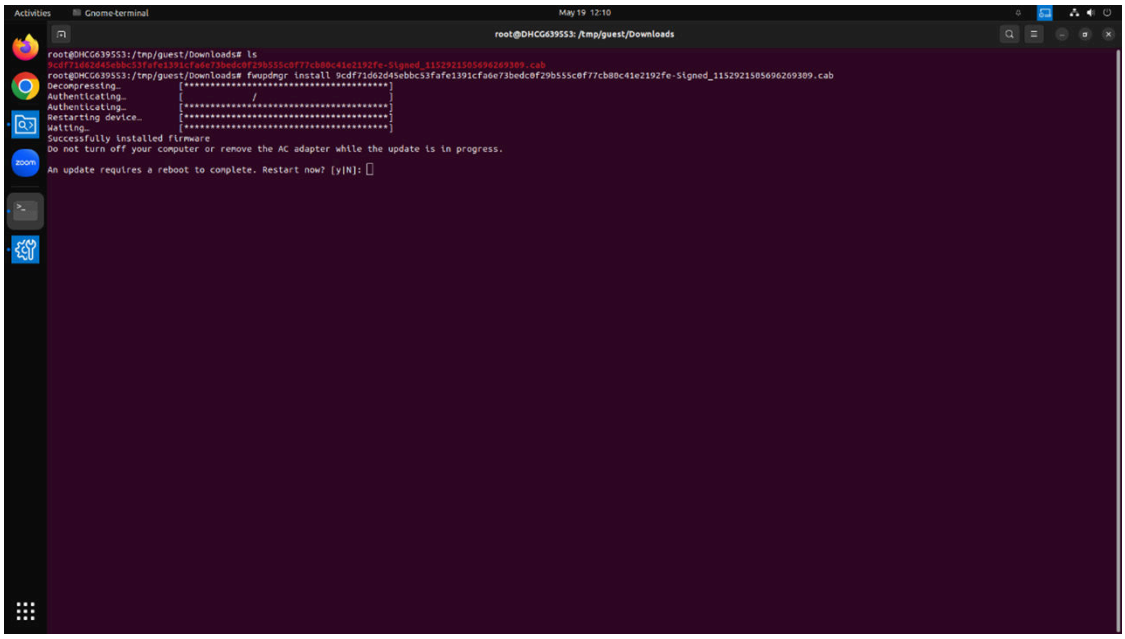


Figure 40. Terminal

3. Press the **y** key to reboot the device.
   The device restarts and starts updating the BIOS automatically.

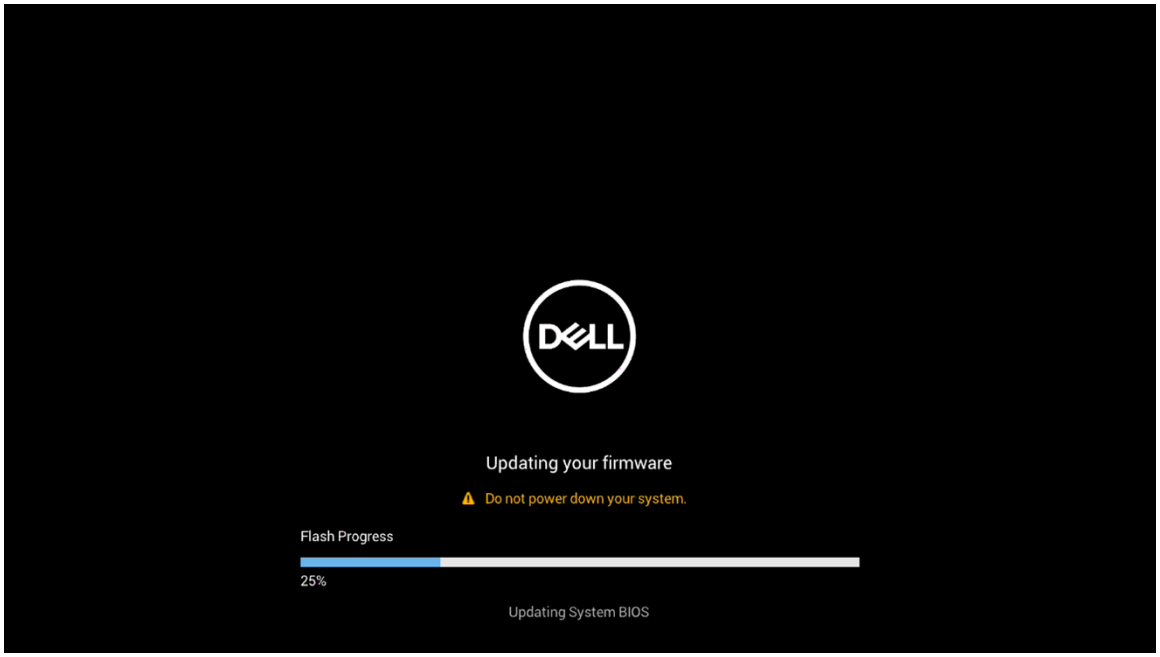


Figure 41. Updating System BIOS

3

Registering Dell Hybrid Client to Wyse Management Suite

End User License Agreement and First Boot setup Wizard

Displays for the following scenarios

When you boot the device for the first time or when you send **Factory Reset** command from Wyse Management Suite, the following windows are displayed for below scenarios:

- When Auto Discovery (DHCP\DNS) is configured and End User License Agreement is accepted in Wyse Management Suite, the user gets End User License Agreement and it will be automatically accepted without displaying the First Boot Wizard window to the user.
- When Auto Discovery (DHCP\DNS) is configured and End User License Agreement is not accepted in Wyse Management Suite, End User License Agreement is displayed to the user and First Boot Wizard Window is not displayed.
- When Auto Discovery (DHCP\DNS) is not configured or Auto Discovery fails, End User License Agreement screen is displayed. Once the user accepts the End User License Agreement, First Boot Wizard window is displayed.

End User License Agreement

Steps

1. The following is the first screen which is displayed when you access **Dell Technologies End User License Agreement (EULA)** . Select **View EULA in English** option from this dialogue box.



Figure 42. End User License Agreement

2. In the next window, select **I agree to the Terms and Conditions** check box and click **Agree**.

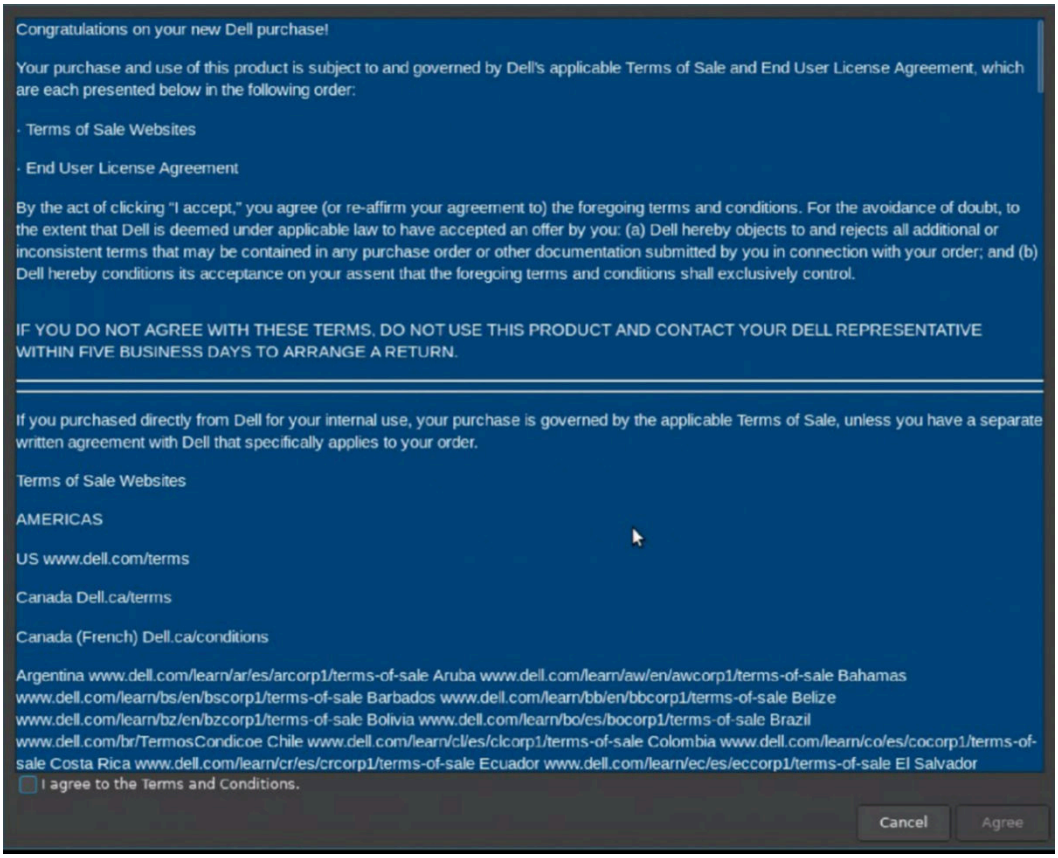


Figure 43. Terms and Conditions

Dell Hybrid Client Setup Wizard

About this task

First Boot Wizard application runs for the first time when you start a device with Dell Hybrid Client. The device starts the setup Wizard application before you enter the Dell Hybrid Client desktop. Use this application to perform tasks, such as configuring system preferences, setting up the network connectivity, and Management Server connectivity.

Steps

1. Once EULA accepted Dell Hybrid Client Setup Wizard, the page will start as shown in below figure.

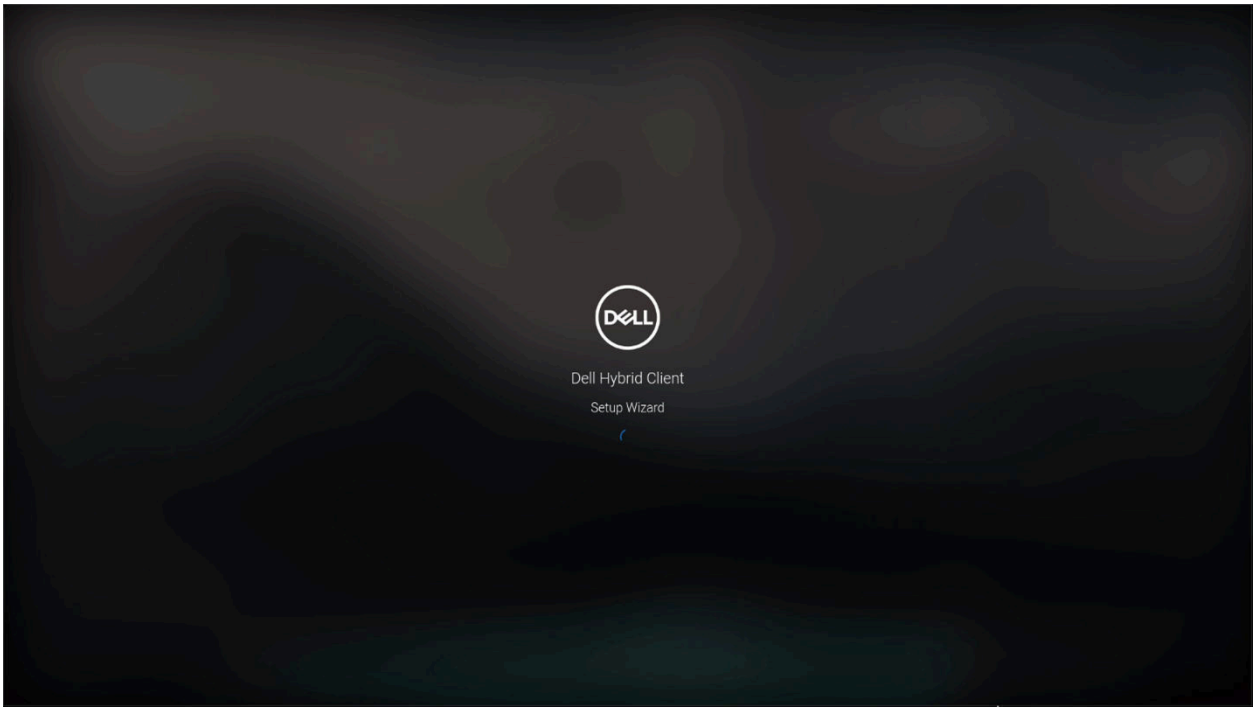


Figure 44. Setup Wizard

2. Do not change default values and click on **Save and Continue**.

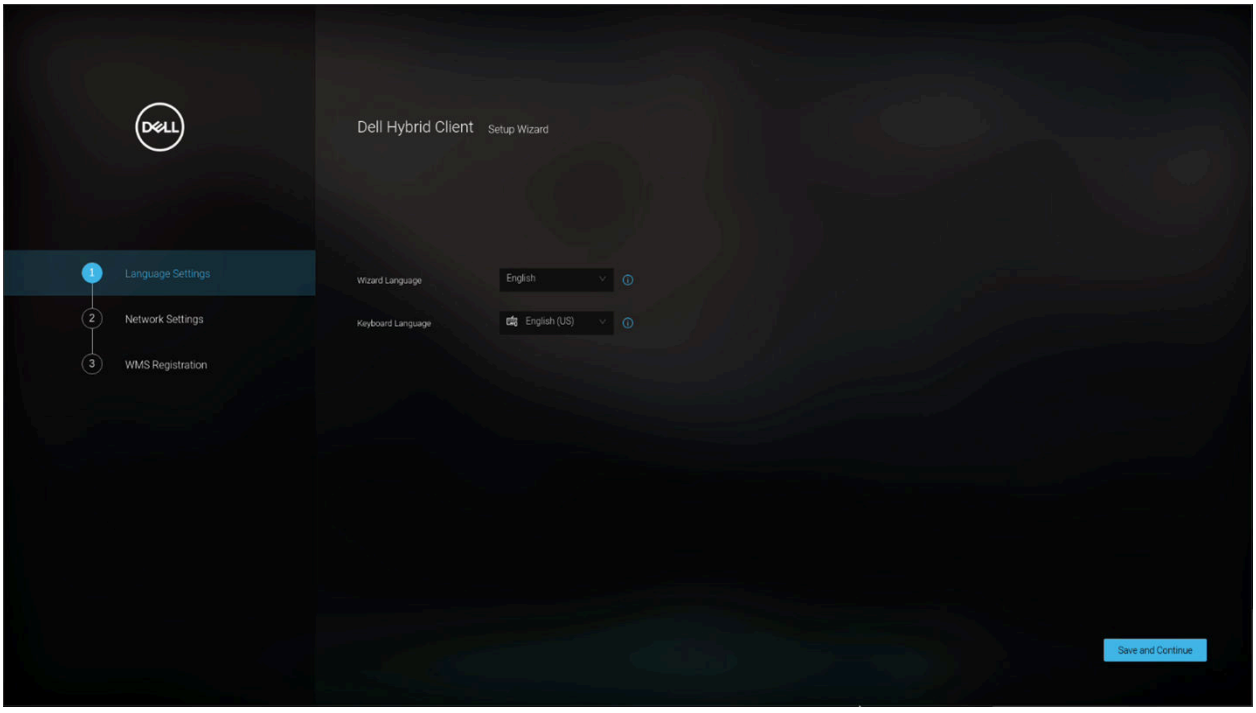


Figure 45. Language Settings

3. The next step is to configure network as shown in below figure

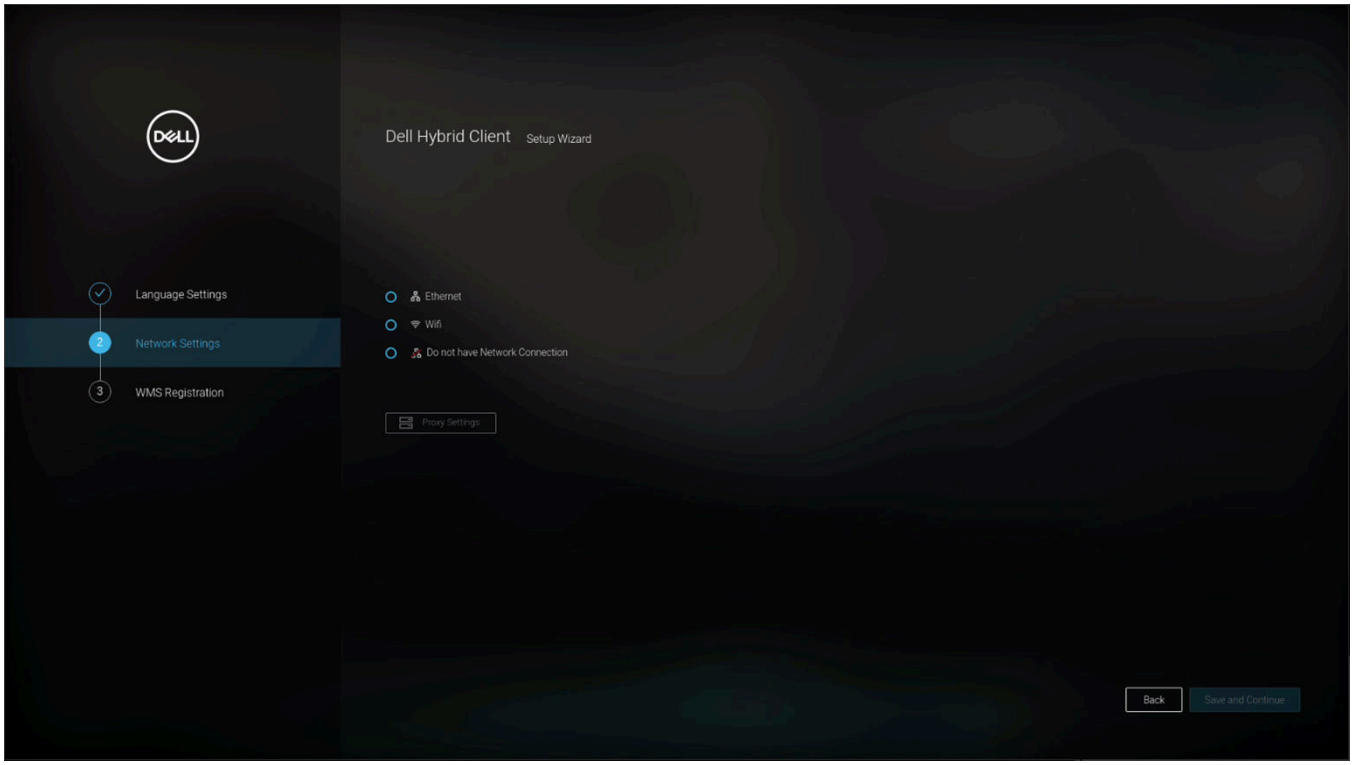


Figure 46. Network Settings

Configuring Ethernet and Wyse Management Suite registration

When connected to the wired LAN ethernet, clicking on the **Ethernet** radio button on the screen will display connected local area network connections.

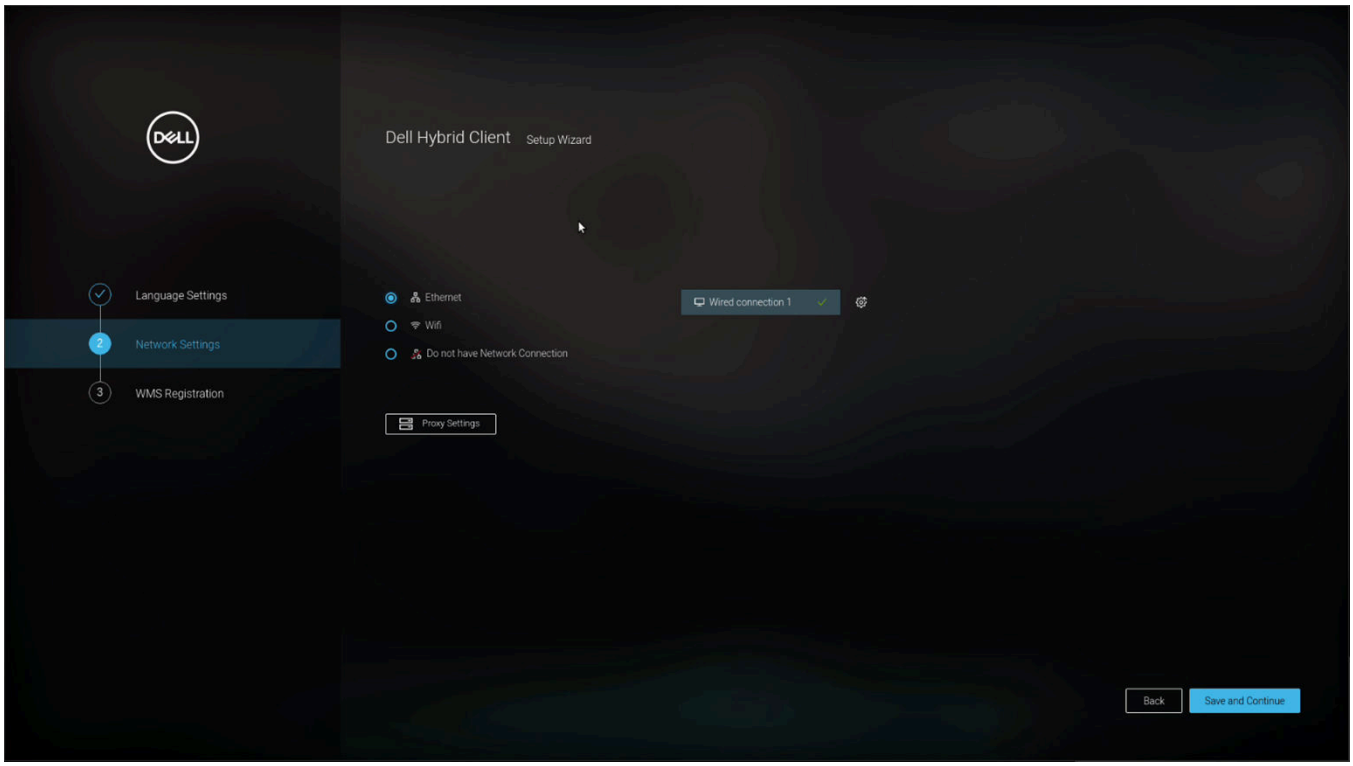


Figure 47. Network Settings

If there is no active LAN connection, **No active Ethernet connection found** is displayed upon clicking Ethernet radio Button.

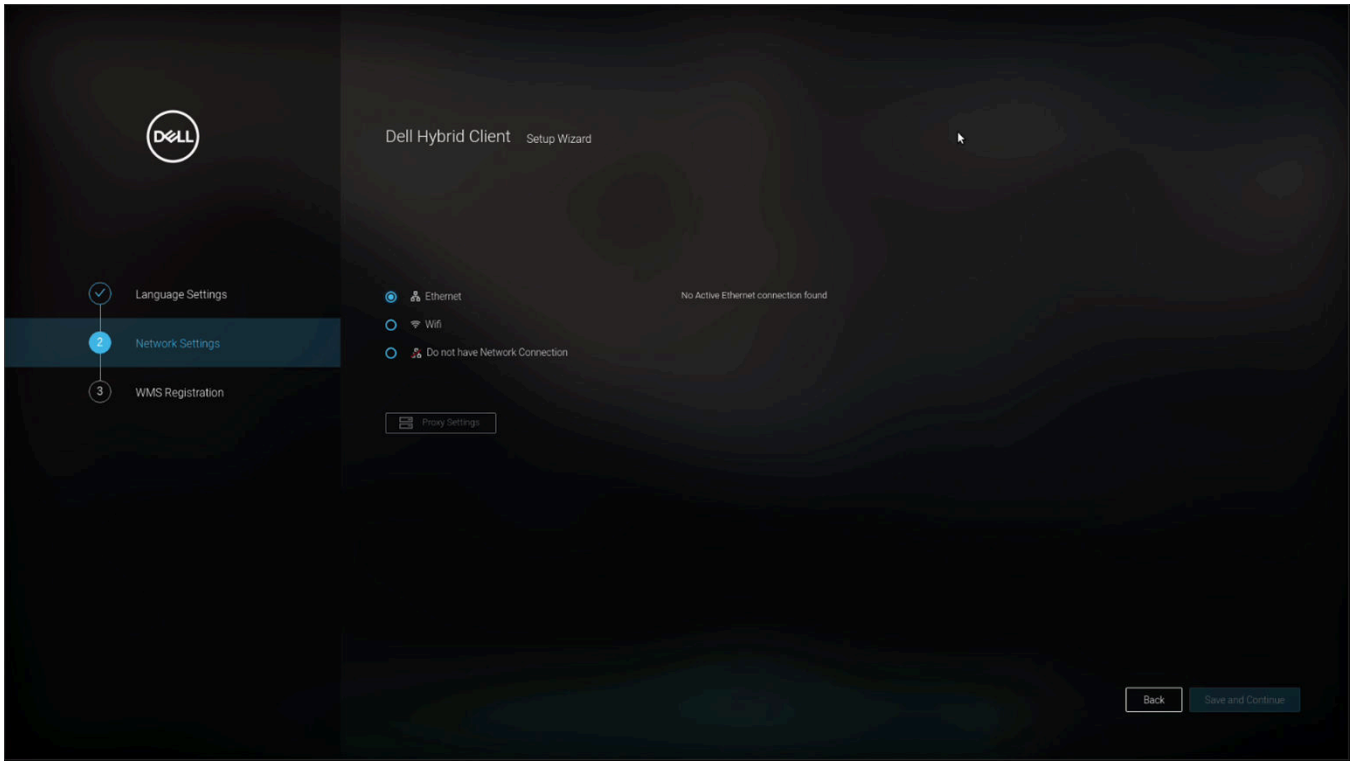


Figure 48. No active Ethernet connection found

If active LAN is connected, clicking on **Settings** button should expands **Additional Network Settings**.

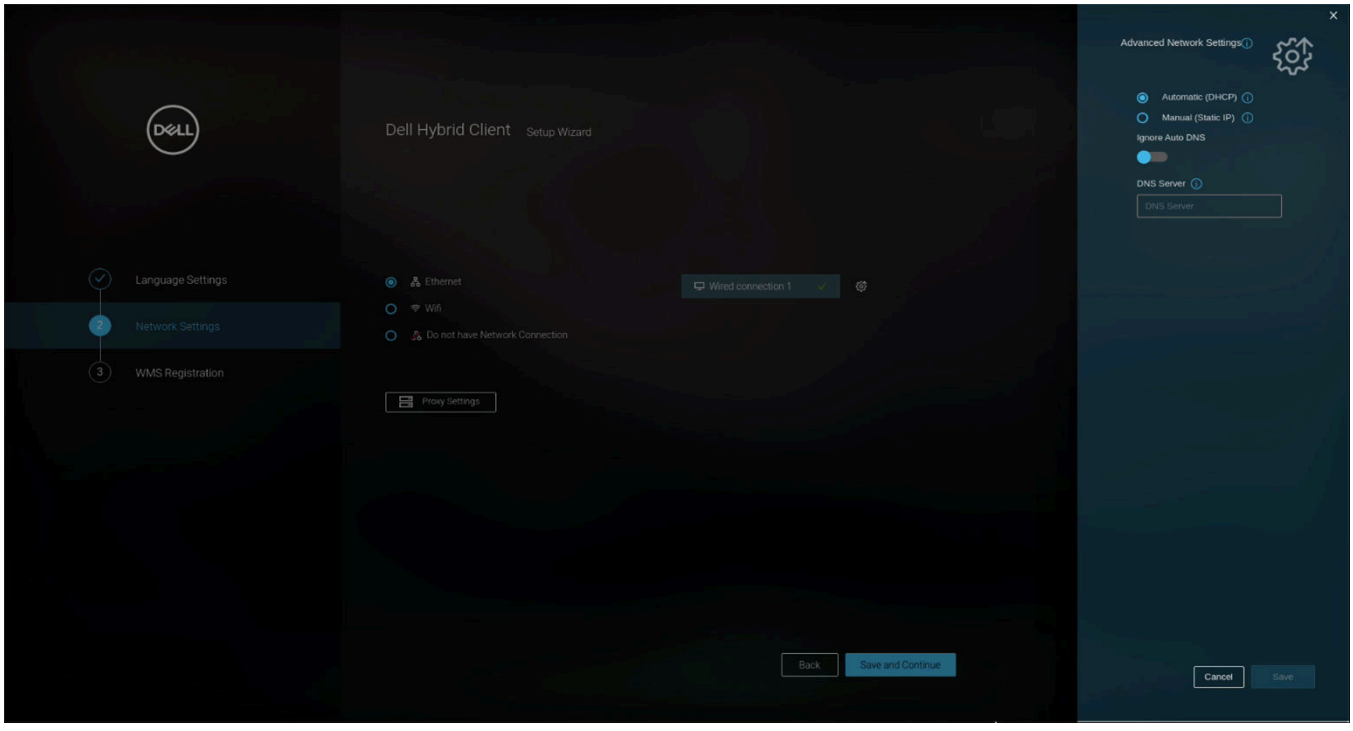


Figure 49. Additional Network Settings

In **Advance Settings**, user can select **Automatic (DHCP)** or **Manual (Static IP)** and also DNS can be configured.

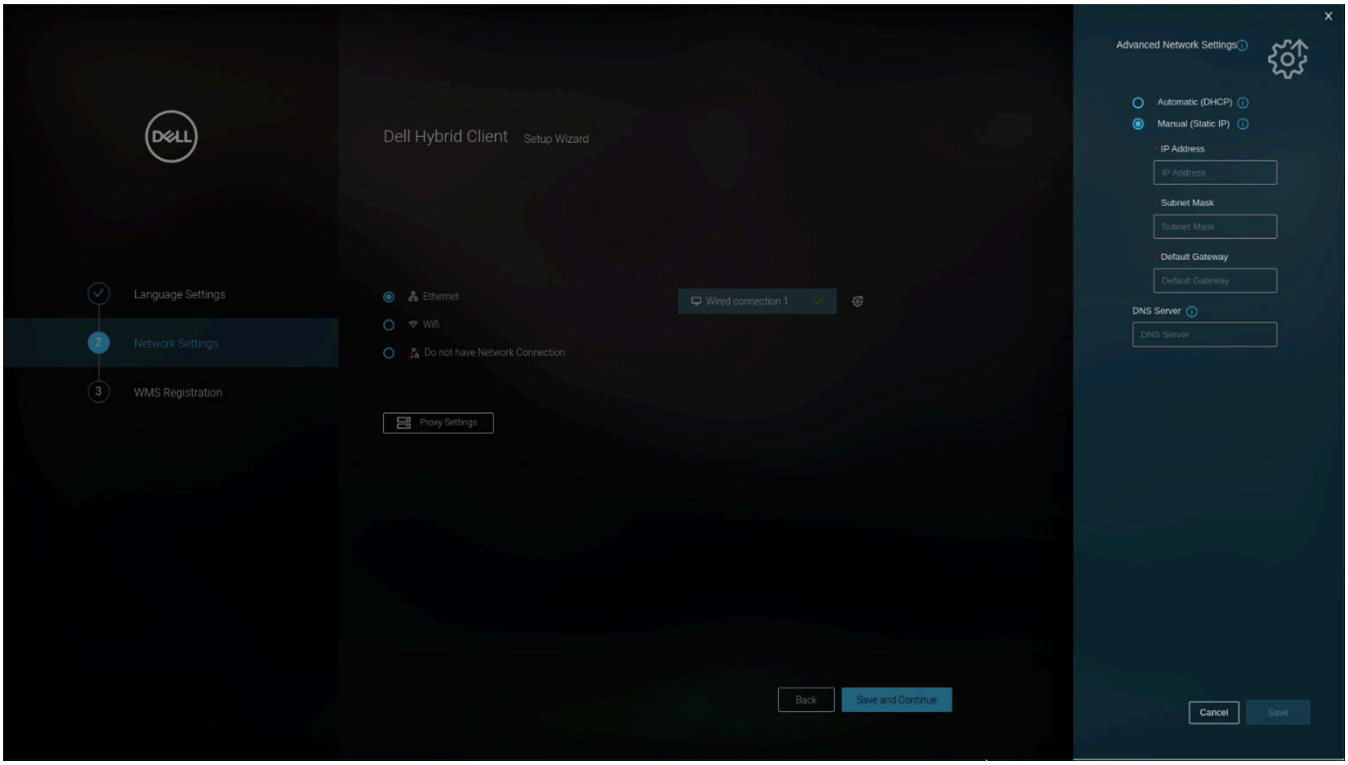


Figure 50. Advance Settings

User can configure proxy by clicking **Proxy Settings**. User can configure **Proxy server address** and **Port**.

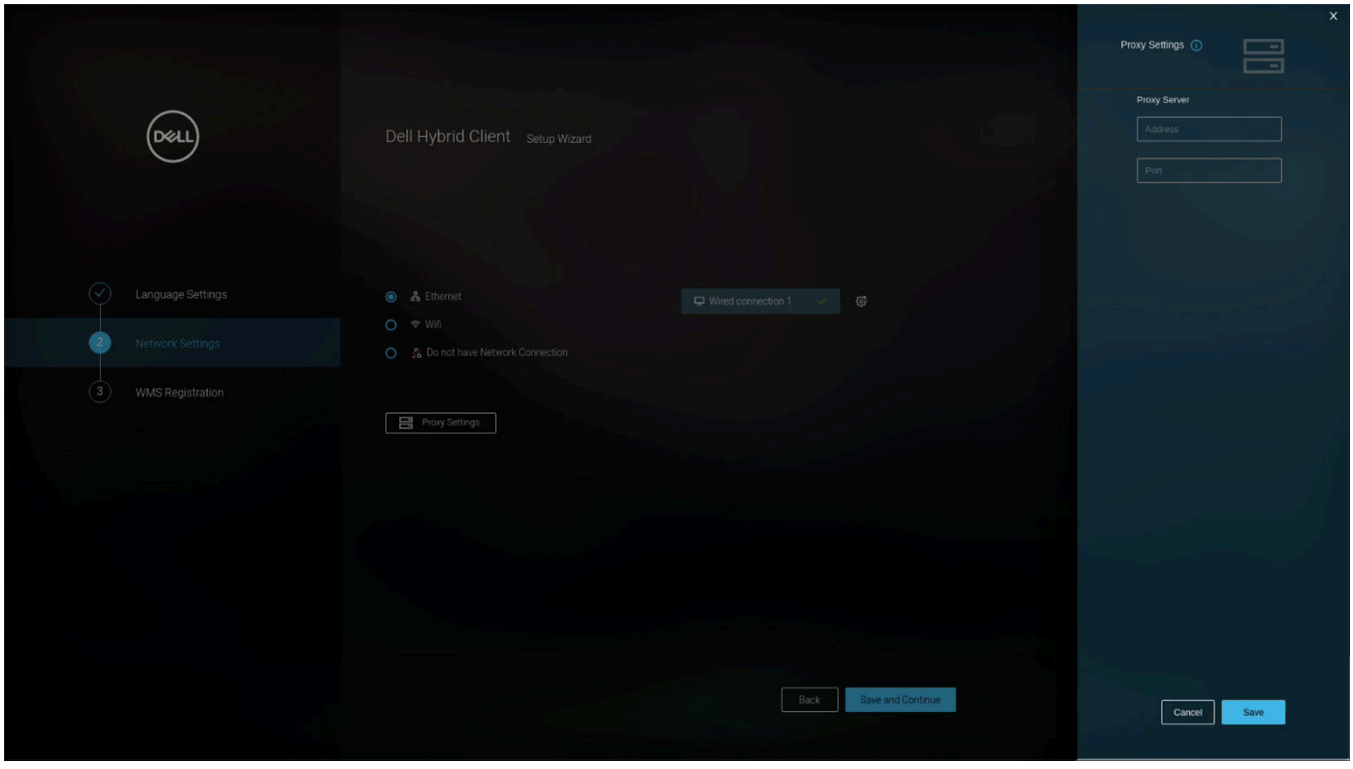


Figure 51. Proxy Settings

Click **Save and Continue**, Setup Wizard will continue to Wyse Management Suite registration page.

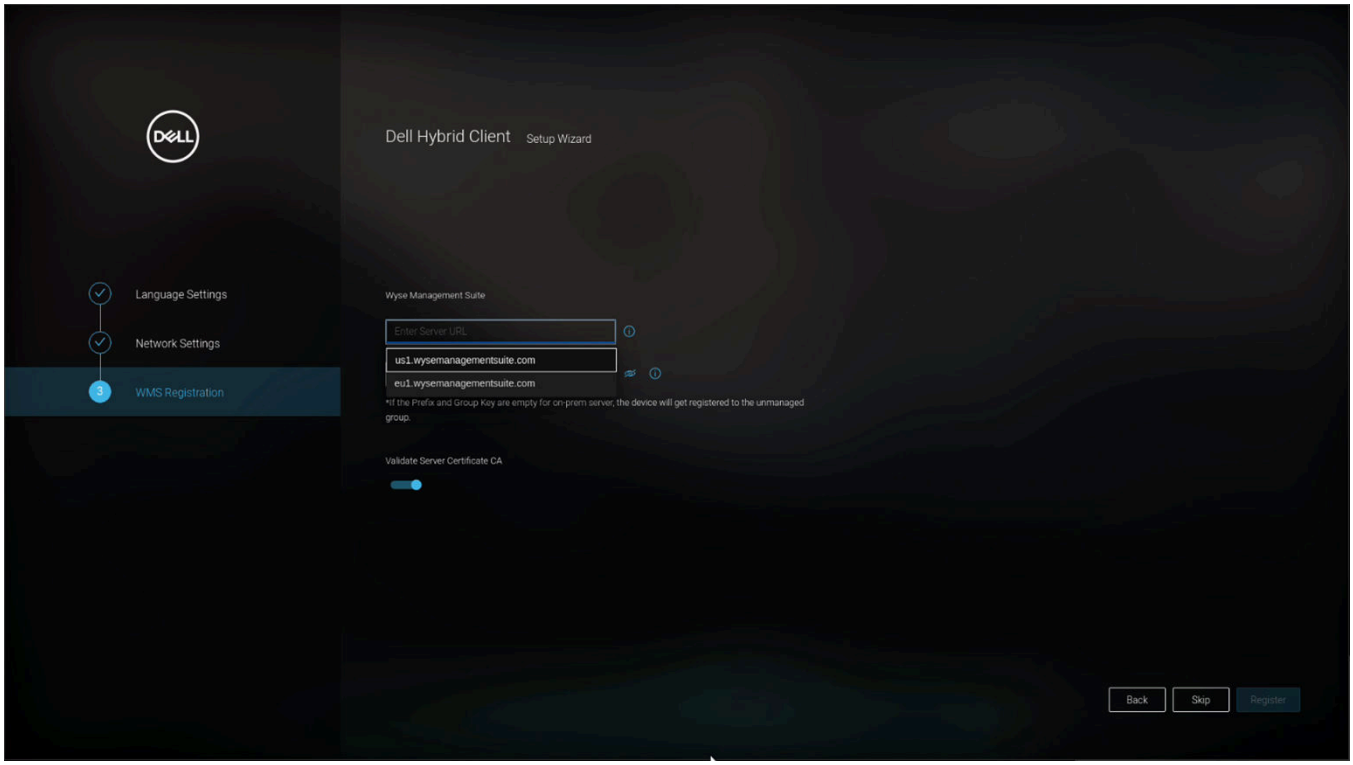


Figure 52. Save and Continue

Click on **Skip** button and device will continue to **Guest login** (Auto login to be done on first boot).

Configuring Wi-Fi and WMS Registration

About this task

If you want to configure Wi-Fi network, follow steps that are given below:

Steps

1. If you select **Wi-Fi** option, a list of all available wireless networks is displayed.

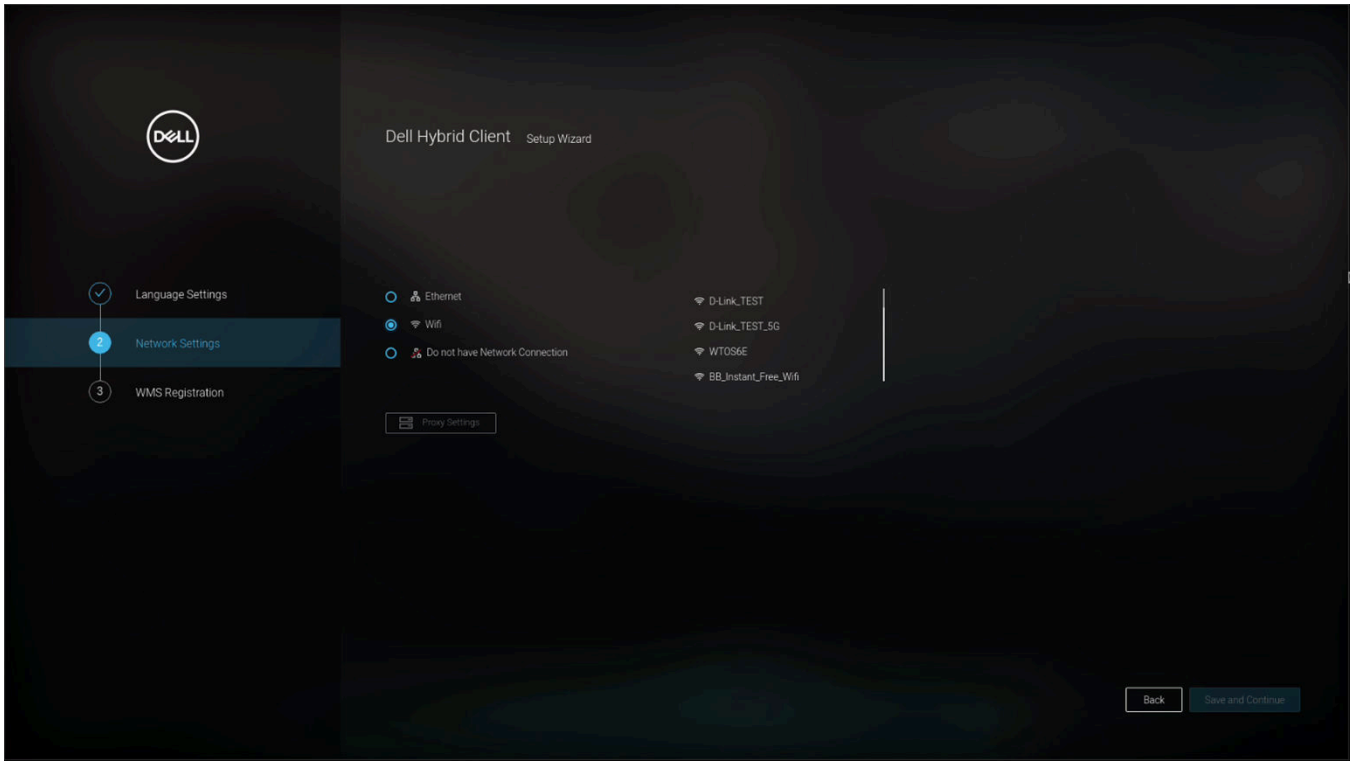


Figure 53. Wi-Fi

2. After clicking on Wi-Fi, screen will prompt for **Wi-Fi credentials**.

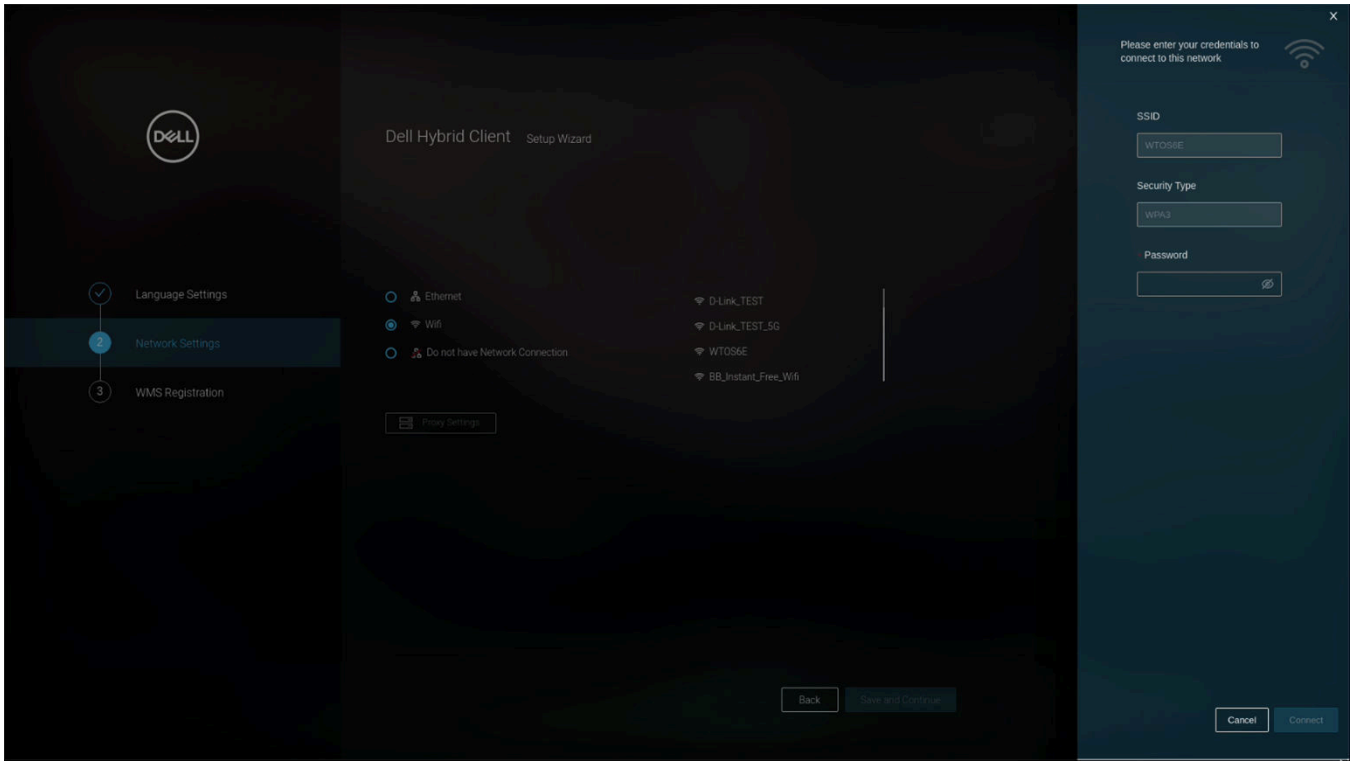


Figure 54. Wi-Fi credentials

3. User can configure proxy by clicking **Proxy Settings**. User can configure **Proxy server address** and **Port**.

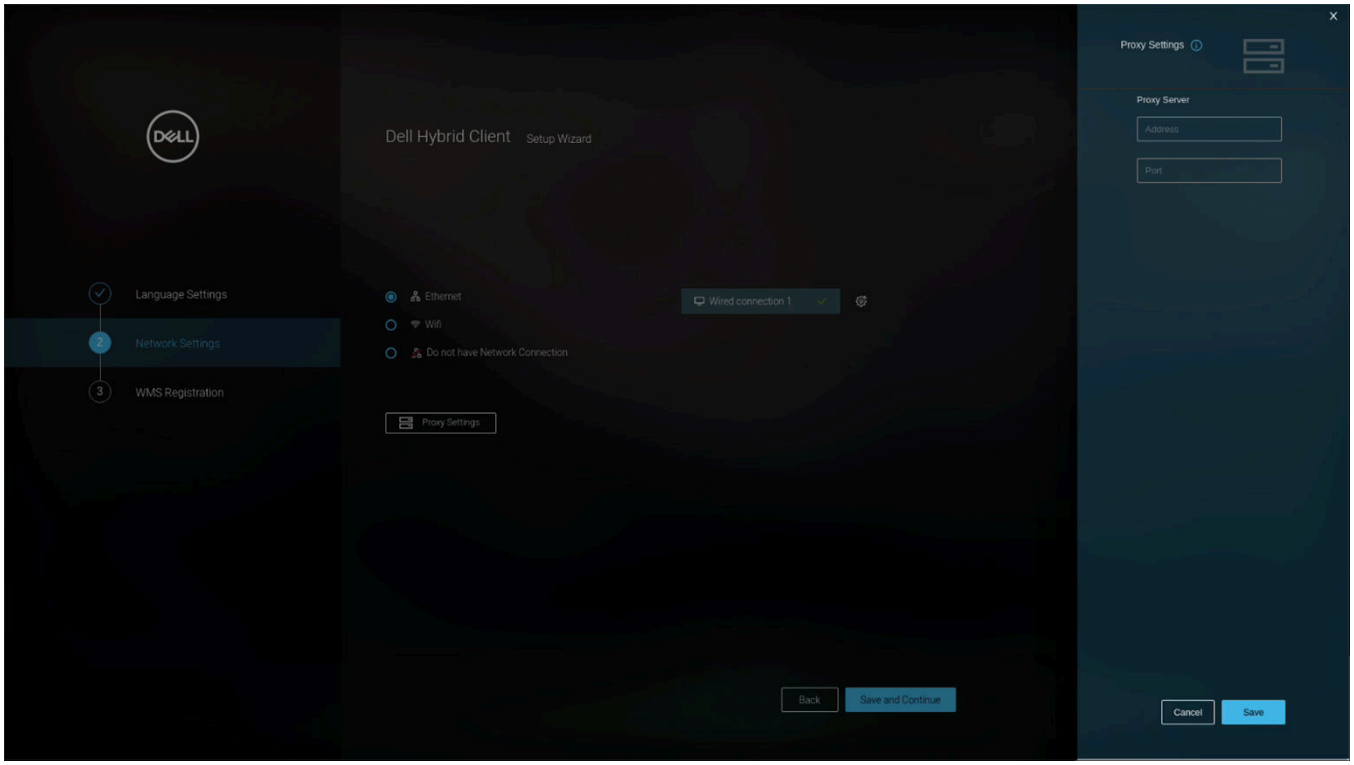


Figure 55. Proxy Settings

4. After entering the credentials, click **Setting icon**. It should expand **Additional Network Settings** as shown in the figure below.

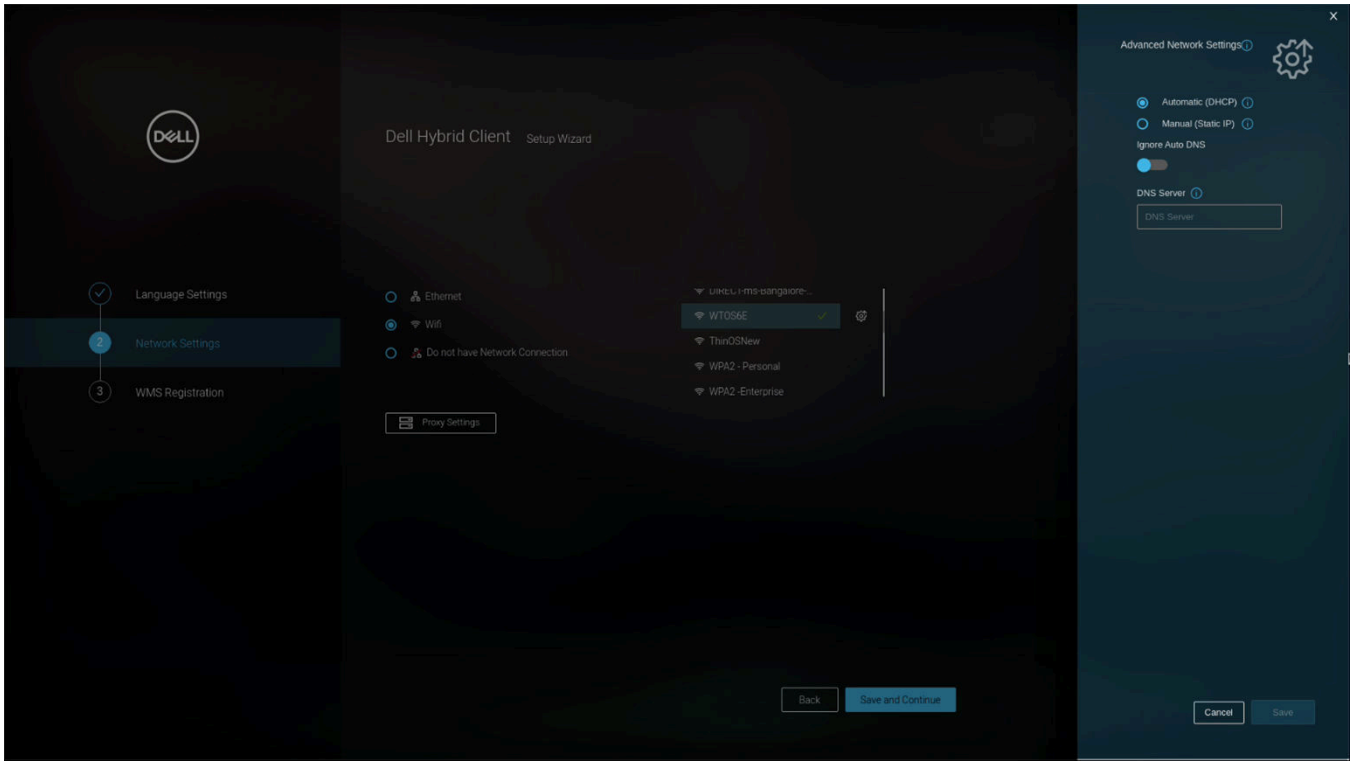


Figure 56. Additional Network Settings

5. In Advance Settings, user can select **Automatic (DHCP)** or **Manual (Static IP)**. DNS can also be configured as shown in the figure below.

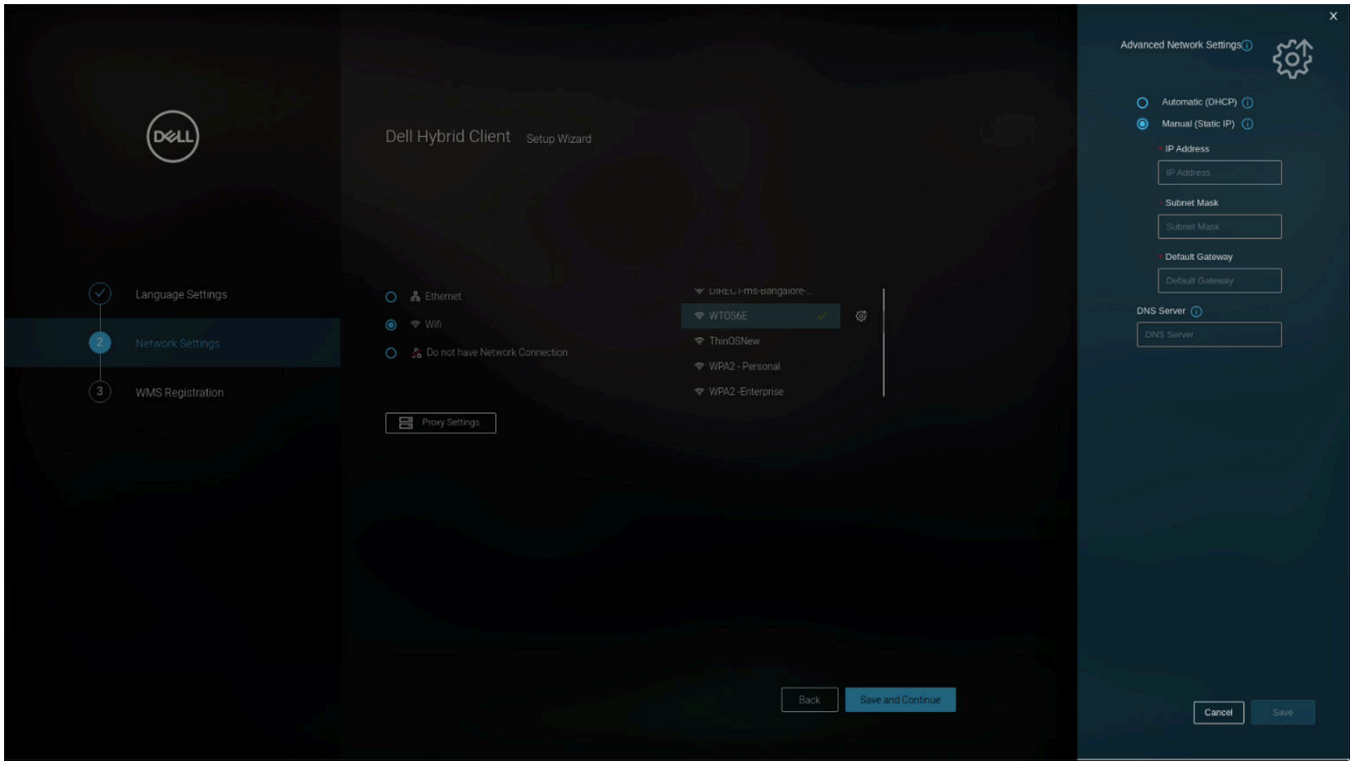


Figure 57. Advance Settings

6. Click **Save and Continue**, Setup Wizard goes to WMS Registration page as shown in the figure.

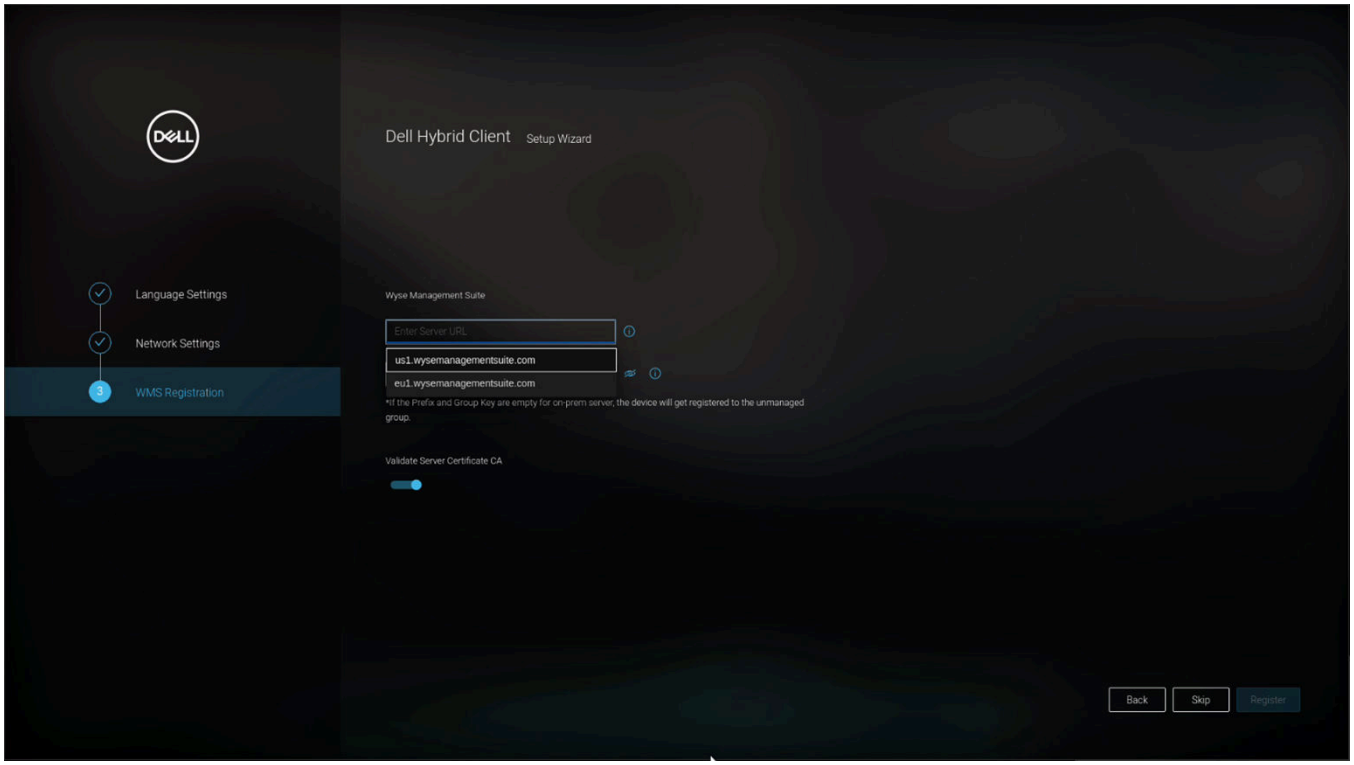


Figure 58. WMS Registration page

The device will go to Guest login (Auto login on first Boot) after clicking **Skip**.

Do not have Network Connection

Steps

1. If the user selects **Do not have Network Connection** option and clicks on **Save and Continue**, it skips the Wyse Management Suite Registration process and takes the user to the Dell Hybrid Client Login window.
2. Click **Save and Continue**, Wizard skips Wyse Management Registration and goes to Guest login (Auto login on first Boot).

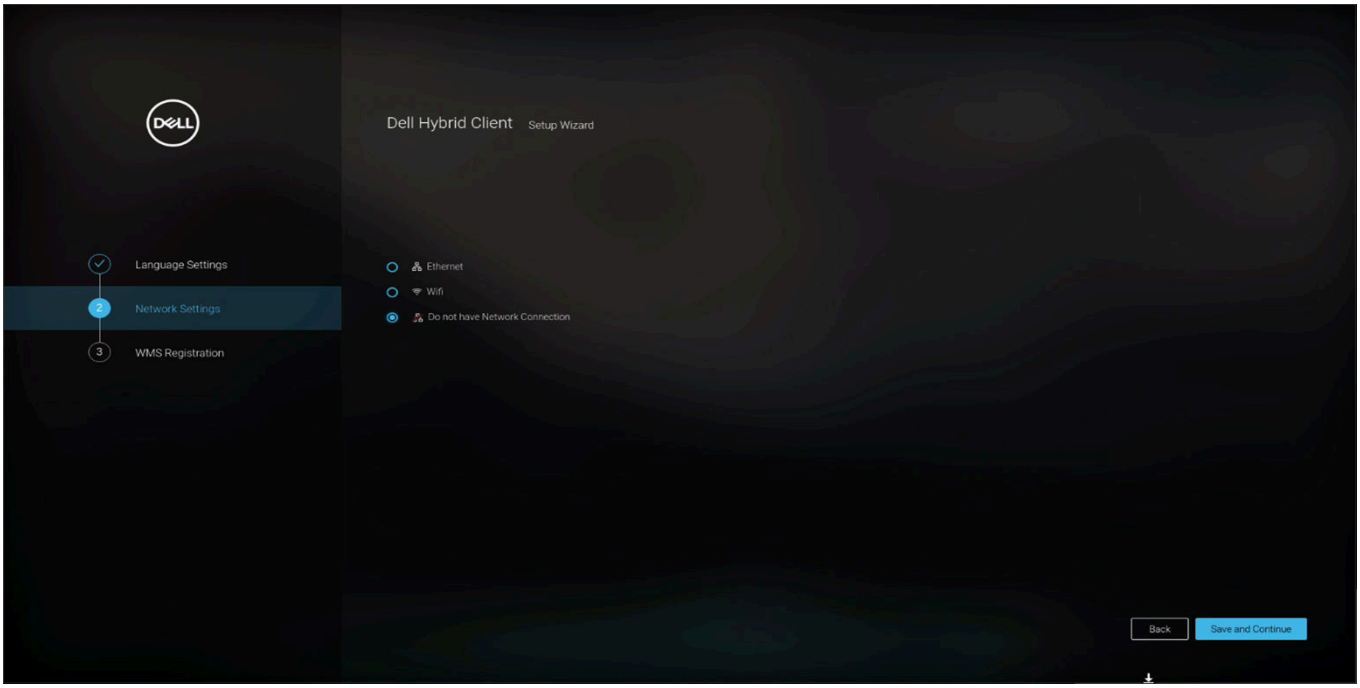


Figure 59. Setup Wizard

3. Apply Configuration page during Guest Login.

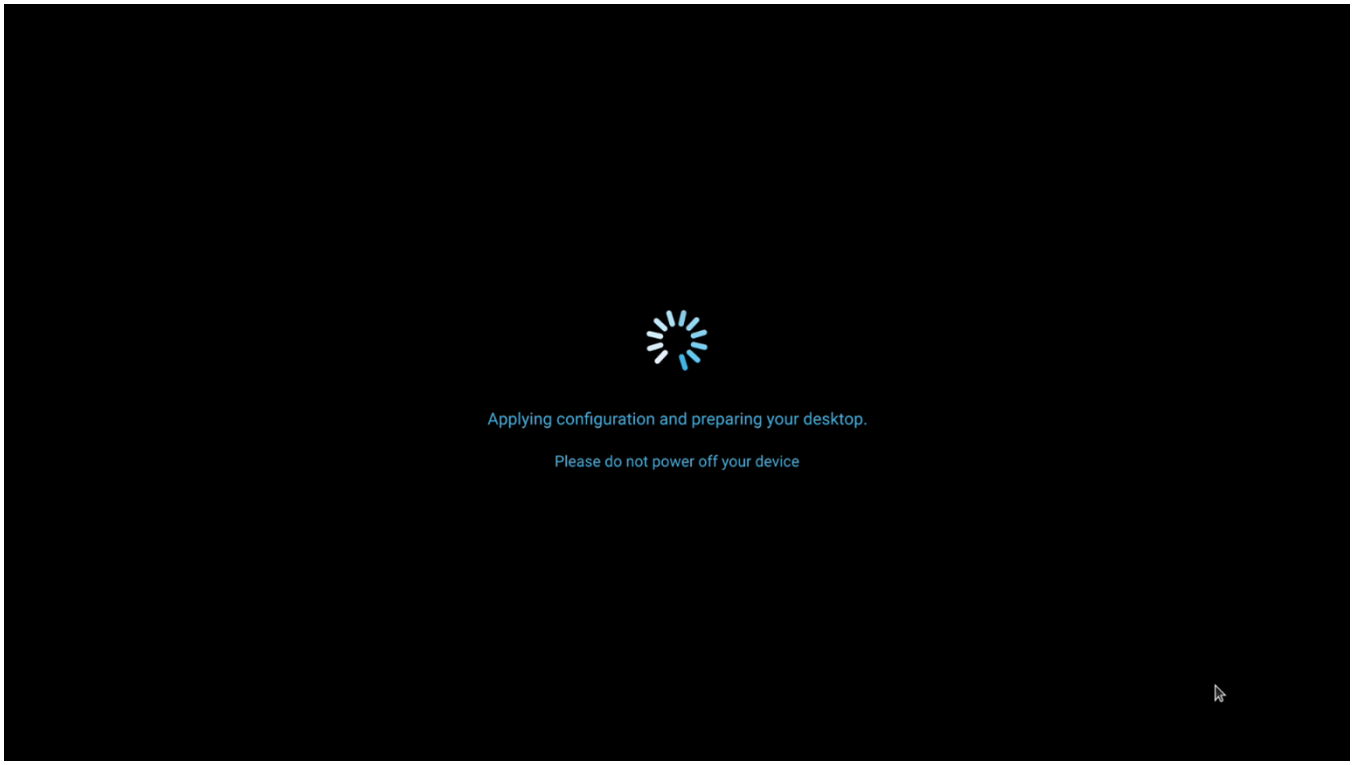


Figure 60. Apply Configuration

Register Dell Hybrid Client if Skipped Registration in Setup wizard

Prerequisites

Before registering the device, ensure that your device has network connectivity to contact the Wyse Management Suite server.

NOTE: You must authenticate with Device serial number (Service Tag) to open the Dell Client Agent (DCA) window and register the device to Wyse Management Suite.

Steps

1. Log in to Dell Hybrid Client as a guest user. By default, the username is **`guest`** and there is no password by default for **`guest`** username.
2. Configure the following options:
   a. On the top bar, click
   
   (**System Information** icon).
   The **System Information** window is displayed.
   b. In the **Hardware** section, note the serial number of the device. This acts as the default password to launch Dell Client Agent. The password is case-sensitive.
   c. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
   d. Click the **Device Settings** icon.
   The **Device Settings** pane is displayed.
   e. Click **Dell Client Agent**.
   The **Authentication Required** window is displayed.
   f. Enter the serial number of the device and click **Authenticate**.
   Upon successful authentication, the **Dell Client Agent** window is displayed.
3. Click **Registration**.
   The default status is displayed as **Discovery In Progress**.
4. To register manually, click the **Cancel** button.
5. In the **WMS Server** field, enter the URL of the Wyse Management Suite server.
6. In the **Group Token** field, enter your group registration key. The group token is a unique key for registering your devices to groups directly.
   NOTE: If the tenant and group fields are empty, the device is registered to the unmanaged group. However, the group token is mandatory for registering the device to a public cloud.
7. Click the **ON/OFF** button to enable or disable the **Validate Server Certificate CA** option. Enable this option to perform the server certificate validation for all device-to-server communication.
   The CA Validation option is enabled automatically and cannot be disabled if a public cloud URL is entered.
8. Click **Register** to register your device on the Wyse Management Suite server.
   When your device is successfully registered, the status is displayed as **Registered** with the green color tick next to the **Registration Status** label. The caption of the **Register** button changes to **Unregister**.
   NOTE: Once the device is registered, the password to launch Dell Client Agent will be set to the system password.

Registering Dell Hybrid Client by using DHCP option tags

For registering Dell Hybrid Client by using DHCP option tags, see the *Registering Dell Hybrid Client by using DHCP option tags* section in *Dell Wyse Management Suite 4.1 or later Administrator's Guide* at www.dell.com/support.

Registering Dell Hybrid Client by using DNS SRV record

For registering Dell Hybrid Client by using DNS SRV record, see the *Registering Dell Hybrid Client by using DNS SRV record* section in *Dell Wyse Management Suite 4.1 or later Administrator's Guide* at www.dell.com/support.

Enrollment Validation

In Wyse Management Suite, the **Enrollment Validation** option is introduced where the tenant must manually approve before the device is registered to a group. When the **Enrollment Validation** option is enabled, the devices are in **Pending Validation** state in the **Devices** page. The tenant can select a single device or multiple devices in the **Devices** page by selecting the **Enrollment Validation Pending** filter from the **Status** drop-down list and validate the enrollment. You can also click the **Enrollment Pending** link on the **Dashboard** page. The devices are moved to the intended group after they are validated. The validation status of the devices is also displayed in the **Devices** section on the **Dashboard** page.

Prerequisites

- You must enable the **Enrollment Validation** option when you install Wyse Management Suite—OOBE screen or in the **Portal Administration** page—**Setup** option.

  NOTE: The Enrollment Validation option is enabled by default when installing Wyse Management Suite for the first time or when using a Wyse Management Suite Cloud.
- The device must be in Enrollment Pending state.

Steps

1. Select the check box of the device that you want to validate.
2. Click the **Validate Enrollment** option.
   An **Alert** window is displayed.
3. Click **Send Command**.
   The device moves to the wanted group, and the device is registered.

4

Getting started with Dell Hybrid Client

Desktop overview

Dell Hybrid Client boots to the desktop after a successful login. This is the default screen that is displayed after you log in to the device—without autolaunch of any connections or applications. The desktop screen in Dell Hybrid Client uses the GNOME user interface that is present in the Ubuntu operating system, but is customized to create a Dell Hybrid Client environment. The Dell Hybrid Client desktop has a Dell default background with a horizontal top bar and a vertical task bar.

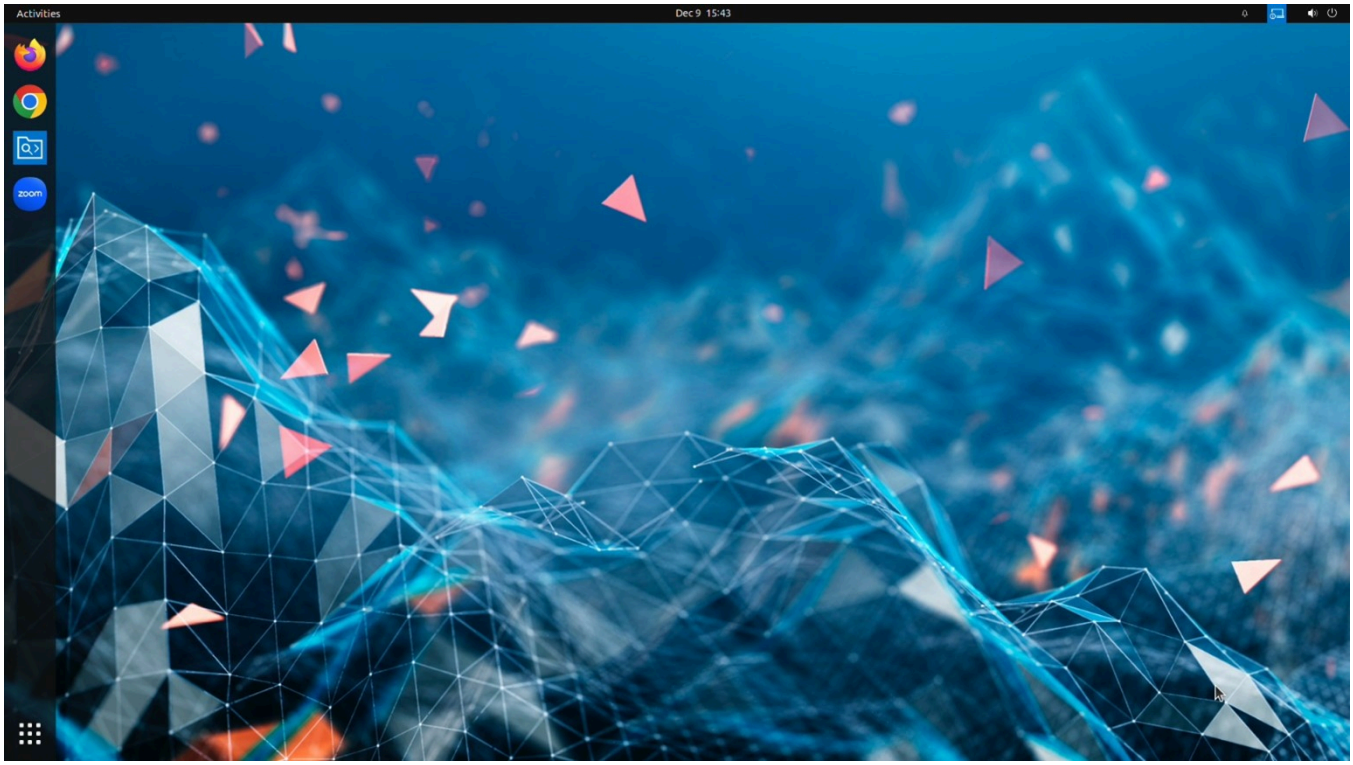


Figure 61. Desktop Ubuntu 22.04

The Dell Hybrid Client desktop consists of the following screen elements:

- **Show Applications** ( )—Displays the applications menu that provides access to all the Dell Hybrid Client configurations.
- **Top bar**—Displays time and provides access to **Activities** overview, Clock and calendar, System Information, System menu, and the Notification icon.
- **Taskbar**—Displays all your favorite applications.

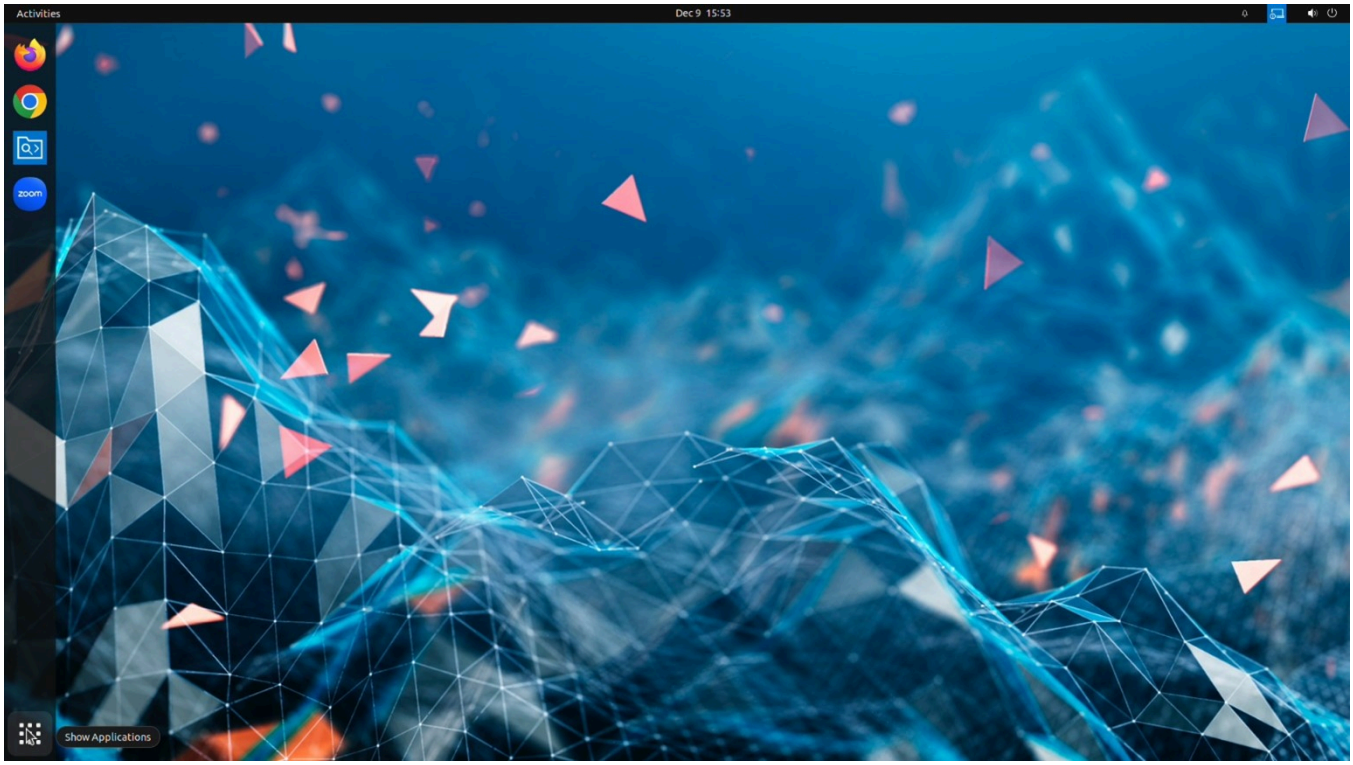


Figure 62. Show Applications

Configure the date and time using Wyse Management Suite

Use Wyse Management Suite to configure the date and time settings for the Dell Hybrid Client.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Region & Language Settings**, and click **Region and Time**.
6. Click the **Auto Time Zone** toggle key to ON state to allow the device to automatically update the system time based on the geographical location. This option is enabled by default and is set based on the Internet provider time zone.
7. If the Auto Time Zone option is not enabled, select the time zone from the drop-down list.
8. From the **Time Format** drop-down list, select the time format—12 Hours or 24 Hours.
9. To configure the time server, do the following:
   a. Under the **Advanced** tab, expand **Region & Language Settings**, and click **Time Server**.
   b. Specify the FQDN or IP address of the time server. Maximum allowed length is 127 characters.

   NOTE: You can configure multiple time servers. Each value must be separated by a semicolon.

   NOTE: By Default Auto Time Zone is enabled.
10. Click **Save and Publish**.

Configure the date and time using Device Settings

Use Device Settings to configure the date and time settings for the Dell Hybrid Client

Steps

1. Log in to Dell Hybrid Client.
2. Click on **Show Application** on bottom left corner.
3. Click on **Device Settings** icon.
4. Navigate to **Region and Language Settings**.
5. In **Region Settings** tab **Auto Time Zone** toggle key is enabled by default.
6. To set different time zone, disable the **Auto Time Zone** toggle key.
7. From **Time Zone** drop down list, select the required region and the time format—12 Hours or 24 Hours.
8. To configure the time server, do the following:
   - a. Under the **Region and Language Settings** click on **Time Server Settings** tab.
   b. Specify the FQDN or IP address of the time server. Maximum allowed length is 127 characters.
9. Click on **Save & Apply**.

Using the top bar

Use the top bar to access Activities overview, Clock and calendar, System Information, System menu, and Notification icon.

Table 4. Top bar elements

Element	Description
Activities	Displays all the running windows and user interface applications. When you enter the overview, all the running windows are displayed as live thumbnails on the current workspace. You can use a workspace to group similar type of windows. For more information about workspace, see the *Ubuntu documentation* at help.ubuntu.com/.
Clock and calendar	Displays the current date and calendar.
System Information icon	Displays the System Information icon that allows you to access the **System Information** window.
System menu	Displays the following system settings: • **Volume icon**—Enables you to increase or decrease the speaker volume. • **Wired Connection**—Enables you to turn on or turn off the wired connection. • **WiFi connection**—Enables you to turn on or turn off a wireless connection. You can select a wireless network in the **Wi-Fi Networks** window. • **Lock Screen rotation**—Enables you to rotate your device lock screen. This option is only available on supported platforms. • **Bluetooth icon**—Enables you to turn on or turn off Bluetooth. The Bluetooth icon is only shown if Bluetooth is enabled. • **VPN icon**—Enables you to connect or disconnect a VPN. The VPN icon is only shown if VPN is enabled. • **Log out**—Enables you to log off from the current user. • **Suspend**—Enables you to enter the sleep mode. • **Restart**—Enables you to restart your system. • **Power off**—Enables you to shut down your system.
Notification icon	Displays a notification icon in the notification area. It shows notifications that are related to system connections.
Keyboard layout selection	Displays the configured keyboard layouts. The keyboard layout selection icon is displayed only when multiple keyboard layouts are configured from Wyse Management Suite or Device Settings UI. User can switch between the keyboard layouts. Click the **Show keyboard Layout** option to view the arrangement of keys for the selected keyboard layout.

Using the taskbar

Dell Hybrid Client consists of a vertical taskbar on the left of the desktop screen. It displays all applications that are added to favorites. Any GUI application that is active is automatically pinned to the taskbar.

By default, the following application icons are added to the taskbar:

- Google Chrome
- Mozilla Firefox
- File Explorer
- Zoom application

You can click any of the application icons to start it. You can also add your frequently used or favorite applications to the taskbar.

Applications overview screen

Use the applications overview screen on Dell Hybrid Client to access all the local configurations, Broker agent connections, web browsers and so on. To access the applications overview screen, click the **Show Applications** button ( ) at the lower-left corner of the desktop screen.

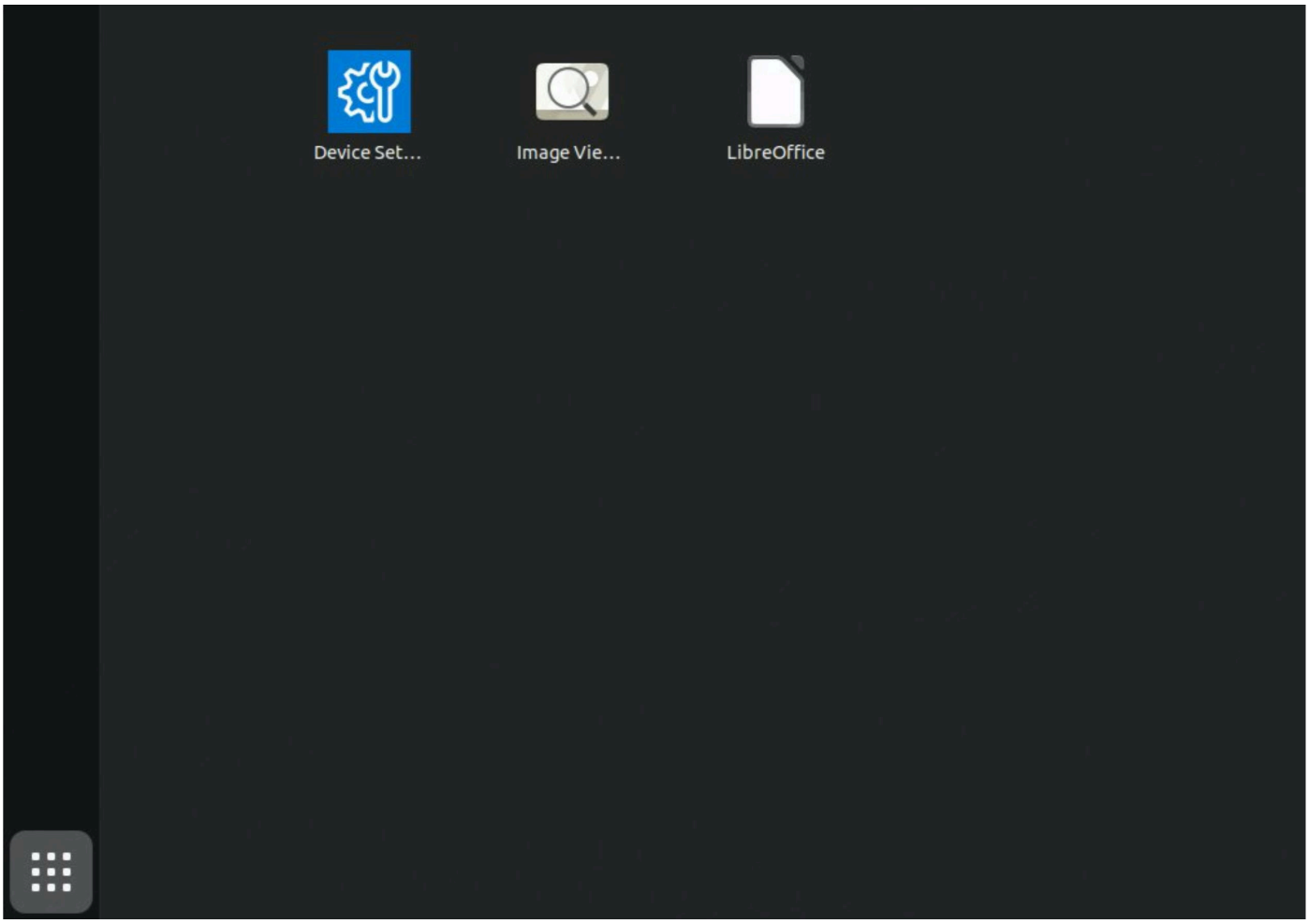


Figure 63. Show Applications

The application overview screen consists of the following screen elements:

- **Search box**—Enables you to search for applications by typing the application name in the **Search** text box.
- **Firefox browser**—-Enables you to browse the web using the Mozilla Firefox web browser.
- **Chrome browser**—Enables you to browse the web using the Google Chrome web browser.

- **File Explorer**—Enables you to manage all the local, cloud, and external files and folders.
- **Device Settings**—Enables you to configure the local configurations, such as, **Network**, **Monitor**, **Peripherals**, **Display Personalization**, **Region and Language**, **Power**, **Password**, and **Dell Client Agent**. The **Device Settings** icon is displayed on the Application overview screen.
- **Libre Office Suite**—Enables you to create and edit text documents, spreadsheets, presentation, drawings, and so on.
- **Image Viewer**—Enables you to open an image file.
- **Zoom application**—Enables you to join a Zoom meeting.
- **Connection and application shortcuts**—Enables you to quickly access all the available VDI connections, published applications, and cloud applications. VDI clients are not available as a default application.
- **Pin applications to the desktop or favorites**—You can pin applications to the desktop or favorites. Locate an application on the application overview screen, right-click the application icon, and click **Add to desktop(Only for Ubuntu 20.04)** or **Add to Favorites**.

  NOTE: To delete pinned icons, select specific icon and press **DEL** key on the keyboard.

Log Out, Suspend, Restart, or Power Off

The **Power Off** option enables you to shut down the device powered by Dell Hybrid Client. The **Suspend** option makes your thin client enter sleep mode. The **Restart** option enables you to perform a full restart of the device powered by Dell Hybrid Client. The **Log out** option enables you to log out from the current account. If the data roaming feature is enabled, the logoff, shut down, or restart may take approximately twenty seconds to one minute based on the network bandwidth and size of the data roaming profile. If network is not available, the logoff, shut down, or restart may take approximately one minute.

Steps

1. On the top bar, click the **System menu** icon.
2. Do either of the following:
   - Click the **Log Out** button and do one of the following:
     - Click the **Log Out** button to log out of your user account.
     - Click the **Cancel** option to cancel the log out action.
   - Click the **Suspend** option to enter the sleep mode.
   - Click the **Restart** option and do one of the following:
     - Click the **Restart** option to immediately shut down the device.

       NOTE: The device automatically restarts after 60 s.
     - **Cancel**—Click the **Cancel** option to cancel system shutdown.
   - Click the **Power Off** option and do one of the following:
     - Click the **Power Off** option to immediately shut down the device.

       NOTE: The device automatically restarts after 60 s.
     - Click the **Cancel** option to cancel system shutdown.

NOTE: Log Out, Suspend, Restart, or Power Off options can be enabled or disabled from **Advanced** > **Privacy & Security** > **Account Privileges** > **Customize** on Wyse Management Suite.

Lock your desktop

You can use Windows key + L combination on your keyboard to lock the desktop.

5

Policy settings overview

Managing the Dell Hybrid Client policy settings from Wyse Management Suite

You can configure and manage your devices powered by Dell Hybrid Client using the **Dell Hybrid Client 2.x** policy settings on Wyse Management Suite. To configure the Dell Hybrid Client settings, do the following:

1. Go to the **Groups & Configs** page, and select a group.
2. From the **Edit Policies** drop-down menu, click **Dell Hybrid Client 2.x**.

   The **Configuration Control | Dell Hybrid Client 2.x** window is displayed.

3. Click the **Standard** tab or the **Advanced** tab.

   The **Standard** tab lists all the configured settings. The **Advanced** tab lists all the settings.

4. Select the options that you want to configure.
5. In the respective fields, click the option that you want to configure.
6. Configure the options as required.
7. Click **Save & Publish**.

NOTE: After you click **Save & Publish**, the configured settings are also displayed in the **Standard** tab.

The following table lists the feature set that you can configure in the **Configuration Control | Dell Hybrid Client 2.x** window:

Table 5. Dell Hybrid Client Policy Settings

Feature	Sub feature—Device Policy Group	Sub feature—User Policy Group
Region & Language Settings	Language	Not applicable
	Region and Time	Region and Time
	Time Server	Not applicable
Privacy & Security	Account Privileges	Account Privileges
	Certificate	Not applicable
	System Password	Not applicable
	Guest User Account Properties	Not applicable
	Local User Account Properties	Not applicable
	Log Configuration	Not applicable
	SCEP	Not applicable
	Security Profile	Not applicable
	SSH Server	Not applicable
	USB Lockdown	Not applicable
	VNC Server	Not applicable
Broker Settings	Citrix Broker Settings	Citrix Broker Settings
	Teradici Broker Settings	Teradici Broker Settings
	AVD Cloud Settings	AVD Cloud Settings

Table 5. Dell Hybrid Client Policy Settings (continued)

Feature	Sub feature—Device Policy Group	Sub feature—User Policy Group
	VMware Broker Settings	VMware Broker Settings
	Microsoft Remote Desktop Settings	Microsoft Remote Desktop Settings
Session Settings	Global Session Settings	Global Session Settings
	Citrix Session Settings	Citrix Session Settings
	Teradici Session Settings	Teradici Session Settings
	AVD Session Settings	AVD Session Settings
	VMware Session Settings	VMware Session Settings
	Microsoft Remote Desktop Session Settings	Microsoft Remote Desktop Session Settings
VDI Configuration Editor	Citrix Configuration Editor	Citrix Configuration Editor
File Affiliation	Citrix File Type Association	Citrix File Type Association
	File Affiliation Settings	File Affiliation Settings
	RDP File Type Association	RDP File Type Association
	VMware File Type Association	VMware File Type Association
Login Experience	Login Settings	Not applicable
	Login screen power options	Not applicable
	Previously Logged-in User List	Not applicable
	Banner Message	Not applicable
Personalization	Desktop	Desktop
	Custom Info	Not applicable
	Not applicable	User Data Roaming
Peripheral Management	Audio	Not applicable
	Single/Multi Display settings	Single/Multi Display settings
	Keyboard	Keyboard
	Mouse	Mouse
	Printers	Not applicable
Network Configuration	802-1x Authentication	Not applicable
	Bluetooth Settings	Not applicable
	Proxy Settings	Not applicable
	VPN	Not applicable
	Wireless	Not applicable
Browser Settings	Browser Shortcuts	Browser Shortcuts
	Default Browser	Default Browser
	Firefox Settings	Firefox Settings
	Google Chrome Settings	Google Chrome Settings
Custom Connection Settings	Custom Connections	Custom Connections
Application Security Settings	Image Viewer	Image Viewer
	Keyboard Shortcuts	Not applicable

Table 5. Dell Hybrid Client Policy Settings (continued)

Feature	Sub feature—Device Policy Group	Sub feature—User Policy Group
	Libre Office	Libre Office
	VLC Media player	VLC Media player
Network Drives	Network Drives List	Network Drives List
Power Settings	Not applicable	Power Profile
	Power Saving	Power Saving
	Suspend & Power Button	Suspend & Power Button
WMS Settings	Deployment Settings	Not applicable
	WMS Client Settings	Not applicable
Troubleshooting	Log Configuration	Not applicable
Firmware	Kernel update	Not applicable
License and Agreement	End-user License Agreement	Not applicable
BIOS	Select your platform	Not applicable

Viewing system information

Use the **System Information** window to view the Identity, Network, Packages, Copyright, and About.

