Dell Hybrid Client

Version 1.x Administrator's Guide

Notes, cautions, and warnings

(i) **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.**

Contents

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 powered by Dell Hybrid Client, thereby eliminating the need for IT support to visit 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 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. The Wyse Management Suite mobile application enables administrators to view critical alerts, notifications on the dashboard, and send real-time commands.

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.

Supported platforms

Dell Hybrid Client 1.6 is a software solution that can be deployed on Ubuntu 20.04-based platforms with a minimum memory or RAM of 8 GB and disk storage of 32 GB or higher capacity.

Ubuntu 20.04-based devices that have Dell Client Agent - Enabler (DCA Enabler) installed can be converted to Dell Hybrid Client version 1.6 using Wyse Management Suite.

- The following platforms are preinstalled with Dell Hybrid Client:
  - Wyse 5070
  - Wyse 5070 Extended
  - OptiPlex 3090 Ultra
  - OptiPlex 7090 Ultra
  - Latitude 3320

  (i) **NOTE:** Dell Hybrid Client version 1.6 is shipped on Wyse 5070, Wyse 5070 Extended, OptiPlex 3090 Ultra, OptiPlex 7090 Ultra, and Latitude 3320 devices after January 2022.

- The following existing platforms with earlier versions of Dell Hybrid Client can be upgraded to Dell Hybrid Client version 1.6 using Wyse Management Suite:
  - Wyse 5070
  - Wyse 5070 Extended
  - OptiPlex 7070 Ultra
  - OptiPlex 3090 Ultra
  - OptiPlex 7090 Ultra
  - Latitude 3320

For information about the supported platforms and configurations for the Dell Hybrid Client conversion, see the *Dell Hybrid Client Version 1.x Conversion and Upgrade Guide* at www.dell.com/support.

(i) **NOTE:** Wyse 5070 devices with 16 GB storage are compatible only with Dell Hybrid Client version 1.1.

Supported management software

Table 1. Supported management software

Dell Hybrid Client version	Supported management software
1.0	Wyse Management Suite Pro Edition 3.0 and later

Table 1. Supported management software (continued)

Dell Hybrid Client version	Supported management software
1.1	Wyse Management Suite Pro Edition 3.1 and later
1.5	Wyse Management Suite Pro Edition 3.2 and later
1.6	Wyse Management Suite Pro Edition 3.5 and later

Supported operating system

Dell Hybrid Client is an application stack based on the Ubuntu operating system. It is a desktop solution by Dell that follows the Software-as-a-Service (SaaS) model of software delivery.

Table 2. Supported operating system

Dell Hybrid Client version	Base operating system
1.0	Ubuntu 18.04
1.1	Ubuntu 18.04
1.5	Ubuntu 20.04
1.6	Ubuntu 20.04

Salient features of Dell Hybrid Client

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

- **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.
- **Active Directory authentication**—Dell Hybrid Client supports user authentication with Active Directory—local AD and On-Prem User Sync with Azure AD.
- **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 applications depending on the mode which is active.
  - **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.
  - **VDI mode**—In the VDI mode, the client shows the VDI published applications.

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

What is new in Dell Hybrid Client 1.6 release?

In the Dell Hybrid Client version 1.6 release, the following features are newly supported:

- Wyse Management Suite Pro version 3.5. See, Supported management software
- Additional language add-ons. See, Multi language support.
- Additional language layouts. See, Configure the peripheral settings locally.
- Pin applications and browser URLs to desktop. See, Pin an application to desktop and Create a desktop shortcut to a browser URL.
- BIOS firmware upgrade using Wyse Management Suite. See, Upgrade BIOS.
- Browser settings enhancements that include command-line parameters and policy configurations. See, Configure the browser shortcut settings and Custom policy configuration for Firefox and Chrome

- Support for PFX certificates. See, Install a certificate.
- Block keyboard shortcuts. See, Block keyboard shortcuts.
- Switch user capability. See, Switch users.
- System Information enhancements that include Wyse Management Suite registration status and ENERGY STAR ratings. See, Viewing system information.
- Supports certificate-based smart card authentication. See, Log in as a domain user using a smart card.
- Ability to log in to Dell Hybrid Client when the Wyse Management Suite license has expired.
- EULA acceptance from Wyse Management Suite. See, Accept EULA.
- Persistent local user. See, Configure the local user account settings and Log in as a local user.
- Open box security profile. See, Configure the security profile settings.
- Automatic Time Zone. See, Configure the date and time.
- Power control settings. See, Configure the power control settings.
- Third-party application dependency resolution. See, Installing third-party applications.
- Secure Certificate Enrollment Protocol. See, Simple Certificate Enrollment Protocol.
- IEEE 802.1x network authentication. See, Network authentication using IEEE 802.1x.
- Ability to change the log password. See, Change the log password.
- Single application mode. See, Configuring the single application mode.
- Device Settings enhancements that include Advanced Settings. See, Configure the advanced settings locally.
- Troubleshooting menus. See, Configure the troubleshooting options.
- Network Drive configuration from Device Settings. See, Configure the network drive locally.
- Enhanced single or multidisplay settings. See, Configure the display settings.
- Dell File Explorer usability and UI enhancements. See, About Dell File Explorer.
- Box personal storage. See, Connect to Box cloud drive.
- Azure Virtual Desktop. See, Configuring Azure Virtual Desktop.
- Imprivata PIE enablement. See, Configuring Imprivata PIE.
- Ability to automatically launch VDI applications. See, Configuring the VDI environment.
- Optimization package for better performance. See the *Dell Hybrid Client Version 1.x Release Notes* at www.dell.com/support.

What's new in Dell Hybrid Client 1.5 release?

In the Dell Hybrid Client version 1.5 release, the following features are newly supported:

- Ubuntu 20.04 operating system.
- Wyse Management Suite Pro version 3.2.
- Additional hardware platforms—OptiPlex 3090 Ultra, OptiPlex 7090 Ultra and Latitude 3320. See, Supported platforms.
- Different levels of **Security Profiles** to enhance device security for deploying third-party applications. See, Configure the security profile settings.
- **Power Profiles** to provide efficient power management capabilities for devices. See, Configure the power profile settings.
- **Virtual Private Network (VPN)** to connect to your corporate network from home or external networks. See, Configure the VPN settings.
- ZFS file system to encrypt the user home directory on Dell Hybrid Client. See, User data encryption using ZFS file system.
- Multifactor authentication for local and Active Directory login using a smart card. See, Log in as a domain user using a smart card
- Multifactor authentication for browser-based Azure and Google Workspace login to cloud applications using a smart card. See, Multifactor authentication for cloud applications.
- Multi-factor authentication from initial login to the Citrix VDI session (SSO) using a smart card. See, Single Sign-On (SSO) to VDI applications.
- Multifactor authentication for Citrix and VMware VDI sessions using a smart card. See, Multifactor authentication for VDI applications.
- Single Sign-on (SSO) into Google Cloud using Active Directory Federation Services (ADFS). See, Connect to Google Workspace.
- Personal OneDrive account for Azure and Google Workspace. See, Configure personal accounts for Azure and Configure personal accounts for Google Cloud.
- Automatic and immediate synchronization of file data when a file is edited on the local, network share, cloud, or VDI. See, Using Dell File Explorer.
- **Open with** function that enables you to choose an application to open a file in Dell File Explorer. See, Open with functionality.

- Autoupdate policy to automatically update certain applications when a new version of the application is launched on Dell Hybrid Client. Configure the autoupdate settings.
- Advanced user data roaming across devices that are powered by Dell Hybrid Client. See Configure the user profile roaming settings.
- **Secure Boot** to guard the boot process of the device that is powered by Dell Hybrid Client. This option is enabled by default.
- Ability to generate a random GRUB password when the device that is powered by Dell Hybrid Client is powered on for the first time. See, Generate the GRUB password.
- Ability to format a USB storage device that is connected to Dell Hybrid Client. See, Format a USB device.
- Enhanced User Interface for Device Settings and Dell File Explorer. See, Configuring the local settings and Using Dell File Explorer.
- Menu options under the Dell Hybrid Client Policy Settings on Wyse Management Suite version 3.2 are rearranged for better grouping and visibility. See, Managing the Dell Hybrid Client policy settings.

What's new in Dell Hybrid Client 1.1 release?

- Ability to convert Wyse 5070 devices running Windows 10 IoT Enterprise, ThinLinux 2.x, or ThinOS 8.6 (Maintenance Release 8 and later) to Dell Hybrid Client. For more information about the conversion process, see the *Dell Hybrid Client Conversion Guide* at www.dell.com.support.
- Ability to convert OptiPlex 7070 devices running Windows 10 and Ubuntu 18.04 to Dell Hybrid Client. For more information about the conversion process, see the *Dell Hybrid Client Conversion Guide* at www.dell.com.support.
- Ability to remotely connect to Dell Hybrid Client using the SSH protocol. See, Configure the SSH settings.
- Ability to remotely connect to Dell Hybrid Client using VNC. See, Configure the VNC settings.
- Ability to enable or disable the access to desktop shortcuts. See, Enable or disable access to desktop shortcuts.
- Supports custom connections for browser shortcuts and local applications on Dell Hybrid Client. See, Configure the custom connection settings and Configure the browser shortcut settings.
- Supports the autologin feature for a guest user. See, Configure the guest user account settings.
- Supports installation of unsigned and custom-signed third-party applications in addition to Dell-signed applications. See, Installing third-party applications.
- Supports localized User Interface for Dell Hybrid Client. See, Multilanguage support.
- (i) **NOTE:** Configuration User Interface must be updated to v1.0.112 for on-premises Wyse Management Suite v3.1 to support Dell Hybrid Client 1.1 features. You can download the Configuration User Interface package from the Wyse Management Suite drivers page at www.dell.com/support. For public cloud tenants or customers, the Configuration User Interface package is upgraded by Dell Technologies. For more information about how to upload and apply the Configuration User Interface package, see the *Dell Wyse Management Suite v3.1 Administrator's Guide* at www.dell.com/support.

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 v1.x Release Notes* provides information about new features and known issues in each Dell Hybrid Client release.
- The *Dell Hybrid Client v1.x Conversion Guide* provides information about how to convert your devices running ThinOS, ThinLinux, Windows, or Ubuntu to Dell Hybrid Client.
- The *Dell Hybrid Client v1.x Security Guide* provides guidelines that help you maximize the security of your devices powered by Dell Hybrid Client.
- The *Dell Hybrid Client v1.x Restore Guide* provides steps to restore Dell Hybrid Client to its factory state on a supported device.
- The *Dell Wyse Management Suite 3.x Administrator's Guide* provides information about configuration, and maintenance of the devices powered by Dell Hybrid Client by using the Wyse Management Suite console.

Dell Hybrid Client installation

Dell Hybrid Client 1.6 is a software solution that can be deployed on Ubuntu 20.04-based platforms with a minimum memory or RAM of 8 GB and disk storage of 32 GB or higher capacity.

Ubuntu 20.04-based devices that have Dell Client Agent - Enabler (DCA Enabler) installed can be converted to Dell Hybrid Client version 1.6 using Wyse Management Suite.

- The following platforms are preinstalled with Dell Hybrid Client:
  - Wyse 5070
  - Wyse 5070 Extended
  - OptiPlex 3090 Ultra
  - OptiPlex 7090 Ultra
  - Latitude 3320

  (i) **NOTE:** Dell Hybrid Client version 1.6 is shipped on Wyse 5070, Wyse 5070 Extended, OptiPlex 3090 Ultra, OptiPlex 7090 Ultra, and Latitude 3320 devices after January 2022.

- The following existing platforms with earlier versions of Dell Hybrid Client can be upgraded to Dell Hybrid Client version 1.6 using Wyse Management Suite:
  - Wyse 5070
  - Wyse 5070 Extended
  - OptiPlex 7070 Ultra
  - OptiPlex 3090 Ultra
  - OptiPlex 7090 Ultra
  - Latitude 3320

DCA-Enabler (DCAE)

Dell Client Agent-Enabler is a client agent for managing Dell Hybrid Client on devices. DCA-Enabler allows you to do the following actions that are managed by Wyse Management Suite:

- Registration
- Real-Time Commands (RTC)
- Unregistration from server
- Standard Application Policy
- Only certificate policy

You must do the following to install Dell Hybrid Client on the device:

1. Register the device to Wyse Management Suite using one of the following methods:
   - Register automatically by configuring the appropriate option tags on the DHCP server. See, Registering Dell Hybrid Client by using DHCP option tags.
   - Register automatically by configuring the appropriate DNS SRV records on the DNS server. See, Registering Dell Hybrid Client by using DNS SRV record.
   - Register using manual discovery method (reg.json). See the *Register Dell Hybrid Client by using manual discovery method* section in *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.
2. Reimage your device using the **Reimage** option on Wyse Management Suite. For more information about how to reimage the device, see Dell Hybrid Client recovery imaging.

