

# Dell Hybrid Client

## Version 1.x Security Configuration Guide



## Notes, cautions, and warnings

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

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

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

<b>Chapter 1: Preface</b> .....	<b>4</b>
Legal disclaimer.....	4
Scope of document.....	4
Document references.....	4
Resources and support.....	4
Security resources.....	5
Getting help.....	5
Reporting security vulnerabilities.....	5
<b>Chapter 2: Security quick reference</b> .....	<b>6</b>
Supported platforms.....	6
Security profiles.....	7
USB device security.....	8
GRUB password security.....	8
BIOS password security.....	8
Application deployment security.....	8
<b>Chapter 3: Product and subsystem security</b> .....	<b>9</b>
Product overview.....	9
Authentication.....	10
Login security settings.....	11
User and credential management.....	11
Authentication to external systems.....	12
Authorization.....	12
Network security.....	13
Data security.....	13
Cryptography.....	14
Auditing and logging.....	14
Request log files using Wyse Management Suite.....	14
Extract log files using Device Settings.....	14
Extract VDI log files.....	14
Code or product integrity.....	15
<b>Chapter 4: Contacting Dell</b> .....	<b>16</b>

# Preface

## Topics:

- [Legal disclaimer](#)
- [Scope of document](#)
- [Document references](#)
- [Security resources](#)
- [Getting help](#)
- [Reporting security vulnerabilities](#)

## Legal disclaimer

**THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall Dell Technologies, its affiliates or suppliers, be liable for any damages whatsoever arising from or related to the information contained herein or actions that you decide to take based thereon, including any direct, indirect, incidental, consequential, loss of business profits or special damages, even if Dell Technologies, its affiliates or suppliers have been advised of the possibility of such damages.**

The Security Configuration Guide intends to be a reference. The guidance is provided based on a diverse set of installed systems and may not represent the actual risk/guidance to your local installation and individual environment. It is recommended that all users determine the applicability of this information to their individual environments and take appropriate actions. All aspects of this Security Configuration Guide are subject to change without notice and on a case-by-case basis. Your use of the information contained in this document or materials linked herein is at your own risk. Dell reserves the right to change or update this document in its sole discretion and without notice at any time.

## Scope of document

This guide contains information about the security features of Dell Hybrid Client. The document provides guidelines that help you maximize the security of your devices in your environment. You will understand the expectations that Dell has of the environment in which the Dell Hybrid Client is deployed.

## Document references

The following documents provide a comprehensive reference to the Dell Hybrid Client software:

- [Dell Hybrid Client Version 1.x Administrator's Guide](#)
- [Dell Hybrid Client Version 1.x Conversion and Upgrade Guide](#)
- [Dell Hybrid Client Version 1.x Release Notes](#)
- [Dell Hybrid Client Version 1.x Restore Guide](#)

You can access the manuals available at [www.dell.com/support/manuals](http://www.dell.com/support/manuals).

## Resources and support

### Accessing documents using the product search

1. Go to [www.dell.com/support](http://www.dell.com/support).

2. In the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box, type the product name. For example, **OptiPlex 7070 Ultra** or **Dell Hybrid Client**. A list of matching products is displayed.
3. Select your product.
4. Click **Documentation**.

## Accessing documents using product selector

You can also access documents by selecting your product.

1. Go to [www.dell.com/support](http://www.dell.com/support).
2. Click **Browse all products**.
3. Click your product category and then click the sub-categories if available.
4. Click the product name.
5. Click the **Documentation** tab.

## Security resources

Dell Technologies provides customers with timely information, guidance, and mitigation options to minimize risks associated with security vulnerabilities. Dell Technologies recommends that you run the most recent version of the software available and apply any remediation, workarounds, or mitigation at the earliest opportunity. For information about security advisories and notices for all Dell Technologies product, go to [www.dell.com/support/security](http://www.dell.com/support/security).

## Getting help

The [Dell support page](#) provides access to licensing information, product documentation, advisories, software downloads, how-to videos, and troubleshooting information. Dell Product Support is available to field your calls for issues regarding your deployment of the Dell Hybrid Client software. Dell Technologies recommends that you sign in to your Dell account to receive driver notifications.

## Reporting security vulnerabilities

Dell takes reports of potential security vulnerabilities in our products very seriously. If you discover a security vulnerability, you are encouraged to report it to Dell immediately.

For information on how to report a security issue to Dell, see the Dell Vulnerability Response Policy on the Dell support site. To access the Dell Vulnerability Response Policy, do the following:

1. Go to [www.dell.com/support](http://www.dell.com/support).
2. In the search bar, enter **Dell Vulnerability Response Policy**, and press Enter.
3. From the search results, click the **Dell Vulnerability Response Policy** link. The **Dell Vulnerability Response Policy page** is displayed.