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

The **System Information** window displays the following information:

- **Identity** tab—Displays information such as system details, hardware details, BIOS version, and custom information.
  - **System**—Displays information about the current user, Wyse Management Suite registration status, MQTT status, AD status, domain name, terminal name, product name, platform, and Uptime.
  - **Hardware**—Displays information about the processor type, processor speed, total memory, free memory, media size, Device UUID, and serial number.
  - **BIOS**—Displays information about the BIOS version.
  - **Custom Info**—Displays information about the location, contact, and custom.
- **Network** tab—Displays information that is related to Ethernet and WiFi connections.
  - **Interface information**—Displays information about the MAC address, network speed, and Maximum Transmission Unit (MTU).
  - **Network Device** option—Displays Not Connected if network is not connected. If WiFi or Ethernet is connected, user can select the network and check the details.
  - **IP information**—Displays information about the IP address, IPv6 address, subnet mask, gateway, domain, primary DNS, secondary DNS, DHCP server, lease, and elapsed.
- **Packages** tab—Displays all add-ons that are installed on your device. The add-ons are listed with the attributes, such as package name, version, size, and status. The **Original** value in the **Status** column specifies the integrated add-ons in the Dell Hybrid Client. By default, only Dell packages are displayed. To view all packages, click the **Show All Packages** button.
- **Copyright** tab—Displays the software copyright and patent notices.
- **About** tab—Displays the Dell Hybrid Client version, operating system version, kernel version, Full Disk Encryption and ENERGY STAR ratings

  NOTE: Ubuntu 22.04 Non-FDE device shown as Yes and Ubuntu 22.04 FDE device is shown as No.

.

Configure the GDM Login Screen power control settings

Prerequisites

Ensure that you have enabled the GDM login screen power option using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **Login Screen Power Options**.
6. Enable or disable **GDM login screen power off** to configure the power options in GDM login Screen.
7. Click **Save & Publish**.

   NOTE: By default, this option is enabled. If this option is disabled **Suspend** and **Power Off** options are also disabled in GDM login Screen.

Account Privileges

Account Privileges option is introduced under **Privacy & Security** in Wyse Management Suite. By using **Account Privileges**, users can set the following Privilege Levels. The Privilege Leveles are applicable for **Device Group Policy** & **User Group Policy**.

- **Default**—This is the default restriction. Users are allowed to access Browsers, DHC Apps, Device Settings, VDI Apps, Productivity Apps, Power controls, System information, Print screen, Task bar, and Advanced Settings, and Dell Client Agent with password Authentication. You can enable single application mode under this option. See Single application mode.
- **None**—This is a restricted mode. All default applications and Device Settings are not accessible.
- **Customize**—This option allows the administrator to customize the user settings and application access that are enabled from Wyse Management Suite. By default all the options under **Customize** are disabled. Users must enable the required settings.
- **High**—This option does not have any restrictions. Users are allowed access to all options same as **Default**, and additionally users can access Advanced Settings and Dell Client Agent without any Authentication. You can enable single application mode under this option. See Single application mode.

  NOTE: For Device settings option/section **Disabled** from Wyse Management Suite is grayed out. Lock icon is displayed on specific options and a caption that states **These settings are managed by Organization** is displayed to users. By Default, all options under **Customize** are disabled. If a security profile is set to Open Box, then the account privilege level **High** will apply always.

Configure Account Privilege

Dell Hybrid Client enables you to restrict access to application shortcuts that added to the Dell Hybrid Client desktop and favorites. You can use Wyse Management Suite to configure the access control settings.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Account Privileges**.

6. Select any of the following from the **Privilege Level** drop-down list:
   - Select **Default** from the **Privilege Level** drop-down list to enable access to the Dell Hybrid client default apps and settings. By default, this options is selected.
   - Select **None** from the **Privilege Level** drop-down list to disable all default apps and Device Settings.

     NOTE: With **None**, configured connections are listed.
   - Select**Customize** from the **Privilege Level** to customize the user settings and application access that are enabled from Wyse Management Suite.
   - Select **High** from the **Privilege Level** to have access to all options same as **Default** and additionally user can access Advanced Settings and DCA without any Authentication.
7. Click **Save and Publish**.

Customize Account Privileges

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Account Privileges**.
6. Select **Customize** privilege level from the **Privilege Level** drop-down.

   Configure the following options based on your requirement:
   - **Web browsers**—Google Chrome and Firefox.
   - **Dell Hybrid Client apps**—Dell File Explorer and Device Settings.
   - **VDI apps**—Citrix, VMware, RDP, and AVD.
   - **Productivity apps**—VLC Media Player, Image Viewer, Libre Office, and Zoom.
   - **Power Control Settings**—Power off, Restart, Suspend, and Logout.
   - **System Information**—System information on DHC Top bar.

     NOTE: When you disable access to an application, you cannot access the application from desktop and favorites.

     NOTE: When **Customize** is selected all options listed under **Customize** is disabled by default and the admin must enable all the required options.

Single application mode

Dell Hybrid Client enables you to limit the device to present or use a single application that takes over the local gnome desktop. When enabled, it prevents users from accessing the desktop functions or other features on the device outside the single application mode.

Table 6. Supported applications

Application	Arguments supported	Example
Firefox	Yes	Website URL
Google Chrome	Yes	Website URL
Citrix	Yes	Citrix server URL
VMware	Yes	VMware server URL
Anyware	No	Not applicable
Azure Virtual Desktop	No	Not applicable
Azure Cloud Home	No	Not applicable
GCP Cloud Home	No	Not applicable

Table 6. Supported applications (continued)

Application	Arguments supported	Example
LibreOffice	No	Not applicable
Custom	Yes	Executable binary path. For example **/usr/bin/zoom**

- If you select Custom, you must provide the executable binary path.
- If GCP or Azure cloud home is selected in single application mode, you must configure the corresponding File Affiliation settings. If File Affiliation is disabled, the desktop is launched without any application.
- For Azure Virtual Desktop, the AVD broker must be enabled from Wyse Management Suite.
- Gnome-shell as a process is not allowed to run in single application mode. If started by the user or any other process, a warning message is displayed and the user session is logged off in 5 seconds.
- Single application mode can be configured from both device policy group and user policy group.
- User policy group takes priority over device policy group configurations.
- User data roaming and autolaunch features are disabled in single application mode.
- Granular support for Citrix, VMware, Anyware and Browsers that enables users to select already created connection from Broker Settings or Browser Settings.

Configure the single application mode settings

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.

   NOTE: The single application mode option is available for both device policy group and user policy group.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Account Privileges**.
6. Select either **Default** or **High** privilege level to enable single application mode.
7. Click the **Enable Single Application Mode** toggle key to enable the single application mode.
8. Select an application.
9. Enter the application arguments, if applicable.
10. If you select the application as **Custom**, enter the application path.

    This path is used to fetch the desktop file and launch the application. If the desktop file is not available, the application is directly launched using the specified path with or without firejail depending on the configured security profile.

    With custom, gnome-terminal cannot be configured as an application due to security concerns.

11. From the **Application Exit Action** drop-down list, select an action to be performed when the user closes the configured application that is launched in single application mode.

    The application exit action for custom applications is applied only for the parent process.

    For VMware standard application in single application mode, the application exit action is applied when all the VMware windows including published applications are closed.

    For Citrix standard app in single application mode, the application exit action is applied when the Citrix Workspace window is closed.

    Administrator must configure File Affiliation along with the single application mode to view the Azure or Google Cloud home page.

    Single Application Mode is now much more granularly configurable so that Administrator can choose the created connection. Additionally available options to configure the settings granularly are displayed under each option. For example, if Firefox or Google Chrome is selected, it will list an additional option **Existing Browser Setting** where the user can add the created connection name. Enable **Browser Shortcut** switch and in the **Shortcut Name** field enter the created connection name.

12. Click **Save and Publish**.

Next steps

Log in to the Dell Hybrid Client. Upon successful authentication, you are presented with the configured application. When you close the application, the configured exit action is applied.

Configure the custom connection settings

Dell Hybrid Client enables you to create and manage custom connections. You can use Wyse Management Suite to configure the custom connection settings.

Prerequisites

- As an administrator, you must install the optional custom connection add-on to create custom connections. To install the custom connection add-on on Dell Hybrid Client, do the following:
  1. Go to www.dell.com/support.
  2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device or type Dell Hybrid Client.
  3. Click the product from search results to open the product support page.
  4. On the product support page, click **Drivers & downloads**.
  5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the **Ubuntu** operating system. For information about the version of the Ubuntu operating system that is supported in each Dell Hybrid Client release, see Supported operating system.
  6. From the list, locate the custom connection add-on entry and click the download icon.
  7. After the add-on is downloaded successfully, use the standard application policy on Wyse Management Suite to deploy the add-on to Dell Hybrid Client. Ensure that you upload the downloaded add-on to the local repository on Wyse Management Suite. For more information about how to deploy a Standard App Policy, see the *Wyse Management Suite 4.1 Administrator's Guide* at www.dell.com/support.
- For configuring Custom connection with gnome-terminal, the option `/usr/bin/gnome-terminal --disable-factory` should be added.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Custom Connection Settings**, and click **Custom Connections**.
6. Click **Add Row** and configure the following settings for a single custom connection:
   a. Enter the connection name to be displayed on Dell Hybrid Client.
   b. In the Command field, enter the validated shell commands or scripts. The shell commands or scripts run when you click the connection icon on the Dell Hybrid Client desktop.

      NOTE: Do not use unknown commands or applications with unknown options for better security.

   c. Click the **Auto Launch Connection after Logon** toggle key to enable or disable the option. If enabled, the connection is automatically connected after you log in to your Dell Hybrid Client.
   d. Click the **Auto Reconnect** toggle key to enable or disable the option. If enabled, the connection is automatically reconnected after you disconnect from the session. You must also specify the time duration in seconds to delay the reconnection attempt after a disconnection occurs.
   e. Browse and upload an icon for the custom connection. You can also choose to use the default icon as the connection icon.
7. To create multiple custom connections, repeat step 6.
8. Click **Save and Publish**.

Next steps

Log in to Dell Hybrid Client and click the custom connection icon on the desktop to launch the session.

Set custom values for registry location

Dell Hybrid Client enables you to use two methods to set the custom values for registry location.

- Use the command *set_custom_info <key>:<value>* in developers mode, where *<key>* can have one of the following values:
  - Custom1
  - Custom2
  - Custom3
  - Contact
  - Location

  The *<value>* may be set as the required value for the particular key. Here are a few examples:

  ```
  set_custom_info "Custom3:$somevariable"
   set_custom_info "Location:$somevariable" "Custom1:$somevariable2"
  ```

  Example as a script:

  ```
  Location_name=$(dnsdomainname |cut -f1 -d'.')

   # get machine ID and assign to variable
   machID=$(cat '/etc/machine-id')

   # set Location at location and machine ID in custom info 3
   set_custom_info "Custom3:$machID" "location:$Location_name"
  ```

- Custom values for registry location can be set from Wyse Management Suite, using the .sh and .py files. You can create a Standard Application policy and push it from Wyse Management Suite.

NOTE: The custom info values set from Wyse Management Suite device policy settings have higher priority over values set locally by using the *set-custom-info* command. For Deploying the scripts, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Multilanguage support

Dell Hybrid Client supports localized user interface to view system menus and local applications such as Device Settings and Dell File Explorer in your preferred language. The following languages are supported:

- English—Default selection is English
- French—France
- German
- Italian
- Spanish—Latin America
- Japanese
- Korean
- Chinese Simplified
- Chinese Traditional
- Russian
- Portuguese-Brazil
- Hebrew

Dell Hybrid Client Supports four Nordic languages:

- Danish
- Finnish
- Norwegian
- Swedish

Dell Hybrid Client supports the following locales for:

- Spanish—Argentina
- Spanish-Latin America
- Spanish—Chile
- Spanish—Colombia

- Spanish—Mexico
- Spanish—Peru
- Spanish—United States

To set your preferred language on Dell Hybrid Client, do the following:

1. Download and install the language add-on using Wyse Management Suite. See, Download and install language add-ons on Dell Hybrid Client.
2. Configure the language settings using Wyse Management Suite. See, Configure the language settings using Wyse Management Suite.

NOTE: When you set a language, only the system local language is changed. Keyboard input language must be selected separately.

Download and install language add-ons on Dell Hybrid Client

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device or type Dell Hybrid Client.
3. Click the product from search results to open the product support page.
4. On the product support page, click **Drivers & downloads**.
5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the **Ubuntu** operating system. For information about the version of the Ubuntu operating system that is supported in each Dell Hybrid Client release, see Supported operating system.
6. From the list, locate the language pack add-on entry and click the download icon.

   The following are the language packages that are available for Dell Hybrid Client:

   - **Full Language add-on package**—Localization add-on for Dell Hybrid Client that consists of all the supported language packs in a single package file.
     - Deploying the add-on installs all the supported language packs on Dell Hybrid Client.
     - Multiple language packs can be installed using Wyse Management Suite.

   NOTE: Deployment will only copy the language files to the device. The installation is triggered only when the Language is selected from Wyse Management Suite. Only selected languages are installed after applying the language settings.

7. After the add-on is downloaded successfully, use the standard application policy on Wyse Management Suite to deploy the add-on to Dell Hybrid Client. Ensure that you upload the downloaded add-on to the local repository on Wyse Management Suite. For more information about how to deploy a Standard App Policy, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Next steps

Configure the language settings using Wyse Management Suite. See, Configure the language settings using Wyse Management Suite.

Configure the language settings using Wyse Management Suite

Prerequisites

Ensure that you have installed the required language add-ons on Dell Hybrid Client.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Region & Language Settings**, and click **Language**.

6. From the **Language** drop-down list, select the system language that you want to use for Dell Hybrid Client.
7. If you select the language as **Spanish**, select the locale.
8. If you want to install multiple language packs, select one or more language check boxes from the **Additional language** packs drop-down list.

   NOTE: Language add-ons are not uninstalled when you clear the check box selection.

9. Click **Save and Publish**.

6

Configuring the VDI environment

In a Virtual Desktop Infrastructure (VDI) environment, a Broker agent is a software entity that enables you to connect a published desktop. The Broker agent facilitates the VDI environment to securely and efficiently manage the centrally hosted desktop environments.

Dell Hybrid Client supports the following VDI connections, both on-premises and on the cloud:

- Citrix
- VMware Blast, PCoIP, and RDP
- Anyware
- Imprivata
- Dell RDP
- Azure Virtual Desktop, formerly known as Windows Virtual Desktop.

NOTE: VDI packages are released as optional Pacakages. Restart is required post installing any VDI package. Customers must install the required VDI packages first before configuring VDI from Wyse Management Suite. You can download the Citrix RTME package from the Citrix website and install the component.

NOTE: Imprivata supports Ubuntu 22.04.

Single Sign-On (SSO) to VDI applications

Dell Hybrid Client supports Single Sign-On (SSO) to VDI applications. It enables you to log in only one time with one set of credentials to get access to all your applications.

- **Citrix SSO**—SSO is supported only when using a Citrix StoreFront connection. SSO feature is enabled when you log in to a remote session from the local device. Citrix SSO is supported using a smart card. Citrix SSO works only for domain users.

  NOTE: SSO is not supported on Citrix PNAgent connections and for applications inside the session.

  To use the SSO feature, you must enable the following options from Citrix Delivery controller:

  - **Domain Pass-Through**—This option must be enabled in **Store Service** > **Manager Authentication Methods** on Citrix Studio. For information about the steps to configure Citrix feature for Pass-Through Authentication feature, see *How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication* article (CTX133982) at support.citrix.com.
  - **HTTP Basic**—This option must be enabled in **Store Service** > **Manager Authentication Methods** on Citrix Studio.
  - **Smart card authentication**—This option must be configured on the StoreFront console. This option enables you to use a smart card to authenticate user from initial login to the Citrix VDI session. When using the smart card authentication for Citrix SSO, ensure that you have configured the PIN on your smart card, and installed the required smart card certificates on Dell Hybrid Client. For information about how to configure the smart card support in Citrix Workspace app for Linux, see the *Citrix documentation for Citrix Workspace app* for Linux at docs.citrix.com.
- **RDP SSO**—RDP supports SSO. You must create the RDP connection with FQDN, and the device time must be synchronized with the domain time of the RDP server. SSO is supported from Windows 10 1607 and Windows 2016 onwards. However, SSO is not supported for applications inside the session.

  To use the SSO feature, you must enable the following options on the windows server:

  - **Windows Defender Remote Credential Guard**—This option must be enabled on the server side. For information about the steps to enable Windows Defender Remote Credential Guard, see the *Enable Windows Defender Remote Credential Guard* article at docs.microsoft.com.
  - **Allow log on through Remote Desktop Services**—This option must be enabled in the local security policy. You can access the **Local Security Policy** window using `secpol.msc`.
- **VMware SSO**—Single Sign-On (SSO) is not supported on VMware connections and File Type Association (FTA).

Multifactor authentication for VDI applications

Dell Hybrid Client supports multifactor authentication for Citrix and VMware using a smart card PIN. This option enables you to log in to a VDI session using a smart card PIN. This feature is supported from Dell Hybrid Client version 1.5 onwards.

As prerequisites, you must do the following:

- Ensure that you have configured the Citrix StoreFront server for smart card support on the StoreFront console. For information about how to configure the smart card support in Citrix Workspace app for Linux, see the *Citrix documentation for Citrix Workspace app* for Linux at docs.citrix.com.
- Ensure that you have configured the Horizon server for smart card support. For information about how to configure the smart card support in Horizon Administrator, see the *VMware Horizon documentation* at docs.vmware.com.
- Ensure that you have configured the PIN on your smart card. For information about how to configure the PIN for your smart card, see the smart card product documentation on the respective vendor websites.
- Ensure that you have installed the required smart card certificates on Dell Hybrid Client. For information about how to install a certificate using Wyse Management Suite, see Install a certificate.

Example:

1. Configure the VDI server infrastructure to use a smart card.
2. Log in to Dell Hybrid Client.
3. Connect a smart card reader to the device powered by Dell Hybrid Client.
4. Tap your smart card on the smart card reader.
5. Enter the smart card PIN to authenticate the user.

   Upon successful authentication, the Citrix session is directly launched on Dell Hybrid Client.

NOTE: Dell RDP does not support Multifactor authentication.

Global Session Settings

Global Session Settings option is added under **Session Settings** to configure the VDI global settings.

Configure Global Session Settings

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Session Settings**, and click **Global Session Settings**.
6. Configure the following settings:
   - **Local Resources and USB Redirection**—
     - Click **Enable USB Redirection** toggle key to enable redirection of USB devices into remote session.
     - Click **Add Row** under**Include USB VID/PID** to specify **Vendor ID** and **Product ID** of the devices that must be included.
     - Click **Add Row** under **Exclude USB VID/PID** to specify **Vendor ID** and **Product ID** of the devices that must be excluded.

     NOTE: The option is not applicable for RDP and AVD connections.
   - **Display Settings**—
     - **Resolution**— Select a manual remote display resolution if the resolution must be different from what is configured.

       NOTE: The option is not applicable for AVD connection.
     - **Add VDI Shortcuts To Desktop**— Enable the **Add VDI Shortcuts To Desktop** toggle key to add VDI shortcuts to Desktop. If this option is turned off, the VDI shortcuts are added to the Favorite bar.
       - If **Add VDI Shortcuts To Desktop** toggle key is enabled, the **On Desktop (All Applications)** drop-down is displayed.

- If **Add VDI Shortcuts To Desktop** toggle key is disabled, the **On Favourites (All Applications)** drop-down is displayed.

  NOTE: The drop-down selection specifies what must be displayed to the user during a broker connection. **All** displays both published application desktops. If you select **None**, no icons are displayed. If you select **Applications Only**, only the published applications are displayed. If you select **Desktops Only**, only the published desktops are displayed. The drop-down items are same for both **On Desktop (All Applications)** and **On Favourites (All Applications)**. By default **On Desktop (All Applications) / On Favourites (All Applications)** is set to **None**.

  NOTE: The option is not applicable for Anyware and AVD connections.

- **Advanced Settings**
  - **Sound**—Enable the **Sound** toggle key to allow sound in VDI sessions.

  NOTE: The option is not applicable for VMware and Anyware connections.

Configuring Citrix

Citrix offers a complete virtualization solution, where all applications and resources are deployed on a centralized server, and published to remote devices. The Citrix Workspace app client installed on Dell Hybrid Client allows you to interact with the application GUI, while all the application processes are performed on the server.

This section provides information about how to configure a Citrix connection and other Citrix features using Wyse Management Suite.

Dell Hybrid Client supports the following Citrix features that you can configure using Wyse Management Suite:

Table 7. Supported Citrix features

Feature	Description
File Type Association	Establishes the relationship between a file type and a supporting application on the server or the local machine.
Single Sign-On	Enables you to log in to the Citrix store without asking for username, password, and domain locally. The username, password, and domain are deployed from Wyse Management Suite and Citrix uses these credentials to log in to the store or published application.
Smart card Login	Enables you to use a smart card to authenticate the user, and launch the Citrix session.
USB Redirection	Enables the connected USB devices to be redirected from the client device to a Citrix virtual desktop. You can use a wide variety of USB devices in your Citrix session as though the USB devices were physically connected into the session. You can specify the list of USB devices to be allowed based on the Vendor ID, Product ID, Device Class, and Subclass ID.
Autolaunch	Enables you to configure the Citrix connection to launch automatically when the user logs in to the client. This feature is supported from Dell Hybrid Client version 1.6 onwards.
Client Drive Mapping	Enables you to associate a local drive with a remote session.
COM Port Mapping	Enables you to map the serial device on the server to the serial device on the local device.
Transparent Key Passthrough	Determines how the mapping of certain Windows key combinations is used when connecting to Citrix sessions. When **Local** is set, the key combinations are applied to the local desktop. When **Remote** is set, the key combinations are applied to seamless and non-seamless ICA sessions provided windows have the keyboard focus. When **Full Screen Only** is set, the key combinations are applied to the non-seamless ICA session in full screen mode.
HotKey mapping	Enables you to create key combinations for shortcuts.
UDP audio support	Use User Datagram Protocol (UDP) to support audio in a Citrix session.
Multi-Monitor Support	Use multiple displays in a Citrix session.
H264 Support	Use H.264 video codec to compress graphics during video playback in Citrix session.
Multimedia Redirection	Enables the audio and video to be rendered on the endpoint device instead of running on the server side.

Table 7. Supported Citrix features (continued)

Feature	Description
WebPage Redirection or Browser Content Redirection	Enables the web browser content, including HTML5 videos, to be redirected to the client and not redirected on the VDA side. It prevents the rendering of included webpages on the VDA side.
Multistream and HTML5 redirection	Enables you to use the multimedia redirection features of HDX MediaStream to include HTML5 audio and video.
Middle Button Paste	Enables you to use the mouse's middle button for paste functionality.
Application Name	Specifies the published application or desktop name. The application or desktop name is case-sensitive.
Allow access to microphone and webcam	Enables you to access microphone and webcam inside a Citrix session.
Store Name	Specifies the name of the store through which the connection for the StoreFront server is established.
Compression	Enables you to compress data for better server performance.
Low Bandwidth	Enables optimization for low-speed connections, such as reducing audio quality or decreasing protocol-specific cache size.
Resolution	Specifies the connection display resolution. Seamless option is applicable only for Published Application and Storefront connections.
Encryption	Specifies the connection security level. The highest level is 128-bit security and the lowest level is Basic.
Save MultiMonitor Preference	Enables you to save the position of a desktop session and relaunch it in the same position when using multiple displays.
H.264	Enables H.264 encoding for media packets which are received from the server. This results in better performance for multimedia redirection and webcam redirection.
Purge Login Credentials	Removes the saved login credentials for enhanced security.

NOTE: HDX adaptive transport must be disabled in the Citrix server configuration for Multiport to work.

NOTE: To enable the autoscroll functionality in the Citrix session, you must disable the Middle Button Paste option from Wyse Management Suite.

Citrix Installation

Citrix workspace addon must be installed in Dell Hybrid Client through **Apps & Data** > **App Policies** > **Dell Hybrid Client** from Wyse Management Suite.

Configure Citrix Broker Connection using Wyse Management Suite

This section describes the procedure to configure the Broker settings for a Citrix session using Wyse Management Suite.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced tab**.
5. Expand **Broker Settings** and click **Citrix Broker Settings**.
6. In the Citrix Connection section, click **Add Row**.
7. Configure the Citrix session options as per your requirement. You must configure the following options for all Citrix connection. You can see the Citrix Broker Settings image.
   a. Connection Name
   b. Host
   c. Store Name

8. Click **Save & Publish**.

Create a connection to launch a specific application from the Citrix server:

To create the application specific connection, enter the application name in the Desktop/Application Name field.

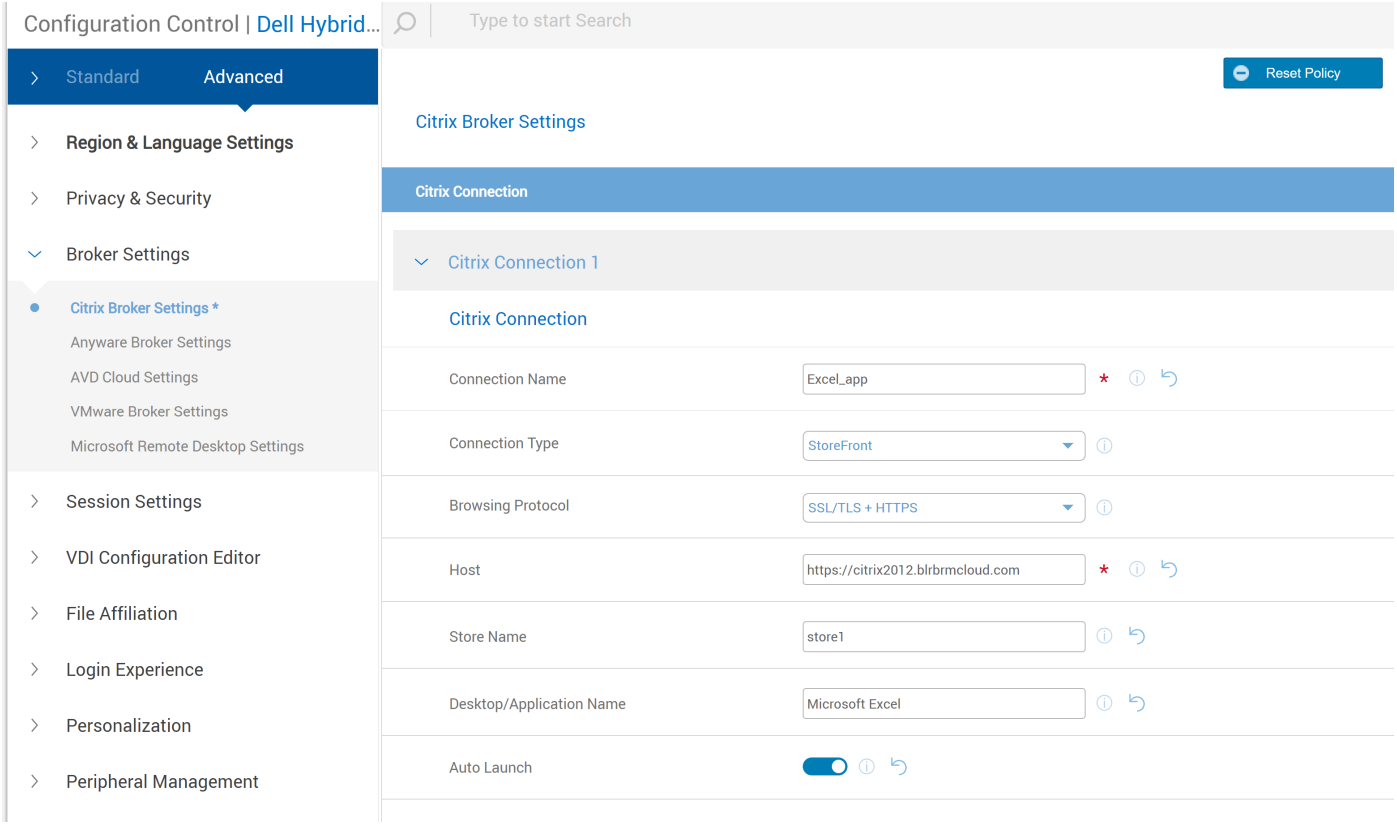


Figure 64. Citrix Broker Settings

Create a connection to launch multiple applications from the Citrix server

To create the connection for multiple applications, enter the applications name in the Desktop/Application Name field and separate them by a semicolon (;).

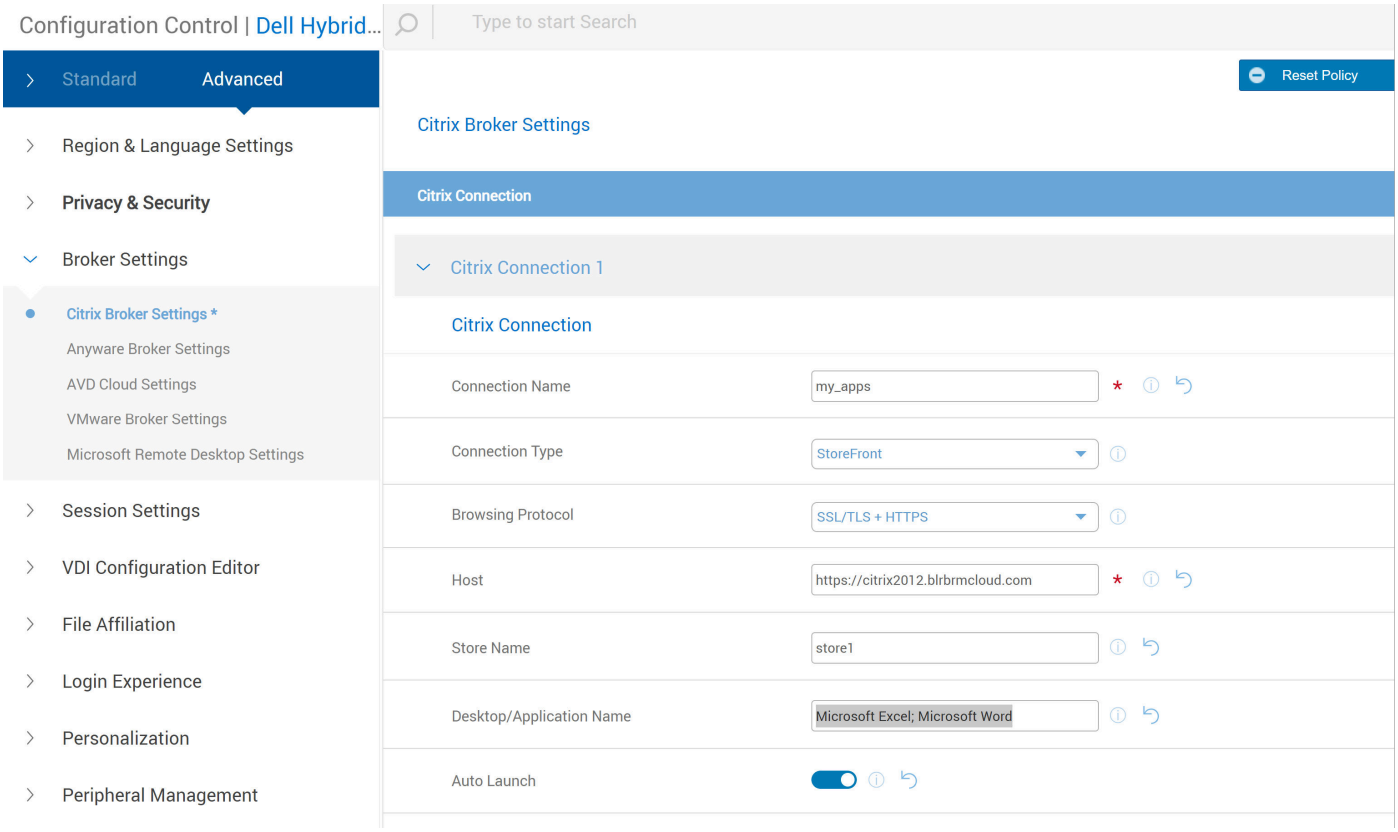


Figure 65. Citrix Broker Settings

Create a connection to launch all applications from the Citrix server

To create the connection for all applications in the Citrix server, do not enter the applications name in the **Desktop/ Application Name** field.

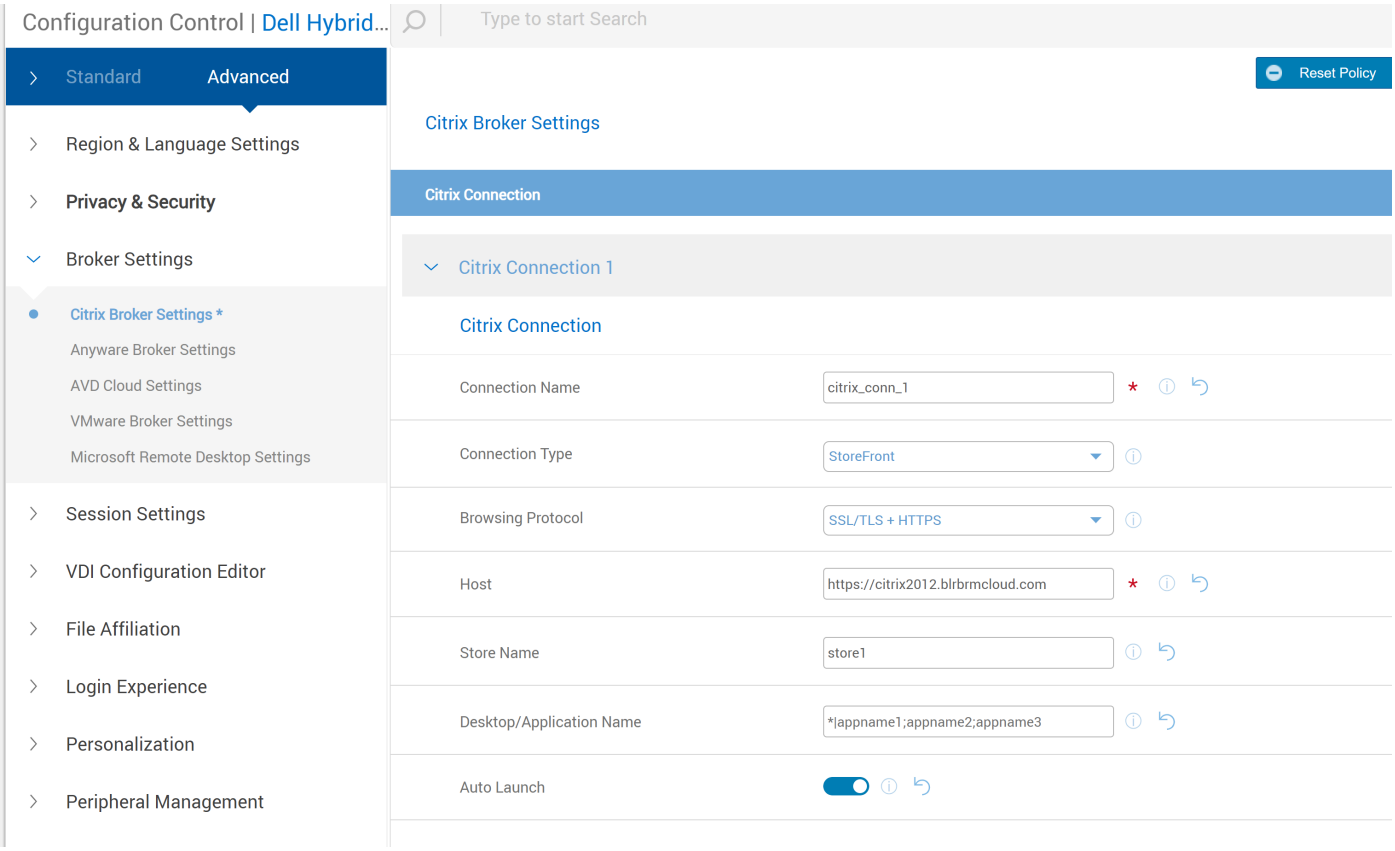


Figure 66. Citrix Broker Settings

Configure Citrix Session Settings

This session describes the procedure to configure the Citrix Session Settings.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced tab**.
5. Expand **Session Settings** and click **Citrix Session Settings**.
6. Configure the following settings:
   - **Citrix Session Settings:**
     - **Encryption -** Select the connect security level from the **Encryption** drop-down list. The highest level is **RC5 (128 bit)**, and the lowest level is **Basic**.
     - **Compression -** Enable or disable the compression during the session by using the **Compression** toggle key.
     - **Low Bandwidth -** Enable or disable optimization for low bandwidth connections by using the **Low Bandwidth** toggle key. After you enable the option, audio quality is reduced, and protocol specific cache size is reduced.
     - **Keyboard Layout Mode -** Specify the keyboard layout mode for the Citrix session by using the **Keyboard Layout Mode** drop-down list. The default value is **Server Default**. You can also select **Specific Keyboard** and enter the layout in the **Keyboard Layout** field.
   - **Smartcard Settings:**
     - **Smartcard Login -** Enable or disable logging into the Citrix server through a smart card by using the **Smartcard Login** toggle key. The parameter is not applicable for PA connections. You can select the smart card type from the **Smartcard Type** drop-down list after you enable the option.
   - **Local Resources and USB Redirection:**
     - **Allow access to microphone and webcam -** Enable or disable the **Allow access to microphone and webcam** toggle key to allow or deny access to the microphone and webcam in a Citrix session.
     - **HDX Webcam Device -** You can enter the webcam device path in the **HDX Webcam Device** field if there are multiple webcams present.
   - **COM Port Mapping Settings -** Click **Add Row** to select **COMPorts** and **COMDrive**.
   - **Client Drive Mapping settings:**

- **Local File Access -** Enable or disable the **Local File Access** toggle key to allow or deny access to the local files and drives.
- **Dynamic Drive Mapping -** List the devices to enable or disable the mapping.
- **Configure the Drive Mapping Settings -** Click **Add Row** to select **Drive Letter, Drive Access, and Drive Path**.

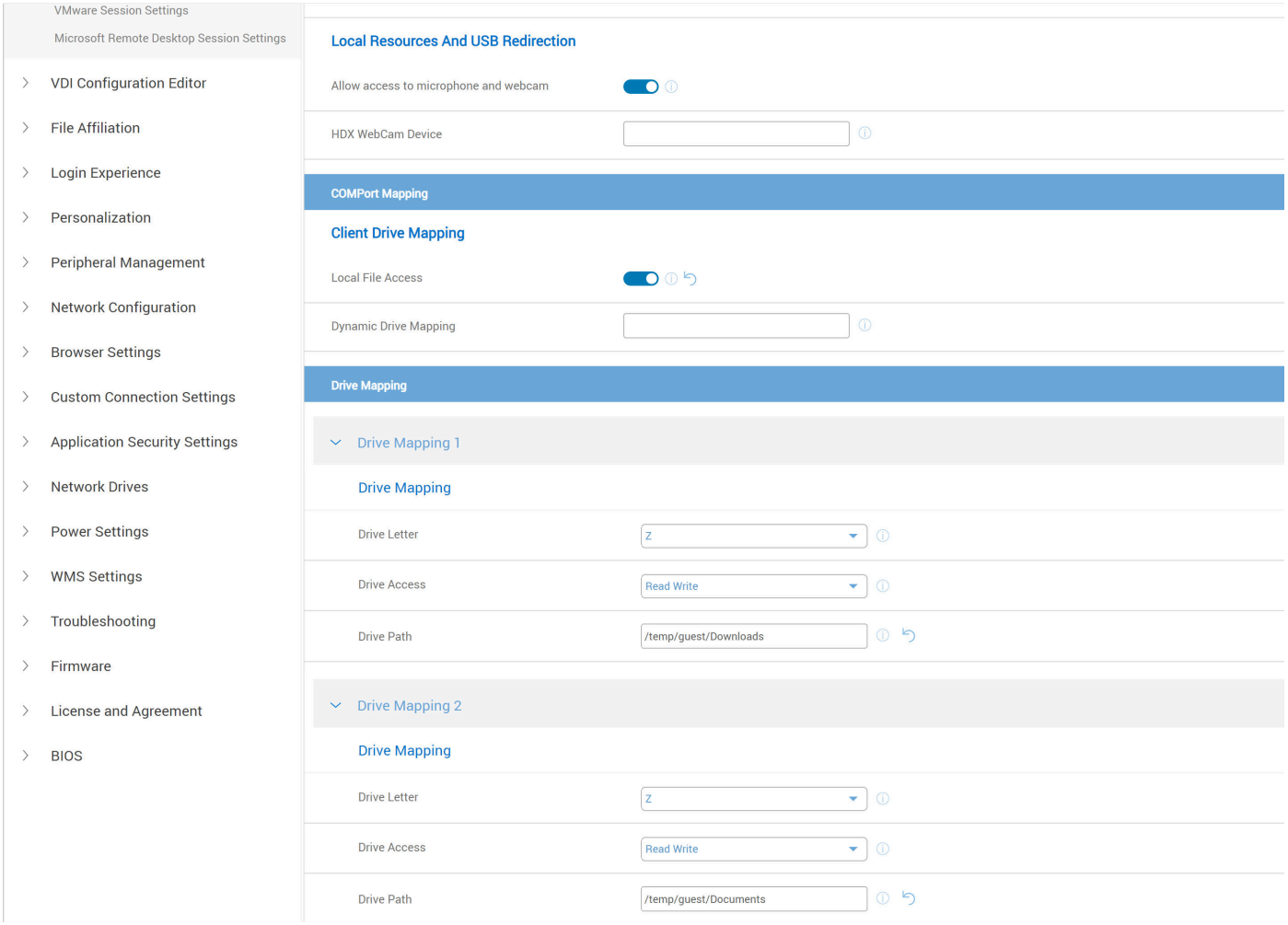


Figure 67. Drive Mapping Settings

- **Hotkey Settings:**
  - **Transparent Key Passthrough -** Enable the keyboard shortcut sequences defined by the local Windows manager in the session by selecting an option from the **Transparent Key Passthrough** drop-down list.
  - **Stop Direct Key Handling (Shift) -** Select a key from the drop-down list.
  - **Stop Direct Key Handling (Char) -** Select a key from the drop-down list.
  - **Configure HotKey Mapping Settings -** Click **Add Row** to select **Function, HotKey, and Keys**.

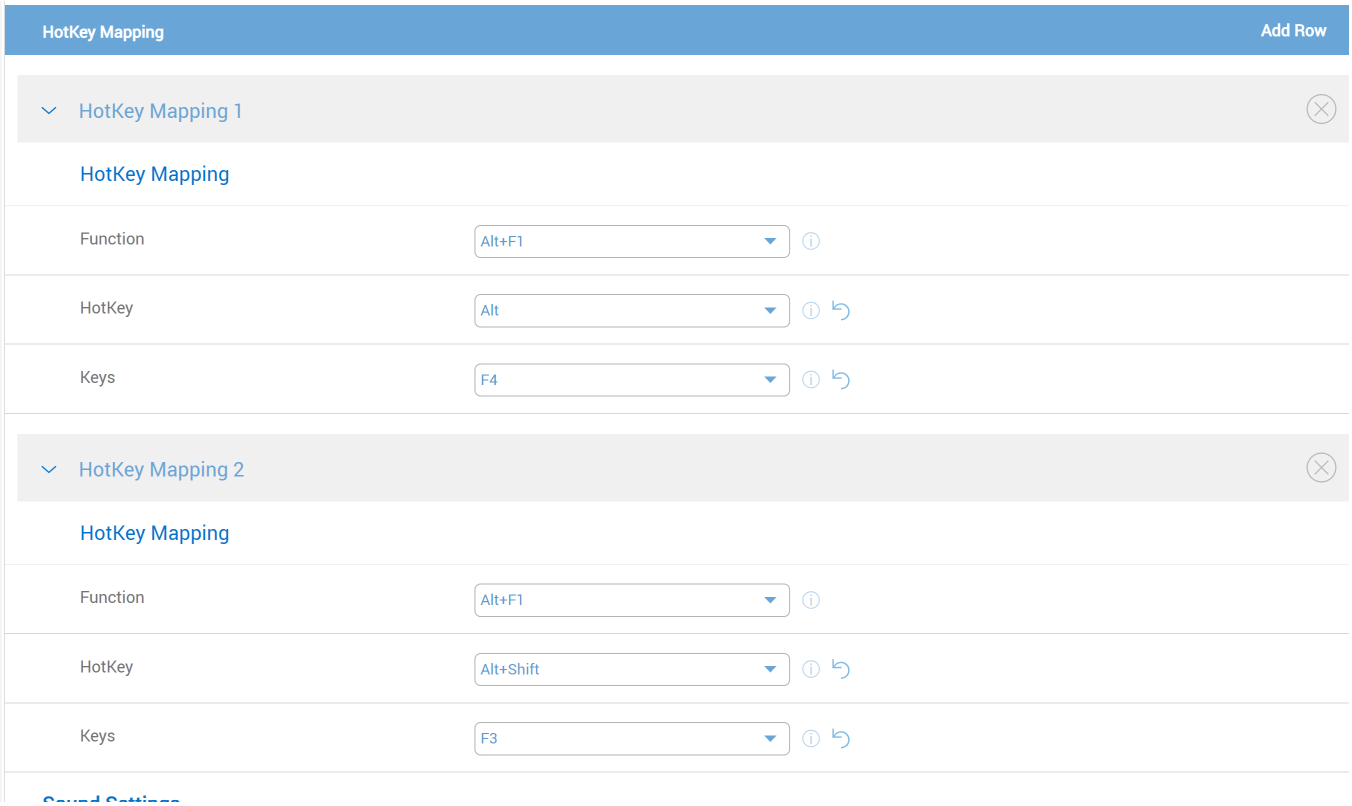


Figure 68. HotKey Mapping

- **Sound Settings:**
  - **UDP Audio -** Enable or disable the real-time audio data packet exchange by using the **UDP Audio** toggle key.
  - **UDP Audio Port Maximum -** Enter the maximum value of the UDP port range that you want to configure for real-time audio data packet exchange. The default value is 16509.
  - **UDP Audio Port Minimum -** Enter the minimum value of the UDP port range that you want to configure for real-time audio data packet exchange. The default value is 16500.
- **Advanced Session Settings:**
  - **Save Multimonitor Preference -** Save the position of the monitors that are used in a multimonitor environment during a Citrix session and relaunch it in the next session by enabling the **Save Multimonitor Preference** toggle key.
  - **H264 -** Enable or disable the **H264** encoding for media packets.
  - **MMR -** Enable or disable **multimedia redirection**.
  - **Webpage Redirection -** Enable or disable browser content redirection.
  - **MultiStream -** Enable or disable using multiple streams while connecting to a multistream ICA enabled server.
  - **Desktop Viewer Toolbar -** Enable or disable the **Desktop Viewer Toolbar** at the top of the HDX screen.
  - **Middle Button Paste -** Enable or disable the option to paste using the middle mouse button while in a session.
  - **Purge Login Credentials -** Enable this option to purge all credentials and tokens.

7. Click **Save & Publish**.

NOTE: If a user configures session settings values, it takes effect for broker connection.

Connect to a Citrix session

Citrix offers a complete virtualization solution, where all applications and resources are deployed on a centralized server, and published to remote devices. Dell Hybrid Client integrates the Citrix Workspace app. Citrix Workspace app enables you to access all your virtual apps, desktops, and other Citrix products from a single workspace UI.

Prerequisites

- Ensure that you have configured the Citrix Broker agent settings using Wyse Management Suite. For more information about Dell Hybrid Client policy settings, see Managing the Dell Hybrid Client policy settings.
- Ensure that you have installed valid certificates that are required to connect to Citrix Virtual Desktops and Apps. For more information about installing certificates, see Install a certificate.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
   All the Citrix-published desktops and applications are displayed.
3. Click a desktop icon to launch the published desktop, or click an application icon to launch an application.

   NOTE: You can launch a Citrix session from the Firefox browser. The desktop or the application file is downloaded and is launched from the browser. You cannot launch the Citrix session from the Chrome browser.

Desktop Restart for Citrix Session

User can enable the restart option for Windows desktops under Citrix Workspace app to get a fresh session every time they log in to the Citrix session even when connected to the same Citrix desktop.

The affected operating system is Citrix XenDesktop

The affected versions are:

- Citrix Workspace Application version 2211 and later.
- Citrix XenDesktop version 2209 and later.

For more information about enabling the restart feature for the published Citrix desktops, see How to Enable the Citrix XenDesktop Restart Option for Dell Hybrid Client.

Citrix Configuration Editor

The Citrix configuration editor enables the administrator to configure the Citrix-related settings by dynamically modifying the Citrix configuration files.

The following Citrix VDI settings are supported:

- Citrix INI settings
- Citrix XML settings
- Citrix Keyboard layout settings

Configuring Citrix Configuration Editor using Wyse Management Suite

Prerequisites

About this task

This section describes the procedure to configure the Citrix Configuration Editor using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
   The **Citrix Configuration Editor** page is displayed.

Configuring Citrix INI Settings

About this task

This section describes the procedure to configure the Citrix INI settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row** under the file column.
   The following INI files are listed:
   - Module.ini
   - All_Regions.ini
   - ·wfclient.ini
   - wfclient.template
   - appsrv.ini

Configuring module.ini settings

About this task

This section describes the procedure to configure the Citrix module.ini settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **module.ini** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.
8. Click **Save & Publish**.

Configuring wfclient.ini settings

About this task

This section describes the procedure to configure the Citrix wfclient.ini settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **wfclient.ini** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.
8. Click **Save & Publish**.

Configuring All_Regions.ini settings

About this task

This section describes the procedure to configure the All_Regions.ini settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **All_Regions.ini** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.
8. Click **Save & Publish**.

Configuring wfclient.template settings

About this task

This section describes the procedure to configure the wfclient.ini settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **wfclient.template** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.
8. Click **Save & Publish**.

Configuring appsrv.ini settings

About this task

This section describes the procedure to configure the appsrv.ini settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **appsrv.ini** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.
8. Click **Save & Publish**.

Configuring Citrix XML Settings

About this task

This section describes the procedure to configure the Citrix XML settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.

4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row** under the file column of **Citrix XML Settings**.
   The following XML file is listed:
   - AuthManConfig.xml

Configuring AuthManConfig.xml settings

About this task

This section describes the procedure to configure the AuthManConfig.xml settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **AuthManConfig.xml** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.
8. Click **Save & Publish**.

Configuring Keyboard Layout Settings

About this task

This section describes the procedure to configure the Keyboard Layout settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row** under the file column of **Citrix Keyboard Layout Settings**.
   The following Keyboard Layout file is listed:
   - kbdlayoutmap.tbl

Configuring kbdlayoutmap.tbl settings

About this task

This section describes the procedure to configure the kbdlayoutmap.tbl settings using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **VDI Configuration Editor**, and click **Citrix Configuration Editor**.
6. Click on **Add Row**and select file as **kbdlayoutmap.tbl** and operation as **Add or Update**.
7. Enter **Section**, **Key** and **Value** fields.

8. Click **Save & Publish**.

Configuring Anyware

Anyware is used for delivering remote desktops and applications using PCoIP protocol. The Anyware app client is installed on Dell Hybrid Client through which you can interact with the application GUI.

Anyware Installation

Anyware addon must be installed in Dell Hybrid Client through **Apps & Data** > **App Policies** > **Dell Hybrid Client** from Wyse Management Suite.

Configuring Anyware Broker Connection using Wyse Management Suite

This section describes the procedure to configure the Broker Settings for a Anyware session using Wyse Management Suite.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Broker Settings** and click **Anyware Broker Settings**.
6. In the **Anyware Connection** section, click **Add Row**.
7. You can configure the following Anyware Broker settings.

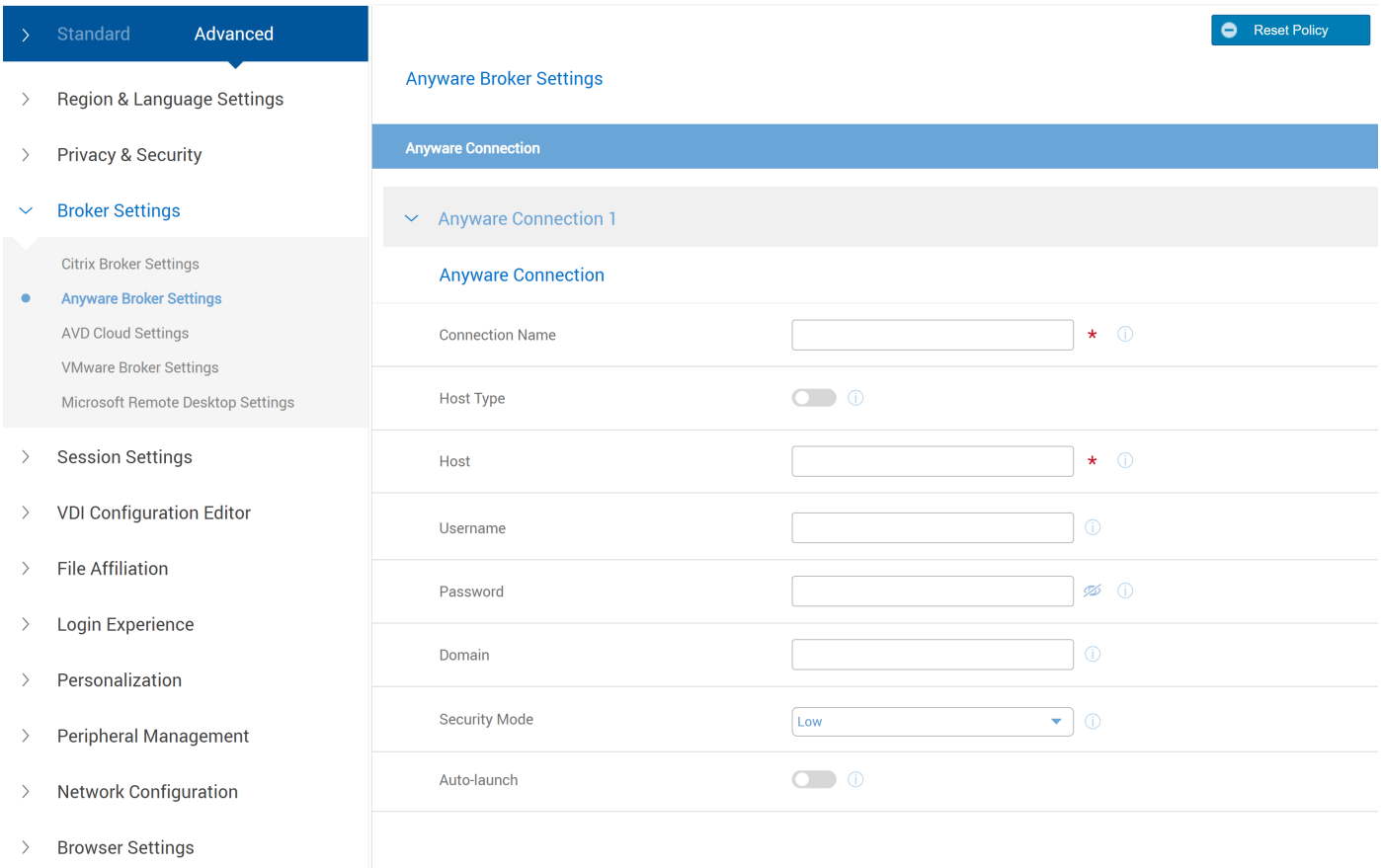


Figure 69. Anyware Broker Settings

- **Connection Name -** Enter the Anyware connection name. The name must be unique for each session.

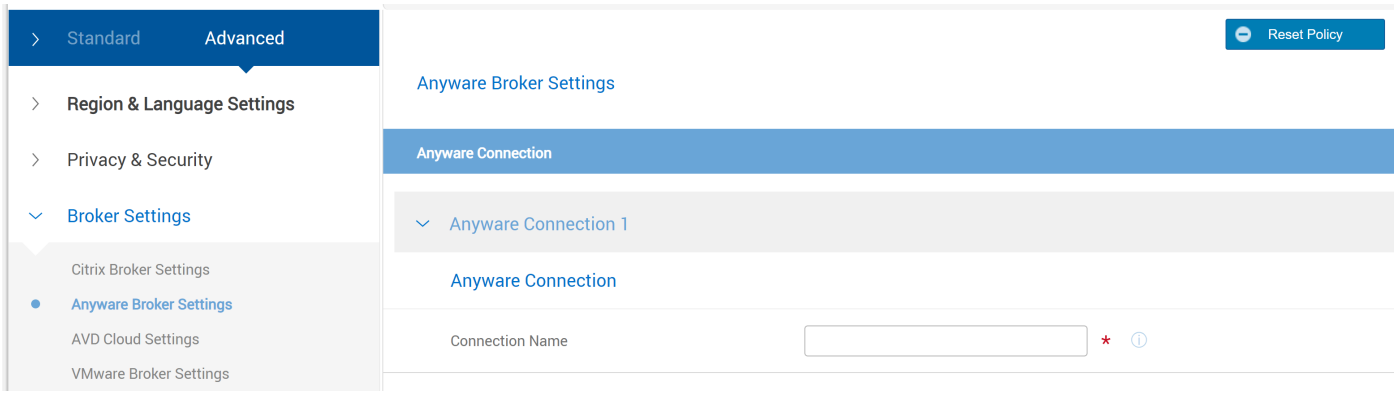


Figure 70. Connection Name

- **Host Type -** Enable if you want to enable hard host. The default is connection broker.

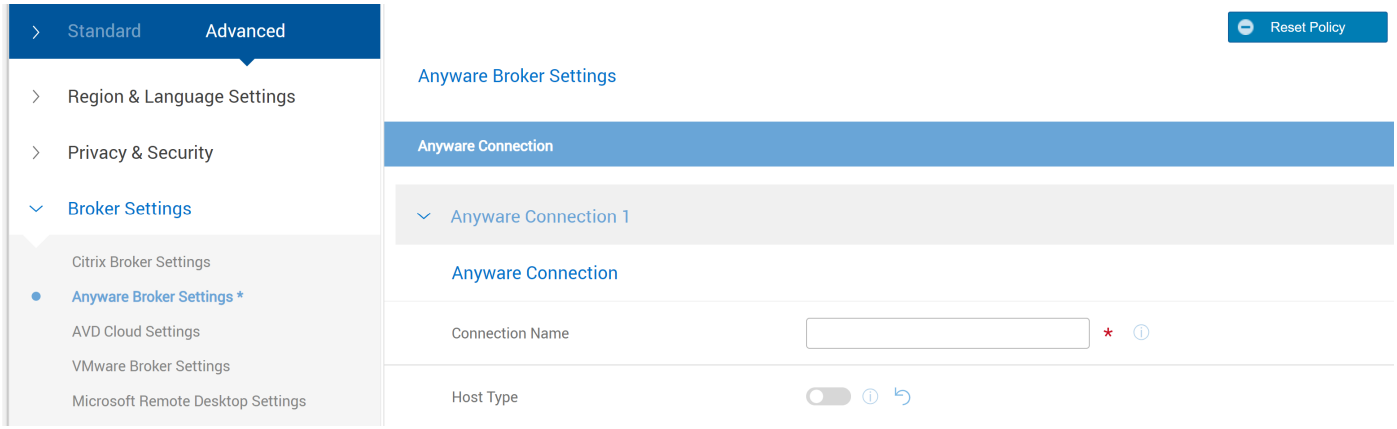


Figure 71. Host Type

- **Host:**
  - **Hard Host (If Host type is enabled) -** Specify the Anyware Hard Host IP or URL where the remote workstation card agent is installed.

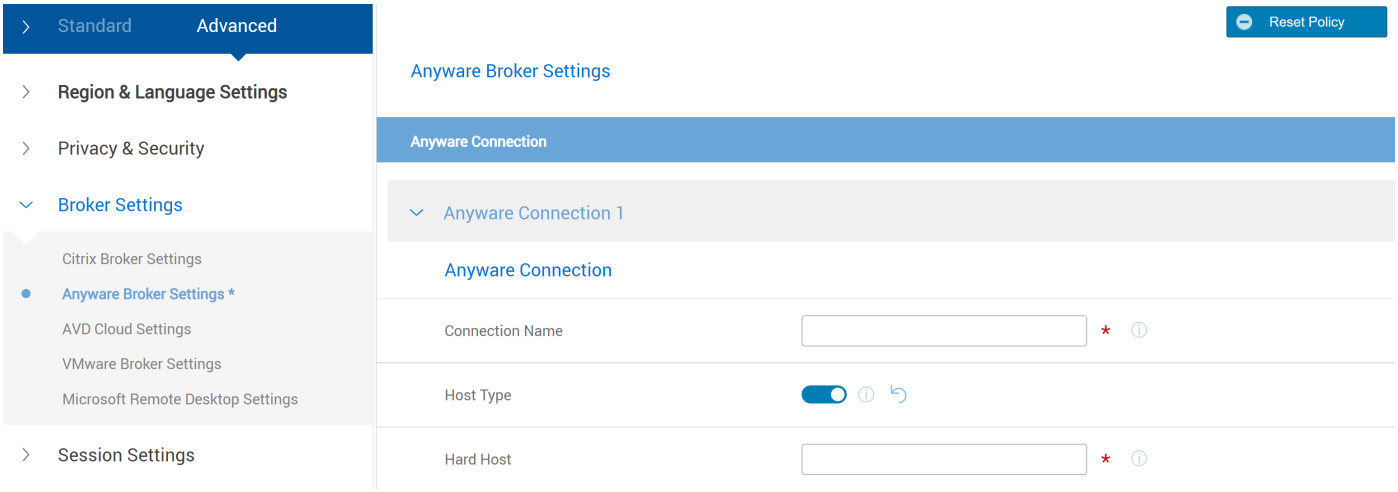


Figure 72. Hard Host

  - **Host (If Hard Host is disabled) -** Specify the connection broker IP or URL where the Anyware agent is installed.

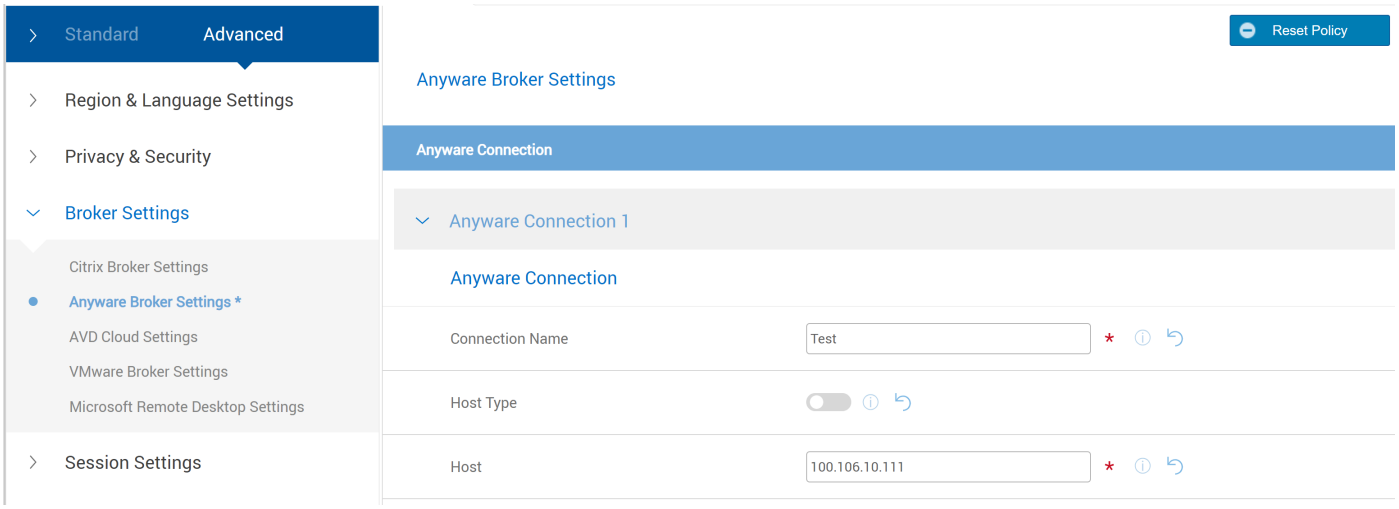


Figure 73. Host

- **Username -** Enter the username that is sent to the connection broker.

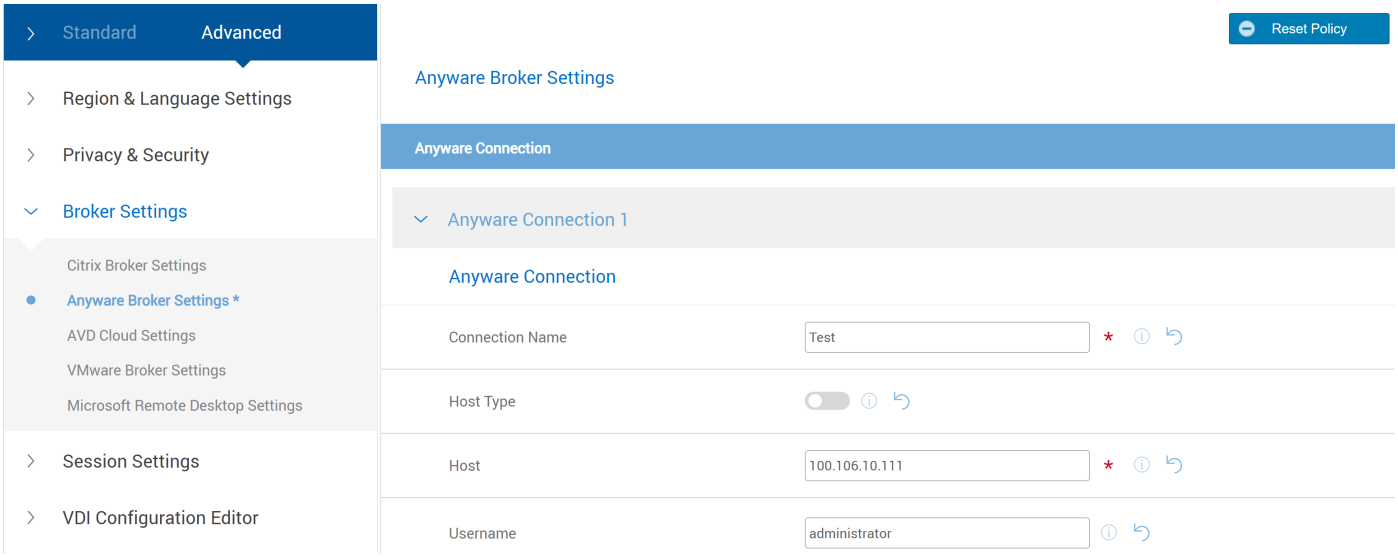


Figure 74. Username

- **Password -** Enter the password that is sent to the connection broker.

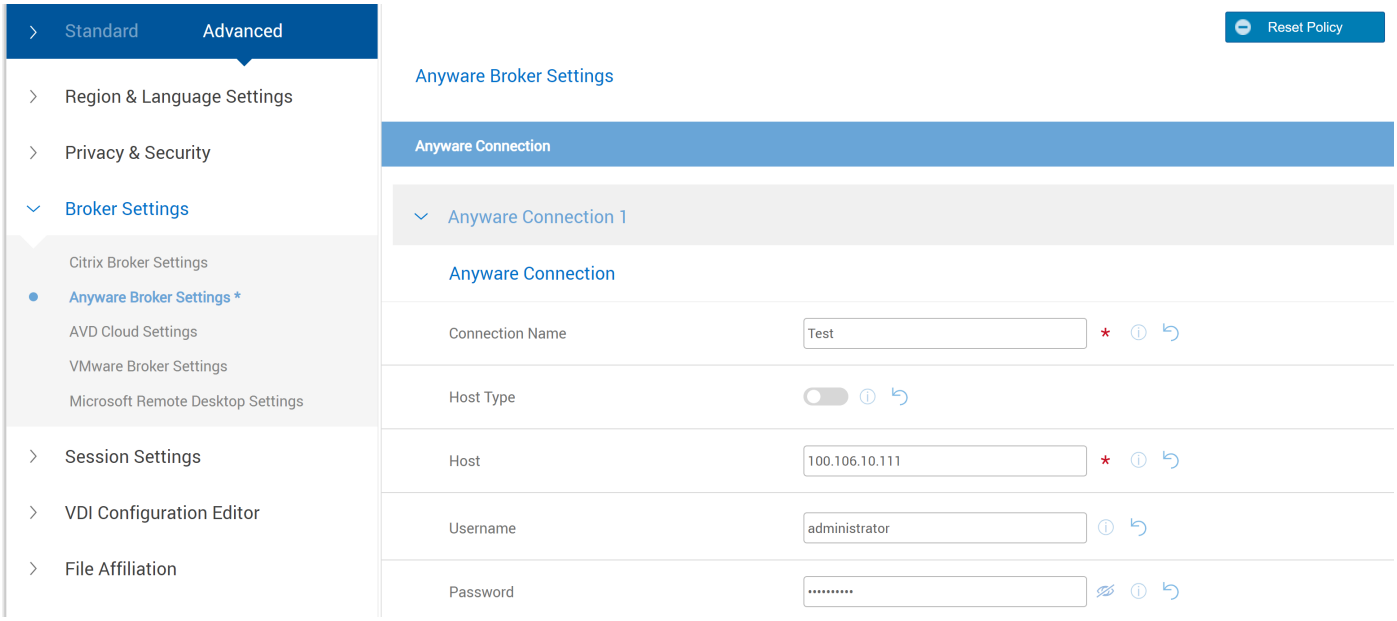


Figure 75. Password

- **Domain -** Enter the domain that is sent to the connection broker.

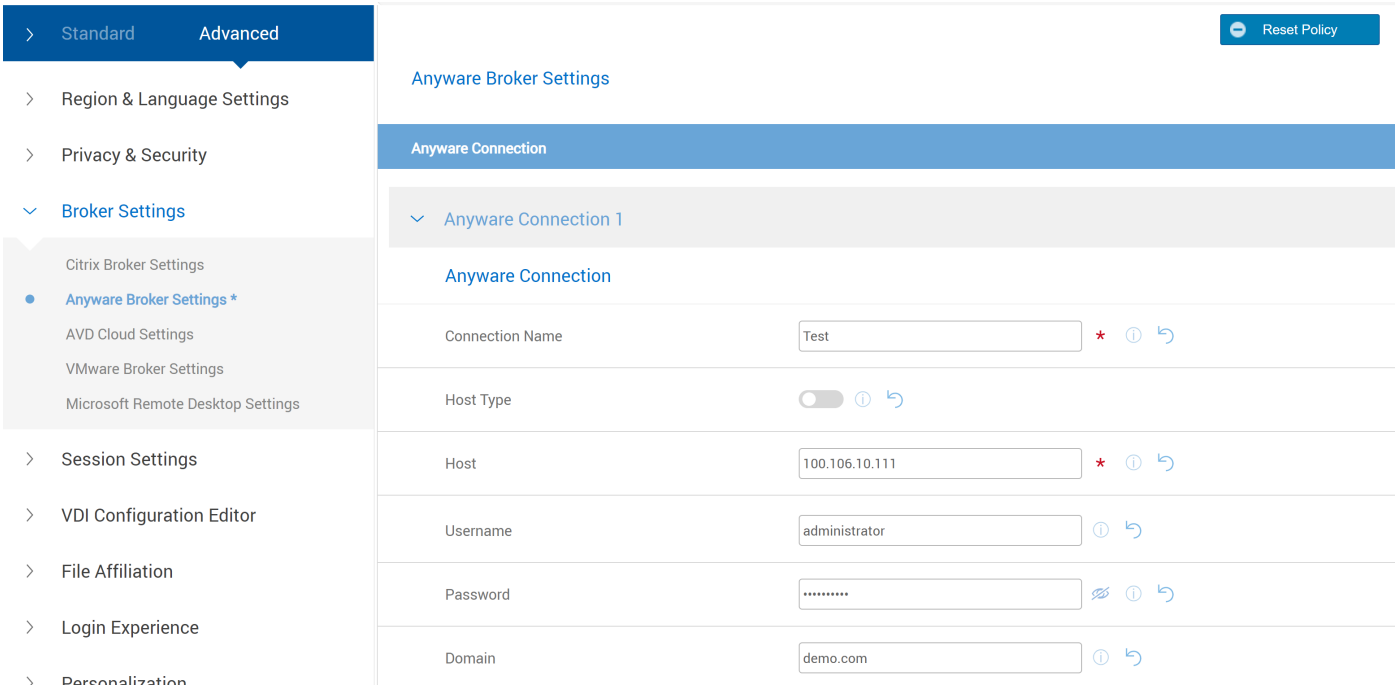


Figure 76. Domain

- **Security Mode -** Select the security mode as Low, High, or Medium.

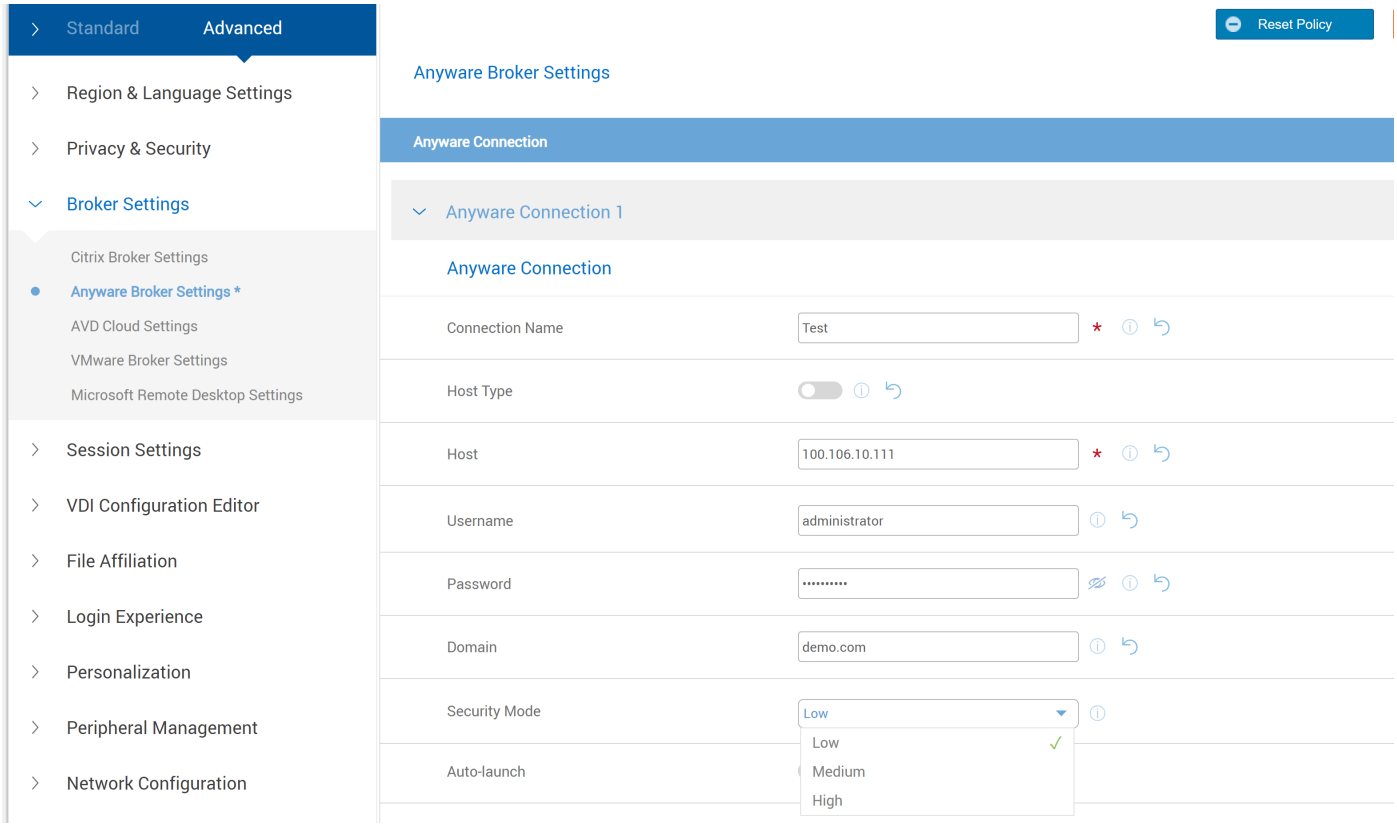


Figure 77. Security Mode

NOTE: If Security Mode is set as High, then you must upload the domain certificate in WMS.

Go to **WMS** > **Dell Hybrid Client 2.x** > **Advanced Settings** > **Privacy & Security** > **Certificate**.

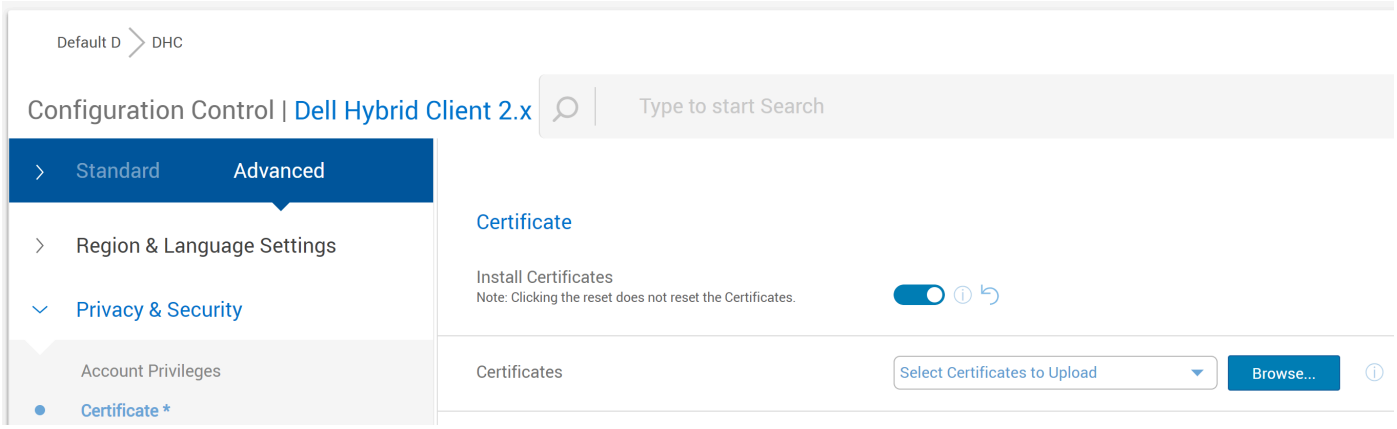


Figure 78. Certificate

- **Auto-launch -** Enable the toggle key if the connection must be auto launched.

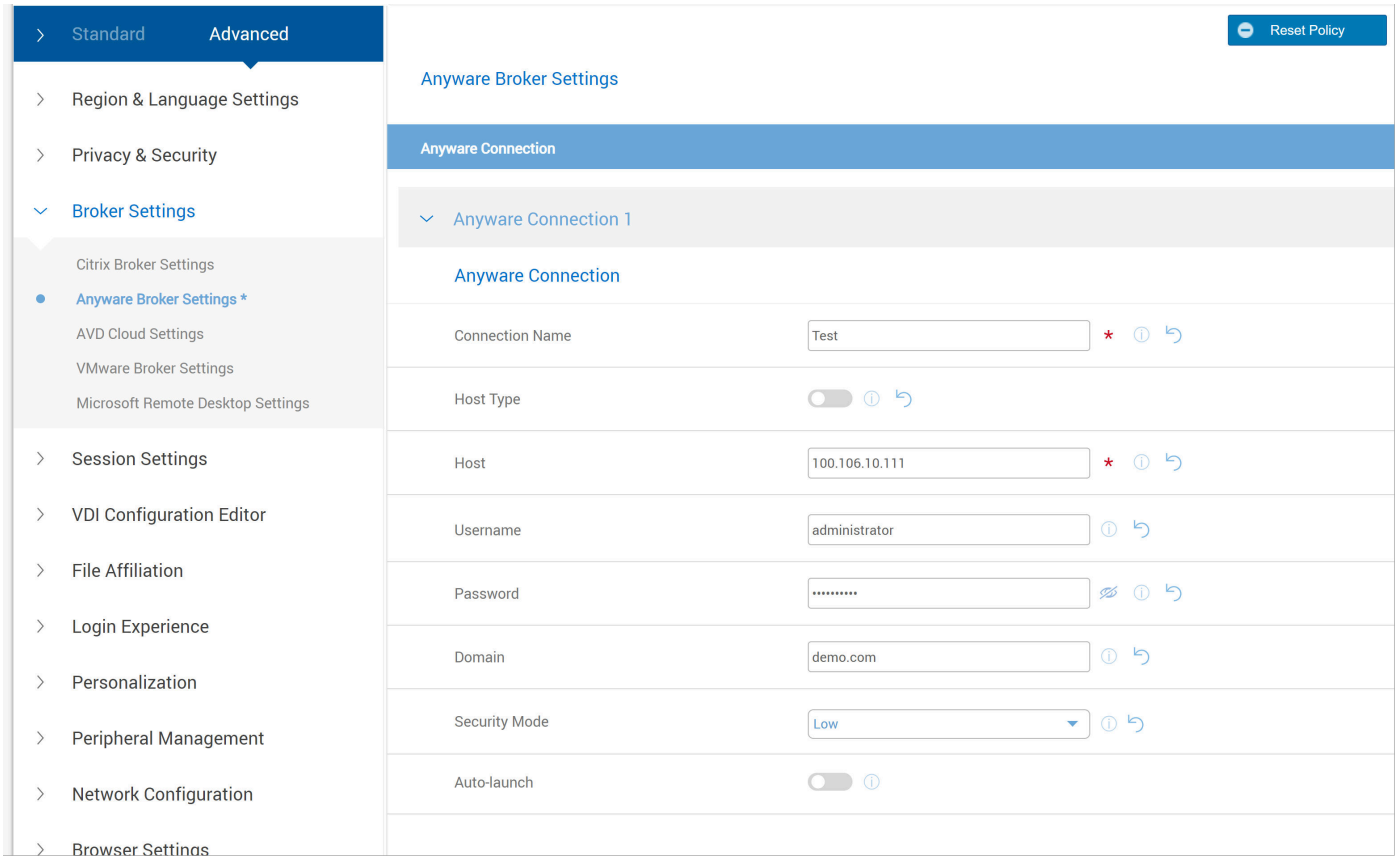


Figure 79. Auto-launch

Configuring Anyware Session Settings from Wyse Management Suite

This session describes the procedure to configure the Anyware session settings using Wyse Management Suite.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced Settings**.
5. Expand **Session Settings** and click **Anyware Session Settings**.
6. You can configure the following session settings.

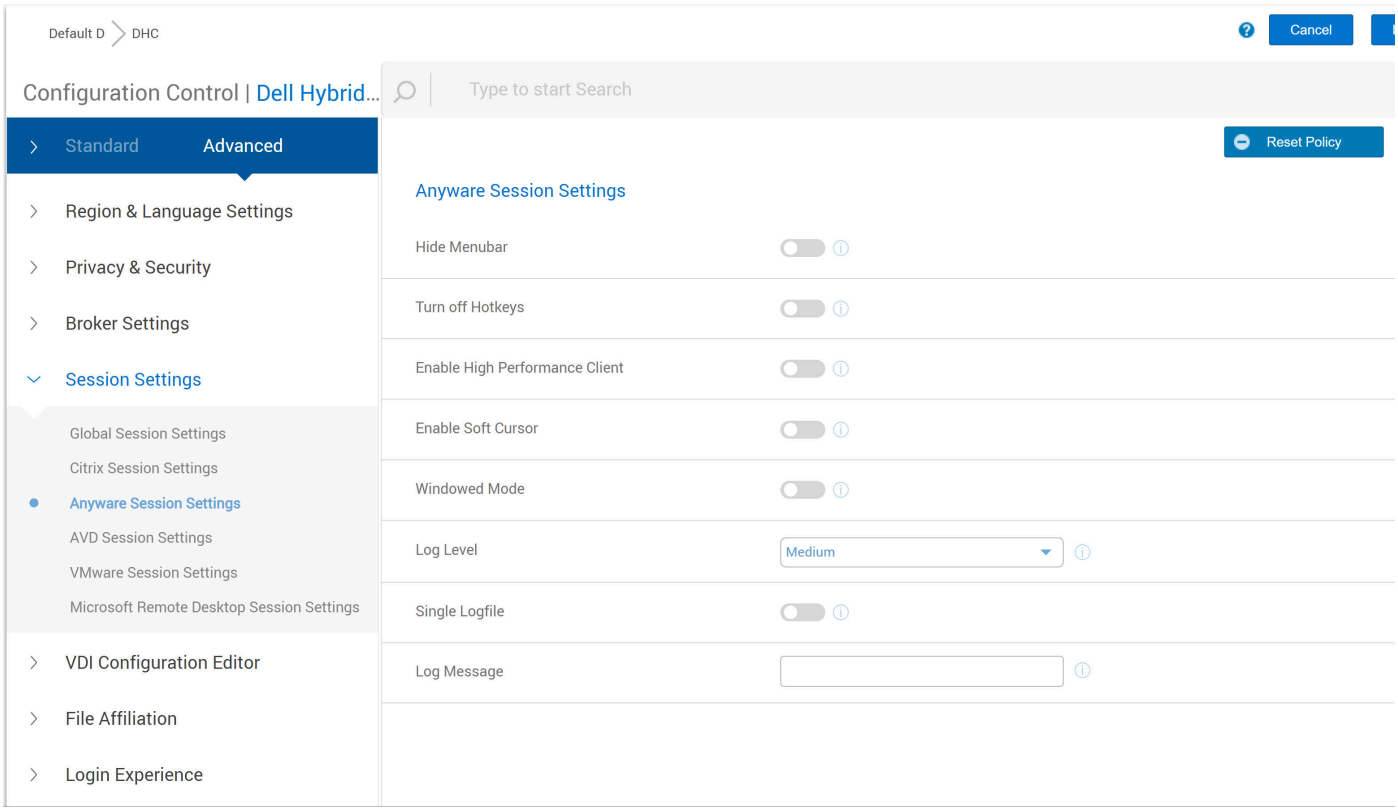


Figure 80. Anyware Session Settings

- **Hide Menubar** - Enable to disable the menubar.

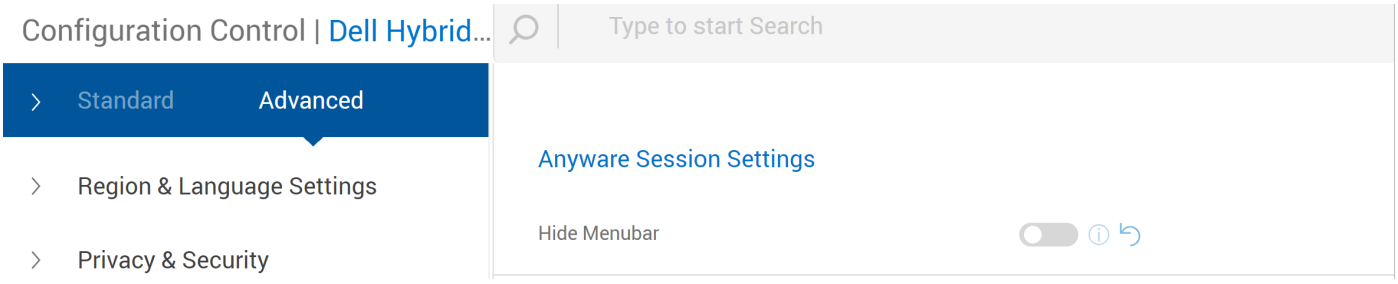


Figure 81. Hide Menubar

- **Turn off Hotkeys** - Enable to disable the Hotkeys.

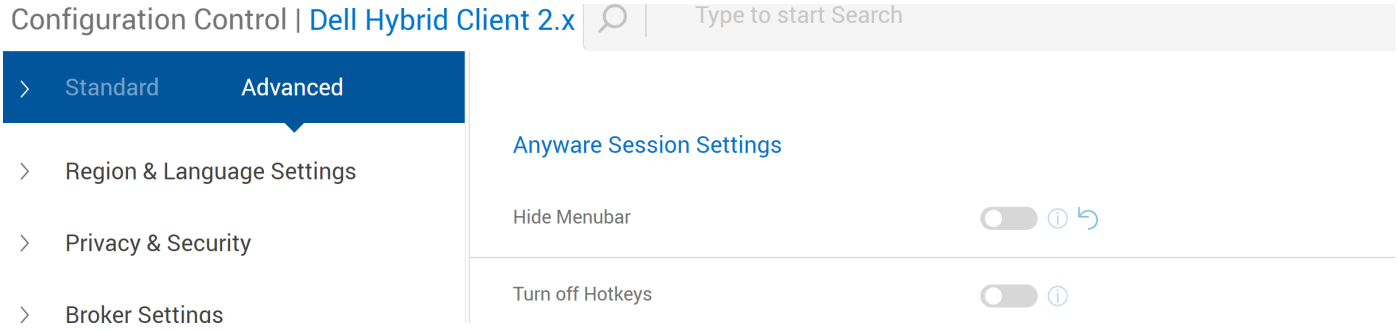


Figure 82. Turn off Hotkeys

- **Enable High Performance Client** - Enable PCoIP High Performance Client.

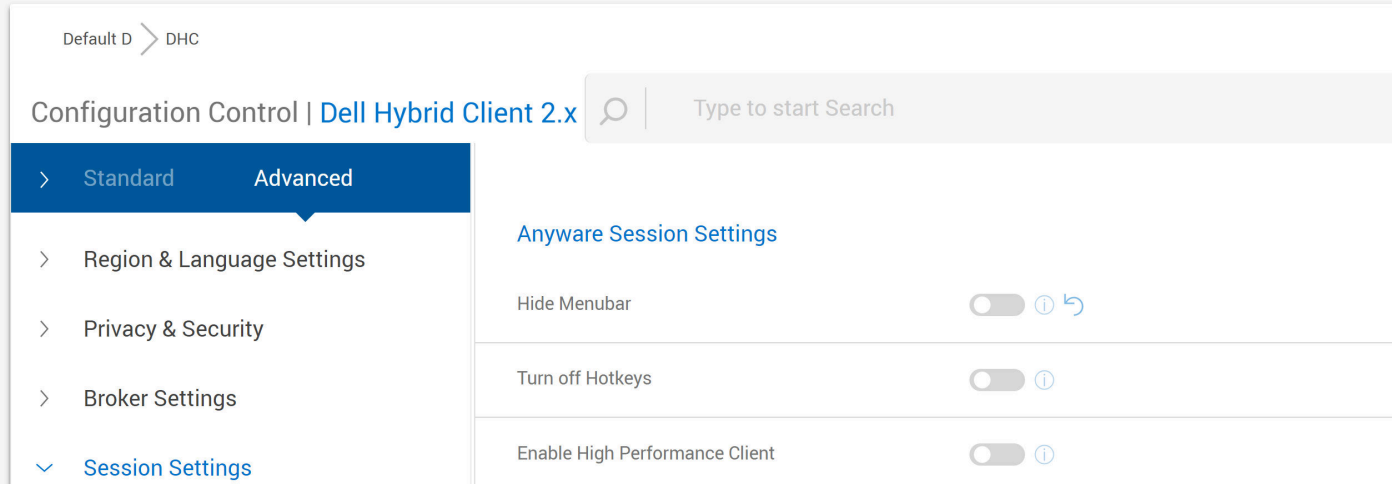


Figure 83. Enable High Performance Client

- **Enable Soft Cursor** - Enable for Software cursor rendering.

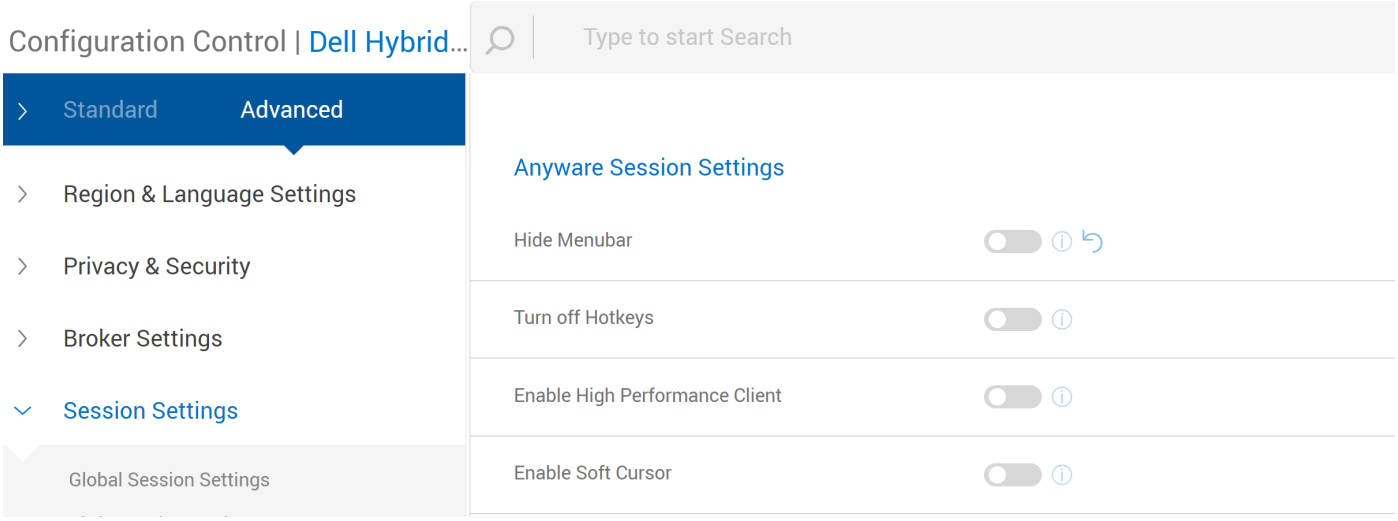


Figure 84. Enable Soft Cursor

- **Windowed Mode** - Enable to launch host in windowed mode.