Depending on the version of the Dell Hybrid Client software that you have installed on your device, configure the following options when you start Dell Hybrid Client for the first time:

- **Devices powered by Dell Hybrid Client version 1.6**—A random GRUB password is generated. As an administrator, you must change the **GRUB** password using Wyse Management Suite. Bremen user is renamed as admin user. The password is same as the GRUB password. You can use the GRUB password to access the admin account for managing sudo or elevated privileges. For more information about how to change GRUB password, see Enable GRUB menu password protection.
- **Devices powered by Dell Hybrid Client version 1.5**—A random GRUB password is generated. As an administrator, you must change the **GRUB** password using Wyse Management Suite. There is no provision to change the Bremen password as you can use GRUB password itself to access the Bremen account for managing sudo or elevated privileges. For more information about how to change GRUB password, see Enable GRUB menu password protection.

- **Devices powered by Dell Hybrid Client version 1.1**—As an administrator, you must change the default **GRUB** password and **Bremen** password using Wyse Management Suite. For more information about how to change GRUB password and Bremen password, see Enable GRUB menu password protection and Configure the Bremen password.

Firmware upgrade

Use Wyse Management Suite to upgrade your Dell Hybrid Client firmware to the latest version. Before upgrading to Dell Hybrid Client version 1.6, you must first install the **dhc-disable-sleep-suspend** package using Wyse Management Suite.

For detailed information about the upgrade process, see the *Dell Hybrid Client Version 1.x Conversion and Upgrade Guide* at www.dell.com/support.

Table 3. Supported management software for firmware upgrade

Dell Hybrid Client firmware upgrade scenario	Supported management software
1.0 to 1.1	Wyse Management Suite Pro Edition 3.1 and later
1.0 or 1.1 to 1.5	Wyse Management Suite Pro Edition 3.2 and later
1.0, 1.1, or 1.5 to 1.6	Wyse Management Suite Pro Edition 3.5 and later

Upgrade BIOS

From Dell Hybrid Client version 1.6 onwards, you can use Wyse Management Suite to upgrade BIOS.

Prerequisites

- Register your device to Wyse Management Suite and create a group.
- Do the following 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 `.cab` file.

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—`\repository\hybridClientApps`.

   For example, `C:\WMS\LocalRepo\repository\hybridClientApps` for on premises and `C:\WMSRepo3\repository\hybridClientApps` for remote repository.
3. In the **Apps & Data** tab, under **App Policies**, click **Hybrid Client**.
4. Click **Add Policy**.
5. Enter the policy name, group name, task, and OS type.
6. From the **Application** drop-down list, select the BIOS file.
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.
9. Click **Update**.
   After the BIOS is downloaded successfully, the device restarts and updates the BIOS automatically.

Registering Dell Hybrid Client to Wyse Management Suite

Register Dell Hybrid Client manually

Prerequisites

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

ⓘ **NOTE:** If you are using Dell Hybrid Client 1.6 and later versions, you must authenticate to open the Dell Client Agent (DCA) window and register the device to Wyse Management Suite.

ⓘ **NOTE:** If you are using Dell Hybrid Client 1.5 and earlier versions, you can register the device only from the guest user account. As a guest user, you can unregister the device from Wyse Management Suite only in developers mode. Domain users cannot unregister the device from Wyse Management Suite.

Steps

1. Log in to Dell Hybrid Client as a guest user. By default, the username is `guest`.
2. Depending on the Dell Hybrid Client version that is installed on the device, configure the following options:
   - If you are running Dell Hybrid Client 1.5 and earlier versions, do the following:

     a. On the top bar, click .

     b. Click **Dell Client Agent**.

        The **Dell Client Agent** window is displayed.

   - If you are running Dell Hybrid Client 1.6, do the following:

     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 the Dell Client Agent window for the first time.

     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:** From Dell Hybrid Client version 1.6 onwards, user can unregister the device after authenticating to the DCA window using the GRUB password. If you are using earlier versions of Dell Hybrid Client, administrators or guest users cannot unregister the device directly from the **Dell Client Agent** window. To unregister the device, you must either enter the dev mode or use the Wyse Management Suite console.

Registering Dell Hybrid Client by using DHCP option tags

Table 4. Register Dell Hybrid Client by using DHCP option tags

Option Tag	Description
Name—WMS **Data Type**—String **Code**—165 **Description**—WMS Server URL	This tag specifies the Wyse Management Suite server URL. For example, `https://wms.dell.com:443` or `https://www.wysemanagementsuite.com`.
Name—CA Validation **Data Type**—String **Code**—167 **Description**—Certificate Authority Validation	You can enable or disable CA validation option if you are registering your devices with Wyse Management Suite on private cloud. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False**, if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. > ⓘ **NOTE:** If the value is not configured, **True** is considered as the default value.
Name—GroupToken **Data Type**—String **Code**—199 **Description**—Group Token	This tag is required to register your device with Wyse Management Suite on a public cloud or on-premises. If the tag is not available, devices are automatically registered to the unmanaged group during on-premises installation.

> ⓘ **NOTE:** You must manually log in as a guest user on each device, accept the End-User License Agreement (EULA), and then wait for the device to register to Wyse Management Suite.

Registering Dell Hybrid Client by using DNS SRV record

DNS-based device registration is supported on Dell Hybrid Clients. You can register devices with the Wyse Management Suite server if DNS SRV record fields are set with valid values.

Table 5. Configuring device by using DNS SRV record

URL/Tag	Description
Record Name—_WMS_MGMT **Record FQDN**— _WMS_MGMT._tcp.<Domainname> **Record Type**— SRV	This record specifies the Wyse Management Suite server URL. While configuring the SRV record, add the port number 443 in port number field, and provide the Wyse Management Suite URL in the **Host** field. For example, `https://wms.dell.com:443`, where wms.dell.com is the fully qualified domain name of the server where Wyse Management Suite is installed and 443 is the port number.
Record Name—_WMS_GROUPTOKEN **Record FQDN**— _WMS_GROUPTOKEN.<Domain> **Record Type**— TEXT	This tag is required to register your device with Wyse Management Suite on public cloud. If the tag is not available, devices are automatically registered to the unmanaged group during on-premises installation.
Record Name—_WMS_CAVALIDATION **Record FQDN**— _WMS_CAVALIDATION.<Domain> **Record Type**—TEXT	You can enable or disable the CA validation option if you are registering your devices with Wyse Management Suite on private cloud. Enter **True**, if you have imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. Enter **False**, if you have not imported the SSL certificates from a well-known authority for https communication between the client and Wyse Management Suite server. ⓘ **NOTE:** If the value is not configured, **True** is considered as the default value.

ⓘ **NOTE:** You must manually log in as a guest user on each device, accept the End-User License Agreement (EULA), and then wait for the device to register to Wyse Management Suite.

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 auto-discovered 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.

ⓘ **NOTE:** The **Enrollment Validation** option is disabled for existing tenants in the public cloud or when you upgrade on-premise tenants.

The validation status of the devices is also displayed in the **Devices** section on the **Dashboard** page.

For more information about validating enrollment, see Validate the enrollment of a device.

Validate the enrollment of a device

You can enable **Enrollment Validation** to allow administrators to control the manual and auto registration process of devices powered by Dell Hybrid Client to a group. You can filter the devices in **Pending Validation** state by clicking the **Pending** count in the **Dashboard** page or by selecting the **Enrollment Validation Pending** in the **Status** drop-down list on the **Devices** 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.

> (i) **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

Managing user accounts

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

(i) **NOTE:** The local user account is supported from Dell Hybrid Client version 1.6 onwards.

- **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.
- **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 disable, 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.
- **Guest user**—Enables users to access Dell Hybrid Client when they do not have an AD account. 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.

(i) **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.

(i) **NOTE:** When the autologin feature is enabled, the local user takes priority over the guest user.

Joining Active Directory

Dell Hybrid Client supports user authentication with Active Directory, both local AD and On-prem User Sync with Azure AD. 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

- 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.
- 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 group.

   (i) **NOTE:** The Domain join SignOn option is available on the default device policy group.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Login Experience**, and click **Domain join**.

   (i) **NOTE:** If you are using Dell Hybrid Client earlier than version 1.6, expand **SignOn** 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.
9. In the **Domain** field, enter the complete domain name. For example, test.local, test.com, and child.test.com.
10. 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`.

11. In the **Workgroup** field, enter the name of the workgroup specific to your organization.
12. 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.

   (i) **NOTE:** Domain unjoin is not supported on devices that are upgraded from Dell Hybrid Client v1.0.1288 to v1.1.1618. Workaround is to reimage the device from Wyse Management Suite.

Next steps

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

Configure the guest user account settings

The Guest account is a low-privilege account that is available for users who do not have an AD account, but need access to Dell Hybrid Client. You can enable or disable the guest user account using Wyse Management Suite. If you have logged in as a guest user, 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.

   (i) **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.

Next steps

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

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. The local user account is supported from Dell Hybrid Client 1.6 onwards.

Steps

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

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **Advanced Local User Account Properties**.

   > (i) **NOTE:** If you want to add a local user in Dell Hybrid Client 1.1.01 release, use the **Local User Account Properties** available under **Privacy & Security**.

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.

> (i) **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.

> (i) **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**.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.

4. Click the **Advanced** tab.

5. Expand **Login Experience**, and click **Previously Logged-in User List**.

ⓘ **NOTE:** If you are using Dell Hybrid Client earlier than version 1.6, **SignOn**, 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.

GRUB menu password

GRUB is the default boot loader for Dell Hybrid Client. Dell Hybrid Client enables you to set a password for the GRUB boot menu to restrict access to the following operations:

● Enabling dev mode to access the terminal—You can use the Bremen account on this mode to manage sudo or elevated privileges.
● User access to the GRUB boot menu

A random GRUB password is generated when you start a device that is powered by Dell Hybrid Client for the first time. This feature is available from Dell Hybrid Client version 1.5 onwards.

As an administrator, you must change the default GRUB password. For information about how to set the GRUB password, see Enable GRUB menu password protection.

ⓘ **NOTE:** Changing the GRUB password is mandatory and you cannot leave the password field blank.

GRUB password change compliant—When the GRUB password is changed, the device compliance status on the **Devices** page on Wyse Management Suite displays green. This feature is available from Wyse Management Suite Pro version 3.2 onwards.

When you hover over the green mark, the status is displayed as **Compliant**. If the default GRUB password is not changed, the device compliance status shows red. When you hover over the red mark, the status is displayed as **Grub password not changed**. The administrator must change the GRUB password to change the device status to **Compliant**.

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

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

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

Enable GRUB Menu 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **GRUB Password**.
6. In the **GRUB 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 GRUB Menu password during the initial setup for improved security.

7. Click **Save & Publish**.
8. Power on the device.
9. During boot, keep tapping the Esc key to enter the GRUB menu. When prompted, enter the password that you have specified in Wyse Management Suite.

View the GRUB 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.
   (i) **NOTE:** If you are using Dell Hybrid Client earlier than version 1.6, click **GRUB Password** from the **More Actions** drop-down list.
5. Select the **Show Password** check box to view the password.
6. Click **OK** to close the dialog box.

Generate the GRUB password

If the device registration to the Wyse Management Suite server fails, the administrator can generate a GRUB password using the **Portal Administration** tab on the Wyse Management Suite console. This feature is available from Dell Hybrid Client version 1.5 onwards.

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.

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

Getting started with Dell Hybrid Client

Accept End User License Agreement using Wyse Management Suite

From Dell Hybrid Client 1.6 onwards, you can read and accept EULA from Wyse Management Suite. If you have accepted EULA on Wyse Management Suite, the EULA acceptance window is not displayed on the device screen when you boot the device for the first time. If the administrator has accepted EULA on Wyse Management Suite and if your device is discovered using DNS/DHCP, EULA is not displayed on the device. If your device is not automatically discovered, you must manually accept EULA on the device.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **License and Agreement**, and click **End-User License Agreement**.
6. From the **EULA** drop-down list, select **Read EULA**.
   The license and Agreement window is displayed.
7. Read the EULA and click **Accept**.
8. Click **Save and Publish**.

Logging in to your Dell Hybrid Client

It is recommended that you connect the device using a wired network connection.

ⓘ **NOTE:** From Dell Hybrid Client 1.6 onwards, user can log in to the device even when the Wyse Management Suite license has expired.

Log in as a guest user

As a **guest user**, you can log in to the guest account. By default, the guest user account is enabled on your Dell Hybrid Client. If you have logged in as a guest user, 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.