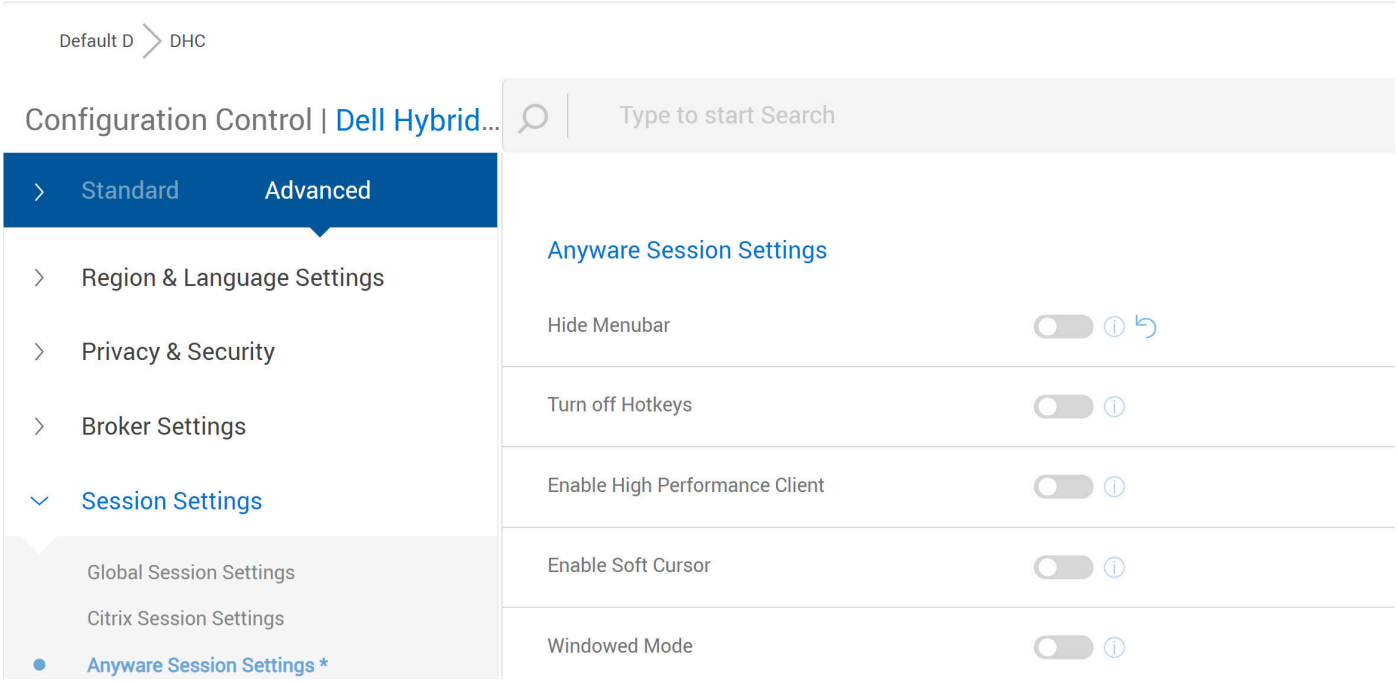


Figure 85. Windowed Mode

- **Log Level** - Select the log level as per your preference.

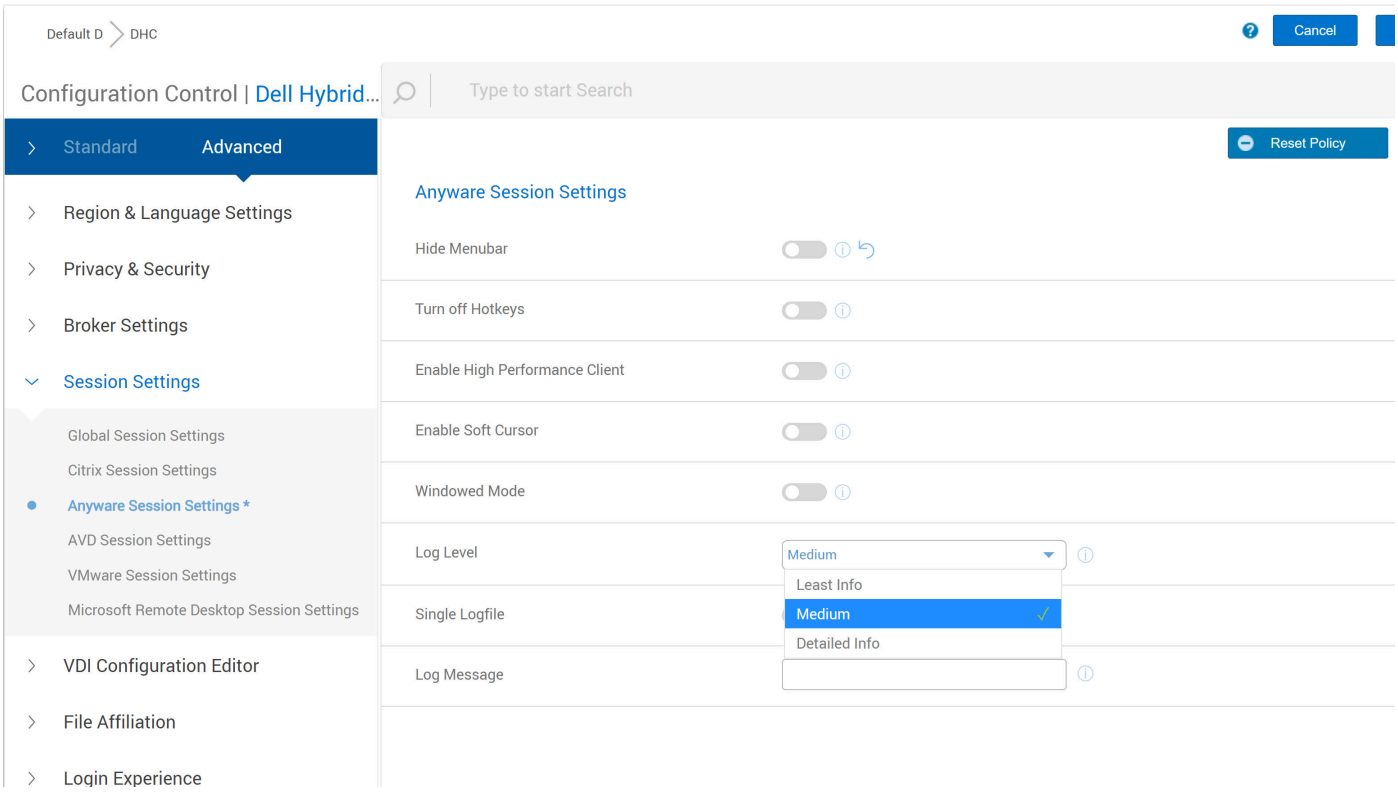


Figure 86. Log Level

- **Single Logfile** - Enable to store all session logs.

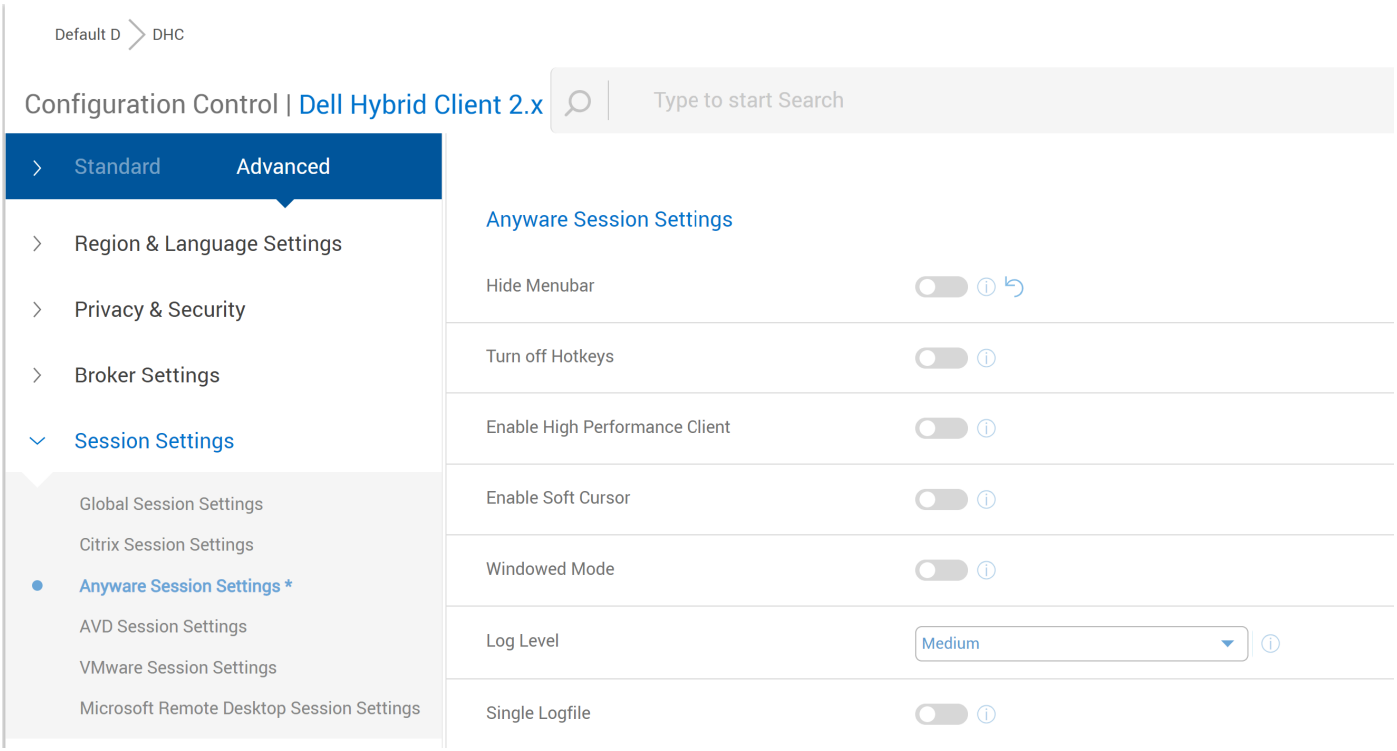


Figure 87. Single Logfile

- **Log Message** - Enter the log message that you want to add to the log file.

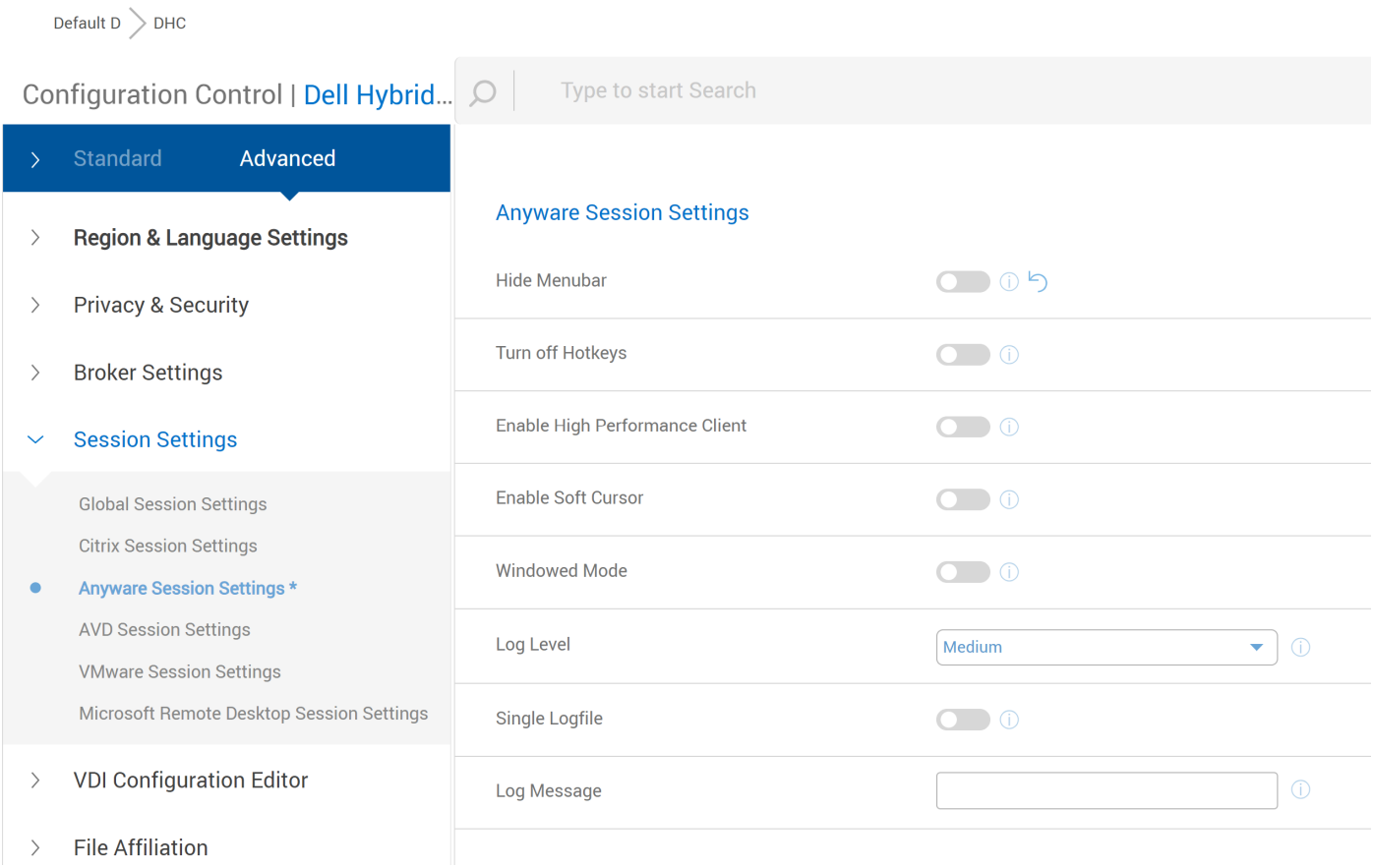


Figure 88. Log Message

NOTE: If you configure session settings values, then it takes effect for broker connection.

Configuring Azure Virtual Desktop

Azure Virtual Desktop(AVD), formerly known as Windows Virtual Desktop, is a comprehensive desktop and application virtualization service. The AVD client enables you to access the virtual desktops and applications that are hosted on Azure cloud and on-premises infrastructure.

This section provides information about how to configure an Azure Virtual Desktop connection and other AVD features.

NOTE: AVD session performance has been improved in Dell Hybrid Client 2.5.

Dell Hybrid Client supports the following features:

Table 8. Supported Azure Virtual Desktop features

Feature	Description
Single Sign-On	Enables you to log in to Azure Virtual Desktop without asking for username, password, and domain locally. The username, password, and domain are deployed from Wyse Management Suite and Azure Virtual Desktop uses these credentials to log in to the published application.
Cloud workspace	Supports two types of cloud workspace: • **ARMv2**—The new Azure Resource Manager that is integrated into Azure portal. • **MS-Prod**—The classic Windows Virtual Desktop.
Add or delete cloud accounts	Enables you to add or delete a cloud account from the local AVD client.
Add or delete on-premises accounts	Enables you to add or delete a cloud account from the local AVD client.
Add, delete, or edit on-premises connections	Enables you to add, edit, or delete an on-premises connection from the local AVD client. You can also configure these options using Wyse Management Suite.
Autolaunch	Enables you to configure the AVD connection to launch automatically when the user logs in to the client.
Drive mapping	Enables you to associate a local drive with a remote session. Dell Hybrid Client supports up to twenty-six folder paths.
Audio ON/OFF	Enables you to enable or disable audio on the remote desktop.
AVD Multimonitor	Supports AVD multimonitor.

Configure the Azure Virtual Desktop broker settings

Prerequisites

Ensure that you have an Azure Active Directory configured and Azure Virtual Desktop resources are deployed on the Azure cloud.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Broker Settings** , and click **AVD Cloud Settings**.
6. Click the **Enable Azure Virtual Desktop** toggle key to ON state.

   NOTE: By default, the ARMv2 cloud workspace is enabled.

7. Configure the Azure Virtual Desktop session options as per your requirement.
8. Click **Save & Publish**.

Manage Azure Virtual Desktop connections locally

You can use the Azure Virtual Desktop client to manage both cloud and on-premises connections.

Prerequisites

- Ensure that the Azure Virtual Desktop option is enabled from Wyse Management Suite.
- Ensure that you have enabled the cloud connection or on-premises connection from Wyse Management Suite.

NOTE: By default, the Azure Virtual Desktop client is disabled. When you launch the Azure Virtual Desktop client on the local device, a message—`AVD is not configured from WMS. Please configure and try again`—is displayed.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
3. Click the Azure Virtual Desktop client icon.

   Azure Virtual Desktop cloud connections and on-premises connections are displayed. If SSO is configured, the hosted desktops and applications are automatically listed on the screen. If SSO is not configured, the Azure Virtual Desktop client prompts the user to enter the username and password. Upon successful authentication, the hosted desktops and applications are displayed. Azure Virtual Desktop session login does not support SSO on first login.
4. To add a cloud account, click the **+** icon next to the **AVD CONNECTIONS** section.

   NOTE: You can use the delete icon to remove an existing cloud account.

   NOTE: Both list view and grid view are supported for listing the connections.
5. To add an on-premises connection, click the **+** icon next to the **ON-PREMISES CONNECTIONS** section.

   NOTE: You can use the edit icon on the configuration tab to modify connections settings for the existing on-premises connection. You can use the delete icon to remove the on-premises connection.

   NOTE: Both list view and grid view are supported for listing the connections.
6. To launch a desktop or an application, double-click the corresponding icon.
   The Azure Virtual Desktop client prompts for the password.

   NOTE: Use the refresh connection option to refresh a connection for a specific user account. Clicking this option refreshes connections and reloads all the hosted desktops and applications.
7. Enter the password.
   Upon successful authentication, the desktop or application is launched on the screen.

Connect to an Azure Virtual Desktop session

Prerequisites

- Ensure that you have configured the Azure Virtual Desktop Broker settings using Wyse Management Suite. See, Configure the AVD broker connection.
- Ensure that you have enabled the cloud connection or on-premises connection from Wyse Management Suite. See, Configure the AVD broker connection.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
3. Click the AVD client icon.

   AVD cloud connections and on-premises connections are displayed. If SSO is configured, the hosted desktops and applications are automatically listed on the screen. If SSO is not configured, the AVD client prompts the user to enter the username and password. Upon successful authentication, the hosted desktops and applications are displayed.

Azure Virtual Desktop limitations

- Connection shortcuts on the favorite bar for Azure Virtual Desktop connections are not supported. Connections are accessible only from the AVD client.
- Smart card and biometric-based user logins are not supported.
- USB redirection is not supported.
- Remote desktop feed are supported for multi monitor. But the Remote application can only be launched on primary monitor.

Configuring VMware

VMware virtualization enables you to run multiple virtual machines on a single physical machine. VMware Horizon Client is a locally installed software application that communicates between View Connection Server and Dell Hybrid Client. It provides access to centrally hosted virtual desktops from your Dell Hybrid Client.

This section provides information about how to configure a VMware connection and other VMware features using Wyse Management Suite.

Dell Hybrid Client supports the following VMware features that you can configure using Wyse Management Suite:

Table 9. Supported VMware features

Feature	Description
PCoIP, RDP, and Blast protocol support	Specifies the communication protocol that is used to display the VMware desktop.
Non-Interactive Mode	Specifies the mode of connection launch. The noninteractive mode is disabled, it displays all the published application and desktop icons after a successful connection to the server. You can start the applications or desktop sessions based on your choice.
Autolaunch	Enables you to configure the VMware connection to launch automatically when the user logs in to the client. This feature is supported from Dell Hybrid Client version 1.6 onwards.
Published Application	Enables you to open a published application from the VMware cloud or server. If disabled, the device connects to a remote desktop session.
Reconnect Application Mode	Enables you to reconnect the last opened application if the VMware session gets disconnected abruptly. The Reconnect Application Mode option is applicable only for PCoIP and BLAST.
Window Resolution	Enables you to set a window resolution for the VMware desktop session.
Auto-Connect USB on Insert	Enables you to automatically connect your USB drive to the device after you plug-in the USB drive.
Automatically Connect USB at Startup	Enables you to automatically connect your USB drive to the device when you start the system.
Client Driver Mapping	Enables you to associate a local drive with the remote session.
Access Removable Storage	Enables you to permit access to use removable storage devices.
USB Redirection	USB Redirection allows the connected USB devices to be redirected from client machines to VMware virtual desktops. You can use a wide variety of USB devices in your VMware session as though the USB devices were physically connected into the session. You can specify the list of USB devices to be allowed based on the Vendor ID, Product ID, Device Class, and Subclass ID.
File Type Association	Establishes the relationship between a file type and a supporting application on the server or the local machine.
Lock Server URL/Host Field	Enables you to lock or unlock the server URL or host field.
Unauthenticated Access	Specifies whether the Horizon client should attempt to log in anonymously to the server.
Desktop Name	Specifies the VMware published desktop name.
Minimized Mode	Enables you to launch a desktop or an application in minimized mode.

Table 9. Supported VMware features (continued)

Feature	Description
Security Mode	Enables you to define the security mode
UDP	Enables the User Datagram Protocol (UDP) communications protocol for VMware.
Auto Hide Toolbar	Enables you to automatically hide the toolbar in the VMware session window.
Full screen Mode for VMware Connection Window	Enables you to launch the VMware connection window in the full screen mode.
Full screen Drop-down Menu Bar	Specifies whether the drop-down menu bar should be enabled in the full screen mode.
Exit On Disconnect	Specifies whether the Horizon server should not retry connecting if there is a connection error.

VMware Installation

VMware View Client addon must be installed in Dell Hybrid Client through **Apps & Data** > **App Policies** > **Dell Hybrid Client** from Wyse Management Suite.

Configure VMware Broker Connection from Wyse Management Suite

This section provides the procedure to configure the VMware broker connection using Wyse Management Suite.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Broker Settings** and click **VMware Broker Settings**.
6. In the **VMware Connection** section, click **Add Row**.
7. Configure the VMware connection options as per your requirement. You can see this image.
8. Click **Save & Publish**.

Create Connection to Launch a Specific Application from the VMware Server

To create the application specific connection, enter the application name in the **Desktop/Application Name** field.

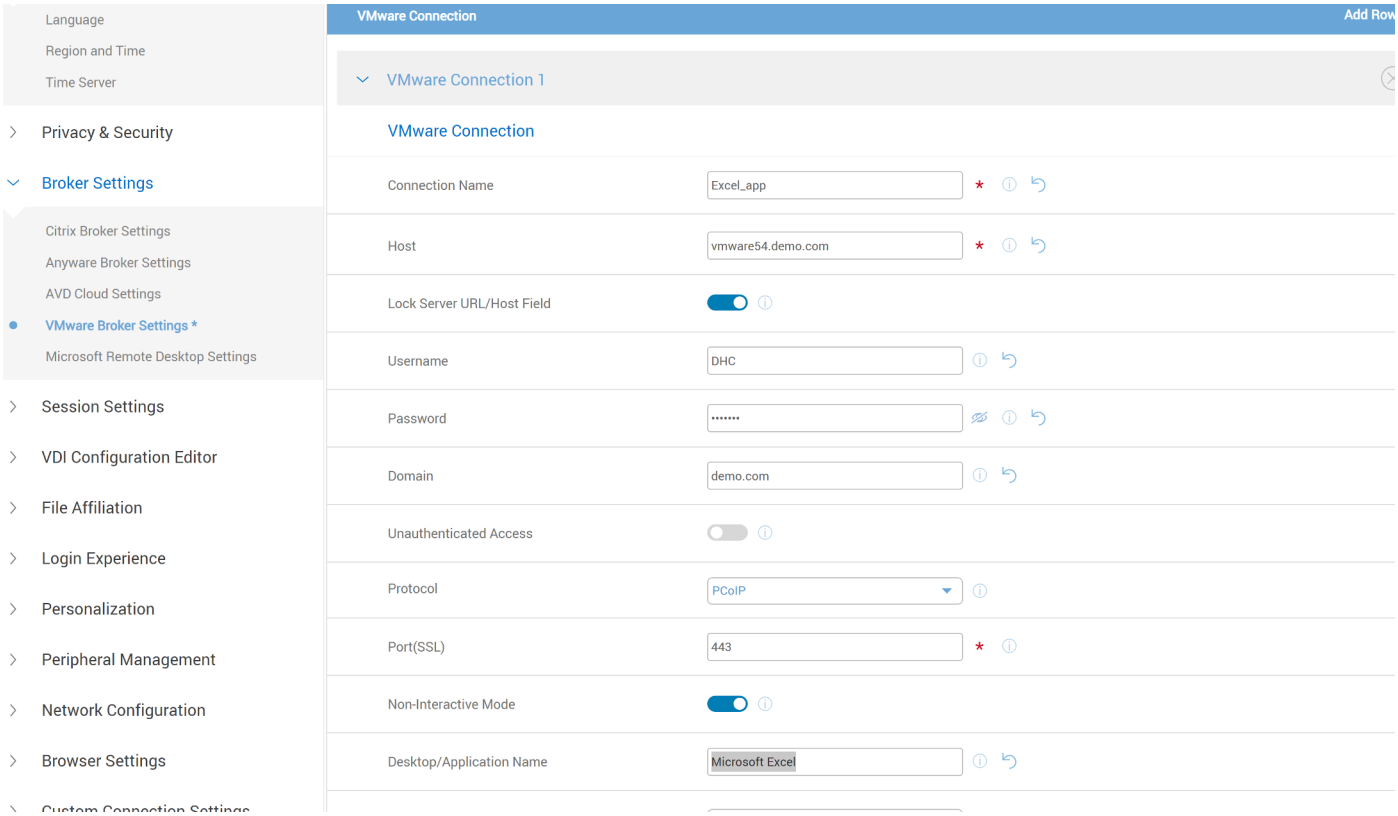


Figure 89. VMware Broker Settings

Create Connection to Launch Multiple Applications from the VMware Server

To create the connection for multiple applications, enter the applications name in the **Desktop/Application Name** field and separate them by a semicolon (;).

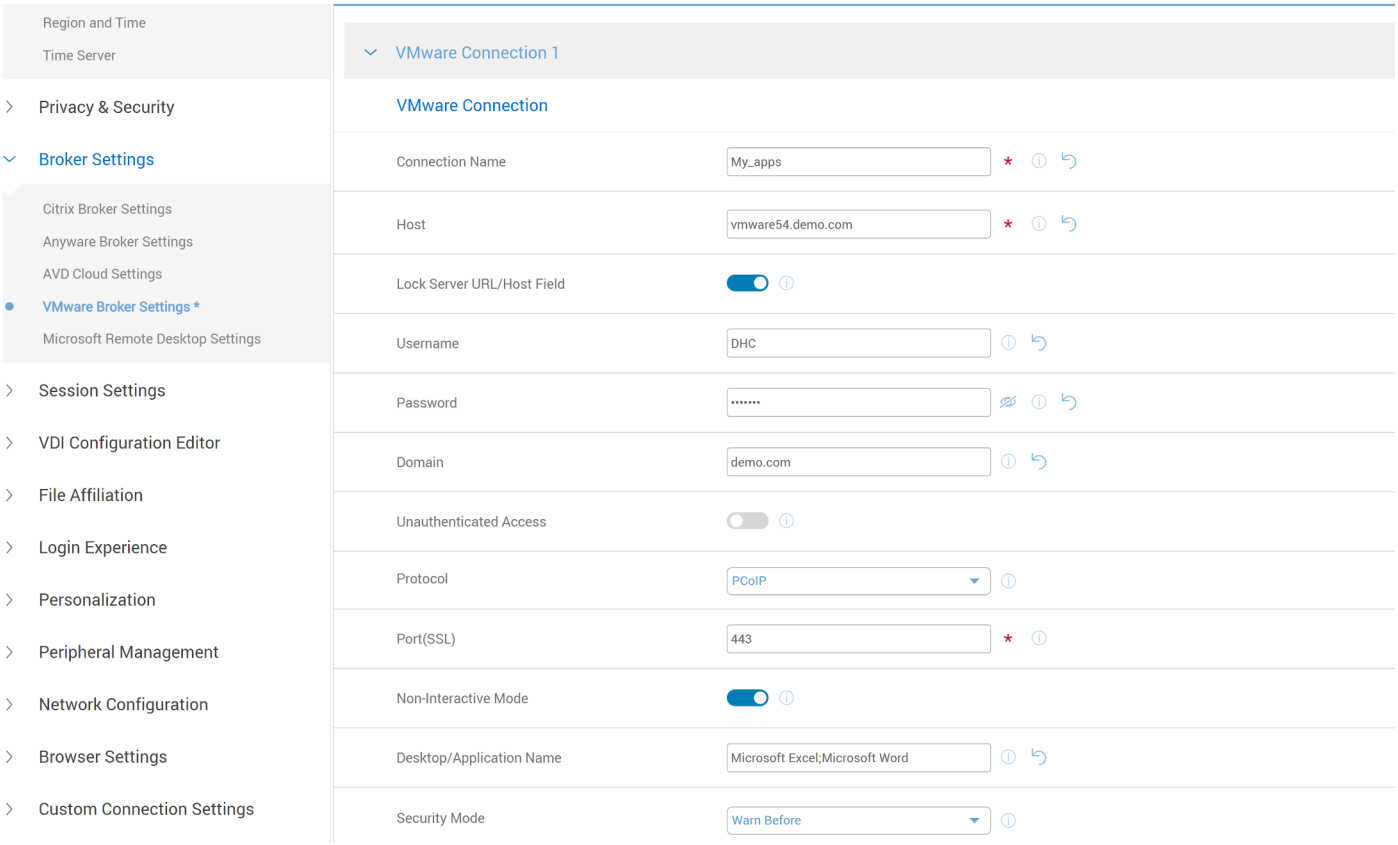


Figure 90. VMware Broker Settings

Create Connection to Launch All Applications from the VMware Server

To create the connection for all applications in the VMware server, do not enter the applications name in the **Desktop/ Application Name** field.

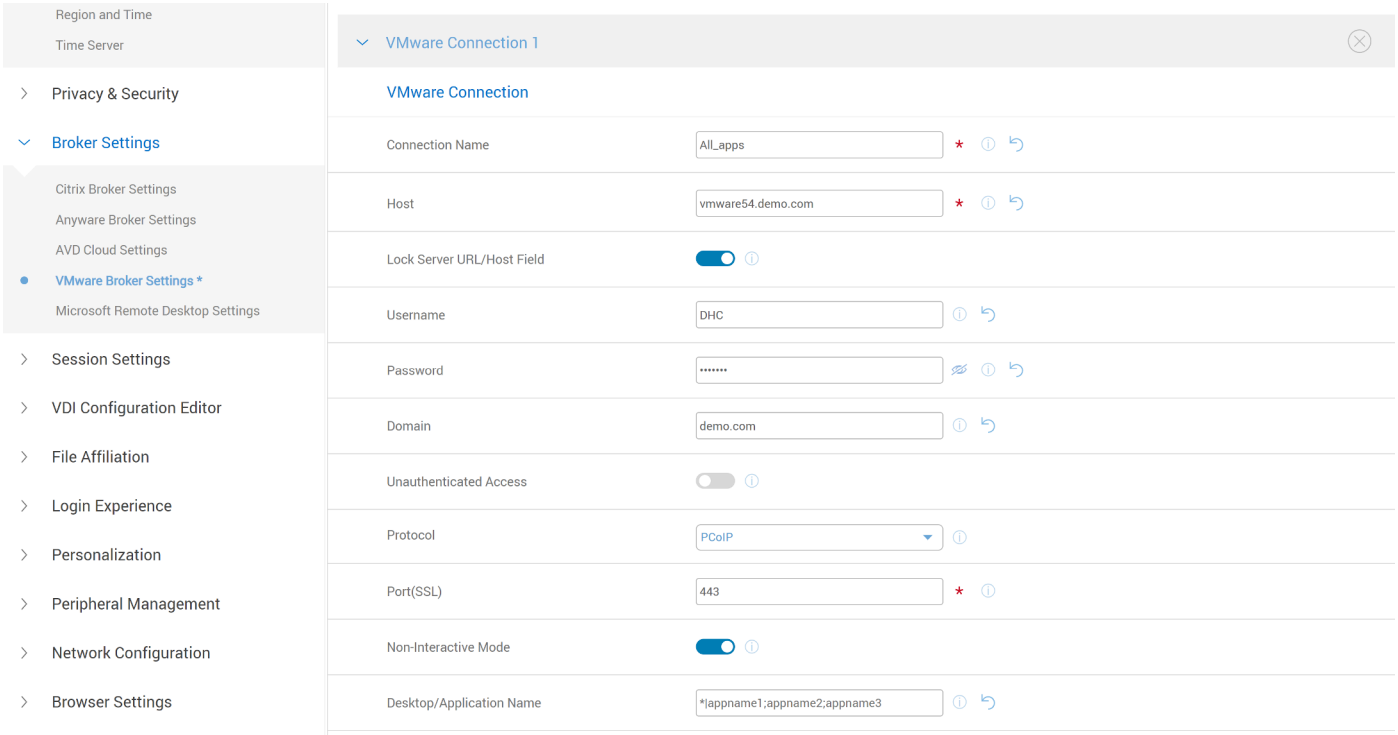


Figure 91. VMware Broker Settings

VMware multiple monitor position support

Dell Hybrid Client 2310 supports configuration of multiple monitors of VMware session.

You can configure the following options for VMware multi monitor position.

- **Auto Reconnect** - Enable to allow auto reconnecting to the connection or application.
- **All Monitors** - Enable full screen mode across all monitors. After you enable this option, you get **Monitors List** option.
  - **Monitors List** - It allows you to specify which adjacent monitors to use for Horizon Client. You can use -monitors=numbered list to specify which subset of the monitors to use, for example - 1,2. The monitors must also be in the format of $DHCP(N) where N is a number that ranges from 128 to 254.
- **Additional Parameters** - You can mention additional parameters, for example - view.allowEnableHEVC none and view.autoConnectDesktop "desktop name".

NOTE: VMware supports monitor id positioning of horizontal multiple monitor setups only.

Configure VMware Session Settings

This session describes the procedure to configure the VMware session settings.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced tab**.
5. Expand **Session Settings** and click **VMware Session Settings**.
6. Configure the following settings:
   - **Basic Settings:**
     - **Minimized Mode -** Enables you to launch a desktop or an application in **minimized mode**.
     - **UDP -** Enables the **User Datagram Protocol (UDP)** communications protocol for VMware.
     - **Auto Hide Toolbar -** Enables you to automatically hide the toolbar in the VMware session window.
     - **Full screen Mode for VMware Connection Window -** Enables you to launch the VMware connection window in the full screen mode.
     - **Full screen Drop-down Menu Bar -** Specifies whether the drop-down menu bar should be enabled in the full screen mode.
     - **Exit On Disconnect -** Specifies whether the Horizon server should not retry connecting if there is a connection error.
     - **Drive Mapping -** Enables mapping of user home directory in the VDI session.
   - **BLAST Protocol Specific Settings:**
     - **Reconnect Applications Mode -** Enables you to reconnect the last opened application if the VMware session gets disconnected abruptly.
     - **H.264 Decoding-** H.264 works by encoding HDMI audio and video signals into an IP stream that can be transmitted over an IP network. A decoder converts the signals back to an uncompressed HDMI format.
     - **H.264 High Color Accuracy -** To allow increased color fidelity when H.264 decoding is allowed in Horizon Client, select the High Color Accuracy.
     - **High Efficiency Video Decoding -** Enables or disables **High Efficiency Video decoding**.
     - **Use OS Proxy Setting -** Enables or disables Blast connections to use operating system proxy settings.

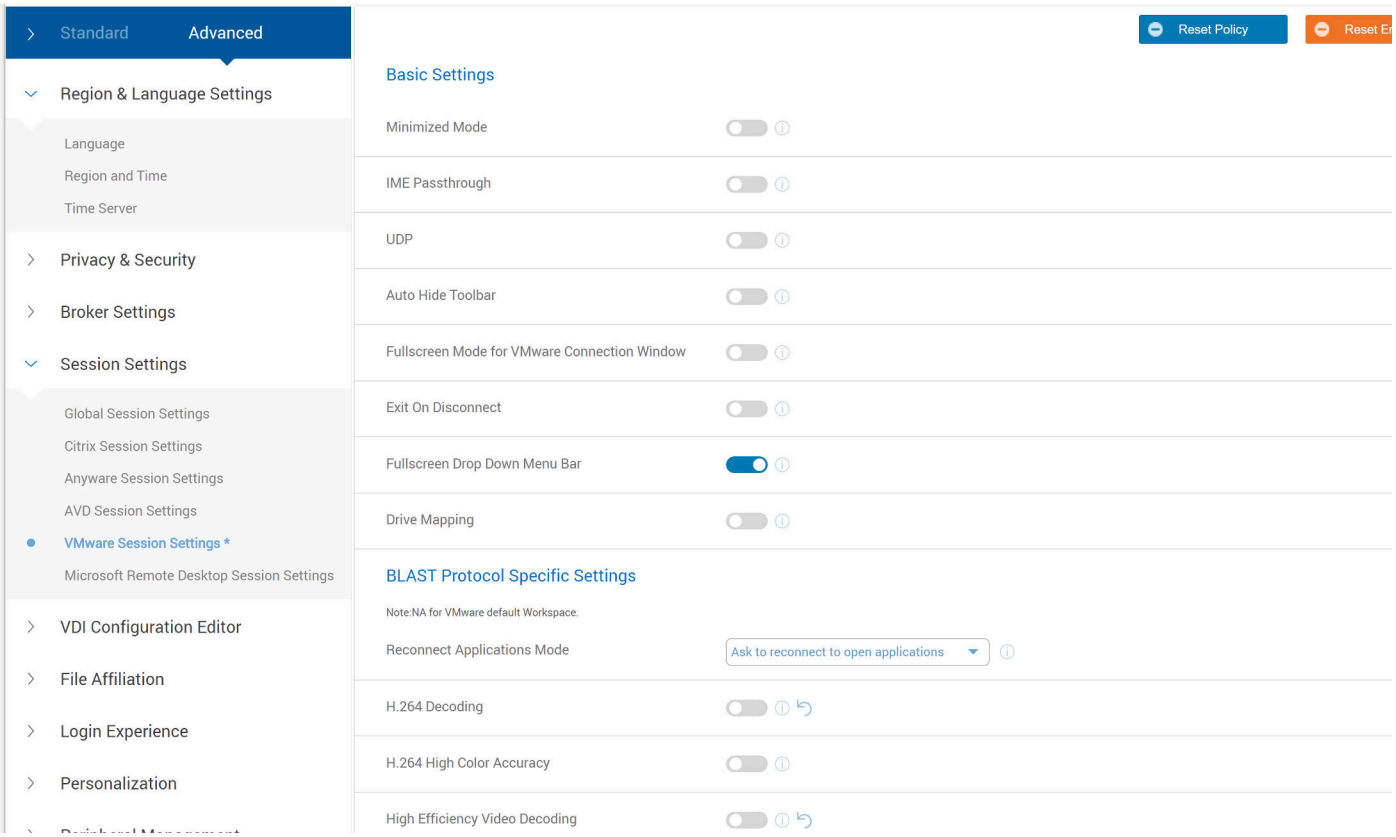


Figure 92. Basic and BLAST Protocol Specific Settings

- **PCOIP Protocol Specific Settings:**
  - **Reconnect Applications Mode -** Enables you to reconnect the last opened application if the VMware session gets disconnected abruptly.
- **USB Redirection settings:**
  - **Auto-connect USB On Insert -** Set auto-connect USB when connected.
  - **Auto-connect USB At Startup -** Set auto-connect USB at startup.

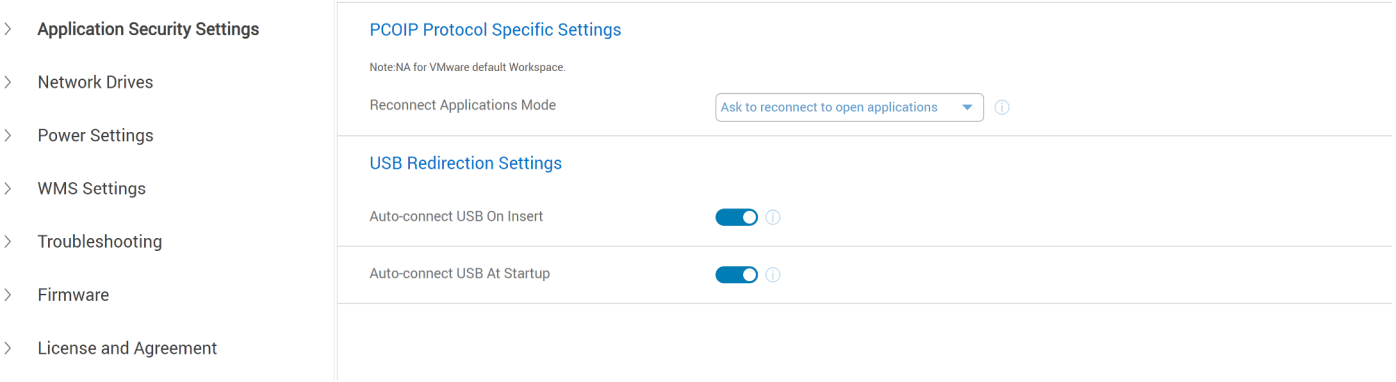


Figure 93. PCOIP Protocol Specific and USB Redirection Settings

NOTE: If you configure session settings values, it takes effect for broker connection.

Connect to a VMware session

VMware virtualization provides hosted desktops and applications through a single platform to end users. VMware Horizon Client is a locally installed software application that communicates between View Connection Server and Dell Hybrid Client. It provides access to centrally hosted virtual desktops from your Dell Hybrid Client.

Prerequisites

Ensure that you have configured the VMware View Client Broker agent settings using Wyse Management Suite. For more information about *Dell Hybrid Client policy settings*, see Configure the VMware Broker Connection from Wyse Management Suite.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
   All the VMware desktops and applications are displayed.
3. Click a desktop icon to launch the published desktop, or click an application icon to launch an application.

VMware connection with DHCP Option Tag

This section provides a procedure to create a VMware connection with DHCP option tags from Wyse Management Suite.

Prerequisites

- Install the **VMware addon** from the latest Dell Hybrid Client package.

Steps

1. Log in to Wyse Management Suite using your administrator credentials.
2. Go to **Groups & Configs** > **Edit Policies** > **Dell Hybrid Client 2.x** > **Advanced**.
3. Click **Broker Settings** and click **VMware Broker Settings** and **Add Row**.

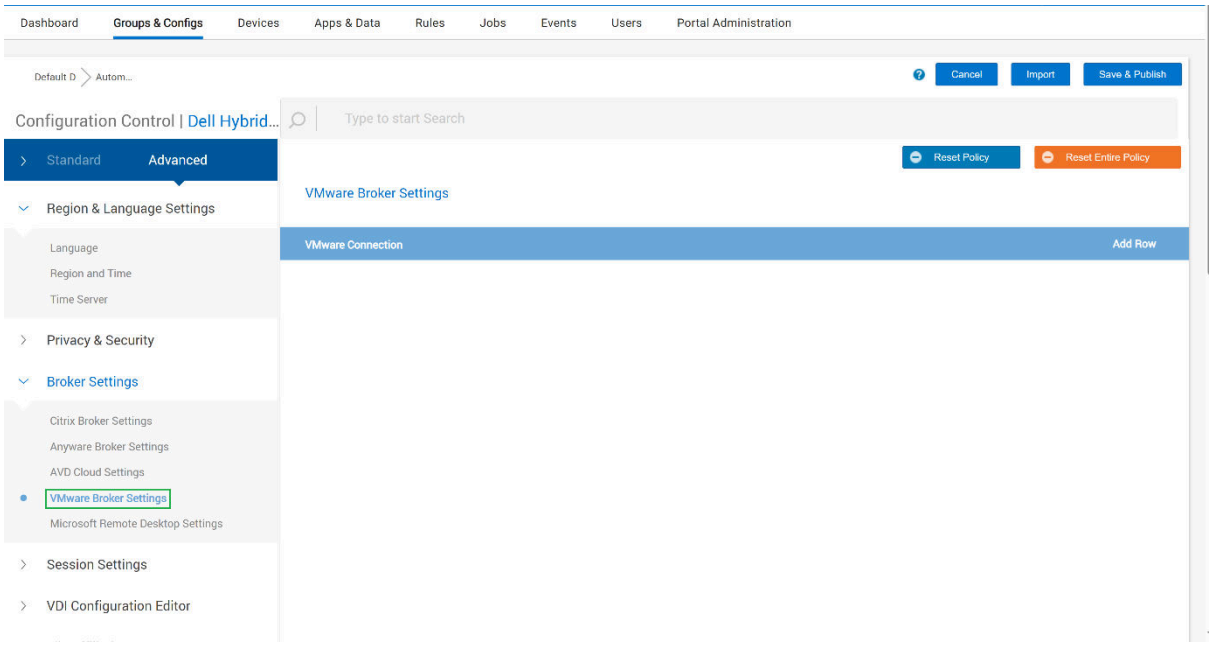


Figure 94. VMware Broker Settings

4. Provide the configured DHCP values: **Connection Name**, **Host**, **Username**, **Password**, **Domain**, and **Port**.

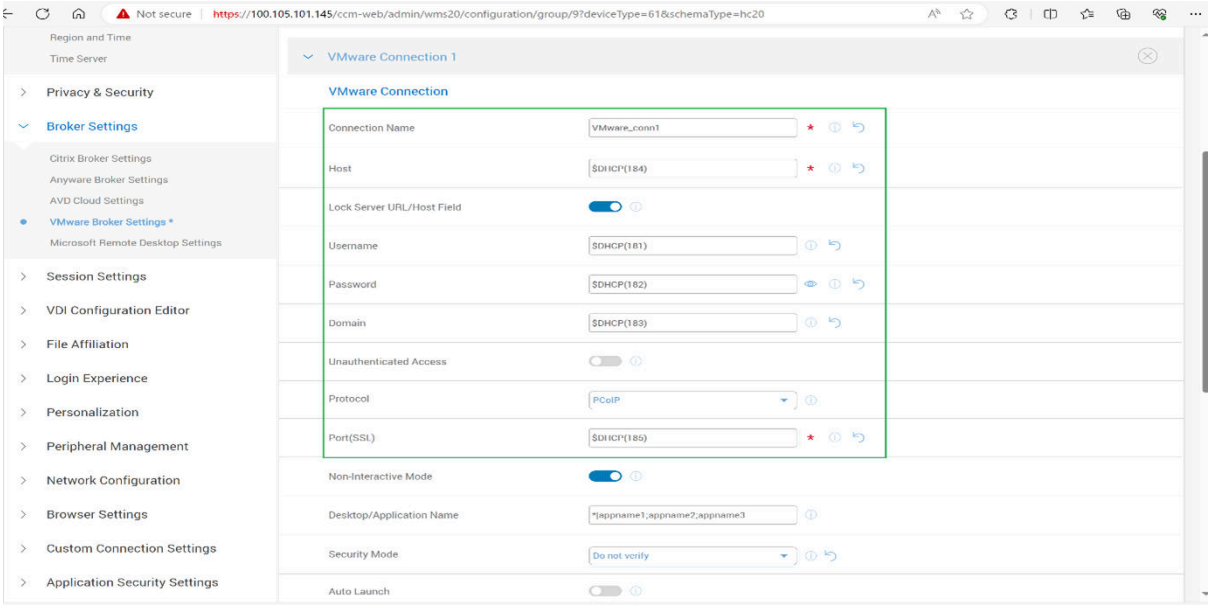


Figure 95. VMware Connection

5. Click **Save & Publish**.
6. Log in to Dell Hybrid Client and click the **VMware connection** icon that is created on the desktop to launch.

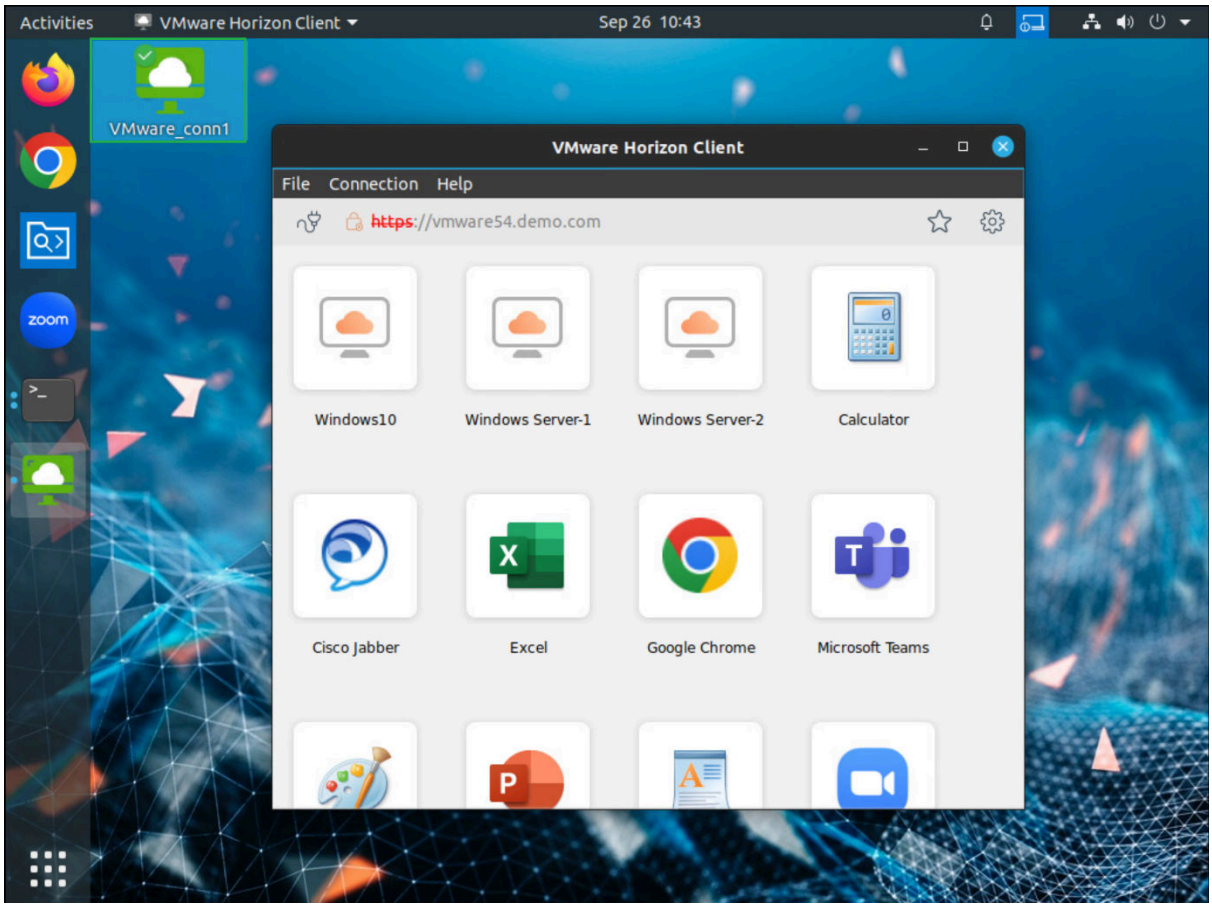


Figure 96. VMware Horizon Client

VMware launches successfully without asking any credentials.

Configuring RDP

Dell RDP allows you to access and manage the data and resources of a remote device using an Internet connection.

This section provides information about how to configure an RDP connection and other Dell RDP features using Wyse Management Suite.

Dell Hybrid Client supports the following Dell RDP features that you can configure using Wyse Management Suite:

Table 10. Supported Dell RDP features

Feature	Description
Single Sign-On support	Enables you to log in to a remote desktop session without asking for username, password, and domain locally.
Autolaunch	Enables you to configure the Citrix connection to launch automatically when the user logs in to the client. This feature is supported from Dell Hybrid Client version 1.6 onwards.
RD Gateway support	Enables you to access remote applications from a web browser when connected to an internal network.
Remote Application	Enables you to access remote applications in an RDP session.
Wallpaper	Enables you to change the wallpaper in an RDP session.
Font Smoothing	Enables font smoothing for remote connections. When you enable this option, fonts appear clear and smooth on the remote desktop.
Menu And Animation	Enables animation for menus and windows on the remote desktop.
Grab Keyboard Events	Enables all keyboard events within the connection window to be sent to the connection applications.
Low Bandwidth	Enables you to handle the network performance based on the network bandwidth.
Window Resolution	Enables you to set a window resolution for the desktop session.
Sound redirection	Enables you to redirect the sound to a local or a remote session.
Color Depth	Enables you to specify the session color mode.
Drive Mapping	Enables you to associate a local drive with the remote session.
Default RDP icon	Enables you to connect to a remote desktop or to use a published application from the desktop that is not configured from Wyse Management Suite.
Server Authentication Level	Server authentication verifies that you are connecting to the intended remote system. The strength of verification required to connect is determined by the option selected—**Connect and Don't warn me**, **Warn me**, and **Do not connect**.
File Type Association	Establishes the relationship between a file type and a supporting application on the server or the local machine.

RDP Installation

RDP addon must be installed in Dell Hybrid Client through **Apps & Data** > **App Policies** > **Dell Hybrid Client** from Wyse Management Suite.

Configuring RDP Broker Settings from Wyse Management Suite

This section provides the procedure to configure the RDP broker settings using Wyse Management Suite.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Broker Settings** and click **Microsoft Remote Desktop Settings**.

6. You can configure the following settings:

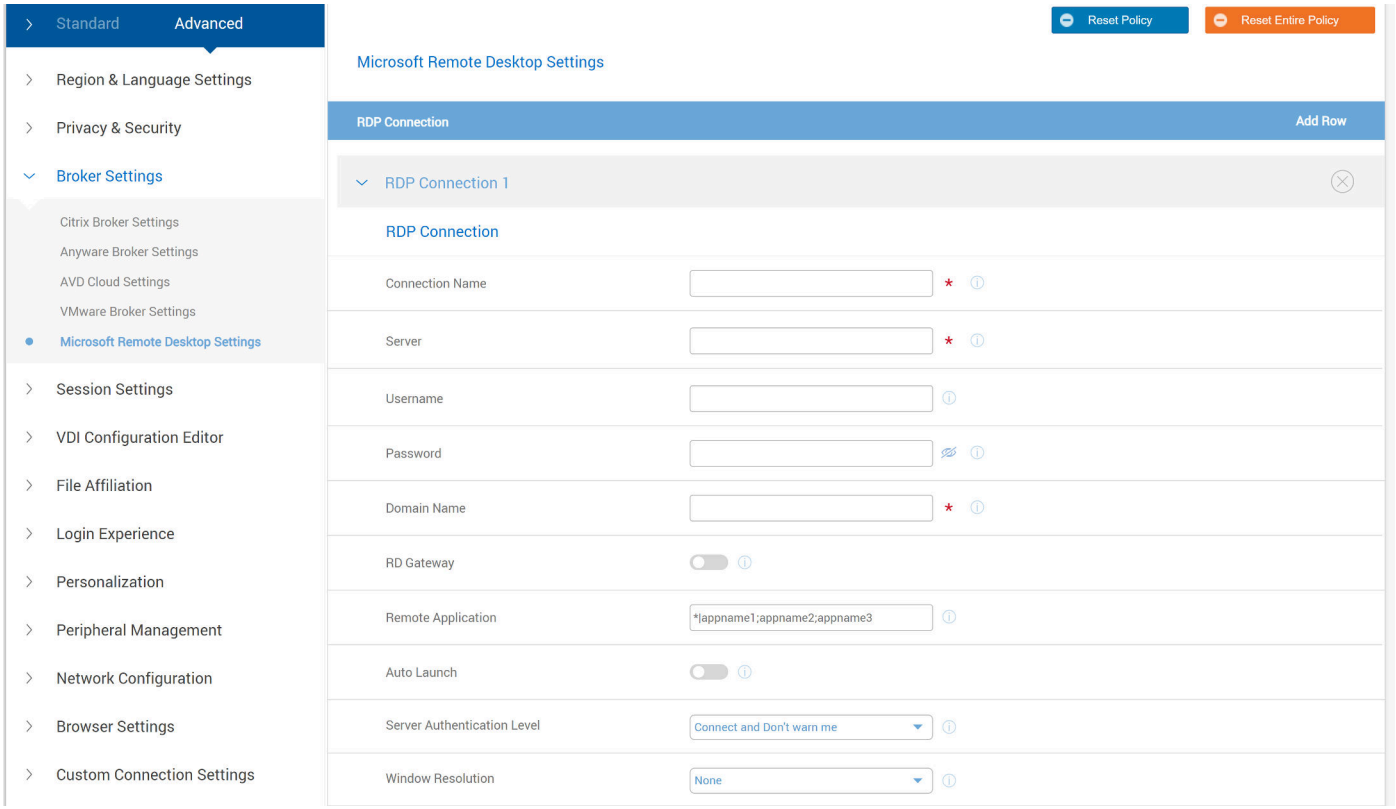


Figure 97. Microsoft Remote Desktop Settings

- **Connection Name** - Enter RDP connection name. A shortcut for RDP is created on Desktop/Favorite.
- **Server** - Specify the server IP address or Server Name.
- **Username** - Specify a username to connect to the application server.
- **Password** - Specify the Password to connect to the application server.
- **Domain Name** - Specify the Domain name.
- **RD Gateway** - Enables you to access remote applications from a web browser when connected to an internal network. You can specify RD Gateway server, RD Username, RD Password, and RD Domain.

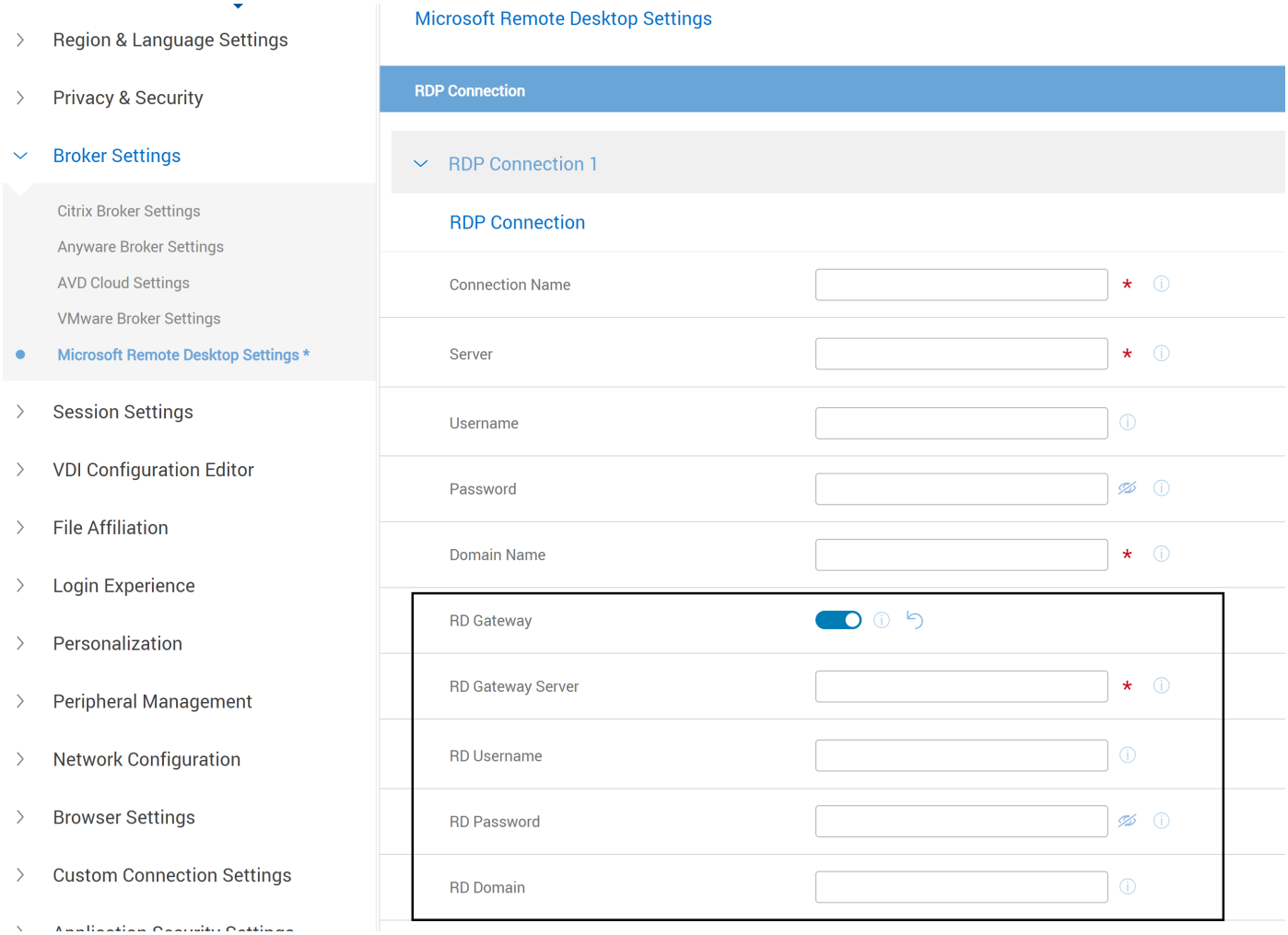


Figure 98. Microsoft Remote Desktop Settings

- **Remote Application** - Enables you to access remote applications in an RDP session. You can specify multiple application names by seperating them by semicolon (;).
- **Auto Launch** - Enables you to configure the Citrix connection to launch automatically when you log in to the client.

  NOTE: If you enter multiple applications, then auto launch is applicable for the first application.
- **Server Authentication Level** - Server authentication verifies that you are connected to the intended remote system. The level of verification must establish the connection is determined by the selected option for connecting.



Figure 99. Microsoft Remote Desktop Settings

- **Window Resolution** - You can select the window resolution from the drop-down.

  NOTE: If you select from Window Resolution from broker settings, then global settings resolution value does not take effect.

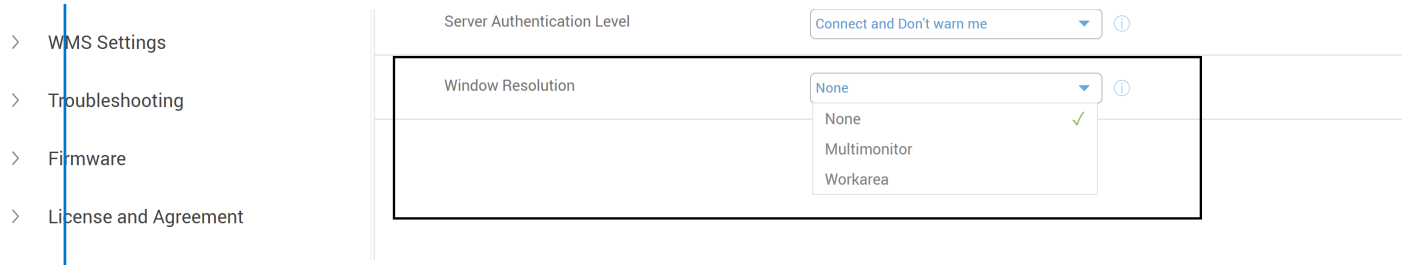


Figure 100. Microsoft Remote Desktop Settings

Configuring RDP Session Settings from Wyse Management Suite

This session describes the procedure to configure the RDP session settings using Wyse Management Suite.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced tab**.
5. Expand **Session Settings** and click **Microsoft Remote Desktop Session Settings**.
6. You can configure the following settings for RDP session.

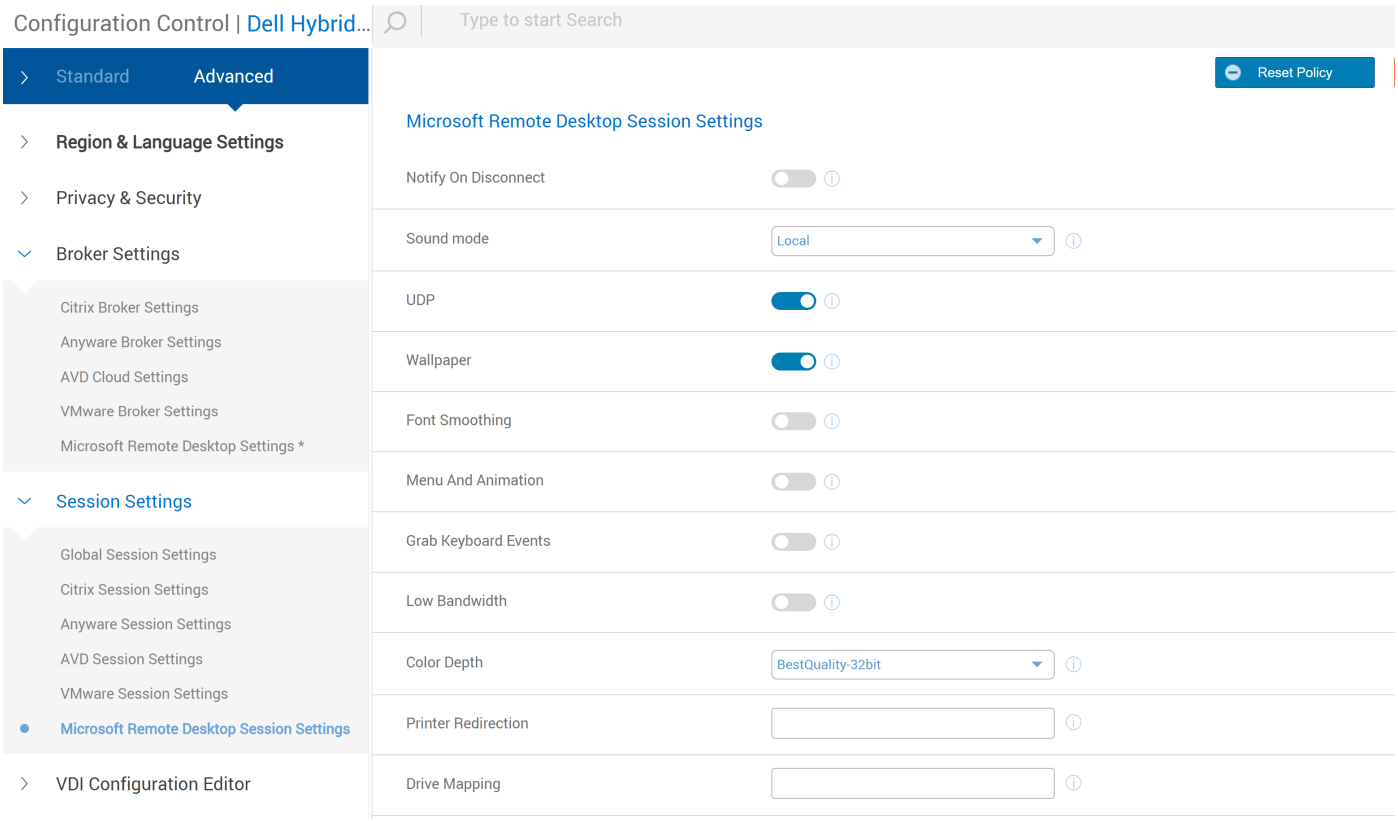


Figure 101. Microsoft Remote Desktop Sessions Settings

- **Notify On Disconnect -** Enable or disable the **Notify On Disconnect** toggle key for turning on or turning off the notification during disconnection.
- **Sound mode -** The drop-down provides two options: **Local and Remote**. Selecting **Local** enables sound on the local machine, While selecting **Remote** enables sound on the remote machine.
- **UDP -** If this option is enabled, it enables the **UDP** networking in the session.
- **Wallpaper -** Enables you to change the wallpaper in an RDP session.
- **Font Smoothing -** Enables the font smoothing when fonts are rendered.
- **Menu And Animation -** Enables the menu and animation in the session.
- **Grab Keyboard Events -** Enables the keyboard event grabbing in any direct RDP connection session.

- **Low Bandwidth -** Enables the low bandwidth connectivity for RDP sessions. After you enable Low Bandwidth, you should select the bandwidth option from the Speed Level drop-down list. The performance is handled based on the bandwidth that you select.

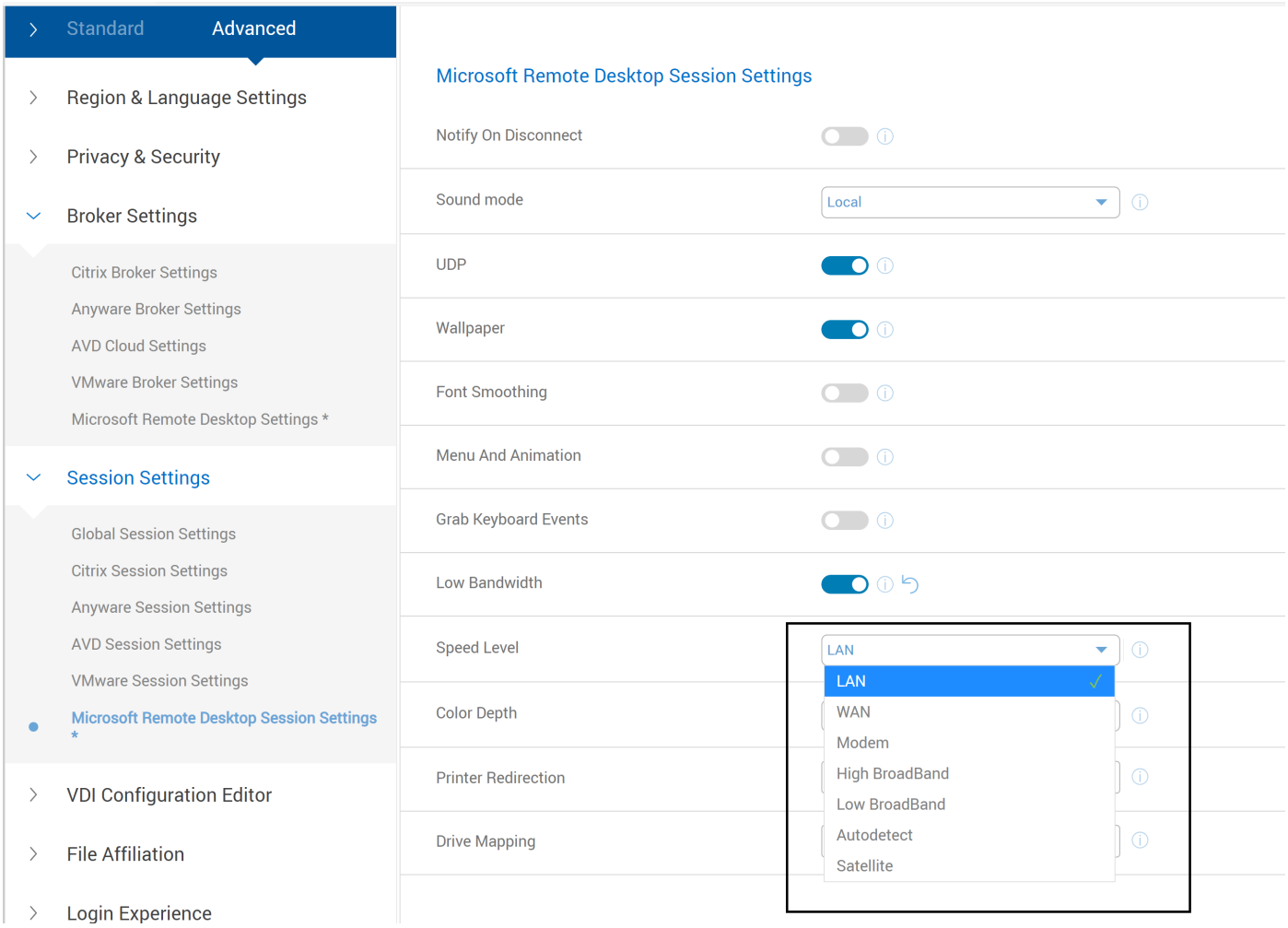


Figure 102. Microsoft Remote Desktop Session Settings

- **Color Depth -** You can select the color mode from the Color Depth drop-down list.

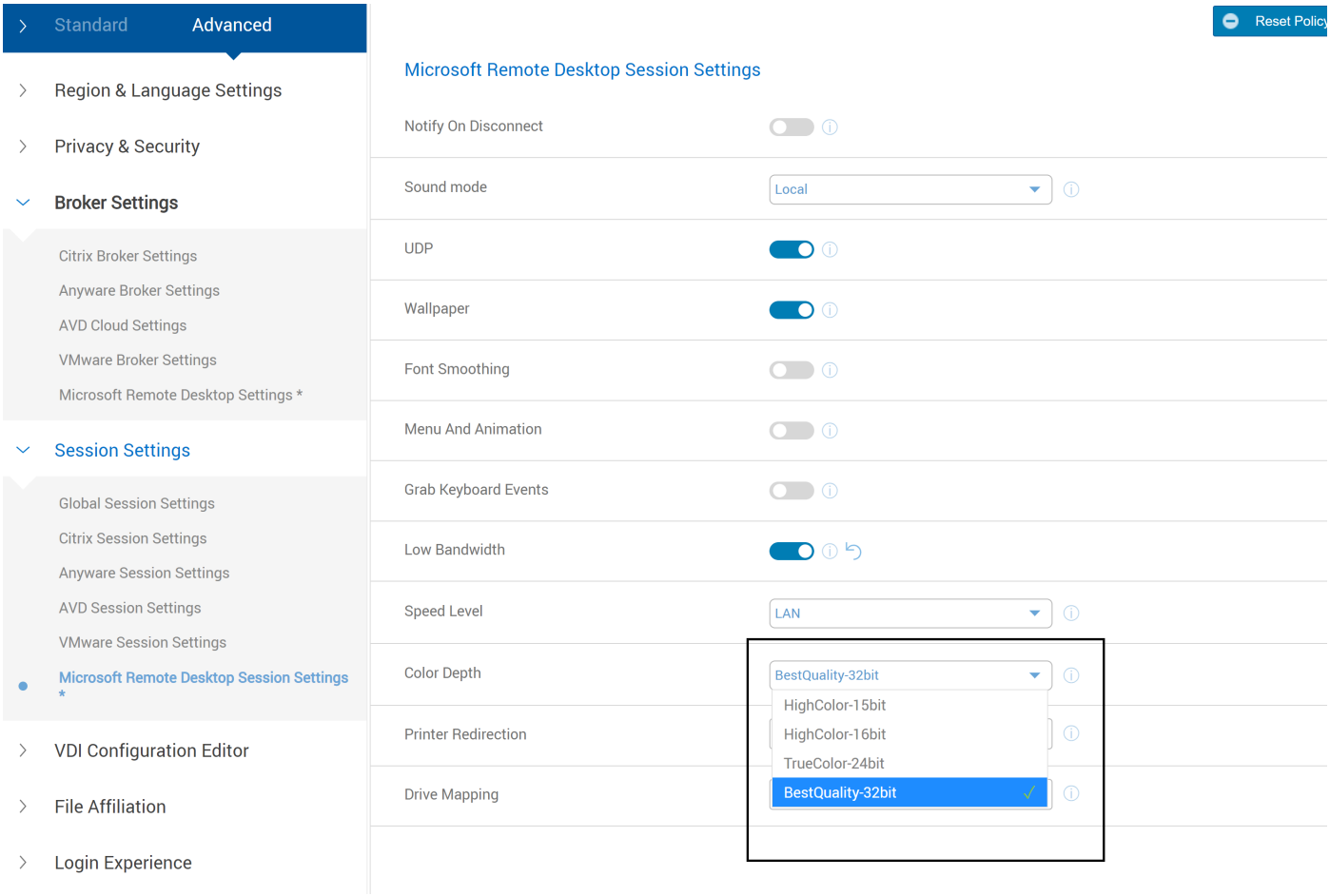


Figure 103. Microsoft Remote Desktop Session Settings

- **Printer Redirection -** You can enter the printer path for printer redirection.
- **Drive Mapping -** You can enter the drive paths for drive mapping. A maximum of 26 drive paths are supported. For example, /tmp/drive.

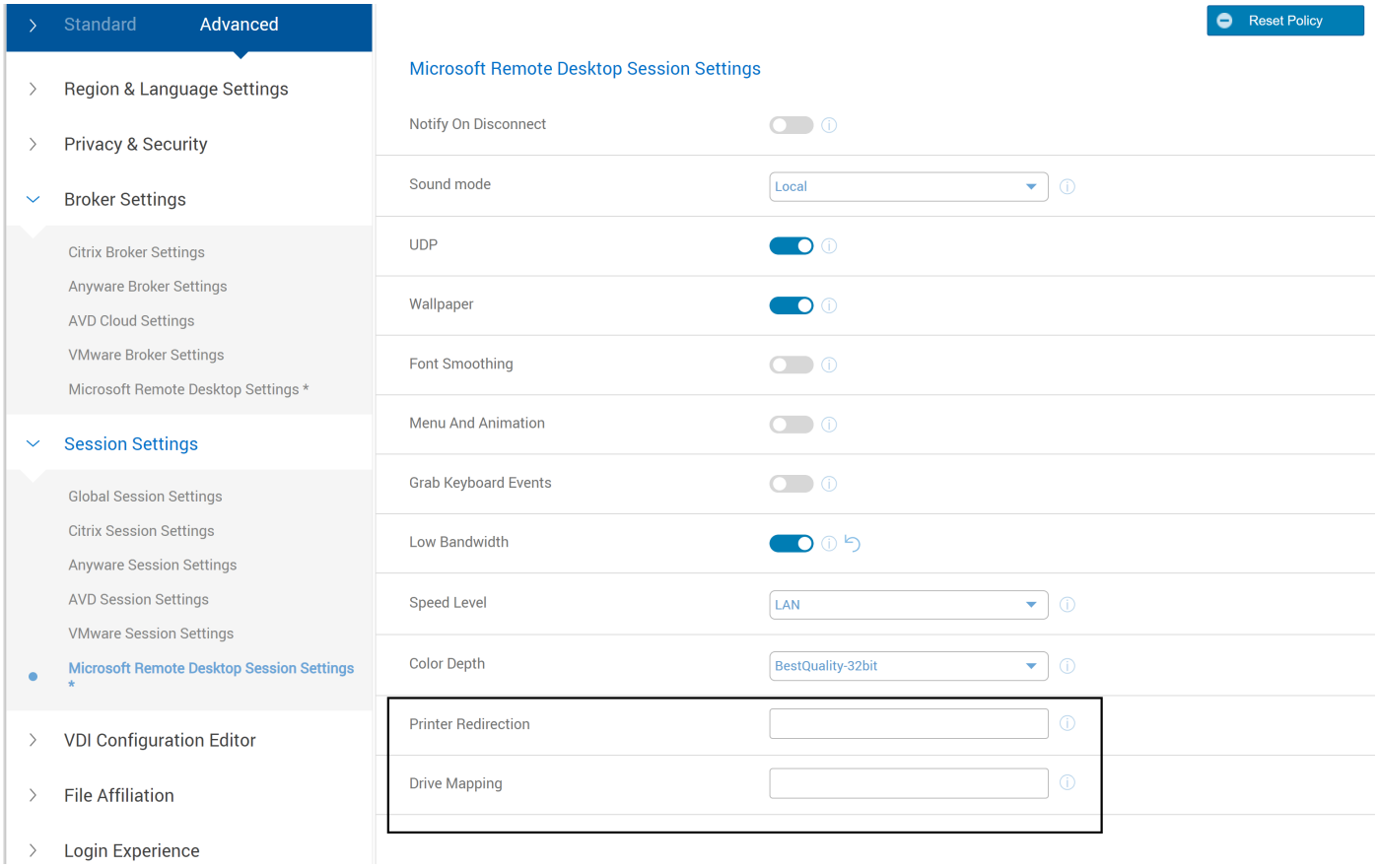


Figure 104. Microsoft Remote Desktop Session Settings

NOTE: If you configure session settings values, then it takes effect for broker connection.

Connect to an RDP session

Using Remote Desktop application, you can access and manage the data and resources of a remote device using an Internet connection. Dell Hybrid Client supports Single-Sign On (SSO) to RD web.

Prerequisites

Ensure that you have configured the RDP Broker agent settings using Wyse Management Suite. For more information about Dell Hybrid Client policy settings, see Managing the Dell Hybrid Client policy settings.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
   All RDP desktops are displayed.
3. Click a desktop icon to launch the RDP desktop.

Connect to an RDP session using TS Gateway with WebSocket

WebSocket provides a mechanism for fast, secure two-way communication between a client and a server over the web using HTTP(S). The WebSocket protocol enables two-way communication between the browser-based applications and the servers that do not rely on the multiple HTTP connections. The protocol consists of a handshake followed by basic message framing, layered over Transmission Control Protocol (TCP). The data is transferred immediately over a full-duplex single socket connection, allowing messages to be sent and received from both endpoints in real time.

Prerequisites

Enable Terminal Services Gateway (TSGW) and WebSocket protocol for the applications and desktops from the RDS server.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **RDP**, and click **Microsoft RDP Broker Session**.
6. Click **Add Row**.
7. In the **RDP Connection** section, do the following:
   a. Click the **RD Gateway** toggle key to enable RD Gateway.
   b. In the **RDP Gateway Server** field, enter the RD Gateway host address.
   c. Specify the RDP username, password, and domain.
8. Click **Save & Publish**.
9. Log in to Dell Hybrid Client.
10. Connect to an RDP desktop.
    In the TSG server, there is only one entry from the client with TCP port to send and receive information.

Configuring Imprivata

Imprivata enables secure authentication to virtual desktops and applications. Dell Hybrid Client supports Imprivata with Citrix and VMware. Fast User Switching (FUS), Azure Virtual Desktop (AVD) and WyseRDP are not supported.

Imprivata client is supported in two different modes:

- **Imprivata as a connection**—This is similar to other VDI connections. Imprivata shortcut is created in the favorite bar on Dell Hybrid Client. When the user clicks the shortcut icon, the Imprivata client is launched.
- **Imprivata as PIE mode**—By Default Imprivata is launched in PIE mode and launches Imprivata in fullscreen/kiosk mode without the need for user to log in Dell Hybrid Client.

Dell Hybrid Client supports the following types of user authentication:

- Using the username and password.
- Using the smart card authentication.

Configure the Imprivata as Connection mode

Prerequisites

- Configure the VDI settings on the Imprivata OneSign Server Web Console.
- Configure the computer policies on the Imprivata OneSign server.
- Configure the authentication type—username and password or smart card—on the Imprivata OneSign server.
- Ensure that you have installed valid certificates that are required to connect to the Imprivata session. For more information about installing certificates, see Install a certificate.
- Ensure that you have given DNS.

About this task

This section describes the procedure to configure the global connection settings for Imprivata using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device group.
   The Imprivata settings are available only for device-level group policy.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **3rd Party Authentication**.
6. From the **Authentication Type** drop-down list, select **Imprivata**.
7. Configure the following Imprivata session options as per your requirement:
   - **Bootstrap Server**—Enter the Bootstrap appliance name or the IP address.
   - **Mainloader server same as Bootstrap**—Enable this option to keep the mainloader server the same as the Bootstrap server.
     NOTE: If you disable this option, you must provide the Mainloader server appliance name or the IP address.
   - **Agent server same as Bootstrap**—Enable this option to keep the Agent server the same as the Bootstrap server.
     NOTE: If you disable this option, you must provide the Agent server appliance name or the IP address.
   - **Connection Mode**—Enable this option to use Imprivata in connection mode.

   NOTE: Imprivata does not support Ubuntu 22.04 .

   NOTE: CA Certificate Mandatory is for Imprivata.

Connect to an Imprivata PIE mode

Prerequisites

- Ensure that you have configured the Imprivata session settings using Wyse Management Suite. For more information about Dell Hybrid Client policy settings, see Managing the Dell Hybrid Client policy settings.
- Ensure that you have installed valid certificates that are required to connect to the Imprivata session. For more information about installing certificates, see Install a certificate.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device group.
   The Imprivata settings are available only for device-level group policy.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **3rd Party Authentication**.
6. From the **Authentication Type** drop-down list, select **Imprivata**.
7. Configure the Imprivata session options as per your requirement.
8. Click **Save & Publish**.
   After you restart the client, Imprivata launches in full screen.

Logging in to a VDI session using a smart card

Dell Hybrid Client supports the smart card authentication to log in to the Citrix session using a web browser. It enables you to use a smart card to authenticate the user, and launch the Citrix VDI sessions. Smart card Broker authentication is supported on Citrix, VMware, and Imprivata sessions in their respective native clients.

Prerequisites

- Ensure that you have enabled the smart card login option and defined the smart card type on Wyse Management Suite, for connecting to a Citrix session. Also, ensure that you configured the smart card authentication option on the StoreFront server. The smart card authentication is not applicable for PNAgent connections.
- Ensure that you have configured the smart card authentication type on the Horizon Connection server, for connection to a Horizon session.

- Ensure that you have configured the smart card authentication type on Imprivata OneSign server, for connection to an Imprivata session.

Steps

1. Turn on the device powered by Dell Hybrid Client.
2. Log in as AD user.
3. Connect a supported smart card reader to the device.
4. Connect your card on the smart card reader.

   NOTE: Tap the card in case of RFID card for Imprivata Connection.

5. Enter the smart card PIN to authenticate the user.
   Dell Hybrid Client authenticates the user and starts the VDI connection.

Example

Table 11. Smart Card & Readers

Smart Card & Readers
Card_IDPrimeMD840B_white_PVC
YubiKey Neo 5.0
CAC Smart Card

Install a certificate

Use Wyse Management Suite to install server and client certificates that are required in your work environment. When you import a certificate, it is also imported into the Firefox and Chrome keystores. However, Chrome requires SSL Certificates to list the site name(s) in the subject alternative name (SAN) to be trusted on server. PFX certificates are supported. The certificate is stored in the certificate store and users can visit a website securely (HTTPS) through Firefox and Chrome browsers.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device group.

   NOTE: The **Certificates** option is only applicable to Device Policy Group.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Certificate**.
6. Click the **Install Certificates** toggle key to enable the automatic installation of certificates.
7. Browse and select the certificates that you want to upload.
   All the uploaded certificates are listed in the **Select Certificates to Upload** drop-down list.
8. From the **Select Certificates to Upload** drop-down list, select one or more certificates to install based on your requirement.
9. Click **Save & Publish**.
   Certificates are automatically installed on the client.

View Installed certificates

Steps

1. Go to the **Devices** page, and locate your device that is powered by Dell Hybrid Client.
2. Click Click the device name.
   The **Device Details** page is displayed.

3. Go to **System Info** > **Operating System Details** > **Installed Certificates** to view the installed certificates.

Unified Communications optimization

Unified Communications and Collaboration solution allows real-time video conferencing, instant messaging, and team collaboration that enables you to work together more effectively.

Dell Hybrid Client supports the following Unified Communications optimization in a VDI environment:

- Dell Hybrid Client supports UC optimization for WebEx (Teams and Meeting) and Jabber.
- UC Optimization packages are released as optional addons with Dell Hybrid Client.
- Provides stable and full-featured calling and meeting experience for VDI users.
- UC Optimization is supported on VMware and Citrix VDIs.
- Teams

  NOTE: You must install the Multimedia Extension Fix add-on for VDI to use the Teams application in a VDI session. For information on how to install the add-on, see Multimedia add-on package for VDI.
- Zoom

You must install the device plugins for each UC along with dependencies.

Zoom plug-in for VDI

The Zoom application for VDI is a Unified Communications solution that is offered by Zoom for virtual deployments. It supports enterprise video conferencing and screen sharing on virtual desktops. Zoom offloads media processing from the virtual desktop server to the thin client. All audio and video signals are routed directly between the endpoints. You can use the Zoom application to make and receive calls in the VDI session.

Prerequisites

Install the **Multimedia Extension Fix Add-on for VDI** to use the Zoom application in a VDI session. For information about how to download and install the multimedia add-on package, see Multimedia add-on package for VDI.

NOTE: **VDI-jabberoffload**, **VDI-webexoffload**,**Zoom plugin for VMware**, and **Zoom plugin for Citrix** are delivered as optional add-ons.

About this task

To download and install the optional Zoom plug-ins for VDI, do the following:

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device or type Dell Hybrid Client.
3. Click the product from search results to open the product support page.
4. On the product support page, click **Drivers & downloads**.
5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the **Ubuntu 20.04 or 22.04** operating system. For information about the version of the Ubuntu operating system that is supported in each Dell Hybrid Client release, see Supported operating system.
6. From the list, locate the Zoom Plugin addon for Citrix or Zoom Plugin for VMware add-on entry and click the download icon.
7. After the add-on is downloaded successfully, use the application policy on Wyse Management Suite to deploy the add-on to Dell Hybrid Client. Ensure that you upload the downloaded add-on to the local repository on Wyse Management Suite. For more information about how to deploy an application policy, see the *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.

   For more information about using the Zoom application in VDI, see the *Quick Start Guides* at support.zoom.us.

Multimedia add-on package for VDI

The **Dell Hybrid Client Multimedia Extension Fix Add-on for VDI** package must be installed to enable HTML5 multimedia redirection in a VDI session. Installing this add-on enables you to play YouTube on Internet Explorer inside a remote desktop session.

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device or type Dell Hybrid Client.
3. Click the product from search results to open the product support page.
4. On the product support page, click **Drivers & downloads**.
5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the **Ubuntu 20.04 or 22.04** operating system. For information about the version of the Ubuntu 20.04 or 22.04 operating system that is supported in each Dell Hybrid Client release, see Supported operating system.
6. From the list, locate the **multimedia-extension-VDI-addon** entry and click the download icon.
7. After the add-on is downloaded successfully, use the application policy on Wyse Management Suite to deploy the add-on to Dell Hybrid Client. Ensure that you upload the downloaded add-on to the local repository on Wyse Management Suite. For more information about how to deploy an application policy, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Bloomberg keyboard support for VDI

The Bloomberg Keyboard is a standard personal computer keyboard that has been designed for use with the Bloomberg Professional® service. Bloomberg keyboard supports Citrix, VMware, and Anyware VDIs with Dell Hybrid Client.

Bundle and Addon Naming

Dell Hybrid Client supports **Ubuntu 20.04** and **Ubuntu 22.04**. For Bundle and add-on, a common nomenclature is introduced for helping Wyse Management Suite admin identify the add-on for corresponding operating system.

For 20.04, Base Bundle name is **DellHybridClient_2310.xxx_U20.04.tar.gz**

Where **2310** represents the release version and **U20.04** represents the Operating System Ubuntu 20.04.

For 22.04, Base Bundle name is **DellHybridClient_2310.xxx_U22.04.tar.gz**

Where **2310** represents the release version and **U22.04** represents the Operating System Ubuntu 22.04.

Similarly, add-on names are generated as below:

DHC<dhc_v>-<parent_name/NULL>-<child_name>_<major_v/00>-<minor_v>_<ubuntu_v/all>

dhc_v is DHC release version, here its 2310

Parent_name is related module of Add-On.

Example: LP = Language Pack, VDI = Virtual Desktop Infrastructure

Child_name is add-on name

Major and minor version is version of add-on

Ubuntu_v is Ubuntu version for which this add-on is released(all indicated supported for 20.04 and 22.04)

File Type Association

A File Type Association (FTA) is a correlation between a file type and an application. File types are determined by a file name extension. For example, `.docx`, `.pptx`, `.txt`, `.png`, `.xlsx`, and so on. Dell Hybrid Client supports the file type association for Citrix, VMware, and RDP VDI applications. To open local files or network shared files using VDI applications, you must configure the FTA settings and set the File Affiliation for VDI mode using Wyse Management Suite.

NOTE: File Type Association is not supported for Azure Virtual Desktop.

Configure the File Type Association for Citrix

Dell Hybrid Client supports the file type association for Citrix VDI applications. Extensions and application names that are configured from the Citrix server are fetched automatically during login. You must configure the File Affiliation settings for VDI mode. When you launch a file from File Explorer, the VDI application that supports the file type opens the file automatically.

Prerequisites

Ensure that the Citrix server has published applications for which you can set file type association.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.

   NOTE: In Wyse Management Suite version 4.0 or later, the FTA options under the Hybrid Client policy settings are rearranged for better grouping and visibility. See, Managing the Dell Hybrid Client policy settings.

5. Expand **File Affiliation** and click **Citrix File Type Association**.
6. In the **Citrix File Type Association Configuration** section, click **Add row**.

   NOTE: File Type Association settings are independent of the Citrix Broker settings. Both the FTA and broker settings must be configured separately based on your requirement. If FTA is configured, you can access files from Dell File Explorer with configured Citrix published applications.

7. In the **Host** field, enter the StoreFront URL.
   Examples—`https://citrix.customer.local`, `https://citrix.customer.local/citrix/store`, or `https://citrix.customer.local/citrix/store/discovery`.
8. In the **Store Name** field, specify the name of the store through which the StoreFront server connection is established.
9. Click **Save and Publish**.

Next steps

Configure the File Affiliation for VDI mode. For more information, see File Affiliation.

Configure the File Type Association for VMware

Dell Hybrid Client supports the file type association for VMware VDI applications. As an administrator, you must provide file extensions and respective application names for VMware FTA settings using Wyse Management Suite. You must also configure the File Affiliation settings for VDI mode. When you launch a file from Dell File Explorer, the VDI application that supports the file type opens the file automatically.

Prerequisites

Ensure that the VMware server has published applications for which you can set file type association.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.

NOTE: In Wyse Management Suite 4.0 and later versions, the FTA options under the Dell Hybrid Client policy settings are rearranged for better grouping and visibility. See, Managing the Dell Hybrid Client policy settings.

5. Expand **File Affiliation** and click **VMware File Type Association**.
6. In the **VMware File Type Association Configuration** section, click **Add row**.

   NOTE: File Type Association settings are independent of the VMware Broker settings. Both the FTA and broker settings must be configured separately based on your requirement. If FTA is configured, you can access files from Dell File Explorer with configured VMware published applications.

7. In the **Host** field, enter the server name or the IP address.
8. In the **Username** field, enter the name of the user to connect to the application server.
9. In the **Password** field, enter the password that is required to log in to the application server.
10. In the **Domain** field, enter the domain name in a Windows network where the VMware server is located.
11. From the **Protocol** drop-down list, select the preferred connection protocol—**PCoIP** or **Blast**.
12. In the **File Type Association configuration** field, enter the application name with extension.

    You can add single or multiple entries. Use the format `extension1: application name, extension2: application name` to specify your application names. For example, `.docx:microsoft word 2010, .pptx:microsoft powerpoint 2010`.
13. Click **Save and Publish**.

Next steps

Configure the File Affiliation for VDI mode. For more information, see File Affiliation.

Configure the File Type Association for RDP

Dell Hybrid Client supports the file type association for RDP applications. Extensions and application names that are configured from the RDP Broker agent server are fetched automatically during login. You must configure the File Affiliation settings for VDI mode. When you launch a file from File Explorer, the VDI application that supports the file type opens the file automatically.

Prerequisites

Ensure that the Remote Desktop Connection (RDP) server has published applications for which you can set file type association.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.

   NOTE: In Wyse Management Suite 4.0 and later versions, the FTA options under the Dell Hybrid Client policy settings are rearranged for better grouping and visibility. See, Managing the Dell Hybrid Client policy settings.

5. Expand **File Affiliation** and click **RDP File Type Association**.
6. In the **RDP File Type Association Configuration** section, click **Add row**.

   NOTE: File Type Association settings are independent of the RDP Broker settings. Both the FTA and broker settings must be configured separately based on your requirement. If FTA is configured, you can access files from Dell File Explorer with configured RDP published Applications.

7. In the **Server** field, enter the server name or the IP address.
8. In the **Username** field, enter the name of the user to connect to the application server.

   NOTE: Single Sign-On works by default. Username, password, and domain must be entered only when you are accessing RDP from Internet where SSO is not supported.

9. In the **Password** field, enter the password that is required to log in to the application server.
10. In the **Domain** field, enter the domain name.
11. To enable RD Gateway, click the **RD Gateway** toggle key. This option enables authorized user to connect to resources in internal network.
    a. In the **RD Username** field, enter the name of the RD user to connect to the RD Gateway server.
    b. In the **RD Password** field, enter the password that is required to log in to the RD Gateway server.
    c. In the **RD Domain** field, enter the RD domain name.
12. Click **Save and Publish**.

Next steps

Configure the File Affiliation for VDI mode. For more information, see File Affiliation.

7

Managing user accounts

Dell Hybrid Client offers three types of user accounts, **Active Directory (AD) user**, **Local user**, and **Guest user**.

- **Guest user**—Enables users to access Dell Hybrid Client. By default, the guest account is enabled. If you want to disable, configure, or add a password for the guest account, you must use Wyse Management Suite. For more information about how to configure a guest account, see Configure a guest user account properties.

  NOTE: With **Guest user** login, user data and local device settings are not preserved after a restart or if you log off and log back in.

  NOTE: Only during First boot Device, the program will auto log in to Guest user if registration skipped in setup wizard.
- **Local user**—Enables local users to access Dell Hybrid Client without domain registration. By default, the local user account is disabled. If you want to enable, configure, or add a password for the local user account, you must use Wyse Management Suite. For more information about how to configure a local user account, see Configure a local user account properties.
- **AD user**—Enables users to connect to the work domain using their Active Directory credentials. For information about joining AD and authentication, see Joining Active Directory.

NOTE: By default, the user list of last logged-in users is not displayed on the login screen. For information about how to view the user list on the login screen, see Show user list on the Dell Hybrid Client login screen.

NOTE: When the auto login feature is enabled, the local user takes priority over the guest user if local users are configured with auto login.

NOTE: The configuration applied during each login has been optimized in DHC 2.5 release.

Configure the guest user account settings

The Guest account is a low-privilege account that is available for users. You can enable or disable the guest user account using Wyse Management Suite. If you have logged in as a guest user data, local configurations are not preserved across logins. For example, when a guest user configures a wallpaper setting locally, the setting is restored to the default wallpaper when the user logs out and logs back in. However, when the same wallpaper is configured from Wyse Management Suite (Device User Policies), the setting changes are applied to the subsequent guest user logins.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Guest User Account Properties**.
6. Click the **Guest user account** toggle key to enable or disable the guest user account. By default, the guest user account is enabled.
7. Click the **Password prompt guest account** toggle key to ON state to enable the password prompt for the guest account.
8. In the **Set password for Guest user** field, enter the password for the guest user account.

   The minimum password length is nine characters and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. Do not use your username as your password.

   NOTE: When password fails to set, the password does not get updated for the guest user. You can view the failure error message on the **Events** tab in Wyse Management Suite.
9. Click the **Auto SignOn** toggle key to ON state to enable the guest user to automatically log in to Dell Hybrid Client.

10. Click the **Remove Device Lock and Password prompt on wakeup** toggle key to ON state to enable the option. After the device or display resumes from sleep mode, the lock screen is no longer displayed and the device does not prompt for a password.
11. Click **Save and Publish**.

    After receiving the configuration, the client displays a restart notification if the auto signon is enabled, remove device lock is enabled, or the guest user password is configured. Close the notification and log off manually to apply the configuration.

Configure the local user account settings

The local user account is created by Administrators to enable users to log in to Dell Hybrid Client without domain registration. You can enable or disable the local user account using Wyse Management Suite. If you have logged in as a local user, device configurations are preserved across logins.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Local User Account Properties**.
6. Click the **Local user account** toggle key to enable or disable the local user account. By default, the local user account is disabled.
7. In the **Set username for Local user** field, enter the username for the local user account.
8. In the **Set password for Local user** field, enter the password for the local user account.

   The minimum password length is nine characters and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. You must avoid the $% combination. Do not use your username as your password. Numeric numbers cannot be in sequence.
9. Click the **Auto SignOn** toggle key to ON state to enable the local user to automatically log in to Dell Hybrid Client.
10. Click the **Admin Rights** toggle key to grant administrative rights to the local user. If enabled, the local user can run the root commands using sudo.
11. Click the **Remove Device Lock and Password prompt on wakeup** toggle key to ON state to enable the option. After the device or display resumes from sleep mode, the lock screen is no longer displayed and the device does not prompt for a password.
12. Click **Save and Publish**.

> **NOTE:** When multiple local user accounts are added and the auto sign-on feature is enabled for multiple users, only the first user is selected will auto sign-on.

> **NOTE:** When the device fails to create a user, you can view the **Events** tab in Wyse Management Suite to analyze the failure.

> **NOTE:** Dell Hybrid Client supports up to 8 local users.

Next steps

Log in to Dell Hybrid Client as a local user. See, Log in as a local user.

You can change the user password either using Wyse Management Suite or the Device Settings UI. See, Change local user credentials using Wyse Management Suite and Change the account password locally.

Configure multiple local user accounts

Dell Hybrid Client supports up to eight local user accounts on a single device. Each local user home directory is protected with ZFS. One local user cannot view the data of another local user. The data of each local user is preserved across logins.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Local User Account Properties**.
6. Click the **Local user account** toggle key to enable or disable the local user account. By default, the local user account is disabled.
7. In the **Local User** section, click **Add Row**, and configure the following options:
   a. In the **Set username for Local user** field, enter the username for the local user account.
   b. In the **Set password for Local user** field, enter the password for the local user account.

      The minimum password length is nine characters and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. You must avoid the $% combination. Do not use your username as your password.
   c. Click the **Auto SignOn** toggle key to ON state to enable the local user to automatically log in to Dell Hybrid Client.
   d. Click the **Admin Rights** toggle key to grant administrative rights to the local user. If enabled, the local user can run the root commands using sudo.
   e. Click the **Remove Device Lock and Password prompt on wakeup** toggle key to ON state to enable the option. After the device or display resumes from sleep mode, the lock screen is no longer displayed and the device does not prompt for a password.
8. To add multiple local users, repeat step 7.
9. Click **Save and Publish**.

   A restart notification is displayed on the device if you modify the auto signon, admin rights, and remove lock settings.

   NOTE: When multiple local user accounts are added and the auto sign-on feature is enabled for multiple users, only the first user is selected for auto sign-on.

   NOTE: When the device fails to create a user, you can view the **Events** tab in Wyse Management Suite to analyze the failure.

Next steps

Log in to Dell Hybrid Client as a local user. See, Log in as a local user.

Change local user credentials from Wyse Management Suite

Prerequisites

Ensure that the local user account is enabled on your device.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Devices** page.
3. Locate your device and click the device name.
   The **Device Details** page is displayed.
4. From the More Actions drop-down list, click **Change User Credentials**.
5. Enter the name of the local user.
6. Enter the new password.

The minimum password length is nine characters, and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. Do not use your username as your password.

7. Click **Send Command**.

Log in as a local user

As a **local user**, you can log in to Dell Hybrid Client without domain registration. By default, the local user account is disabled on your Dell Hybrid Client. You can enable the local user account using Wyse Management Suite. If you have logged in as a local user, local configurations are preserved across logins.

Prerequisites

Ensure that the local account is not disabled by the Wyse Management Suite administrator. For more information about configuring the local account properties, see Configure a local user account properties.

Steps

1. Start the device powered by Dell Hybrid Client.
2. On the login screen, enter the username of the local user.
3. Press **Enter**.
4. Enter the password.
5. Enter **Key** to log in.
   Dell Hybrid Client boots to the desktop screen.
   NOTE: If the previously logged-in user list option is enabled on Wyse Management Suite, Dell Hybrid Client shows user accounts on the login screen. See, Show user list on the Dell Hybrid Client login screen.

Joining Active Directory

Dell Hybrid Client supports user authentication with Active Directory. Active Directory allows an administrator to enable or disable the user authentication to specific domains. Dell Hybrid Client supports login with Active Directory user. You can also use a smart card to log in as a domain user.

Prerequisites

For Ubuntu 20.04 smart card login, smartcardloginenabler package from Wyse Management Suite must be installed.

- Ensure that the DNS server is configured correctly.
- Ensure that the date and time of your Dell Hybrid Client are synchronized with the date and time of the domain server. For more information about how to configure date and time using Wyse Management Suite, see, Configure the date and time.
  NOTE: By default **Auto time zone** is enabled and works if Internet is enabled.
- Ensure that the Dell Hybrid Client is registered to Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
   NOTE: The Domain join SignOn option is available on the device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **Domain join**.
6. Click the **Join Domain** toggle key to enable domain joining.
7. In the **Username** field, enter the name of the user who has the relevant permission to join a device to Active Directory.
8. In the **Password** field, enter the password of the user.

NOTE: Both **Organization Unit** and **Workgroup** fields are optional and customers can configure them according to their domain settings.

- In the **Organizational Unit** field, enter the name of your enterprise organizational unit. For multiple Organizational Units (OUs), you must mention the sublevels that are separated by a forward slash **/**. For example, if the full distinguished name is **OU=test,OU=blrtest,OU=blr,DC=blrbrmcloud,DC=com**, the OU name must be specified as **/blr/blrtest/test**.
- In the **Workgroup** field, enter the name of the workgroup specific to your organization.

9. In the **Domain** field, enter the complete domain name. For example, test.local, test.com, and child.test.com.
10. Click **Save and Publish**.

    If the user has logged in to the device, the **Restart Now** option is displayed. If the device is not in the logged-in state (locked state or the login screen), the device restarts automatically.

Next steps

Log in to the Dell Hybrid Client as a domain user. See, Log in as a domain user.

Log in as a domain user using Active Directory credentials

As a **domain user**, you can securely connect to the work domain using the Active Directory credentials.

Prerequisites

Ensure that the **Domain Join** option is configured on Wyse Management Suite. For information about joining AD and authentication, see Joining Active Directory.

Steps

1. Start the device powered by Dell Hybrid Client.
2. On the login screen, enter the domain credentials. For example, `domain\username` or `username@domain.com`.
3. Press **Enter**.
4. Enter the domain password.
5. Press the **Enter** key to log in.
   Dell Hybrid Client boots to the desktop screen.

   NOTE: If the previously logged-in user list option is enabled on Wyse Management Suite, Dell Hybrid Client shows user accounts on the login screen. See, Show user list on the Dell Hybrid Client login screen.

Direct Domain Login

Direct Domain Login allows the user to log into the Dell Hybrid Client using the Active Directory (AD) credential without making the device a member of AD. Direct login will also support both SSO for clients and application.

Configuring the direct domain login

Prerequisites

Ensure that the DNS server is configured correctly on the DHC or DHCP Server.

Ensure that the date and time of your thin client are synchronized with the date and time of the domain server.

About this task

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **Login Settings**.
6. Select the **Direct Domain Login** from the drop down.
7. Enter admin user credentials in the **Username** and **Password** field.
8. **Click Save & Publish**.
   A restart notification will be notified in the device.

   NOTE: After restarting the device, the user can log in to DHC using domain credential.

Banner message on device login screen

Enable the banner message on device login screen to add a banner message. User can add the banner message in the banner message field which will get displayed on the login screen.

Configuring banner message

About this task

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies**> **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **Banner Message**.
6. Click the **Banner Message** toggle key to enable the option and type **Message Value** up to 500 characters .
7. Click **Save & Publish**.
   A Logout notification will be notified in the device.

Log in as a domain user using a smart card

Dell Hybrid Client enables a domain user to log in to the device using a smart card. Dell Hybrid Client supports **Yubikey** and **Gemalto** smart cards. Dell Hybrid Client supports certificate-based smart card authentication to log in to the device. Both .pfx and .cer certificates are supported.

Prerequisites

- Ensure that the smart card user certificates are installed on Dell Hybrid Client. **Gemalto** and **Yubikey** supports PFX and CER certificates.
- If you are using Gemalto smart cards, ensure that you install the Gemalto driver package on Dell Hybrid Client from the Gemalto website.
- Ensure that you have configured the PIN on your smart card. For information about how to configure the PIN for your smart card, see the smart card product documentation on the respective vendor websites.

NOTE:

Smart Card Device login is now supported for Ubuntu 22.04.

For Ubuntu 20.04, you must install Smart Card enabler Add-on.

Steps

1. Start the device.

2. Connect a supported smart card reader to the device.
3. Connect your card on the smart card reader.
4. On the login screen, enter the username.
5. Enter the smart card PIN.
   Dell Hybrid Client authenticates the user and boots to the desktop screen.

Show user list on the Dell Hybrid Client login screen

You can allow Dell Hybrid Client to display the account name of the previously logged-in users on the login screen. By default, the user list is not displayed on the login screen. This option is applicable only to a device policy group.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **Previously Logged-in User List**.
6. Click the **Previously Logged-in User List** toggle key to enable the option.
7. Click **Save & Publish**.
8. Turn on the device.
   Dell Hybrid Client displays the previously logged-in user list on the login screen.

System password

System is the default boot loader for Dell Hybrid Client. Dell Hybrid Client enables you to set a password for the System boot menu to restrict User access to the System boot menu. System password is generated when you start a device that is powered by Dell Hybrid Client for the first time. As an administrator, you must change the default System password. For information about how to set the System password, see Enable System menu password protection.

NOTE: Changing the System password is mandatory and you cannot leave the password field blank. The same System password is applied for System (Admin) password as well.

Change Admin (System) Password Protection

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **System Password**.
6. In the **System Password** field, enter the password. The minimum password length is nine characters and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character.

   NOTE: As an administrator, you must change the System password during the initial setup for improved security.

7. Click **Save & Publish**.

View the System password

Prerequisites

Ensure that your device is registered to Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Devices** page.
3. Locate your Dell Hybrid Client-based device and click the device name.
4. From the **More Actions** drop-down list, click **System Password**.
   The **View System Password** dialog box is displayed.
5. Select the **Show Password** check box to view the password.
6. Click **OK** to close the dialog box.

Device compliant

System Password Compliant and **BIOS Password Compliant**.

When the System and BIOS passwords are changed, the device compliance status on the **Devices** page on Wyse Management Suite displays green.

When you hover over the green mark, the status is displayed as **Compliant**. If the default System or BIOS password is not changed, the device compliance status shows red. When you hover over the red mark, the status is displayed as **System/BIOS password not changed**. The administrator must change both the System and BIOS passwords to change the device status to **Compliant**, and to display the device-compliant status as green.

If the same device is unregistered and registered again, the changed System password is resynchronized during check-in to Wyse Management Suite. The device compliance status shows green, and the administrator does not have to change the System password again.

You can use the Wyse Management Suite console to view the System password. For more information about how to view the System password, see View the System password.

If the device registration fails, the administrator can still generate a System password using the serial number and Universally Unique Identifier (UUID) of that particular device. For more information about how to generate the System password, see Generate the default System password.

Generate the default System password

If the device registration to the Wyse Management Suite server fails, the administrator can generate a System password using the **Portal Administration** tab on the Wyse Management Suite console.

Prerequisites

Ensure that you have collected the Serial Number and the device Universally Unique Identifier (UUID) details from the **System Information** dialog box on your local device.

About this task

NOTE: Some devices will come to compliant state after changing system password.

Steps

1. Log in Wyse Management Suite.
2. Go to the **Portal Administration** page.
3. In the **Console Settings** section, click **Dell Hybrid Client**.
4. Enter the serial number of the device.
5. Enter the UUID of the device.
6. From the **Hybrid Client Version** drop-down list, select **Hybrid Client 1.8+**.

7. Click **Generate Password**.
   The **View System Password** dialog box is displayed.
8. Select the **Show Password** check box to view the System Password.
9. Click **OK** to close the dialog box.

User Personalization

Dell Hybrid Client supports user personalized roaming for certain configurations that are managed using the **Device Settings** window on the local device.

User Personalization feature is only applicable to **Domain Users**.

A user can configure user-specific settings on one device, and the same settings are enabled on another device when the user is logging in through the **Domain User**.

By default, the user personalization roaming option is disabled.

Configure the User Personalization Roaming Settings

This section provides the procedure on how to configure the user personalization roaming settings.

Prerequisites

On the Dell Hybrid Client policy settings, go to **Advanced tab** > **WMS Settings** > **WMS Client Settings** and ensure that the **Enable Session Reporting** option is enabled.

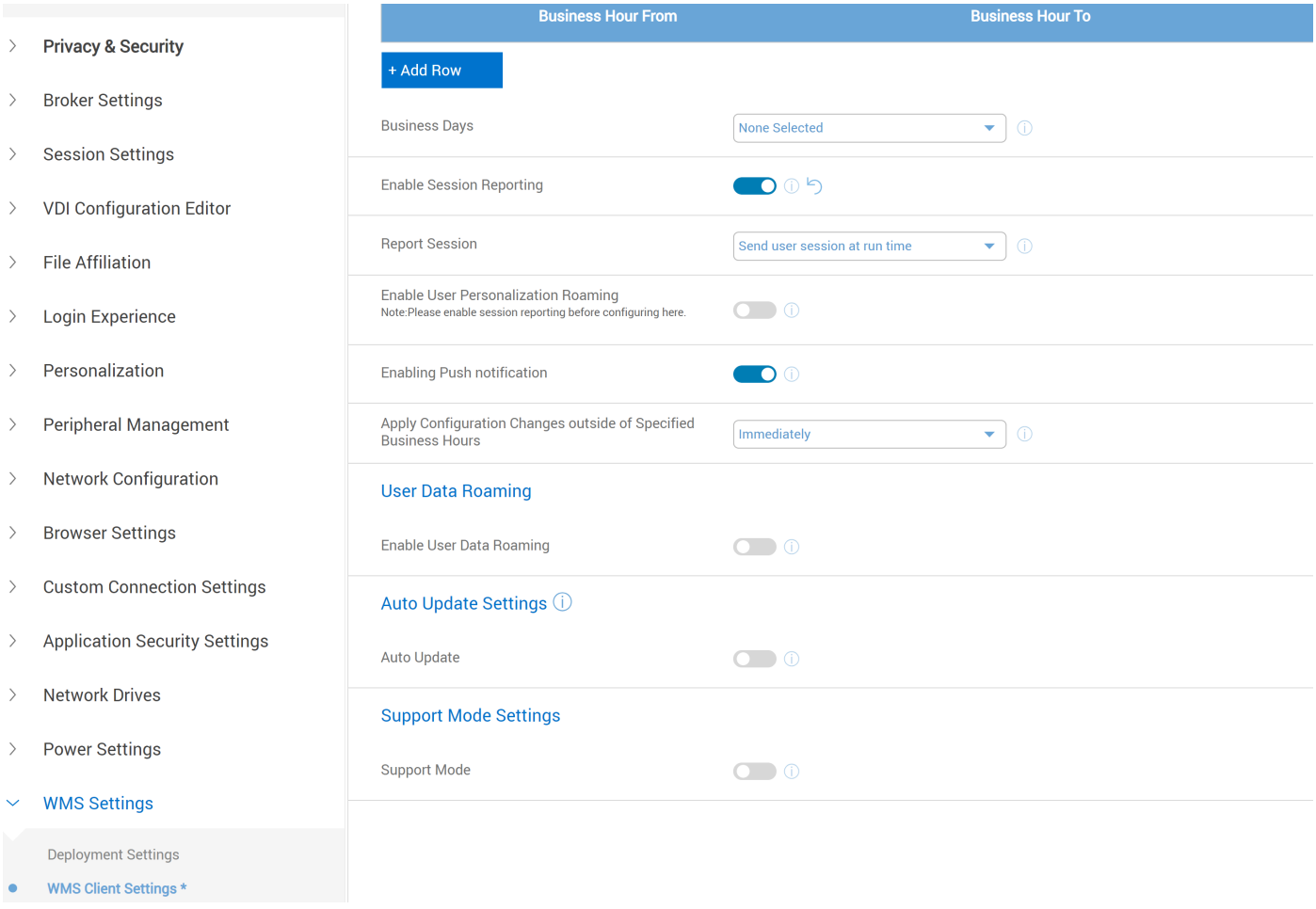


Figure 105. WMS Client Settings

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, select your preferred **Device Policy** group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**. The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **WMS Settings** and click **WMS Client Settings**.
6. Click the **Enable User Personalization Roaming** toggle switch to enable the option.

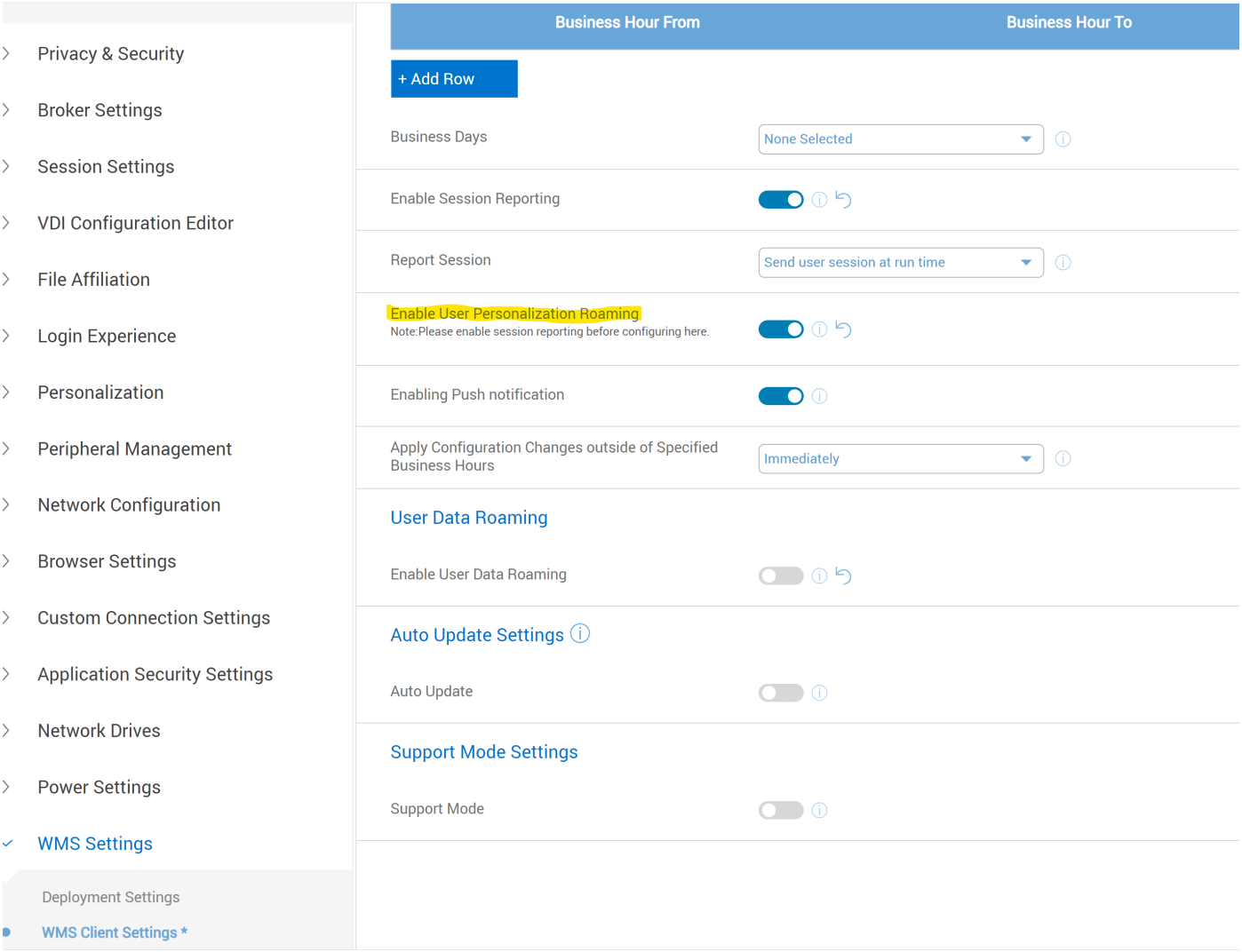


Figure 106. WMS Client Settings

7. Click **Save & Publish**.

   The following options are supported as part of user personalization on Dell Hybrid Client:

   - **Peripherals Management:**
     - Mouse
     - Speed
     - Swap
     - Scroll Wheel
     - Pointer Size
   - **Keyboard:**
     - Keyboard Repeat Rate
     - Keyboard Repeat Delay
     - Keyboard Layout
     - Num Lock

- **Display Personalization:**
  - Desktop Color
  - Wallpaper Mode
  - Scale
  - Brightness
  - Dock Icon Size
  - Dock position
  - Auto hide dock
- **Region Settings:**
  - Time Zone
  - Time Format
- **Power Settings:**
  - Power saving:
    - Wi-Fi
  - Suspend and Power:
    - Blank screen
    - Auto suspend
    - Power action button
  - Power Profile
  - Troubleshooting General - Print Screen

    These options can be configured using Device settings on the local client and using Wyse Management Suite as well.

Example

For Example, In **Device Settings** a **Mouse** pointer size is configured as **Big** as shown in the below image.

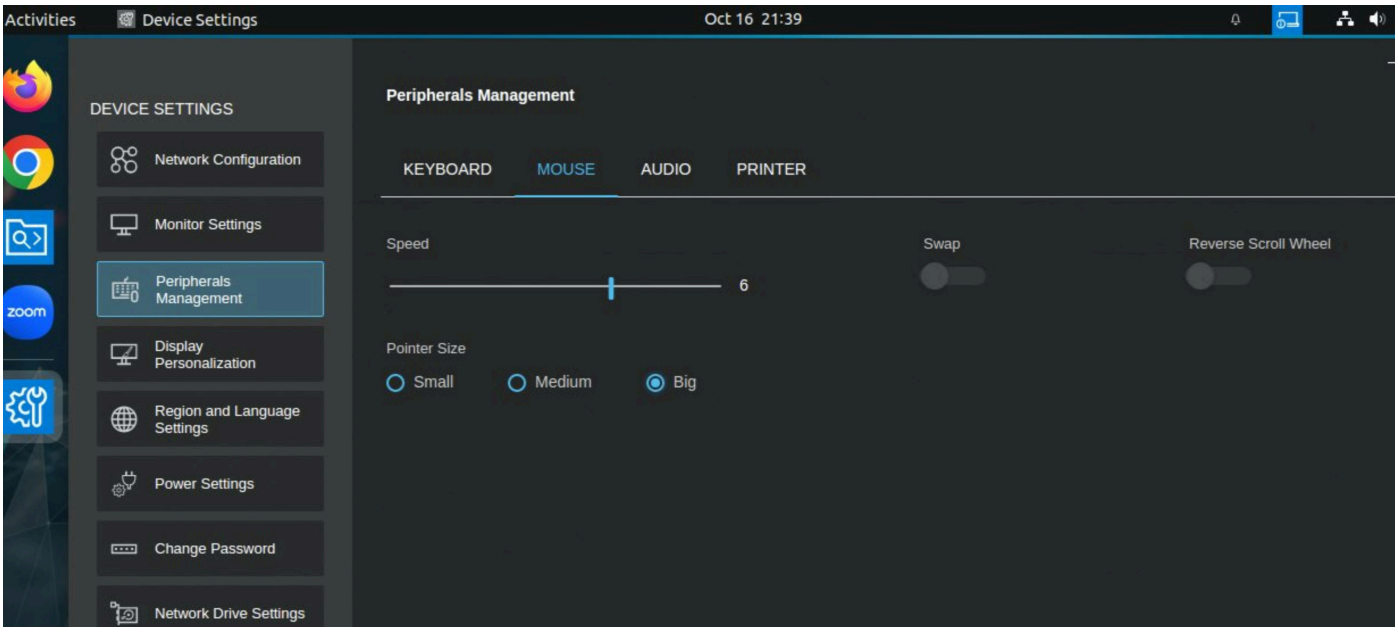


Figure 107. Peripheral Management

Logout Device A, once **User Personalization Roaming** is enabled from Wyse Management Suite.

Log in to Device B with the same user. Mouse pointer size should be **Big** in Device B.

8

Configure VPN settings

Configure VPN Settings

Dell Hybrid Client enables you to connect to your corporate network from home or external networks using a virtual private network. Dell Hybrid Client uses the OpenConnect client that is based on the SSL protocol to a VPN Connection.

You can configure VPN details using Dell Hybrid Client Devices Settings or Wyse Management Suite.

Configure VPN from Wyse Management Suite

You can configure a VPN using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.

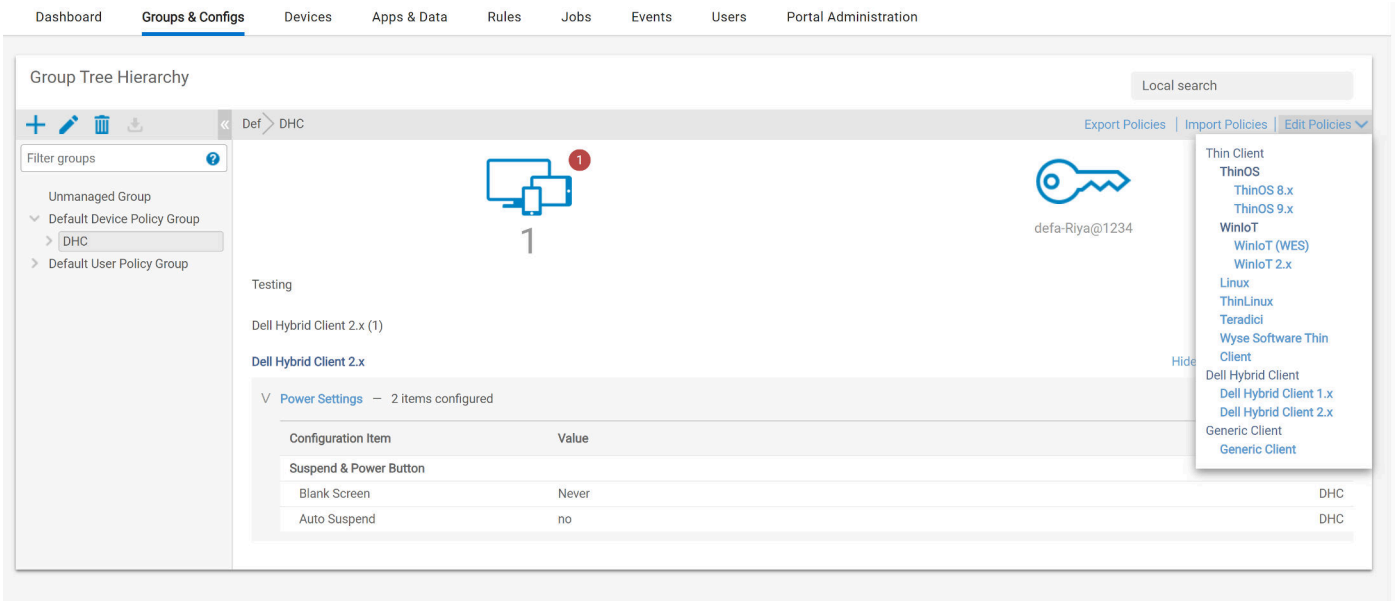


Figure 108. Configuration Control | Dell Hybrid Client 2.x

4. Click the **Advanced** tab.
5. Expand **Network Configuration** and click **VPN**.

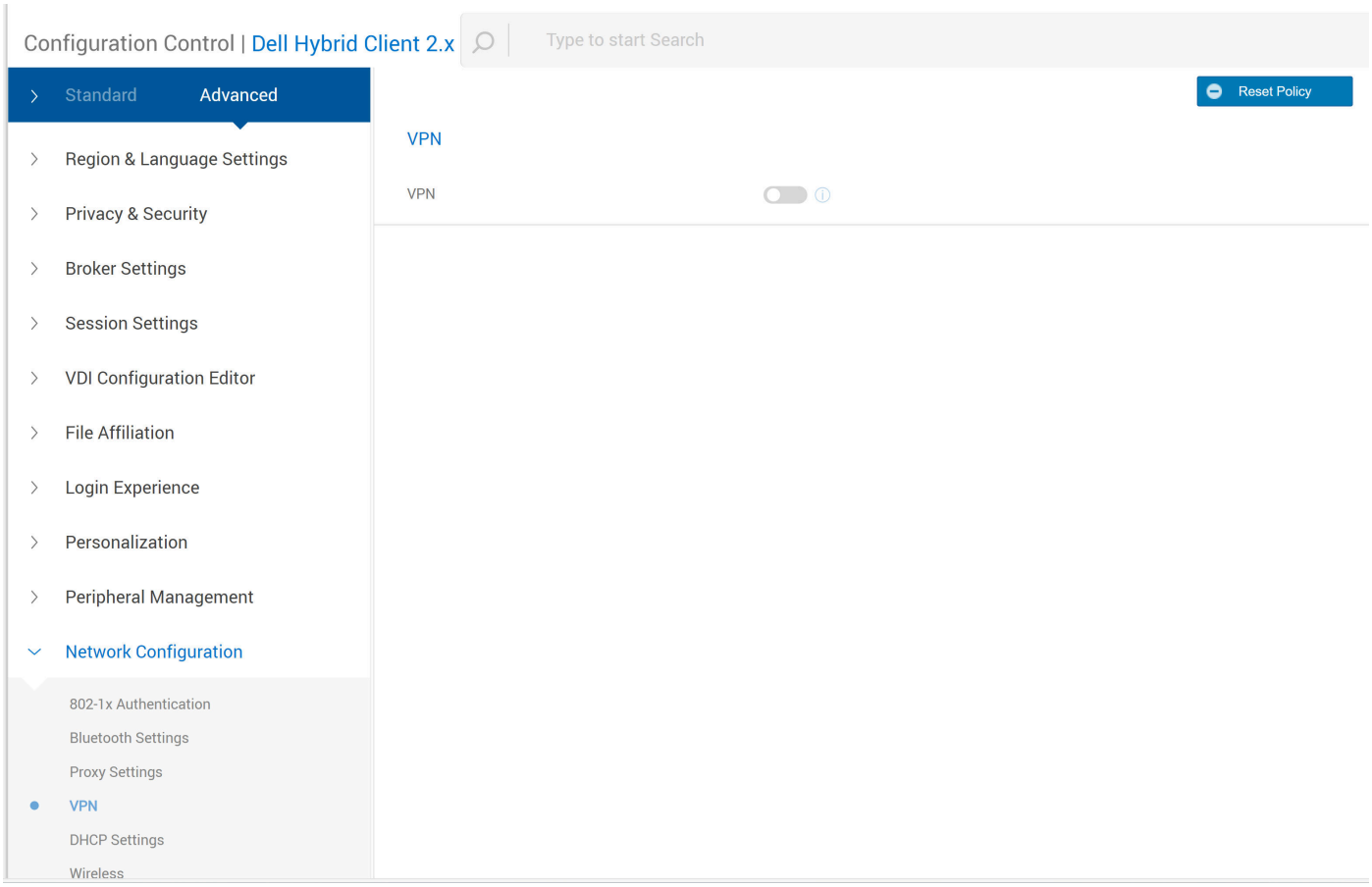


Figure 109. VPN

6. Click the **VPN** toggle switch to enable the VPN connection.
7. In the **VPN Server URL** field, enter the IP address or FQDN of the VPN server.
8. From the **Protocol** drop-down list, select either **Cisco AnyConnect** or **GlobalProtect** based on your preference.

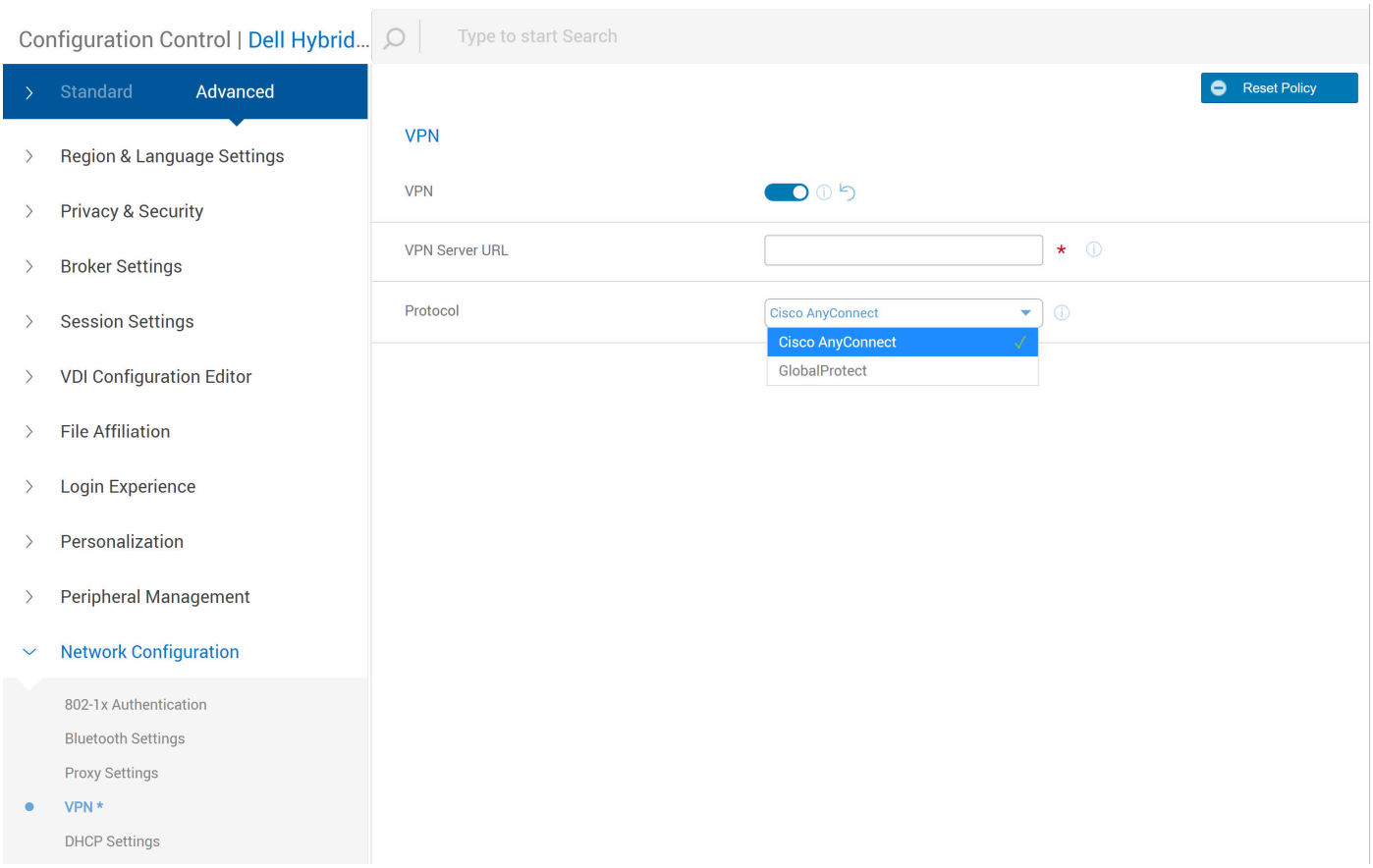


Figure 110. Protocol

9. Click **Save & Publish**.

Configure VPN from Device Settings

You can configure the VPN using Device Settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** option.
4. Click **Network Configuration**.

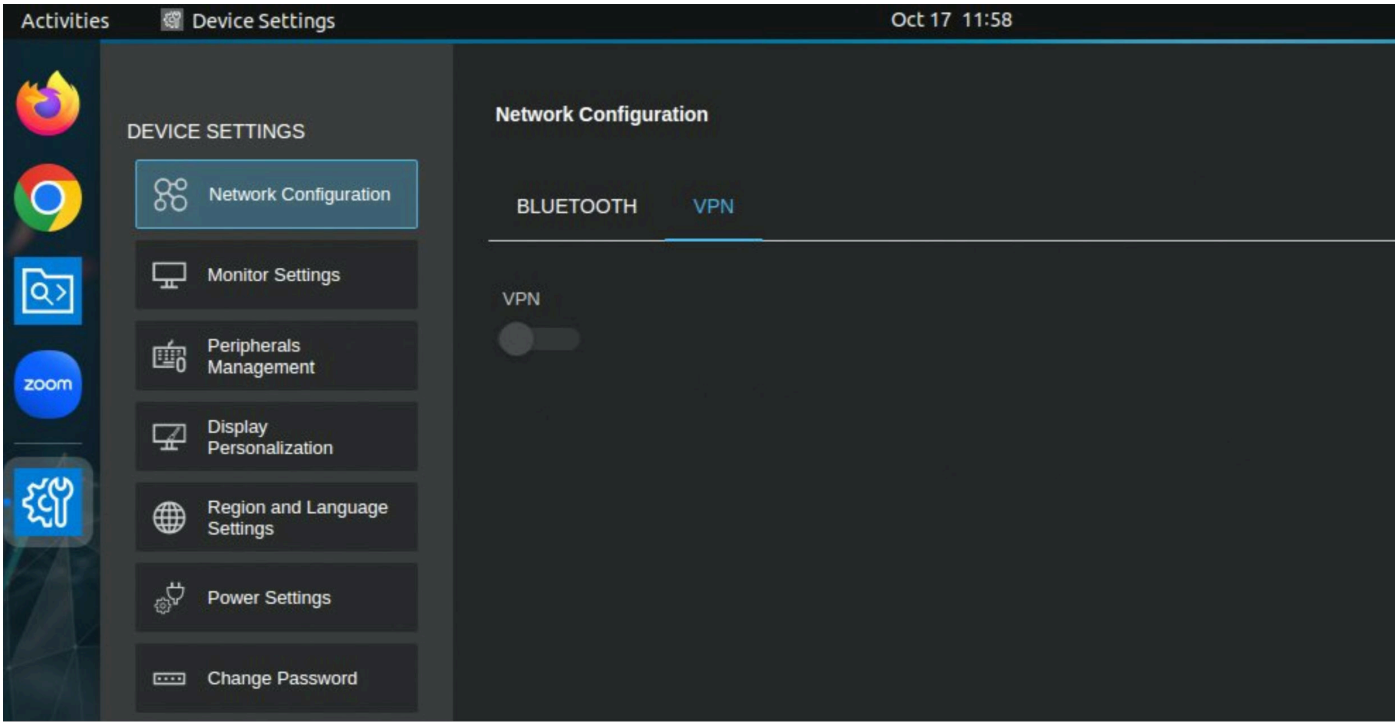


Figure 111. Network Configuration

5. Configure the VPN with the following network settings based on your requirement:

   VPN- Use this option to configure the VPN settings. This option is available from Dell Hybrid Client 1.5 onwards. Click the VPN tab, and do the following:

   a. Click the **VPN** toggle switch to enable the VPN connection.
   b. In the **VPN Server URL** field, enter the IP address, hostname, or FQDN of the VPN server.
   c. From the **Protocol** drop-down list, select either CiscoAnyConnect or GlobalProtect based on your preference.

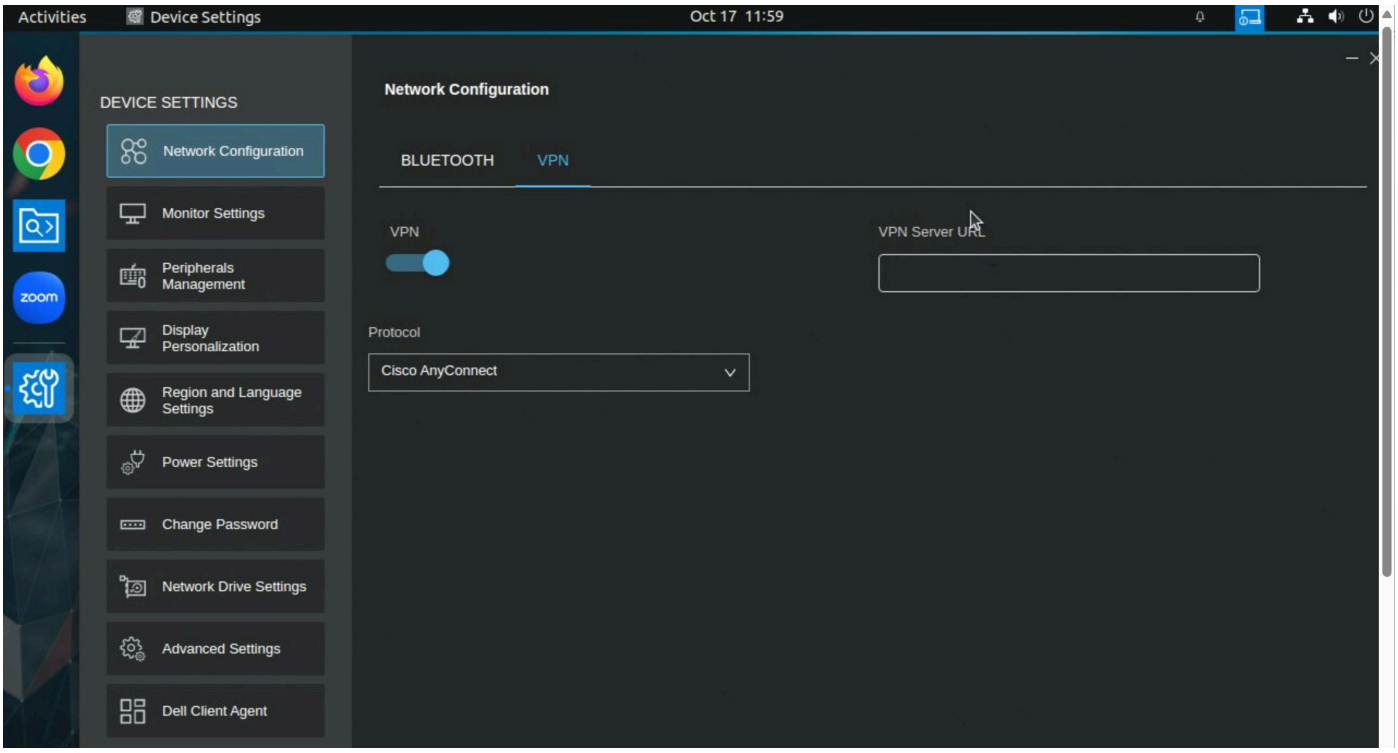


Figure 112. VPN

6. Click **Save & Apply**.

Connect to a VPN on Dell Hybrid Client

Prerequisites

- Ensure that VPN settings are configured either on Wyse Management Suite or the local Dell Hybrid Client UI. See, Configure the VPN settings and Configure the network settings locally.
- Ensure that VPN certificates are installed on Dell Hybrid Client using the Wyse Management Suite app policy.

Steps

1. On the top bar, click the **System Menu** icon.

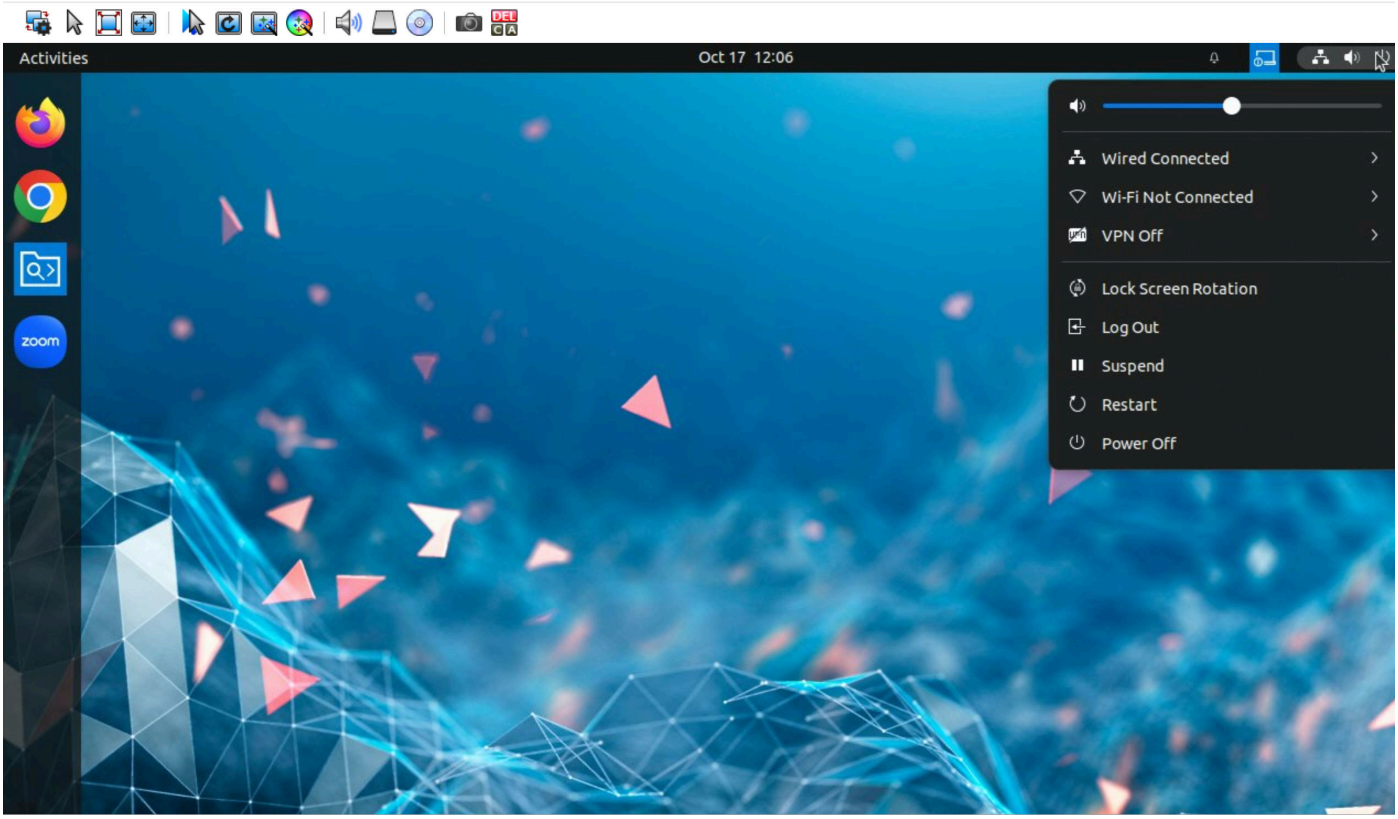


Figure 113. System Menu

2. Click the **VPN** button, and then click **Connect**.
The **Connect to VPN** dialog box is displayed.

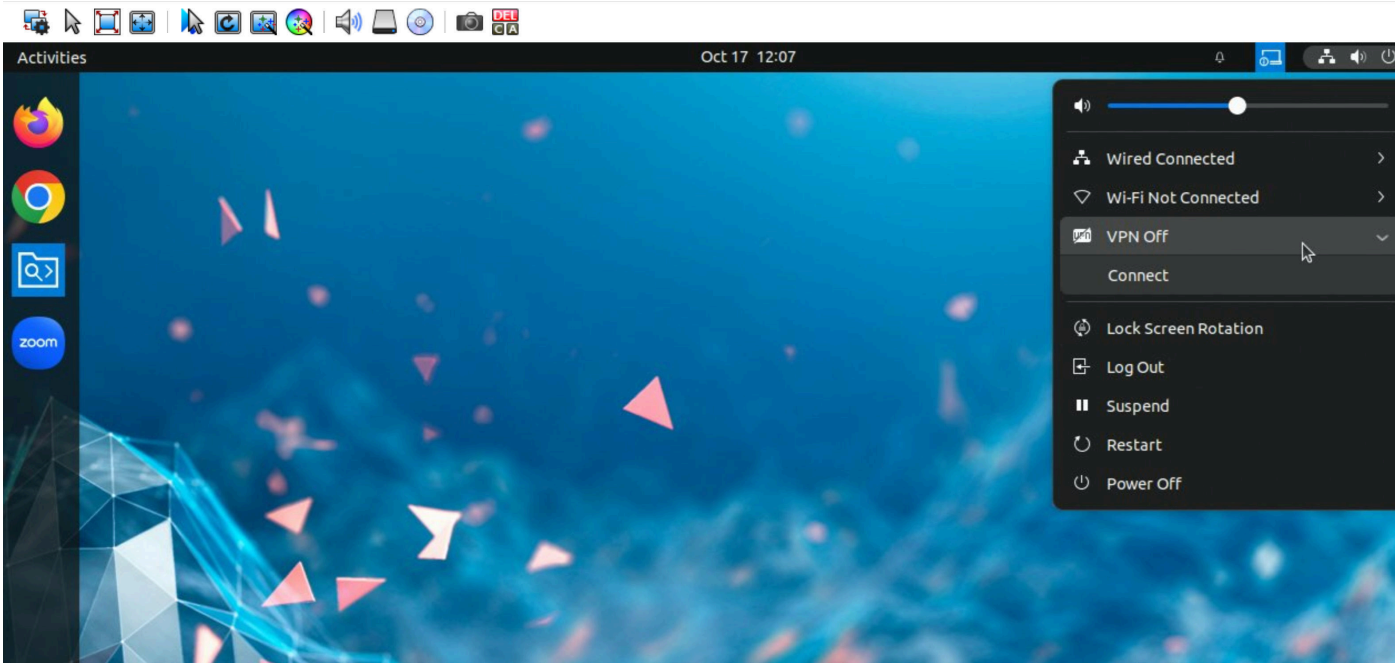


Figure 114. Connect to VPN

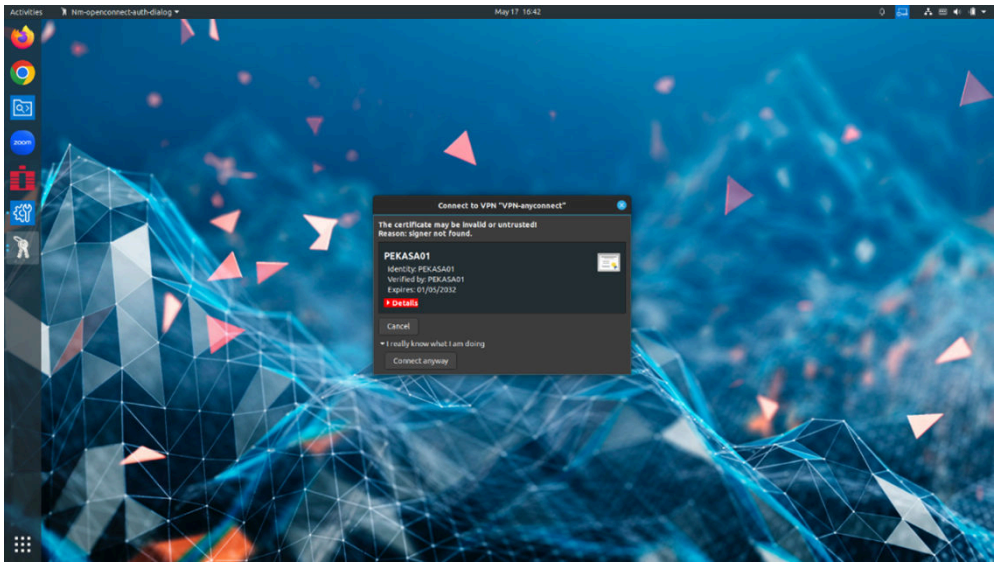


Figure 115. Connect to VPN

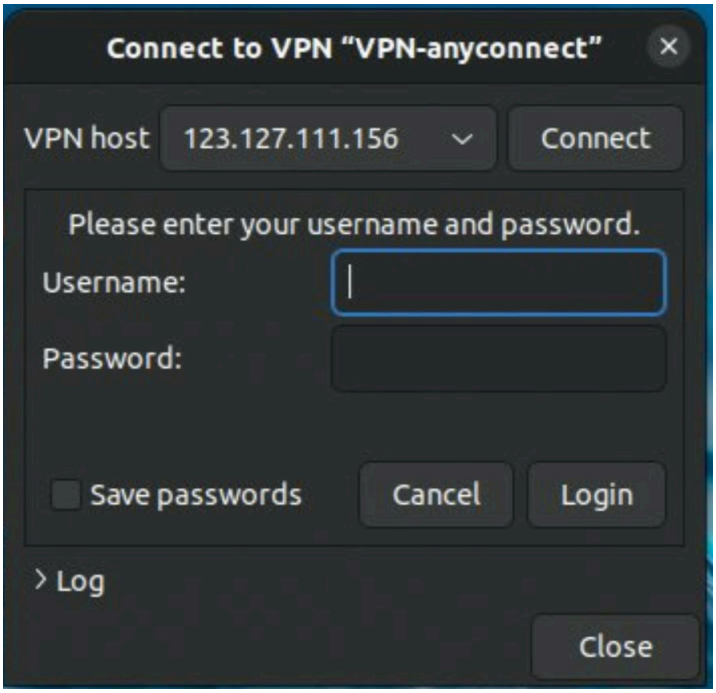


Figure 116. Username and Password

3. Enter the username and password.
4. Click **Login**.
   After the successful login, the VPN is connected.

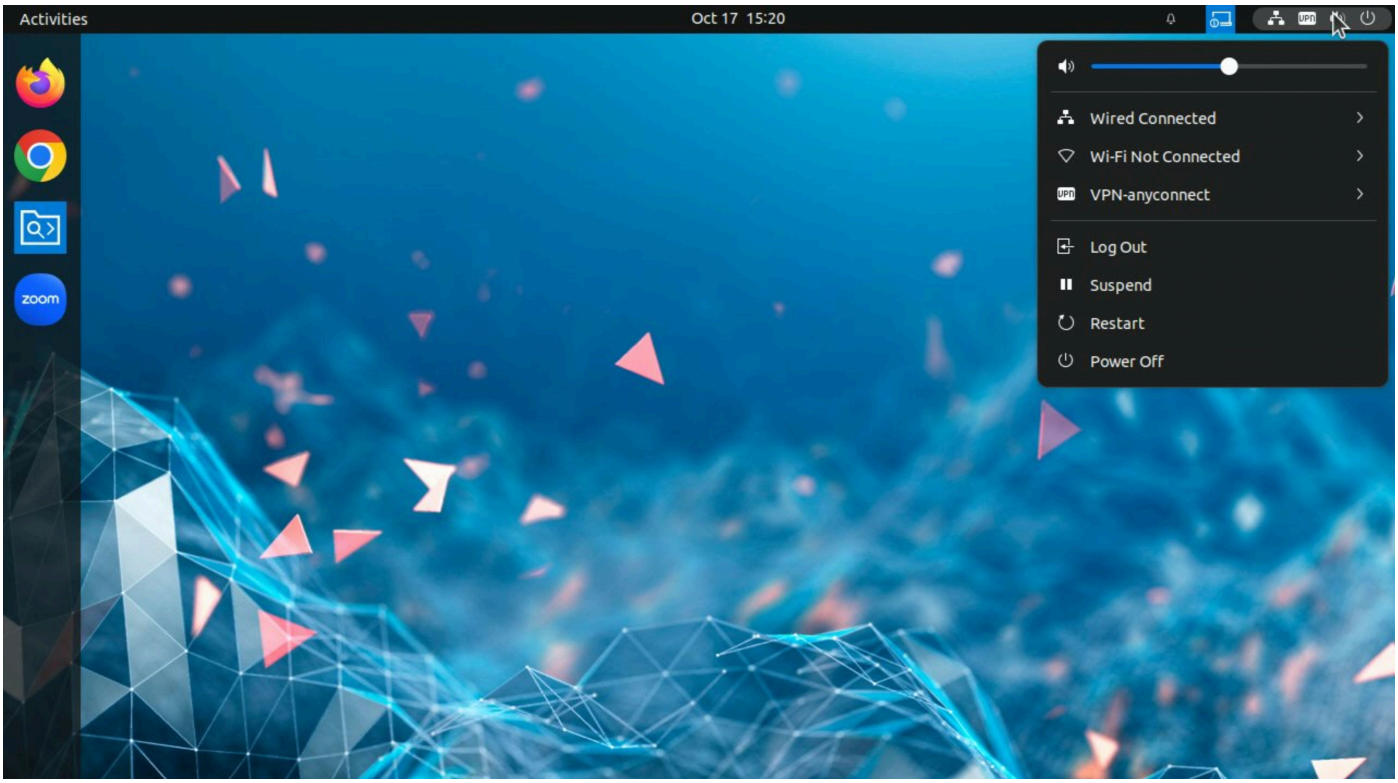


Figure 117. VPN connected

Configure the power profile settings

Power Profiles provide efficient power management capabilities for devices that are powered by Dell Hybrid Client.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred user group.

   NOTE: The power profile option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Power Settings** and click **Power Profile**.
6. From the **Power Profile** drop-down list, select one of the following options:
   - **Energy Saving**—This mode saves power on your device by reducing system performance.
   - **Balanced**—By default, the Balanced power mode is selected. This mode balances energy consumption and system performance by adapting the processor speed of the device to your activity.
   - **Maximum Performance**—This mode maximizes system performance by running processor at higher speeds.
7. Click **Save & Publish**.

   NOTE: You can also configure the power profile settings locally on Dell Hybrid Client. User personalization is supported for domain users if the power profile settings is changed from the **Device Settings** window and if the user personalization feature is enabled on Wyse Management Suite. See, Configure the power settings locally.

User Data Roaming

- Dell Hybrid Client supports user data roaming across devices that is powered by Dell Hybrid Client.
- User Data Roaming is only applicable to **Domain User** which is part of User Group Policy.
- When a user logs in to another device with the same username, all opened applications (VDI) and browser data are restored from the previous device.
- By default, the User Data Roaming option is disabled.
- When Wyse Management Suite Repository Storage is 70% full, then the User Data Roaming functionality does not work.

Configure the User Data Roaming Settings

This section provides the procedure to configure the user data roaming settings.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred **Device Policy** group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **WMS Settings** and click **WMS Client Settings**.
6. In the **User Data Roaming** section, click the **Enable User Data Roaming** toggle switch to enable the option.

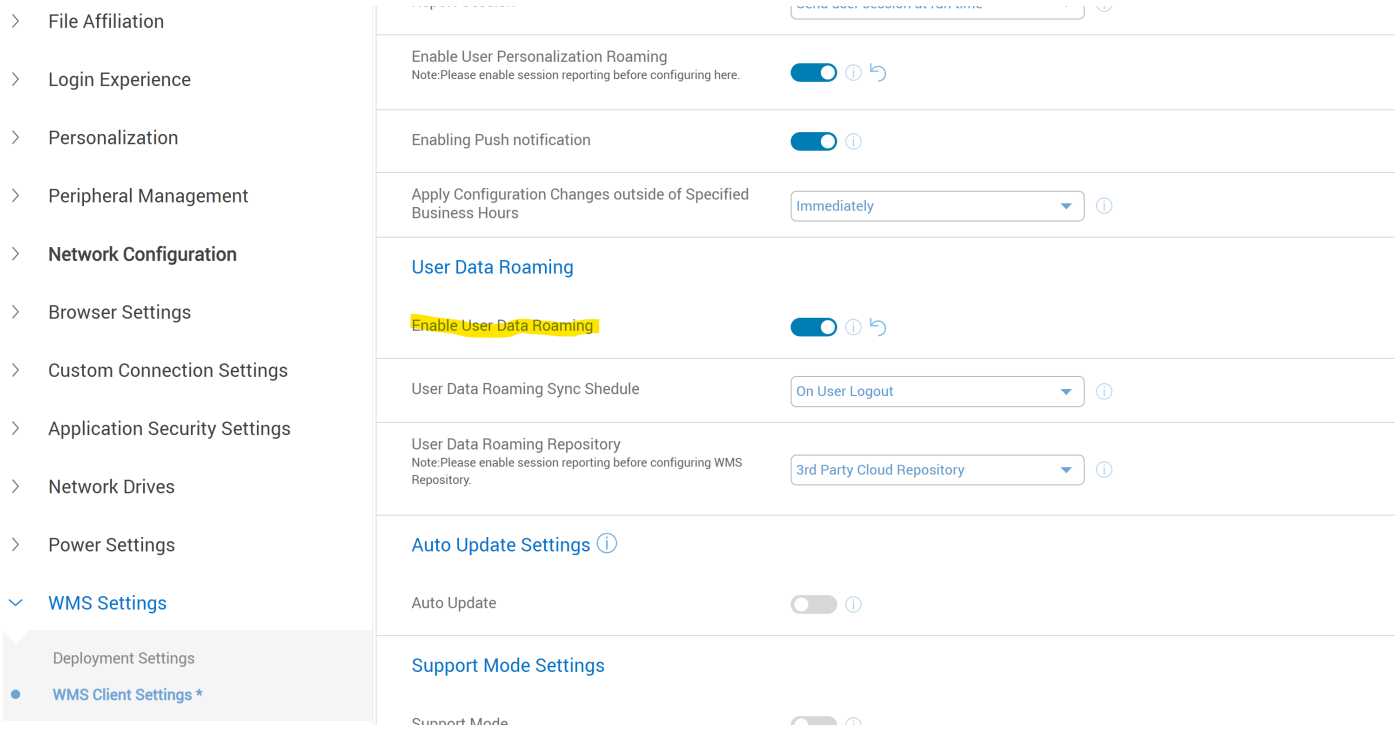


Figure 118. WMS Client Settings

7. Specify whether the user data roaming must be synchronized when the user logs out of Dell Hybrid Client.

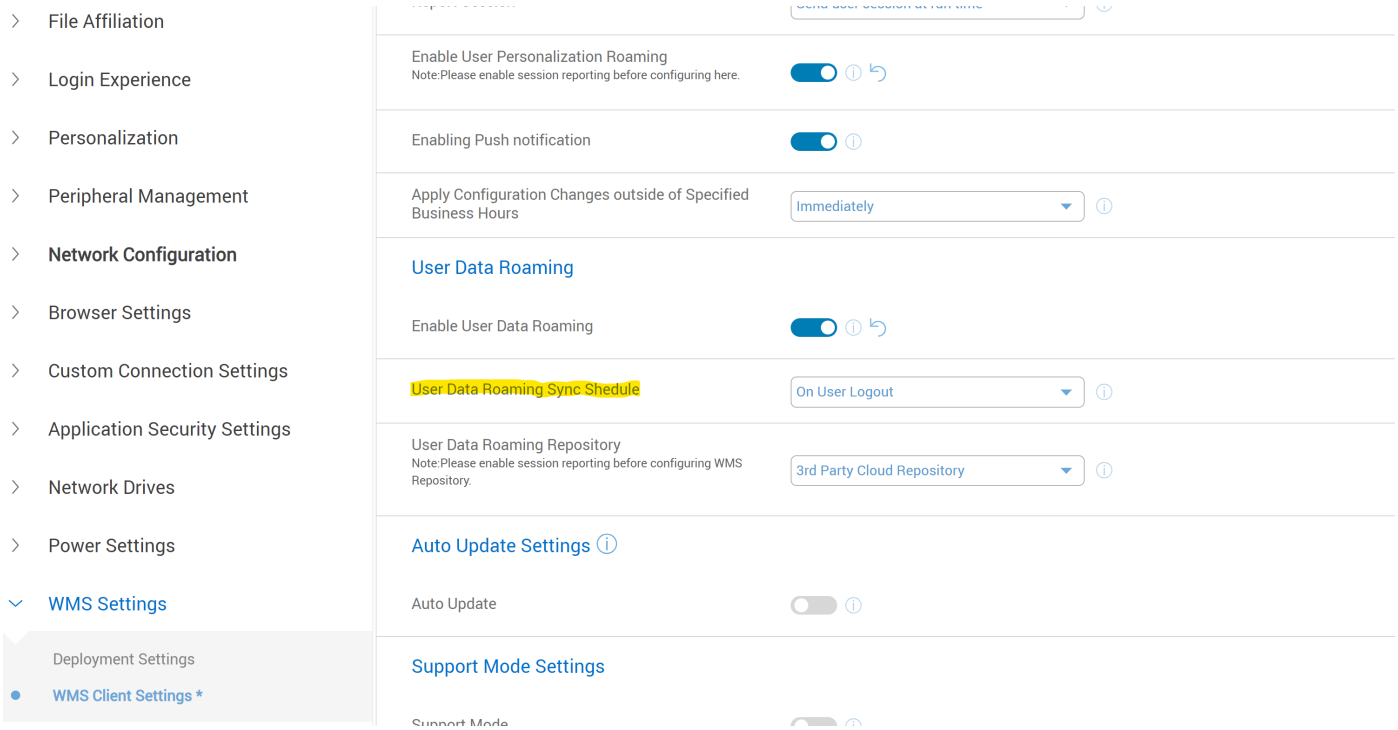


Figure 119. WMS Client Settings

8. From the **User Data Roaming Repository** drop-down list, select either **WMS Repository** or **3rd Party Cloud Repository**.

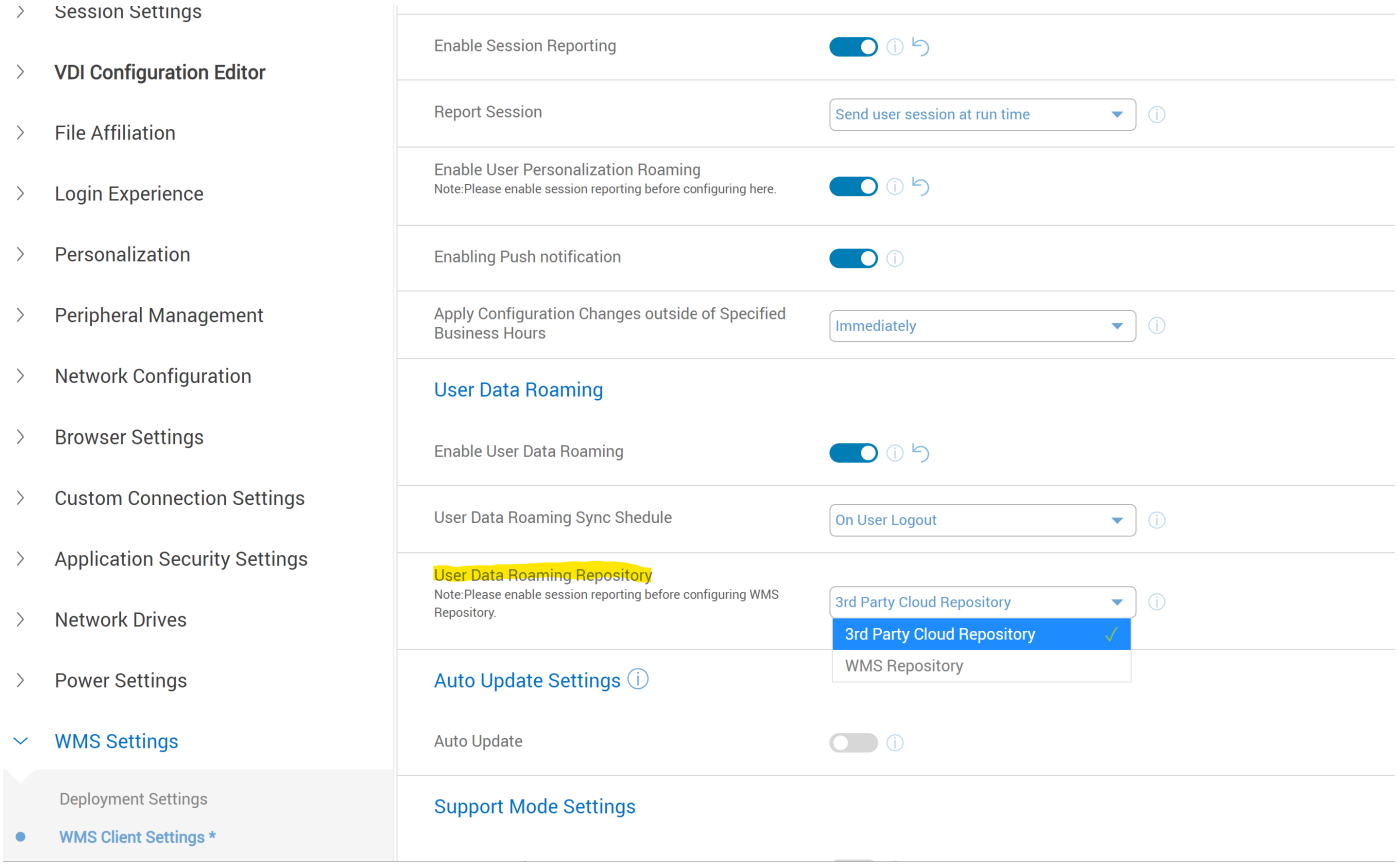


Figure 120. WMS Client Settings

NOTE: You must add Cloud configuration Azure/GCP from **File Affiliation** to use third-party Cloud Repository.

NOTE: Enable Session reporting configuration if the User Data Roaming Repository is selected as WMS Repository.

9. Click **Save & Publish**.

Switch users(Inactivity Action)

Dell Hybrid Client supports switching between users by using the Ubuntu capability. If you lock the system and leave the system idle, the user is logged out or the device is powered off after the timeout period is elapsed. This feature enables multiple users to log in to Dell Hybrid Client when a particular user locks the system and leaves the system idle.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Power Settings** and click **Suspend & Power Button**.
6. Click the **Inactivity Action** toggle key.
7. Select the inactive timeout period.
8. From the **Action after Timeout** drop-down list, select either **Logout** or **Shutdown**. This determines the action to be performed by the device after the timeout period is elapsed.
9. Click **Save & Publish**.

Block keyboard shortcut keys

Dell Hybrid Client allows you to disable certain keyboard shortcut key combinations. You can block the keyboard shortcut keys, making them unavailable for users. The blocked keyboard combinations do not work in any of the local desktop or applications excluding the VDI sessions. Blocking of keyboard shortcut keys is not supported within VDI sessions.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.

   NOTE: The block keyboard shortcut keys option is available only for device policy groups.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Application Security Settings**, and click **Keyboard Shortcut keys**.
6. Click the **Block Keyboard Shortcut keys** toggle switch to enable the option.
7. To block a specific keyboard shortcut keys, do the following:
   a. Click **Add Row**.
   b. From the **Modifiers** drop-down list, select a modifier key.
8. To block multiple keyboard shortcut keys, repeat step 7.
9. Click **Save and Publish**.

Configure Keyboard Layout for Login Screen using Wyse Management Suite

About this task

The following are the steps to configure keyboard layout by using Wyse Management Suite.

Steps

1. Register Dell Hybrid Client device to Wyse Management Suite.
2. Log in to Wyse Management Suite.
3. Go to **Groups & Configs** page and select your preferred group.
4. Click `Edit Policies > Dell Hybrid Client > Dell Hybrid Client 2.x`. Hybrid Client page is displayed.
5. Click the **Advance** tab.
6. Expand Peripheral Management and click **Keyboard**. Use this option to configure the Keyboard Layout option.
7. From the Keyboard Layout drop-down, select any keyboard layout (example- English).
8. Select any Keyboard Layout from the keyboard layout List (example- French). Save and publish.
9. Log out the device and in the login screen check if the selected keyboard is applied.
10. On login screen, enter **Username** and **Password**. It takes input with selected keyboard layout.

    NOTE: Keyboard layout for Chinese, Korean, and Japanese must install full language package from Wyse Management Suite and has to configure system with respective language for the particular layout.

    NOTE: If you select keyboard layout from Wyse management suite, it is applicable for Dell Hybrid Client Login Screen and Dell Hybrid Client Desktop. But if you select keyboard layout from device settings, it is applicable only for Dell Hybrid Client Desktop.

Simplified Certificate Enrollment Protocol

Simplified Certificate Enrollment Protocol (SCEP) is used in a closed network where all end-points are trusted. The goal of SCEP is to support the secure issuance of 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). The network device has a private key and an associated certificate that is issued by a CA. Applications on the device may use the key and its associated certificate to interact with other entities on the network.

You can configure SCEP settings using Wyse Management Suite and Device Settings. See, Configure SCEP using Wyse Management Suite and Configure SCEP locally.

Configure the SCEP settings using Wyse Management Suite

Prerequisites

- Ensure that you have a Windows server with Active Directory (AD), Domain Name Server (DNS), Active Directory Certificate Services (ADCS), and Network Device Enrollment Service (NDES) configured. This server acts as the SCEP server and must contain CA certificates.
- Ensure that you have the (Radius) server with AD for 802.1.x authentication.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **SCEP**.
6. Click the **Enable SCEP** toggle key.
7. To add a single certificate, click **Add Row**, and configure the following settings:
   a. In the **Certificate Name** field, specify the certificate name.
   b. If the 802.1x authentication is enabled, you can select either **User** or **Machine** from the Authentication Mode drop-down list. Based on your selection, user or machine mode certificates are obtained from the SCEP server.

      NOTE: If you select the user mode authentication for AD User, the enrolled certificate is available only for that particular AD user.

   c. In the **SCEP URL** field, enter the complete URL path of the SCEP server.
   d. In the **Challenge Password** field, enter the Certificate Enrollment Challenge Password. You can obtain the challenge password from the SCEP server.

   NOTE: If you are adding SCEP from Wyse Management Suite, **Yes** is selected as the default value for the **SCEP from WMS** option. This selection cannot be changed by the administrator.

   NOTE: SCEP can be configured with device serial number as SCEP certificate name. The special characters that can be used for these are **$SN** and **$sn**. These special characters can be used in 802 configuration also as SCEP certificate name.

8. To add multiple certificates, repeat step 7.
9. Click **Save & Publish**.

Network authentication using IEEE 802.1x

IEEE 802.1x is the standard used for authenticating a device on the network. You can configure the IEEE 802.1x authentication for a wired network connection using Wyse Management Suite. The following 802.1x authentication types are supported:

- EAP-PEAP (MSCHAPv2)—Supports seamless 802.1x authentication that uses Active Directory domain user credentials for EAP-MSCHAPv2 authentication.

- EAP-TLS—Supports certificate-based authentication that uses SCEP for certificate enrollment.

NOTE: When you select the 802.1x user mode or machine mode, the corresponding SCEP must be selected for all configurations.

Configure the EAP-PEAP MSCHAPv2 user mode authentication

Prerequisites

- If you are using a SCEP certificate, ensure that you have enabled SCEP using Wyse Management Suite and the SCEP certificate is already enrolled. See, Configure SCEP.
- If you are using a CA certificate, ensure that the CA certificate is available for authentication.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Network Configuration**, and click **802-1x Authentication**.
6. Click the **Enable 802-1x** toggle key to enable the 802-1x authentication for wired connection on the Ethernet 0 port.
7. From the **Authentication Type** drop-down list, select **Protected EAP (PEAP)**.
8. From the **Authentication Mode** drop-down list, select **User**.

   NOTE: Only domain user is supported for PEAP user mode authentication. Local and Guest user is not supported.

9. From the **PEAP Version** drop-down list, select the PEAP version for authentication—**Automatic**, **Version 0**, or **Version 1**.
10. To use a SCEP certificate, enable the **Use SCEP certificate** toggle key and enter the SCEP certificate name. By default Use SCEP certificate is enabled.
11. To use a CA certificate, enable **CA Certificate Required** toggle key.

    If the CA certificate is added from the **Privacy & Security** > **Certificate** section, disable **Use SCEP Certificate** toggle key and enable **CA Certificate required**. Enter that particular CA certificate name.
12. From the **Inner Authentication** drop-down list, select **MSCHAPv2**.
13. Click **Save & Publish**.

Next steps

Log in to the Dell Hybrid Client-powered device as a domain user. The 802.1x is triggered and the 802-1 authentication automatically starts.

If log in is successful, the device gets the IP address from the protected LAN. If log in is unsuccessful, the 802.1x authentication fails and the device remains in the guest LAN.

When you log out or restart, the device will move to guest LAN by sending an EAPOL logoff to switch and disable the 802.1x configuration.

Configure the EAP-PEAP MSCHAPv2 machine mode authentication

Prerequisites

- If you are using a SCEP certificate, ensure that you have enabled SCEP using Wyse Management Suite and the SCEP certificate is already enrolled. See, Configure SCEP.
- If you are using a CA certificate, ensure that the CA certificate is available for authentication.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.

The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.

4. Click the **Advanced** tab.
5. Expand **Network Configuration**, and click **802-1x Authentication**.
6. Click the **Enable 802-1x** toggle key to enable the 802-1x authentication for wired connection on the Ethernet 0 port.
7. From the **Authentication Type** drop-down list, select **Protected EAP (PEAP)**.
8. From the **Authentication Mode** drop-down list, select **Machine**.

   NOTE: Guest user along with Domain and Local user are supported for PEAP machine mode authentication.

9. From the **PEAP Version** drop-down list, select the PEAP version for authentication—**Automatic**, **Version 0**, or **Version 1**.
10. To use a SCEP certificate, enable the **Use SCEP certificate** toggle key and enter the SCEP certificate name. By default Use scep certificate is enabled.
11. To use a CA certificate, enable the **CA Certificate Required** toggle key and enter the CA certificate name.

    If the CA certificate is added from the **Privacy & Security** > **Certificate** section, disable **Use SCEP Certificate** toggle key and enable **CA Certificate required**. Enter that particular CA certificate name.
12. From the **Inner Authentication** drop-down list, select **MSCHAPv2**.
13. Enter the machine password. This password is used to authenticate the device.

    Administrator has to set password for targeted computer objects registered in domain and the same password is recommended for single group.

    NOTE: If the device is not joined in domain, Administrator has to create computer object manually using the computer name of the machine.

14. Click **Save & Publish**.

Next steps

Log in to the Dell Hybrid Client-powered device as a domain user or local user. The 802.1x launcher is triggered and the 802-1 authentication automatically starts.

If log in is successful, the device gets the IP address from the protected LAN. If log in is unsuccessful, the 802.1x authentication fails and the device remains in the guest LAN.

When you log out or restart, the device will move to guest LAN by sending an EAPOL logoff to switch and disable the 802.1x configuration.

Configure the EAP-TLS user mode authentication

Prerequisites

- Ensure that you have enabled SCEP using Wyse Management Suite and the SCEP certificate is already enrolled. See, Configure SCEP.
- If you are using a CA certificate, ensure that the CA certificate is available for authentication.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Network Configuration**, and click **802-1x Authentication**.
6. Click the **Enable 802-1x** toggle key to enable the 802-1x authentication for wired connection on the Ethernet 0 port.
7. From the **Authentication Type** drop-down list, select **TLS**.
8. From the **Authentication Mode** drop-down list, select **User**.

   NOTE: Only domain user is supported for TLS user mode authentication. Local and Guest users are not supported.

9. Enter the SCEP certificate name.
10. To use a CA certificate, click the **CA Certificate Required** toggle key.

11. Enter any Password in **Private Key** password field to encrypt/Decrypt the SCEP certificates during 802.1x Authentication.
12. Click **Save & Publish**.

Next steps

Log in to the Dell Hybrid Client-powered device as a domain user. The 802.1x is triggered and the 802-1 authentication automatically starts.

If log in is successful, the user certificate is enrolled via SCEP and the device gets IP address from the protected LAN. If log in is unsuccessful, the 802.1x authentication fails and the device remains in the Guest LAN.

When you log out or restart, the device will move to guest LAN by sending an EAPOL logoff to switch and disable the 802.1x configuration.

Configure the EAP-TLS machine mode authentication

Prerequisites

- Ensure that you have enabled SCEP using Wyse Management Suite and the SCEP certificate is already enrolled. See, Configure SCEP.
- If you are using a CA certificate, ensure that the CA certificate is available for authentication.
- Ensure that the user certificate and the private key certificate are available for authentication.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device policy group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Network Configuration**, and click **802-1x Authentication**.
6. Click the **Enable 802-1x** toggle key to enable the 802-1x authentication for wired connection on the Ethernet 0 port.
7. From the **Authentication Type** drop-down list, select **TLS**.
8. From the **Authentication Mode** drop-down list, select **Machine**.

   NOTE: Guest, Domain user and Local users are supported for TLS machine mode authentication.

9. Enter the SCEP certificate name.
10. To use a CA certificate, click the **CA Certificate Required** toggle key.
11. Enter any Password in **Private Key** password field to encrypt/Decrypt the SCEP certificates during 802.1x Authentication.
12. Click **Save & Publish**.

Next steps

Log in to the Dell Hybrid Client-powered device as a domain user or local user. The 802.1x launcher is triggered and the 802-1 authentication automatically starts.

If log in is successful, the user certificate is enrolled via SCEP and the device gets IP address from the protected LAN. If log in is unsuccessful, the 802.1x authentication fails and the device remains in the Guest LAN.

When you log out or restart, the device will move to guest LAN by sending an EAPOL logoff to switch and disable the 802.1x configuration.

Connect to hidden Wi-Fi networks using Wyse Management Suite

Steps

1. Log in to Wyse Management Suite.

2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Network Configuration**, and click **Wireless**.
6. Click **Add Row** and enter the details of the wireless connection.
7. Click **Save & Publish**.

9

User applications

When you log in to Dell Hybrid Client, certain default applications are displayed on the **Applications overview** screen.

Browse the Internet

Dell Hybrid Client enables you to browse the web securely. On Dell Hybrid Client, website tracking is disabled to ensure that the enterprise data or browser history is untracked. Use either Google Chrome or Mozilla Firefox to browse the web.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
   The **Application Overview** screen is displayed.
3. Click any of the following browser icons to launch the corresponding web browser.
   - **Mozilla Firefox**
   - **Google Chrome**

   NOTE: Dell Hybrid Client 2310 supports the configuration of monitor position of the Chrome browser.

   Figure 121. Monitor Id
4. Enter the URL of the web page in the address bar, and start browsing the web.

Enable or disable multicontainers for Firefox

Dell Hybrid Client supports the multicontainer feature that provides privacy for the Mozilla Firefox browser. It ensures that the cookies downloaded by one container are not available to other containers. All your logged in sessions, site preferences, and other browser data are not carried over to the new container. By default, the multicontainer feature is enabled on Dell Hybrid Client.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click **Firefox settings**.
6. Click the **MultiContainers** toggle key to enable or disable the multicontainer feature.

   NOTE: By default **Multicontainers** is enabled.
7. Click **Save and Publish**.
8. Log in to Dell Hybrid Client and open the Mozilla Firefox web browser.
9. If the multicontainer feature is enabled, click the **Containers** icon and select the container that you want to open.
   For more information about multicontainers, see the *Mozilla Firefox documentation* at support.mozilla.org.

Enable or disable site isolation for Chrome

Dell Hybrid Client supports the site isolation feature that provides security for your Google Chrome browser. It ensures that pages from different websites use different processes, wherein each process runs in a sandbox that limits what the process is allowed to do. By default, the site isolation feature is enabled on Dell Hybrid Client.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click **Google Chrome settings**.
6. Click the **Site isolation** toggle key to enable or disable the site isolation feature.

   NOTE: By default **Site isolation** is enabled.

7. Click **Save and Publish**.
8. Log in to Dell Hybrid Client and open the Google Chrome web browser.
9. Go to your preferred website.
   If the site isolation feature is enabled, all websites that you browse run in a dedicated rendering process, which is isolated from each other.

   For more information about site isolation, see the *Google Chrome documentation* at support.google.com.

Enable or disable plugins for Chrome

Dell Hybrid Client supports plugins that can be used to enhance your browsing experience.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click **Google Chrome settings**.
6. Click the **Plugins** toggle key to enable or disable plugins for Google Chrome.
7. Click **Save and Publish**.
8. Log in to the device and access the Google Chrome web browser.

Custom policy configuration for Firefox and Chrome

Custom policy configurations are supported for Firefox and Chrome browsers.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click either **Firefox settings** or **Google Chrome settings**.
6. In the **Policy Configuration** field, enter one or more custom policy names. Each policy name must be associated with a key value. If you are specifying multiple policy names, each policy name must be separated by a comma.

NOTE: For more information about policy names of Google Chrome, see the Google Chome documentation at support.google.com.

NOTE: For more information about policy names of Mozilla Firefox, see the Mozilla Firefox documentation at support.mozilla.org.

7. Click **Save and Publish**.

Allow and Deny access to websites

Dell Hybrid Client enables you to allow or block access to websites. You can block certain websites, making them inaccessible from the browser. You can exclude certain websites from blocking, making them accessible from the browser.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click either **Firefox settings** or **Google Chrome settings** based on your preference.
6. From the **URL Settings** drop-down menu, select **Website Access Control**.
7. To configure the **URL Denylist** settings, click **Add Row**, and enter the URL of the website that you want to block.
8. To configure the **URL Allowlist** settings, click **Add Row**, and enter the URL of the website that you want users to access.
9. Click **Save & Publish**.

Example

- Allow only specific websites:
  - Deny `".org", ".com"`
  - Allow selected sites—`"mail.example.com"`, `"wikipedia.org"`, `"google.com"`.
- Deny all access to a domain, except to the mail server using HTTPS and to the main page:
  - Deny `"example.com"`
  - Allow `"https://mail.example.com"`.
  - Allow `".example.com"`, and may be `".www.example.com"`.
- Deny all access to YouTube, except for selected videos:
  - Deny `"youtube.com"`
  - Allow `"youtube.com/watch?v=V1"`.
  - Allow `"youtube.com/watch?v=V2"`.

Block .com and allow google.com

NOTE:

Mozilla Firefox supports only HTTP and HTTPS. When you are adding the URL that you want to block, you must specify the URL without HTTP, or HTTPS. By default, the HTTP, or HTTPS prefix is added to the website URL. For example, instead of `https://www.youtube.com`, you must specify only youtube.com or www.youtube.com. The same guideline is applicable when configuring URLs that you want to access.

Configure the browser shortcut settings

Dell Hybrid Client enables you to create website shortcuts to open your preferred website in a specific web browser. You can use Wyse Management Suite to configure the browser shortcut settings.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.

The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.

4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click **Browser Shortcuts**.
6. Click **Add Row** and configure the following settings for a single browser shortcut:
   a. In the **Shortcut Name** field, enter the name for the website shortcut.
   b. In the **URL** field, enter a secure URL of the website that you want to access.
   c. From the **Browser** drop-down list, select a browser on which you want the shortcut to be launched.
   d. From the **Window Size** drop-down list, select the window size of the browser shortcut.
   e. In the **Additional Arguments** field, enter the command line argument. Multiple arguments can be added by using space as a delimiter. This option is available from Dell Hybrid Client 1.6 onwards.
   f. Click the **Auto Launch Shortcut on Logon** toggle key to enable or disable the option. If enabled, the website URL that you specify is automatically launched after you log in to Dell Hybrid Client.
   g. Click the **Auto Reconnect** toggle key to enable or disable the option. If enabled, the connection automatically reconnects after you close the session.
   h. Enter the time duration in seconds to delay the reconnection attempt after a disconnection occurs.
7. Browse and upload an icon for the browser shortcut. You can also use the default icon as the browser shortcut icon.
8. To create multiple browser shortcuts, repeat step 6.
9. Click **Save and Publish**.