Prerequisites

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

Steps

1. Start the device powered by Dell Hybrid Client.
2. On the login screen, enter the username as `guest`.
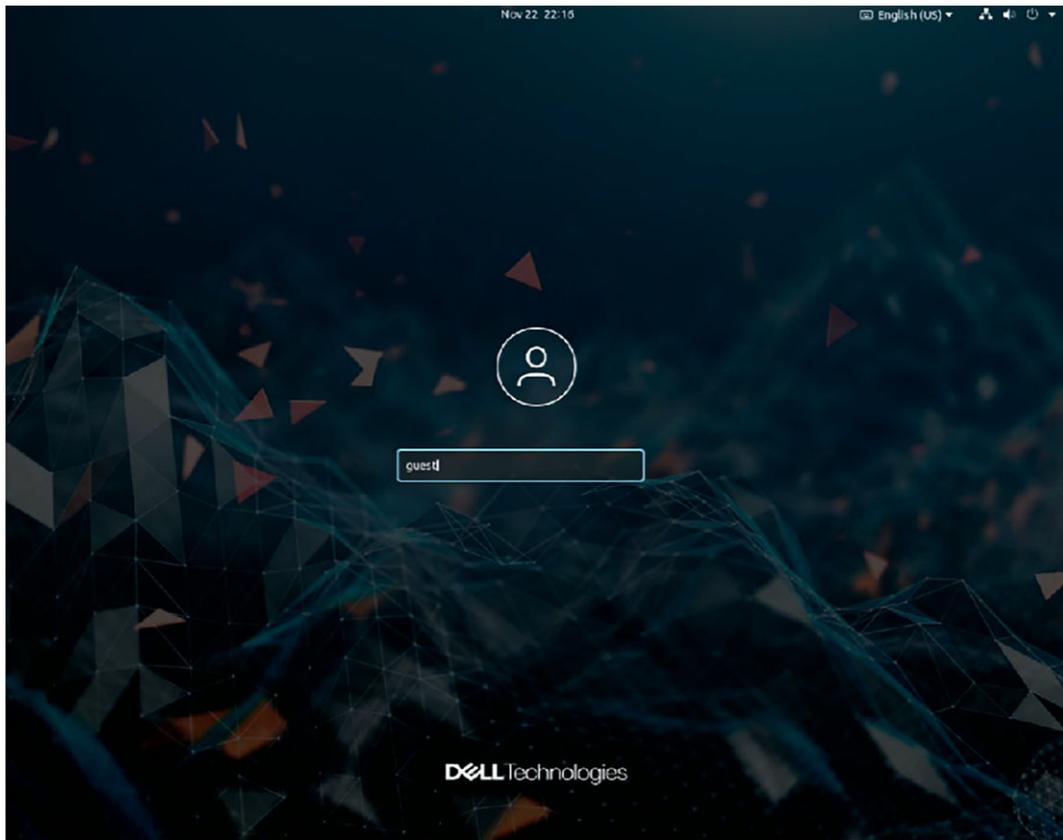
Figure 1. Username screen — Dell Hybrid Client version 1.6

> (i) **NOTE:** If the auto sign-on option is enabled, the guest user can automatically log in to Dell Hybrid Client without entering the username.

3. Press **Enter**.

   Dell Hybrid Client boots to the desktop screen.

   > (i) **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.

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`.
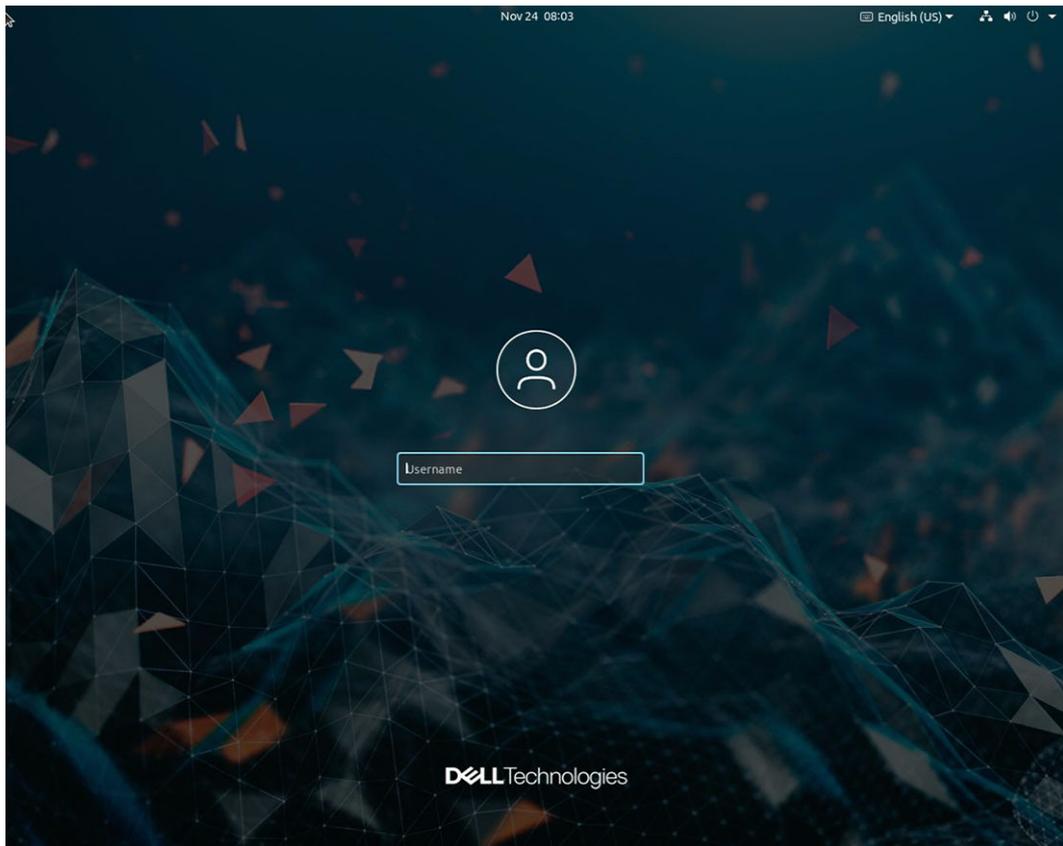
Figure 2. Username screen — Dell Hybrid Client v1.6

3. Press **Enter**.
4. Enter the domain password.
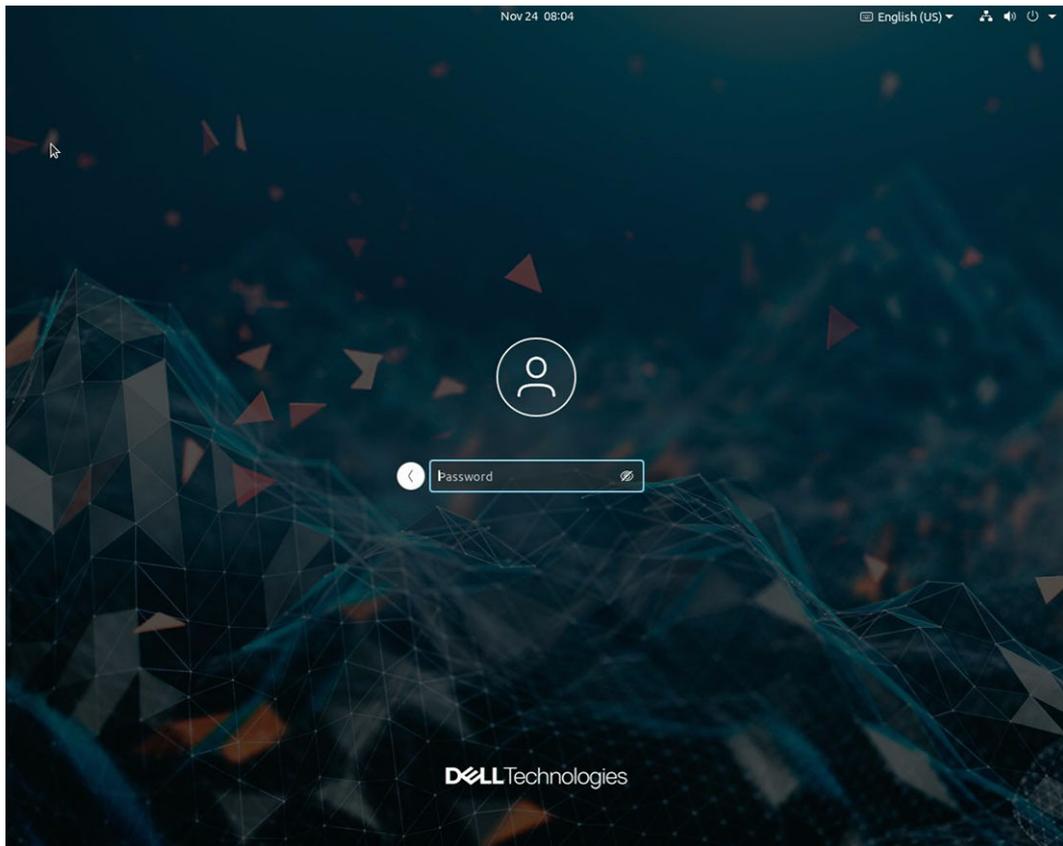
Figure 3. Password screen — Dell Hybrid Client v1.6

5. Click **Sign 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.

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**.

   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.

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. This feature is available from Dell Hybrid Client version 1.5 onwards. 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. When using Wyse Management Suite to deploy the driver package, set the security profile to **Low**.
- 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.

Steps

1. Start the device.
2. Connect a supported smart card reader to the device.
3. Tap 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.

Configure the date and time

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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. This option is applicable from Dell Hybrid Client version 1.6 onwards.
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.

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

10. Click **Save and Publish**.

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.

(i) **NOTE:** In every Dell Hybrid Client release, the default desktop background wallpaper may be changed.
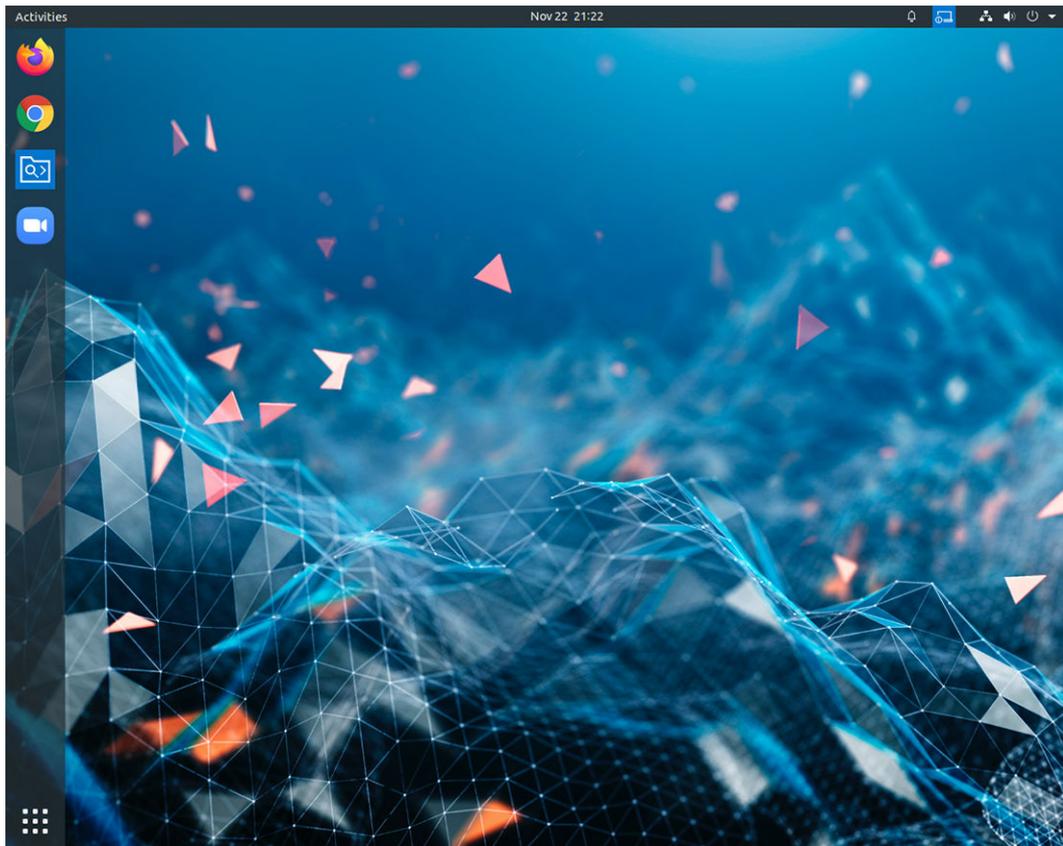
Figure 4. Desktop overview — Dell Hybrid Client version 1.6

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. If you are using Dell Hybrid Client 1.5 and earlier versions, the DCA icon is displayed on the top bar.
- **Taskbar**—Displays all your favorite applications.

Using the top bar

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

Table 6. 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.
Dell Client Agent icon ▦	Displays the Dell icon that allows you to access the **Dell Client Agent (DCA)** settings window. This option is applicable only for DHC 1.5 and earlier versions.
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.