Create a desktop shortcut to a browser URL

Dell Hybrid Client allows you to pin a URL from the browser to the desktop for quick access. To pin a browser URL, drag and drop the URL to the desktop. A browser shortcut is created on the desktop. Double-click the desktop shortcut, and the URL is launched in the default browser. If the same domain user logs in to another device, the pinned URL shortcut is still displayed on the desktop.

Steps

1. Log in to Dell Hybrid Client.
2. Launch a web browser.
3. Based on the web browser, do the following:
   - **Firefox browser**
     a. Type the URL in the address bar.
     b. Insert a space after the URL.
     c. Select the full URL including the extra space.
     d. Drag and drop the URL to the desktop.
   - **Chrome browser**
     a. In the address bar, type the website URL.
     b. Drag and drop the URL to the desktop.
4. Go to the desktop.
   A browser shortcut is created.

Next steps

Double-click the desktop shortcut. The website URL is launched in the default browser.

Using Dell File Explorer

Dell File Explorer is a file browser that provides a simple way to manage your local, cloud, network, and external files on your client. Files are launched using local, VDI, or cloud applications based on the priority set in the File Affiliation settings. For more information about how to configure the File Affiliation settings, see File Affiliation.

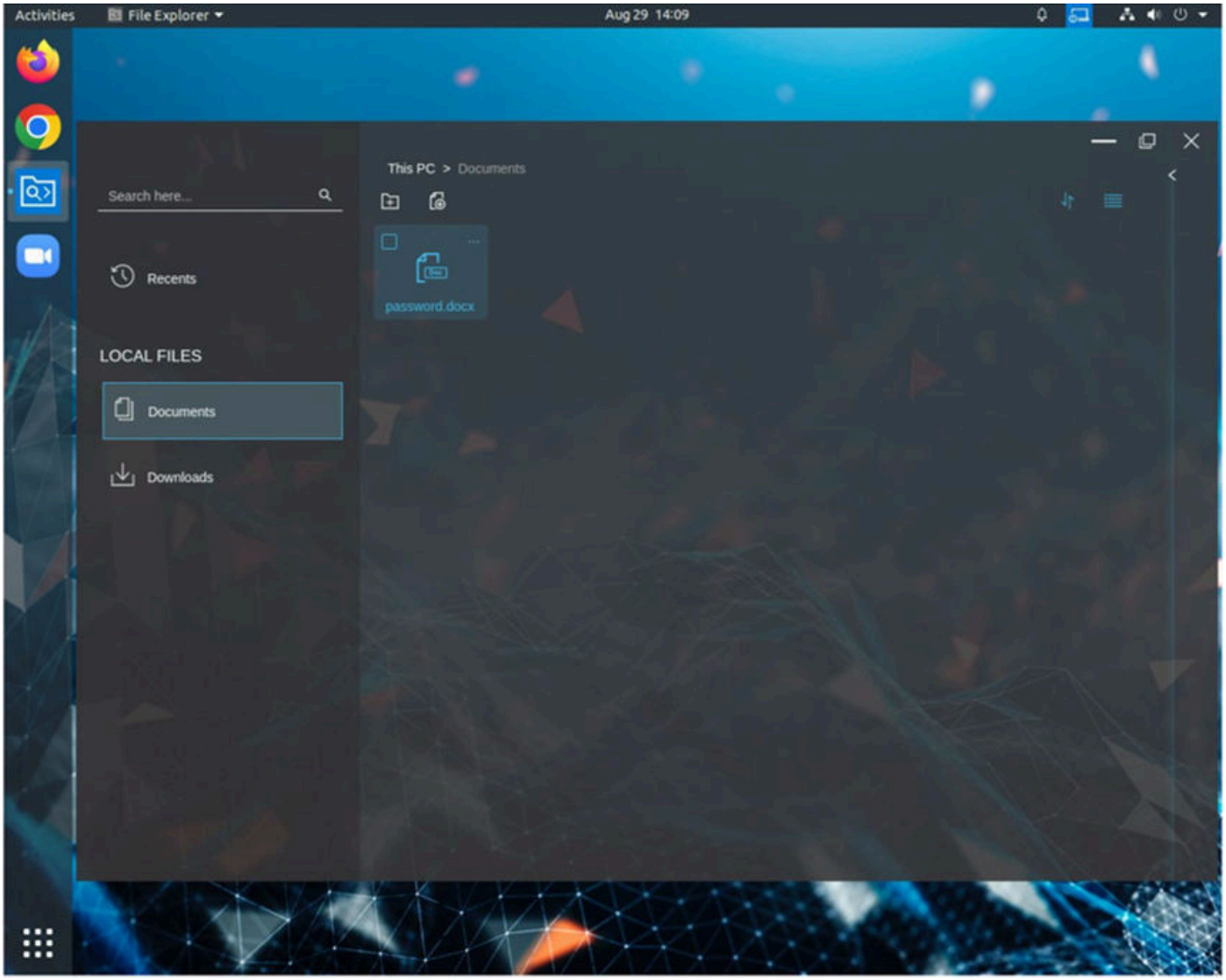


Figure 122. File Explorer

You can use the file explorer to do the following:

- View your files, folders, and drives.
- View file attributes such as **Name**, **Size**, **Modified**, **Location**, and **Offline**.
- Search and sort your files.
- Access local files and folders.
- Access cloud files.
- Access external files that are stored on a USB drive or downloaded from web.
- Access network shares.

File explorer supports the following file operations:

- Create a file.
- Open a file.
- Open with your preferred application*.
- Upload a file.
- Compress a file or folder*.
- Uncompress a file*.
- Delete a file.
- Copy a file.
- Move a file.
- Rename a file.

To access the File Explorer, click the **Show Applications** icon on the desktop screen, and then click the **File Explorer** icon.

Table 12. File Explorer Components

Component	Description
Left pane	The left pane displays the navigation pane that contains the file and folder structure of Dell Hybrid Client. You can view the following categories: • **LOCAL FILES**—Displays the files and folders on your local client. By default, **Documents** and **Downloads** folders are displayed. Users can access only their respective local documents and downloads folders from the current drive in File Explorer for security reasons. The **Pictures** folder is available if the **Print Screen** option is enabled. • **One Drive/Google Drive/Box Account**—Displays the files and folder on your Azure cloud, Google cloud, or Box personal account. Use the **Sync** button to synchronize cloud files to the client, so files can be accessed from File Explorer. Any local file uploaded to cloud is available in the following location: ○ Cloud root for GCP. ○ Uploads folder for Azure. ○ All Files folder for Box. **NOTE:** Multiple cloud providers for the same user account can be configured. **NOTE:** As a guest user, you can access the corporate cloud accounts. • **EXTERNAL FILES**—Displays the files and folder on your connected USB drive and network shares.
Right pane	The right pane displays the additional options available in the File Explorer. • **Files and Bytes**—Displays the total number of selected files and the total size of all the files combined. • **Create New File**—Enables you to create a file in the current folder. Click the **Create New File** icon to create a file. • **Add New Folder**—Enables you to create a folder in the current folder. Click the **Add New Folder** icon to add a folder. • **Recents**—Displays all the recently viewed files and documents.
Search box	Global file search provides the ability to search for documents across any folder.
Select multiple files	The select check box enables you to select one or more files in the current folder (including the cloud corporate or personal accounts).
File and folder listing	Displays the files and folders in the current folder. You can change the current view by clicking the list or grid buttons. • **List view**—Click the List view icon to display files and folders vertically as a single column. • **Grid view**—Click the icon Grid view to display files and folders in a particular pattern, wherein the cells are arranged vertically and horizontally within the grid list.
Sorting lists	This option enables you to sort the file list using the following field columns: • **Name**—Click the column header to sort the list by file name. Files are sorted alphabetically. • **Date Modified**—Click the column header to sort the list by date modified. Files are sorted either in ascending order or descending order. • **Size**—Click the column header to sort the list by file size. Files are sorted either in ascending order or descending order. • **Type**—Click the column header to sort the list by file type.
Drag and Drop files	Enables you to quickly upload a file to cloud using the Drag-and-Drop box on the right side.

Table 13. File Explorer—additional features

Feature	Summary
File synchronization	Dell Hybrid Client supports automatic and immediate synchronization of file data when a file is edited on the local, network share, VDI, or cloud. File synchronization happens automatically and the user does not need to relogin to Dell Hybrid Client for the functionality to work. For example, opening the cloud drive files in VDI or local applications and any modifications are synchronized automatically.

Table 13. File Explorer—additional features (continued)

Feature	Summary
Copy and Paste	Copy and Paste function is supported between local to local drivers and external drives. The progress bar is supported for the copy function.
Move one or more files	Move function is supported between local to local drivers and external drives. The progress bar is supported for the move function.
Compress files	Compress function enables you to reduce the size of a file or folder that is stored locally. A smaller zip file is created when you use the compress function.
Uncompress files	Uncompress function enables you to extract a zip file that is stored locally. The user has the capability to uncompress a password-protected ZIP file.
Open with function	Open with function enables you to select the application to open a file. This feature is based on the File Affiliation Mode that is configured. See, Open with functionality. The open with function is supported for files that are listed in the Recents and Search Results section.
Offline mode	Cloud files can be made available in offline mode, where user can use the file when network is not available. Cloud files are saved offline automatically when there is no network connection. Offline files are automatically synchronized when the network is available. You can also save cloud files manually for offline use. For more information about saving cloud files for offline use, see Save cloud files for offline use.

For more information about the feature limitations, see the latest *Dell Hybrid Client Release Notes* at www.dell.com/support.

Create a file

Steps

1. On the desktop screen, click the **Show Applications** icon.
   The **Applications Overview** screen is displayed.
2. Click the **File Explorer** icon.
3. Go to the location where you want to create a file.
4. In the right pane, click the **Create New File** icon.
   The **Create New File** dialog box is displayed.
5. Enter the name of the file.
6. From the drop-down list, select the file type. For example, docx, ppt.
7. Click **Create**.

Add a folder

Steps

1. On the desktop screen, click the **Show Applications** icon.
   The **Applications Overview** screen is displayed.
2. Click the **File Explorer** icon.
3. Go to the location where you want to add a folder.
4. In the right pane, click the **Add New Folder** icon.
   The **Add New Folder** dialog box is displayed.
5. Enter the name of the folder.
6. Click **Create**.

Open with functionality

The **Open with** function enables you to select your preferred application to open a file. You can choose not to use the default option to open the file. This option is based on the File Affiliation Mode that is configured on Wyse Management Suite.

Table 14. Open with options

File Affiliation Mode	Open with options
Cloud	No options are available.
Cloud + Local	• Cloud application option is listed. • Local applications are listed based on supported formats of installed applications in Dell Hybrid Client. For example, Dell Hybrid Client is configured to open an XLS file with the LibreOffice Excel application.
VDI	No options are available.
VDI + Local	• VDI applications are listed based on the VDI Broker agent connections that are configured in Wyse Management Suite. • Local applications are listed based on supported formats of installed applications in Dell Hybrid Client. For example, Dell Hybrid Client is configured to open an XLS file with the LibreOffice Excel application.
Cloud + VDI + Local	• Cloud application option is listed. • VDI applications are listed based on the VDI Broker agent connections that are configured in Wyse Management Suite. • Local applications are listed based on supported formats of installed applications in Dell Hybrid Client. For example, Dell Hybrid Client is configured to open an XLS file with the LibreOffice Excel application.

To use the **Open with** function, do the following:

1. Open the **Dell File Explorer** utility.
2. Locate a file, and click the three dots.
3. Click **Open With**.

   A submenu is displayed with the available local or VDI application names. For cloud, the application name is displayed as **Cloud**.
4. Select your preferred application to open the file.

Save cloud files for offline use

Cloud files can be manually saved for offline use, where a user can use the file when network is not available. If you manually set the file to offline mode, you must log off and log in again and then discard the offline file to synchronize the file to cloud.

Prerequisites

Ensure that you have configured the cloud provider—Azure, Google Cloud or Box personal drive.

About this task

This procedure describes the steps to manually save a cloud file offline on Dell Hybrid Client.

Steps

1. Log in to the Dell Hybrid Client.
2. Go to **File Explorer** > **CLOUD DRIVE** (One Drive or Google Drive).
   All the available cloud files or documents are listed.
3. Locate a file and click the three vertical dots that is located in the same row.
4. Click **Save Offline**.
   The file is saved offline, and a green tick is displayed for the **Offline** status.

Next steps

To change offline files to online manually, do the following:

1. Locate the offline file.
2. Click the three vertical dots that is located in the same row.
3. Click **Discard Offline File**.

Format a USB device

Dell Hybrid Client enables you to format a USB device. You can format a used USB device or a new USB device that contains an unformatted file system.

Prerequisites

Ensure that you have configured the **USB Lockdown** option on Wyse Management Suite to allow access to your USB device.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Connect your USB device.
3. Open the **Dell File Explorer** and do either of the following based on your preference:
   - If you want to reformat a used USB drive, locate the USB drive under **EXTERNAL FILES**, and click the three horizontal dots.
   - If you connect a USB device that contains an unformatted file system, the **Unformatted partition detected, would you like to format it** message is displayed.
4. Click **Format**.
   The **Format** dialog box is displayed.
5. Select a file system, and click **Format**.
   A progress bar is displayed. The USB device is formatted to use the file system that you have selected.

Configure a network drive using Wyse Management Suite

A network drive is a drive or share that you can access over a network. Dell Hybrid Client enables you to mount or map a network shared drives using network file sharing protocols. The supported protocols are Server Message Block (SMB), Common Internet File System (CIFS), FTPS, and Samba Share.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Network Drives**, and click **Network Drivers List**.
6. Click **Add Row**.
7. In the **Network drives settings** section, do the following:
   a. In the **Name** field, enter a name for your network drive or share.
   b. From the **Type** drop-down list, select the type of the network share—**Smb/Samba**, **CIFS**, or **FTPS**.

      NOTE: FTPS network drives get mounted only when appropriate certificates are added, such as Iris.local and Cert. You can use the certificate option under **Privacy & Security** on Wyse Management Suite to install the certificates on Dell Hybrid Client.

8. In the **Share URL** field, enter the address of the server in the form of URL.
   - If you are using the network share type as **SMB/Samba** or **CIFS**, enter the share URL in the format `//serverIP/path`. For example, `//1xx.1xx.1x.1xx/test`.
   - If you are using the network share type as **FTPS**, enter the share URL in the format `serverIP`. For example, `105.105.55.122`.
9. If you want anonymous users to access the network share, enable the **Anonymous mode** toggle key.

   NOTE: By default Anonymous mode is disabled.

10. If you want specific users to access the network share, disable the **Anonymous mode**, and do the following:
    a. Enter the username.
    b. Enter the password.

c. Enter the domain name.

11. Click **Save & Publish**.
12. Log in to Dell Hybrid Client, open **File Explorer**, and access the network shared drive that you have mapped.

Access local applications

By default, the following applications are installed on your Dell Hybrid Client:

- **Image Viewer**—Enables you to open most of the image files.
- **Libre Office**—Enables you to view, create, or edit text documents, spreadsheets, and presentations.

NOTE: If the **Mount** option is disabled on Wyse Management Suite for any of the local applications, you cannot open the file from an external USB drive. To access the files from an external USB drive, enable the mount option for respective application from Wyse Management Suite.

To access a local application, do the following:

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.

   The **Application Overview** screen is displayed.
3. Click the application icon to launch the corresponding application.

Pin an application to desktop

Dell Hybrid Client allows you to pin an application to the desktop for quick access.

About this task

NOTE: Pin to Desktop feature is not supported on Ubuntu 22.04.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Locate an application and right-click the application icon.
4. Click **Add to Desktop**.
   A shortcut of the application is added to the desktop.

   NOTE: To delete pinned icons, select specific icon and press **DEL** key on the keyboard.

Next steps

Double-click the desktop shortcut. The application is launched.

Using the Zoom application

Zoom application is a Unified Communications solution that is offered by Zoom. It supports enterprise video conferencing and screen sharing. You can use the Zoom application to make and receive calls.

Steps

1. Log in to Dell Hybrid Client.
2. Click the **Show Applications** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the Zoom application icon.
   The Zoom login window is displayed.
4. Join the meeting using one of the following methods:

- If you want to join without signing in, click **Join a Meeting** and enter the meeting ID number and name.
- If you want to sign in to your Zoom account, click **Sign in** and enter your login credentials.

For more information about using the Zoom application, see the *Quick Start Guides* at https://support.zoom.us.

Installing third-party applications

Dell Hybrid Client enables you to install Dell-signed, unsigned, and custom signed third-party applications.

NOTE: Dell is not responsible for any security vulnerabilities, licenses, or other functionality-related issues that may occur due to the deployment of third-party applications. Ensure that you are aware of the functionality and impact of deploying third-party applications on Dell Hybrid Client.

Use Wyse Management Suite to deploy application packages to devices powered by Dell Hybrid Client. By default, all applications that are delivered by Dell are signed packages.

Some third-party applications may require dependency packages to work. Installation of such applications may fail if its dependencies are not installed. Ensure that all dependencies of a given application are provided along with the main application package.

When you are installing a third-party Debian package, the Dell Hybrid Client-powered device checks for dependency. When the dependency check fails, the device reports the dependency error details to Wyse Management Suite. You can view the dependency details along with the failed status on the Wyse Management Suite page.

You can configure the policy settings on the **Apps and Data** page. Deployment of application policies to the device can be scheduled immediately or later, based on your time zone.

NOTE: If you have configured the Dell Hybrid Client policy settings before the add-on installation, you must reapply the configured settings after you deploy the add-on. Alternatively you can log out and log back in.

For more information about how to deploy an application package using Wyse Management Suite, see the *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Install a Dell-signed application

Prerequisites

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword field, type the model number of your device** or type Dell Hybrid Client.
3. Click the product from search results to open the product support page.
4. On the product support page, click **Drivers & downloads**.
5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the Ubuntu operating system.
6. From the list, locate the required application and click download icon.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Configure the following options:
   a. Expand **Privacy & Security** and click **Security Profile**.
   b. From the **Security Profile** drop-down list, select **High** or **Medium**. The default option is set to **Medium**.
   c. Specify a port number or a range of port numbers in a Comma-Separated Value (CSV) format.
   d. Click **Save and Publish**.
6. Use the standard application policy or the advanced application policy to deploy the Dell-signed application to Dell Hybrid Client.
   For information about how to use the standard application policy or the advanced application policy, see the *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Install a custom-signed application

Prerequisites

Ensure that you get your application signed and have procured the signed certificate from the concerned authority.

- Do the following to create Self Signed certificate:
  1. Generate a Private Key.

     ```
     genrsa -des3 -out private_key_file_name.key 2048
     ```

  2. Generate a Certificate Signing Request (CSR).

     ```
     openssl req -new -key private_key_file_name.key -sha256 -out csr_file_name.csr
     ```

  3. Generating a Self-Signed Certificate.

     ```
     x509 -req -days 365 -in csr_file_name.csr -signkey private_key_file_name.key
     -sha256 -out cert_file_name.cer
     ```

  4. Sign a binary.

     ```
     openssl dgst -sha256 -sign private_key_file_name.key -out
     binary_file_name.signature binary_file_name
     ```

  5. Create bundle package along with signature
     - Copy `binary_file_name.signature` and `binary_file_name` to linux system.
     - Open terminal and navigate to the folder where both the files are copied.
     - Execute `$ tar -czf binary_file_name.tar.gz binary_file_name.signature binary_file_name`.

       NOTE: Note: `Binary_file_name` should be the same as the file name that is used during binary signing in above steps. For example, if the file name is `test.deb`, then execute `$ tar -czf test.tar.gz test.signature test.deb`.

- Do the following to test offline verification of signature of the signed binary:
  1. To test the binary.

     ```
     openssl x509 -pubkey -noout -in cert_file_name.cer > public_key_file_name.cer
     ```

  2. Verify a binary with signature.

     ```
     openssl dgst -sha256 -verify public_key_file_name.cer -signature
     binary_file_name.signature binary_file_name
     ```

- Continue with the steps to install the created certificate using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Depending on the version of the Dell Hybrid Client software that you have installed on your device, configure the following options:
   a. Expand **Privacy & Security** and click **Certificates**.
   b. Enable **Install Certificate**, browse and upload created one or more self signed certificates. Supported file types are **.crt** and **.cer**.
   c. Click **Save and Publish**.
6. Use the standard application policy or the advanced application policy to deploy the custom-signed application to Dell Hybrid Client.
   For information about how to use the standard application policy or the advanced application policy, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Install an unsigned application

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Depending on the version of the Dell Hybrid Client software that you have installed on your device, configure the following options:
   a. Expand **Privacy & Security** and click **Security Profile**.
      NOTE: To configure the security profile settings, see Configure the security profile settings.
   b. From the **Security Profile** drop-down list, select **Low**.
   c. Click **Save and Publish**.

   NOTE: Use the option with caution as installing unsigned third-party applications may be insecure and can make the device vulnerable to security threats.

6. Use the standard application policy or the advanced application policy to deploy the unsigned application to Dell Hybrid Client.
   When using the advanced application policy, you can place any file in the client drive by selecting the file and using the **Pre install** option. In the script file, mention the source as `/etc/WMSApps`. The destination path is a user-specific directory.

   For information about how to use the standard application policy or the advanced application policy, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

Download files from Wyse Management Suite to local drive

Prerequisites

Security profile must be set us **Low**.

Steps

1. Copy the file and the prescript file to `C:\WMS\LocalRepo\repository\hybridClientApps path`.
2. On Wyse Management Suite, go to **Apps & Data**, and click **Hybrid Client** in the **App Polices** section.
3. Click **Advanced Policy**.
4. Enter the policy name.
5. From the **Group** drop-down list, select your preferred group.
6. From the **Task** drop-down list, select **Install Application**.
7. From the **OS Type** drop-down list, select **Hybrid Client**.
8. Click **Add app** and do the following:
   a. From the **Apps** drop-down list, select the file.
   b. From the **Pre-Install** drop-down list, select the `.sh` file.
   c. Specify the install timeout period.
9. Save and deploy the policy to the device.
10. After successful deployment, open File Explorer on Dell Hybrid Client and verify if the file is available in the Documents folder.

10

Configuring the local device settings

You can configure the local settings on the device using the **Device Settings** menu.

NOTE: Any settings that are configured locally on Dell Hybrid Client take precedence over the settings that were configured using Wyse Management Suite. To customize or have precedence from Wyse Management Suite, the user must click **Reset to Default** from **Device Settings**.

To access the **Device Settings** menu, click the **Show Applications** icon on the desktop screen, and then click **Device Settings**.

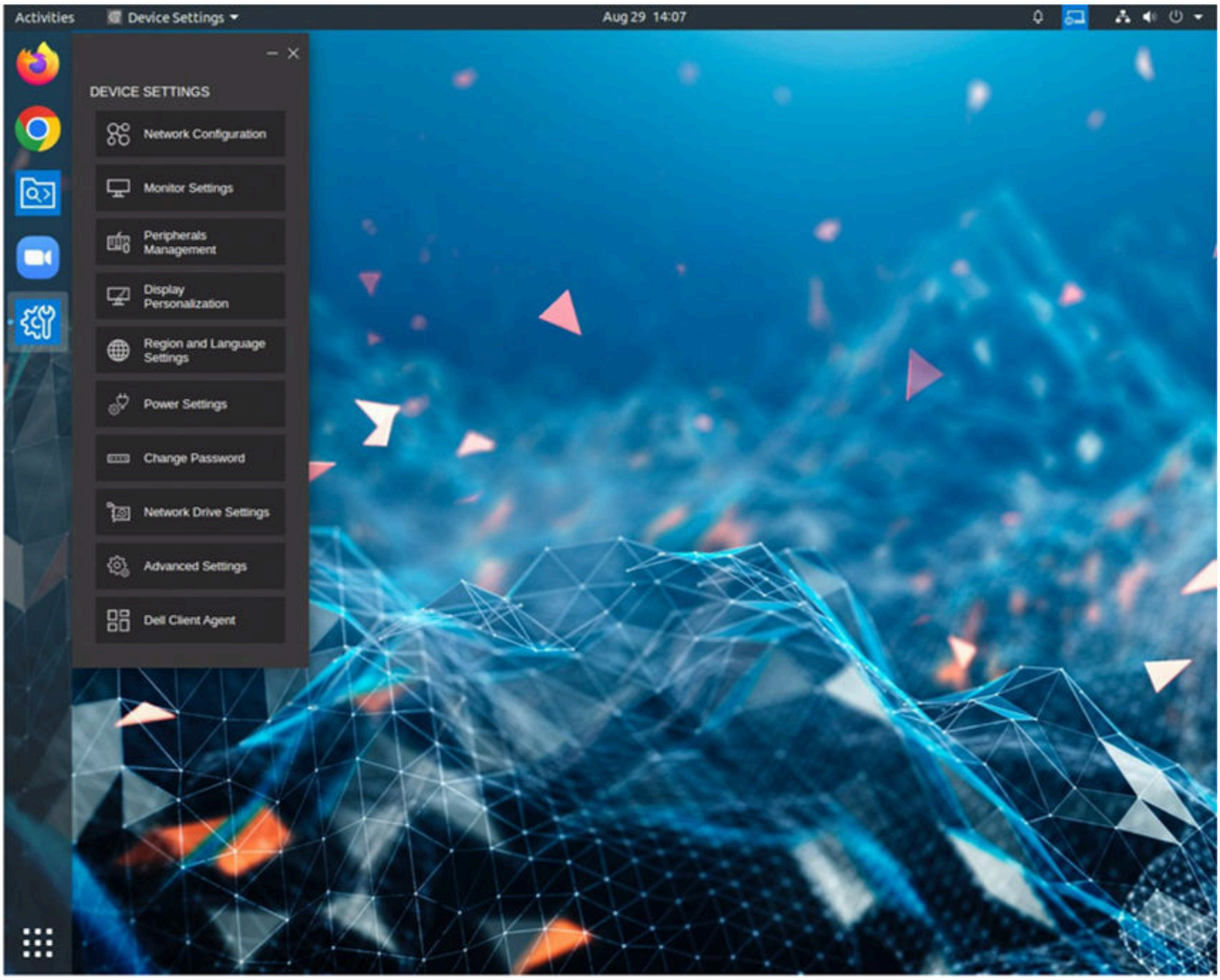


Figure 123. Device Settings

Network

A network drive, also known as network attached storage, is a storage space that is accessible over a network. It allows users to store and share files and folders, providing a centralized storage solution for organizations and individuals.

Dell hybrid client supports various ways to connect and access network drives, including SMB (Server Message Block), FTP (File Transfer Protocol), and CIFS (Common Internet File System.

Network Configuration using Device Settings

Use the **Device Settings** window on Dell Hybrid Client to configure the network settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Network Configuration**.
5. Configure the following network settings based on your requirement:
   - **Bluetooth**—Use this option to configure Bluetooth.

     Click the **Bluetooth** tab, and do the following:

     a. Click the **Advanced** settings.
     b. Click the **ON/OFF** button to enable or disable Bluetooth.
   - **VPN**—Use this option to configure the VPN settings. This option is available from Dell Hybrid Client version 1.5 onwards.

     Click the **VPN** tab, and do the following:

     a. Click the **VPN** toggle switch to enable the VPN connection.
     b. In the **VPN Server URL** field, enter the IP address, hostname, or FQDN of the VPN server.
     c. From the **Protocol** drop-down list, select either **CiscoAnyConnect** or **GlobalProtect** based on your preference.
   - To configure wireless, select **Wi-Fi** from **Network Configuration** > **Advanced Settings** and click your Wi-Fi network from the list of available networks.
6. Close the application.

Network Configuration using Wyse Management Suite

Use the **Wyse Management Suite** on Dell Hybrid Client to configure the network settings.

Steps

1. Log in to **Wyse Management Suite**.
2. Go to the **Groups & Configs** page and select your preferred device group.
3. Click **Edit Polices** > **Dell Hybrid Client 2. x.**
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Network Drives** and click **Network Drives List**.
6. Click on **Add Row** and configure **network drive entry**.
7. Click **Save & Publish**.
   Open **Dell File Explorer** on your device. All the configured network drives are listed under the **External Files** section.

Connect to hidden Wi-Fi networks

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.

4. Go to **Network Configuration** > **Advanced Settings**.
5. Click the three dots at the upper-right corner, and select **Connect to Hidden Network** to enable the option.
6. Select the **Connection Type** as **New**.
7. Enter the network details and click **Connect**.
   If the connection is successful, the name of the connected network is shown in the **Visible Networks** list.

Example

Proxy settings in device settings

User can configure proxy setting using device settings in Dell Hybrid Client 2.5.

User will be able to add or modify proxy details when device is in unregistered state. Proxy details will be grayed out when device is in registered state.

Proxy in Quick Start Wizard

In Dell Hybrid Client 2.5, the user can configure proxy settings from quick start wizard followed which the user can register to Wyse Management Suite. For more information, see Configuring Proxy.

Configuring proxy in device settings

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click **Show Application** icon on the desktop screen.
   The **Application Overview** screen is displayed.
3. Click the **Device Settings** icon .
   The **Device Settings** window is displayed.
4. Go to **Advanced Settings**. Prompt for Authentication add Credential
5. Prompt for **Authentication** and add **Credential**.
6. Go to **Network configuration**> **PROXY** window and add **PROXY** Details
7. Click **Save & Apply**.

Configuring the Display Settings

Use the **Device Settings** window on the Dell Hybrid Client to configure your monitor. You can also configure the display settings using Wyse Management Suite.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Monitor Settings**.
5. Click **IDENTIFY MONITORS** to identify the connected monitors.
6. Click **ADDITIONAL MONITOR SETTINGS** to configure the monitor settings.
7. Click **Displays** tab to configure the following settings:
   - Click **Join Displays** to join the edges of two displays and create a larger display space. This setting is only available when you connect two or more monitors.
   - Click **Mirror** to mirror the content from the primary display to the other connected displays. This setting is only available when you connect two or more monitors.

- Click **Single Display** to have only the selected display activated. This setting is only available when you connect two or more monitors.
- Click the **Orientation** drop-down list to select the orientation.
- Click the **Resolution** drop-down list to select the resolution.
- Click the **Refresh Rate** drop-down list to select the refresh rate.
- Enable the **Adjust for TV** toggle key to resize the display according to a connected TV.
- Click **100%** or **200%** next to **Scale** for scaling the resolution.
- Enable or disable fractional scaling using the **Fractional Scaling** toggle key.

8. Click the Night Light tab to configure the following settings:
   - Enable or disable the night light options using the **Night Light** toggle key.
   - Click the **Schedule** drop-down to choose **Sunset to Sunrise** or **Manual Schedule**.
   - Click **+** or **-** to set **From** and **To** for manually scheduling night light.
   - Use the **Color Temperature** slider to select **Less warm** or **More warm**.
9. Click **Apply**.

   NOTE: To apply display configurations from WMS, disable the monitor settings from Account Privileges to use Single or Multiple display settings.

   NOTE: When you turn off and turn on the monitor during an active VDI session, the session is minimized and you must maximize the session, or close the session and launch back for full screen mode.

Configure the display personalization settings

Use the **Device Settings** window on the Dell Hybrid Client to configure your display personalization settings. Display personalization settings enable you to manage the look and feel of your desktop. You can also configure the display personalization using Wyse Management Suite.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Display Personalization**, and configure the following settings:
   a. From the **Desktop Color** picker, select your desktop color.
   b. Browse and select a wallpaper to change your desktop background. You must place the image files in the **Downloads** or **Pictures** folder.
   c. From the **Wallpaper Mode** drop-down list, select a fit option for your wallpaper.

      NOTE: If you do not upload a wallpaper either using Wyse Management Suite or the Device Settings UI, the Wallpaper Mode must be set to None in order to choose a different desktop color.

   d. Use the **Scale** slider to adjust the wallpaper size.
   e. Use the **Brightness** slider to adjust the desktop brightness.
   f. Use the **Dock Icon Size** slider to adjust the size of the dock icon
   g. From the **Dock Position** drop-down list, select the position for the dock icon.
   h. Click the **Auto Hide Dock** slide switch to automatically hide the dock.
   i. Click **Save & Apply**.

   NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

   NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.

5. Close the application.

Configure the region and language settings

Use the **Device Settings** window on Dell Hybrid Client to configure your region and language settings. You can also configure the region and language settings using Wyse Management Suite.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Region and Language Settings**, and configure the following settings:
   - **Region Settings**—Use this option to configure time zone and time format.

     Click the **Region Settings** tab, and do the following:

     a. Click the **Auto Time Zone** toggle key to ON state to allow the device to automatically update the system time depending on the geographical location.

     NOTE: By default **Auto time zone** is enabled and it sets to current internet timezone if internet is available. If no internet connection is present, by default the time zone is set to **America/New_York**.

     b. If the Auto Time Zone option is disabled, select a time zone from the drop-down list.
     c. Select a **Time Format** from the following options:
        - **12 Hours**
        - **24 Hours**
     d. Click **Save & Apply**.

     NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

     NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.
   - **Time Server Settings**—Use this option to configure the **Time Server Settings** settings.

     Click the **Time Server Settings** tab, and do the following:

     a. In the **Time Server** field, enter the IP addresses or host names of the time server.
     b. Click **Save & Apply**.

     NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

     NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.
   - **Language Settings**—Use this option to configure the **Language** settings.

     Click the **Language Settings** tab, and do the following:
     - From the **Language** drop-down list, select your preferred language. All language packages that are installed using Wyse Management Suite are listed.
     - Click **Save & Apply**.

     NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

     NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.
5. Close the application.

Configure the power settings

Use the **Device Settings** window on Dell Hybrid Client to configure the power settings. You can also configure the power settings using Wyse Management Suite.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** menu is displayed.
4. Click **Power Settings**, and configure the following settings:
   - **Power Saving**—Use this option to configure the **Power Saving** settings.

     Click the **Power Saving** tab, and do the following:

     a. Click the **Enable or Disable WiFi to save power** toggle key to disable WiFi to save power.
     b. Click **Save & Apply**.

     NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

     NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.
   - **Suspend & Power**—Use this option to configure the **Suspend & Power** settings.

     Click the **Suspend & Power** tab, and do the following:

     a. From the **Blank Screen** drop-down list, select the idle time after which the blank screen is to be displayed.
     b. Click the **Auto Suspend** toggle key to enable the device to enter the power state automatically after the specified idle time.
     c. From the **Delay** drop-down list, select the time to wait after a period of inactivity.
     d. From the **Power Button Action**, select the action of the Dell Hybrid Client to be performed after the idle time has elapsed. The following are the available options:
        - **Suspend**
        - **Power Off**
        - **Nothing**
        - **Power off and Restart**—If this option is selected, you must manually log out of your user account.
     e. Click **Save & Apply**.

     NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

     NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.
   - **Power Profile**—Use this option to configure the **Power Profile** settings. This option is available from Dell Hybrid Client version 1.5 onwards.

     Click the **Power Profile** tab, and do the following:

     a. From the **Power Profile** drop-down list, select one of the following options:
        - **Energy Saving**—This mode saves power on your device by reducing system performance.
        - **Balanced**—By default, the Balanced power mode is selected. This mode balances energy consumption and system performance by adapting the processor speed of the device to your activity.
        - **Maximum Performance**—This mode maximizes system performance by running processor at higher speeds.
     b. Click **Save & Apply**.

     NOTE: Use the **Reset to Default** button to reset your settings to default values. Wyse Management Suite configurations are applied if they are published before clicking the **Reset to Default** button. **Reset to Default** resets only the for current page.

     NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.

5. Close the application.

Inactive Timeout

In Dell Hybrid Client 2.5, the user can dynamically configure inactive timeout period from 15 to 300 minutes.

Configuring Inactive Timeout

About this task

This section describes the procedure to configure the inactive timeout using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Power Settings**, and click **Suspend & Power Button**.
6. Enable **Inactivity Action** toggle key .
   Inactive Timeout field will be displayed.
7. User can enter any values between 15 to 300 minutes in **Inactive Timeout** field.

Change the password

Use the **Device Settings** window on the Dell Hybrid Client to change your account password. This option is applicable for all user accounts—local user, domain user, and guest user.

Prerequisites

NOTE: Changing Guest user password only works, when password is already set from Wyse Management Suite.

As a domain user, you must be aware of the Active Directory password complexity policies.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Change Password**.
   The **Change Password** window is displayed.
5. Enter the old password.
6. Enter the new password.

   The minimum password length is nine characters and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. Your password cannot be your username. The password complexity requirement is not applicable for domain users.
7. Confirm the new password.
8. Click **Save & Apply**.

   NOTE: To discard your unsaved changes across the application, click the **Discard Changes** button.

Configure the network drive locally

Use the **Device Settings** window on Dell Hybrid Client to configure the network drive. You can also configure the network drive using Wyse Management Suite.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Network Drive Settings**.
5. To add a network drive, click the **Add** button.
   A network drive entry is created.
6. Click the network drive entry and configure the following options:
   a. Enter the name for the network drive.

      NOTE: The network drive name must be unique across Wyse Management Suite configuration and Device Settings.

   b. Enter the address of the server in the form of URL.
      - If you are using the network share type as SMB/Samba or CIFS, enter the share URL in the format //serverIP/ path. For example, //10x.10x.1x.1xx/test.
      - If you are using the network share type as FTPS, enter the share URL in the format serverIP. For example,10x.10x.1x.1xx. You must preconfigure the certificates if you are setting up FTPS network share.

   c. Select the type of the network share—Smb/Samba, CIFS, or FTPS.
   d. If you want anonymous users to access the network share, click the Anonymous mode toggle key.
   e. If you want specific users to access the network share, disable the Anonymous mode, and specify the username, password, and the domain name.
7. To add multiple network drives, repeat step 5.
8. Click **Save & Apply**.

Next steps

Open Dell File Explorer on your device. All the configured network drives are listed under the **External Files** section.

NOTE: The configured network drives load automatically after user logs in to the device.

Configure the advanced settings

Use the **Advanced Settings** page on Dell Hybrid Client to configure the settings for Troubleshooting, Terminal, SCEP, and Network connection. The **Advanced Settings** page is password-protected and is accessible only after the authentication is successful.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** pane is displayed.
4. Click **Advanced Settings**.
   The **Authentication Required** window is displayed.
5. Enter the System password and click **Authenticate**.
   Upon successful authentication, the **Advanced Settings** screen is displayed.
6. On the **Advanced Settings** screen, configure the following options:
   - **Troubleshooting**—Use this option to troubleshoot your device. See, Configure the troubleshooting options.

- **Terminal**—Use this option to access the terminal window to run root commands using sudo. See, Access the terminal window.
- **SCEP**—Use this option to add a SCEP certificate. See, Configure SCEP locally.
- **Network Configuration**—Use this option to configure the wired and wireless network connection. See, Configure the wired and wireless network settings.

7. Close the application.

   If the system is idle for 5 minutes or the **Advanced Settings** window is closed, Administrator needs to re-authenticate to view the **Advanced Settings** window.

Configure the troubleshooting options

Use the **Troubleshooting** window under Advanced Settings to configure the troubleshooting options. These options allow the IT administrator to diagnose and resolve the device-related issues that may occur during the initial setup.

Steps

1. On the **Advanced Settings** screen, click **Troubleshooting**.
2. Click the **General** tab and do the following:
   - **Export CMOS**—Use this option to extract the CMOS settings and certain BIOS settings to the USB drive, Network share, or the Downloads folder based on your target device selection. This option helps to verify the CMOS settings of the device. Before clicking the option, you must select the destination for export—**Downloads folder**, **USB Drive**, and **Network share**.
   - **Export Logs**—Use this option to export the system log files to the USB drive, Network share, or the Downloads folder based on your target device selection. This option helps to analyze various technical behaviors of the Dell Hybrid Client-powered device. Before clicking the option, you must select the destination for export—**Downloads folder**, **USB Drive**, and **Network share**.
   - **Export WMS settings**—Use this option to export the system log files to the USB drive, Network share, or the Downloads folder based on your target device selection. Use this option to verify the current Wyse Management Suite configurations that are applied to the device. Before clicking the option, you must select the destination for export—**Downloads folder**, **USB Drive**, and **Network share**.
   - **Reset CMOS**—Use this option to reset CMOS to factory default settings.
   - **PrintScreen**—Use the toggle key to enable the Print Screen key on your keyboard. Enabling the Print Screen allows you to take a screenshot of the whole screen.
3. Click the **Ping** tab and do the following:
   a. Enter the IP address, or the DNS-registered hostname of the target.
   b. Specify the packet count.

      NOTE: By default, the ping count range is set to 25.

   c. Click **Start**.
      The data area displays the ping response messages. The ping command sends one echo request per second, calculates round-trip times and packet loss statistics, and displays a brief summary upon completing the calculation. If the host is operational and on the network, it responds to the echo request. By default, echo requests are sent until interrupted by clicking Stop.
4. Click the **Traceroute** tab and do the following:
   a. Enter the IP address, or the DNS-registered hostname of the target.
   b. Click **Start**.
      The data area displays round-trip response time and identifying information for each device in the path. The tracert utility traces the path from your device to a network host. The host parameter is either a valid hostname or an IP address. The tracert utility sends out a packet of information three times to each device in the path. The round-trip response time and the identifier information are displayed in the message box.
5. Click the **Trace** tab and do the following:
   - **Network Packets**—Use this option to capture the network-related logs. Before clicking the option, you must select the destination for export—**Downloads folder**, **USB Drive**, and **Network share**. To start logging the unexpected error messages, click **Start**. Only .pcap file format is supported.
   - **USB Packets**—Use this option to capture the USB packets. Before clicking the option, you must select the destination for export—**Downloads folder**, **USB Drive**, and **Network share**. To start logging the unexpected error messages, click **Start**. Only .pcap file format is supported.
6. Click the **Core Dump** tab and do the following:

a. Select a specific process from the list of processes.
b. Select the destination for export—**USB drive** or **Network share**.
c. Click **Export** if you want to export core dump logs.
d. Click **Export Crash Dump** if you want to export crash dump logs.

NOTE: If crash files are available in the `/var/crash` location, you can export the crash dump to a target device. If crash files are not available, a notification stating that no crash files are present is displayed when you click the export crash dump option.

7. Close the window.

Access the terminal window

Steps

1. On the **Advanced Settings** screen, click **Terminal**.
   A security warning is displayed.
2. Read the security warning and click **Yes**.
   The terminal window is launched.

   NOTE: If the system is idle for 5 minutes, the terminal window is hidden. Administrator needs to reauthenticate to view the terminal.

   By default there is no user with sudo privileges in the system. Only after the terminal window is opened, the admin user is enabled with sudo permissions. If the terminal window is closed or if you log in to the device again, the admin user access is disabled.

   The admin password can be determined as per the device compliance status.

   - If the device is compliant, the admin password is same as the System Password that is set from Wyse Management Suite.
   - If the device is non-compliant, the admin password is same as the randomized password that can be generated from Wyse Management Suite. The randomized password is based on the serial number and UUID of the device. For more information about how to generate the System password, see Generate the default System password.

How to launch the terminal shortcut

You can launch the terminal shortcut on the device or single application mode.

Terminal Shortcut on the Device

This section provides the steps to launch the terminal shortcut on the device.

Steps

1. Press **ctrl + alt + T** on the keyboard.
   Authentication window is displayed.

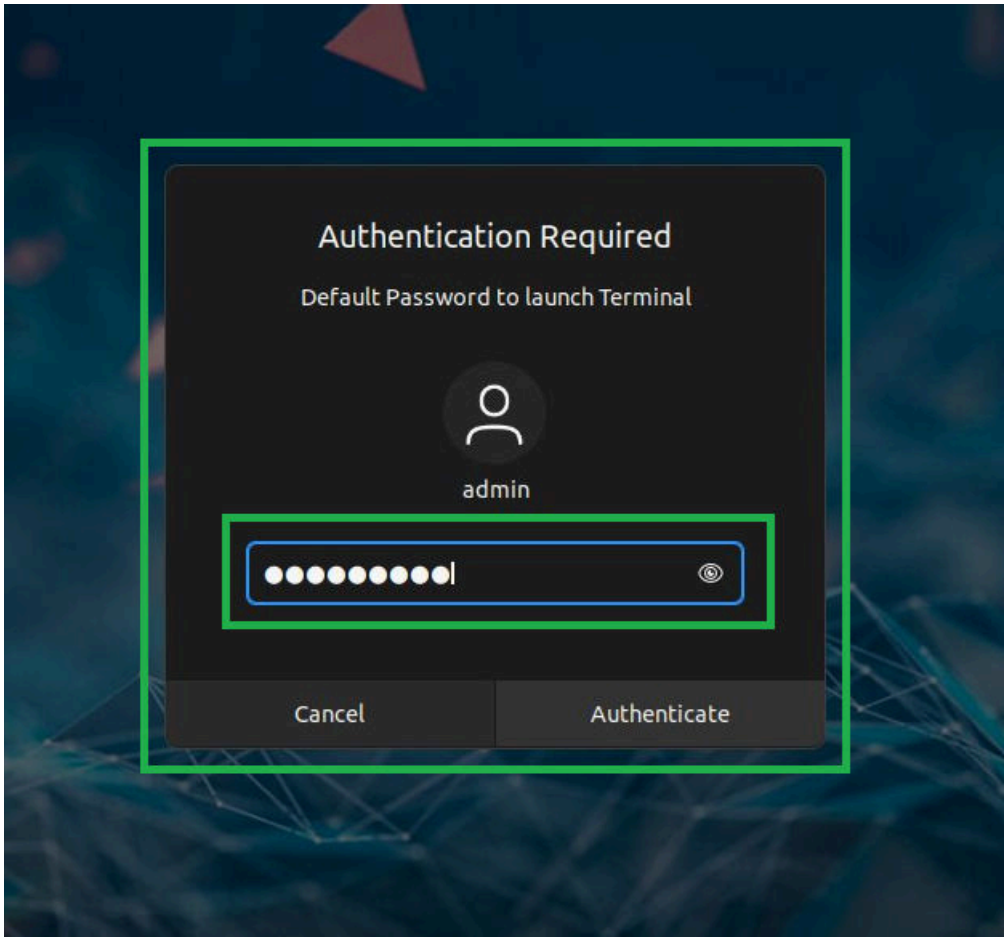


Figure 124. Authentication Required

2. Enter the **password** and click **Authenticate**.
   Terminal Shortcut window is displayed.

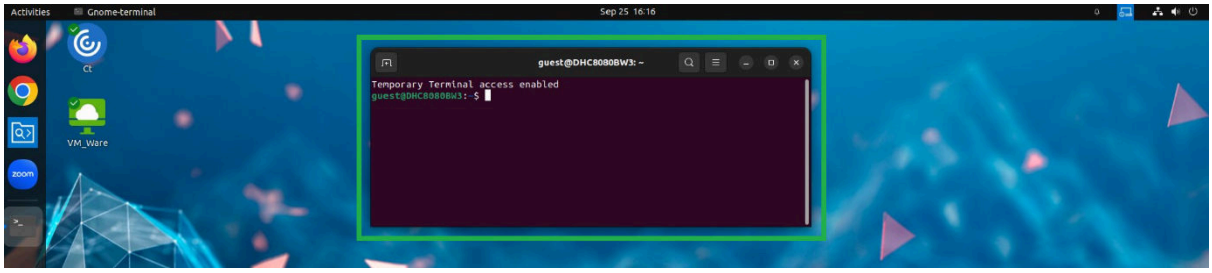


Figure 125. Terminal Shortcut

Terminal Shortcut on the Single Application Mode

This section provides the steps to launch the terminal shortcut on the single application mode.

Steps

1. Log in to Wyse Management Suite using your administrator credentials.
2. Go to **Groups & Configs** > **Edit Policies** > **Dell Hybrid Client 2.x configuration** > **Advanced** tab.
3. Go to **Privacy & Security** and click **Account Privileges**. Enable a single application mode and select any application.

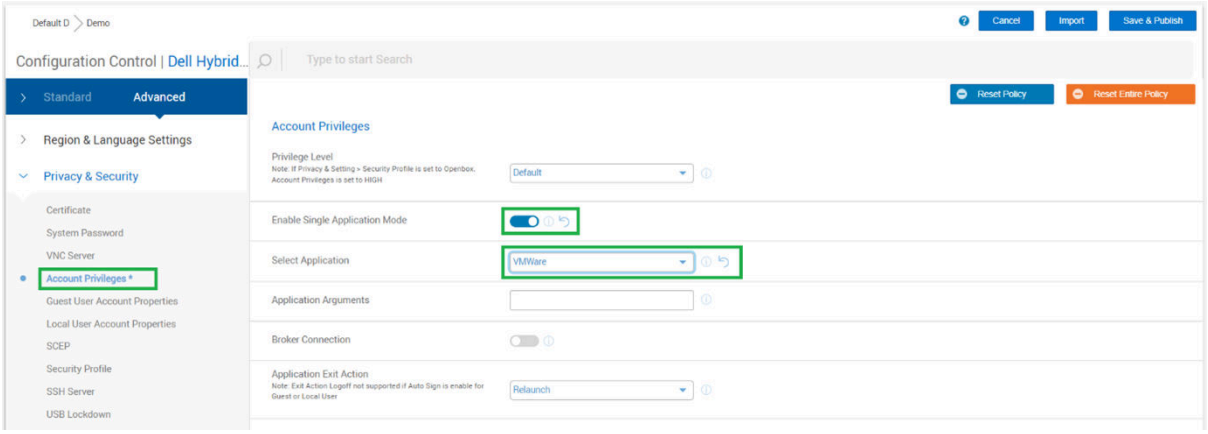


Figure 126. Account Privileges

4. Log off from the device and login back to single application mode.

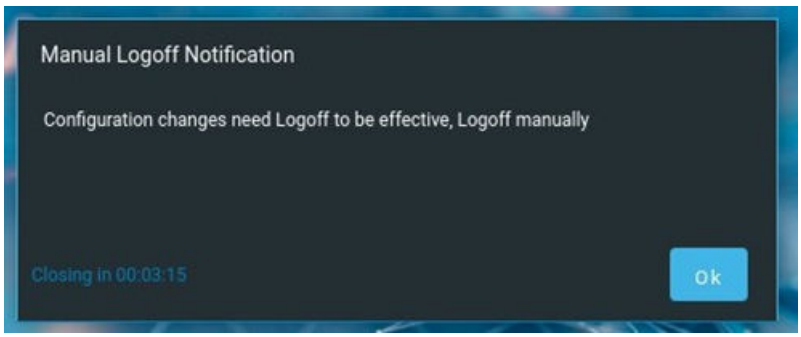


Figure 127. Manual Logoff Notification

5. Press **ctrl + alt + T** on keyboard.
   Authentication window is displayed.

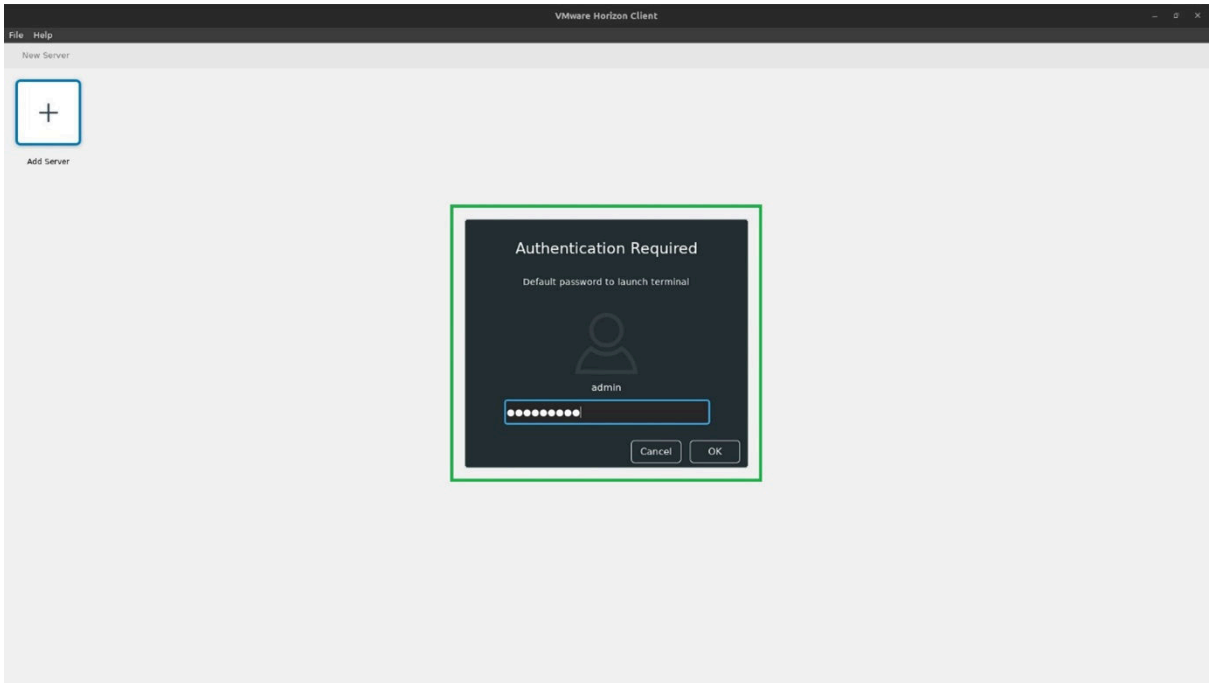


Figure 128. Authentication Required

6. Enter the **system password** and click **OK**.
   Terminal shortcut window is displayed.

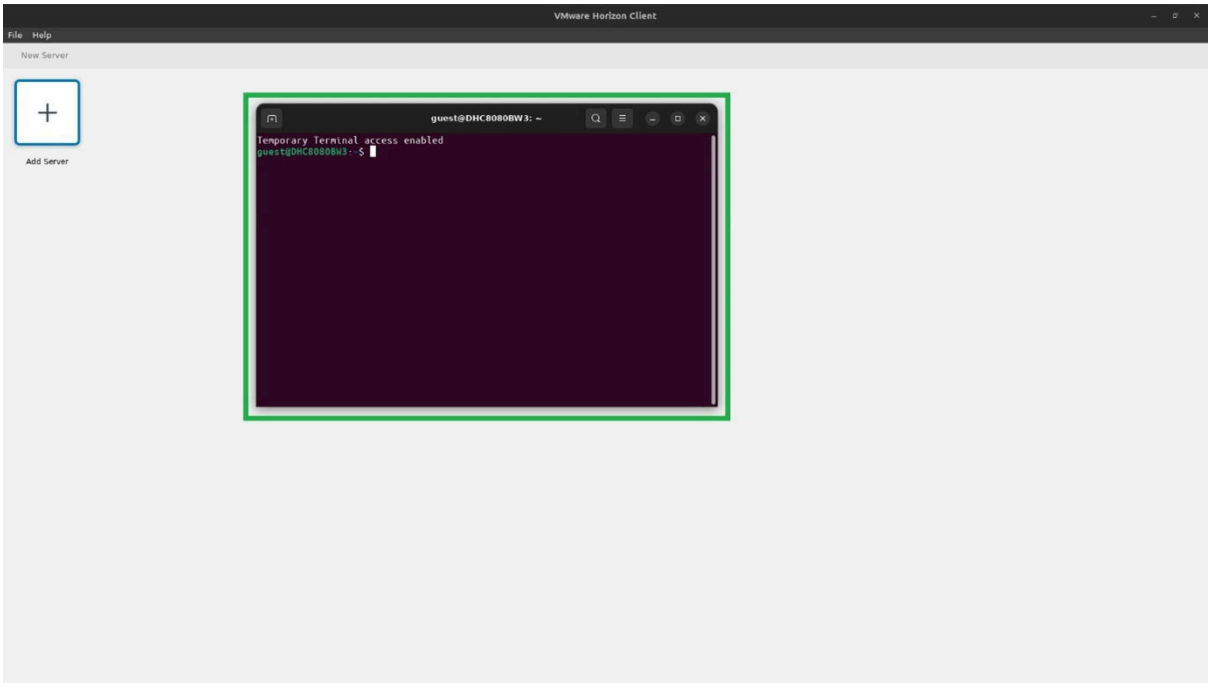


Figure 129. Terminal Shortcut

Configure SCEP locally

Use the **SCEP** window under Advanced Settings to configure the SCEP options. These options can be used in scenarios where a one time password needs to be set or a policy such as password expires in 10 minutes must be configured.

Steps

1. On the **Advanced Settings** screen, click **SCEP**.
2. To enroll a certificate, click the **Add** button.
   A SCEP entry is created.
3. Click the SCEP entry and specify the following details:
   a. Enter the certificate name.

      NOTE: The certificate name must be unique across Wyse Management Suite configuration and Device Settings.

      NOTE: SCEP can be configured with device serial number as SCEP certificate name. The special characters that can be used for this are **$SN** and **$sn**. These special characters can be used in 802 configuration also as SCEP certificate name.

   b. Select the authentication mode.
   c. Enter the SCEP URL.
   d. Enter the Challenge Password.
4. To add multiple certificates, repeat step 2.
5. Click **Save & Apply**.

Configure the wired and wireless Advanced Network Settings

Steps

1. On the **Advanced Settings** screen, click **Network Configuration**.

2. Click the **Ethernet** tab and configure the following options for a wired connection:
   - **Auto**—If you configure the Ethernet settings through the DHCP options, the **Auto** toggle key is turned on.
   - **Manual**—If your device is not connected to any network, you can manually create an Ethernet connection.

     To create an Ethernet connection manually, configure the following options:

     - Click the **Manual** toggle key to enable the manual method.
     - From the **IPv4 Method** drop-down list, select the type of IPv4 configuration.
     - Enter the IP address of the DNS server in the **IPv4 DNS** field.
     - Enter the domain for DNS lookups in the **IPv4 DNS** search field.
     - Click the **IPv4 Ignore Auto DNS** toggle key to ignore the automatically configured DNS.
     - Enter the IP route in the **IPv4 Routes** field.
     - Click the **IPv4 Ignore Auto Routes** toggle key to ignore the automatically configured routes.
     - Enter the IP address of the connection in the **IPv4 ip4** field.
     - Enter the default Gateway in the **IPv4 gw4** field.
     - Enter the network mask in the **IPv4 Netmask** field.
     - Enter the size of the Maximum Transmission Unit in the **MTU** field.
3. Click the **Wireless** tab and configure the options for a wireless connection. This option is available only if the device is connected to WiFi. The wireless network name (SSID) is automatically displayed upon successful connection.
   a. Enter the IP address of the DNS server in the **IPv4 DNS** field.
   b. Click the **IPv4 Ignore Auto DNS** toggle key to ignore the automatically configured DNS.
4. Click **Save & Apply**.

Configure the Dell Client Agent (DCA) settings manually

Use the **Device Settings** window to configure Dell Client Agent (DCA) setting that enables you to manually register your Dell Hybrid Client to Wyse Management Suite.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Dell Client Agent** and the **Authentication Required** window is displayed.
5. Enter the system password and click **Authenticate**.

   The initial password is the serial number of that particular device. You can access the device serial number from the System Information window. If the device is registered to Wyse Management Suite, the Dell Client Agent password is based on the device compliant status.

   - If the device is compliant, the Dell Client Agent password is same as the system password that is set from Wyse Management Suite.
   - If the device is non-compliant, the Dell Client Agent password is same as the randomized password that is generated using Wyse Management Suite. The randomized password is based on Serial Number and UUID of the device. For more information about how to generate the system password, see Generate the default system password.

   NOTE: If the device is unregistered from Wyse Management Suite, the Dell Client Agent password is same as the device serial number.

   Upon successful authentication, the **Dell Client Agent** window is displayed.
6. Click **Registration**, and do the following:
   a. To register manually, click the **Cancel** button. The default status is displayed as **Discovery In Progress**.
   b. In the **WMS Server** field, enter the URL of Wyse Management Suite server.
   c. In the **Group Token** field, enter your group registration key. The Group Token is a unique key for registering your devices to Groups directly.

NOTE: If the tenant and group are empty, the device is registered to the unmanaged group. However, the group token is mandatory for registering the device to a public cloud.

d. Click the **ON/OFF** button to enable or disable the **Validate Server Certificate CA** option. Enable this option to perform server certificate validation for all device-to-server communication.

   If a public cloud URL is entered, the CA Validation option is enabled automatically and cannot be disabled.

e. Click **Register** to register your device powered by Dell Hybrid Client on the Wyse Management Suite server.

   When your device is successfully registered, the status is displayed as **Registered** with the green color tick next to the **Registration Status** label. The caption of the **Register** button changes to **Unregister**. A notification that is relevant to the current activity is displayed on the screen.

7. Click **Support**, and enable the **Support Mode** option for troubleshooting purposes. This option can be enabled by an administrator from Wyse Management Suite.
8. Click **About** to view the version of the Dell Client Agent.
9. Close the application.

   If the system is idle for 5 minutes, the **Dell Client Agent** window is closed. Administrator needs to re-authenticate to view the **Dell Client Agent** window.

10. Dell Client Agent UI Enhancements
    - Dell Client Agent (DCA) improved server URL validation and added capability to detect invalid IP address.
    - Added **Notification server status** in registration section to check MQTT status.
    - Added **Event logs** under support section.
    - Added support to perform live debugging for Dell Client Agent through Event logs.

11

Configuring the Cloud environment

In cloud-based computing, you can access web applications and services that run on remote servers using the Internet. Dell Hybrid Client enables you to access cloud applications and cloud drives seamlessly.

Dell Hybrid Client supports the following cloud applications:

- **Azure Office 365**
- **Google Workspace (formerly G Suite)**

Dell Hybrid Client supports the following cloud storage:

- **OneDrive**—Supports both enterprise and personal OneDrive accounts.
- **Google Drive**—Supports both enterprise and personal OneDrive accounts*. Personal cloud accounts are supported.
- **Box Drive**—Supports only personal Box accounts.

NOTE: OneDrive access is supported only when setting up the Office 365 configuration. If Office 365 is not configured, you cannot access OneDrive from File Explorer. However, you can access OneDrive directly from the web browser.

NOTE: You can use the same user account and configure multiple cloud providers—Azure, GCP, and Box.

Offline mode—Cloud files can be made available in offline mode using File Explorer, where user can use the file when network is not available. For more information, see Using Dell File Explorer and Save cloud files for offline use.

Single Sign-On (SSO) to cloud applications

Dell Hybrid Client supports Single Sign-On (SSO) to cloud applications and web applications. It enables you to log in only one time with one set of credentials to get access to all your applications. You can seamlessly launch the cloud application after logging in as a domain user without entering the credentials again.

- **Azure SSO**—Dell Hybrid Client supports SSO for Azure.
- **Google Workspace SSO**—Dell Hybrid Client supports SSO for Google Workspace (formerly G Suite) using Active Directory Federation Services (ADFS) authentication.

Multifactor authentication for cloud applications

Dell Hybrid Client supports multifactor authentication for Azure Single Sign-on (SSO) using a smart card PIN. This option enables you to log in to the device using a smart card PIN and then seamlessly access the Cloud storage without entering the credentials again.

Azure AD supports smart card login with on-premises Active Directory Federation Services (ADFS) and Active Directory.

To use the multifactor authentication feature for cloud applications, you must do the following:

- Ensure that you have set up the on-premises ADFS server. For information about how to configure the ADFS server, see the *Azure documentation* at https://docs.microsoft.com.
- Ensure that you have configured the on-premises AD and specified the ADFS URL using Wyse Management Suite. For information about how to configure the Azure AD settings using Wyse Management Suite, see Connect to Azure.
- Ensure that you have configured the PIN on your smart card. For information about how to configure the PIN for your smart card, see the smart card product documentation on the respective vendor websites.
- Ensure that you have installed the required smart card certificates on Dell Hybrid Client. For information about how to install a certificate using Wyse Management Suite, see Install a certificate.

Example:

1. Specify the ADFS server URL using Wyse Management Suite.
2. Connect a smart card reader to the device powered by Dell Hybrid Client.
3. Tap your smart card on the smart card reader.
4. Enter the smart card PIN to authenticate the user.

Upon successful authentication, you can directly access the cloud storage from the Dell File Explorer utility on Dell Hybrid Client.

NOTE: Google Cloud does not support Multifactor authentication using a smart card.

File Affiliation

File Affiliation is a distinct setting within the Dell Hybrid Client, in which you can restrict the user's ability to access files depending on the mode that is active. Use Wyse Management Suite to configure the File Afflilation settings. This feature is applicable to both device policy groups and user policy groups.

- **Cloud mode**—In the Cloud mode, the client shows applications that are supported by Cloud services.
- **Local mode**—In the Local mode, the client shows the local applications that are installed and configured using Wyse Management Suite.
- **VDI mode**—In the VDI mode, the client shows VDI-published applications.

  NOTE: File Affiliation is not supported for Azure Virtual Desktop, Imprivata connections.

In the offline mode, the system shows the tools and applications that operate on the cached files. On the same device, you can configure different modes for different users using User Policy Groups.

You can enable one of the following modes using Wyse Management Suite:

- **Cloud**
- **Cloud + Local**
- **VDI**
- **VDI + Local**
- **Cloud + VDI + Local**

The **Open with** function is supported. This feature enables end-users to open a file in Dell File Explorer as per configuration that is set from Wyse Management Suite for file affiliation. See, Using Dell File Explorer.

NOTE: If File Affiliation is undefined, the file opens locally provided the local mapping is valid. If the local mapping is not available, you cannot open the application and an error message is displayed.

Configure the Cloud + Local Mode

Use the Cloud + Local Mode to open all your files either on the cloud or the local system.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select **Cloud + Local**.
7. Select a priority, either **Cloud** or **Local**.

   If the priority is set to **Cloud**, files open on the cloud. If cloud is not configured, files open on the local system.

   If the priority is set to **Local**, files check the local mapping first. If the local mapping is valid, file opens with the local application.

8. For the cloud environment, select the cloud service provider from the following options:
   - **Azure**—Select **Azure** and do the following:
     a. Enter the Azure Client ID.
     b. Enter the Azure Tenant Name.
     c. Enter the Azure Client Secret.
     d. Browse and select the icon for Cloud Home. If you do not configure this option, the default icon is used.

     For more information about connecting to the Azure Active Directory, see Connect to Azure Active Directory.

For more information about creating browser shortcuts for files, see Create shortcuts for cloud files.

- **GCP**—Select **Azure** and do the following:
  a. Enter the GCP Client ID.
  b. Enter the GCP Client Secret.
  c. Browse and select the icon for Cloud Home. If you do not configure this option, the default icon is used.

  For more information about connecting to the G Suite, see Connect to G Suite.

  For more information about creating browser shortcuts for files, see Create shortcuts for cloud files.

- **Box**—Select **Box (Personal storage)** and do the following:
  - Enter the Box Client ID.
  - Enter the Box Client Secret.

  For more information about connecting to Box cloud drive, see Connect to the Box cloud drive.

  NOTE: Box account is a personal cloud storage without any associated applications. If the Box account is configured along with an Azure or GCP corporate account, we can launch local files using Azure or GCP corporate account but you cannot launch the local files with Box cloud directly. This can be done by uploading the local file to Box cloud and opening the file using the respective personal Box account.

9. Log in to Dell Hybrid Client.
10. Double-click a file.

    The file opens on the cloud or the local system based on the priority defined. If there is no network (offline), the file opens on the local system provided the local mapping is valid. If local mapping is not available, you cannot open the file and an error message is displayed.

Example

- **Open a Microsoft PowerPoint using Azure cloud**
  1. Configure the **Cloud + Local** mode for File Affiliation using Wyse Management Suite. The priority is set to Azure Cloud.
  2. Log in to the client.

     You are automatically logged in to Azure with SSO authentication.

  3. Go to the File Explorer.
  4. Open the Microsoft PowerPoint file.

     The file is launched from the cloud application. If there is no network, the file opens with the local application.

- **Open a Microsoft PowerPoint using Google cloud**
  1. Configure the **Cloud + Local** mode for File Affiliation using Wyse Management Suite. The priority is set to GCP Cloud.
  2. Log in to the client.
  3. Go to the File Explorer.
  4. Open the Microsoft PowerPoint file.

     The GCP authentication screen is displayed.

  5. Enter the login credentials.

     After the successful authentication, the file is launched from the GCP webapp. If there is no network, the file opens with the local application.

Configure the VDI Mode

Use the VDI Mode to enable all your files to open only in the VDI environment.

Prerequisites

Ensure that you have configured the File Type Association settings for the respective VDI connections using Wyse Management Suite. For more information about how to configure the File Type Association settings, see File Type Association.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select **VDI**.

   For more information about configuring the VDI environment, see Configuring the VDI environment.
7. Log in to Dell Hybrid Client.
8. Double-click a file.
   The file opens within the VDI environment. If there is no network (offline) or mapping is not available in the VDI database, you cannot open the file and an error message is displayed.

Example

Open a Microsoft Excel file using VDI application

1. Configure the File Type Association `.xls` for the VDI connection using Wyse Management Suite.
2. Configure the **VDI** mode for File Affiliation using Wyse Management Suite.
3. Log in to the client.
4. Go to the File Explorer.
5. Open the Excel file.

   The file is launched from the VDI published application. If there is no network, you cannot open the file.

Configure the VDI + Local Mode

Use the VDI + Local Mode to enable all your files to open either in VDI or on the local system.

Prerequisites

Ensure that you have configured the File Type Association settings for the respective VDI connections using Wyse Management Suite. For more information about how to configure the File Type Association settings, see File Type Association.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation**.
6. From the **File Affiliation** drop-down list, select **VDI + Local**.
7. Select a priority, either **VDI** or **Local**.

   If the priority is set to **VDI**, files open within the VDI environment. If VDI is not configured, files open with the local applications.

   If the priority is set to **Local**, files check the local mapping first. If the local mapping is valid, files open with the local applications.

   For more information about configuring the VDI environment, see Configuring the VDI environment.
8. Log in to Dell Hybrid Client.
9. Double-click a file.
   The file opens on the VDI or the local system based on the priority defined. If there is no network (offline) or mapping is not available in the VDI database, the file opens with the local applications. This is applicable only if the local mapping is valid. If local mapping is not available, you cannot open the file and an error message is displayed.

Example

Open a Microsoft Excel file using VDI application

1. Configure the File Type Association `.xls` for the VDI connection using Wyse Management Suite.
2. Configure the **VDI + Local** mode for File Affiliation using Wyse Management Suite. The priority is set to VDI.
3. Log in to the client.

4. Go to the File Explorer.
5. Open the Excel file.

   The file is launched from the VDI published application. If there is no network, the file opens with the local applications.

Configure the Cloud + VDI + Local Mode

Use the Cloud + VDI + Local Mode to enable all your files to open on the cloud, VDI, or with the local applications.

Prerequisites

Ensure that you have configured the File Type Association settings for the respective VDI connections using Wyse Management Suite. For more information about how to configure the File Type Association settings, see File Type Association.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select **Cloud + VDI + Local**.
7. Specify the first priority and the second priority from the respective drop-down lists. By default, first priority is set to **None selected**.

   If **Cloud** is set as the first priority, files open on the cloud. If second priority is defined, files open either in VDI or on the local system based on your selection.

   If **VDI** is set as the first priority, files open within the VDI environment. If second priority is defined, files open either on the cloud or the local system based on your selection.

   If the priority is set to **local**, files check the local mapping first. If the local mapping is valid, files open with the local applications. If second priority is defined, files open either on cloud or in VDI based on your selection.

8. For the cloud environment, select the cloud service provider from the following options:
   - **Azure**—Select **Azure** and do the following:
     a. Enter the Azure Client ID.
     b. Enter the Azure Tenant Name.
     c. Enter the Azure Client Secret.
     d. Browse and select the icon for Cloud Home. If you do not configure this option, the default icon is used.

     For more information about connecting to the Azure Active Directory, see Connect to Azure Active Directory.

     For more information about creating browser shortcuts for files, see Create shortcuts for cloud files.

   - **GCP**—Select **Azure** and do the following:
     a. Enter the GCP Client ID.
     b. Enter the GCP Client Secret.
     c. Browse and select the icon for Cloud Home. If you do not configure this option, the default icon is used.

     For more information about connecting to the G Suite, see Connect to G Suite.

     For more information about creating browser shortcuts for files, see Create shortcuts for cloud files.

   - **Box**—Select **Box (Personal storage)** and do the following:
     - Enter the Box Client ID.
     - Enter the Box Client Secret.

     For more information about connecting to Box cloud drive, see Connect to the Box cloud drive.

9. Log in to Dell Hybrid Client.
10. Click a file.

The file opens on the cloud, VDI, or the local system based on the priority defined. If there is no network (offline) or network mapping is not available in the network database, the file opens with the local applications. This is applicable only if the local mapping is valid. If the local mapping is not available, you cannot open the file and an error message is displayed.

Example

Open a Microsoft Excel file using VDI and other file extensions from cloud or local application:

1. Configure the File Type Association `.xls` for the VDI connection using Wyse Management Suite.
2. Configure the **Cloud + VDI + Local** mode for File Affiliation using Wyse Management Suite. The first priority is set to VDI, and second priority is set to Cloud.
3. Log in to the client.
4. Go to the File Explorer.
5. Open the Excel file.

   The file is launched from the VDI published application. Other file extensions open with cloud application. If the client is unable to connect to VDI, excel file opens in a cloud application. If there is no network, the file is opened with the local applications.

Configure personal accounts for Azure

Dell Hybrid Client enables you to add your personal OneDrive account along with enterprise Azure storage. This feature is supported from Dell Hybrid Client version 1.5 onwards. You can add up to a maximum of five personal accounts.

Prerequisites

Ensure that the **Multitenancy** option is enabled during the initial setup of your cloud provider.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation** and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select one of the following options:
   - **Cloud**
   - **Cloud + Local**
   - **Cloud + VDI + Local**
7. If you have selected **Cloud + Local** or **Cloud + VDI + Local**, select the **Priority** as **Cloud**.
8. From the **Cloud Provider** drop-down list, select **Azure**.
9. Specify the Azure Client ID, Azure Tenant Name, and Azure Client Secret to configure the enterprise Azure storage. For more information about connecting to the Azure Active Directory, Connect to Azure.
10. To enable users to add a personal account for Azure, click the **Add Personal Account** toggle switch.
11. To enable users to add a personal Google Cloud account, click the **Add Personal GCP Account** toggle switch, and do the following:
    a. Enter the GCP Client ID.
    b. Enter the GCP Client Secret.
12. To enable users to add a personal Box account, click the **Add Personal Box Account** toggle switch, and do the following:
    a. Enter the Box Client ID.
    b. Enter the Box Client Secret.
13. Browse and select the icon for Cloud Home. If you do not configure this option, the default icon is used.
14. Click **Save and Publish**.

    NOTE: If you have configured the local option in File Affiliation, and if the network connection is not available, you can access only the cloud files that are saved offline. Use Dell File Explorer to view the offline files.

15. Log in to Dell Hybrid Client.
16. Open **File Explorer**.

17. In the **One Drive** section, click the **Add (+)** button to add your personal account.
18. Enter the credentials to sign in to your personal account.

Configure personal accounts for Google Cloud

Dell Hybrid Client enables you to add your personal OneDrive account along with enterprise Google Cloud storage. This feature is supported from Dell Hybrid Client version 1.5 onwards. You can add up to a maximum of five personal accounts.

Prerequisites

- Ensure that the **Multitenancy** option is enabled during the initial setup of your cloud provider.
- Ensure that you have enabled the Drive Activity API for synchronizing the GCP account. This API must be enabled when you are configuring the GCP account.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation** and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select one of the following options:
   - **Cloud**
   - **Cloud + Local**
   - **Cloud + VDI + Local**
7. If you have selected **Cloud + Local** or **Cloud + VDI + Local**, select the **Priority** as **Cloud**.
8. From the **Cloud Provider** drop-down list, select **GCP**.
9. Specify the GCP Client ID and GCP Client Secret to configure the enterprise Google Cloud storage. For more information about connecting to Google Cloud, see Connect to G Suite.
10. To enable users to add a personal account for Google Cloud, click the **Add Personal Account** toggle switch.
11. To enable users to add a personal Azure account, click the **Add Personal Azure Account** toggle switch, and do the following:
    a. Enter the Azure Client ID.
    b. Enter the Azure Client Secret.
12. To enable users to add a personal Box account, click the **Add Personal Box Account** toggle switch, and do the following:
    a. Enter the Box Client ID.
    b. Enter the Box Client Secret.
13. Browse and select the icon for Cloud Home. If you do not configure this option, the default icon is used.
14. Click **Save and Publish**.
15. Log in to Dell Hybrid Client.
16. Open **File Explorer**.
17. In the **Google Drive** section, click the **Add (+)** button to add your personal account.
18. Enter the credentials to sign in to your personal account.

Connect to Microsoft 365 Apps

Dell Hybrid Client supports only on-prem user sync with Azure AD. Azure Active Directory (Azure AD) is a cloud-based identity and access management service by Microsoft. It enables you to sign in and access both external and internal resources. You can access external resources, such as Microsoft Office 365, the Azure portal, and other SaaS applications. You can access internal resources, such as applications on your corporate network and intranet, along with any cloud applications developed by your organization.

Prerequisites

Ensure that you have an active Azure account. For more information about the Azure Active Directory On-Prem users sync, see the *Azure documentation* at docs.microsoft.com.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select one of the following options:
   - **Cloud**
   - **Cloud+Local**
   - **Cloud+VDI+Local**
7. From the **Cloud Provider** drop-down list, select **Azure**.

   NOTE: You can procure the Azure Client ID, Tenant name, and Client Secret from portal.azure.com. For more information, see the *Azure documentation* at docs.microsoft.com.
8. In the **Azure Client ID** field, enter the ID of the Azure Client.
9. In the **Azure Tenant Name** field, enter the name of the Azure AD tenant.
10. In the **Azure Client Secret** field, enter the secret key of the Azure Client.
11. In the **AD FS URL** field, enter the Active Directory Federated Services (ADFS) URL to enable single sign-on for Azure.
12. To set the icon for Cloud Home, do the following:
    a. Click **Browse** to upload the shortcut icon.
    b. From the **Icon for** drop-down list, select the shortcut icon.

       NOTE: If the **Icon for Cloud Home** option is not configured, the default icon is used.

    You can also create shortcuts for cloud files. For more information, see Create shortcuts for cloud files.
13. Click **Save and Publish**.
14. Log in to Dell Hybrid Client, open **File Explorer**, and click **Azure**.
15. Enter the Azure login credentials.
16. Click either a local file or a cloud file that you want to open.
    The file opens from cloud. If there is no network (offline), cannot open the file and an error message is displayed. However, If you have configured the local option in File Affiliation, and if the network connection is not available, you can access only the cloud files that are saved offline. Use Dell File Explorer to view the offline files.

Connect to Google Workspace Apps

G Suite (formerly Google Apps for Work) is a collection of web applications that are created by Google for your business needs. The Google Workspace account enables you to access several Google applications such as Calendar, Docs, Sheets, Slides, Forms, and more.

Prerequisites

- Ensure that you have an active Google Workspace account. For more information about the Google Workspace features, see the *Google Workspace documentation* at workspace.google.com.
- Ensure that you have enabled the Drive Activity API for synchronizing the GCP account. This API must be enabled when you are configuring the GCP account.

For information about the Cloud Identity help and Google Workspace Admin Help, go to support.google.com.

For information about how to set up Google Cloud for enterprise customers, see the *Enterprise onboarding checklist* at cloud.google.com/docs.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select one of the following options:
   - **Cloud**
   - **Cloud+Local**
   - **Cloud+VDI+Local**
7. From the **Cloud Provider** drop-down list, select **GCP**.

   NOTE: You can procure the Google Client ID and the Client Secret from cloud.google.com. For more information, see the *Google Cloud documentation* at cloud.google.com/iam/docs.
8. In the **GCP Client ID** field, enter the ID of the Google Client ID.
9. In the **GCP Client Secret** field, enter the secret key of the Google Client.
10. In the **AD FS URL** field, enter the Active Directory Federated Services (ADFS) URL to enable single sign-on for Google Cloud.

    The **AD FS URL** option is available from Dell Hybrid Client version 1.5 onwards.
11. Click **Save and Publish**.
12. Log in to Dell Hybrid Client, open **File Explorer**, and click **GCP**.
13. Enter the login credentials.
14. Click the cloud app that you want to open.

Create shortcuts for cloud apps

A desktop shortcut enables you to quickly access your cloud files or applications. Use Wyse Management Suite to create shortcuts for cloud documents, worksheets, presentations, email, and collaboration apps. You can also customize the shortcut icons as per your requirement.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select the cloud option using one of the following modes:
   - **Cloud**
   - **Cloud + Local**
   - **Cloud + VDI + Local**
7. Configure the cloud service provider—**Azure** or **GCP**.
8. Click the **Create shortcut** toggle key for the file or application you want to create a shortcut. The available options are:
   - **Create shortcut for Documents**
   - **Create shortcut for Worksheets**
   - **Create shortcut for Presentations**
   - **Create shortcut for Email**
   - **Create shortcut for Collaboration**. For example, Microsoft Teams.
9. To customize the shortcut icons, do the following:
   a. Click **Browse** to upload the shortcut icon.
   b. From the **Icon for** drop-down list, select the shortcut icon.

10. Click **Save and Publish**.

Connect to Box cloud drive

From Dell Hybrid Client version 1.6 onwards, Box personal storage is supported. Box account is a personal cloud storage without any associated applications. If the Box account is configured along with an Azure or GCP corporate account, we can launch local files using Azure or GCP corporate account but you cannot launch the local files with Box cloud directly. This can be done by uploading the local file to Box cloud and opening the file using the respective personal Box account.

Prerequisites

Ensure that you have an active Box subscription. For more information about the Box drive features, see the *Box documentation* at support.box.com/ and *Guides* at developer.box.com/.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **File Affiliation**, and click **File Affiliation Settings**.
6. From the **File Affiliation** drop-down list, select one of the following options:
   - **Cloud**
   - **Cloud+Local**
   - **Cloud+VDI+Local**
7. From the **Cloud Provider** drop-down list, select **Box (Personal Storage)**.

   NOTE: You can procure the Box Client ID and the Box Client Secret from account.box.com. For more information, see the *Guides* at developer.box.com/.
8. In the **Box Client ID** field, enter the ID of the Box Client ID.
9. In the **Box Client Secret** field, enter the secret key of the Box Client.
10. Click **Save and Publish**.

    NOTE: Dell Hybrid Client supports accessing Box personal account along with Azure and GCP corporate accounts. For more information, see the Configure personal accounts for Azure and Configure personal accounts for Google Gloud.
11. Log in to Dell Hybrid Client, open **File Explorer**, and click the **Box** drive.
12. Enter the login credentials.
    The user must grant access to the drive.
13. Click either a local file or a cloud file that you want to open.
    The file opens with cloud. If there is no network (offline), you cannot open the file and an error message is displayed. However, if you have configured the local option in File Affiliation, and if the network connection is not available, you can access only the cloud files that are saved offline. Use Dell File Explorer to view the offline files.

12

Device security

Security configurations help you to maximize the security posture in your environment. This section describes the mechanisms and methods available to secure the deployment of the Dell Hybrid Client software.

Configure the SSH settings

Using the SSH protocol, you can connect securely to Dell Hybrid Client from a remote device. You can use Wyse Management Suite to configure the SSH settings.

Prerequisites

As an administrator, you must install the optional SSH add-on to enable the SSH access. To install the SSH add-on on Dell Hybrid Client, do the following:

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device or type Dell Hybrid Client.
3. Click the product from search results to open the product support page.
4. On the product support page, click **Drivers & downloads**.
5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the **Ubuntu** operating system. For information about the version of the Ubuntu operating system that is supported in each Dell Hybrid Client release, see Supported operating system.
6. From the list, locate the SSH add-on entry and click the download icon.
7. After the add-on is downloaded successfully, use the application policy on Wyse Management Suite to deploy the add-on to Dell Hybrid Client. Ensure that you upload the downloaded add-on to the local repository on Wyse Management Suite. For more information about how to deploy an application policy, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

   NOTE: If you have configured the Dell Hybrid Client policy settings before the add-on installation, you must reapply the configured settings after you deploy the add-on. Alternatively, you can log off and log back in.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **SSH Server**.
6. Click the **SSH Server** toggle key to enable an SSH connection from a remote device. Use **`sshuser`** as username to establish an SSH connection.
7. Enter a password for the SSH-enabled user.
8. Optionally, you can grant elevated privileges to an SSH-enabled user on the device powered by Dell Hybrid Client. To enable the option, click the **Allow elevated privileges to sshuser** toggle key. If the option is not in use or not required, Dell Technologies recommends keeping the option disabled.

   NOTE: Use the option with caution as granting elevated privileges to an SSH-enabled user may lead to inappropriate use of access on the device.
9. Click **Save and Publish**.

Next steps

1. On a remote device, open the SSH client terminal application.
2. Connect to your Dell Hybrid Client using the username **`sshuser`**. When prompted, enter the password for `sshuser`.

Configure the VNC settings

Dell Hybrid Client can be accessed remotely using VNC. Use Wyse Management Suite to configure the VNC server preferences.

Prerequisites

As an administrator, you must install the VNC optional add-on to enable the VNC access. To install the VNC add-on on Dell Hybrid Client, do the following:

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the model number of your device or type Dell Hybrid Client.
3. Click the product from search results to open the product support page.
4. On the product support page, click **Drivers & downloads**.
5. Depending on the version of Dell Hybrid Client that you have installed on your device, select the **Ubuntu** operating system. For information about the version of the Ubuntu operating system that is supported in each Dell Hybrid Client release, see Supported operating system.
6. From the list, locate the VNC add-on entry and click the download icon.
7. After the add-on is downloaded successfully, use the application policy on Wyse Management Suite to deploy the add-on to Dell Hybrid Client. Ensure that you upload the downloaded add-on to the local repository on Wyse Management Suite. For more information about how to deploy an application policy, see the *Wyse Management Suite Administrator's Guide* at www.dell.com/support.

   NOTE: If you have configured the Dell Hybrid Client policy settings before the add-on installation, you must reapply the configured settings after you deploy the add-on. Alternatively, you can log off and log back in.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **VNC Server**.
6. Click the **VNC Server** toggle key to enable a VNC connection from a remote device.
7. Click the **Warning on VNC access** toggle key if you want to show the VNC access warning at the start of the connection.
8. Click the **Remote access confirmation prompt on session start** toggle key if you want to show the VNC shadowing accept or decline prompt message. If enabled, the confirmation prompt is displayed at the start of the VNC session.
9. Enable the **Password to establish VNC connection** toggle key to show a password prompt when connecting to a remote machine. Dell Technologies recommends that you enable this option to keep your VNC connection secured.

   Remote Access confirmation Prompt on session start and Password to establish VNC connection are enabled by default.
10. Enter a password for the VNC connection.
11. Click **Save and Publish**.

    NOTE: VNC connection works only when the user has logged in to Dell Hybrid Client.

Next steps

1. Start the system on which you want to access VNC.
2. Open the VNC viewer application.
3. Connect to Dell Hybrid Client remotely.

Manage USB devices

Dell Hybrid Client enables you to configure and manage the USB devices that are connected to your device using Wyse Management Suite. You can block access to USB devices, making them inaccessible from the client. This setting cannot be configured from user policy groups.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **USB Lockdown**.
6. In the **USB Lockdown**, configure one of the following options:
   - **Enable all USB devices**—Click the **Enable all** toggle key to enable or disable the option. If this option is enabled, the operating system detects all USB devices that are connected to the device. If this option is disabled, you must enable one of the following options:
     - **Disable all excluding HID**
     - **Disable USB devices using Vendor ID/Product ID**
     - **Disable by USB class**
   - **Disable all excluding HID**—Click the **Disable all excluding HID** toggle key to enable or disable the option. If this option is enabled, the operating system detects only Human Interface Devices (HID) such as keyboard and mouse. If this option is disabled, you must enable one of the following options:
     - **Enable all USB devices**
     - **Disable USB devices using Vendor ID/Product ID**
     - **Disable by USB class**
   - **Disable USB devices using Vendor ID/Product ID**—If the **Enable all** and **Disable all excluding HID** options are disabled, use the **Disable USB devices using Vendor ID/Product ID** feature to block certain USB devices, making them inaccessible from the client. You must specify the Vendor ID (VID) and the Product ID (PID) of the USB devices that you want to disable. To disable a USB device, do the following:
     a. Click **Add Row**.
     b. In the **Vendor ID** field, enter the vendor ID of the USB device.
     c. In the **Product ID** field, enter the product ID of the USB device. This is an optional field.

     For example, `vvvv:pppp`, where `vvvv` is the device vendor ID and `pppp` is the device product ID.
   - **Disable by USB class**—If the **Enable all** and **Disable all excluding HID** options are disabled, you can disable the USB devices by USB class. From the **USB classes to be disabled** drop-down list, select one or more USB classes.
7. Click **Save & Publish**.
8. Log in to the Dell Hybrid Client and connect a USB drive.
   If you have enabled the USB drive, the operating system detects the USB drive that is connected to the client. If you have disabled the USB drive, the operating system cannot detect the USB drive that is connected to the client.

User data encryption using ZFS file system

Dell Hybrid Client is designed to protect a domain user's data such as user files, user database, and user application details. Dell Hybrid Client uses the ZFS file system to encrypt the user home directory. Each user home directory is encrypted with an autogenerated passphrase. When a user logs in to the device, the user home directory of the user is automatically mounted by ZFS. When the user logs out of the device, the user home directory is unmounted by ZFS.

ZFS uses a storage pool that is called Zpool for storing data on a single device. A user quota is defined to limit the amount of disk space that is available to a file system or home directory of a particular user.

- **User quota and Zpool dynamic expansion**—The size of the storage pool and user quota are increased automatically as more user files or directories are added. For example, When a user copies files larger than the allocated user quota, first the size of the user quota is dynamically increased to accommodate the data. A notification is displayed on the Dell Hybrid Client screen to indicate that the user quota has increased. If the user quota expansion reaches the threshold limit of the entire

storage pool, the Zpool is dynamically increased to accommodate the user quota expansion. A notification is displayed on the Dell Hybrid Client screen to indicate that the zpool has increased.

- **User quota dynamic contraction**—The size of the user quota is decreased automatically as more user files are removed. For example, When a user deletes large amount of files, the size of the user quota is dynamically decreased to free up the disk space. A notification is displayed on the Dell Hybrid Client screen to indicate that the user quota has decreased.

For more information about the ZFS file system, see the *Ubuntu documentation* at ubuntu.com.

User data cleanup

As an administrator, you can use Wyse Management Suite to clear user data of a particular user.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Devices** page and locate your device that is powered by Dell Hybrid Client.
3. Click the device name.
   The **Device Details** page is displayed.
4. From the **More Actions** drop-down list, click **Clear User(s) Data**.
   An alert window is displayed.
5. Enter the name of the user.
6. Click **Send Command**.
   The user home directory is deleted from the storage pool.

Configure the security profile settings

Dell Hybrid Client enables you to set **Security Profiles** to provide an enhanced device security for deploying unsigned third-party applications.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred device group.

   NOTE: The security profile option is applicable only for Device Policy Groups.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security** and click **Security Profile**.
6. From the **Security Profile** drop-down list, select one of the following options:
   - **High**—This profile enables you to install Dell-signed, custom-signed, and unsigned Debian files with metadata. Based on the metadata, the firejail is applied.

     NOTE: The firewall and Kernel hardening features are enabled.
   - **Medium**—This profile enables you to install the following types of third-party application packages or files:
     - Dell-signed Debian files
     - Custom-signed Debian files

       NOTE: Before you install a custom-signed Debian package, you must upload the corresponding certificate by using Wyse Management Suite.
     - Unsigned Debian files with or without metadata

     NOTE: The firewall and Kernel hardening features are disabled. If metadata is available, the default firejail profile is enabled. If metadata is not available, and if the desktop file of the application is available in `/usr/share/application` location, the default firejail profile is enabled. If metadata is not available, and if the desktop file of the application is not available in `/usr/share/application` location, the default firejail profile is disabled. For more information about how to configure the application metadata for firejail profile, see Configuring metadata for firejail profiles.

- **Low**—This profile enables you to install all types of file extensions, such as, TAR, Debian, Bundle, Python script, Shell script, Javascript, Image file extensions, and VLC extensions.

  NOTE: The firewall and Kernel hardening features are disabled. Both default and custom firejail profiles are disabled.

- **Openbox**—This profile enables you to install all types of files extensions, such as Debian, Bundle, Python script, Shell script, Javascript, Image file extensions, and VLC extensions without any security restrictions. Enabling this profile permits the full use of the Linux operating system on the device that is registered to Wyse Management Suite.

  All the default applications including Nautilus are available in this mode along with the snapd service, audio selection dialogue, and the logged in user list. Developer tools for browsers and profile manager for Firefox browser are enabled.