Table 6. Top bar elements (continued)

Element	Description
	- **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. - **Bluetooth icon**—Enables you to turn on or turn off Bluetooth. - **VPN icon**—Enables you to connect or disconnect a VPN. - **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

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.
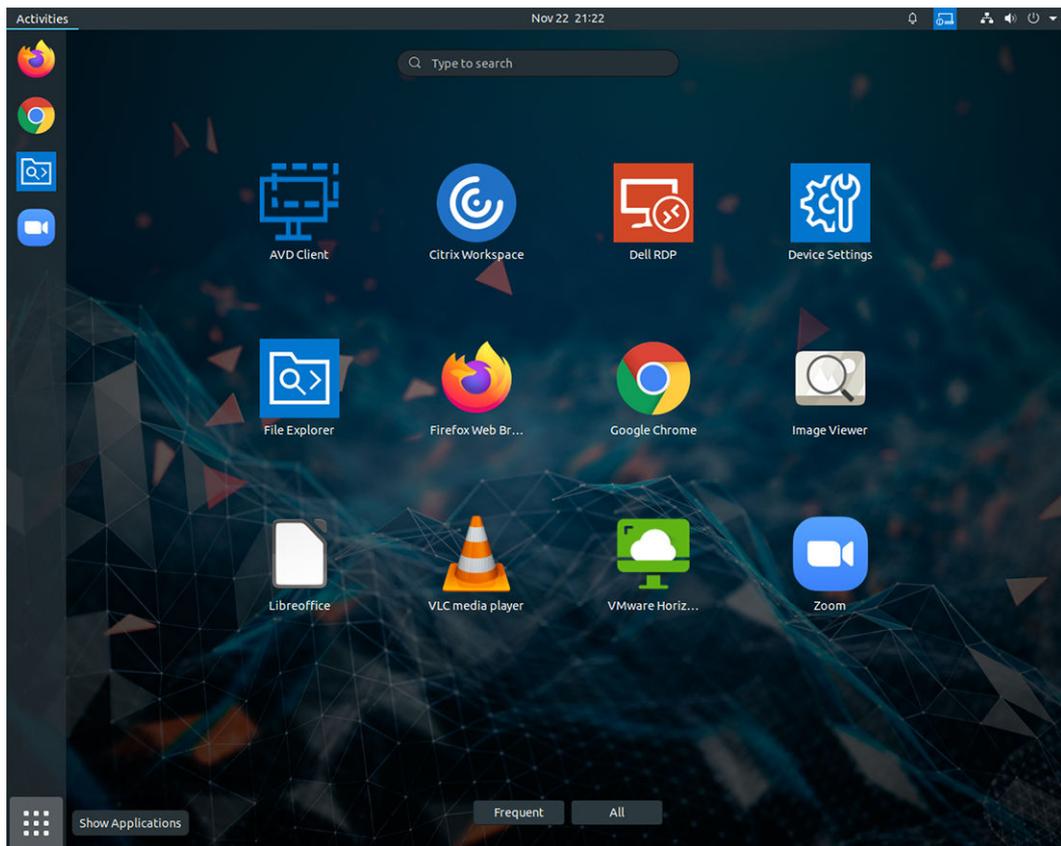
Figure 5. Applications overview screen in Dell Hybrid Client 1.6

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 upon system startup in both user and guest mode.
- **VLC Media Player**—Enables you to play multimedia files.
- **Libre Office Suite**—Enables you to create and edit text documents, spreadsheets, presentation, drawings, and so on.
- **Text Editor**—Enables you to edit your text. This is applicable for Dell Hybrid Client 1.1.01 and 1.5 versions.
- **Image Viewer**—Enables you to open an image file.
- **Zoom client**—Enables you to join a Zoom meeting. Zoom client is not available as a default application on Wyse 5070 devices with 16 GB storage capacity.
- **Connection and application shortcuts**—Enables you to quickly access all the available VDI connections, published applications, and cloud applications. Citrix and VMware clients are not available as a default application on Wyse 5070 devices with 16 GB storage capacity.
- **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** or **Add to Favorites**.

Shut down, log off, or restart

The **Power Off** option enables you to shut down the device powered by Dell Hybrid Client. 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. Click the **Power Off/Log out** button, and do either of the following:
   - **Power Off**—Click the **Power Off** option and do one of the following:
     - **Power Off**—Click the **Power Off** option to immediately shut down the device.
       - (i) **NOTE:** The device automatically restarts after 60 s.
     - **Restart**—Click the **Restart** option to restart the device.
     - **Cancel**—Click the **Cancel** option to cancel system shutdown or restart.
   - **Suspend**—Click the **Suspend** option to enter the sleep mode.
   - **Log out**—Click the **Log out** button and do one of the following:
     - **Log out**—Click the **Log out** button to log out of your user account.
     - **Cancel**—Click the **Cancel** option to cancel the logoff action.

(i) **NOTE:** You can access the Logout and Cancel window by pressing the Ctrl+Alt+Delete key combination.

(i) **NOTE:** Power Off, Restart, Suspend, and Logout options can be enabled or disabled from **Advanced** > **Personalization** > **Desktop** > **Power Control Settings** on Wyse Management Suite.

(i) **NOTE:** The GDM power off options can be enabled or disable from **Advanced** > **Login Experience** > **Login screen power** on Wyse Management Suite.

Lock your desktop

The lock screen functionality enables you to secure your device powered by Dell Hybrid Client when you leave your desk. The lock screen displays the date, time, and volume control.

Steps

1. On the top bar, click the **System menu** icon.
2. Click the **Lock** button to lock your screen.

   (i) **NOTE:** You can press the Super + L key combination on your keyboard to lock the desktop.

Next steps

To unlock your screen, click the **Unlock** button from the **System menu**. You can also press the Esc + Enter key combination on your keyboard to unlock your screen.

Managing the Dell Hybrid Client policy settings

You can configure and manage your devices powered by Dell Hybrid Client using the **Hybrid Client** 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 **Hybrid Client**.

   The **Configuration Control | Hybrid Client** window is displayed.

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

   The **Standard** tab lists all the common settings. The **Advanced** tab lists all the advanced 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**.

(i) **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 | Hybrid Client** window:

Table 7. Dell Hybrid Client policy settings

Feature	Sub feature—User policy group	Sub feature—Device policy group
Peripheral Management	Display settings	Display settings
	Mouse	Printers
	Keyboard	Audio
		Mouse
		Keyboard
Network Configuration	Not applicable	Wireless
		Proxy settings
		Bluetooth settings
		VPN
Browser settings	Google Chrome settings	Browser shortcuts
	Firefox settings	
	Browser shortcuts	
	Default Browser	
Custom Connections	Custom Connections	Custom Connections
Region & Language settings	Region and Time	Region and Time
		Language
		Time Server
Personalization	Desktop	Desktop
	User Data Roaming	Device info
Login Experience	Not applicable	Domain join
		Previously Logged-in User List
Privacy & Security	Not applicable	Security profile*
		Certificate
		Guest user account properties
		USB Lockdown
		GRUB password
		Bremen password¹
		VNC Server
		SSH Server
Power Settings	Power saving	Power saving
	Suspend and Power button	Suspend and Power button
	Power Profile	
Broker Settings	Citrix Broker Settings	Citrix Broker Settings
	VMware Broker Settings	VMware Broker Settings
	Microsoft Remote Desktop Settings	Microsoft Remote Desktop Settings
Session Settings	Citrix Session Settings	Citrix Session Settings
	VMware Session Settings	VMware Session Settings

Table 7. Dell Hybrid Client policy settings (continued)

Feature	Sub feature—User policy group	Sub feature—Device policy group
File Affiliation	File Affiliation	File Affiliation
	Citrix File Type Association	Citrix File Type Association
	VMware File Type Association	VMware File Type Association
	RDP File Type Association	RDP File Type Association
WMS Settings	Not applicable	WMS client settings
		Deployment Settings
Application Security Settings	VLC Media Player	VLC Media Player
	Image Viewer	Image Viewer
	Libre Office	Libre Office
	Application Access Control	Application Access Control
	Application Deployment[1]	Application Deployment[1]
Network Drives	Network Drives list	Network Drives list
BIOS	Not applicable	Select your DHC platform.

*This option is applicable only for devices powered by Dell Hybrid Client version 1.5.

[1]This option is applicable only for devices powered by Dell Hybrid Client version 1.1.

Viewing system information

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

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, 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).
  - **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, and ENERGY STAR ratings. This tab is added from Dell Hybrid Client version 1.6 onwards.
- **Event Logs**—Displays major events.

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**.

Enable or disable access to desktop shortcuts

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Application Security**, and click **Application Access Control**.
6. Enable or disable access to one or more applications from the following categories:
   - **Web browsers**—Google Chrome and Firefox.
   - **Dell Hybrid Client applications**—Dell File Explorer and Device Settings.
   - **VDI applications**—Citrix, VMware, and RDP.
   - **Productivity applications**—Text Editor, VLC Media Player, Image Viewer, Libre Office, and Zoom (supported in Dell Hybrid Client version 1.5).
   - **Single Application Mode configurations**—Enables you to limit the device to present or use a single application that takes over the local gnome desktop. This feature is supported from Dell Hybrid Client version 1.6 onwards. See, Single application mode.

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

7. Click **Save and Publish**.

Configuring the printer settings

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.

Use Wyse Management Suite to configure the following printer settings:

- Configure the LPD printer settings
- Configure the SMB printer settings
- Configure the URI printer settings

Dell Hybrid Client also supports USB printing. When a USB printer is connected to the device, it is automatically detected, and you can print from the local system or VDI.

You can also use the printer setup on the local device to configure your printers. For more information, see Configure the peripheral settings locally.

Configure the LPD printer 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Printers**.
6. In the **Printer Connection** section, click **Add Row**.
7. From the **Printer** Type drop-down list, select **LPD**.
8. Enter the name of the printer in the **Name** field.
9. Enter the hostname in the **Host** field. For LPD printer, you can enter the IP address of the printer.
10. 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.
11. Enter the installed driver name in the **Model** field.
12. Click the **Enable** toggle key to enable the device to access the printer.
13. Click the **Default** toggle key to set the printer as the default printer.
14. Enter the description for your printer in the **Description** field.
15. Enter the network path where the printer is located in the **Location** field.
16. Click **Save & Publish**.
17. Log in to Dell Hybrid Client.
    The configured printer is listed.

Configure the SMB printer 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Printers**.
6. In the **Printer Connection** section, click **Add Row**.
7. From the **Printer** Type drop-down list, select **SMB**.
8. Enter the name of the printer in the **Name** field.
9. Enter the hostname in the **Host** field. For SMB printer, you can enter the UNC path of the printer server or the IP address followed by the printer share name.
10. Enter the name of the domain user in the **Domain User Name** field.
    For example, Workgroup (Domain)\Username.
11. Enter the domain password in the **Password** field.
12. Enter the domain address in the **Domain** field.
13. Enter the installed driver name in the **Model** field.
14. Click the **Enable** toggle key to enable the device to access the printer.
15. Click the **Default** toggle key to set the printer as the default printer.
16. Enter the description for your printer in the **Description** field.

17. Enter the network path where the printer is located in the **Location** field.
18. Click **Save & Publish**.
19. Log in to Dell Hybrid Client.
    The configured printer is listed.

Configure the URI printer 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Peripheral Management**, and click **Printers**.
6. In the **Printer Connection** section, click **Add Row**.
7. From the **Printer** Type drop-down list, select **URI**.
8. Enter the name of the printer in the **Name** field.
9. Enter the Uniform Resource Identifier (URI) in the **URI** field.

   For example, lpd://uncpath or ipaddress/Queuename.
10. Enter the installed driver name in the **Model** field.
11. Click the **Enable** toggle key to enable the device to access the printer.
12. Click the **Default** toggle key to set the printer as the default printer.
13. Enter the description for your printer in the **Description** field.
14. Enter the network path where the printer is located in the **Location** field.
15. Click **Save & Publish**.
16. Log in to Dell Hybrid Client.
    The configured printer is listed.

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 *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.
- In Dell Hybrid Client version 1.5, if a guest user wants to create a custom connection with Terminal, the security profile must be set to **Low**. In this scenario, the custom connection is configured with /usr/bin/gnome-terminal from the Wyse Management Suite server. For more information about how to configure security profiles, see Configure the security profile 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Custom Connections**, 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.

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:
- French—France
- German
- Italian
- Spanish—Latin America
- Japanese
- Korean
- Chinese Simplified
- Chinese Traditional
- Russian
- Portuguese-Brazil
- Hebrew

(i) **NOTE:** Russian, Portuguese-Brazil, and Hebrew are supported from Dell Hybrid Client version 1.6 onwards.

Dell Hybrid Client supports the following six locales for Spanish—Latin America:

- Spanish—Argentina
- Spanish—Chile
- Spanish—Colombia
- Spanish—Mexico
- Spanish—Peru
- Spanish—United States

(i) **NOTE:** From Dell Hybrid Client version 1.5 onwards, multilanguage notifications are supported.

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.

(i) **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:
   - **Individual Language add-on package**—Localization add-on for Dell Hybrid Client that is available as an individual package file for each supported language.
   - **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.

Table 8. Language add-ons

Individual Language add-on	Full Language add-on
Add-on is applicable for all devices that are powered by Dell Hybrid Client.	Add-on is applicable for Dell Hybrid Client-based devices with 32 GB and higher storage capacity.
Deploying the add-on installs only the specific language pack on Dell Hybrid Client.	Deploying the add-on installs all the supported language packs on Dell Hybrid Client.
For a device with 16 GB storage capacity, deploying the add-on uninstalls other languages except English.	Multiple language packs can be installed using Wyse Management Suite.

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 *Dell 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 group.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.

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

9. Click **Save and Publish**.

Configure the VPN settings

Dell Hybrid Client enables you to connect to your corporate network from home or external networks using a virtual private network. This feature is available from Dell Hybrid Client version 1.5 onwards. Dell Hybrid Client uses the OpenConnect client that is based on the SSL protocol for connecting to a VPN connection.

Steps

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

   (i) **NOTE:** The power profile option is applicable only for Device Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.

4. Click the **Advanced** tab.

5. Expand **Network Configuration** and click **VPN**.

6. Click the **VPN** toggle switch to enable the VPN connection.

7. If you want to use a VPN profile, click the **Use Profile File for Config** toggle switch, and specify the server profile file for setting up the VPN connection.

8. Click the **Auto Connect** toggle switch to automatically connect to a VPN connection when the device restarts.

9. In the **VPN Server URL** field, enter the IP address or FQDN of the VPN server.

10. From the **Protocol** drop-down list, select either **Cisco AnyConnect** or **GlobalProtect** based on your preference.

11. Click **Save & Publish**.

   (i) **NOTE:** You can also configure the VPN settings locally on Dell Hybrid Client. See, Configure the network settings locally.

Next steps

Connect to a VPN on Dell Hybrid Client. See, Connect to a VPN.

Connect to a VPN

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. Log in to the device powered by Dell Hybrid Client.

2. On the top bar, click the **System menu** icon.

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

4. Enter the username and password.

5. Click **Login**.

Next steps

To disconnect a VPN, click the VPN button from **System menu** and then click **Disconnect**.

Configure the power profile settings

Power Profiles provide efficient power management capabilities for devices that are powered by Dell Hybrid Client. This feature is available from Dell Hybrid Client version 1.5 onwards.

Steps

1. Log in to Wyse Management Suite.

2. Go to the **Groups & Configs** page, and select your preferred user group.

   (i) **NOTE:** The power profile option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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**.

> (i) **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.

Configure the user data roaming settings

Dell Hybrid Client supports user data roaming across devices that are powered by Dell Hybrid Client. When a user logs in to another device with same username, all opened applications and browser data are restored from the previous device. This feature is applicable from Dell Hybrid Client version 1.5 onwards. By default, the user data roaming option is disabled.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.
7. Specify whether the user data roaming must be synchronized when the user logs out of Dell Hybrid Client.
8. From the **User Data Roaming Repository** drop-down list, select either **WMS Repository** or **3rd Party Cloud Repository**.
9. Click **Save & Publish**.
10. Go to the **Groups & Configs** page, and select your preferred **User Policy** group.
11. Go to the **Advanced** tab, expand **Personalization**, and click **User Data Roaming**.
12. Enable one or more options from the following list to allow data roaming across devices that are powered by Dell Hybrid Client:
    - **Chrome Browser Data**—Bookmarks, current tabs, history, last tabs, preferences, shortcuts, and top sites are supported for data roaming.
    - **Firefox Browser Data**—Bookmarks, downloaded files, previously visited websites, website favicon images, Firefox permissions, search bar history, information that is entered into forms on websites, and file store preferences are supported for data roaming.
    - **Desktop Customization**—Favorite bar customization and App folders customization are supported for data roaming.
    - **Custom Wallpaper**——Custom wallpaper that you have configured is supported for data roaming.
    - **Browser Apps State**—If Firefox or Chrome web browser is open when you log out of the device, it reopens automatically when you log in to another device.
    - **Cloud Data**—The state of cloud files that are opened from the Dell File Explorer, cloud application that are opened from the launcher, and cloud files that are marked offline from the Dell File Explorer are supported for data roaming.
      > (i) **NOTE:** User data roaming is not supported for Box personal accounts.
    - **VDI session**—Citrix, VMware, Remote Desktop Protocol, Azure Virtual Desktop, and sessions are supported for data roaming. The VDI session allows you to open a file using the published and remote application, where the application is launched in a new session. All Citrix, VMware, and Remote Desktop Protocol client connections are created and launched when the session is active while logging off from the previous session.
13. Click **Save & Publish**.

Configure the user personalization roaming settings

Dell Hybrid Client supports user personalized roaming for certain configurations that are managed using the **Device Settings** window on the local device. A user can configure user-specific settings on one device, and the same settings are enabled on another device when the same user is logged in. By default, the user personalization roaming option is disabled.

Prerequisites

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

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.
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—Supported from Dell Hybrid Client v1.5 onwards.
     - Troubleshooting General—Print Screen.

Configure the 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Personalization**, and click **Desktop**.
6. Scroll down the page to view the **Power Control Settings** section.
7. Configure the following options based on your requirement:
   - **Power off**—Click the toggle key to enable or disable the shutdown option.
   - **Restart**—Click the toggle key to enable or disable the reboot option.
   - **Suspend**—Click the toggle key to enable or disable the suspend option.
   - **Logout**—Click the toggle key to enable or disable the logout option.
8. Click **Save & Publish**.

Switch users

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.

   (i) **NOTE:** The change log password option is available for both device and user policy groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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**.

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. This feature is supported from Dell Hybrid Client version 1.6 onwards.

Table 9. Supported applications

Application	Arguments supported	Example
Mozilla Firefox	Yes	Website URL
Google Chrome	Yes	Website URL
VLC Media Player	Yes	MP4 file path
LibreOffice	Yes	Document file path
VMware	Yes	URL with given username and password
Citrix	Yes	Not available. Reserved for parameters for future Citrix releases.

Table 9. Supported applications (continued)

Application	Arguments supported	Example
Azure Virtual Desktop	No	Not available
Azure Cloud Home	No	Not available
GCP Cloud Home	No	Not available

- 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 and Cloud home is enabled in single application mode, 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 s.
- 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. Multiple users can configure different applications in single application mode.
- User data roaming and autolaunch features are disabled in single application mode.

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.

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

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Application Security Settings**, and click **Application Access Control**.
6. Scroll down the page to view the **Single Application Mode Configurations** section.
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.

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.

Block keyboard shortcuts

Dell Hybrid Client allows you to disable certain keyboard shortcut combinations. You can block the keyboard shortcuts, 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 shortcuts 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.

   (i) **NOTE:** The block keyboard shortcuts option is available only for device policy groups.

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

Manage system updates

Dell Hybrid Client automatically updates certain applications and system packages when a new version is launched. This feature is available from Dell Hybrid Client version 1.5 onwards.

The following are the supported packages for autoupdate:

- Individual application packages released by Dell—Google Chrome and Mozilla Firefox.
- Dell Hybrid Client Bundle.
- Dell Hybrid Client Operating System Service pack

To use the autoupdate feature, you must upload the application package to the local repository on Wyse Management Suite.

Configure the autoupdate settings

Steps

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

   (i) **NOTE:** The autoupdate option is applicable only for Device Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **WMS Settings** and click **WMS Client Settings**.
6. In the **Auto Update Settings** section, click the **Auto Update** toggle switch to enable the option.
7. From the **Application** drop-down list, select an application.

   To enable autoupdate for applications other than Chrome and Firefox, you must select the **All** option.

8. From the **Frequency** drop-down list, select either **Weekly** or **Monthly**. This option determines how long the Dell Hybrid Client should wait before checking for updates.
9. Specify the active hours start time and end time for the device. The application automatically updates within the specified active hours provided the updates are available.

10. Specify a date for **Monthly** frequency, or select the number of days for **Weekly** frequency.
11. Click **Save & Publish**.

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.

SCEP is supported from Dell Hybrid Client version 1.6 onwards. 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 to be downloaded from the SCEP server.
   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.

   (i) **NOTE:** If you select the user mode authentication, 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.

   (i) **NOTE:** If you are adding SCEP from Wyse Management Suite, **Yes** is selected as the default value for the **SCEP from WMS** option.

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

Next steps

Log in to the Dell Hybrid Client-powered device. The SCEP certificate is enrolled immediately. If a certificate is not enrolled, the SCEP launcher is displayed on the login screen to fetch the certificate from the server.

Network authentication using IEEE 802.1x

IEEE 802.1x is the standard used for authenticating a device on the network. From Dell Hybrid Client version 1.6 onwards, 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.

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

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

ⓘ **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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 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, click the **Use SCEP certificate** toggle key and enter the SCEP certificate name. If the certificate is added from the **Privacy & Security** > **Certificate** section, specify that particular CA certificate name.
11. To use a CA certificate, click the **CA Certificate Required** toggle key and enter the 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 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-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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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:** Both domain user 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, click the **Use SCEP certificate** toggle key and enter the SCEP certificate name. If the certificate is added from the **Privacy & Security** > **Certificate** section, disable the **Use SCEP certificate** option and specify the certificate name.
11. To use a CA certificate, click the **CA Certificate Required** toggle key and enter the 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 and remains same for all devices in a domain that need to be 802.1x authenticated.
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.
- 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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**.

> (i) **NOTE:** Only domain user is supported for TLS user mode authentication. Local user is not supported.

9. Enter the SCEP certificate name.
10. To use a CA certificate, click the **CA Certificate Required** toggle key.
11. Enter the private key password. This option specifies the base64 encoded password that is required during the creation of a user or client certificate.
12. Click **Save & Publish**.

Next steps

Log in to the Dell Hybrid Client-powered device as a domain 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.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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**.

> (i) **NOTE:** Both domain user and local user 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 the private key password. This option specifies the base64 encoded password that is required during the creation of a user or client certificate.
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.

Configuring the local settings

You can configure the local settings on the device using the **Device Settings** menu. Depending on domain user or guest user, some dialog boxes and options are available for use.

ⓘ **NOTE:** Any settings that are configured locally on Dell Hybrid Client take precedence over the settings that were configured using Wyse Management Suite.

To access the **Device Settings** menu, click the **Show Applications** icon on the desktop screen, and then click **Device Settings**.
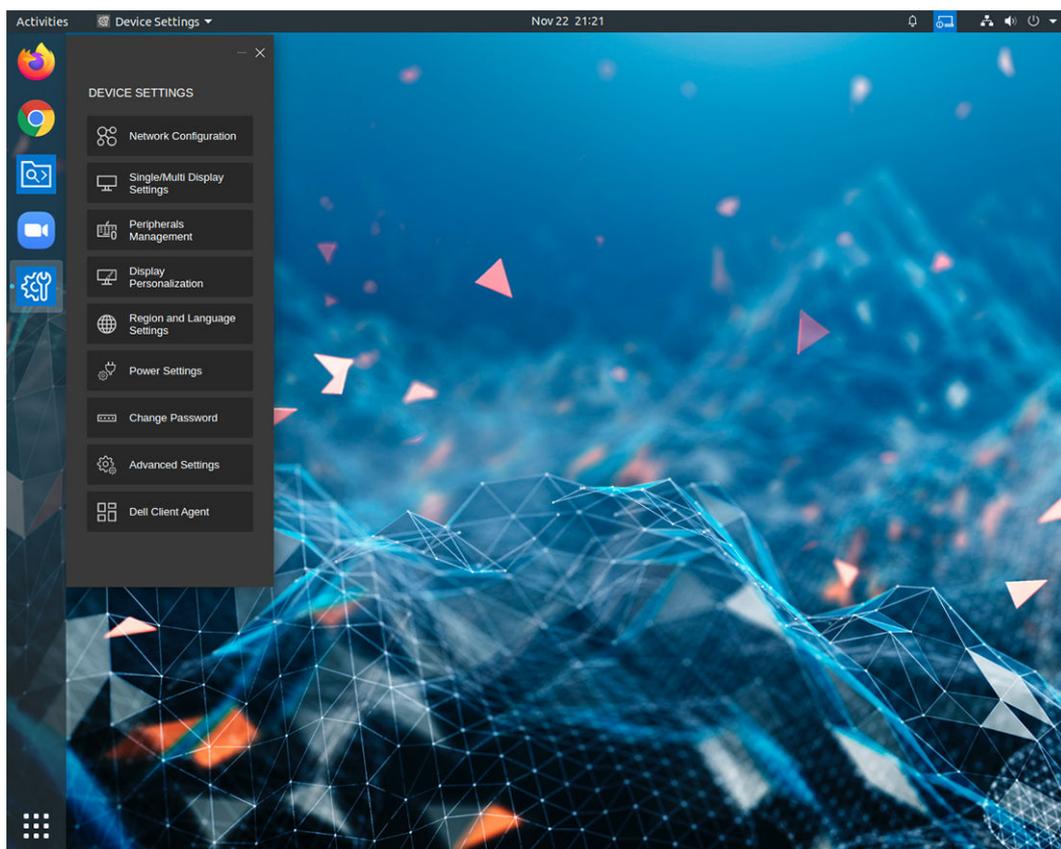
Figure 6. Device Settings menu in Dell Hybrid Client version 1.6

Configure the network settings locally

Use the **Device Settings** window on Dell Hybrid Client to configure the network settings. You can also configure the network 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 **Network Configuration**.