  Dell Hybrid Client components such as Dell File explorer and Device Settings are also available for the logged-in users.

  NOTE: The firewall and Kernel hardening features are disabled. Both default and custom firejail profiles are disabled.

  NOTE: Once the open box mode is selected, you cannot enable **High**, **Medium**, or **Low** modes again.

For more information about security profiles, see the *Dell Hybrid Client 2.x Security Configuration Guide* at www.dell.com/support.

NOTE: In all the security profiles, both Dell-signed and custom-signed—with signature verified in medium and high profiles) (debian and bundle) applications are allowed for installation.

7. If you select the **Security Profile** as **Medium**, browse and select the application certificate.
8. If you select the **Security Profile** as **High**, do the following:
   a. Browse and select the application certificate.
   b. Specify a port number or a range of port numbers in a Comma-Separated Value (CSV) format.
9. Click **Save & Publish**.

Configuring metadata for Firejail profiles

To configure the Firejail profile in **Medium** and **High** security modes, the administrator must add the metadata along with the application package. Depending on the application that needs to be installed, you must modify the metadata, create a JSON file, and then bundle the file along with the Debian package of the application. The bundled package can be deployed to Dell Hybrid Client using Wyse Management Suite.

Use this metadata if you do not want to set granular parameters for the application. The following is an example of the metadata json file for the VLC application:

```
{
  "application": "vlc",
  "applicationType": "external",
  "appVersion": "1.3.00.16851",
  "autoUpdate": true,
  "osType": "HybridClient",
  "osSubType": [
      "Ubuntu 20.04 Desktop"
  ],
  "installerParameters": "",
  "userPromptTimeOut": "2",
  "applicationinstallationTimeOut": "60",
  "filecheckSum": "63xxxxxxxxxxxxxxxxxxxx",
  "dependencies": "",
  "securityConfigSettings": {
     "firejailProfileSettings": {
         "version": "0.9.62",
         "values": [
             {
                 "executableFullPath": "/usr/bin/vlc",
                 "executableDesktopFilePath": "/usr/share/applications/vlc.desktop",
                 "highSecurityGranularSettings": {
                     "blockCriticalAccess": "Yes",
                     "enableRestrictedUserEnvironment": "Yes",
                     "enableRestrictedCommunicationAccess": "Yes",
                     "enableRestrictedFSAccess": "No"
                 }
             },
             {
```

```
                    "executableFullPath": "/usr/bin/vlc_support",
                    "executableDesktopFilePath": "/usr/share/applications/
vlc_support.desktop",
                    "highSecurityGranularSettings": {
                        "blockCriticalAccess": "No",
                        "enableRestrictedUserEnvironment": "Yes",
                        "enableRestrictedCommunicationAccess": "No",
                        "enableRestrictedFSAccess": "No"
                    }
                }
            ]
        }
    }
}
```

NOTE: If the application metadata namely `executableFullPath` and `executableDesktopFilePath` are not available for a given application, you cannot install that application in the **High** security profile.

Use this metadata to set granular parameters for the application. The following is an example of the metadata json file with granular settings for the VLC application:

```
{
  "application": "vlc",
  "applicationType": "external",
  "appVersion": "1.3.00.16851",
  "autoUpdate": true,
  "osType": "HybridClient",
  "osSubType": [
     "Ubuntu 20.04 Desktop"
  ],
  "installerParameters": "",
  "userPromptTimeOut": "2",
  "applicationinstallationTimeOut": "60",
  "filecheckSum": "63xxxxxxxxxxxxxxxxxxxxxxx",
  "dependencies": "",
  "securityConfigSettings": {
      "firejailProfileSettings": {
          "Version":"0.9.62",
          "values": [
              {
                  "executableFullPath": "/usr/bin/vlc",
                  "executableDesktopFilePath": "/usr/share/applications/vlc.desktop",
                  "highSecurityGranularSettings": {
                      "blockCriticalAccess": {
                      "blockSensitiveFileAccess":"Yes",
                      "blockDevelopmentToolsAcces":"No",
                      "blockExecuteAccess":"No",
                      "blockInterpreterToolsAccess":"No",
                      "blockPasswordManagerAccess":"Yes",
                      "blockConfigFilesAccess":"Yes"
                  },
                  "enableRestrictedUserEnvironment": {
                      "enableNewIPCNamespace":"No",
                      "disabl3dHwAccl":"No",
                      "disableDvd":"No",
                      "disableSupplementryGroups":"No",
                      "disableSound":"Yes",
                      "disableTv":"No",
                      "disableU2f":"No",
                      "disableVideo":"No",
                      "disableUserShell":"Yes"
                  },
                  "enableRestrictedCommunicationAccess":  {
                      "enableMachineIdSpoofing":"No",
                      "blockNetworkAccess":"No",
                      "enableFirewallForNewNW":"Yes",
                      "disableDbusAccess":"No"
                  },
                  "enableRestrictedFSAccess": {
                      "enableFileAccessAudit":"No",
                      "disableMount":"No",
```

```
                        "enablePrivateMode":"No",
                        "enablePrivateCache":"No",
                        "enablePrivateDev":"Yes",
                        "enablePrivateLibDirectory":"No",
                        "enablePrivateTmpFs":"No"
                    }
                }
            },
            {
                "executableFullPath": "/usr/bin/vlc_support",
                "executableDesktopFilePath": "/usr/share/applications/
vlc_support.desktop",
                "highSecurityGranularSettings": {
                    "blockCriticalAccess": {
                        "blockSensitiveFileAccess":"Yes",
                        "blockDevelopmentToolsAcces":"No",
                        "blockExecuteAccess":"Yes",
                        "blockInterpreterToolsAccess":"No",
                        "blockPasswordManagerAccess":"Yes",
                        "blockConfigFilesAccess":"Yes"
                    },
                    "enableRestrictedUserEnvironment": {
                        "enableNewIPCNamespace":"No",
                        "disabl3dHwAccl":"No",
                        "disableDvd":"No",
                        "disableSupplementryGroups":"No",
                        "disableSound":"Yes",
                        "disableTv":"No",
                        "disableU2f":"No",
                        "disableVideo":"Yes",
                        disableUserShell":"Yes"
                    },
                    "enableRestrictedCommunicationAccess":  {
                        "enableMachineIdSpoofing":"No",
                        "blockNetworkAccess":"Yes",
                        "enableFirewallForNewNW":"Yes",
                        "disableDbusAccess":"No"
                    },
                    "enableRestrictedFSAccess": {
                        "enableFileAccessAudit":"No",
                        "disableMount":"No",
                        "enablePrivateMode":"No",
                        "enablePrivateCache":"Yes",
                        "enablePrivateDev":"Yes",
                        "enablePrivateLibDirectory":"No",
                        "enablePrivateTmpFs":"No"
                    }
                }
            }
        ]
    }
}
```

13

Dell Hybrid Client troubleshooting

This section provides information about how to analyze and resolve issues you may observe when using Dell Hybrid Client.

Using log files for troubleshooting

You can use log files to analyze issues and troubleshoot your devices powered by Dell Hybrid Client.

NOTE: By default the log level is set as Basic. It is recommended to set the log level to High when the admin wants a detailed log. This would help in better troubleshooting of the product on any field issues.

Request log files using Wyse Management Suite

The device will be enabled to pull the log file using Wyse Management Suite. When this method is used, all the required logs are pulled to the Wyse Management Suite server.

Steps

1. Go to the **Devices** page, and click a particular device.
   The device details are displayed.
2. Click the **Device Log** tab.
3. Click **Request Log File**.
4. After the log files are uploaded to the Wyse Management Suite server, click the **Click here** link, and download the logs.

Troubleshooting

You can configure Log type such as Basic, Medium, and High and Log levels such as INFO, DEBUG, WARNING, ERROR, CRITICAL, EXCEPTION from Wyse Management Suite.

NOTE: By default the log level is set as Basic. It is recommended to set the log level to High when the admin wants a detailed log. This would help in better troubleshooting of the product on any field issues.

Configure the log password

By default, all Dell Hybrid Client log files are password-protected for security reasons. The initial password is same as the randomized password that is generated using the serial number and UUID of the device. This password is unique to a device. As an administrator, you can change the log password using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.

   NOTE: The change log password option is available only for the device policy group.

3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security** and click **Log Password**.
6. Enter the new password.
   The minimum password length is nine characters, and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character.

7. Click **Save & Publish**.

Configure log level from Wyse Management Suite

Steps

1. Register the device to Wyse Management Suite.
2. Log in to Wyse Management Suite as Admin.
3. Select the group to which the device is registered and go to **Edit Policies** > **Hybrid Client** > **Dell Hybrid Client 2.x** > **Advanced Settings**.
4. Click **Log Configuration** under **Troubleshooting**.
5. Select **Log Level** from the three given below:

Table 15. Log Level Configuration

Log Level Configuration	Severity of Logs
Basic	Warning, Error, and Critical Logs are generated in the DHC log files.
Medium	Info, Warning, Error, and Critical Logs are generated in the DHC log files.
High	All types of logs, Debug, Info, Warning, Error, and Critical Logs are generated in the DHC log files.

Download the logs from Wyse Management Suite

Steps

1. Go to **Device details** page in Wyse Management Suite and go to **Device Log** tab.
2. Click **Request Log File** and then click **Send Command** on Alert window.
   Wait for 15 s for the download link to appear.
3. Select **click here** to download the log file.
4. Extract the downloaded file using 7- Zip file manager tool or any other applicable tool and verify.
   By default, all Dell Hybrid Client log files are password-protected for security reasons.

Export log files using Advanced Settings

Prerequisites

Ensure that you have enabled the dev mode in Dell Hybrid Client.

Steps

1. Log in to Dell Hybrid Client.
2. On Dell Hybrid Client, go to **Device Settings**.
3. Go to **Advanced Settings** > **Troubleshooting**.
4. Under **General** tab, click **Export Logs**.
   - **Export to Folder**—You can export the log files to the Download folder.
   - **Export to USB**—You can export the log files to a connected USB drive.
   - **Export to Network Share**—You can export the log files to a shared folder path.

Export VDI log files

- Citrix and VMware logs are available in the Device Log files that are extracted using Wyse Management Suite. For more information about how to extract device logs using Wyse Management Suite, see Request a log file using Wyse Management Suite.
- Dell RDP logs are available in Dell Hybrid Client. To view logs, do the following:
  1. Open Terminal and create new ini file under /tmp in name debugLogConfig.ini.
  2. Add the following lines in an ini file:

```
LogLevel=0xFFFFFFFFFFFFFFFF
logLocation=/tmp/rdpLog.txt
failurelogfilelocation=/tmp/rdpFailLog.xml
```

  3. Save the file as `debugLogConfig.ini` in the `/tmp` location on your device.
  4. Launch the RDP icon. Logs are generated in the `rdpLog.txt` file that is located in the `/tmp` folder.
  5. Open the text editor again.
  6. Open `rdpLog.txt` file from the `/tmp` folder to view the VDI logs.

Device is unable to register to Wyse Management Suite

Problem—Device is unable to register to the Wyse Management Suite server. Dell Client Agent (DCA) UI on the device displays an invalid error code from the Wyse Management Suite server.

Solution—Verify if the device status is displayed as **Not Registered** on the **Device** page in Wyse Management Suite. If the device status is displayed as Not Registered, you can delete the device from **More Actions**. Once the device is removed from the Not Registered status, the device will register successfully.

Enrollment validation is pending

Problem—Device does not appear on the Wyse Management Suite page even though the Dell Client Agent (DCA) UI on the device displays the status as **Registered**.

Solution—Verify if the Enrollment Validation is pending, and validate the enrollment using the **Validate Enrollment** option.

Reset the Dell Hybrid Client to factory default settings

You can send a command from Wyse Management Suite to reset your Dell Hybrid Client to factory default settings. All the Dell Hybrid Client policies that are pushed from Wyse Management Suite are reset to default values when you perform a factory reset.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Devices** page.
3. Apply the filters to find the preferred device.
4. Select the check box of the device.
5. From the **More Actions** drop-down menu, click **Factory Reset**.
   An **Alert** window is displayed.
6. Enter the reason for the client reset.
7. Click **Send Command**.

   NOTE: After factory reset, Setup Wizard will show if Auto Discovery is not configured.

Reimage using Wyse Management Suite

Dell Hybrid Client can be reimaged from Wyse Management Suite. Reimage process will completely reinstall Dell Hybrid Client.

About this task

NOTE: Ensure that you have backed up the data on the target device before you begin the reimage process.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Devices** and select **Devices** from the list.
3. Click on **More Actions** and Click **Reimage**.
   Reimage Alert Message Will Pop up in Wyse Management Suite.
4. Click **Send Command** and it will initiate Reimage.
   Device End will prompt reimage notification.
5. Click **Update Now**.
6. Device will reboot and start booting from Recovery and will prompt for **TPM Clear**. Press **F12** (Only for FDE image).

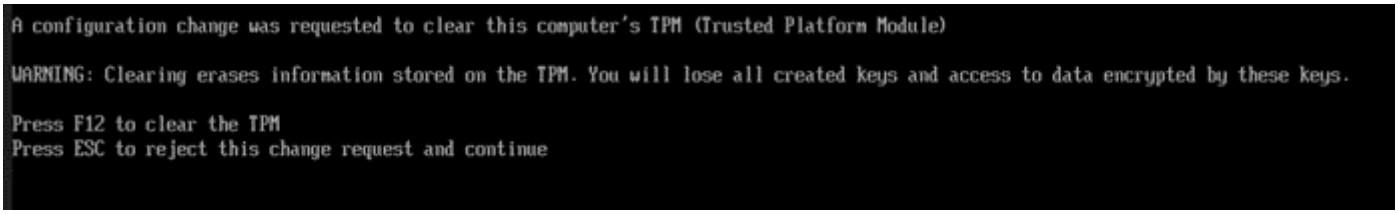


Figure 130. TPM Clear

7. After clicking **F12**, device will reboot and continue to install FDE.
8. Click **Install FDE**. It will also auto execute in 30s (Only for FDE image).



Figure 131. Install FDE

9. Dell Hybrid Client with Full Disk Encryption will begin the installation (Only for FDE image). Once installation is complete, the user will be redirected to Dell Hybrid Client Login Screen.

   NOTE: During installation, device will reboot multiple times. The process should not be interrupted.

10. The device boots into Dell Hybrid Client when the installation is complete. The device will be registered to Wyse Management Suite.

14

Security update cadence

For base operating system packages update, we will be releasing a security add-on package every 3 months to keep the system up to date. Apart from this, if any critical or high vulnerability is discovered in any of the Dell Hybrid Client packages, or included 3rd party packages, we will be releasing the particular add-on with the fix accordingly.

NOTE: Automatic kernel update from the Ubuntu snap store shall be enabled from Wyse Management Suite. Once enabled, the Dell Hybrid Client device automatically installs the kernel updates by downloading from the snap store. This requires access to the Internet connection. Also, this automatic kernel update feature is applicable only for the FDE based device and does not support on non-FDE devices.

15

Frequently Asked Questions (FAQs)

- **Is Dell Hybrid Client an application based on Ubuntu operating system?**

  Yes, Dell Hybrid Client is an application stack based on the Ubuntu operating system. For information about the version of the Ubuntu operating system that is supported in each Dell Hybrid Client release, see Supported operating system.

- **Which edition of Wyse Management Suite does Dell Hybrid Client support?**

  Dell Hybrid Client is supported on the Wyse Management Suite Pro edition. For information about the version of Wyse Management Suite Pro that is supported in each Dell Hybrid Client release, see Supported management software.

- **Can I add a user group based on OUs in Active Directory?**

  Dell Hybrid Client supports OU User Group on Wyse Management Suite.

- **How the admin credentials are used in Direct AD login scenario?**

  The username or password provided from Wyse Management Suite is used only during the setup of configuration for the first time. This happens automatically whenever the admin pushes the configuration from Wyse Management Suite. Also, the credentials are never stored in the device. The username should be in the format of "username@domain" only from Wyse Management Suite.

- **What takes precedence between Wyse Management Suite and Dell Hybrid Client local UI when conflicting settings are enforced?**

  Configurations that are editable from the Device Settings UI take higher priority than those set from the Wyse Management Suite server. Settings that are supported as part of the user profile are preserved only when user personalization is enabled from Wyse Management Suite. These settings are applicable only for the logged-in AD user.

- **Will the changes made to the local device by one user have any effect on the user profile of a second user who logs in to the same device?**

  The user-specific settings are not applied to another user profile. When a user configures the Device Settings using either Wyse Management Suite or the local UI, the user-specific configurations are preserved. Configurations that are not supported in user personalization (profile roaming) are saved locally in the device and are applied to that user profile during the next login.

- **Does Dell Hybrid Client support the Relative Mouse Button feature in VMware Blast or PCoIP?**

  There is no specific setting in Wyse Management Suite to enable or disable the Relative Mouse Button feature. If VMware supports this feature in Linux clients, it will work in Dell Hybrid Client.

- **Who are the major cloud providers supported by Dell Hybrid Client?**

  Dell Hybrid Client supports Microsoft Azure, Google Workspace (formerly G Suite), and Box personal drive.

- **Can you recover Dell Hybrid Client by recovering the partition on the device?**

  Dell Hybrid Client can be recovered from the recovering partition on the device.

- **How to recover the Dell Hybrid Client if the device does not boot to the operating system?**

  You must reimage the device from the recovery partition if you are able to login from Boot menu recovery option. If not, use USB recovery for imaging.

- **Can troubleshooting logs for Dell Hybrid Client be extracted?**

  You can use Wyse Management Suite to extract the log files, extract logs to a USB drive using the local device Advanced Settings.

- **Are the Dell Hybrid Client logs for network trace, USB, and troubleshooting available in Wyse Management Suite?**

  You can extract system logs for network trace, USB, and troubleshooting using Wyse Management Suite.

- **Is there any noticeable delay in searching for the file from VDI to Cloud when priority is set using File Affiliation?**

Dell Hybrid Client will first try to open the file using VDI and if there is any failure, it immediately opens the file from the cloud application.

- **When you recover Dell Hybrid Client, will it also recover the third-party applications?**

  Third-party applications are not recovered when you recover Dell Hybrid Client.

- **How to Backup and Restore the Full Disk Encryption (FDE) Key?**

  Backup:
  - Use the command "snap recovery --show-keys" to get the FDE key.
  - The key has to be stored/noted down manually in a secured place.

  Restore:
  - When device prompts for the key, the user has to enter the respective key from backup.

    NOTE: In Dell Hybrid Client 2.5, the key backup and restore are only manual process and the admin has to manually do the task.

- **How long does the recovery process take on the Wyse 5070 device powered by Dell Hybrid Client?**

  The image recovery process takes approximately 35 minutes on the Wyse 5070 device.

- **Does Dell Hybrid Client support Microsoft Office locally?**

  Dell Hybrid Client does not support the local Microsoft Office. You can use the cloud office to open your files.

- **What is FTA?**

  FTA stands for File Type Association. It is a correlation between a file type and an application. Dell Hybrid Client supports the file type association for Citrix, VMware, and RDP.

- **What is the size of the whole Dell Hybrid Client image?**

  For information about the image size, refer the latest *Dell Hybrid Client 2.5 Release Notes* at www.dell.com/support.

- **What happens when the disk space is nearing its maximum capacity?**

  A warning message is displayed to the user.

- **Can I install any Ubuntu Debian/Bundle Packages on Dell Hybrid Client ?**

  Yes, it can be Installed on Dell Hybrid Client, But the application can not be managed from Wyse Management Suite. VDI client add-ons released on Dell Hybrid Client support only the Wyse Management Suite management options.

- **What to do if the device login fails?**
  - Check that the username and password are valid.
  - Check that the username format is followed.

    The username format must be <username> or <username>@<domain>.

  - If you are still not able to log in to the device, contact your administrator.
- **What is the need of logoff or restart pop-ups?**

  User can use this screen to choose either to log off or restart the device. This action is required for recent configurations from Wyse Management Suite to take effect.

- **What is the standard password requirement?**

  The minimum password length is nine characters and the maximum password length is 127 characters. The password must contain at least one uppercase letter, one lowercase letter, one numeric digit, and one special character. You must avoid the $% combination. The password should not contain the username.

- **What to verify if the Wyse Management Suite registration fails?**
  - Check the network connection and make sure it is established.
  - Check that the DCA settings are configured as expected.
- **How to troubleshoot if the network connection is not working?**
  - Check the network connection status icon from the top bar.
  - Access the Ping option from **Device Settings** > **Troubleshooting**. Try to ping to a valid host or IP address and check if ping is successful.
  - Check that the network cable is properly connected to your device port.
  - If you are using WiFi, check that the device is connected to your preferred access point.
  - If your network connection is still not working, contact your network administrator.

How to configure Single and multiple display settings

- By default, You can configure the Monitor setting from **Device Settings**.
- Only Local and Domain User configurations are preserved after Logout/reboot when configuring from **Device Settings**.
- In Guest, Display configuration is not preserve after Logout/Reboot, if you must preserve display settings across all users then you must configure from **Wyse Management Suite**.

Configuring Display using Device Settings

You can configure the display using Device Settings.

- Configuring Single Display using Device Settings
- Configuring Multi Display using Device Settings

Configuring Single Display using Device Settings

You can configure the single display using Device Settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Monitor Settings**.
5. Click the **Mouse**.
6. Click **Additional Monitor Settings**.

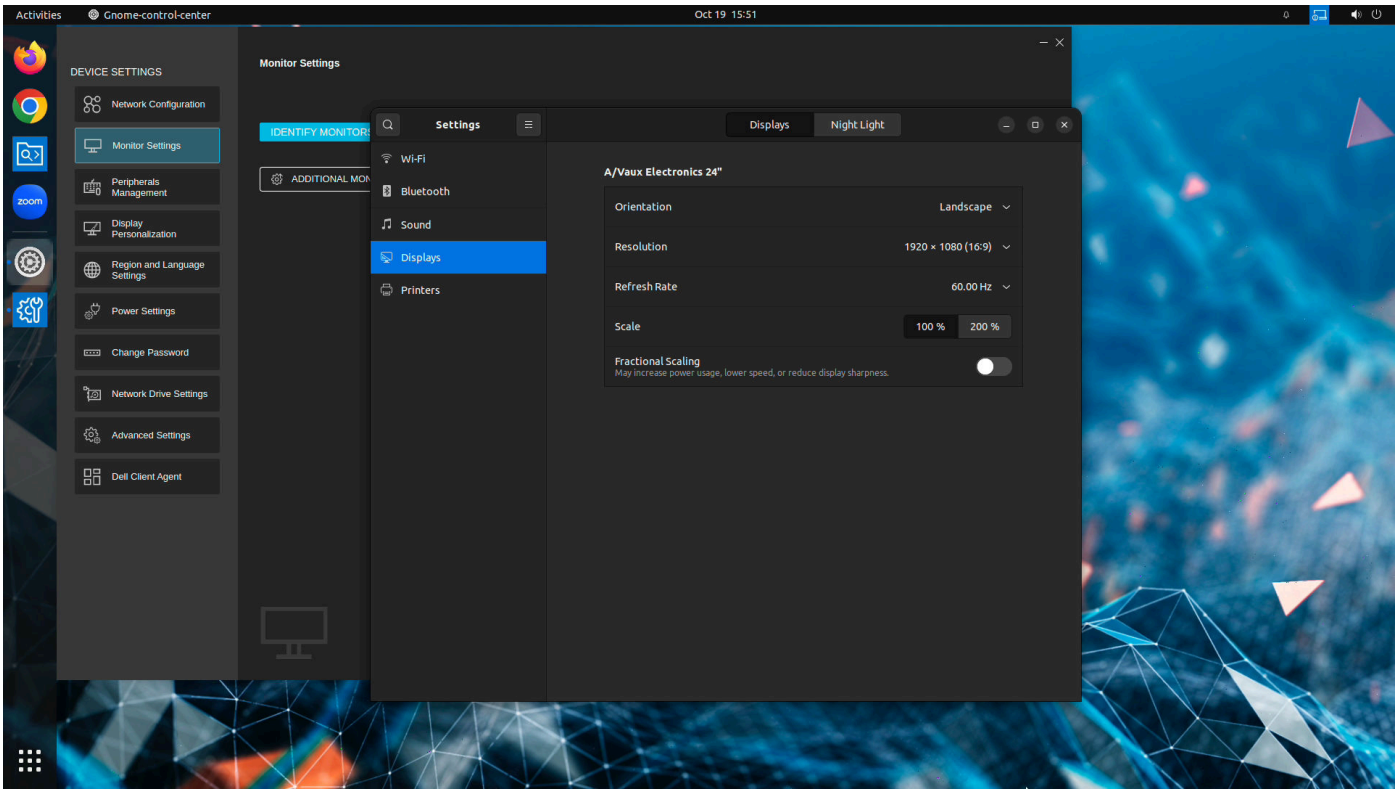


Figure 132. Additional Monitor Settings

You can configure **Orientation**, **Resolution**, and **Scaling** using device level **Monitor Settings**.

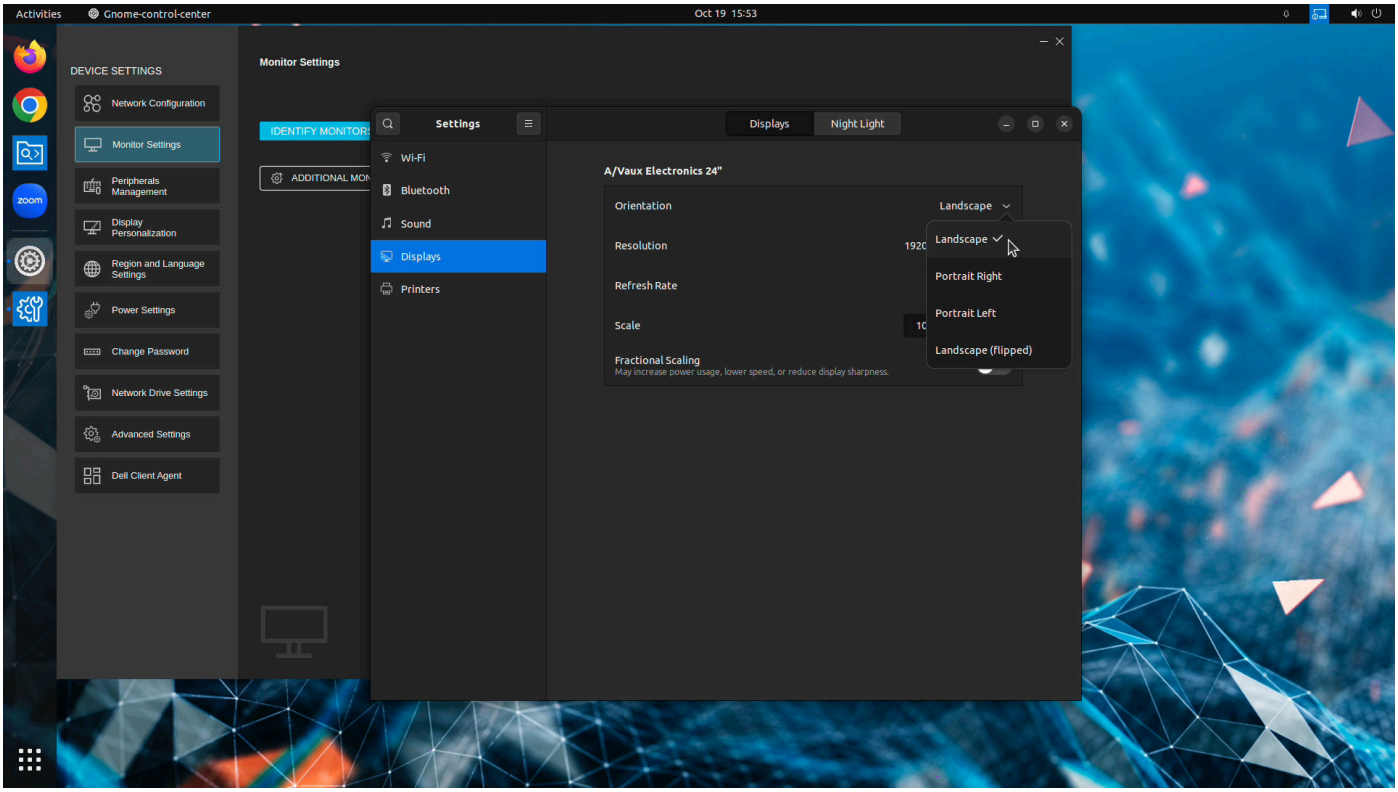


Figure 133. Orientation

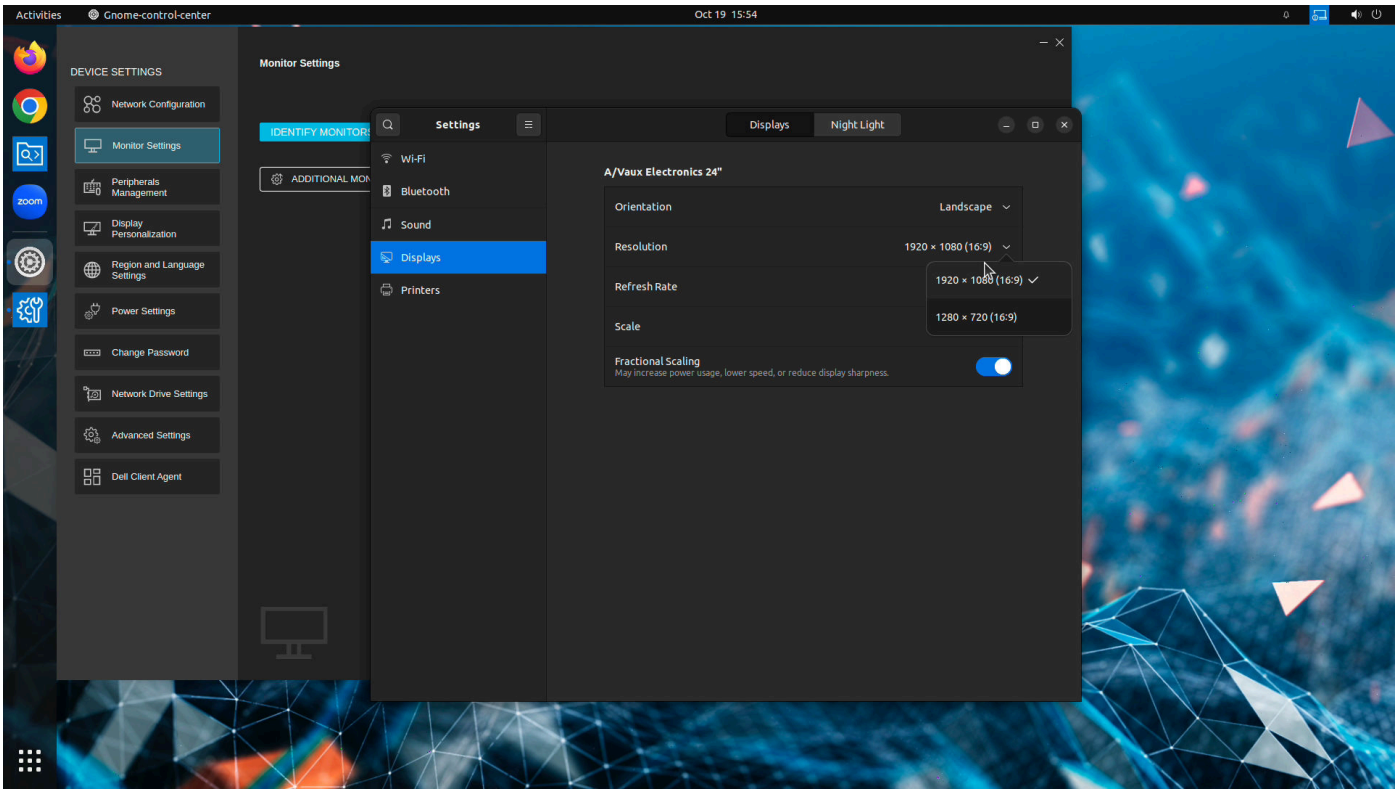


Figure 134. Resolution

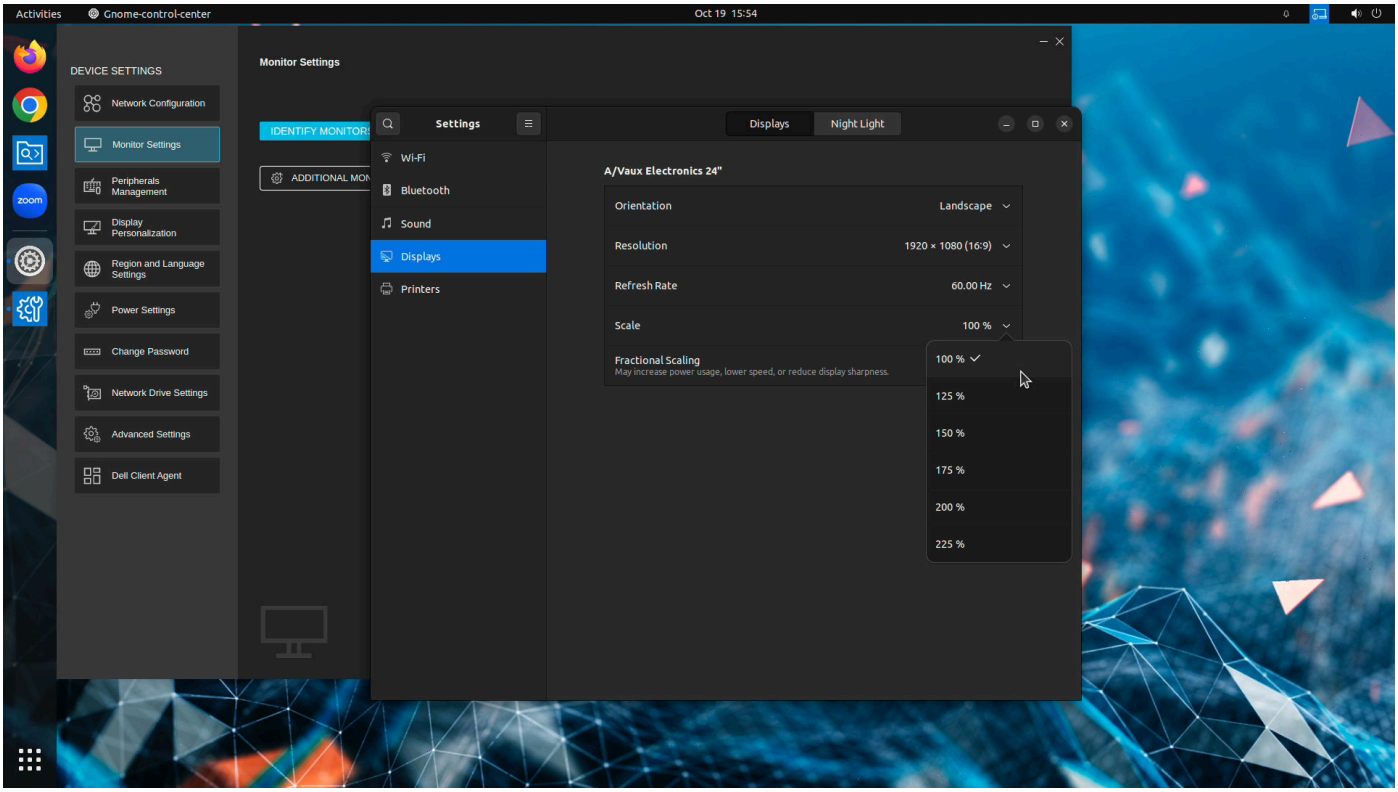


Figure 135. Scale

Configuring Multi Display using Device Settings

You can configure Multi Display using Device Settings.

Multi Display configurations are enabled when more than one monitor are connected.

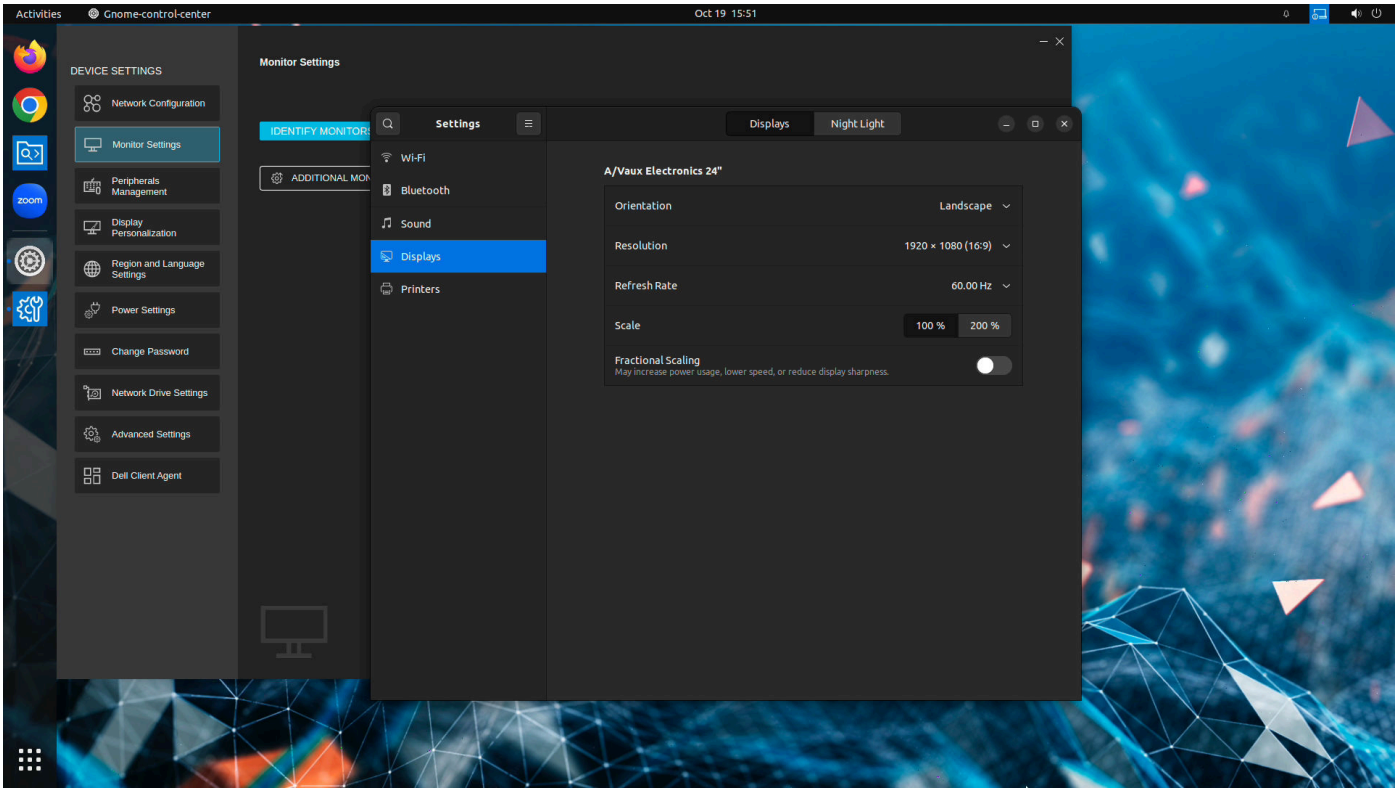


Figure 136. With Single Monitor

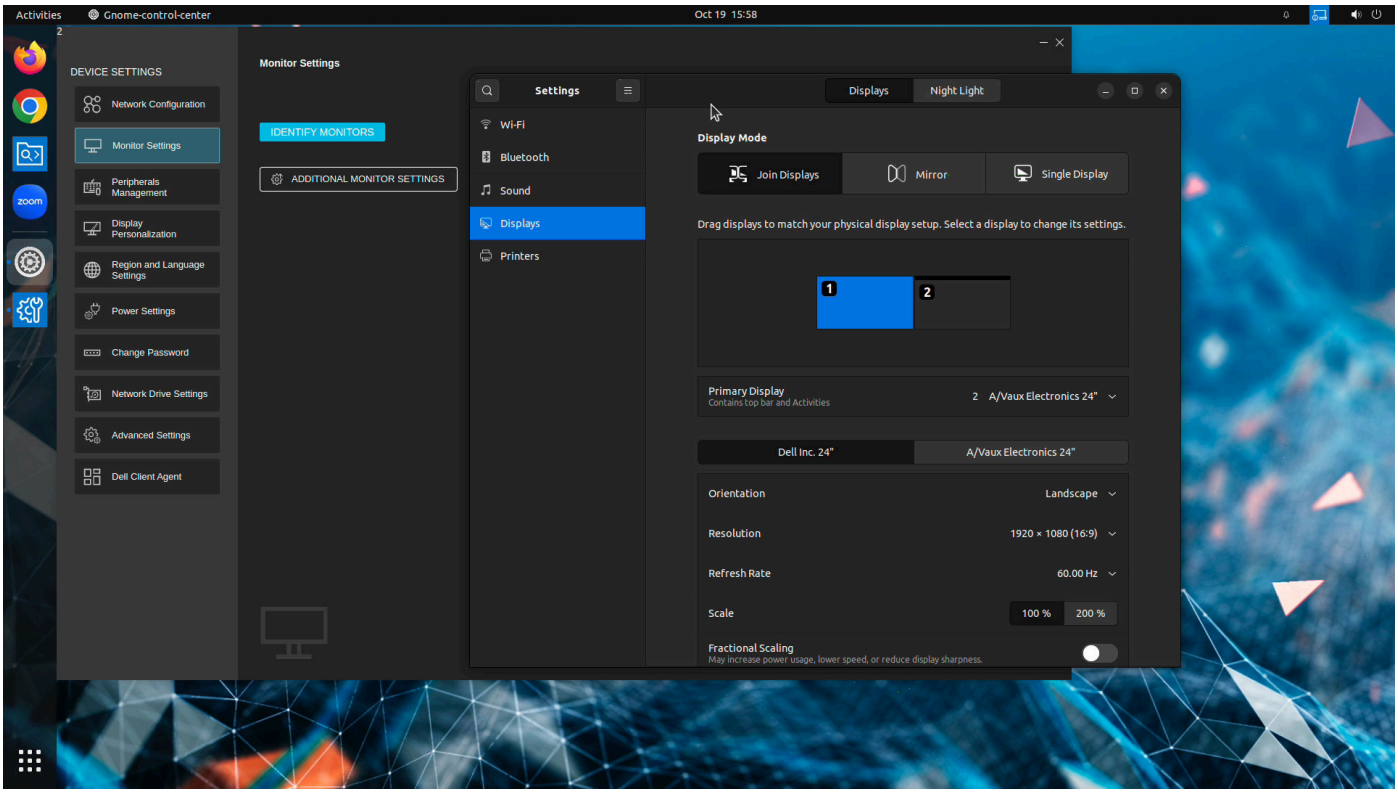


Figure 137. With Dual Monitors

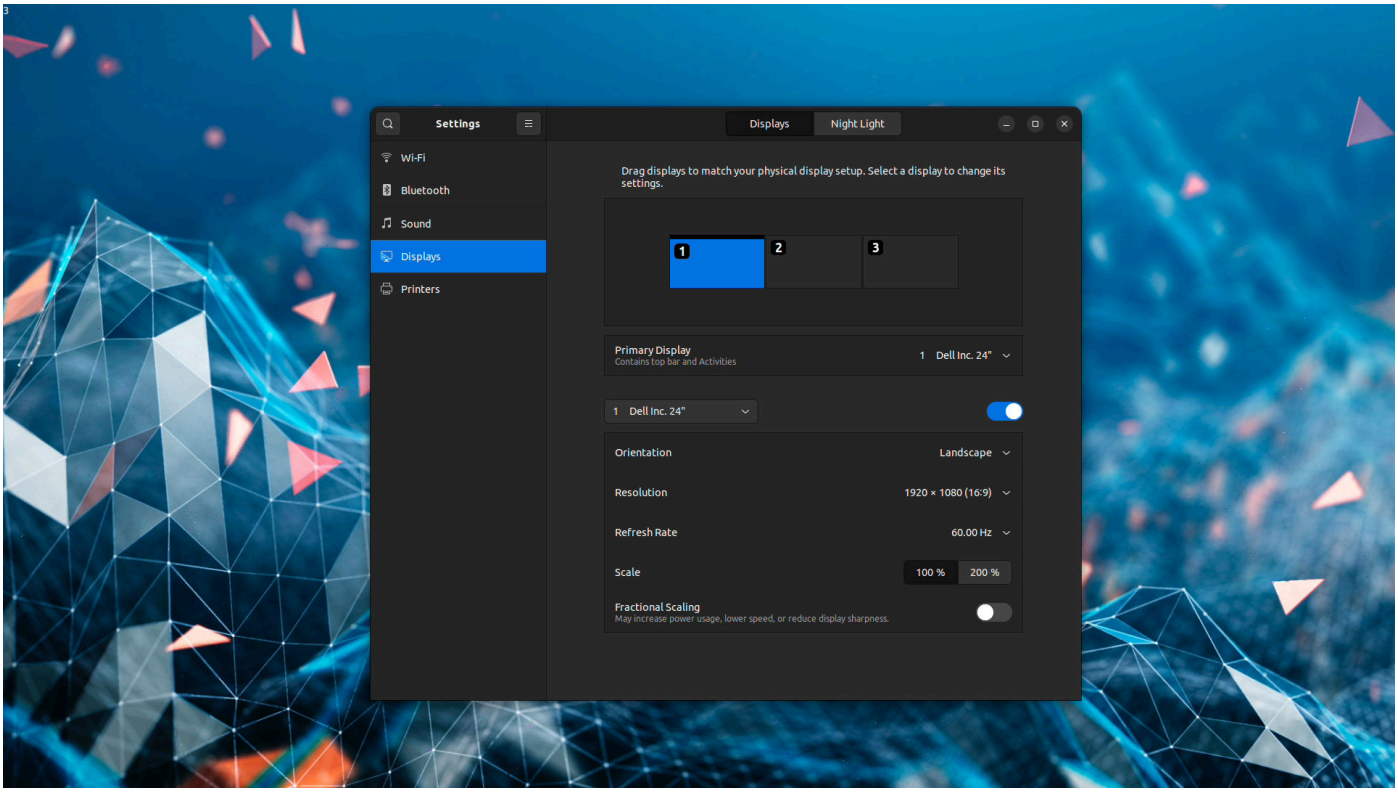


Figure 138. With Three Monitors

NOTE: **Mirror Mode** and **Single Display Mode** are active only when your device is connected with two monitors. When a monitor is more than one, then only Multi Display setting can be configured using Device Settings.

You can configure the following settings:

- **Display Mode:**
  1. **Display Mode** is active when you connect more than one monitor.
  2. Three Display modes are available in Device settings for you to select based on the use case.

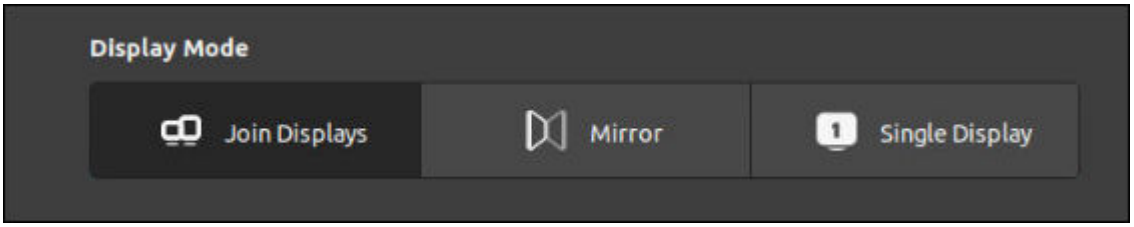


Figure 139. Display Mode

  - **Join Display:**
    a. When two or more monitors are connected, you can use **Join Displays** mode and configure Primary display, Monitor Position, Orientation, Resolution, and Scaling.
    b. You can move display in the Drag and display box to match the physical display setup.

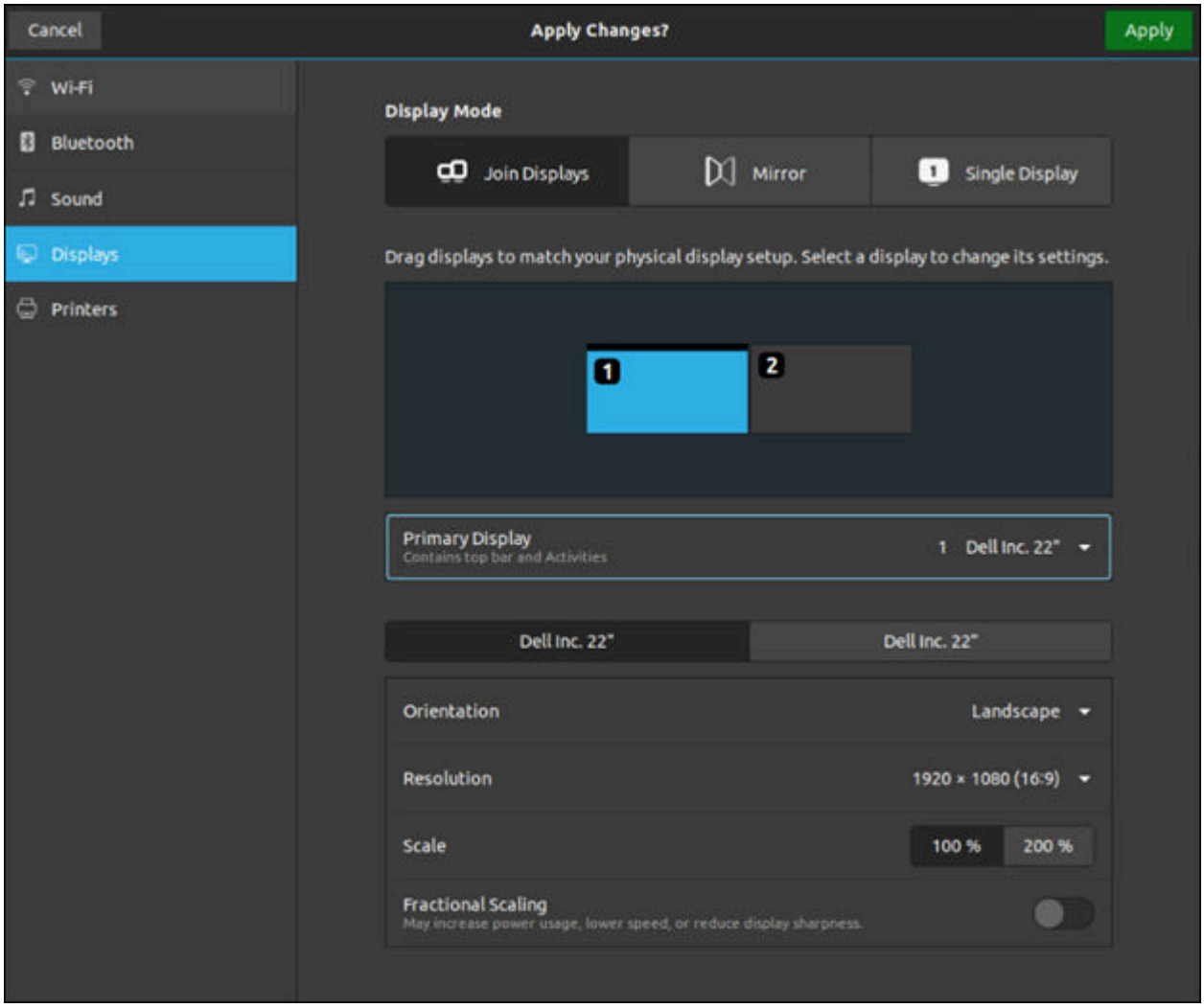


Figure 140. Join Display

- **Mirror:**
  a. **Mirror** mode is active once you connect two monitors. The connected monitors are mirrored.

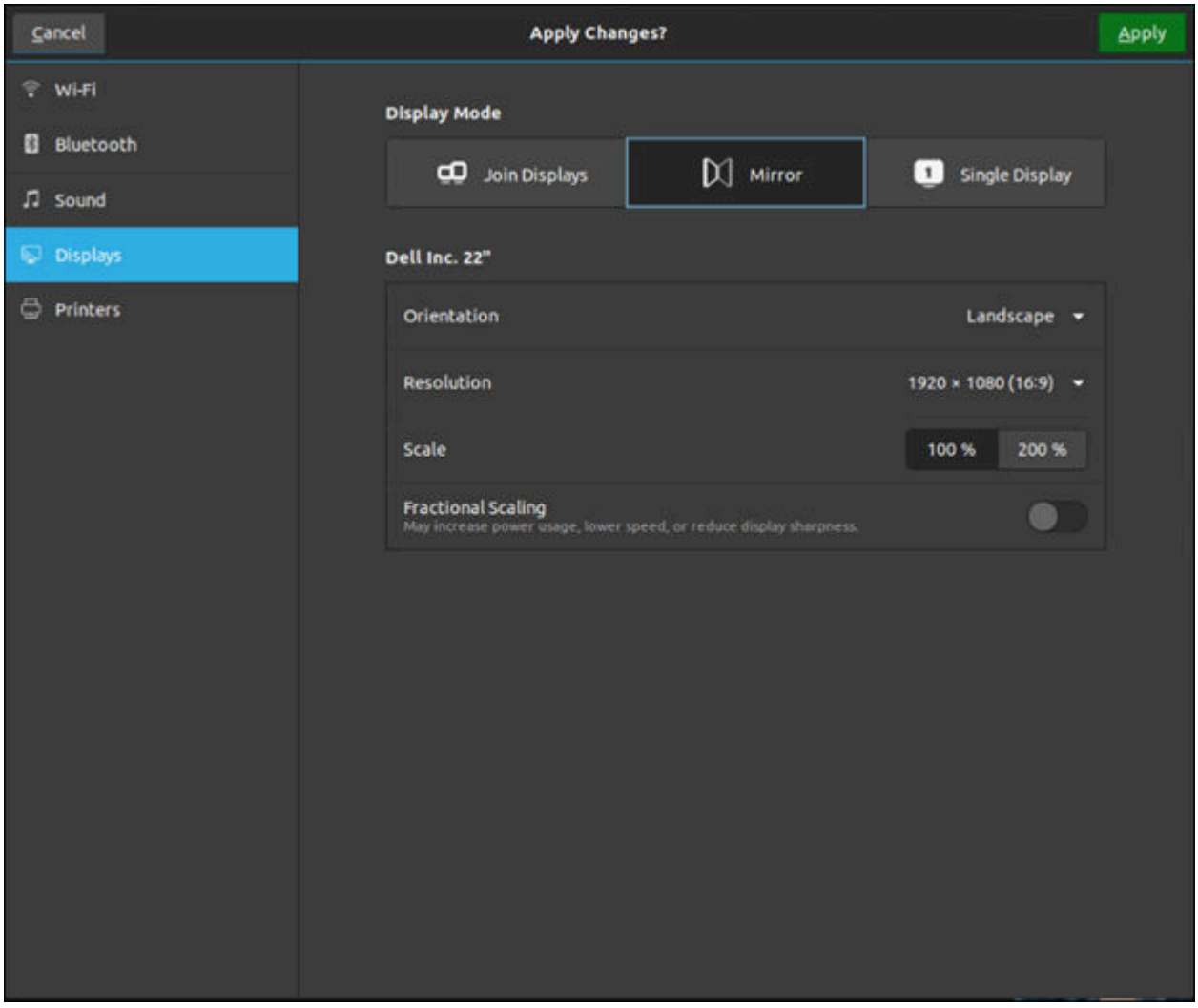


Figure 141. Mirror

NOTE: **Mirror** mode supported only two monitors. When more than two monitors are connected, Join Display or Multi Monitor mode is active.

- **Single Display:**
  a. You can configure a **Single Display** mode when two monitors are connected. In this case, the primary monitor is active and the secondary monitor is blank or in Turned Off state.

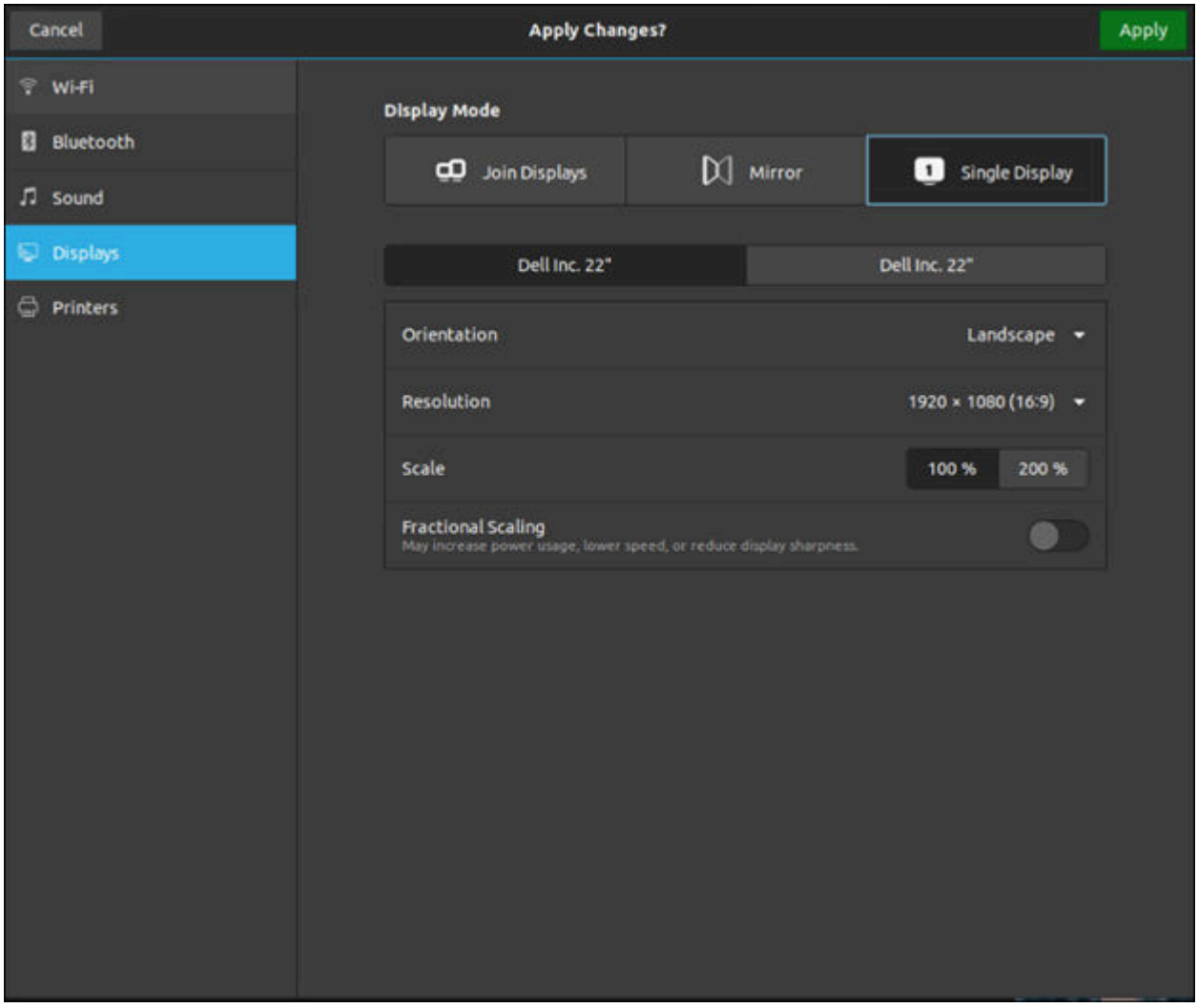


Figure 142. Single Display

Examples for Multi Display Settings from Device Settings

Example 1 - Three Display Monitor with M1 as primary

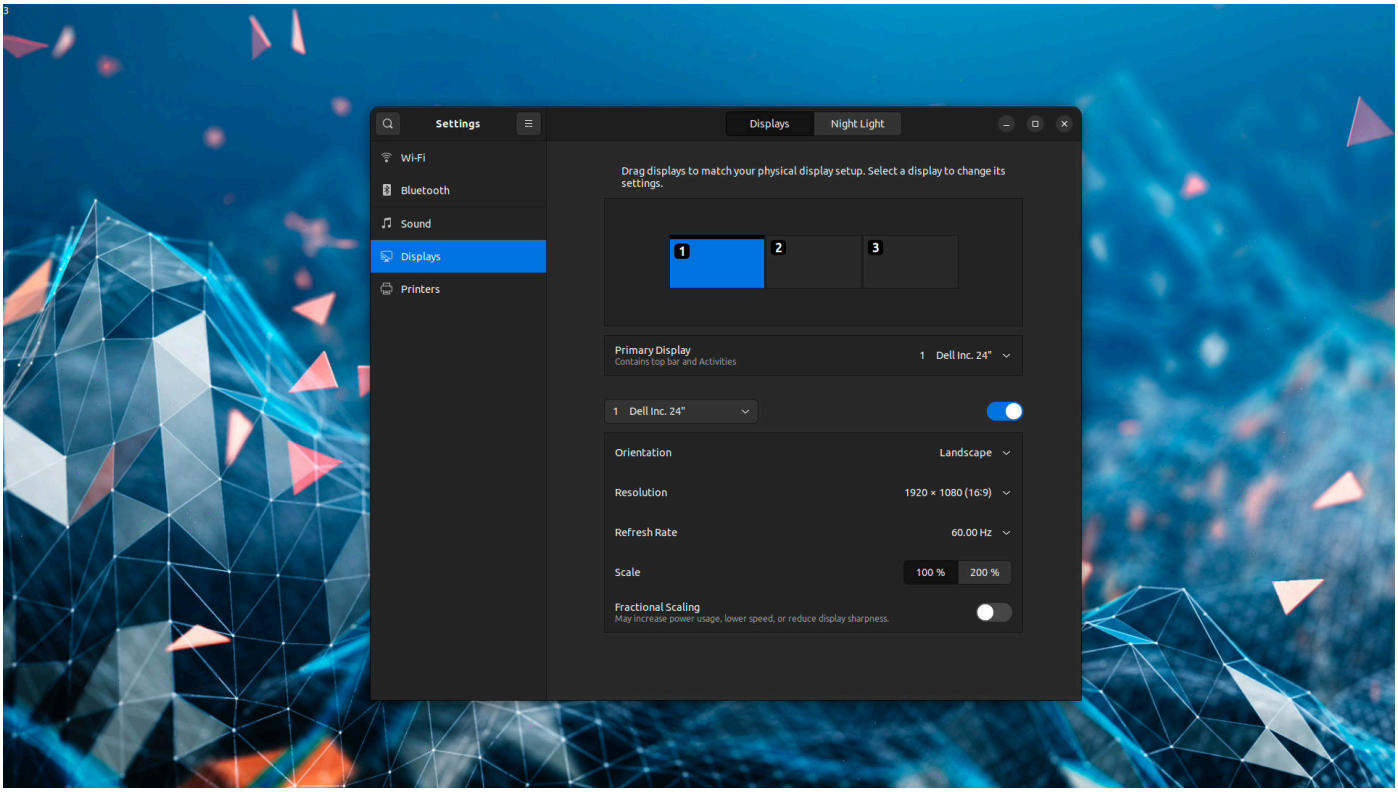


Figure 143. Monitor 1 as primary

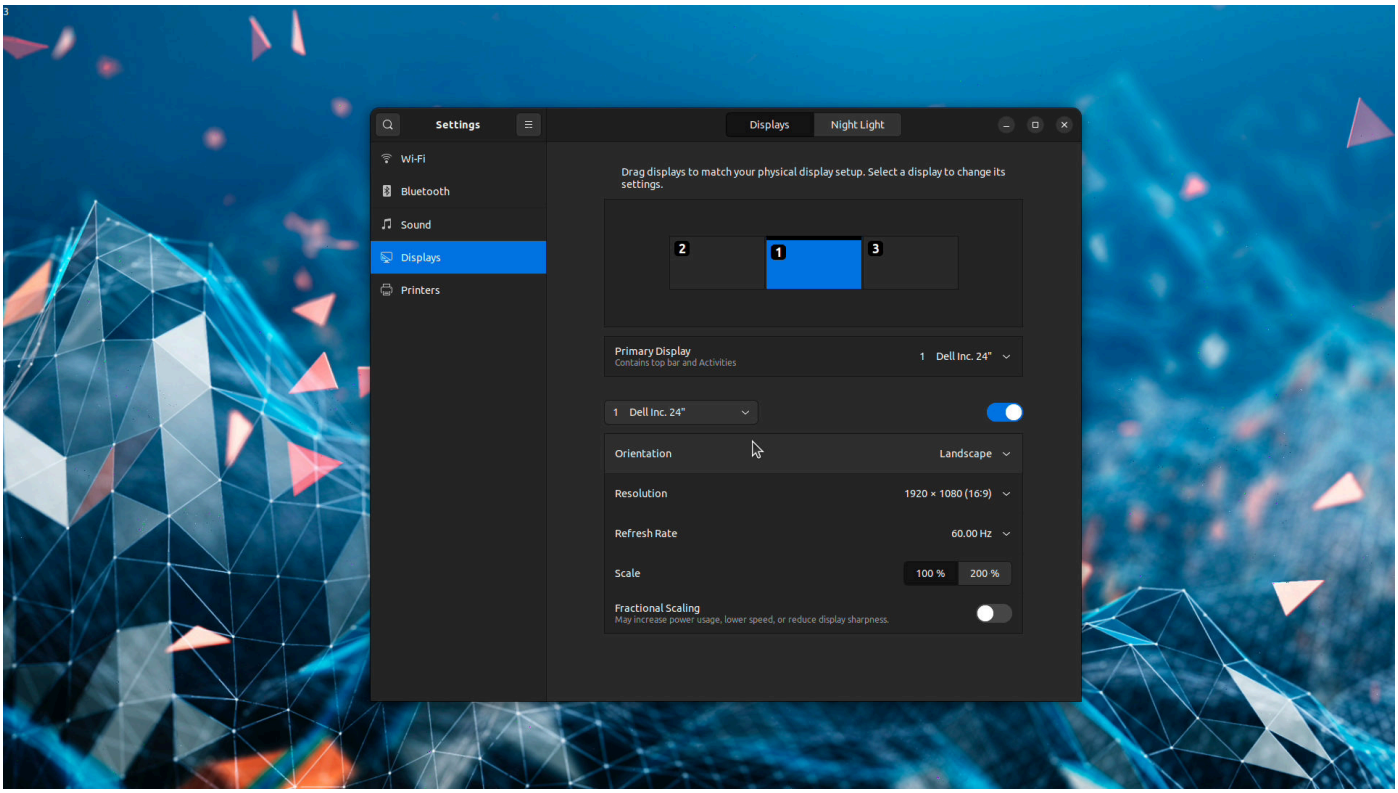


Figure 144. Monitor 1 as primary

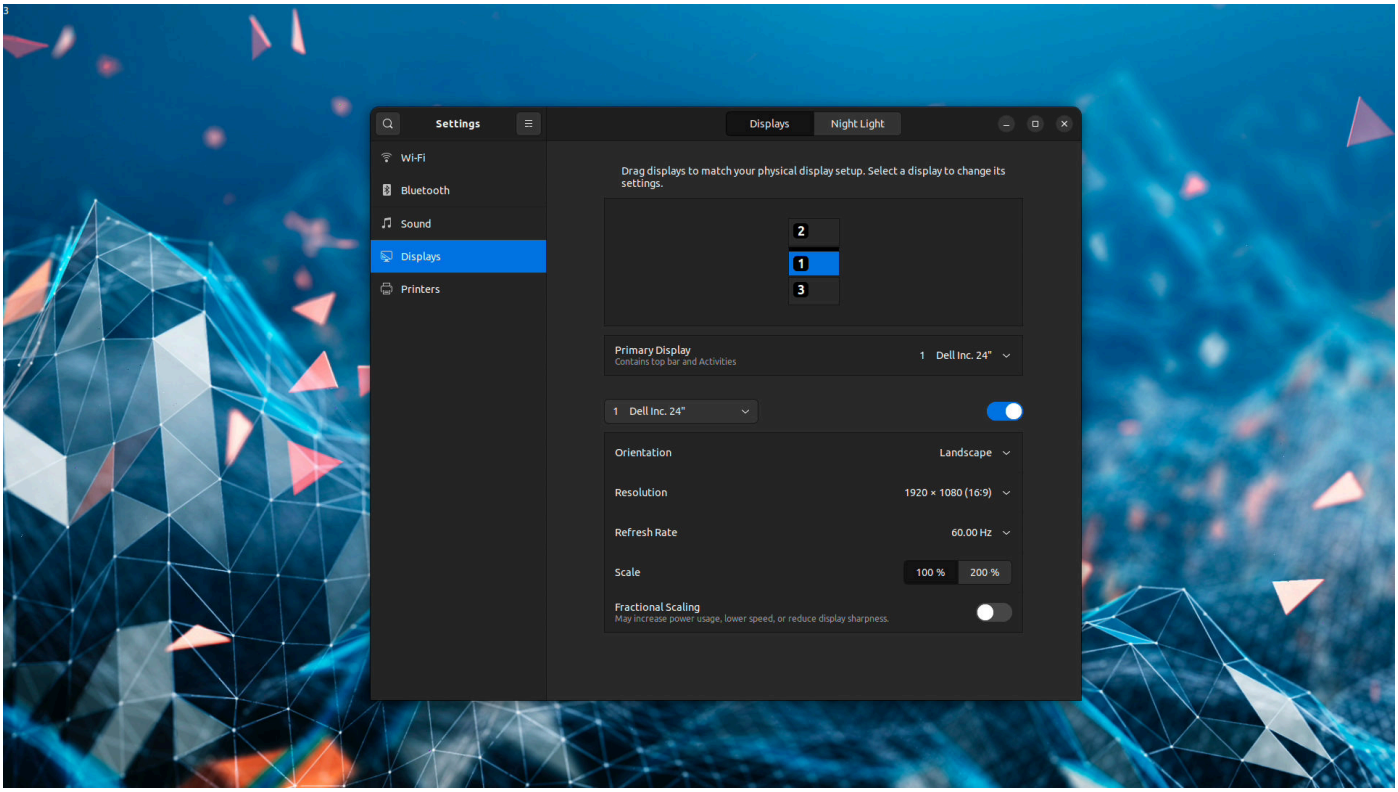


Figure 145. Monitor 1 as primary

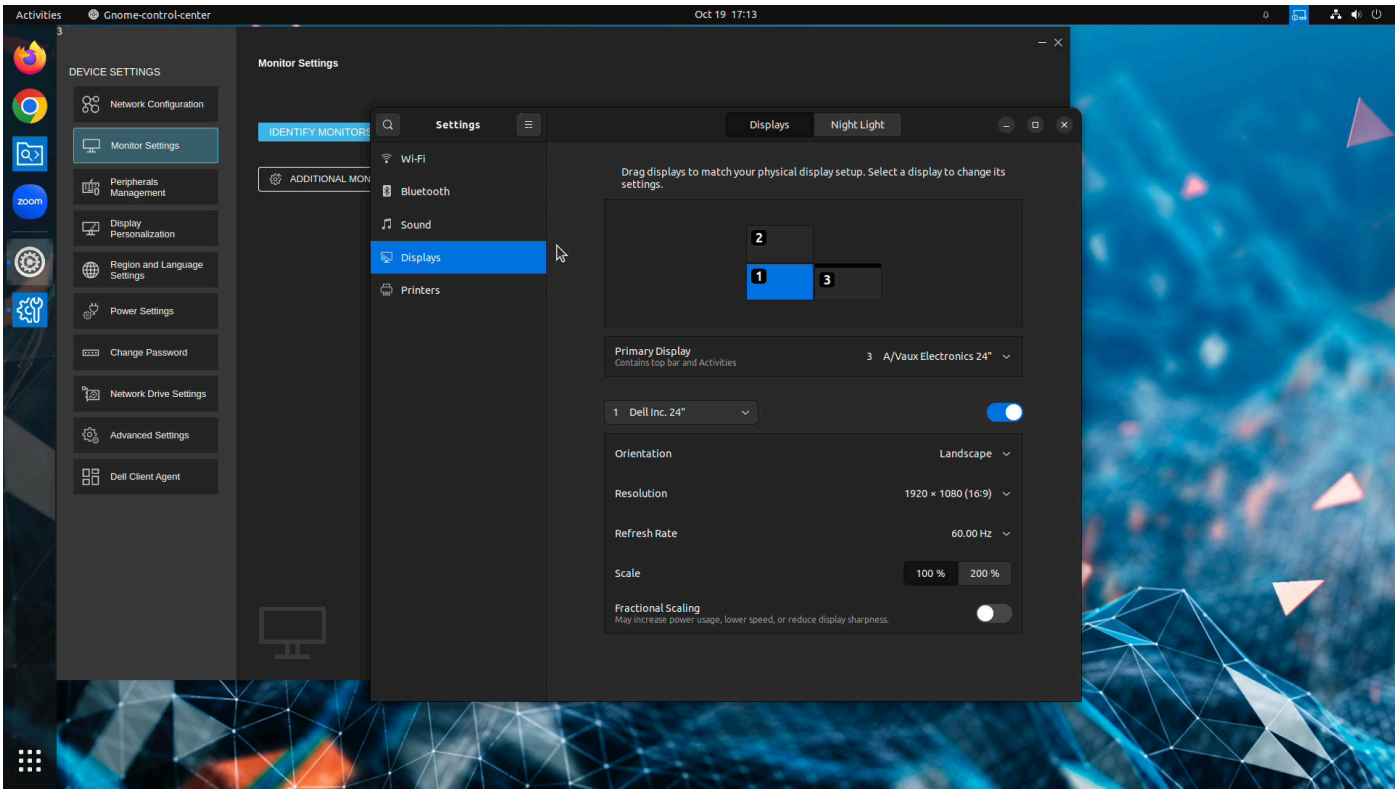


Figure 146. Monitor 1 as primary

Example 2 - Three Display Monitor

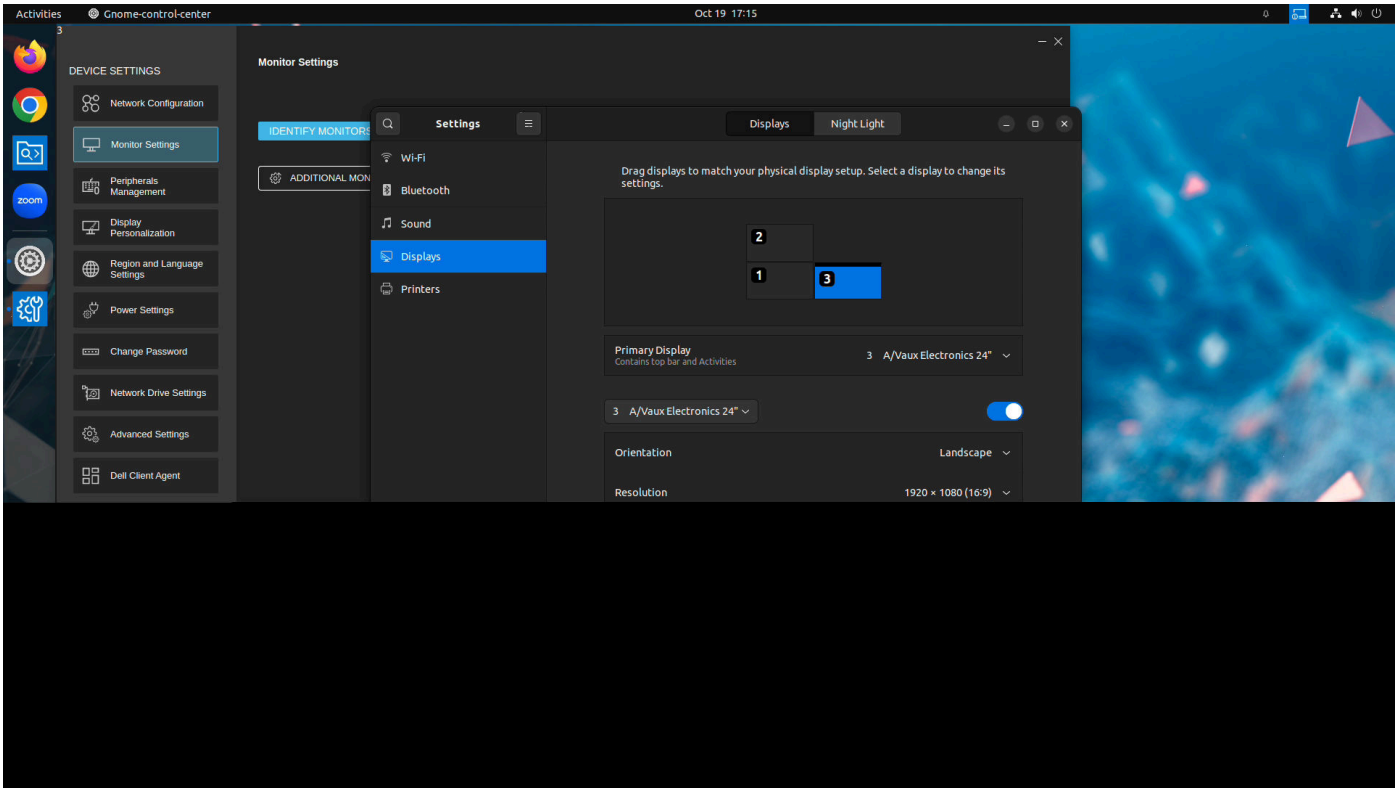


Figure 147. Monitor 3 as primary

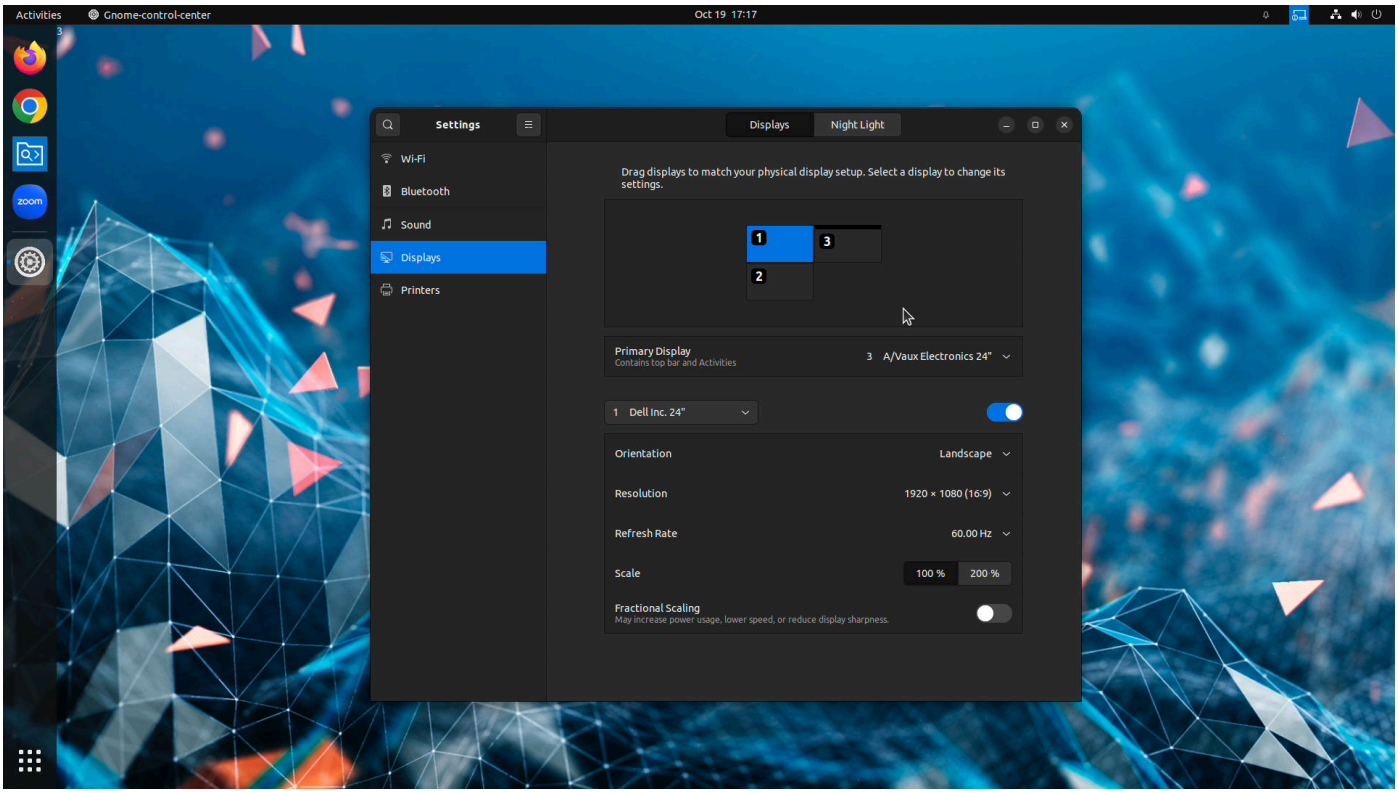


Figure 148. Monitor 1 as primary

Example 3 - Four Display Monitor with M1 as primary

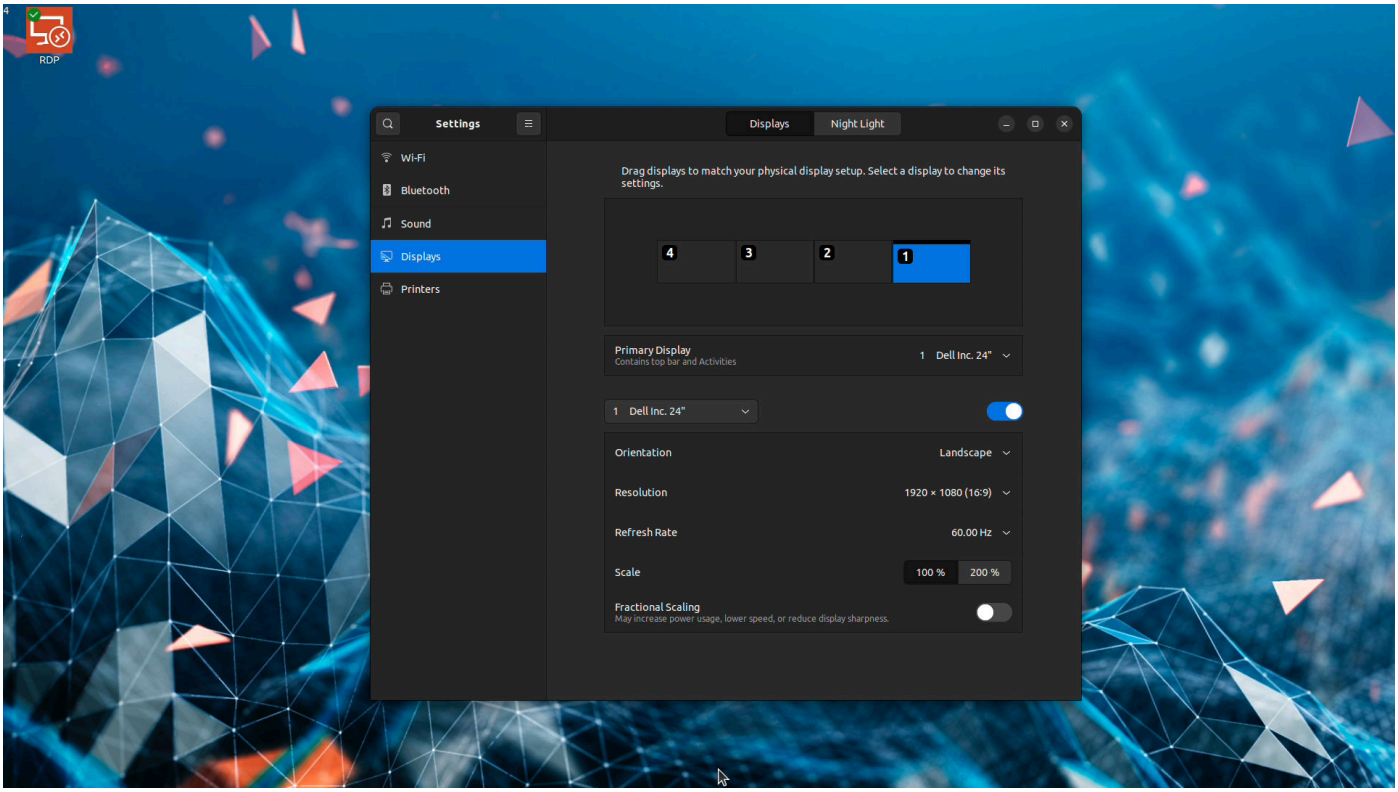


Figure 149. Monitor 1 as primary

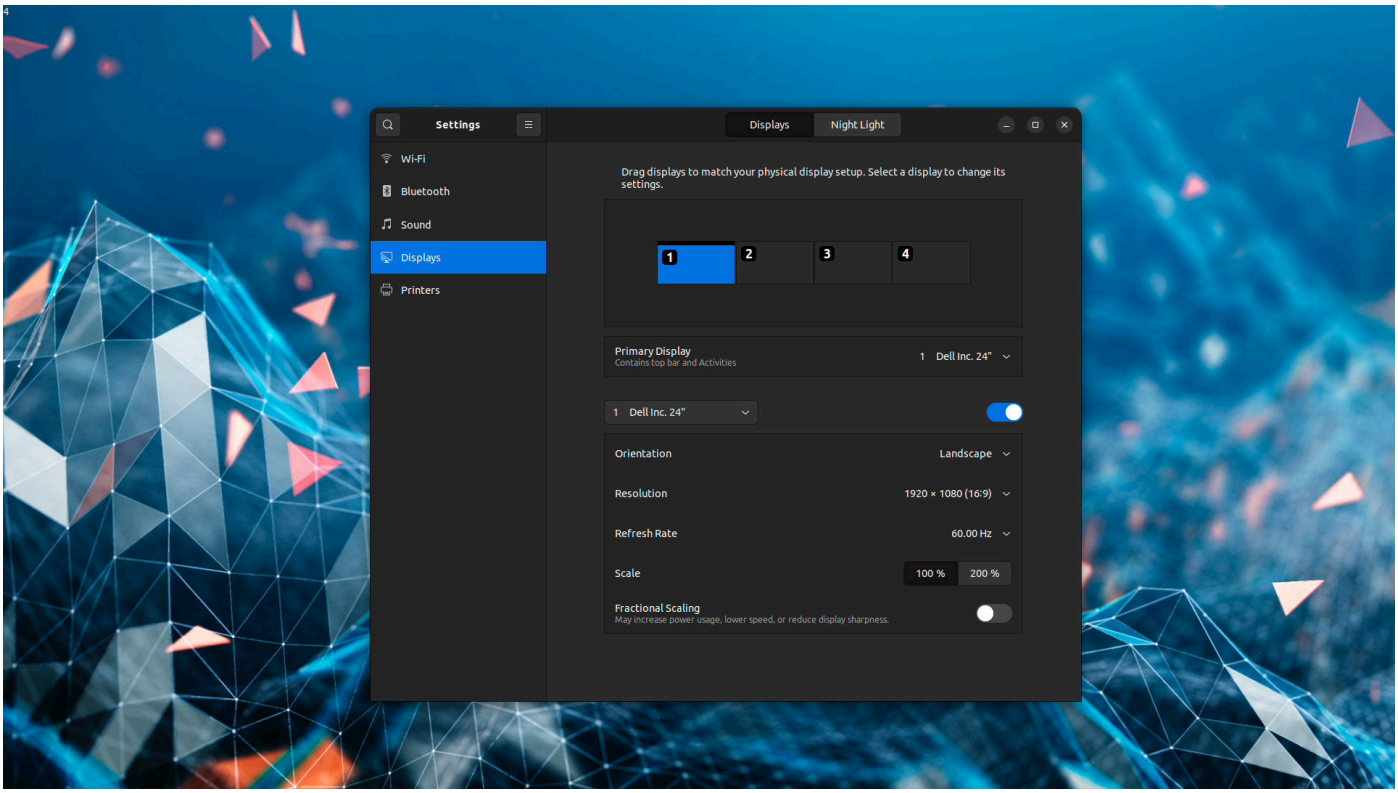


Figure 150. Monitor 1 as primary

Example 4 - Five Display Monitor with M1 as primary

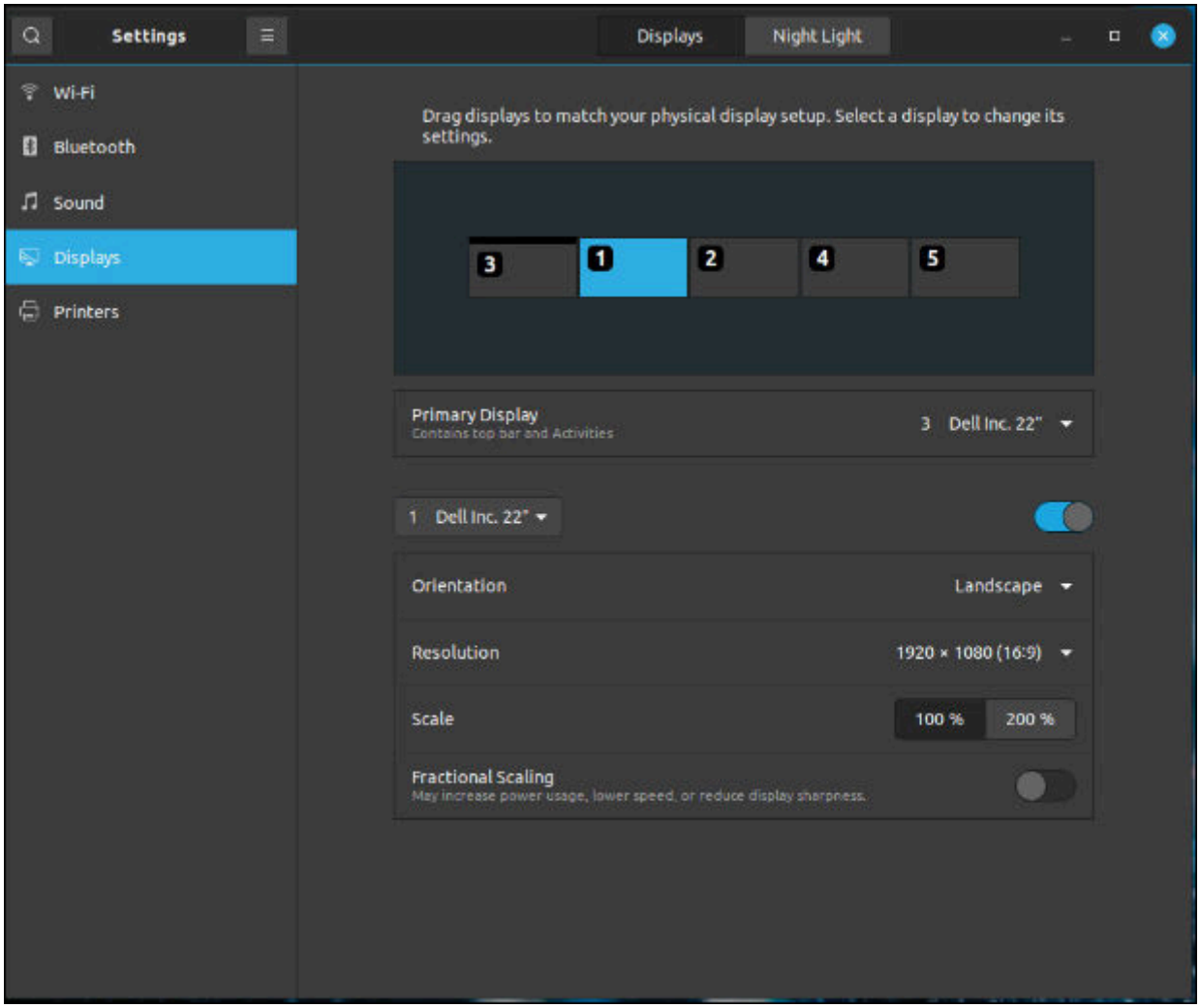


Figure 151. Monitor 1 as primary

Example 5 - Six Display Monitor with M1 as primary

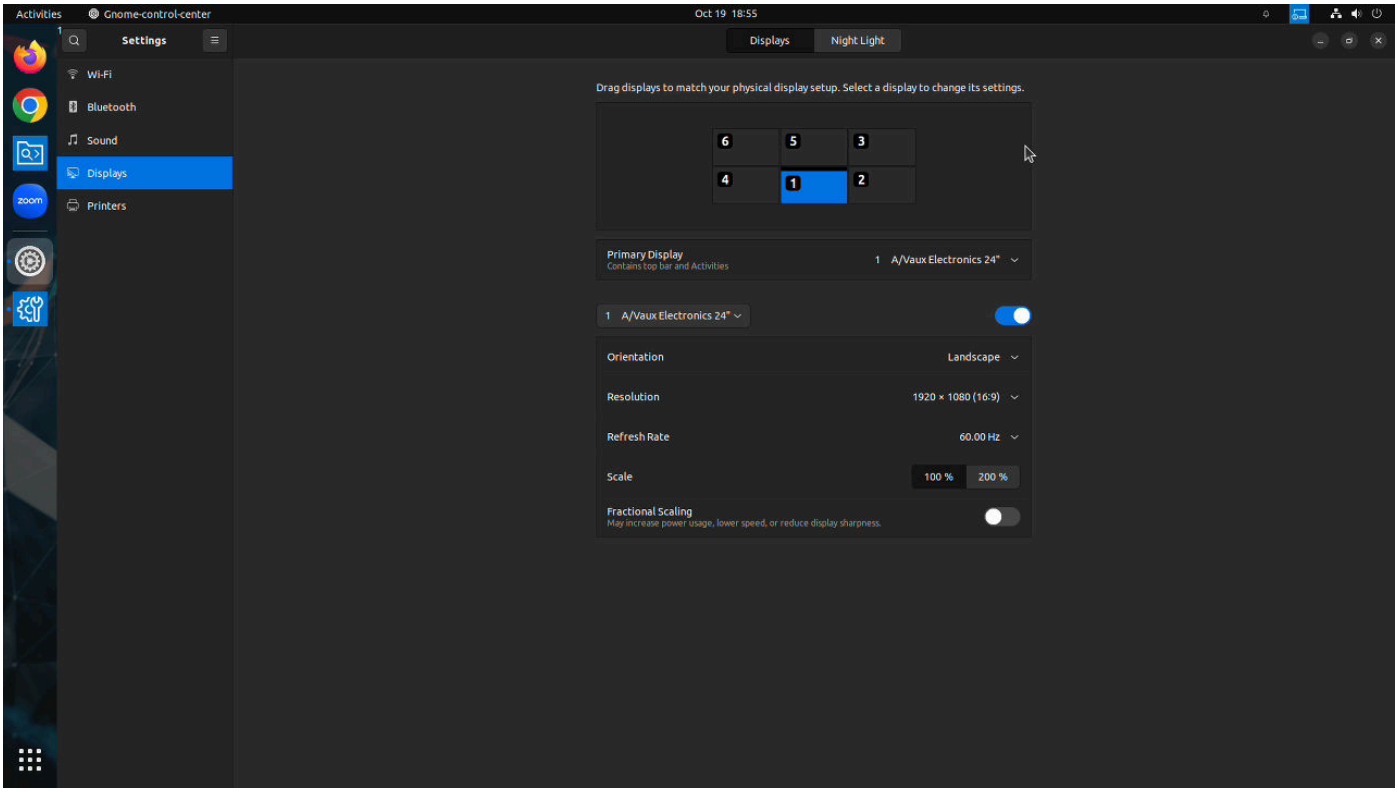


Figure 152. Monitor 1 as primary

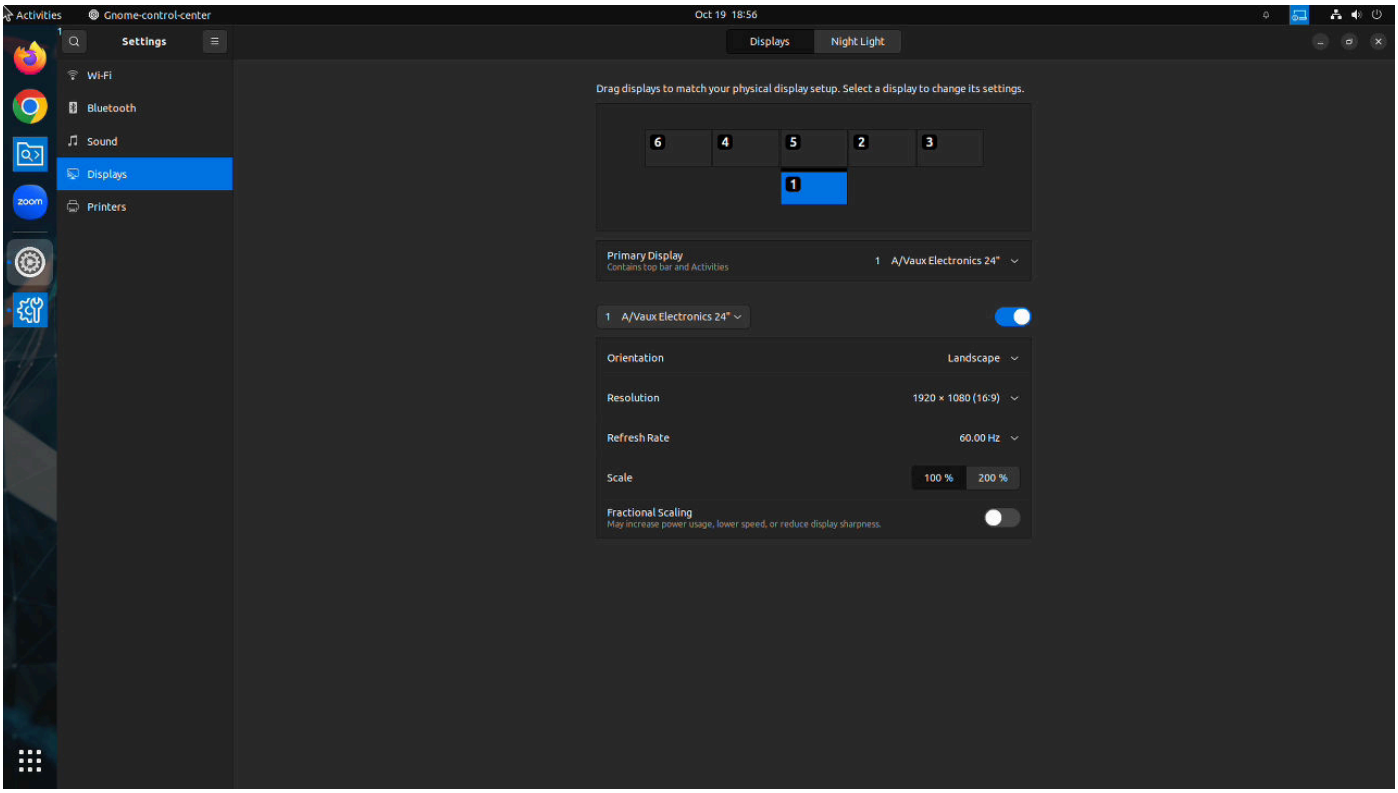


Figure 153. Monitor 1 as primary

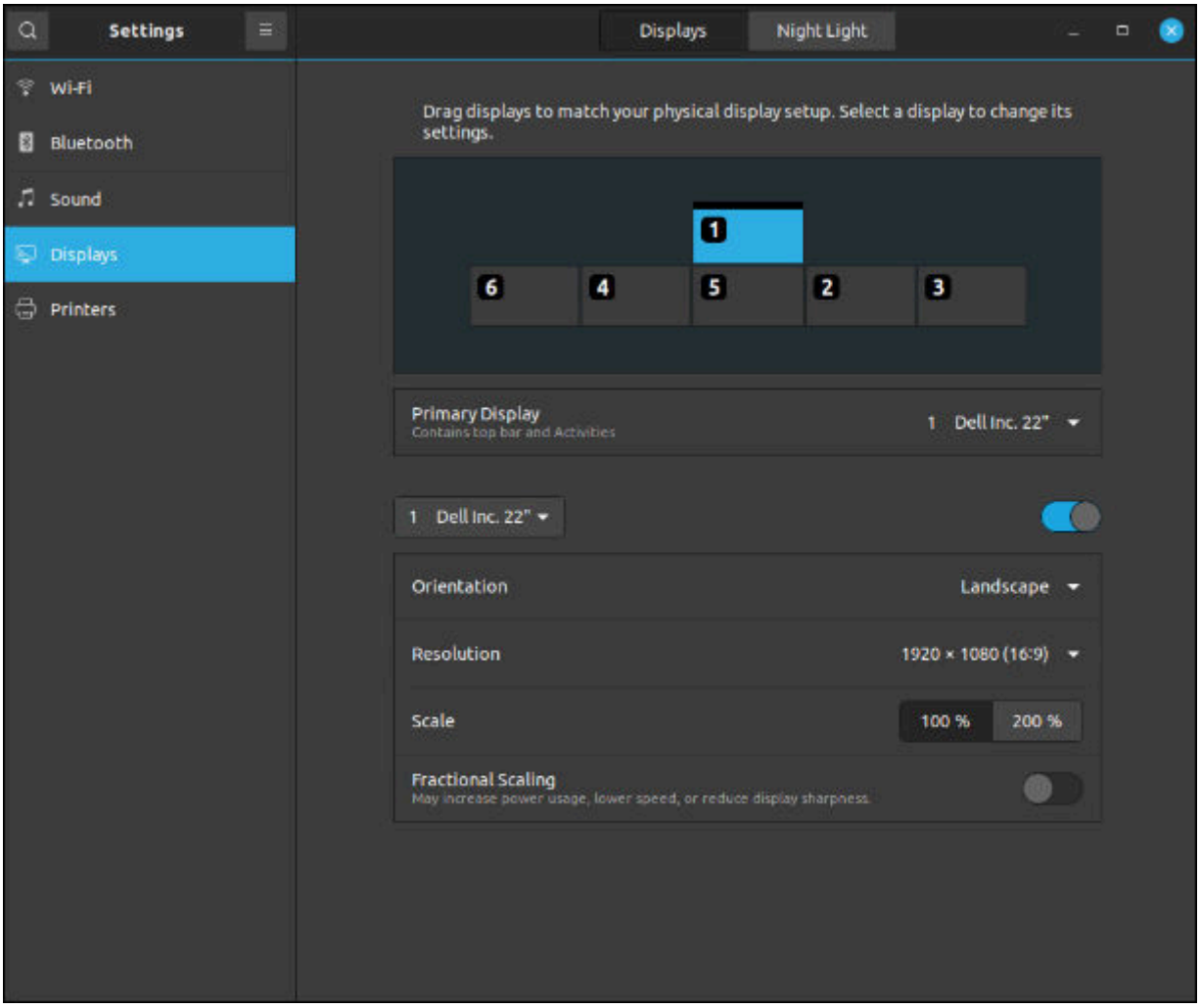


Figure 154. Monitor 1 as primary

Example 6 - Six Display Monitor with M2 as primary along with Portrait settings

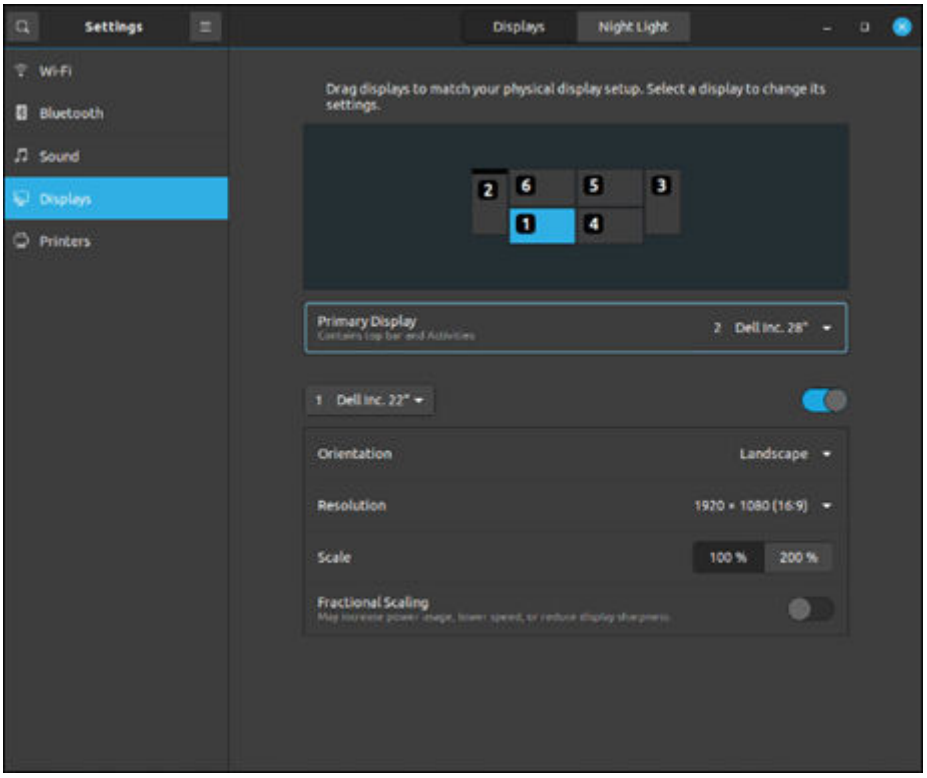


Figure 155. Monitor 1 Settings

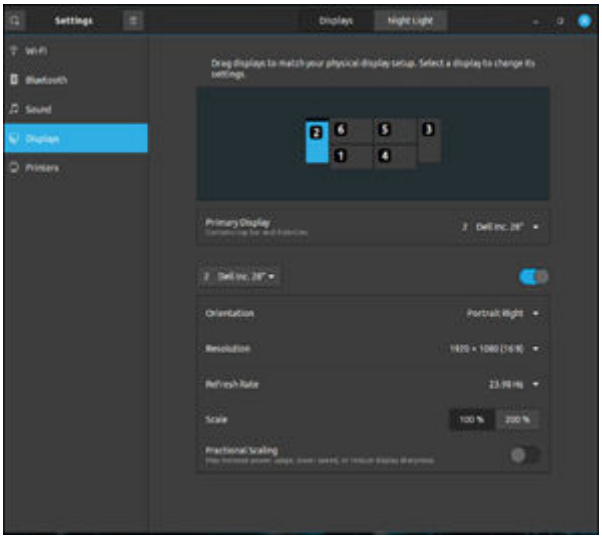


Figure 156. Monitor 2 Settings

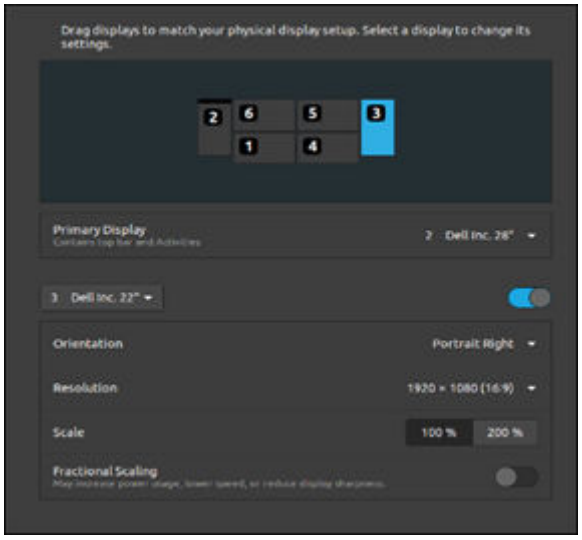


Figure 157. Monitor 3 Settings

Example 7 - Device settings with 6 monitors with different resolution

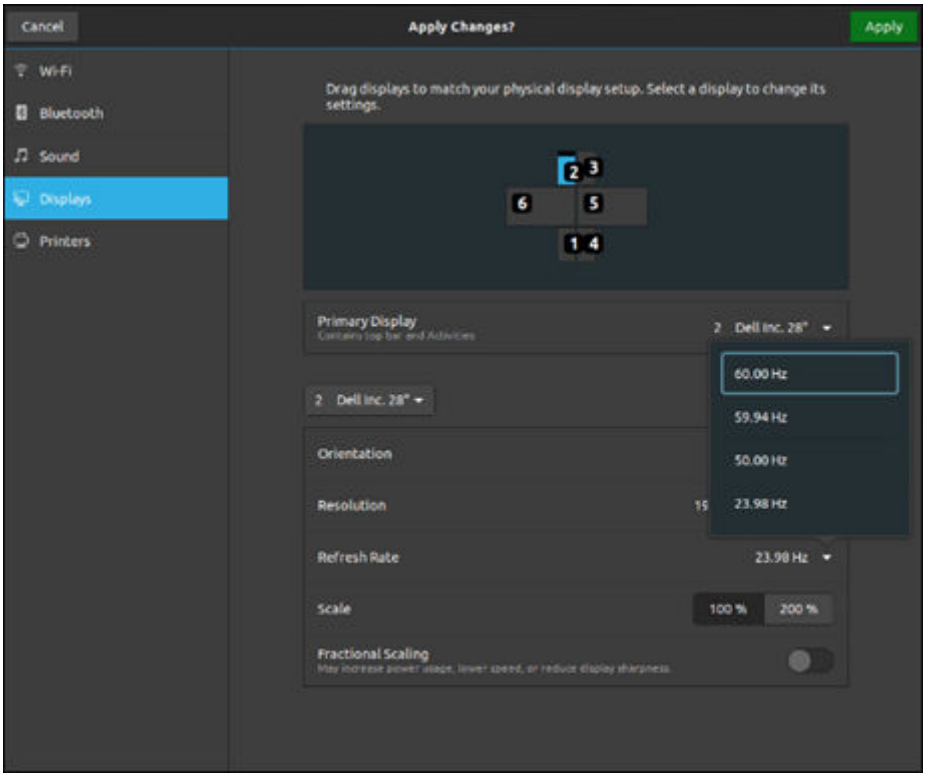


Figure 158. Monitor 2

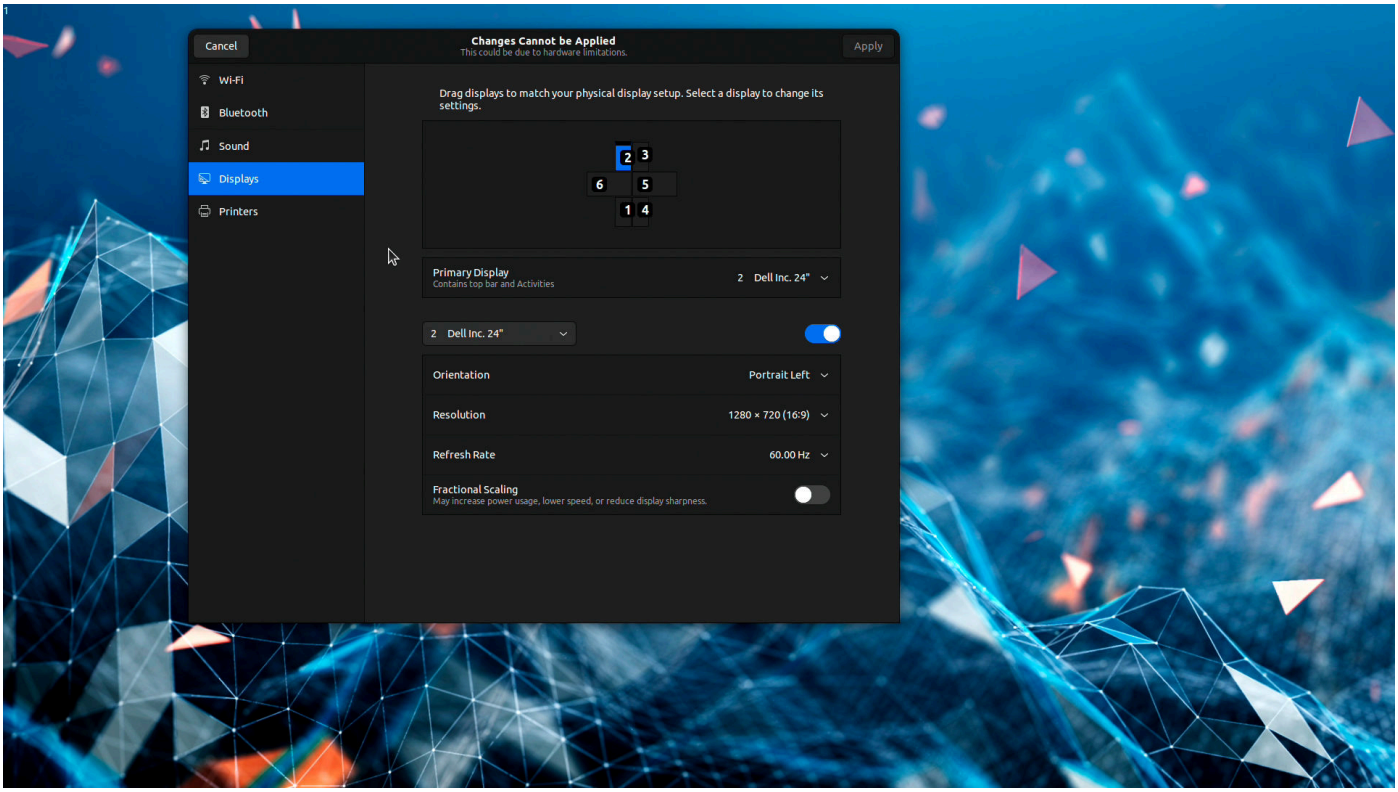


Figure 159. Monitor 2

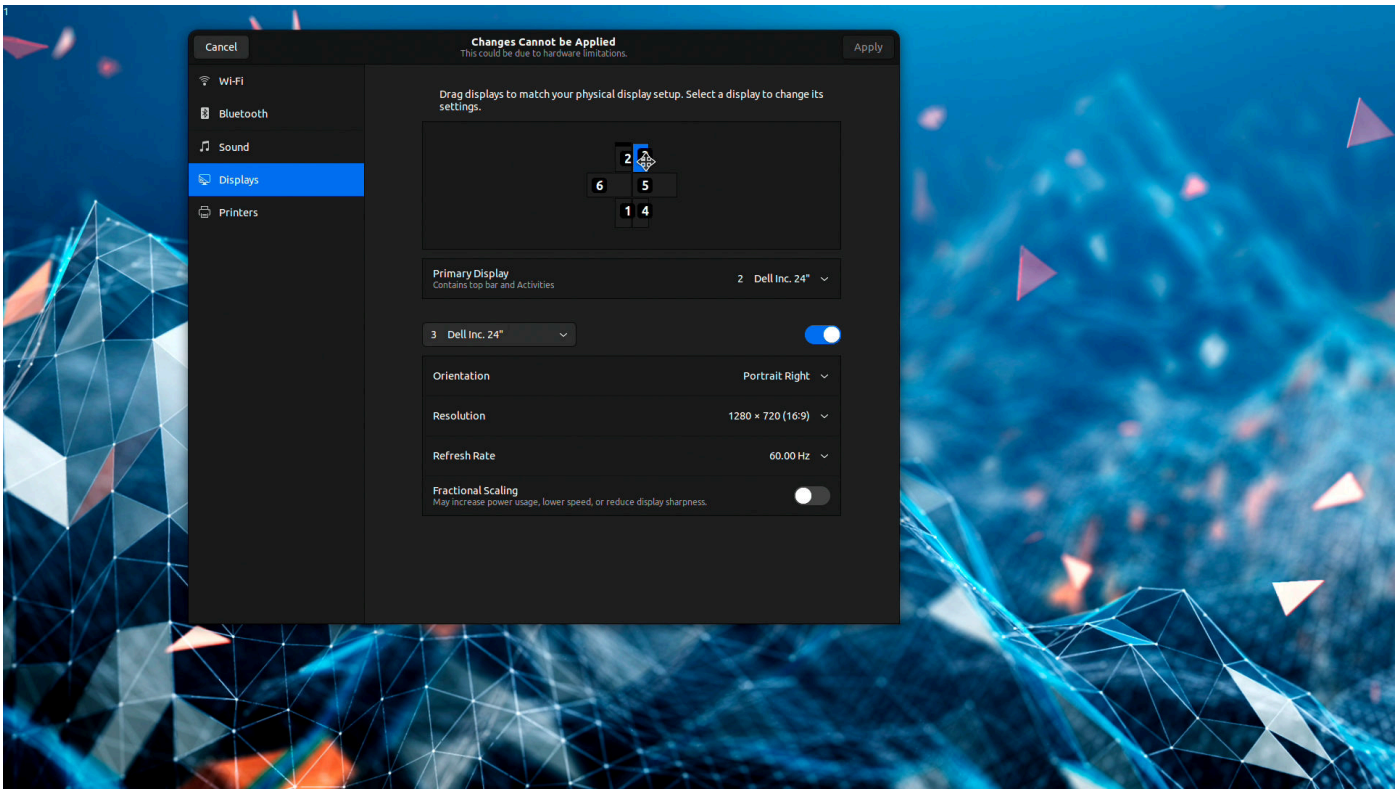


Figure 160. Monitor 3

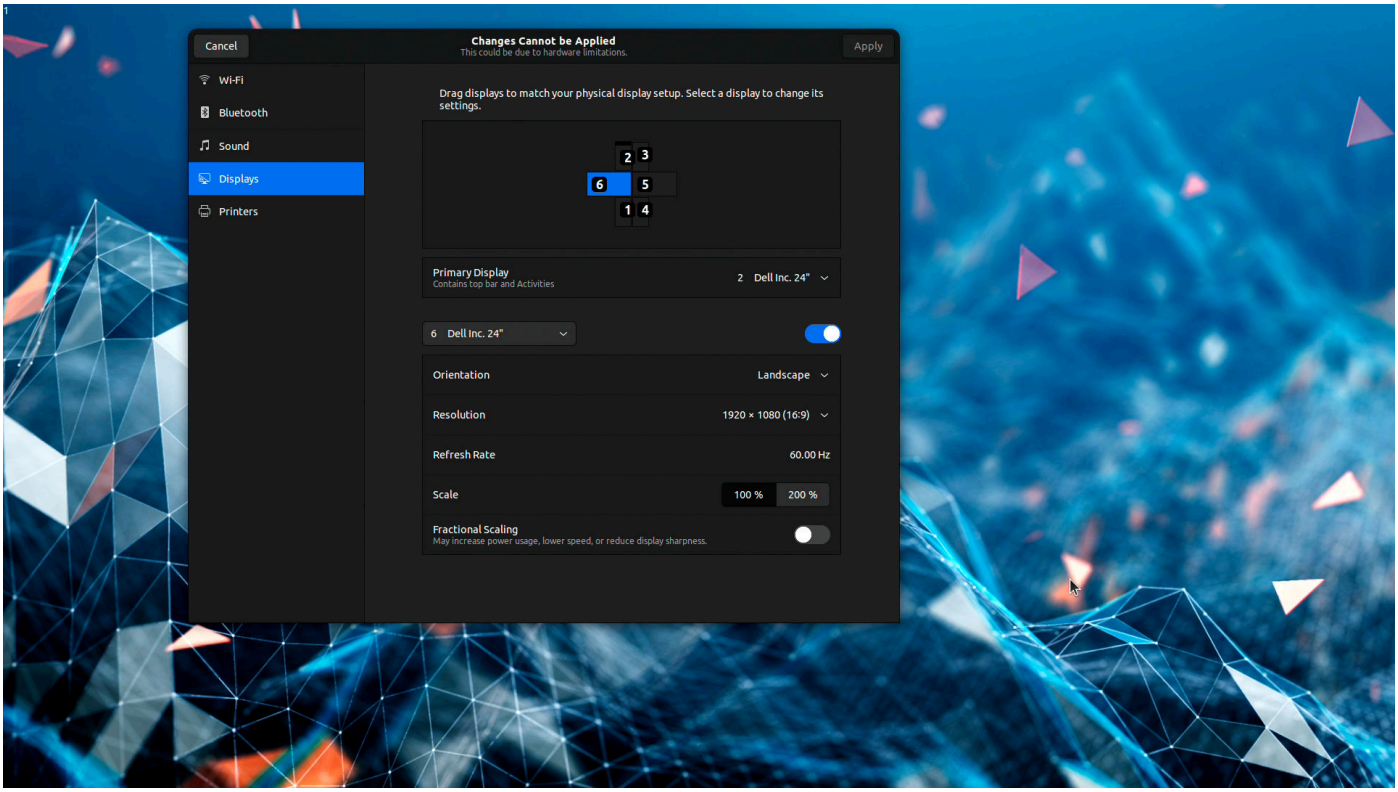


Figure 161. Monitor 6

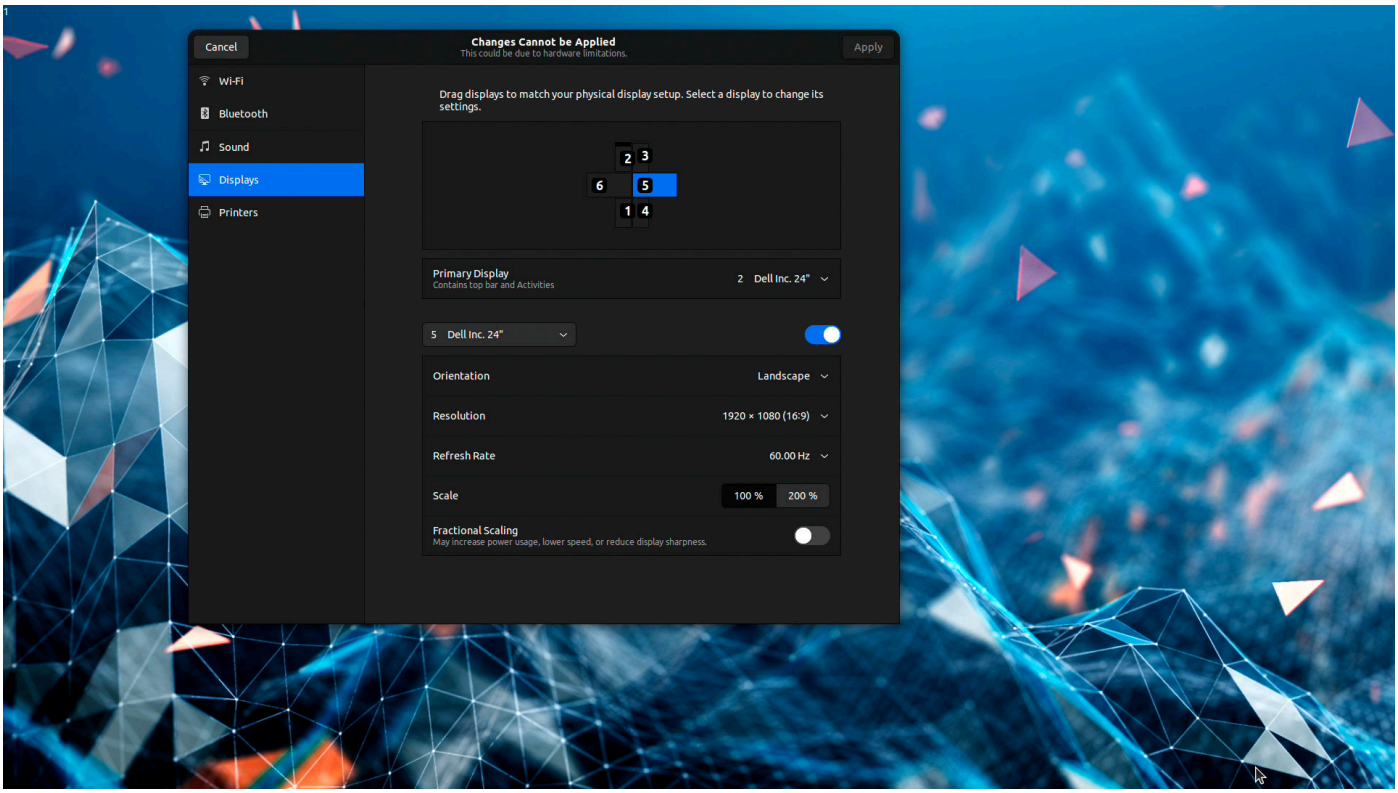


Figure 162. Monitor 5

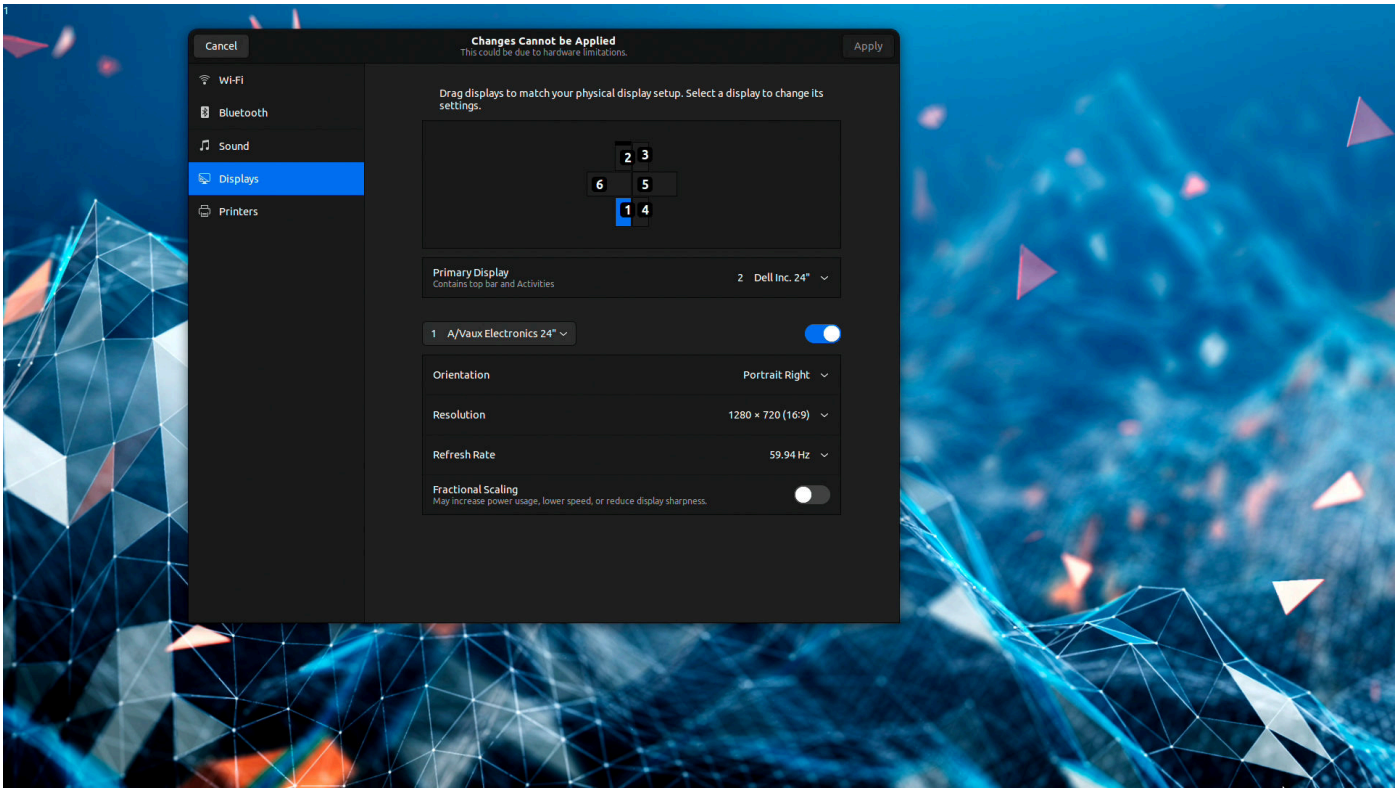


Figure 163. Monitor 1

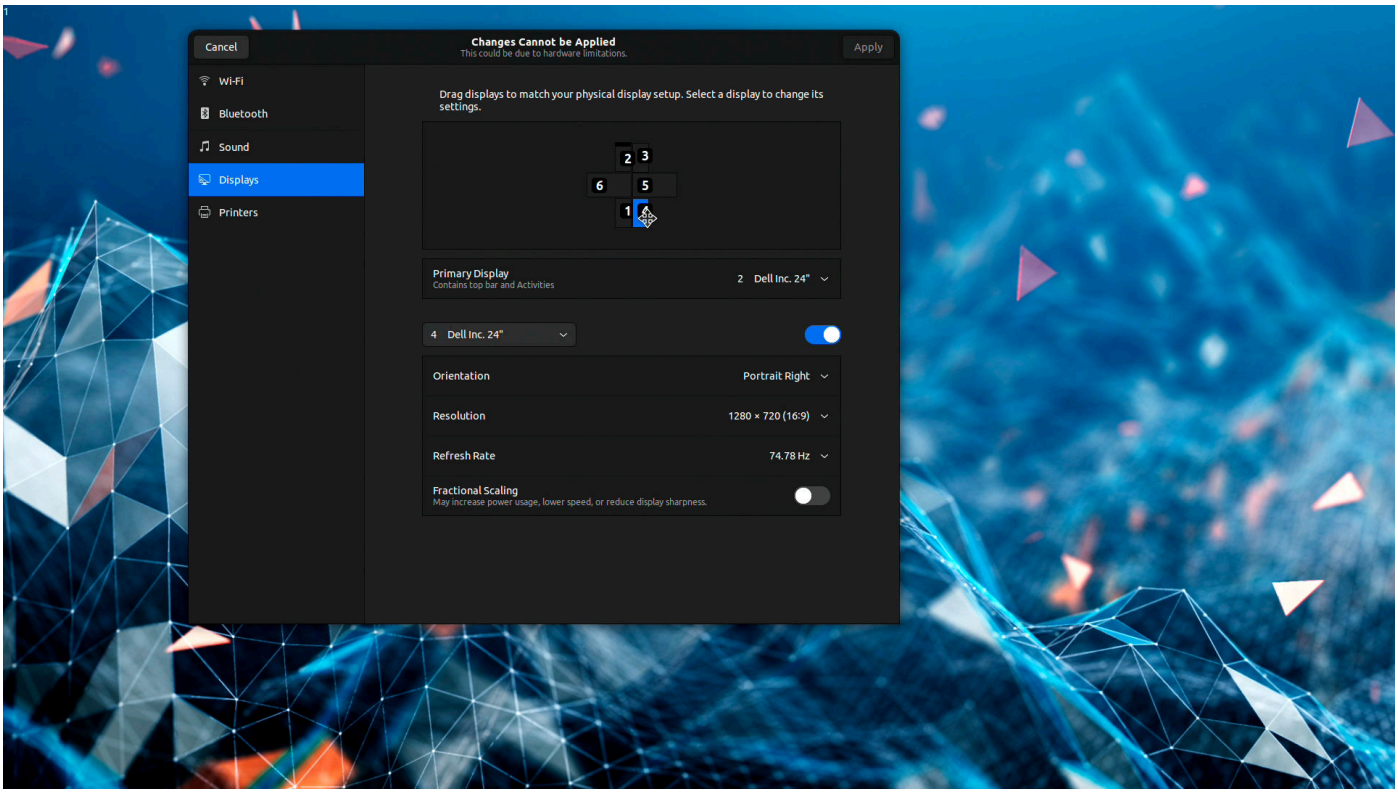


Figure 164. Monitor 4

Configuring Display Settings using Wyse Management Suite

You can configure the display settings using Wyse Management Suite.

Prerequisites

Enable the **Monitor Settings** under **Account Privileges**.

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Acount Privileges**.
6. Select **Customize** in Privilege Level.
7. Enable the **DHC Apps**, **Device Settings**, and then **Monitor Settings**. By default, the **Monitor Settings** option is disabled.

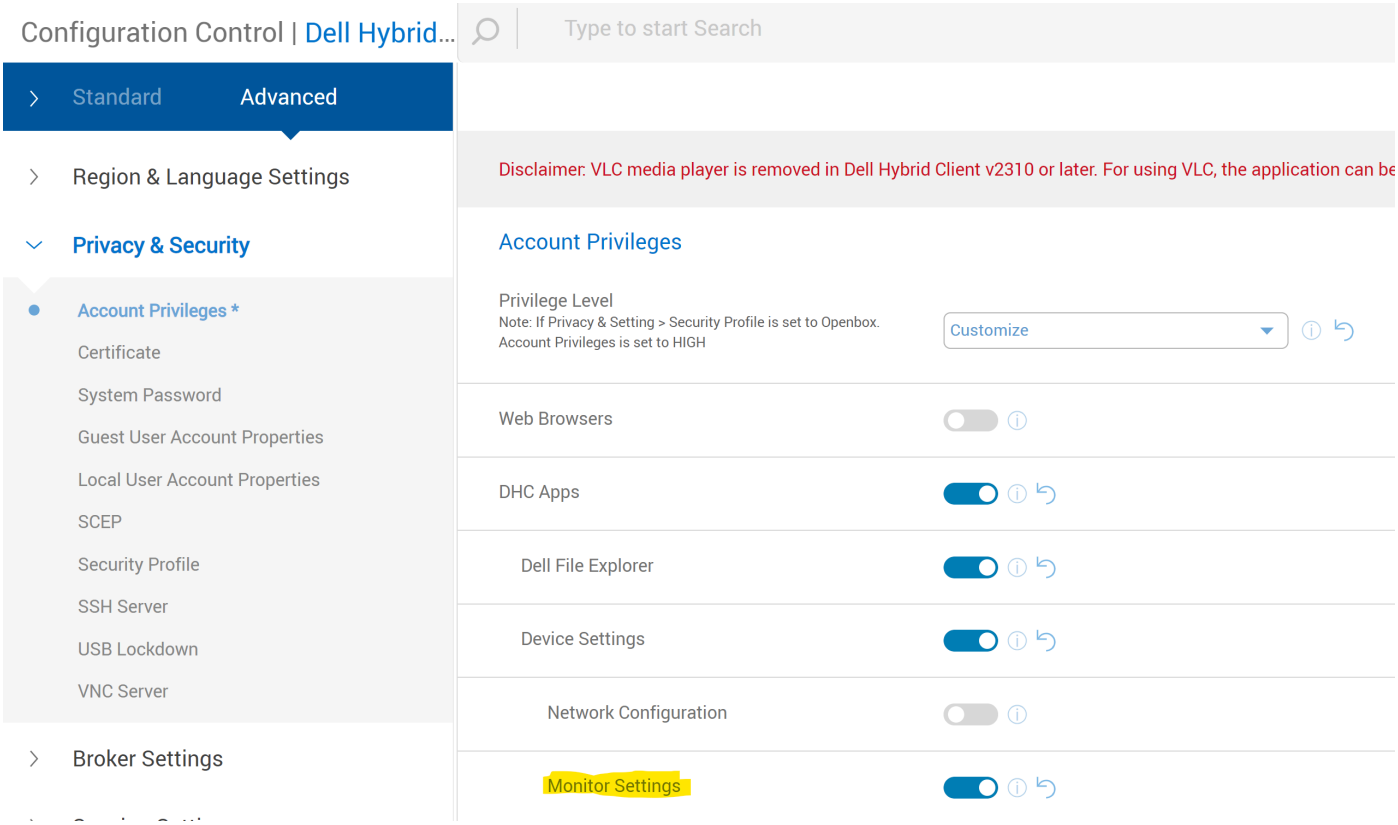


Figure 165. Account Privileges

NOTE: Once the Privilege is set as customized, by default all options are disabled. You must to enable the options as per your requirement. For Example, If you require Dell File Explorer, then you must enable it as in above image. If you want to disable the browser, then you must disable it as in above image.

Configuring Single Display Settings from Wyse Management Suite

You can configure Single Display Settings from Wyse Management Suite.

1. Click **Advanced** Tab.
2. Click **Single/Multi Display settings** under **Peripheral Management**.

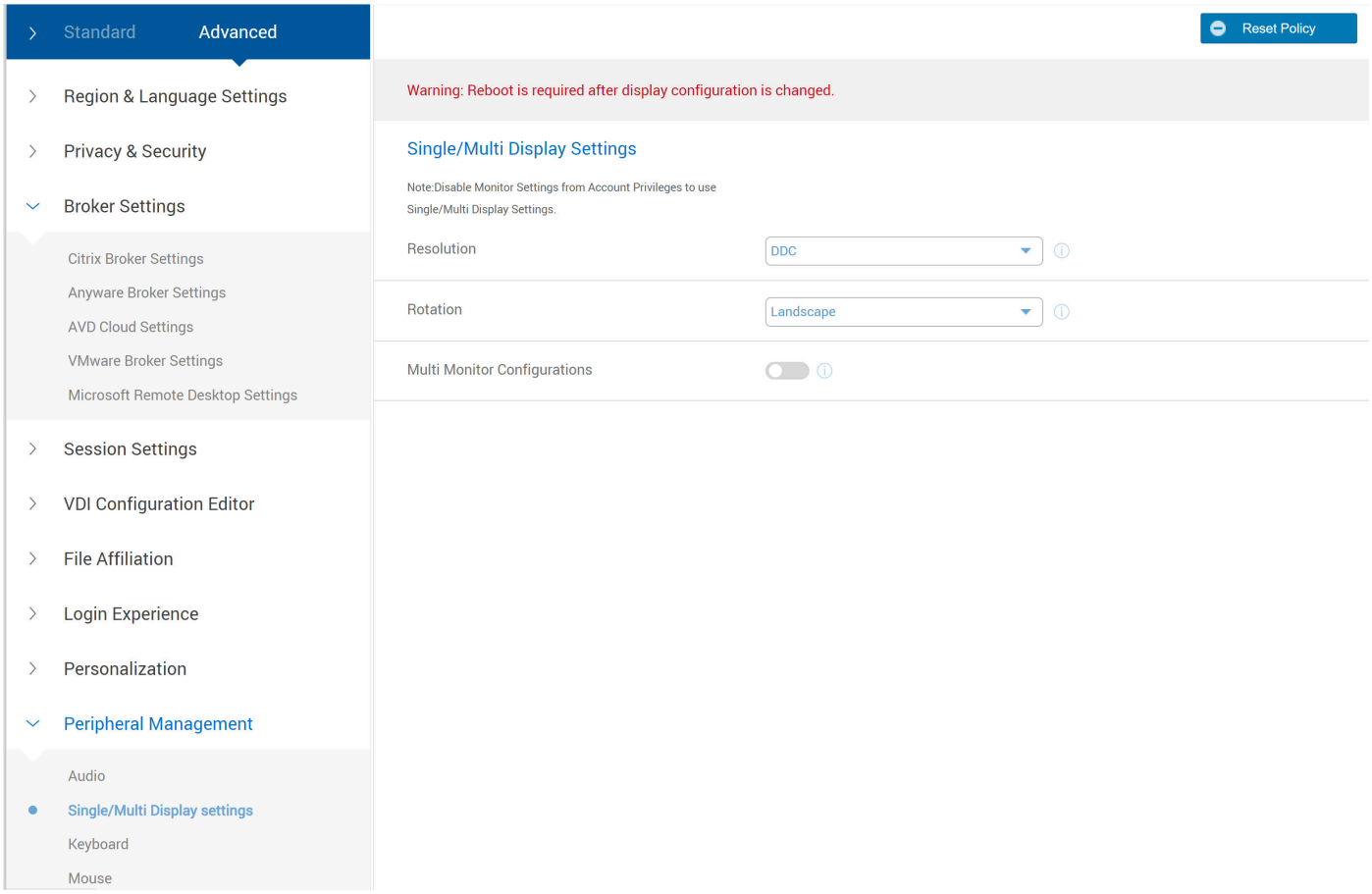


Figure 166. Single/Multi Display Settings

You can configure the following settings:

- **Resolution:** Dell Hybrid Client supports up to 4K monitor resolution. If you want to change your monitor resolution, then you must select one from the drop-down list.

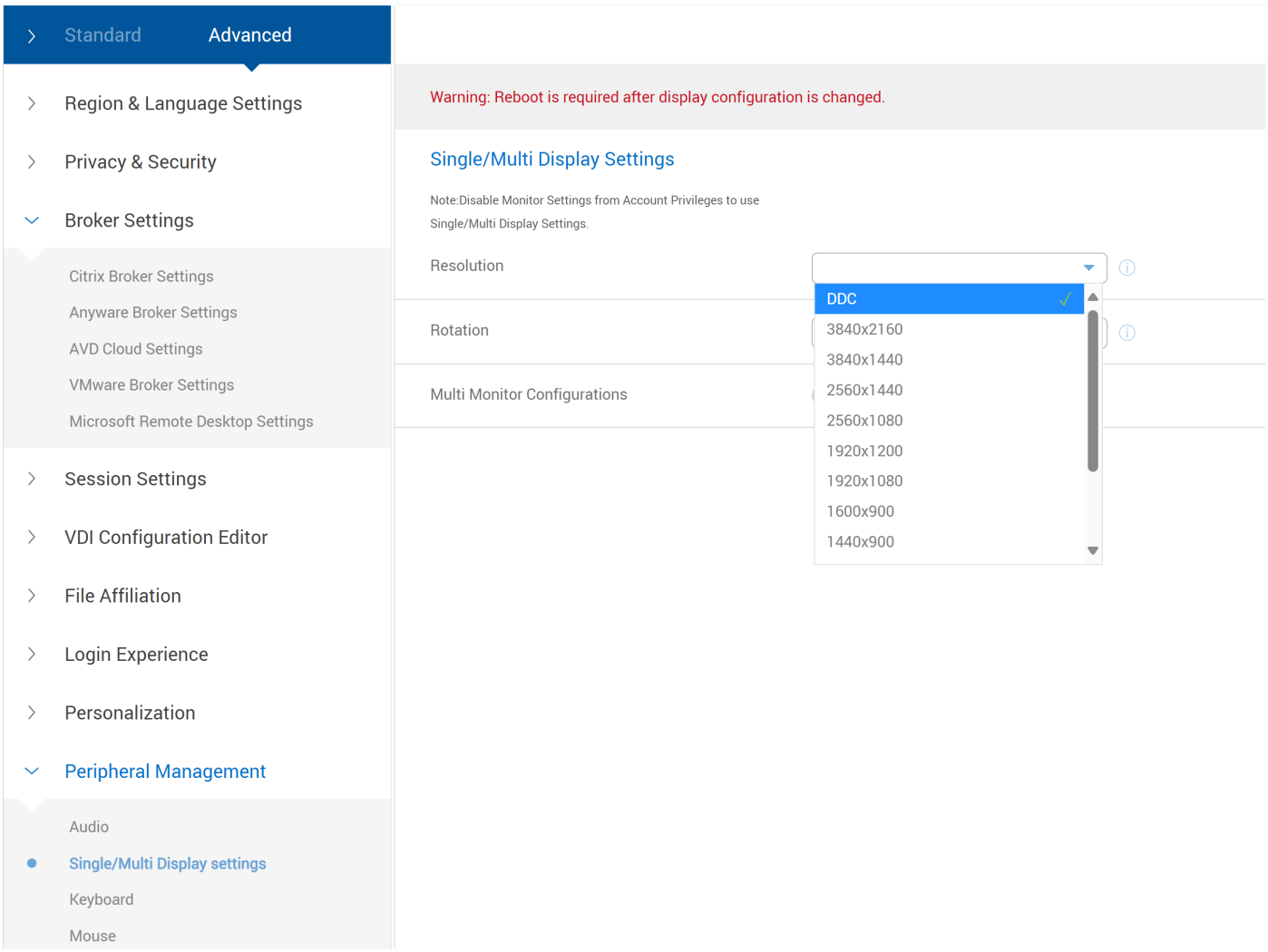


Figure 167. Resolution

- **Rotation:** You can set monitor rotation type as Landscape or Portrait.

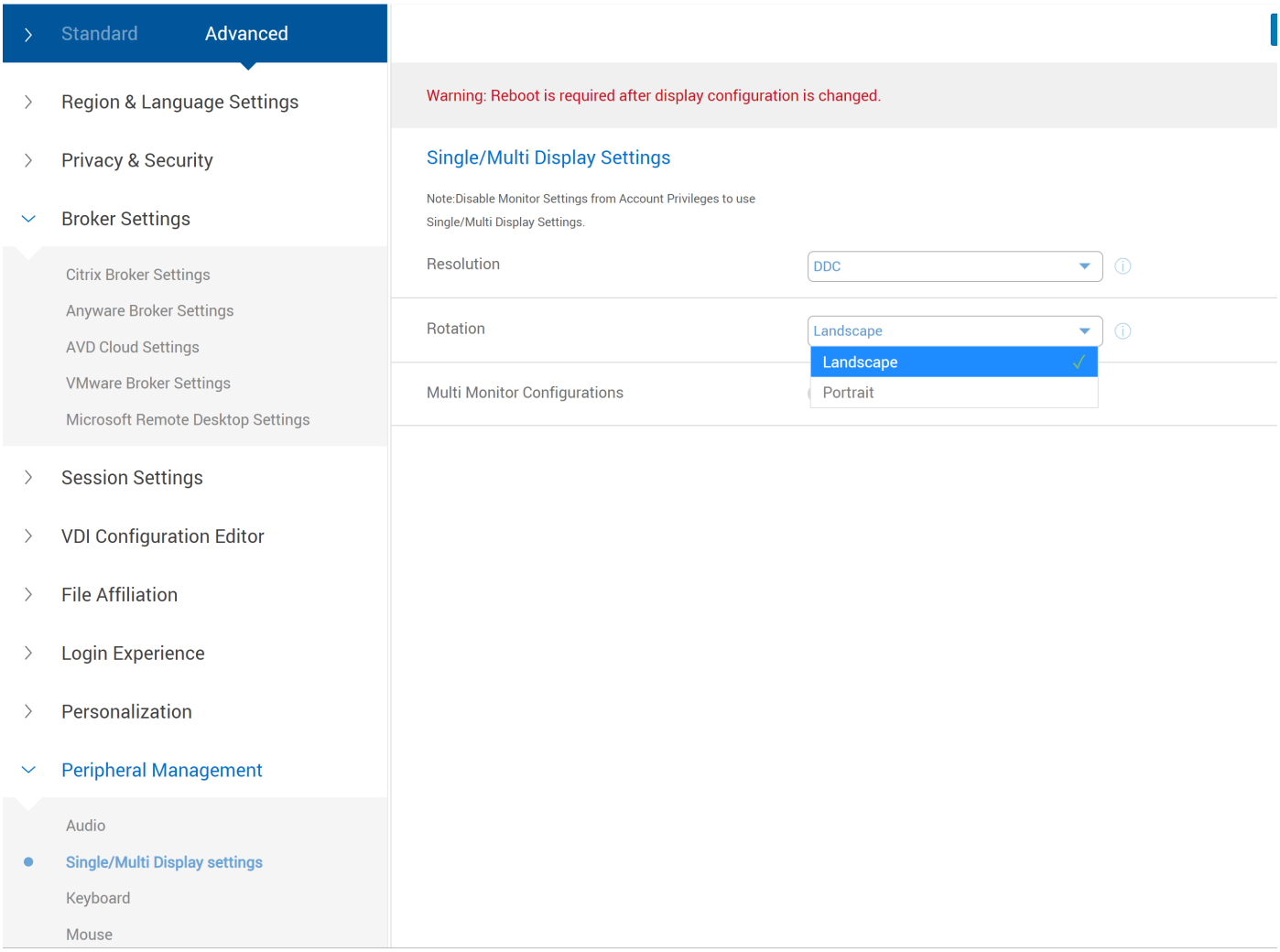


Figure 168. Rotation

Configuring Multi Display Settings from Wyse Management Suite

You can configure Multi Display Settings from Wyse Management Suite.

1. Go to **Advanced** tab.
2. Click **Single/Multi Display settings** under **Peripheral Management**.
3. Enable **Multi Monitor Configurations**.

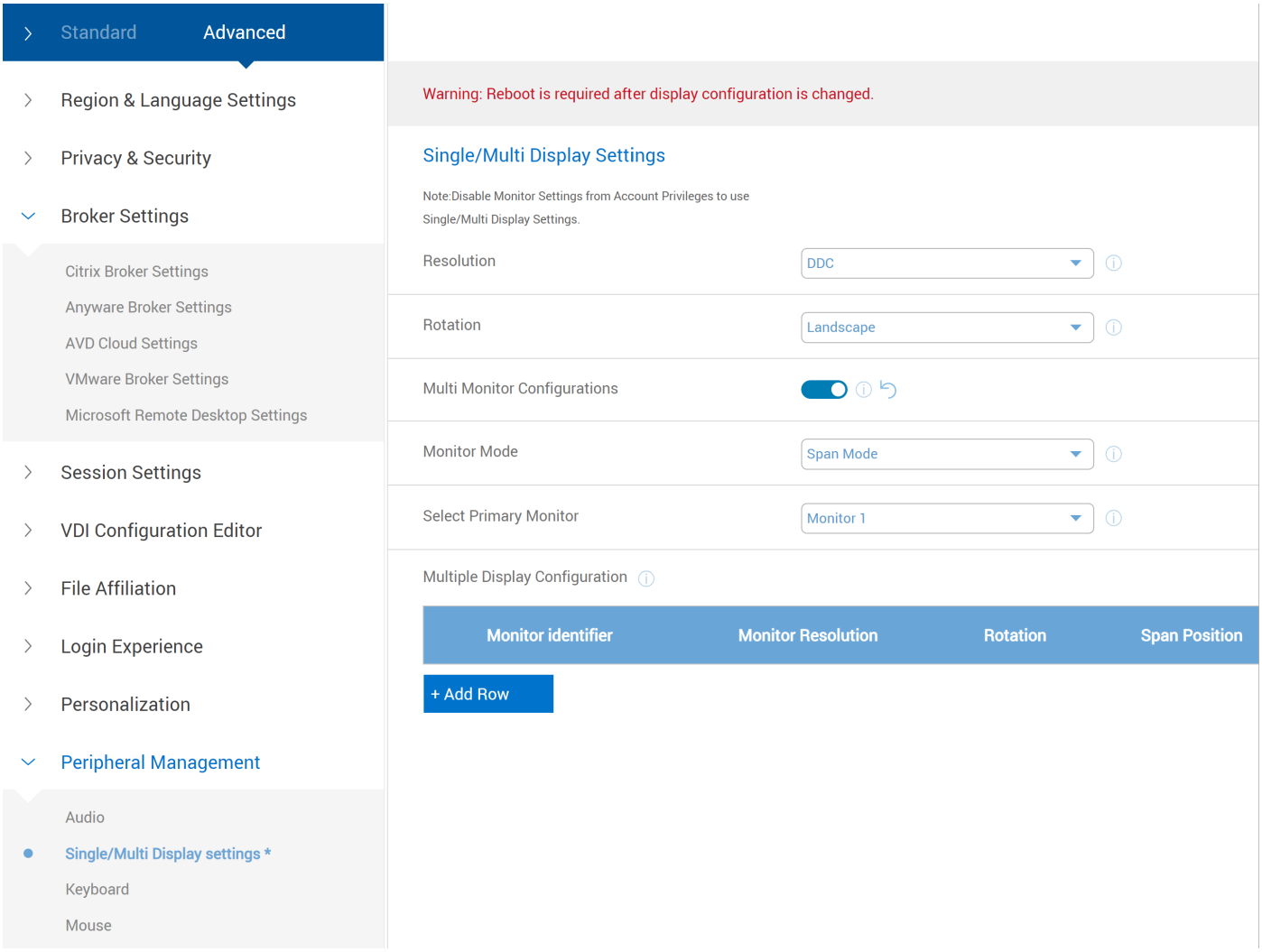


Figure 169. Multi Monitor Configurations

4. In Monitor Mode, you can select any of the two options:
   - **Mirror Mode:** If you want to see same content across two monitors, then **Mirror Mode** must be selected. Mirror mode is applied only when two monitors are plugged. Mirror Mode is applicable when exactly two monitors are connected.

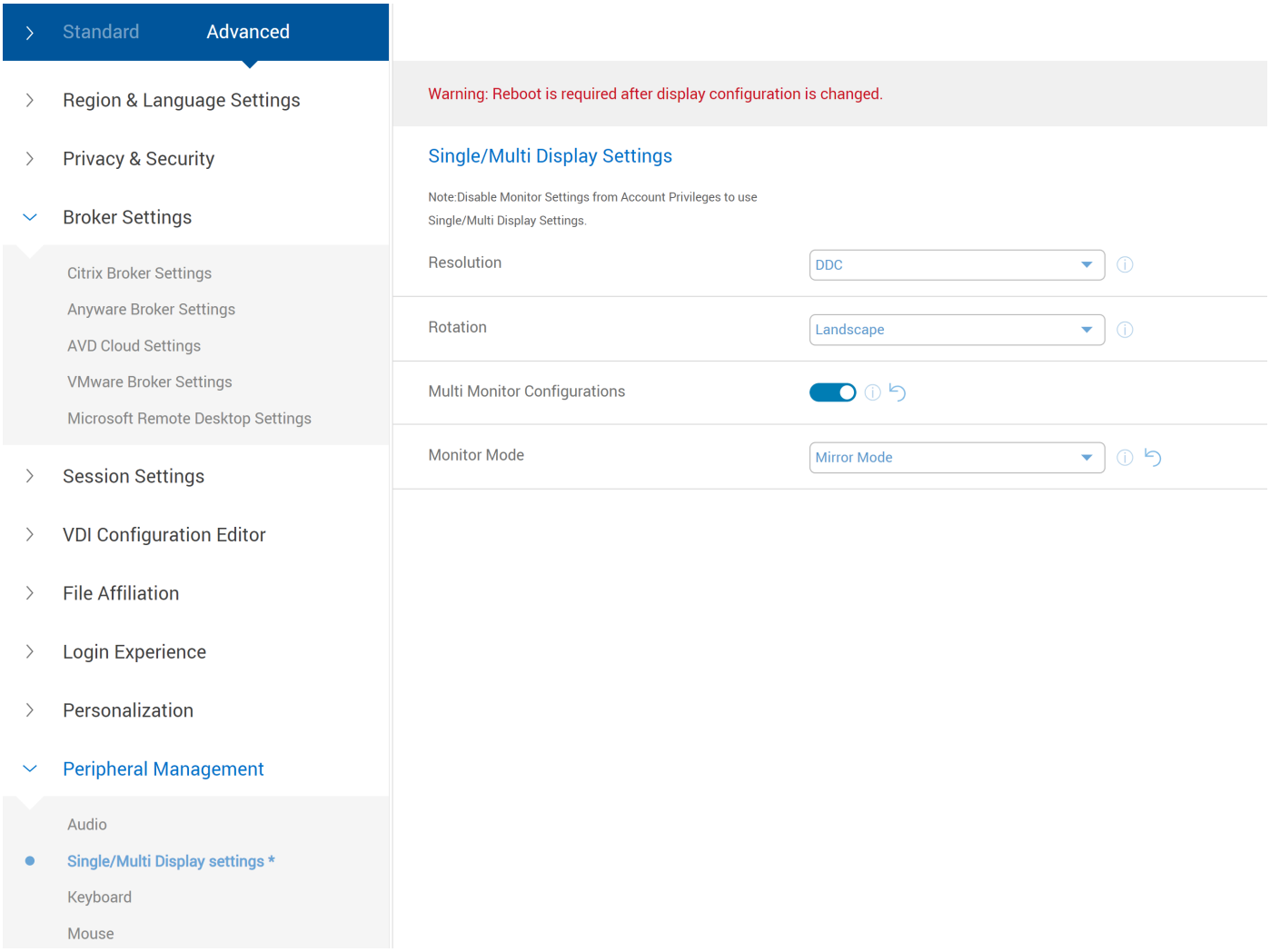


Figure 170. Mirror Mode

- **Span Mode:** When you want to use multiple displays with different content, then Span mode must be selected.

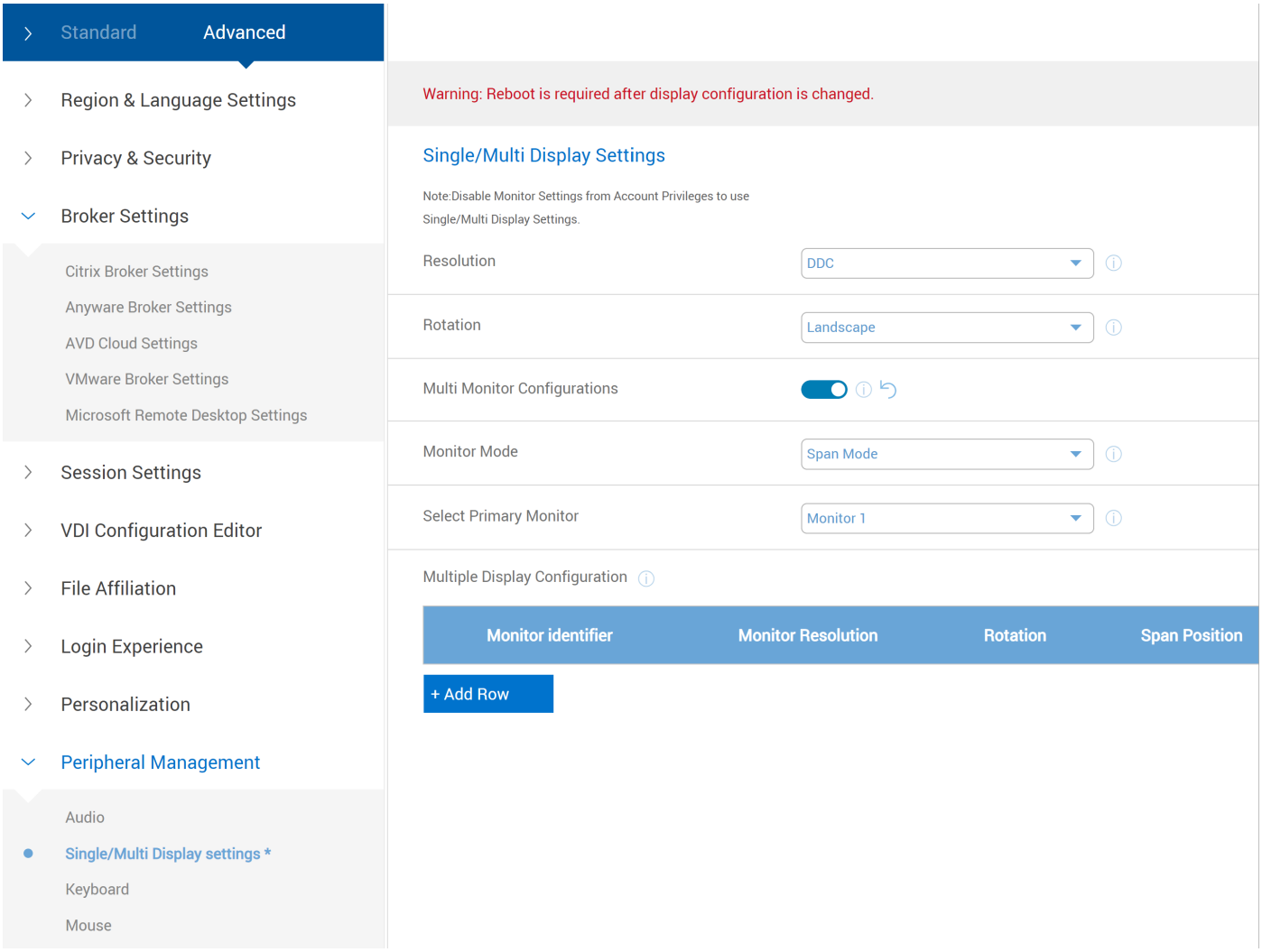


Figure 171. Span Mode

You must configure the following options:

a. **Select Primary Monitor:** Dell Hybrid Client supports up to 6 Monitors.
   i. You must set the primary monitor before configuring other monitors under the **Multiple Display Configuration** tab.
   ii. You must check if the selected primary monitor is not selected in the **Monitor identifier** section under **Multiple Display Configuration** tab.

   Example: If you have 4 monitors, then one is primary and other three is selected under **Monitor identifier** in **Multiple Display Configuration** tab.

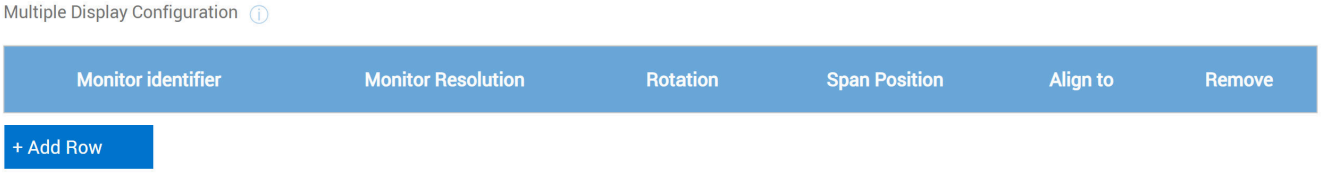


Figure 172. Multiple Display Configuration

b. **Monitor identifier:**
   i. You must select **Monitors** for setting up Resolution, Rotation, and Position.
   ii. You must check if the primary monitor is not selected under the **Monitor identifier**.
c. **Monitor Resolution:** Dell Hybrid Client supports up to 4K Monitors.
   i. If you want to change your monitor resolution, then you must select one from the drop-down list.

ii. If an unsupported monitor resolution is selected, then that monitor goes to DDC.

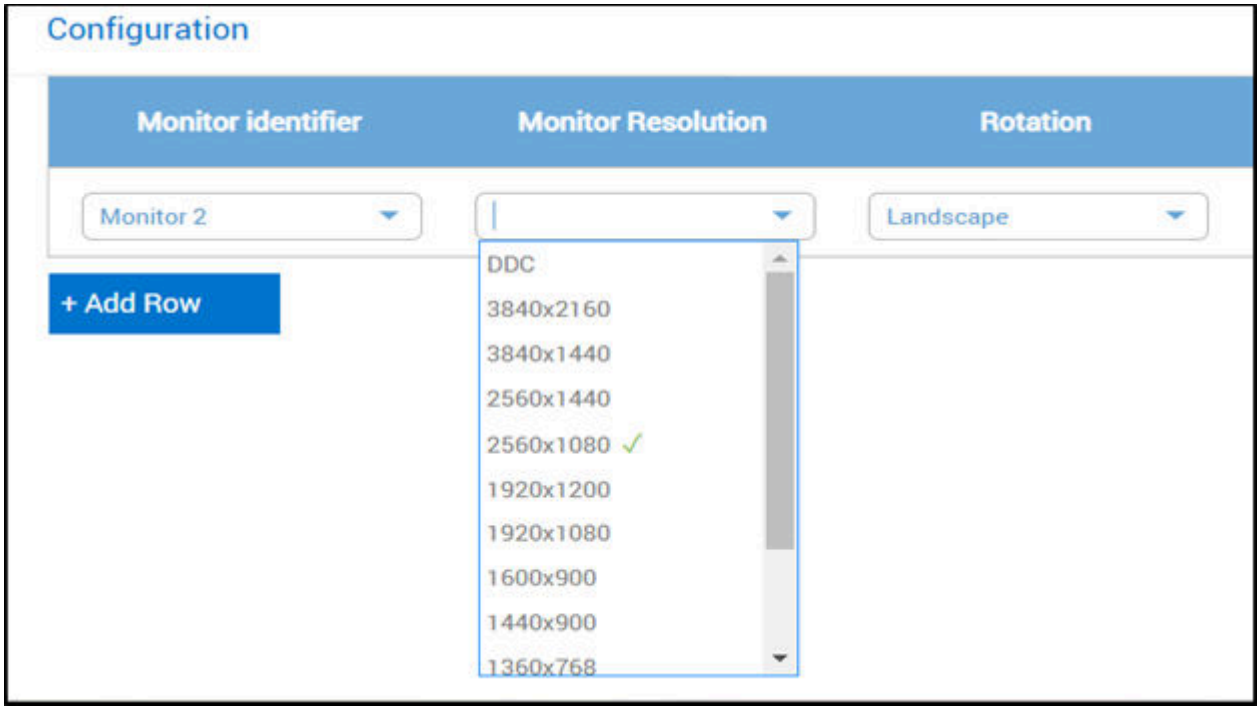


Figure 173. Monitor Resolution

d. **Rotation:**

i. You can provide the orientation of the selected monitor by selecting Portrait or Landscape under **Rotation**.

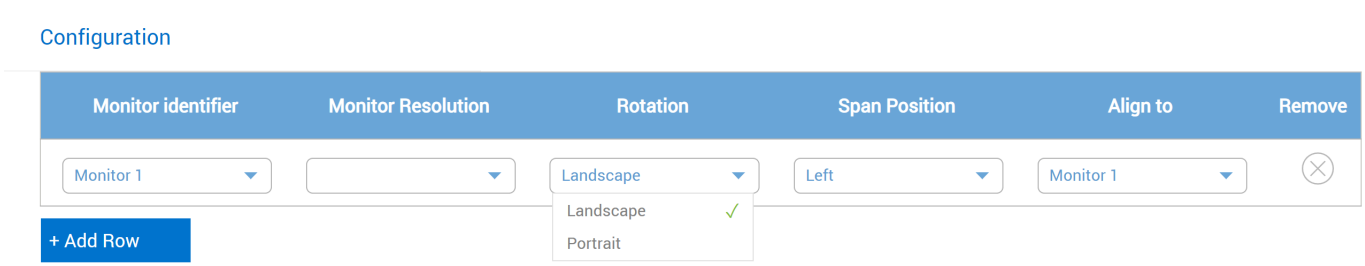


Figure 174. Rotation

e. **Span Position:**

i. You must select position at which the monitor must be displayed in reference with **Align to** section. For more information about how to set Span Position, see example.

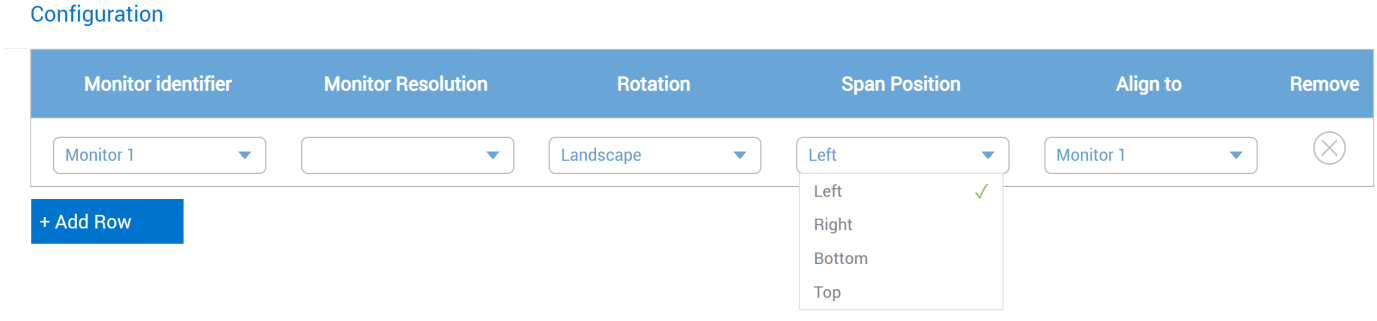


Figure 175. Span Position

f. **Align to:**

i. You must input span position according to which monitor. For more details, check example section.

NOTE: Ensure **Span Position** and **Align to** details are precise to Monitor setup. Refer below examples of not Precise config according to Multi Monitor setup.



Figure 176. Multi Monitor setup

Configuration

Monitor identifier	Monitor Resolution	Rotation	Span Position	Align to	Remove
Monitor 2	DDC	Landscape	Left	Monitor 1	
Monitor 3	DDC	Landscape	Left	Monitor 1	

+ Add Row

Figure 177. Monitor 1

Configuration

Monitor identifier	Monitor Resolution	Rotation	Span Position	Align to	Remove
Monitor 2	DDC	Landscape	Left	Monitor 1	
Monitor 3	DDC	Landscape	Left	Monitor 2	

+ Add Row

Figure 178. Monitor 2

Examples for Multi Display Settings from Wyse Management Suite

Example 1 - 2 Monitor Configuration

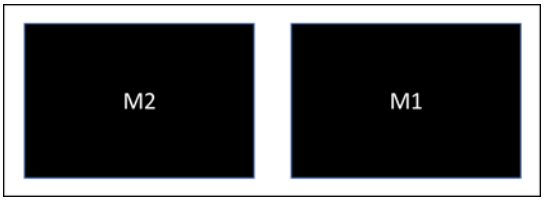


Figure 179. Monitor Position (M1 as Primary)

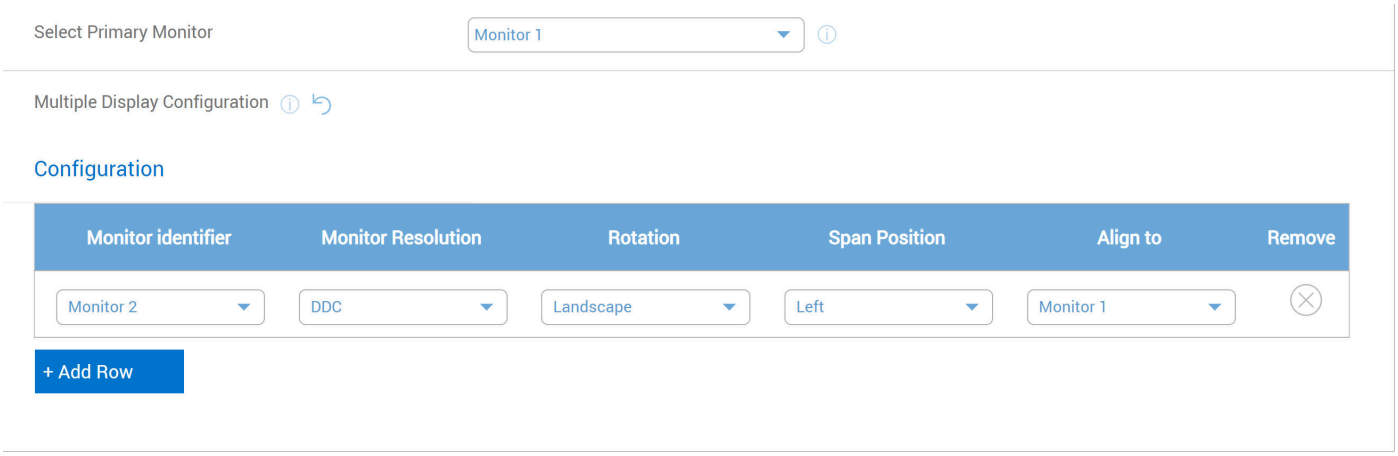


Figure 180. WMS Configuration Page

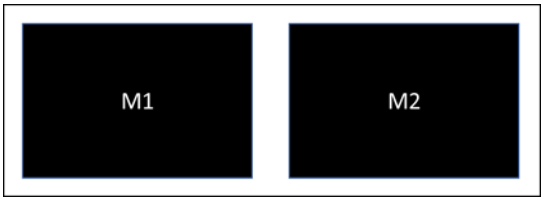


Figure 181. Monitor Position (M2 as Primary)

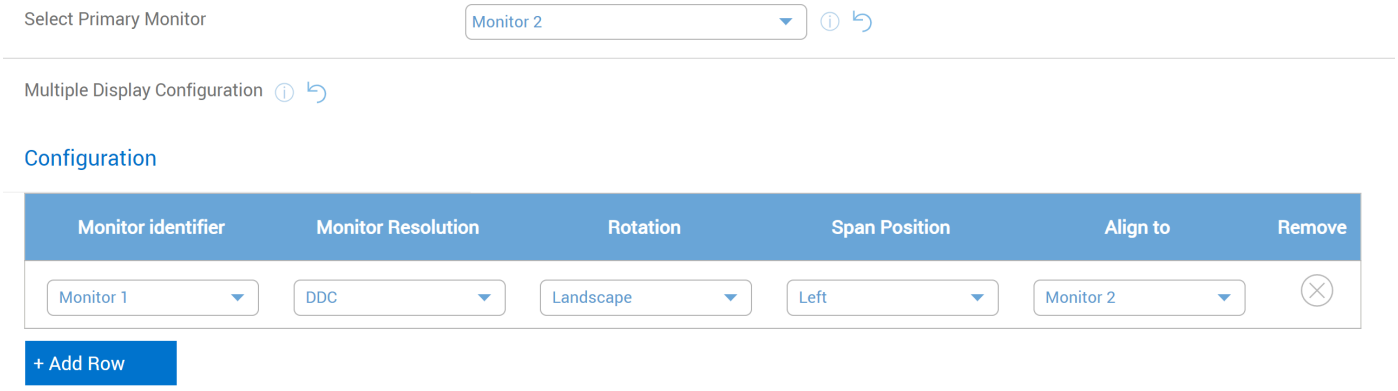


Figure 182. WMS Configuration Page



Figure 183. Monitor Position (M1 as Primary)

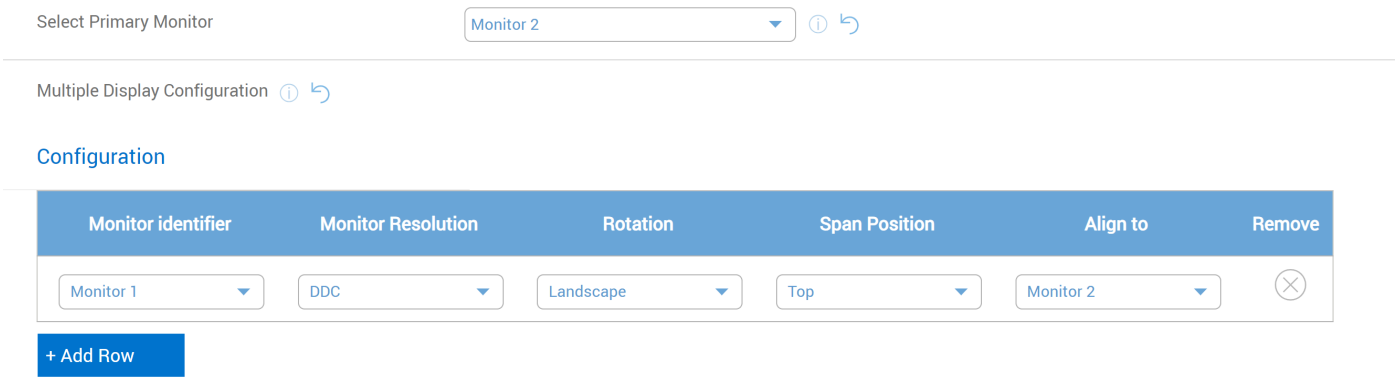


Figure 184. WMS Configuration Page

Example 2 - 3 Monitor Configuration

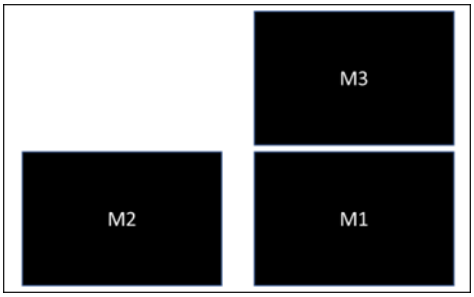


Figure 185. Monitor Position (M3 as Primary)

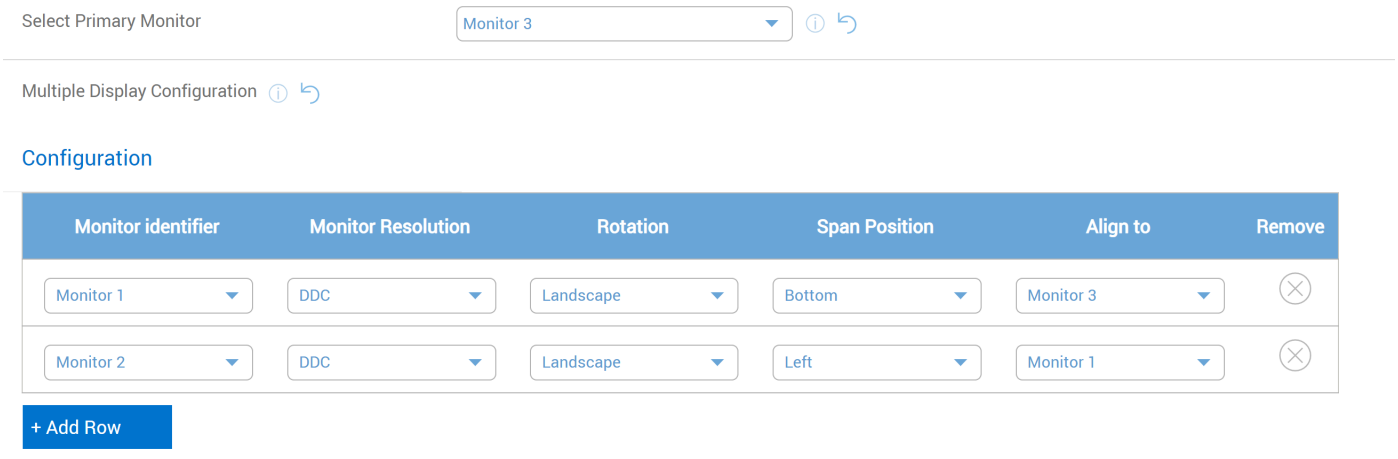


Figure 186. WMS Configuration Page

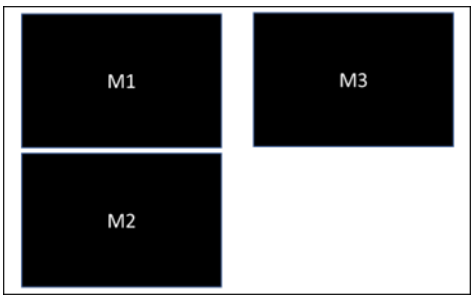


Figure 187. Monitor Position (M1 as Primary)

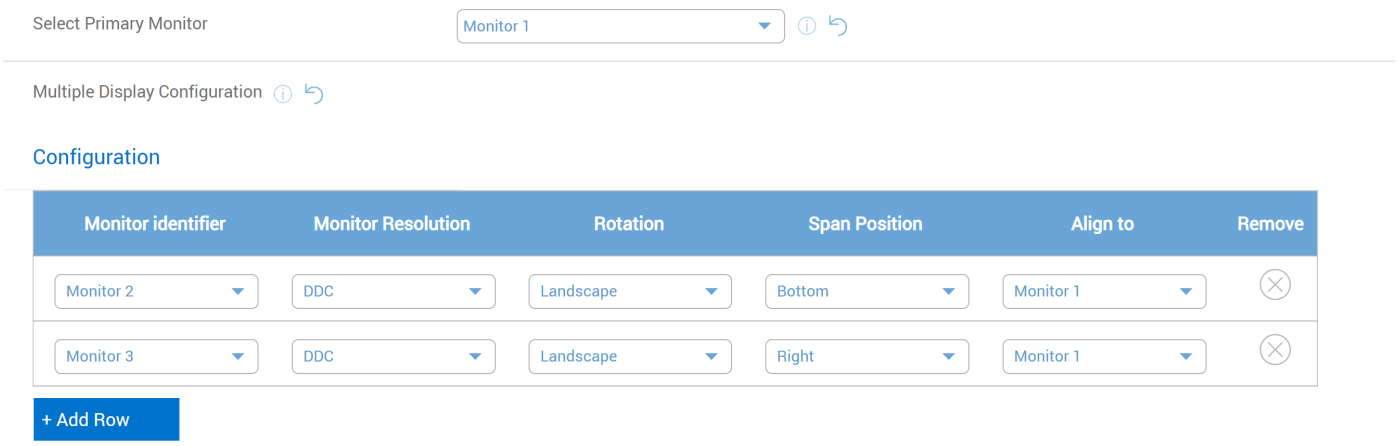


Figure 188. WMS Configuration Page

Example 3 - 5 Monitor Configuration

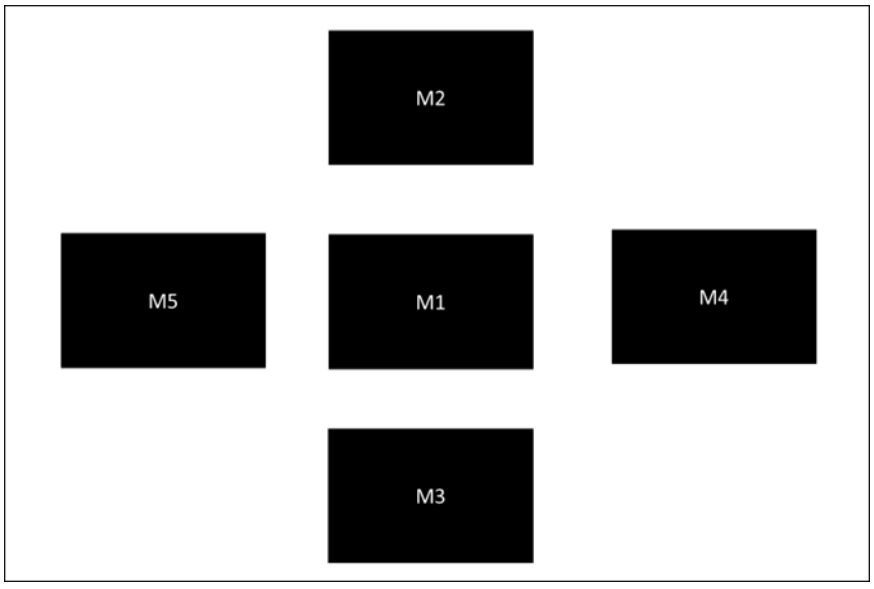


Figure 189. Monitor Position (M1 as Primary)

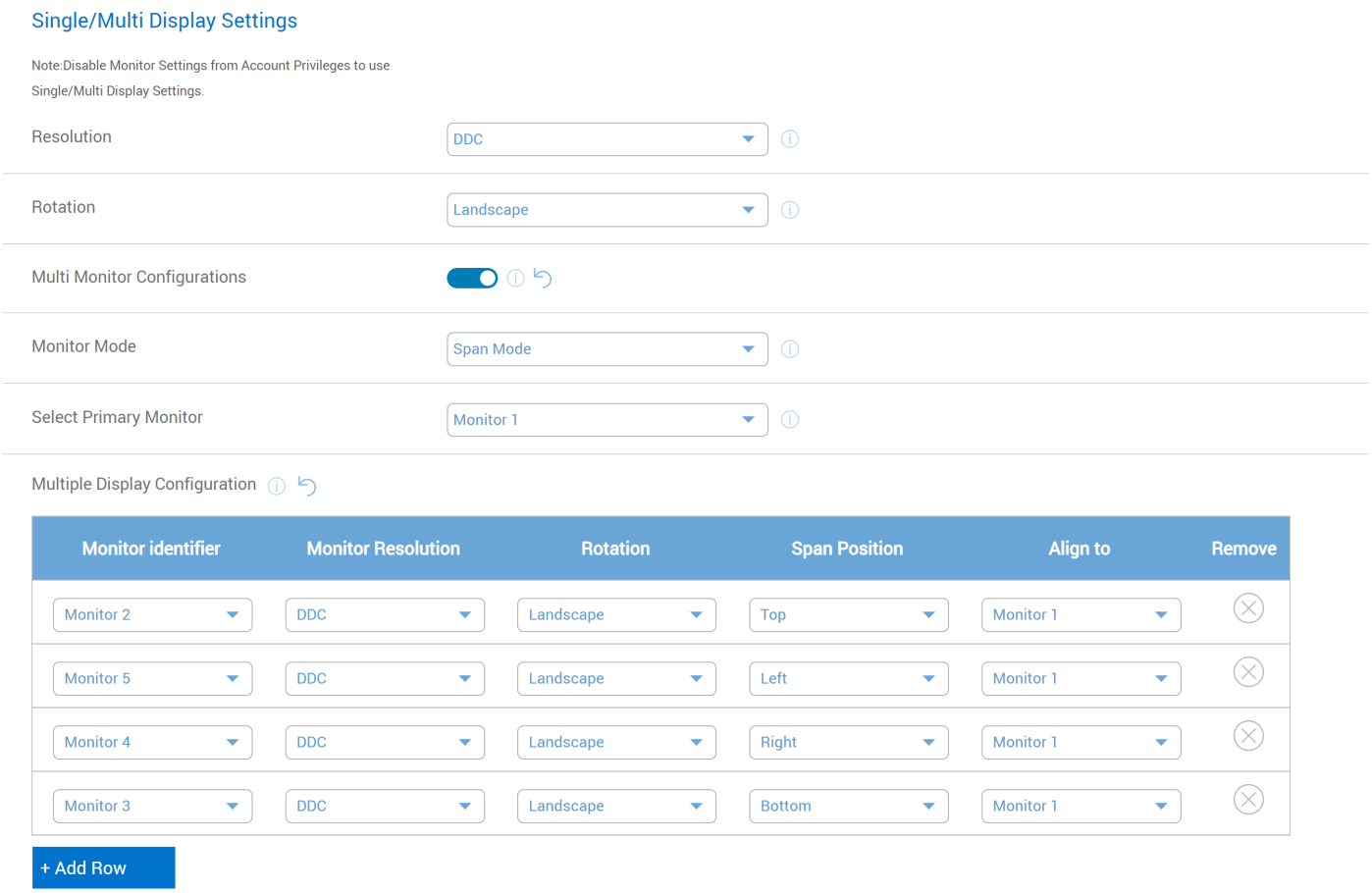


Figure 190. WMS Configuration Page

Example 4 - 5 Monitor Configuration



Figure 191. Monitor Position (M1 as Primary)

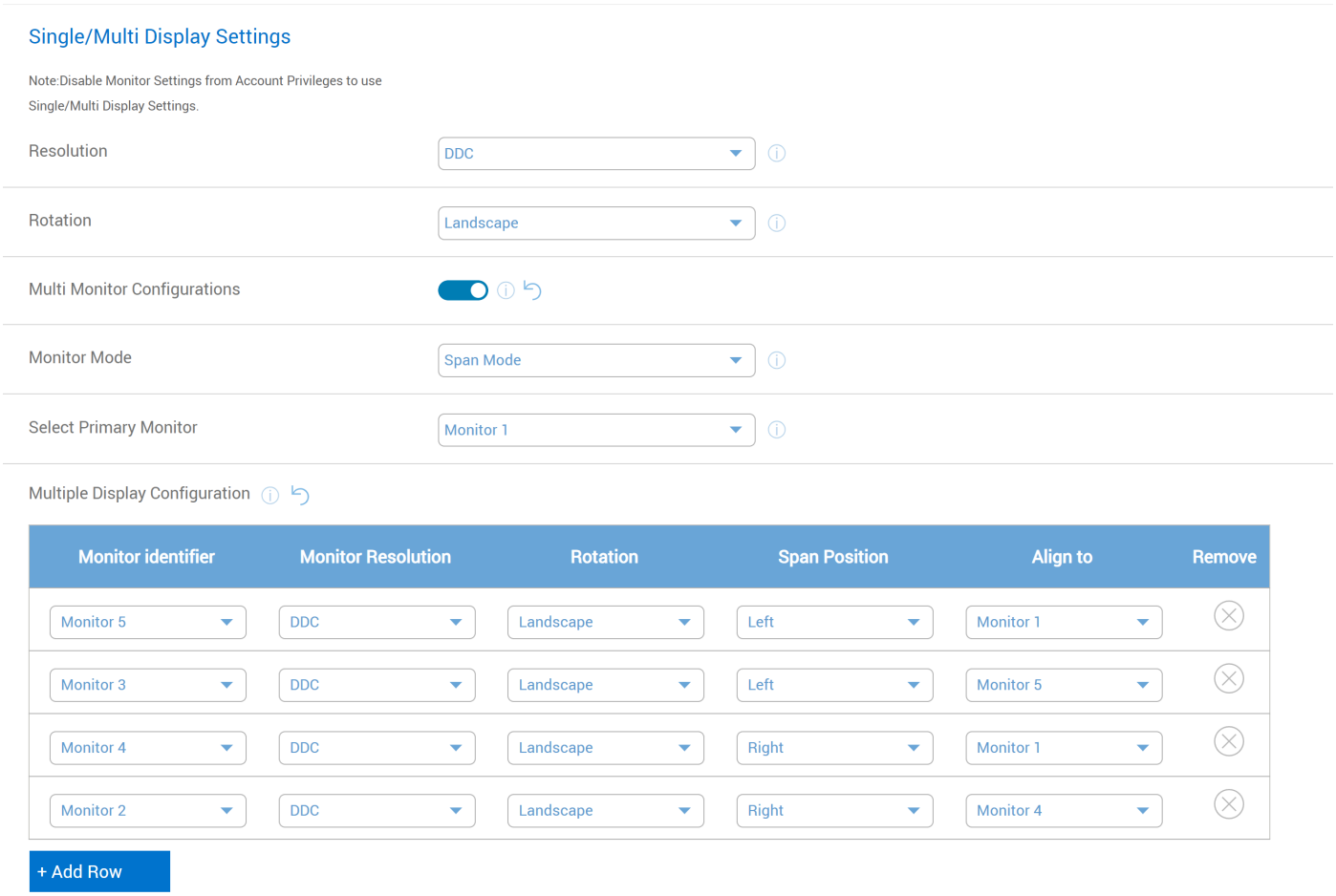


Figure 192. WMS Configuration Page

Example 5 - 5 Monitor Configuration

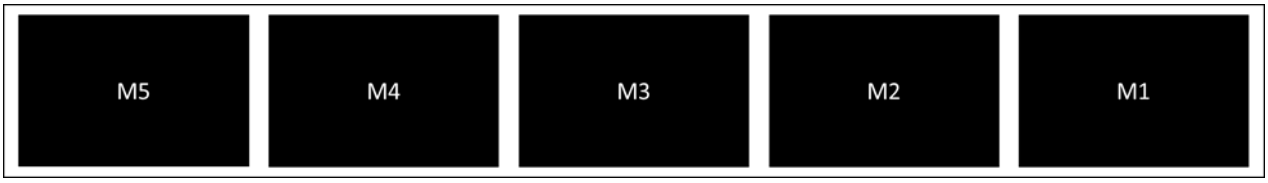


Figure 193. Monitor Position (M3 as Primary)

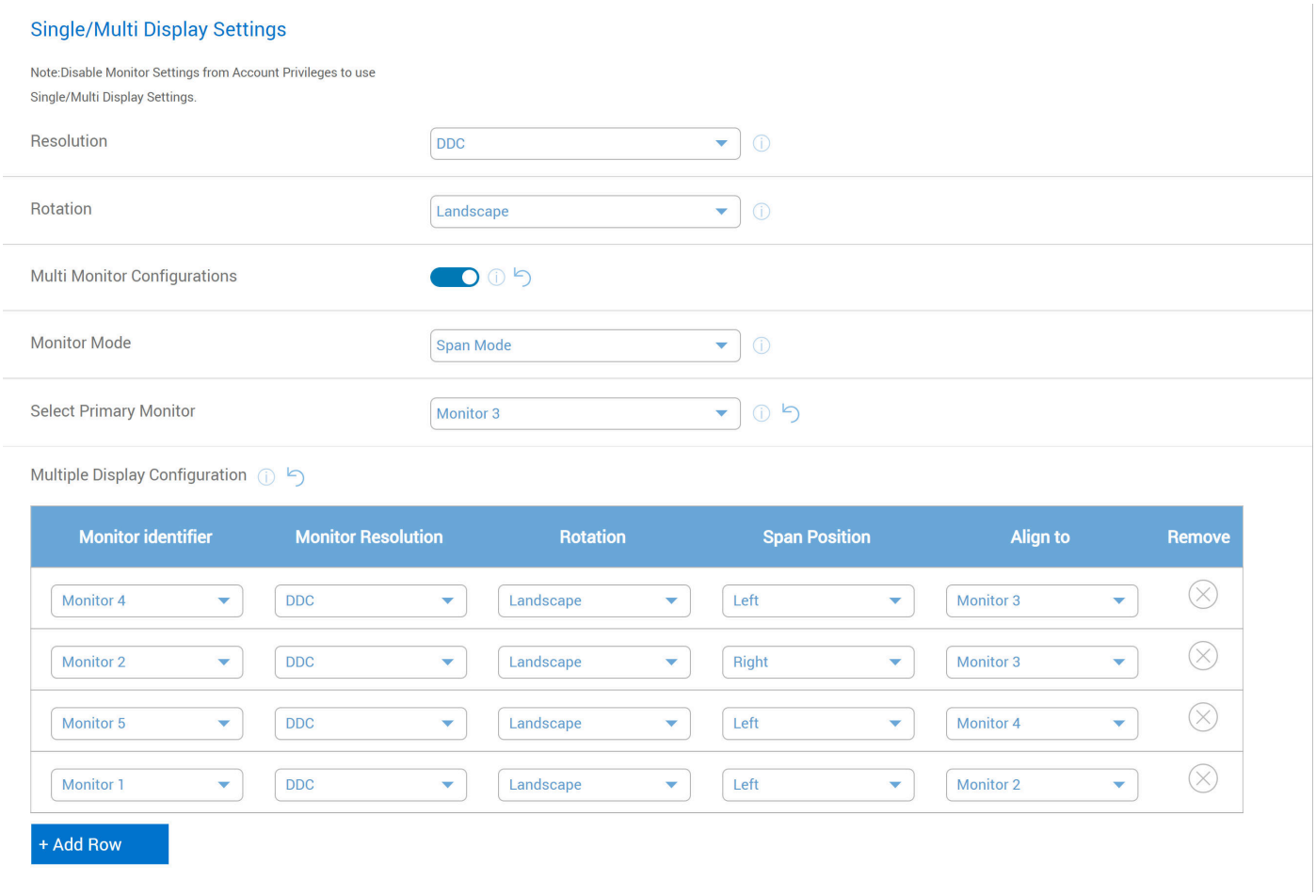


Figure 194. WMS Configuration Page

Example 6 - 6 Monitor Configuration

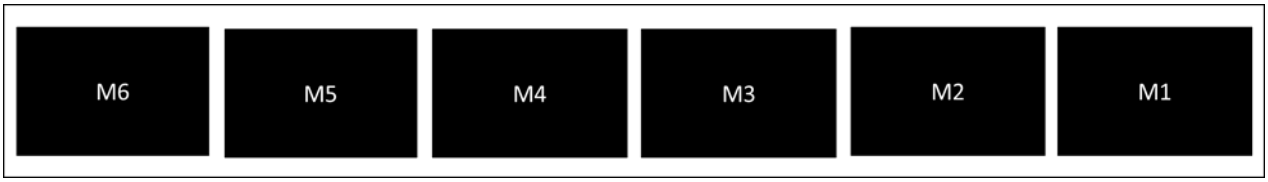


Figure 195. Monitor Position (M6 as Primary)

Single/Multi Display Settings

Note:Disable Monitor Settings from Account Privileges to use Single/Multi Display Settings.