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

   ⓘ **NOTE:** The Ethernet and Wireless settings are moved to the **Advanced Settings** > **Network Configuration** in Dell Hybrid Client version 1.6.

   - **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.

6. Close the application.

Configuring the display settings on Dell Hybrid Client 1.6 and later versions

Use the **Device Settings** window on the Dell Hybrid Client to configure your single or multi-display settings. 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 **Single/Multi Display Settings**.
5. Configure the following display settings based on your requirement:
   a. From the **Primary Monitor Resolution** drop-down list, select a screen resolution for the primary display.
      ⓘ **NOTE:** The selected screen resolution works only if the display that is connected to the device supports the resolution.
   b. Click the **Primary Monitor Rotation** option, either **Landscape** or **Portrait**.
   c. Click the **Multi Monitor Configurations** toggle key to configure the multi-display settings.

      If enabled, configure the following options:

      i. Select one of the following **Display Mode** options:
         - **Span Mode**—Enables you to see all the displays that are spanning as one giant display.
         - **Mirror Mode**—Enables you to see the same screen on multiple displays.
         ⓘ **NOTE:** Mirror Mode is supported only when two displays are connected to the device. You must select span mode if you connecting more than two displays.

         ⓘ **NOTE:** When mirror mode is selected and you want to switch to span mode, you must click the span mode button. The previously applied span mode configuration are loaded. When you click Save & Apply, the previously saved span mode configuration is applied. If the previously configured span mode settings are not saved, the system enters the default span mode. You must use the Identify Monitors option and configure the span mode as per the requirements.
      ii. From the **Select Primary Monitor** drop-down list, select a display that acts as the primary display in a multi-display setup.
      iii. Click the **Identify Monitors** button to show the unique monitor ID on all the connected displays.

         In span mode, you must set the primary display and identify the corresponding displays using the **Identify Monitors** button that highlights the monitor ID.

iv. To configure a display, do the following:
   i. Click the **Add** icon.

      A display entry is created.

   ii. Click the display entry.
   iii. Select the display identifier.
   iv. Set the display resolution.
   v. Set the display rotation.
   vi. Set the span position.
   vii. Set the alignment for each display.
v. To configure multiple displays, repeat step iv.

   ⓘ **NOTE:** When you are adding a new display configuration, the display identifier must be unique across Wyse Management Suite configuration and Device Settings.

   ⓘ **NOTE:** When the span mode is selected, you need not have to configure the primary monitor settings. You do not have to add an entry for the primary monitor by clicking the **Add** icon.

6. Click **Save & Apply**.

   ⓘ **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.

Configuring the display settings on Dell Hybrid Client 1.5 and earlier versions

Use the **Device Settings** window on the Dell Hybrid Client to configure your single or multi-display settings. 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. Configure the following display settings based on your requirement:
   a. From the **Primary Monitor Resolution** drop-down list, select a screen resolution for the primary display.
      ⓘ **NOTE:** The selected screen resolution works only if the display that is connected to the device supports the resolution.
   b. Click the **Rotation** option, either **Landscape** or **Portrait**.
   c. Click the **Enable Multi Monitor** toggle key to configure the multi-display settings.

      If enabled, configure the following options:

      - Select one of the following **Display Mode** options:
        ○ **Span Mode**—Enables you to see all the displays that are spanning as one giant display.
        ○ **Mirror Mode**—Enables you to see the same screen on multiple displays.
      - From the **Monitor Count** drop-down list, select the number of displays that you have connected to the device.
      - From the **Secondary Monitor Resolution** drop-down list, select a screen resolution for the second display.
      - Select the position of the spanned second display from the following **Span Position** options:
        ○ **Left**
        ○ **Right**
        ○ **Bottom**
        ○ **Top**
      - From the **Multi Monitor Common Resolution** drop-down list, select a common screen resolution for multiple displays. This option is displayed when you select the monitor count as more than 3.

- From the **Multi Monitor Common Rotation** drop-down list, select a common rotation option for multiple displays. This option is displayed when you select the monitor count as more than 3.

6. Click **Save & Apply**.

   (i) **NOTE:** Use the **Reset to Default** button to reset your settings to default values. To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.

Configure the peripheral settings locally

Use the **Device Settings** window on the Dell Hybrid Client to configure your peripheral settings. You can also configure the peripherals 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 **Peripherals Management**.
5. Configure the following peripherals settings based on your requirement:
   - **Keyboard**—Use this option to configure the keyboard settings.

     Click the **Keyboard** tab, and configure the following options:

     a. Move the **Keyboard Repeat Rate** slider to set the keyboard repeat rate. The keyboard repeat rate specifies the speed at which the key repeats itself after you press and hold down a key on the keyboard.
     b. Move the **Keyboard Repeat Delay** slider to set the time for Repeat Delay. The keyboard repeat delay specifies the pause between pressing a key on the keyboard and when the key starts repeating itself.
     c. From the **Keyboard Layout** drop-down list, select a keyboard layout. The default value is English (United States).
        (i) **NOTE:** Users can select multiple keyboard layouts and switch between the keyboard layouts directly from the top bar. The Japanese keyboard layout for Hiragana and Kanji variation along with Katakana are supported from Dell Hybrid Client version 1.6 onwards.
     d. Click the **Turn Off Num Lock** toggle key to enable the **Num lock** key on your keyboard. Enabling the Num Lock allows you to use the keypad numeric pad.
     e. Click the **PrintScreen** 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.
        (i) **NOTE:** In Dell Hybrid Client version 1.6, the **PrintScreen** option is moved to the **General** tab of the **Troubleshooting** section under **Advanced Settings**.
     f. Click **Save & Apply**.
        (i) **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.

        (i) **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.
   - **Mouse**—Use this option to configure the mouse settings.

     Click the **Mouse** tab, and configure the following options:

     a. Move the **Speed** slider to set the mouse speed. This option enables you to increase or decrease the speed of the mouse cursor movement.
     b. Click the **Swap** toggle key to swap the left and right mouse buttons for left-handed operations.
     c. Click the **Reverse Scroll Wheel** toggle key to invert the direction of the mouse scroll wheel.
     d. Select the size of the local mouse pointer from the following **Pointer Size** options:
        ○ **Small**
        ○ **Medium**
        ○ **Big**
     e. Click **Save & Apply**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.

- **Audio**—Use this option to configure the audio settings.

    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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.

- **Printer**—Use this option to configure the printer settings. 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.

    You can use the **Printer** settings window of the Ubuntu interface to configure the printer options. For more information about how to configure the printer settings, see the *Ubuntu documentation* at help.ubuntu.com.

6. Close the application.

Configure the display personalization settings locally

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.

     (i) **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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.

5. Close the application.

Configure the region and language settings locally

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. This option is available from Dell Hybrid Client version 1.6 onwards.
     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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. 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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. 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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.
5. Close the application.

Configure the power settings locally

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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. 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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. 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**.

     (i) **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.

     (i) **NOTE:** To discard your changes on the current window, click the back arrow. To discard your unsaved changes across the application, click the **Discard Changes** button.

5. Close the application.

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

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 **Password**.
   The **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**.

   (i) **NOTE:** To discard your changes on the current window, click the back arrow. 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. By default, the network drives feature is disabled in Device Settings.

Prerequisites

Enable the Network Drive option from **Advanced** > **Network Drives** on Wyse Management Suite. This option is available for both device-level and user-level group 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 **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.

      (i) **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 and the configurations are preserved across devices.

Configure the advanced settings locally

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 GRUB 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, 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 GRUB 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.

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.

      (i) **NOTE:** The certificate name must be unique across Wyse Management Suite configuration and Device Settings.

   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 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 do either of the following:
   - If you are running Dell Hybrid Client 1.5 and earlier versions, the **Dell Client Agent** window is displayed.
   - If you are running Dell Hybrid Client 1.6, the **Authentication Required** window is displayed. Enter the default 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 DCA password is based on the device compliant status.

     - If the device is compliant, the DCA password is same as the GRUB password that is set from Wyse Management Suite.
     - If the device is non-compliant, the DCA 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.

     ⓘ **NOTE:** If the device is unregistered from Wyse Management Suite, the DCA password is same as the device serial number.

     Upon successful authentication, the **Dell Client Agent** window is displayed.
5. 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.

      ⓘ **NOTE:** End-users cannot unregister the device from Wyse Management Suite using the **Dell Client Agent** window. Administrator can only unregister the device by using the Wyse Management Suite console.

6. Click **Support**, and enable the **Support Mode** option for troubleshooting purposes. From Dell Hybrid Client version 1.5 onwards, this option can be enabled only by an administrator from Wyse Management Suite.
7. Click **About** to view the version of the Dell Client Agent.
8. 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.

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 ICA
- VMware Blast, PCoIP, and RDP
- Dell RDP
- Azure Virtual Desktop, formerly known as Windows Virtual Desktop—Supported from Dell Hybrid Client 1.6 onwards.

(i) **NOTE:** Citrix Workspace App and VMware Horizon Client are released as optional add-ons for Wyse 5070 devices with 16 GB storage capacity. By default, these add-ons are not installed on these devices. Citrix RealTime Media Engine (RTME) is not part of Dell Hybrid Client build. You can download the Citrix RTME package from the Citrix website and install the component.

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. From Dell Hybrid Client version 1.5 release onwards, Citrix SSO is supported using a smart card.

  (i) **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:

  - **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:

  - **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).
- **Azure Virtual Desktop SSO**-Single Sign-On (SSO) is supported on Azure Virtual Desktop (AVD) connections. If SSO is enabled, the device automatically adds the user account and lists the corresponding published desktops and applications. However, SSO is not supported for launching the application.

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.

> (i) **NOTE:** Dell RDP does not support Multifactor authentication.

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 10. 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

Table 10. Supported Citrix features (continued)

Feature	Description
	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.
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.

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

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

Configure the Citrix broker connection

About this task

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

(i) **NOTE:** You can also use the default VDI native client on Dell Hybrid Client to configure the VDI session.

Steps

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

   (i) **NOTE:** In Wyse Management Suite version 3.2, the VDI 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 **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.
8. Click **Save & Publish**.

Configure the global Citrix settings

About this task

This section describes the procedure to configure the global connection settings for Citrix 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.

   (i) **NOTE:** In Wyse Management Suite version 3.2, the VDI 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 **Session Settings**, and click **Citrix Session Settings**.
6. Configure the following Citrix global settings as per your requirement:
   - **Smartcard Settings**
   - **Local resources and USB redirection**
   - **Client Drive Mapping**
   - **Hotkey Settings**
   - **Hotkey Mapping**
   - **Advanced Session Settings** such as **Save MultiMonitor Preference**, **H.264**, **Multimedia Redirection**, **WebPage Redirection**, **MultiStream**, and **Middle Button Paste**.
7. Click **Save & Publish**.

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.

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 11. 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.

Table 11. Supported VMware features (continued)

Feature	Description
Minimized Mode	Enables you to launch a desktop or an application in minimized mode.
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.

Configure the VMware Broker connection

About this task

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

(i) **NOTE:** You can also use the default VDI native client on Dell Hybrid Client to configure the VDI session.

Steps

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

   (i) **NOTE:** In Wyse Management Suite version 3.2, the VDI 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 **Broker Settings**, and click **VMware Broker Settings**.
6. In the **VMware Connection** section, click **Add Row**.
7. Configure the VMware session options as per your requirement.
8. Click **Save & Publish**.

Configure the global VMware settings

About this task

This section describes the procedure to configure the global connection settings for VMware 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.

   (i) **NOTE:** In Wyse Management Suite version 3.2, the VDI 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 **Session Settings**, and click **VMware Session Settings**.
6. Configure the **USB Redirection** settings.

By default, the USB redirection is enabled for all devices. You can specify the list of USB devices to be allowed based on the Vendor ID, Product ID, Device Class, and Subclass ID.

7. Click **Save & Publish**.

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.

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.

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 12. 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.

Table 12. Supported Dell RDP features (continued)

Feature	Description
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.

Configure the RDP broker connection

About this task

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

(i) **NOTE:** You can also use the default VDI native client on Dell Hybrid Client to configure the VDI session.

Steps

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

   (i) **NOTE:** In Wyse Management Suite version 3.2, the VDI 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 **Broker Settings**, and click **Microsoft Remote Desktop Settings**.
6. In the **RDP Connection** section, click **Add Row**.
7. Configure the RDP session options as per your requirement.
8. Click **Save & Publish**.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 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.