Resolution: DDC

Rotation: Landscape

Multi Monitor Configurations

Monitor Mode: Span Mode

Select Primary Monitor: Monitor 6

Multiple Display Configuration

Monitor identifier	Monitor Resolution	Rotation	Span Position	Align to	Remove
Monitor 5	DDC	Landscape	Right	Monitor 6	
Monitor 4	DDC	Landscape	Right	Monitor 5	
Monitor 3	DDC	Landscape	Right	Monitor 4	
Monitor 2	DDC	Landscape	Right	Monitor 3	
Monitor 1	DDC	Landscape	Right	Monitor 2	

+ Add Row

Figure 196. WMS Configuration Page

Example 7 - 6 Monitor Configuration

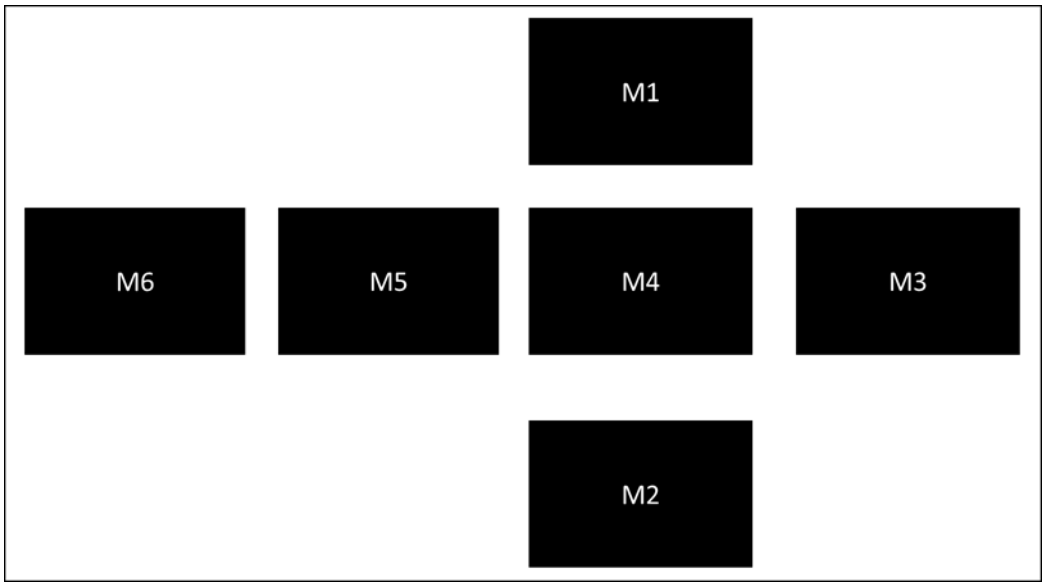


Figure 197. Monitor Position (M4 as Primary)

Single/Multi Display Settings

Note:Disable Monitor Settings from Account Privileges to use Single/Multi Display Settings.

Resolution: DDC

Rotation: Landscape

Multi Monitor Configurations

Monitor Mode: Span Mode

Select Primary Monitor: Monitor 4

Multiple Display Configuration

Monitor identifier	Monitor Resolution	Rotation	Span Position	Align to	Remove
Monitor 1	DDC	Landscape	Top	Monitor 4	
Monitor 2	DDC	Landscape	Bottom	Monitor 4	
Monitor 3	DDC	Landscape	Right	Monitor 4	
Monitor 5	DDC	Landscape	Left	Monitor 4	
Monitor 6	DDC	Landscape	Left	Monitor 4	

+ Add Row

Figure 198. WMS Configuration Page

Example 8 - 6 Monitor Configuration

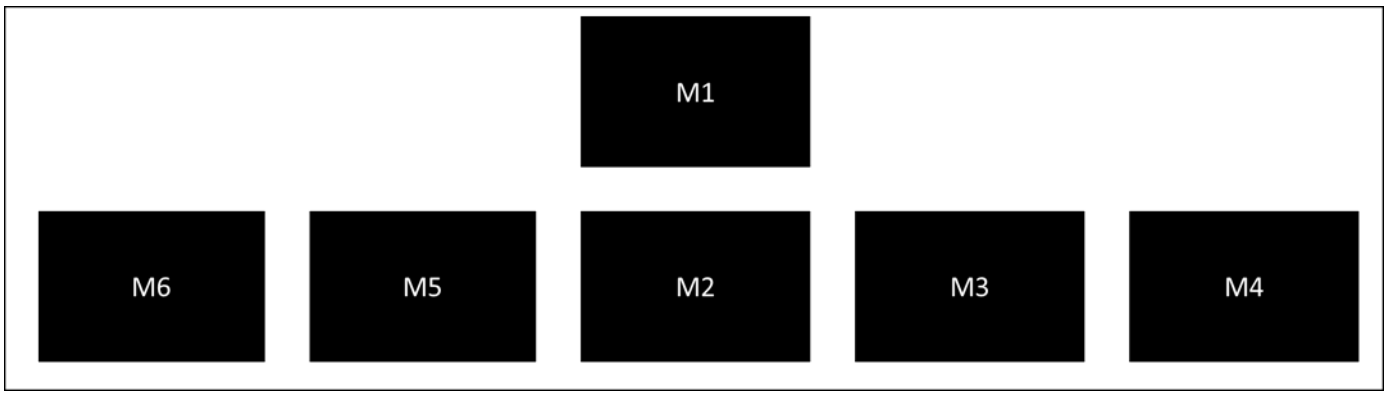


Figure 199. Monitor Position (M1 as Primary)

Single/Multi Display Settings

Note:Disable Monitor Settings from Account Privileges to use Single/Multi Display Settings.

Resolution: DDC

Rotation: Landscape

Multi Monitor Configurations

Monitor Mode: Span Mode

Select Primary Monitor: Monitor 1

Multiple Display Configuration

Monitor identifier	Monitor Resolution	Rotation	Span Position	Align to	Remove
Monitor 2	DDC	Landscape	Bottom	Monitor 1	
Monitor 5	DDC	Landscape	Left	Monitor 2	
Monitor 4	DDC	Landscape	Right	Monitor 2	
Monitor 3	DDC	Landscape	Right	Monitor 3	
Monitor 6	DDC	Landscape	Left	Monitor 5	

+ Add Row

Figure 200. WMS Configuration Page

Example 9 - 6 Monitor Configuration with Different Orientations

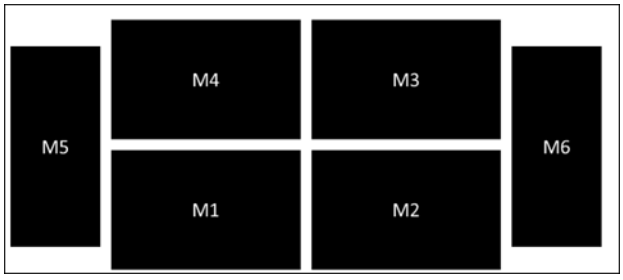


Figure 201. Monitor Position (M1 as Primary)

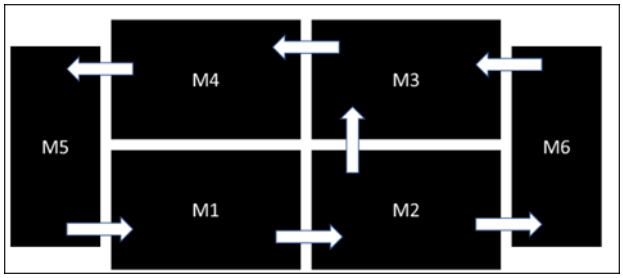


Figure 202. Mouse Pointer Movement (vice versa also moved)

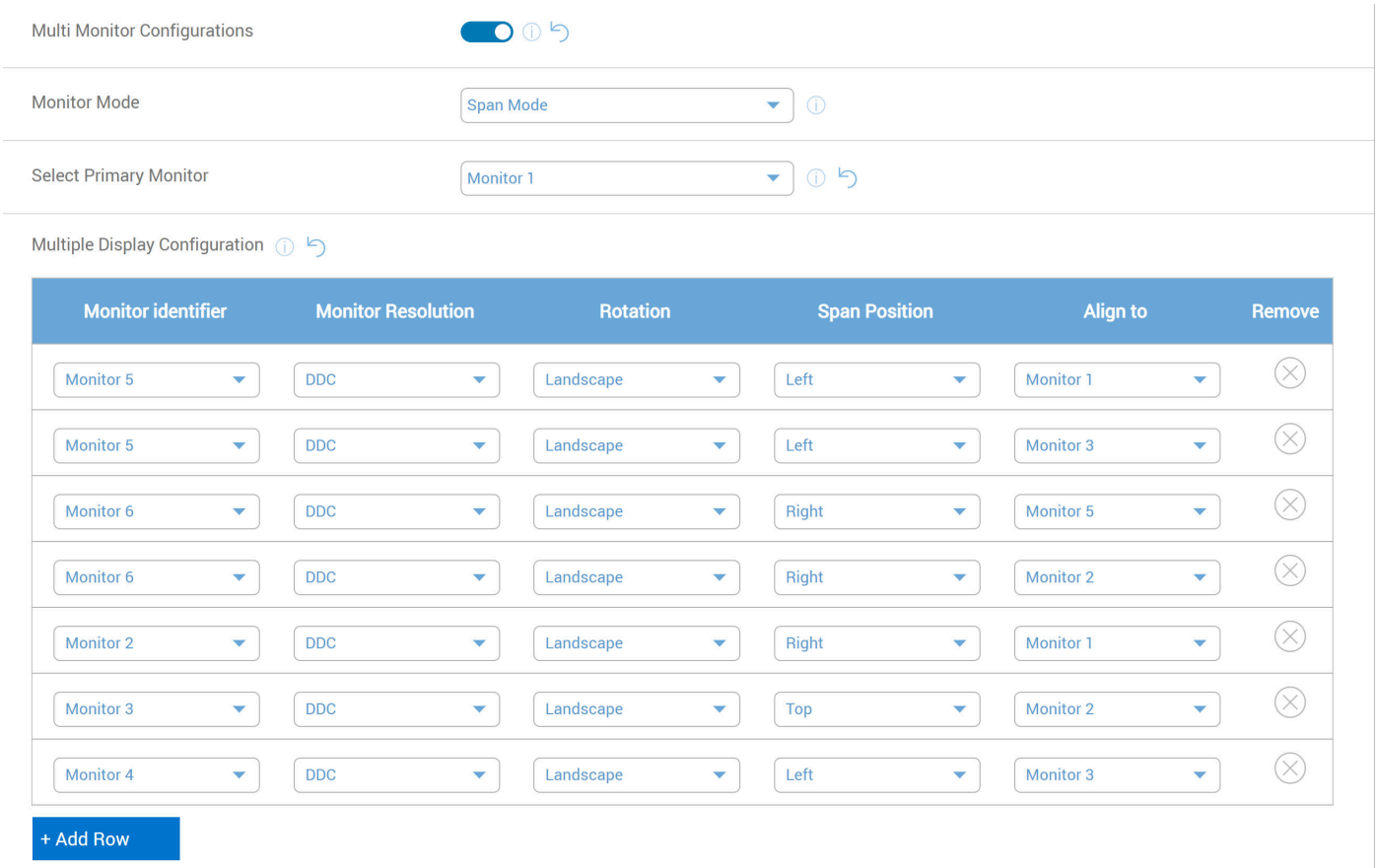


Figure 203. WMS Configuration Page

How to configure the features using Optional Packages

Dell Hybrid Client supports addon installation and addon upgrade with the help of Wyse Management Suite. You can configure the required features with the help of an addon.

For information about the Optional Packages, see *Dell Hybrid Client Version 2310 Release Notes* at Dell Support page.

How to Add optional packages

You can add optional packages (add-ons) using on-premises Wyse Management Suite or Cloud Wyse Management Suite.

Using on-premises Wyse Management Suite

You can add optional packages using on-premises Wyse Management Suite.

Steps

1. Download and copy the package file to `\repository\hybridClientApps`. For example, `C:\WMS\LocalRepo\repository\hybridClientApps`.
2. Go to **Apps & Data** > **App Policies** > **Dell Hybrid Client** > **Add Policy**.
3. Enter the **Policy Name**.
4. From the **Group** drop-down list, select the group.
5. From the **Task** drop-down list, select **Install Application**.

6. From the **OS Type** drop-down list, select **Dell Hybrid Client**.
7. From the **Application** drop-down list, select package.
8. Click **Save** to create a policy.
9. Click **Yes** to schedule the job.
10. Select any of the following options:
    - **Immediately-** Server runs the job immediately.
    - **On device time zone-** Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone-** Server creates one job to run at the date or time of the designated time zone.
11. Check the status of the job by going to the **Jobs** page.
12. Click **Update Now** when an upgrade notification window is displayed on the device.
    Depending on the package or settings, the device reboots after the installation.

Using Cloud Wyse Management Suite

You can add optional packages using Cloud Wyse Management Suite.

About this task

NOTE: All Dell Hybrid Client optional packages are available in Cloud Wyse Management Suite. The packages and files are visible to all the users. Users cannot delete or modify the files. The operator cannot upload ISO files.

Steps

1. Go to **Apps & Data** > **App Inventory** > **Dell Hybrid Client** and verify that the application is registered.
2. Go to **App Policies** > **Dell Hybrid Client**.
3. Click **Add Advanced Policy**.
   The **Add Advanced App Policy** page is displayed.
4. Enter the **Policy Name**.
5. From the **Group** drop-down list, select the group.
6. Select the **Sub Groups** check box to apply the policy to sub groups.
7. From the **Task** drop-down list, select the task.
8. From the **OS Type** drop-down list, select the operating system.
9. Select the **Filter** files based on the extensions checkbox to filter the applications.
10. Click **Add app**, and select one or more applications under **Apps**. For each application, you can select a pre and post-install script under **Pre-Install**, **Post-Install**, and **Install Parameters**.
11. If you want the system to reboot after the application is successfully installed, select **Reboot**.
12. Click **Add app** and repeat the step to add multiple applications.

    NOTE: To stop the application policy at first failure, select Enable app dependency. If this option is not selected, failure of an application affects the policy implementation.

13. To deploy this policy to a specific operating system or a platform, select either **OS Subtype Filter** or **Manufacturer Filter** and **Platform Filter**.
14. Specify the number of minutes the message dialog box should be displayed on the client. A message on the client which gives you time to save your work before the installation begins.
15. To enable delay in implementation of the policy, select the **Allow delay of policy execution** checkbox. If this option is selected, the following drop-down menus are enabled:
    - From the **Max Hours per Delay** drop-down list, select the maximum hours (1-24) which you can delay running the policy.
    - From the **Max delays** drop-down list, select the number of times (1-3) you can delay running the policy.
16. From the **Apply Policy Automatically** drop-down list, select one of the following options:
    - **Do not apply automatically-** This option does not apply a policy automatically to the devices.
    - **Apply the policy to new devices-** This option automatically applies the policy to a registered device which belongs to a selected group or to the device that is moved to a selected group. When this option is selected, the policy is applied to all the new devices that are registered to the group. To run the job on the existing devices present in the group, you must

schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group. The job status of the newly added device count that is registered is not displayed.

- **Apply the policy to devices on check in-** This option is automatically applied to the device at check-in. When this option is selected, the policy is applied to all the devices present in the group. To run the job on existing devices present in the group immediately or at a scheduled time before the device check-in, you must schedule the policy. After you schedule the policy, the job status displays the count of devices that are already present in the group.

17. Specify the number of minutes the message dialog box should be displayed on the client in the **Timeout (1 - 999 min.)** box. Timeout displays a message on the user which gives you time to save your work before the installation begins.
18. To stop the installation process after a defined value, specify the number of minutes in the **Install Timeout** field. The default value is 60 minutes.
19. Click **Save** to create a policy. A message is displayed to enable the administrator to schedule this policy on devices based on group.
20. Select **Yes** to schedule a job on the same page.
21. Select one of the following options:
    - **Immediately-** Server runs the job immediately.
    - **On device time zone-** Server creates one job for each device time zone and schedules the job to the selected date or time of the device time zone.
    - **On selected time zone-** Server creates one job to run at the date or time of the designated time zone.
22. To create the job, click **Preview** and schedules are displayed on the next page.
23. You can check the status of the job by going to the **Jobs** page.

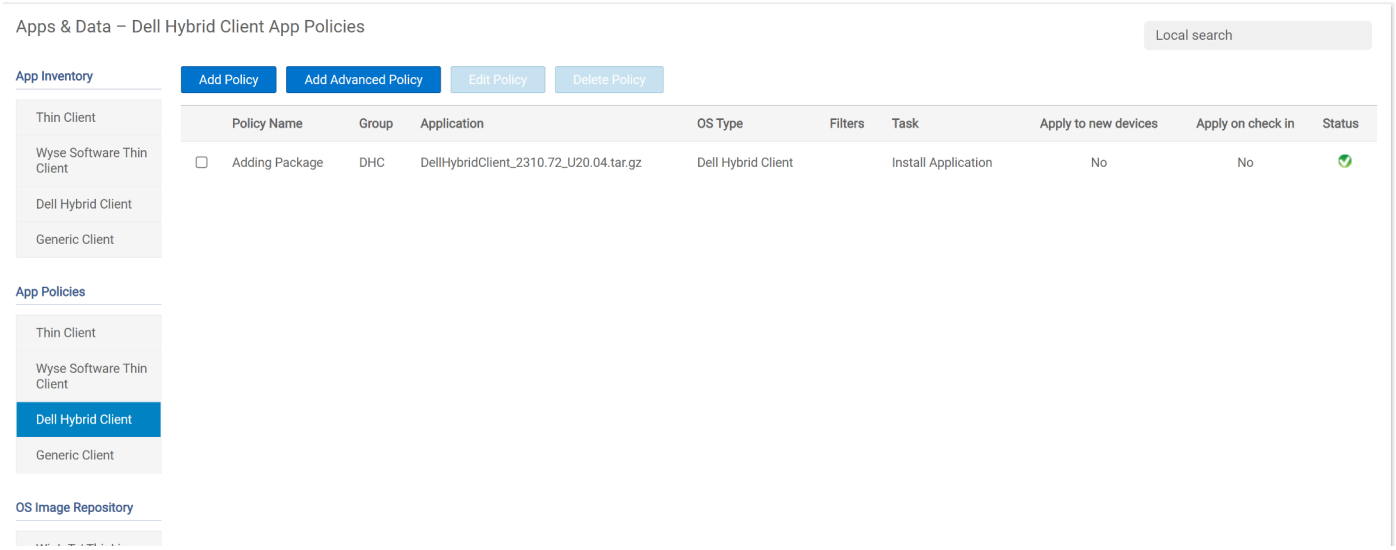


Figure 204. Adding package

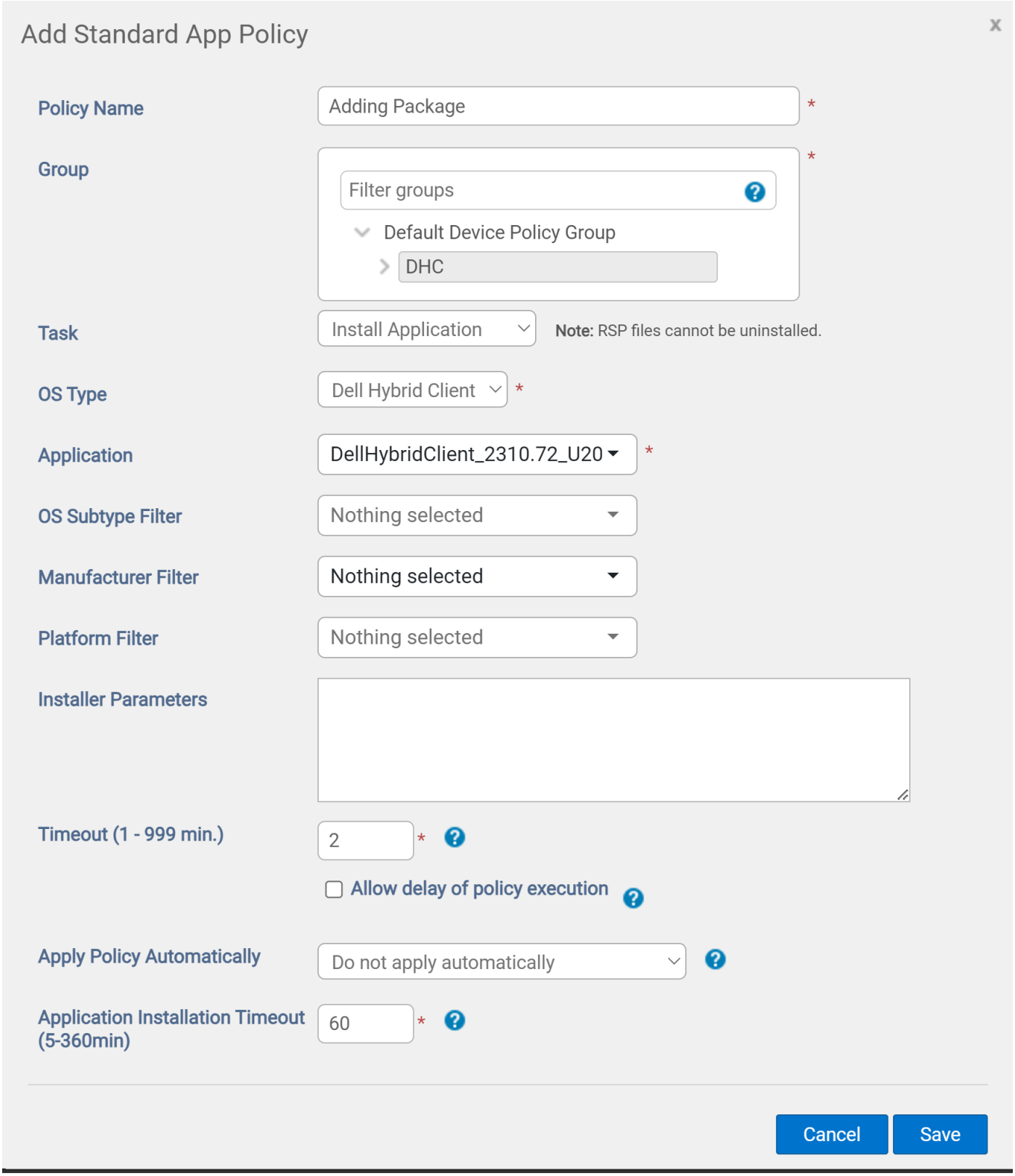


Figure 205. Adding package details

How to View the Installed Packages

1. You can view the installed packages in the **System Information**.

2. To view your system information, click the **System Information** icon on the top bar.
3. It has the **Identity, Network, Packages, Copyright, and About** tabs.
4. Click the **Packages** tab. It displays all add-ons that are installed on your device. The add-ons are listed with the attributes, such as package name, version, size, and status. The Original value in the Status column specifies the integrated add-ons in the Dell Hybrid Client. By default, only Dell packages are displayed. To view all packages, click the **Show All Packages** button.

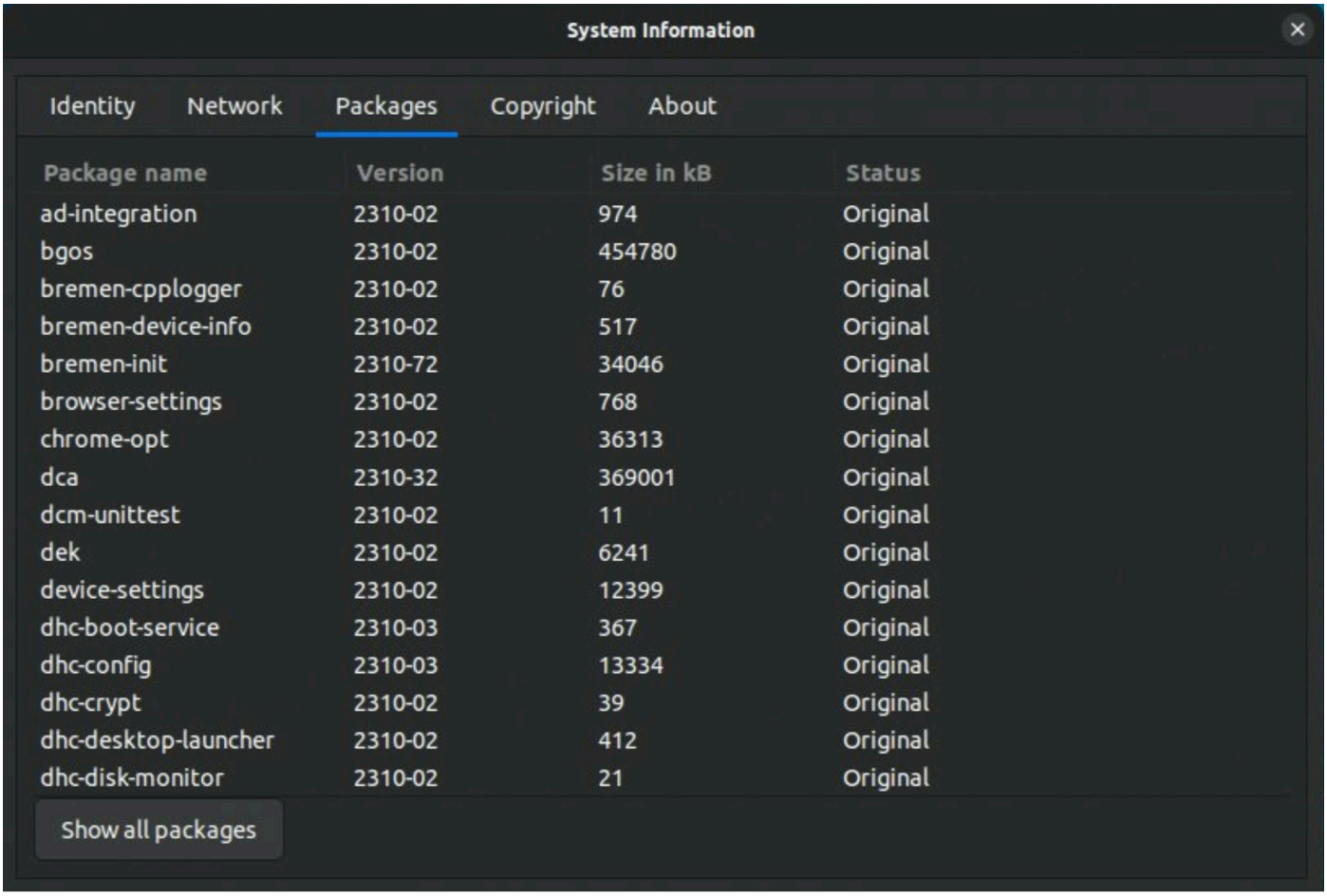


Figure 206. System Information

How to Uninstall the Packages

The following are the steps to uninstall the package.

About this task

NOTE: Uninstallation supports only Debian packages that are installed from Wyse Management Suite. Uninstallation is not supported for tar.gz, and bundle packages are installed from Wyse Management Suite.

Steps

1. Create a policy to remove the package. To create a policy, do the following:
   a. Go to **Apps & Data** > **App Policies** > **Dell Hybrid Client**.
   b. Click **Add Policy**.

      The Add Standard App Policy window is displayed.

   c. Enter the **Policy Name**.
   d. From the **Group** drop-down list, select the group of the device.
   e. From the **Task** drop-down list, select **Uninstall Application**.
   f. From the **Application** drop-down list, select the application that you want to remove.

g. From the **OS Subtype Filter** and **Platform Filter** drop-down lists, select the filters.
h. Click Save.

An Alert window is displayed to schedule the app policy.

i. Click **Later**.

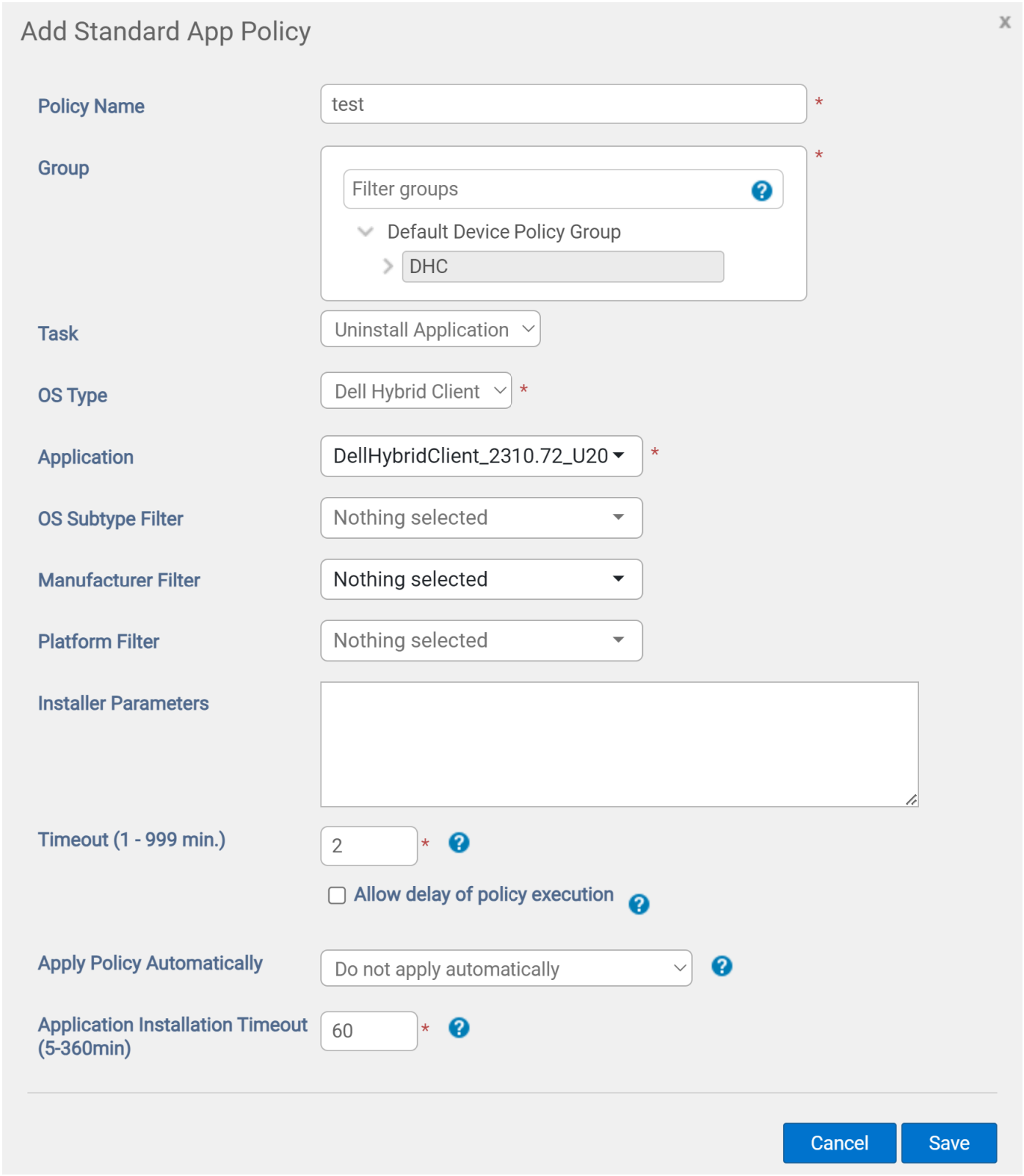


Figure 207. Uninstall package details

2. Go to the **Devices** page and select the device from which you want to remove the package.
3. From the **More Actions** drop-down list, select **Schedule App Policy**.
   The App Policy Job window is displayed.
4. From the **Policy** drop-down list, select the policy that is created to remove the application.
5. From the **Run** drop-down list, select **Immediately**.
6. Click **Preview** and then click **Schedule**. The application is removed from the client.

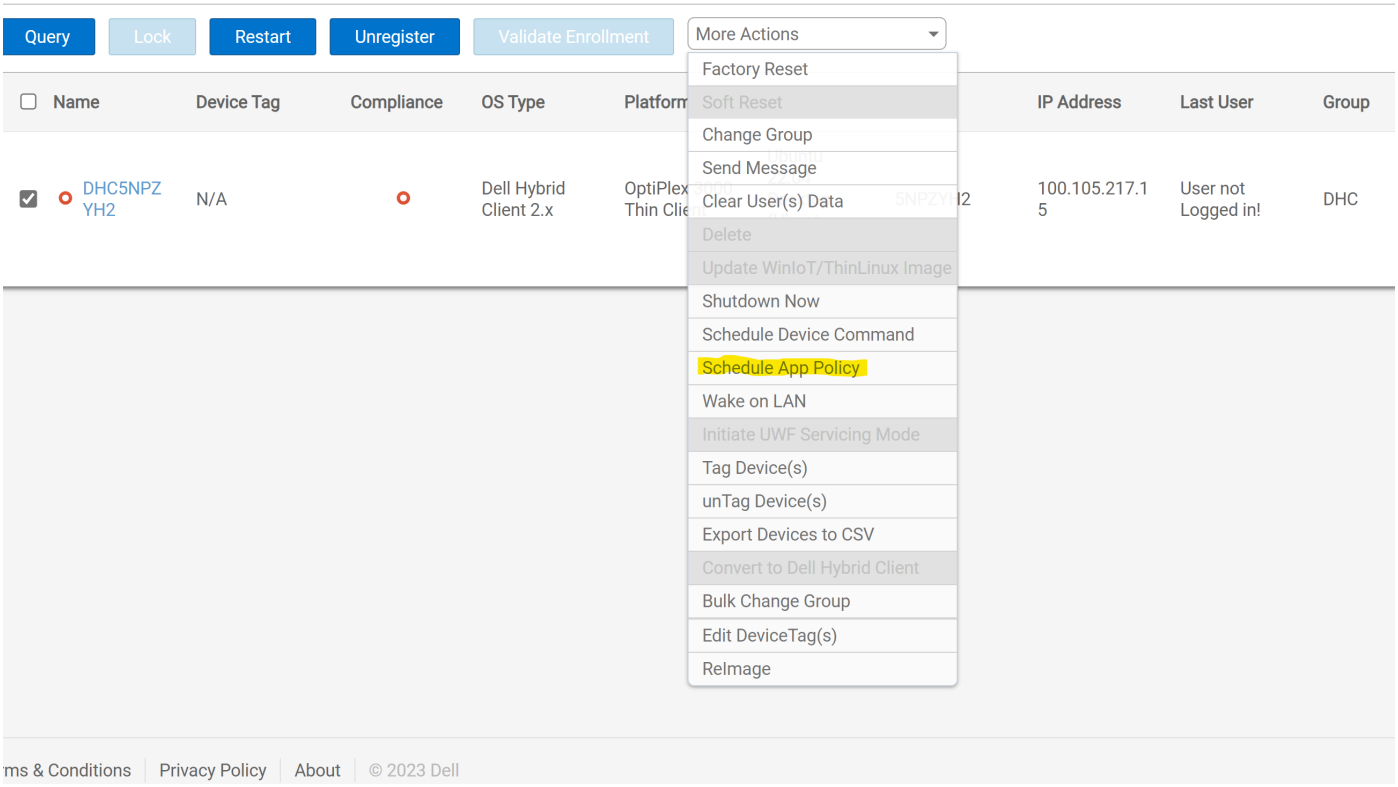


Figure 208. Schedule App Policy

How to configure the Peripheral Management settings

1. You can configure **Peripheral Management** settings from **Device Settings**.
2. Only **Local and Domain User** configuration is preserved after Logout/Reboot when configuring from **Device Settings**.
3. In **Guest**, **Peripheral Management** configuration is not preserve after Logout/Reboot, you must preserve **Peripheral Management** settings across all users then it must be configured from **Wyse Management Suite**.
4. The following are the Peripheral Management settings:
   a. Audio
   b. Keyboard
   c. Mouse
   d. Printers

Configuring Audio using Device Settings

You can configure the audio using Device Settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.

3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Peripherals Management**.
5. Click the **Audio** tab, and then click **Advanced Settings**. You can use the **Sound** settings window of the Ubuntu interface to configure the output, input, sound effects, and applications tab. For more information about how to configure the sound settings, see the Ubuntu documentation at help.ubuntu.com.

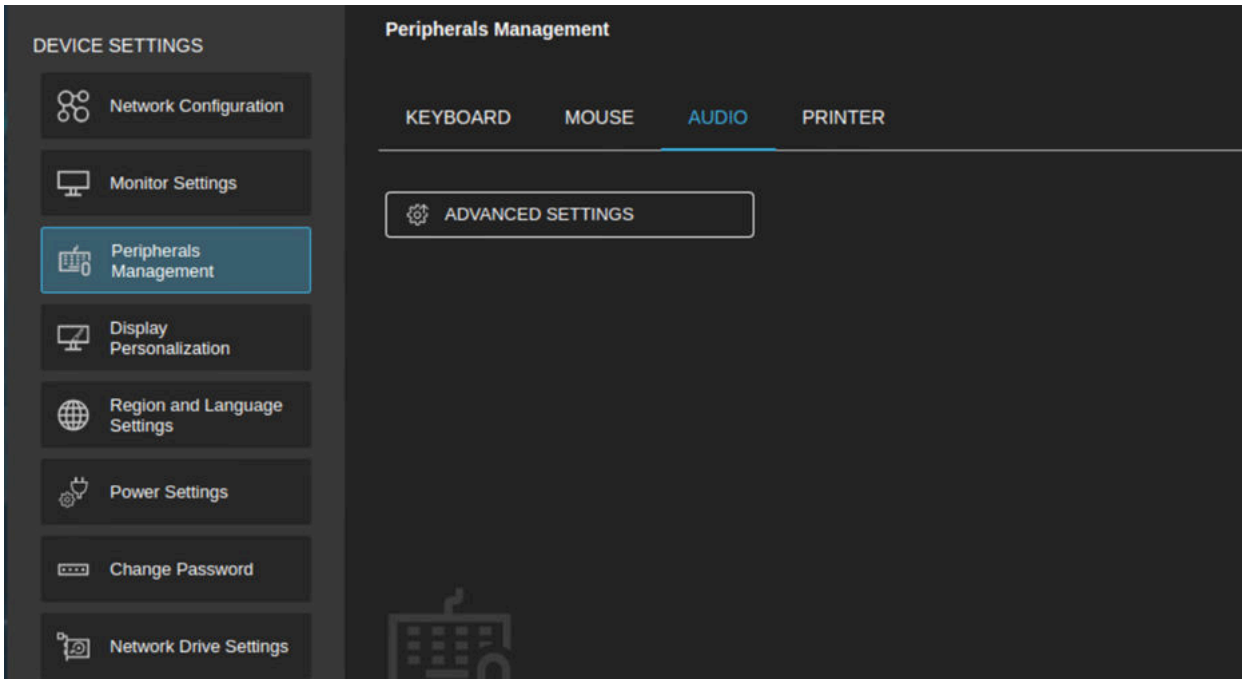


Figure 209. Peripherals Management

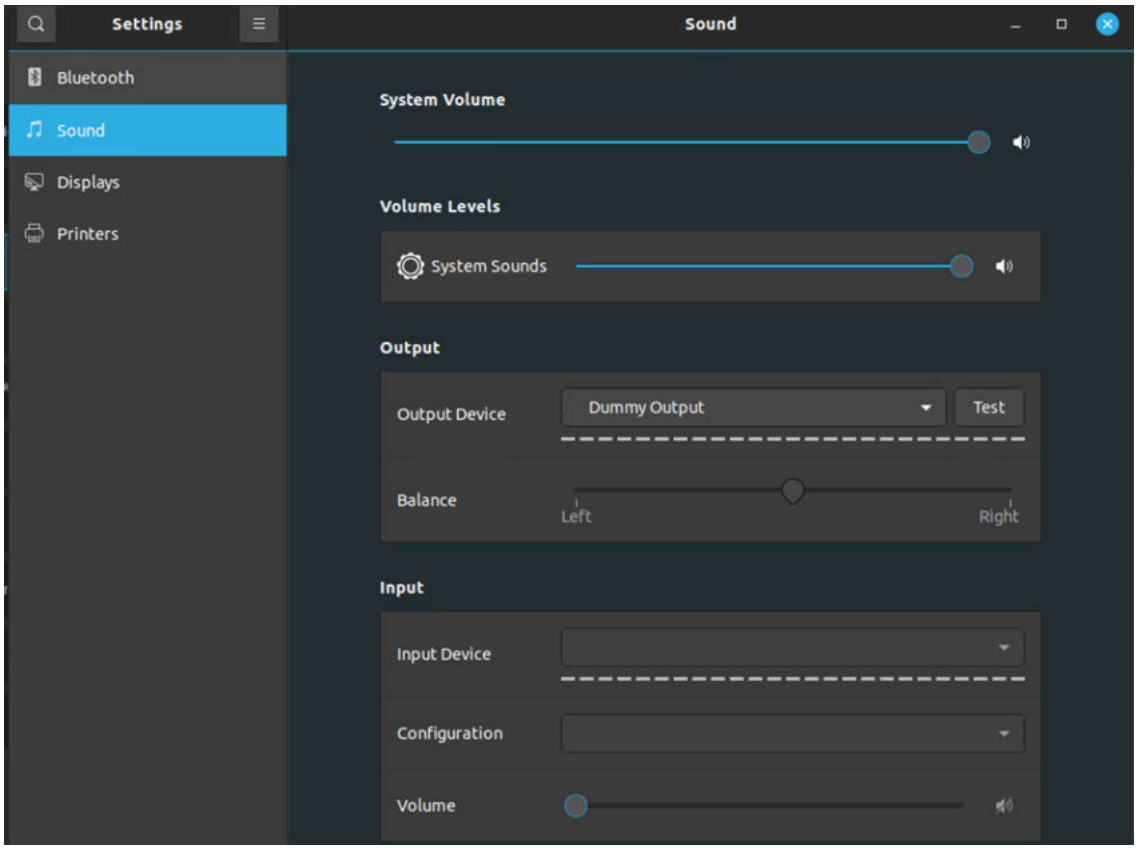


Figure 210. Sound

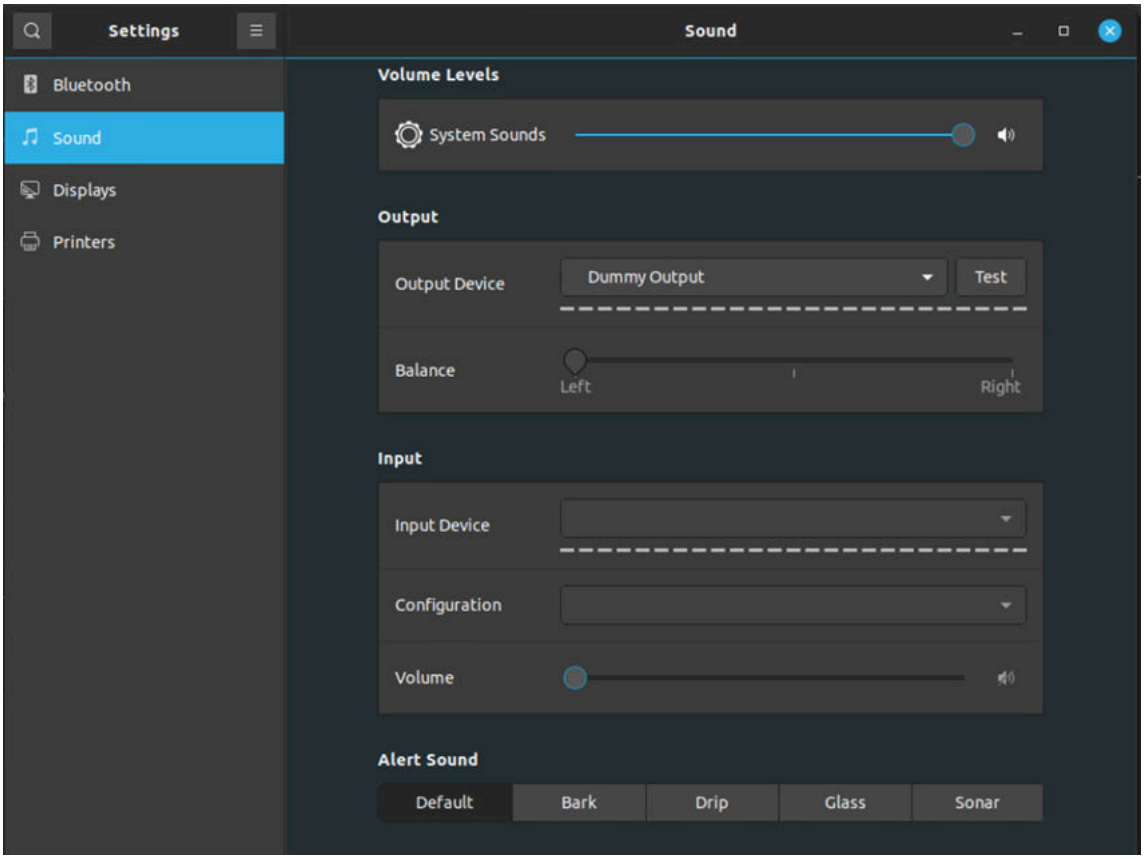


Figure 211. Sound

Configuring Audio using Wyse Management Suite

You can configure the audio using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Audio**.
   You can configure the following audio settings:
   - **Audio Mute-** Click the toggle key to mute the audio.
   - **Microphone Mute-** Click the toggle key to mute the microphone.
   - **Microphone Volume-** Click on the drop-down to adjust the microphone volume.

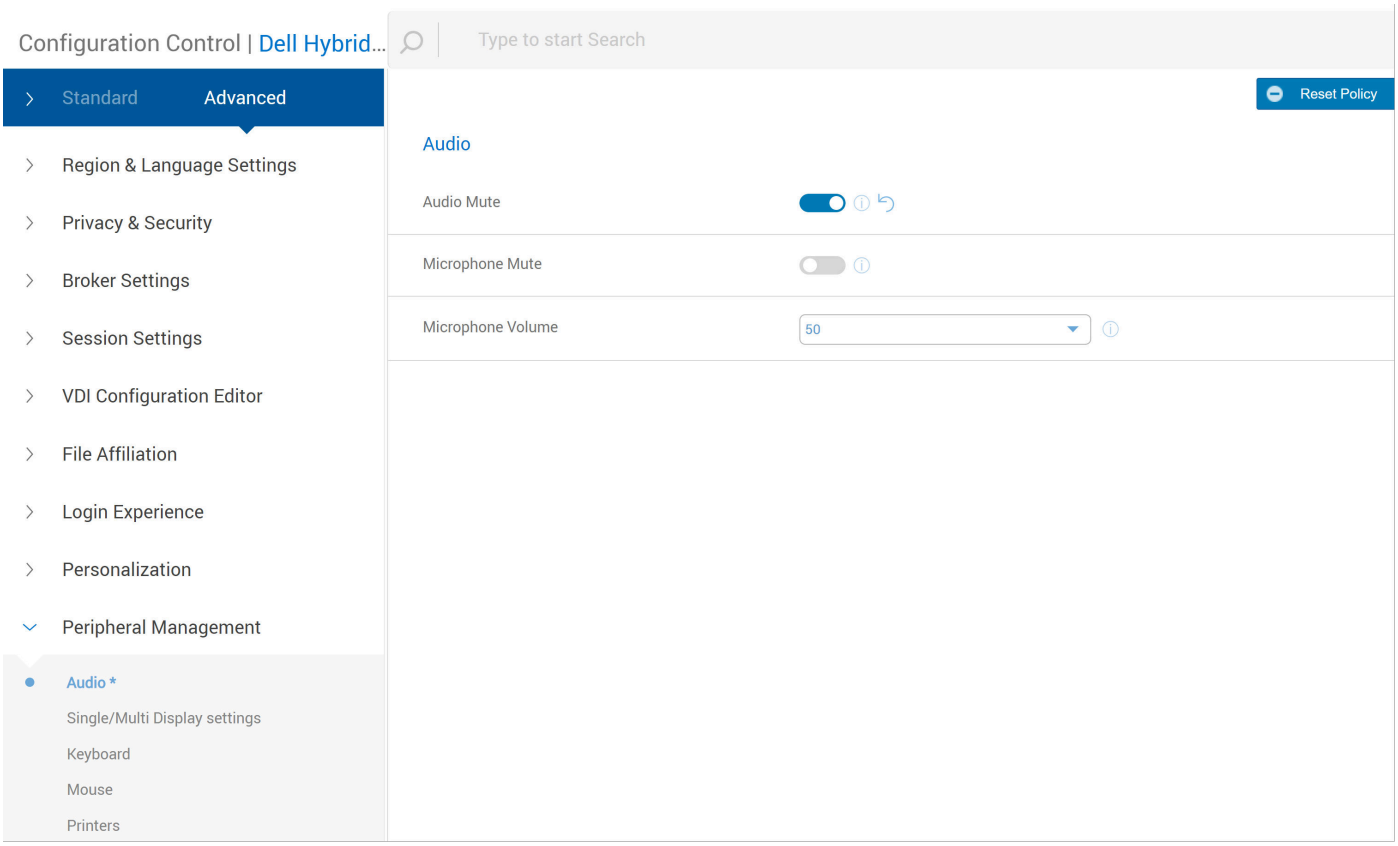


Figure 212. Audio

Configuring Keyboard using Device Settings

You can configure the keyboard using Device Settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Peripherals Management**.
5. Click the **Keyboard**.

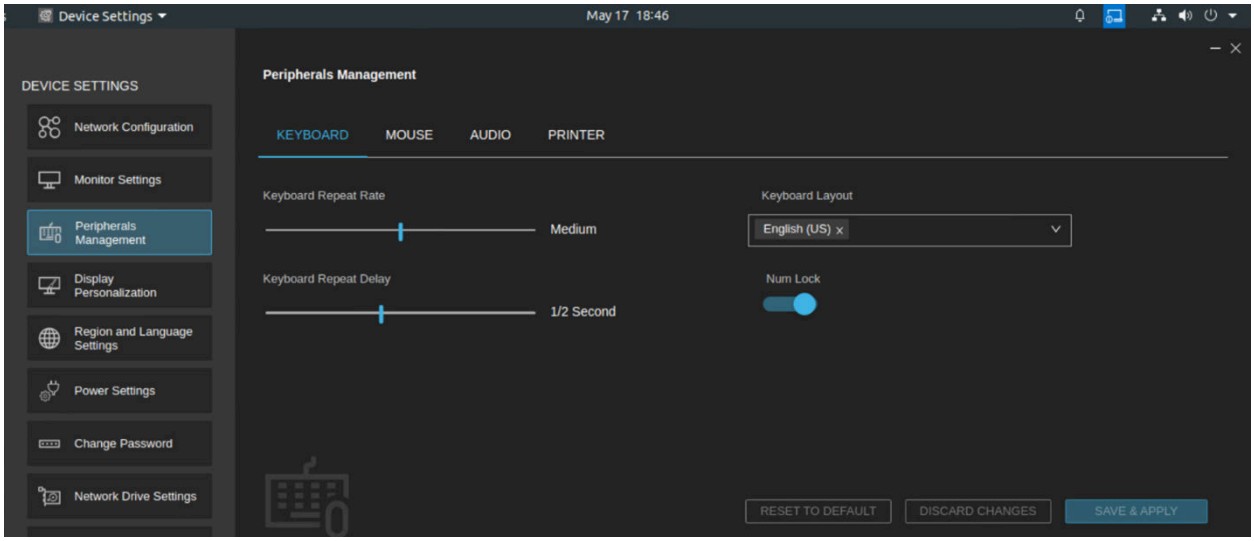


Figure 213. Peripherals Management

Configuring a Keyboard using Wyse Management Suite

You can configure the keyboard using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Keyboard**.
   You can configure the following keyboard settings:
   - **Keyboard Repeat Rate-** Keyboard Repeat Rate is the speed at which a keyboard registers a key being held down and then automatically repeats the key input. This can be set to Slow, Medium, or Fast.
   - **Keyboard Repeat Delay-** It is the duration of time a key must be held down before the keyboard starts generating repeated inputs of that key.
   - **Keyboard Layout-** Select any keyboard layout as the default layout, for example, English.
   - **Keyboard Layout List:**
     a. From the **Keyboard Layout** drop-down, select any keyboard layout as the additional keyboard layout, for example, English.
     b. Select any Keyboard Layout from the **Keyboard Layout** List, for example, French. Save and publish.
     c. Log out the device and in the login screen check if the selected keyboard is applied.
     d. On the login screen, enter **Username and Password**. It takes input with a selected keyboard layout.

     NOTE: The Keyboard Layout for Chinese, Korean, and Japanese must install the full language package from Wyse Management Suite and has to configure the system with the respective language for the particular layout.

     NOTE: If you select keyboard layout from the Wyse Management Suite, it is applicable for Dell Hybrid Client Login Screen and Dell Hybrid Client Desktop. But if you select keyboard layout from device settings, it is applicable only for Dell Hybrid Client Desktop.
   - **Num Lock-** Click on this toggle button to enable or disable the Num Lock
   - **Printscreen-** Click on this toggle button to enable or disable the PrintScreen Note: Press Alt+printscreen or Only PrintScreen button can take the screenshot of the desktop when it is enabled.

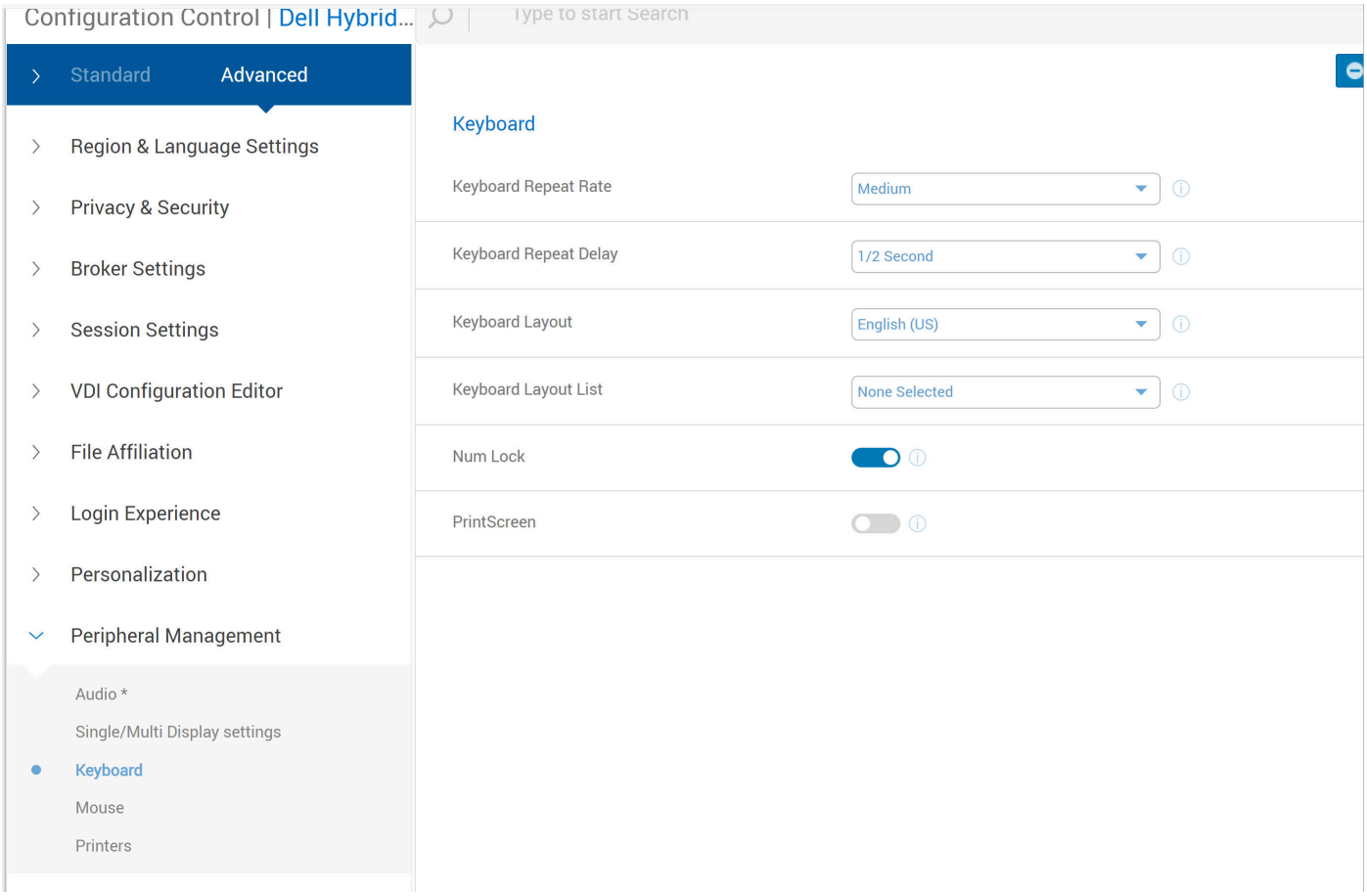


Figure 214. Keyboard

Configuring Mouse using Device Settings

You can configure the mouse using Device Settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Peripherals Management**.
5. Click the **Mouse**.

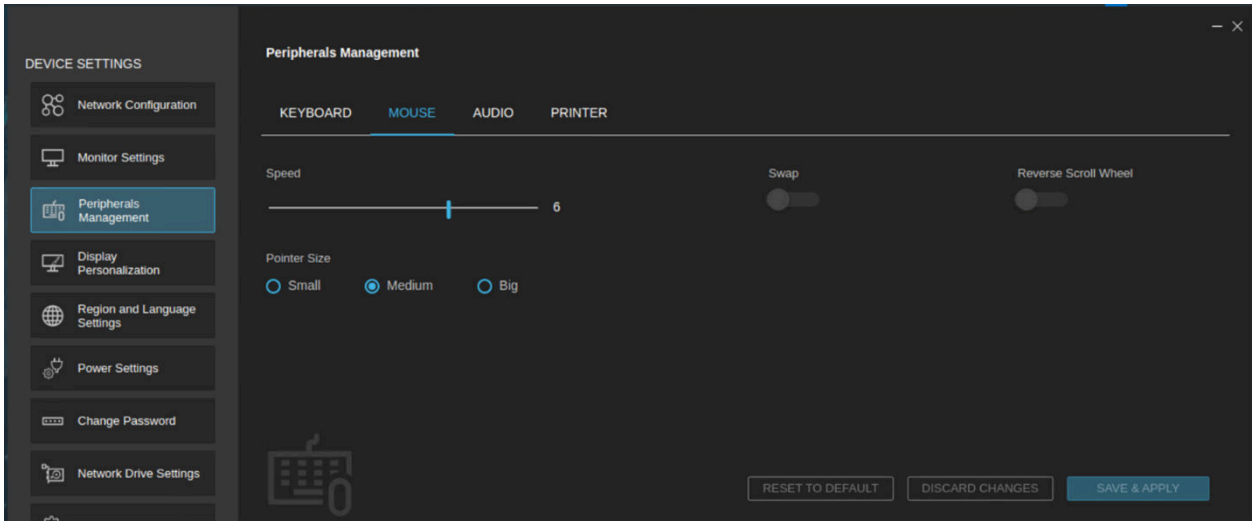


Figure 215. Peripherals Management

Configuring a Mouse using Wyse Management Suite

You can configure the keyboard using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Mouse**.
   You can configure the following mouse settings:
   - **Speed-** This option enables you to increase or decrease the speed of the mouse cursor movement.
   - **Swap Mouse Buttons-** Click the Swap toggle key to swap the left and right mouse buttons for left-handed operations.
   - **Invert scroll Wheel-** Click the Reverse Scroll Wheel toggle key to invert the direction of the mouse scroll wheel.
   - **Cursor Size-** Select the size of the local mouse pointer from the following Pointer Size options:
     a. Small
     b. Medium
     c. Big

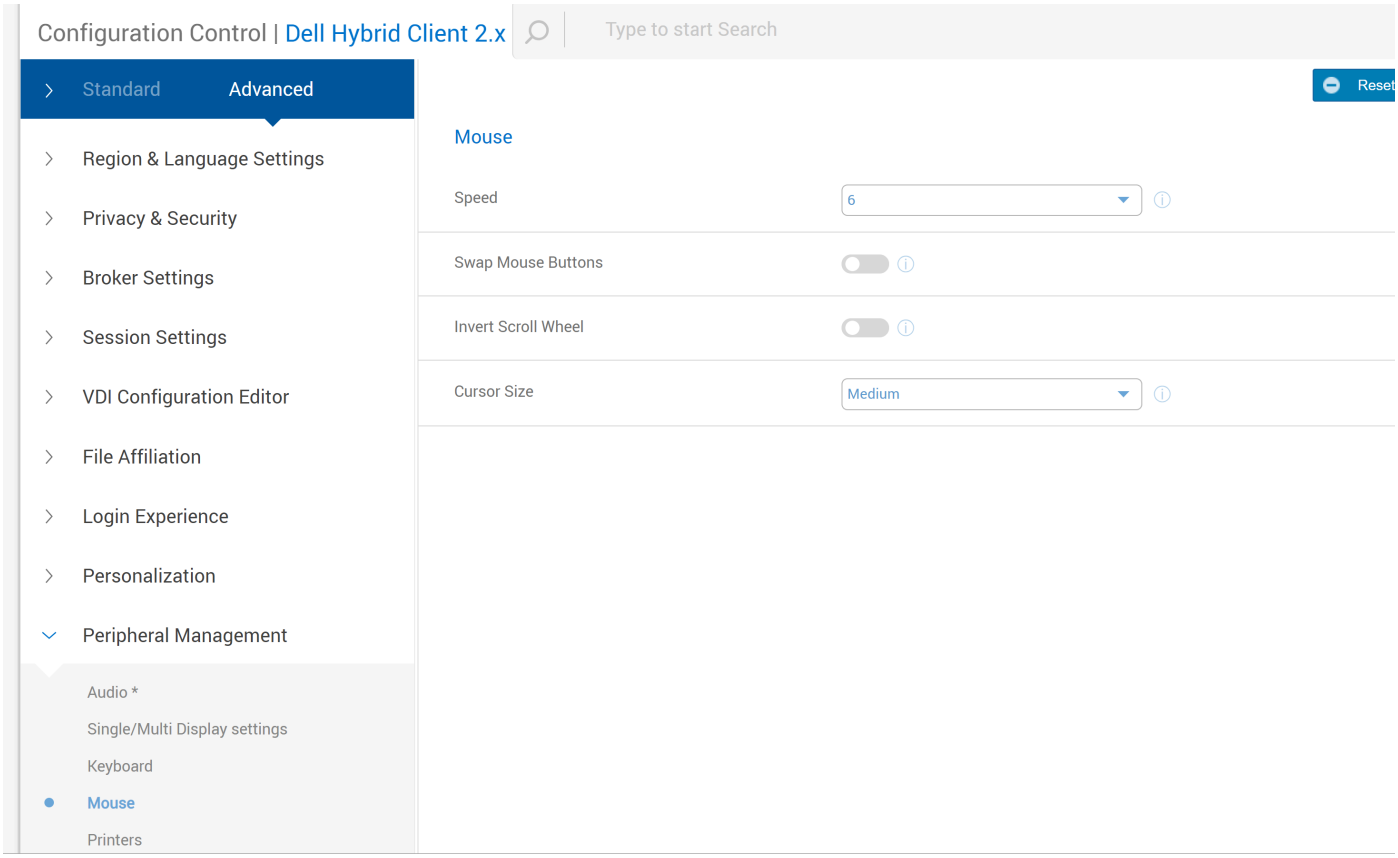


Figure 216. Mouse

Configuring Printer using Device Settings

You can configure the printer using Device Settings.

Steps

1. Log in to the device powered by Dell Hybrid Client.
2. Click the **Show Application** icon on the desktop screen.
   The **Applications Overview** screen is displayed.
3. Click the **Device Settings** icon.
   The **Device Settings** window is displayed.
4. Click **Peripherals Management**.
5. Click the **Printer**.

   Dell Hybrid Client supports network printing using the Line Printer Daemon (LPD) and Server Message Block (SMB) network protocols. You can also use the Uniform Resource Identifier (URI) of the printer for network printing.

   Click the Printer option, and configure the following options:
   - **Advanced Settings-** Use this option to add a local or network printer.
   - **Additional Printer Settings-** Use this option to configure the printer settings.

   User can use the Printer settings window of the Ubuntu interface to configure the printer options.

   NOTE: The Drivers package must be installed for USB printer.

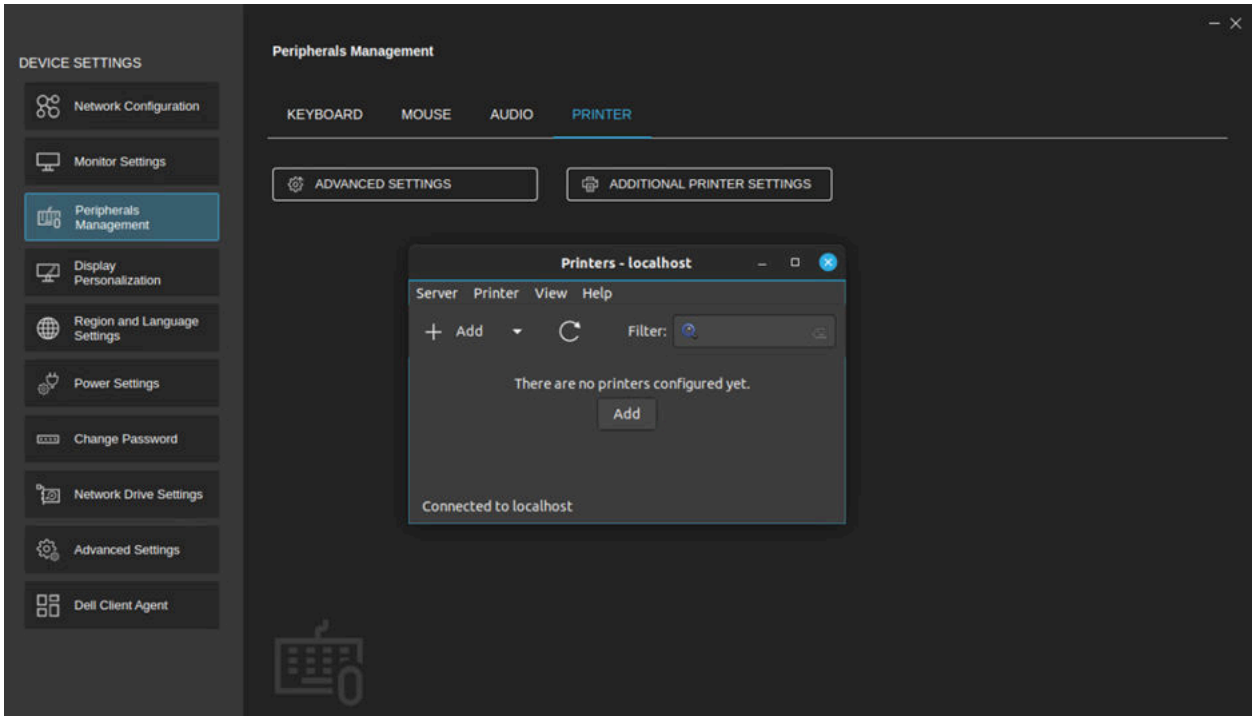


Figure 217. Peripherals Management

Configuring Printer using Wyse Management Suite

You can configure the printer using Wyse Management Suite.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Dell Hybrid Client 2.x**.
   The **Configuration Control | Dell Hybrid Client 2.x** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Printer**.
6. In the **Printer Connection** section, click **Add Row**.
7. **Printer Type:** Click on the drop-down box to select the printer type. You can configure the following printer settings:
   - Configure the LPD Printer Settings
   - Configure the SMB Printer Settings
   - Configure the URI Printer Settings

Configure the LDP Printer Settings

You can configure the LPD printer settings using Wyse Management Suite.

- Enter the name of the printer in the **Name** field.
- Enter the hostname in the **Host** field. For LPD printer, you can enter the IP address of the printer.
- Enter the name of the queue associated with the printer in the **Queue** field. An LPD host maintains a named queue for each supported printer.
- Enter the installed driver name in the **Model** field.
- Click the **Enable** toggle key to enable the device to access the printer.
- Click the **Default** toggle key to set the printer as the default printer.
- Enter the description for your printer in the **Description** field.

- Enter the network path where the printer is located in the **Location** field.

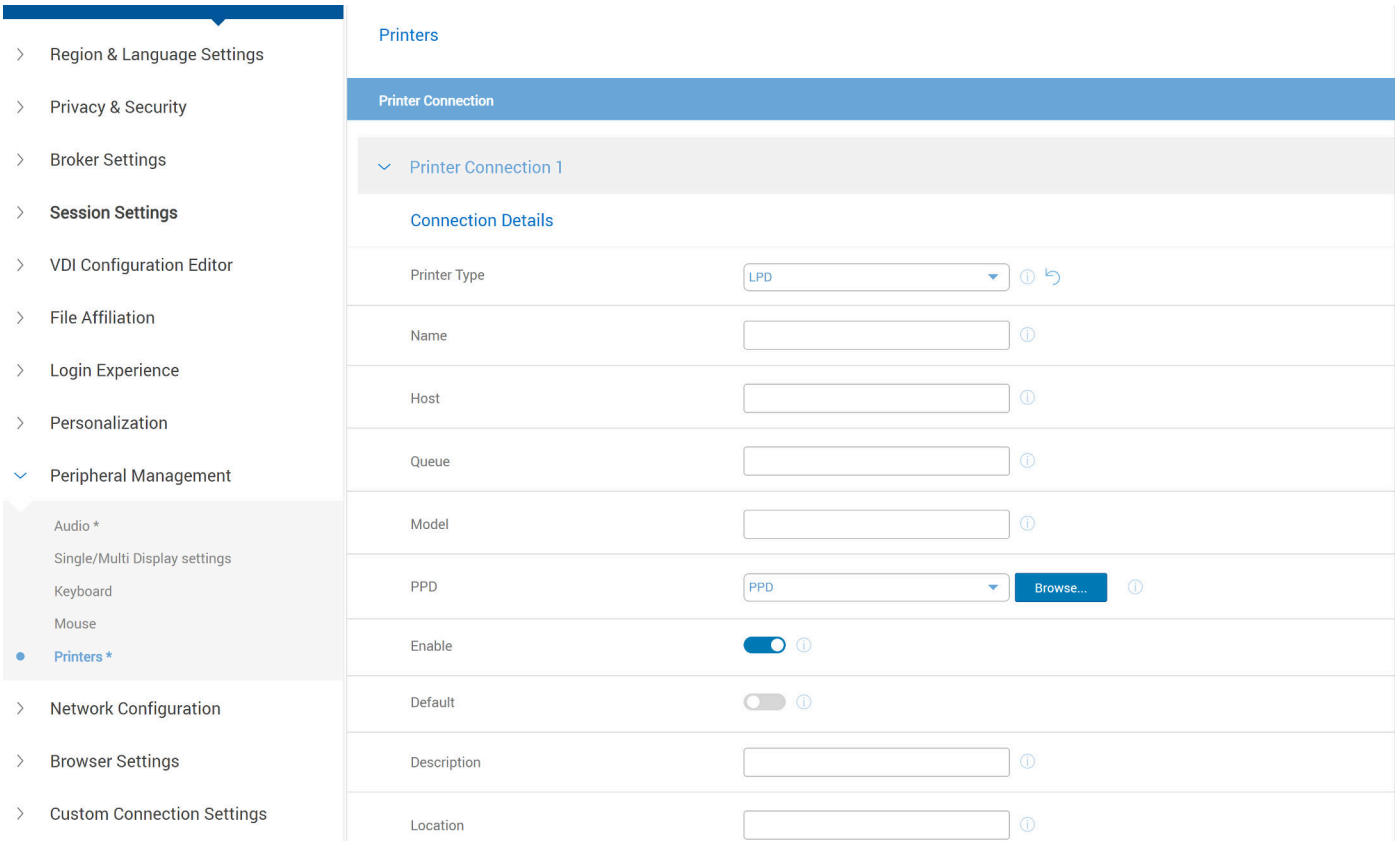


Figure 218. Printers

Configure the SMB Printer Settings

You can configure the SMB printer settings using Wyse Management Suite.

- Enter the name of the printer in the **Name** field.
- Enter the hostname in the **Host** field. For SMB printers, you can enter the UNC path of the printer server or the IP address followed by the printer share name.
- Enter the name of the domain user in the **Domain User Name** field, for example, Workgroup (Domain)\Username.
- Enter the domain password in the **Password** field.
- Enter the domain address in the **Domain** field.
- Enter the installed driver name in the **Model** field.
- Click the **Enable** toggle key to enable the device to access the printer.
- Click the **Default** toggle key to set the printer as the default printer.
- Enter the description for your printer in the **Description** field.
- Enter the network path where the printer is located in the **Location** field.

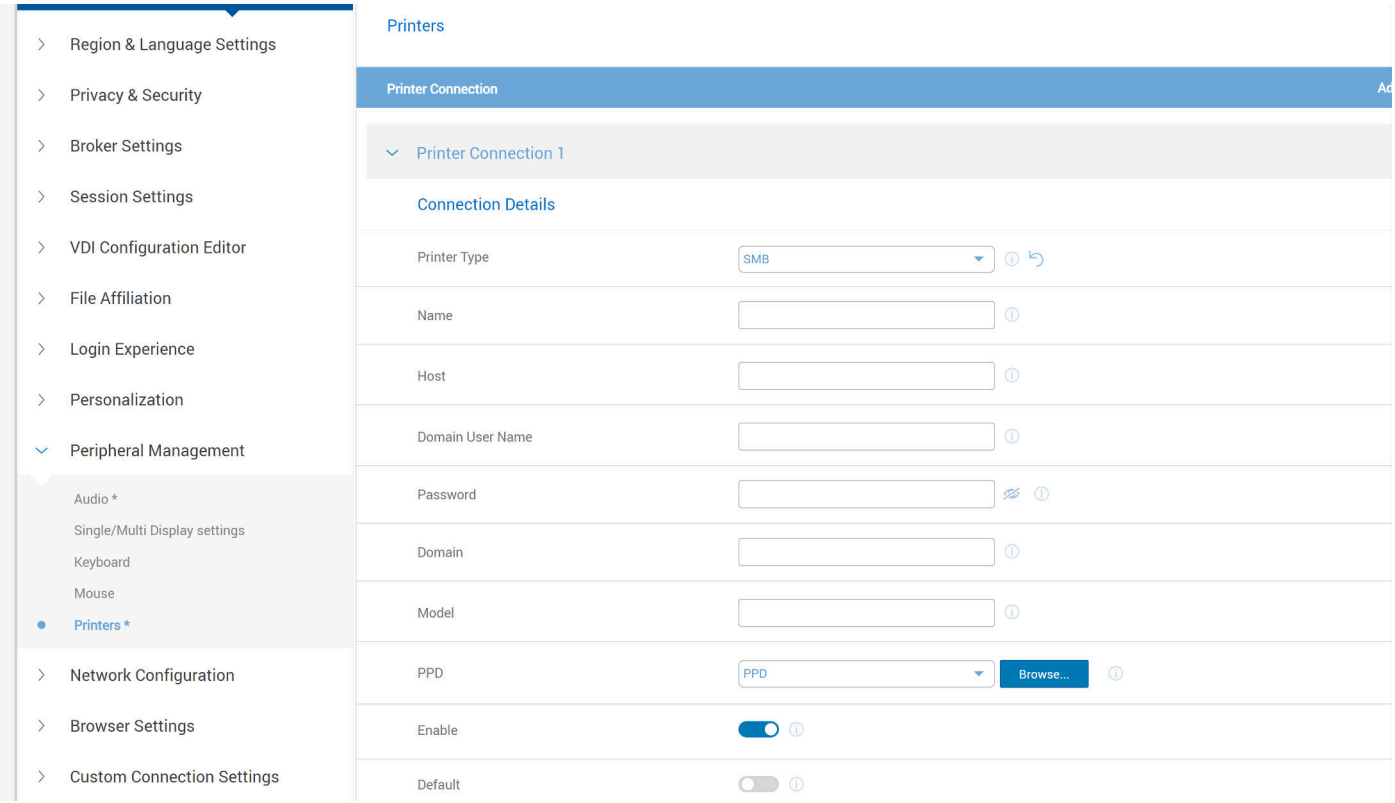


Figure 219. Printer

Configure the URI Printer Settings

You can configure the URI printer settings using Wyse Management Suite.

- Enter the name of the printer in the **Name** field.
- Enter the Uniform Resource Identifier (URI) in the **URI** field. For example, lpd://uncpath or ipaddress/Queuename.
- Enter the installed driver name in the **Model** field.
- Click the **Enable** toggle key to enable the device to access the printer.
- Click the **Default** toggle key to set the printer as the default printer.
- Enter the description for your printer in the **Description** field.
- Enter the network path where the printer is located in the **Location** field.

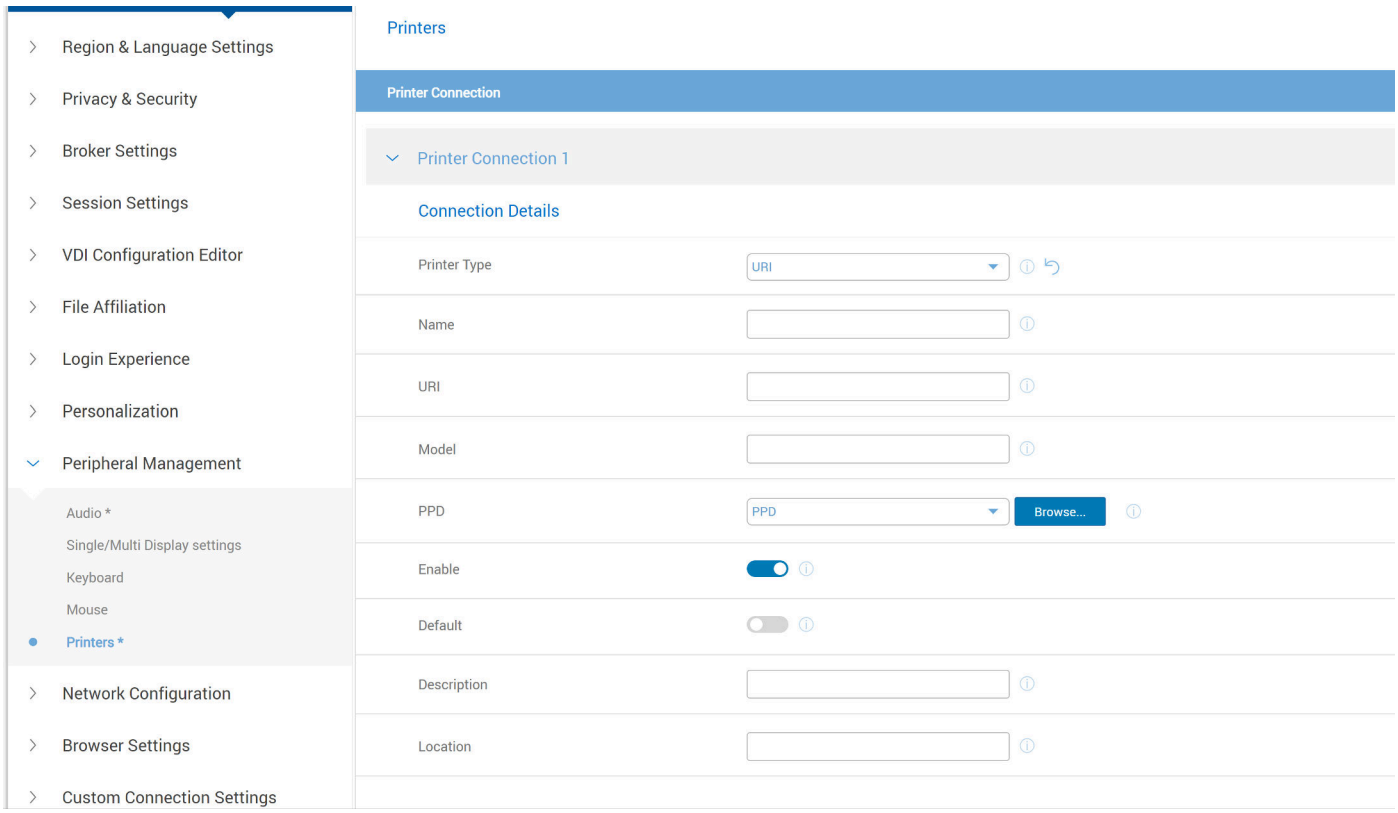


Figure 220. Printer

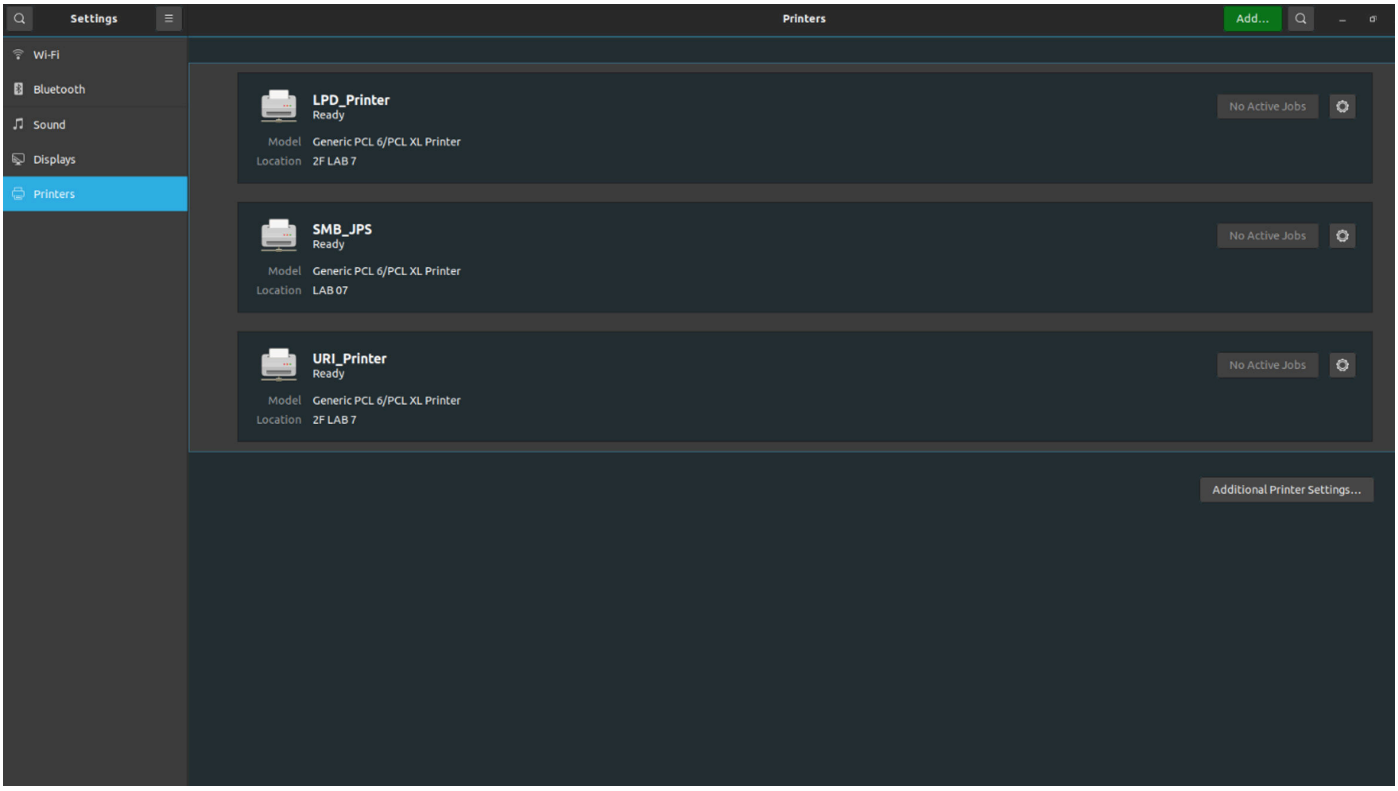


Figure 221. Printers

How to prepare and configure the USB bootable drive with the ISO image

Prerequisites

NOTE: TPM Keys must be cleared before you start the installation since Dell Hybrid Client uses the TPM keys to manage the passwords.

Steps

1. Go to www.dell.com/support.
2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field, type the name of your platform.
3. Click the product from search results to open the product support page.
4. Click the **Drivers & downloads** tab from the product support page.
5. Select **Dell Hybrid Client - Ubuntu 20.04** from the **Operating system** drop-down list.
6. Search for the **Dell Hybrid Client - Conversion image** and download the conversion image for your platform.
   You can download the conversion images for any device from the **Dell Hybrid Client** product support page.
7. Extract the ISO image from the ZIP file.
8. Create a USB bootable media using one of the following methods:
   - For Windows, do the following:
     a. Install the **Dell OS Recovery Tool** on the Windows 10 machine for preparing the USB drive.
     b. Plug in the USB drive to the device and select the USB drive.
     c. Open the **Dell OS Recovery Tool** and select the **SWITCH TO ADVANCED RECOVERY** option.
     d. Under **Select an OS Image**, browse to the extracted ISO file and click **Open**.
     e. Click **NEXT**.
     f. Click **BURN OS**.
   - For Linux, search for the article *How to Download and Use the Dell Operating System Recovery Image in Ubuntu or Linux* at www.dell.com/support and follow the steps from the article.