Dell Hybrid Client supports the following features:

Table 13. 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.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.

   (i) **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 AVD connections locally

You can use the AVD 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.

(i) **NOTE:** By default, the AVD client is disabled. When you launch the AVD 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 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.

4. To add a cloud account, click the **+** icon next to the **AVD CONNECTIONS** section.

   (i) **NOTE:** You can use the delete icon to remove an existing cloud account.

   (i) **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.

   (i) **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.

   (i) **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 AVD client prompts for the password.

   (i) **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.
- Ensure that you have installed valid certificates that are required to connect to the Azure virtual desktop. See, Install a certificate.

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 other VDI connections are not supported. All connections are accessible only from the AVD client.
- File type association for AVD is not supported. User cannot access files from Dell File Explorer using the applications that are listed in the AVD client.
- Smart card and biometric-based user logins are not supported.
- USB redirection is not supported.

Configuring Imprivata PIE

Imprivata enables secure authentication to virtual desktops and applications. Dell Hybrid Client supports Imprivata with Citrix and VMware. This feature is supported from Dell Hybrid Client version 1.6 onwards. 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 autologon**—Administrator must enable the autologon option from the Imprivata Session Settings page on Wyse Management Suite. After you restart the system, the Imprivata client is launched automatically in full screen mode replacing the Ubuntu login screen.

Dell Hybrid Client supports the following types of user authentication:

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

Configure the Imprivata connection settings

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.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Session Settings**, and click **Imprivata Session Settings**.
6. Click the **Imprivata** toggle key to ON state.
7. Configure the Imprivata session options as per your requirement.

   (i) **NOTE:** If the certificate check option is enabled for the Imprivata connection, you must upload the Imprivata appliance root certificate using the Certificate option under **Privacy & Security** on Wyse Management Suite. This certificate is required when you are installing the Imprivata agent for the first time on your device.

8. Click **Save & Publish**.

Connect to an Imprivata OneSign session

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 Dell Hybrid Client using AD or OAuth 2.0.
2. Click the **Show Applications** icon on the desktop screen.
   The Imprivata connection icon is displayed.
3. Double-click the Imprivata connection icon.
   The Imprivata login screen is displayed. You can authenticate using a password or Smart Card based on the configuration set in Imprivata appliance. On successful authentication, the VDI connection is established.

   For information about smart card authentication, see logging in to a VDI session using a smart card.

Logging in to a VDI session using a smart card

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

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

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 the certificate to have a SAN value for the import to succeed. From Dell Hybrid Client version 1.6 onwards, 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.

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

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.

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:

- Skype for Business
- Cisco Jabber
- Cisco WebEx Teams
- Cisco WebEx Meetings
- Microsoft Teams
- Zoom

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

Zoom application 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.

> (i) **NOTE:** Zoom plugins for VDI are preinstalled on devices with 32 GB or higher storage capacity. **Zoom plugin for VMware** and **Zoom plugin for Citrix** are delivered as optional add-ons for Wyse 5070 devices with 16 GB storage capacity.

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** 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 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** 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 **Multimedia Extension Fix Add-on for VDI** 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.

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.

> (i) **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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.

   (i) **NOTE:** In Wyse Management Suite version 3.2, 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 **Citrix File Type Association**.
6. In the **Citrix File Type Association Configuration** section, click **Add row**.

   (i) **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.

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 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.

   (i) **NOTE:** In Wyse Management Suite version 3.2, 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.

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 VDI Broker agent 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.

   ⓘ **NOTE:** In Wyse Management Suite version 3.2, 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.

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.

8

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. Personal cloud accounts are supported from the Dell Hybrid Client 1.5 release onwards.
- **Google Drive**—Supports both enterprise and personal OneDrive accounts*. Personal cloud accounts are supported from the Dell Hybrid Client 1.5 release onwards
- **Box Drive**—Supports only personal Box accounts. This feature is supported from Dell Hybrid Client 1.6 onwards.

ⓘ **NOTE:** From Dell Hybrid Client version 1.1 onwards, 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. From Dell Hybrid Client version 1.5 onwards, you can access your OneDrive account from File Explorer.

ⓘ **NOTE:** From Dell Hybrid Client version 1.6 onwards, 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. This feature is supported from Dell Hybrid Client version 1.5 onwards.

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. This feature is supported from Dell Hybrid Client version 1.5 onwards.

Azure AD supports smart card login with on-premises Active Directory Federated 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.

Connect to Azure

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 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.
    The **AD FS URL** option is available from Dell Hybrid Client version 1.5 onwards.
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.

ⓘ **NOTE:** You can manually upload cloud files of any size. However, the automatic synchronization of VDI files that you edited offline is limited to 4 MB for Azure.

ⓘ **NOTE:**

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 **CLOUD FILES** section, click the **Add (+)** button to add your personal account.
18. Enter the credentials to sign in to your personal account.

Connect to Google Workspace

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 one of the following options:
   - **Cloud**
   - **Cloud+Local**
   - **Cloud+VDI+Local**
7. From the **Cloud Provider** drop-down list, select **GCP**.

   (i) **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 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.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 **CLOUD FILES** section, click the **Add (+)** button to add your personal account.
18. Enter the credentials to sign in to your personal account.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 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.

Create shortcuts for cloud files

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 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**.

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.

  (i) **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**

From Dell Hybrid Client version 1.5 onwards, the **Open with** function is supported. This feature enables end-users to choose an application to open a file in Dell File Explorer. See, Using Dell File Explorer.

(i) **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 Mode

Use the Cloud Mode to enable all your files to open only on the cloud. If cloud is configured, the data roaming feature is enabled automatically.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 **Cloud**.
7. 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.

8. Click **Save and Publish**.
9. Log in to Dell Hybrid Client.
10. Double-click a file.

    The file opens on the cloud only. If there is no network (offline), you cannot open the file and an error message is displayed.

    For more information about how to configure the cloud environment, see Configuring the cloud environment.

Example

- **Open a Microsoft PowerPoint file using Azure cloud**
    1. Configure the **Cloud** mode for File Affiliation using Wyse Management Suite.
    2. Log in to the device as an Active Directory (AD) user.

       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, you cannot open the file.

- **Open a Microsoft PowerPoint file using Google cloud**
    1. Configure the **Cloud** mode for File Affiliation using Wyse Management Suite.
    2. Log in to the device as an Active Directory (AD) user.
    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, you cannot open the file.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 **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. Local mapping enables you to access the local drive. If the local mapping is valid, files open on the local system.

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 on the local system.

- **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 on the local system.

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** > **Hybrid Client**.
    The **Configuration Control | Hybrid Client** 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**.

    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 network 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** > **Hybrid Client**.
    The **Configuration Control | Hybrid Client** 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 on the local system.

    If the priority is set to **Local**, files check the local mapping first. If the local mapping is valid, files open on the local system.

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 cloud or the local system based on the priority defined. If there is no network (offline) or mapping is not available in the network database, the file opens on the local system. 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 on the local system.

Configure the Cloud + VDI + Local Mode

Use the Cloud + VDI + Local Mode to enable all your files to open on the cloud, VDI, or 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 **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 on the local system. 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 on the local system. 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 on the local system.

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**
4. Enter the URL of the web page in the address bar, and start browsing the web.

   (i) **NOTE:** From Dell Hybrid Client version 1.5 onwards, the developer mode is disabled both for Chrome and Firefox by default. It can be enabled only when you set the security profile to **Low**. For information about how to configure the security profiles, see Security profiles.

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 user group.

   (i) **NOTE:** The Multicontainer option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click **Firefox settings**.
6. Click the **Enable MultiContainers** toggle key to enable or disable the multicontainer feature.
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 user group.

   ⓘ **NOTE:** The site isolation option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Browser Settings**, and click **Google Chrome settings**.
6. Click the **Enable site isolation** toggle key to enable or disable the site isolation feature.
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 user group.

   ⓘ **NOTE:** The plugins for Chrome option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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

From Dell Hybrid Client version 1.6 onwards, 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 user group.

   ⓘ **NOTE:** The Multicontainer option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 that are configured in Wyse Management Suite. 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.
7. Click **Save and Publish**.

Allow or block 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 user group.

   (i) **NOTE:** The allow or block access to website option is applicable only for User Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.

   (i) **NOTE:** Ensure that the **Reset website access control settings** option is disabled to access the Blacklist and Whitelist options.

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

(i) **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.

   (i) **NOTE:** The browser shortcuts option is applicable only for user policy groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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 displayed.
   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. This feature is available from Dell Hybrid Client version 1.6 onwards. 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.

   (i) **NOTE:** If the same domain user logs in to another device, the pinned URL shortcut is still displayed on the desktop.

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.
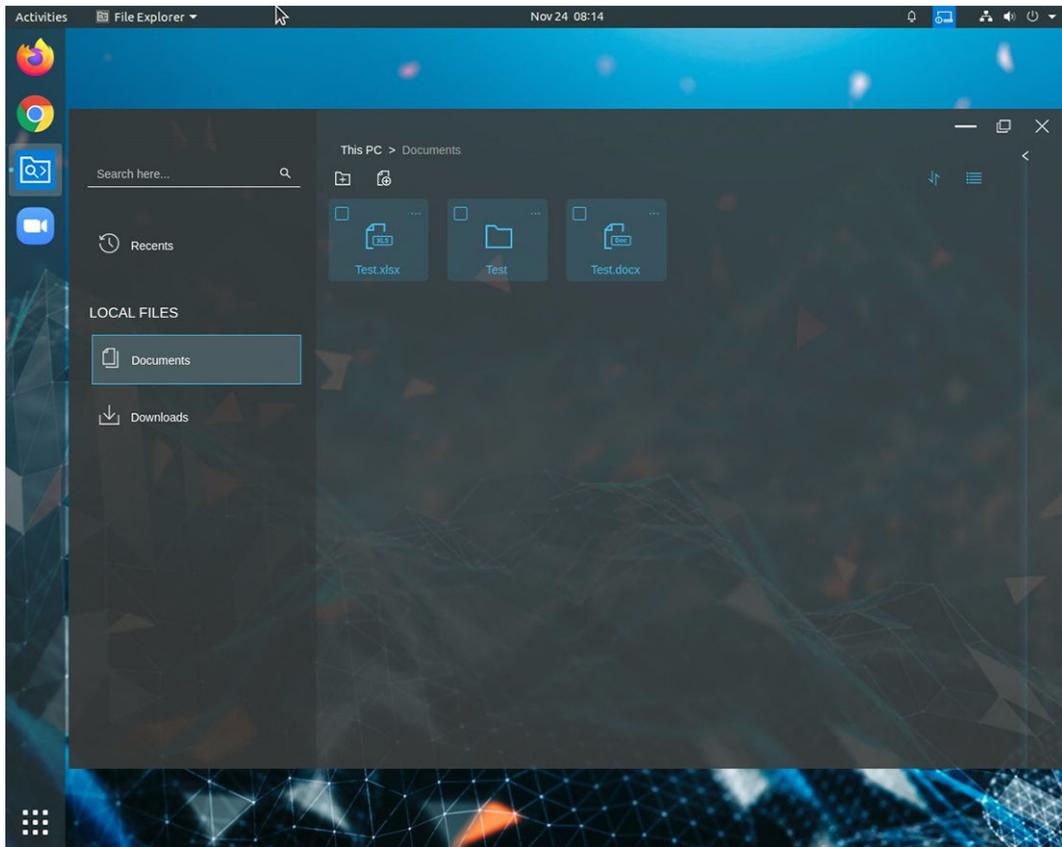
Figure 7. File Explorer in Dell Hybrid Client version 1.6

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.

*Supported from Dell Hybrid Client version 1.5 onwards.

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

Table 14. 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. ● **CLOUD FILES**—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 from Dell Hybrid Client 1.6 onwards. ⓘ **NOTE:** As a guest user, you can access the corporate cloud accounts from Dell Hybrid Client 1.6 onwards. ● **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. This feature is supported from the Dell Hybrid Client version 1.5 release onwards. ● **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 using the Drag-and-Drop method. This is supported from Dell Hybrid Client version 1.6 onwards.

Table 15. File Explorer—additional features

Feature	Summary
File synchronization	**Devices powered by Dell Hybrid Client 1.5 and later versions**—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. **Devices powered by Dell Hybrid Client version 1.1**—File Synchronization happens only when the user logs in the next time on the same device, provided the local file or local drive file is opened in a cloud application. For example, opening the cloud drive files in VDI or local applications and any modifications are only synchronized during next user login.
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 from the Dell Hybrid Client version 1.5 onwards.
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 from the Dell Hybrid Client version 1.5 onwards.
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. This feature is supported from the Dell Hybrid Client version 1.5 release onwards.
Uncompress files	Uncompress function enables you to extract a zip file that is stored locally. From Dell Hybrid Client version 1.6 onwards, 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. This feature is supported from the Dell Hybrid Client version 1.5 release onwards. From Dell Hybrid Client 1.6 onwards, 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. **Devices powered by Dell Hybrid Client 1.5 and later versions**—Offline files are automatically synchronized when the network is available. This feature is supported in the Dell Hybrid Client version 1.5 release onwards. **Devices powered by Dell Hybrid Client version 1.1**—Offline files are automatically synchronized during subsequent cloud logins based on the file modification time. However, the file is automatically deleted after seven days from the time file was marked as offline and not synchronized to cloud. To avoid auto deletion of the file, you should synchronize the file before seven days. 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. (i) **NOTE:** You can manually upload cloud files of any size. However, the automatic synchronization of VDI files that you edited offline is limited to 4 MB for Azure.

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 16. 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 the settings that are configured 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 the settings that are configured 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 the settings that are configured 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 FILES**.
   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. This feature is available from Dell Hybrid Client version 1.5 onwards. 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** utility 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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**.

   (i) **NOTE:** FTP 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, click the **Anonymous mode** toggle key.
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:

- **VLC Media Player**—Enables you to play most of the multimedia files.
- **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.

(i) **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 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.

Configure the application security

The **Application Security** feature restricts your local applications on Dell Hybrid Client using opening files from external USB drives.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Application Security**, and select an application.
6. Click the **Mount** toggle key to enable the option. Enabling the **Mount** option allows the application to access the external USB drive. You can play any multimedia files or open any files from the external USB drive. By default, the **Mount** option is disabled.
7. Click the **Network** toggle key to enable the **Network** option. Enabling the **Network** option allows the VLC media player to access the Internet. You can play any multimedia files from the web.

8. Click **Save & Publish**.
9. Log in to Dell Hybrid Client and launch the application.

Pin an application to desktop

Dell Hybrid Client allows you to pin an application to the desktop for quick access. This feature is available from Dell Hybrid Client version 1.6 onwards.

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.

   (i) **NOTE:** If the same domain user logs in to another device, the pinned shortcuts are still displayed on the desktop.

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. Zoom application is preinstalled on devices with 32 GB or higher storage capacity. If you are using Wyse 5070 Thin Client with 16 GB storage capacity, you must download and install the optional Zoom Client package.

Prerequisites

As an administrator, you must install the optional Zoom Client add-on on Wyse 5070 Thin Clients with 16 GB storage capacity. To install the Zoom Client add-on, 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 Zoom Client 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.

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.

(i) **NOTE:** Performances issues are observed when you use the Zoom application on Dell Hybrid Client-powered Wyse 5070 devices with 16 GB storage capacity.

Installing third-party applications

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

(i) **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.

From Dell Hybrid Client version 1.6 onwards, 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. If you want to install multiple add-ons, ensure that you deploy the add-on one at time. Deployment of application policies to the device can be scheduled immediately or later, based on your time zone.

(i) **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.

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

Ensure that you get your application signed by Dell by contacting your **Dell Sales Representative** and submitting the application file that needs to be signed. Once the signing process is complete, the Dell Sales Representative will deliver the signed 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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:
   - **Devices powered by Dell Hybrid Client 1.5 and later versions**:
     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**.
   - **Devices powered by Dell Hybrid Client version 1.1**:
     a. Expand **Application Security**, and click **Application Deployment**.
     b. Click the **Secure Deployment Mode** toggle key to ON state to allow only Dell-signed applications to be installed on Dell Hybrid Client. By default, the option is enabled.
     c. 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. For detailed steps on how to use the Reporter OpenSSL utility to create custom-signed certificates, see the *How to create a self-signed SSL Certificate using OpenSSL for Reporter 9.x* article at knowledge.broadcom.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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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:
   - **Devices powered by Dell Hybrid Client 1.5 and later versions**:
     a. Expand **Privacy & Security** and click **Security Profile**.
     b. From the **Security Profile** drop-down list, select **Medium**.
     c. Browse and upload one or more signed certificates. Supported file types are `.crt` and `.cer`.
     d. Click **Save and Publish**.
   - **Devices powered by Dell Hybrid Client version 1.1**:
     a. Expand **Application Security**, and click **Application Deployment**.
     b. Click the **Secure Deployment Mode** toggle key to ON state. By default, the option is enabled.
     c. Click the **Allow custom signed application** toggle key to ON state to allow custom-signed applications to be installed on Dell Hybrid Client. By default, the option is disabled.
     d. Browse and upload one or more signed certificates. Supported file types are `.crt` and `.cer`.
     e. 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 *Dell 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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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:
   - **Devices powered by Dell Hybrid Client 1.5 and later versions**:
     a. Expand **Privacy & Security** and click **Security Profile**.
     b. From the **Security Profile** drop-down list, select **Low**.
     c. Click **Save and Publish**.
   - **Devices powered by Dell Hybrid Client version 1.1**:
     a. Expand **Application Security**, and click **Application Deployment**.

b. Click the **Secure Deployment Mode** toggle key to OFF state to allow unsigned applications to be installed on Dell Hybrid Client. By default, the option is disabled.

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

c. Click **Save and Publish**.

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 example, you can copy an MP4 file to the Dell Hybrid Client-powered device using the advanced application policy on Wyse Management Suite. You must use the `.sh` file as a prescript file—`cp /etc/WMSApps/taskbar.mp4 /home/test1@DHC.COM/Documents`.

a. Copy the MP4 file and the prescript file to `C:\WMS\LocalRepo\repository\hybridClientApps` path.
b. On Wyse Management Suite, go to **Apps & Data**, and click **Hybrid Client** in the **App Polices** section.
c. Click **Advanced Policy**.
d. Enter the policy name.
e. From the **Group** drop-down list, select your preferred group.
f. From the **Task** drop-down list, select **Install Application**.
g. From the **OS Type** drop-down list, select **Hybrid Client**.
h. Click **Add app** and do the following:
   i. From the **Apps** drop-down list, select the MP4 file.
   ii. From the **Pre-Install** drop-down list, select the `.sh` file.
   iii. Specify the install timeout period.
i. Save and deploy the policy to the device.
j. After successful deployment, open File Explorer on Dell Hybrid Client and verify if the MP4 file is available in the Documents folder.

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.

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 *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.
   (i) **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.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.
   (i) **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 *Dell Wyse Management Suite Administrator's Guide* at www.dell.com/support.

   (i) **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.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Groups & Configs** page, and select your preferred group.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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. Click 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.
10. Enter a password for the VNC connection.
11. Click **Save and Publish**.

    (i) **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.

Configure the admin password

From Dell Hybrid Client version 1.6 onwards, the bremen user is renamed to admin user. As an administrator, you can use the admin account to manage sudo or elevated privileges. From Dell Hybrid Client version 1.5 onwards, the admin password is same as the randomized Grub password. You can use the Grub password itself to access the admin account.

About this task

This section describes how to configure the GRUB 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.
3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** page is displayed.
4. Click the **Advanced** tab.
5. Expand **Privacy & Security**, and click **GRUB Password**.
6. In the **GRUB 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.
7. Click **Save & Publish**.

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** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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. This feature is available from Dell Hybrid Client version 1.5 onwards. 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. This feature is available from Dell Hybrid Client version 1.5 onwards. The Open Box feature is available from Dell Hybrid Client version 1.6 onwards.

Steps

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

(i) **NOTE:** The security profile option is applicable only for Device Policy Groups.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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.
     (i) **NOTE:** The firewall and Kernel hardening features are disabled.

   - **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
       (i) **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
       (i) **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.
     (i) **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.

     (i) **NOTE:** The firewall and Kernel hardening features are disabled. Both default and custom firejail profiles are disabled.

     (i) **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 1.x Security Configuration Guide* at www.dell.com/support.
   (i) **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": "63xxxxxxxxxxxxxxxxxxxxx",
   "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"
                   }
               }
          ]
      }
   }
}
```

(i) **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": "63xxxxxxxxxxxxxxxxxxxxx",
   "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"
                    }
                }
            }
        ]
    }
}
}
```

12

Dell Hybrid Client recovery imaging

Use Wyse Management Suite to reinstall the Dell Hybrid Client software. During the process, the device uses the hard drive partition for recovery imaging.

Steps

1. Log in to Wyse Management Suite.
2. Go to the **Devices** page.
3. Apply the filters to find your preferred device.
4. Select the check box of the device. You can select one or more devices.
5. From the **More Actions** drop-down list, click **Reimage**.
6. Click **Send Command**.
   The recovery imaging process takes approximately 10 minutes to complete.

Dell Hybrid Client troubleshooting

This section provides information about how to identify and resolve issues you may observe when using Dell Hybrid Client.

Using log files for troubleshooting

You can use log files to identify issues and troubleshoot your devices powered by Dell Hybrid Client.

Enable dev mode in Dell Hybrid Client

Dev Mode enables you to access the terminal application and export system logs.

Steps

1. Turn on the device powered by Dell Hybrid Client.
2. When the Dell logo appears, press the Esc key.
   The Grub Boot menu is displayed.
3. Press the E key to edit the grub option.
4. Enter the grub credentials.
   The default username is **admin**. The GRUB password is set by the administrator. You can view the GRUB password on the Wyse Management Suite console. See, View the GRUB password.
5. Edit the kernel parameter entry as follows:
   a. Add the string **dhc-dev-mode** to the kernel parameter.

   For example,

   ```
   BOOT_IMAGE=/boot/vmlinuz-5.0.0-1040-oem-osp1
   root=UUID=98682104-07b9-4d5e-845a-2d9324c36f60 ro mem_sleep_default =deep quiet
   splash dhc-dev-mode vt.handoff=1
   ```

   b. Press the Ctrl + X key combination to save your changes.
   The device automatically reboots.
6. Log in to Dell Hybrid Client.
   A terminal application is available in the desktop applications menu, and the export system logs option is available in Device Settings.
   - **Dell Hybrid Client 1.5**—Use the Bremen account to manage sudo or elevated privileges. Username is **bremen** and password is either the GRUB password or the password specified by the administrator during the initial setup.
   - **Dell Hybrid Client 1.6 and later**—Bremen root user is renamed to admin. Use the admin account to manage sudo or elevated privileges. Username is **admin** and password is either the GRUB password or the password specified by the administrator during the initial setup.

   ⓘ **NOTE:** The Dev Mode setting is disabled every time when you restart the device.

Next steps

Use the Export System Logs option to extract the Dell Hybrid Client system log files. For more information about how to export system logs, see Extract log files using Device Settings.

Request log files using Wyse Management Suite

The device must 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.

Extract log files using Device Settings

This section is not applicable to Dell Hybrid Client 1.6 and later versions.

Prerequisites

Ensure that you have enabled the dev mode in Dell Hybrid Client.

Steps

1. Log in to Dell Hybrid Client.
2. Connect a USB drive to the device.
3. On Dell Hybrid Client, go to **Device Settings**, and click **Export System Logs**.
   The **Export System Logs** window is displayed.
4. Select the USB device from the list, and click **Export**.
   All the system log files are exported to the USB drive.

Extract 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 the text editor.
  2. Add the following lines in a text 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.

Change 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.

   (i) **NOTE:** The change log password option is available only for the device policy group.

3. Click **Edit Policies** > **Hybrid Client**.
   The **Configuration Control | Hybrid Client** 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**.

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.

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. It is a desktop solution by Dell that follows the Software-as-a-Service (SaaS) model of software delivery. 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.

- **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 across devices. 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 Wyse 5070 device?**

  Dell Hybrid Client can be recovered from the recovering partition on the Wyse 5070 device.

- **How to recover the Dell Hybrid Client if the device does not boot?**

  You must reimage the device from the recovery partition.

- **Can troubleshooting logs for Dell Hybrid Client be extracted?**

  You can use Wyse Management Suite to extract the log files, or enable dev mode on Dell Hybrid Client to extract logs to a USB drive using the local device settings.

- **Are the Dell Hybrid Client logs for network trace, USB, and troubleshooting available in Wyse Management Suite?**

  You can only extract system logs, and Dell Hybrid Client specific modules logs using Wyse Management Suite. Network trace logs are not supported.

- **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 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.

- **If you use an Ubuntu recovery image, how do you reload Dell Hybrid Client?**

  If Dell Hybrid Client is loaded into the recovery partition of the Ubuntu recovery image, you can install Dell Hybrid Client from the recovery partition to the main operating system partition using Wyse Management Suite.

- **What is the size of the whole Dell Hybrid Client image?**

  For information about the image size, refer the latest *Dell Hybrid Client 1.x Release Notes* at www.dell.com/support.

- **Can I install Dell Hybrid Client on Wyse 5070 devices with 16 GB storage?**

  Dell Hybrid Client version 1.5 and later versions are not supported on Wyse 5070 devices with 16 GB storage. However, Dell Hybrid Client version 1.1 is compatible with Wyse 5070 devices with 16 GB storage.

- **What happens when the disk space is nearing its maximum capacity?**

  A warning message is displayed to the user.

- **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.