# Security quick reference

## Topics:

- [Supported platforms](#)
- [Security profiles](#)
- [USB device security](#)
- [GRUB password security](#)
- [BIOS password security](#)
- [Application deployment security](#)

## Supported platforms

Dell Hybrid Client version 1.6 is supported on the following platforms:

- **Wyse 5070 device**—The Dell Hybrid Client software is preloaded and installed on the device.
- **OptiPlex 3000 device**—The Dell Hybrid Client software is preloaded and installed on the device.
- **OptiPlex 7070 Ultra**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 3090 Ultra**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 7090 Ultra**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 3320**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 9420**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 3561**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 5421**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 5521**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 7090 Micro Form Factor**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 7090 Tower**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 7090 Small Form Factor**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 5090 Micro Form Factor**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 5090 Small Form Factor**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 3420**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 3520**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 5560**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 7490 All-in-One**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 3240 Compact**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 7320**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 7420**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 7520**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 9520**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **OptiPlex 5490 All-in-One**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 3650 Tower**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 7560**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 7760**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 3560**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 5320**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 5420**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Latitude 5520**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.

- **Precision 5760**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.
- **Precision 3450 Small Form Factor**—The Dell Hybrid Client software is preloaded with Dell Client Agent-Enabler (DCAE) installed.

## Security profiles

Dell Hybrid Client enables you to set different levels of **Security Profiles** to provide an enhanced device security for deploying third-party applications. This feature is available in Dell Hybrid Client version 1.5 onwards.

As part of security profiles, Dell Hybrid Client supports application sandboxing using Firejail and AppArmor.

Firejail profile restricts the running environment of untrusted applications and thereby enhances the device security. It is based on the Linux kernel sandboxing technology. For more information about the Linux Firejail sandbox, see the Firejail Security Sandbox article at [firejail.wordpress.com](http://firejail.wordpress.com).

AppArmor profile confines a program to only access the specified set of resources. This is based on the setting that specifies what files a given program can access. Enabling this feature adds an additional layer of protection to your applications. For more information about the Ubuntu AppArmor documentation at [help.ubuntu.com](http://help.ubuntu.com).

You can use Wyse Management Suite to configure the security profile settings. For more information about how to configure the security profiles, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

The following table describes different levels of security profiles that can be enabled on Dell Hybrid Client.

**Table 1. Security profiles**

Security feature	Low Security Profile / Open Box	Medium Security Profile —This profile is enabled by default.	High Security Profile
AppArmor profile for the Dell Hybrid Client-bundled applications.	Disabled	Enabled	Enabled
Default Firejail profile for third-party unsigned Debian applications.	Disabled	Enabled by default. If the desktop file of the application is not available in the <code>/usr/share/applications</code> location, the default firejail is disabled. In this case, if the metadata* is provided, the default firejail can be enabled.	Enabled only if the metadata is provided and high granular settings are not available in the metadata.
Firewall support through Uncomplicated Firewall (UFW)	Disabled	Disabled	Enabled
Kernel and operating system hardening.	Disabled	Disabled	Enabled
Developer tools for browsers.	Enabled	Disabled	Disabled
Profile Manager for Firefox.	Enabled	Disabled	Disabled

**NOTE:** The device must be reimaged to bring it back from **Open Box** setting to any other setting such as high, medium, and low profile.

\*For information about the metadata format, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

## USB device security

Dell Hybrid Client enables you to configure and manage the USB devices that are connected to your device. You can block access to USB devices, making them inaccessible from the client. The **USB Lockdown** settings can be configured using Wyse Management Suite. The feature is applicable only for device policy groups.

For more information about how to configure the USB lockdown settings, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

## GRUB password security

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 GRUB boot menu. The GRUB password is unique to each device. As a Wyse Management Suite administrator, you can view the GRUB password from the **More Actions** drop-down list on the **Devices** page on the Wyse Management Suite console. As a Wyse Management Suite administrator, you must change the GRUB password after you register the device for the first time. Changing the default GRUB password is mandatory for the device to be compliant.

**NOTE:** You must enter the GRUB password to access the **Advanced Settings** tab on **Device Settings** UI.

**NOTE:** You must enter the Serial Number or GRUB password to access the DCA UI.

For more information about how to set the GRUB password, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

## BIOS password security

As a Wyse Management Suite administrator, you must change the default BIOS password by using Wyse Management Suite.

The following table lists the default BIOS password for each platform:

**Table 2. Default BIOS password**

Platform name	Default BIOS password
Wyse 5070	Fireport
OptiPlex 7070 Ultra	Not applicable
OptiPlex 3090 Ultra	Not applicable
OptiPlex 7090 Ultra	Not applicable
Latitude 3320	Not applicable

**NOTE:** Except for the Wyse 5070 platform, no password is required for platforms listed in [Supported platforms](#).

For more information about how to set the BIOS password, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

## Application deployment security

Dell Hybrid Client enables you to install Dell-signed, custom-signed, and unsigned third-party applications. This feature is applicable only for devices that are powered by Dell Hybrid Client version 1.1. For deploying third-applications securely on devices that are powered by Dell Hybrid Client version 1.6, see [Security profiles](#). As a Wyse Management Suite administrator, you can use the Wyse Management Suite console to deploy application packages to Dell Hybrid Client-based devices. By default, all applications that are delivered by Dell are signed packages.

For more information about how to configure the application deployment settings, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).



# Product and subsystem security

## Topics:

- Product overview
- Authentication
- Authorization
- Network security
- Data security
- Cryptography
- Auditing and logging
- Code or product integrity

## Product overview

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.

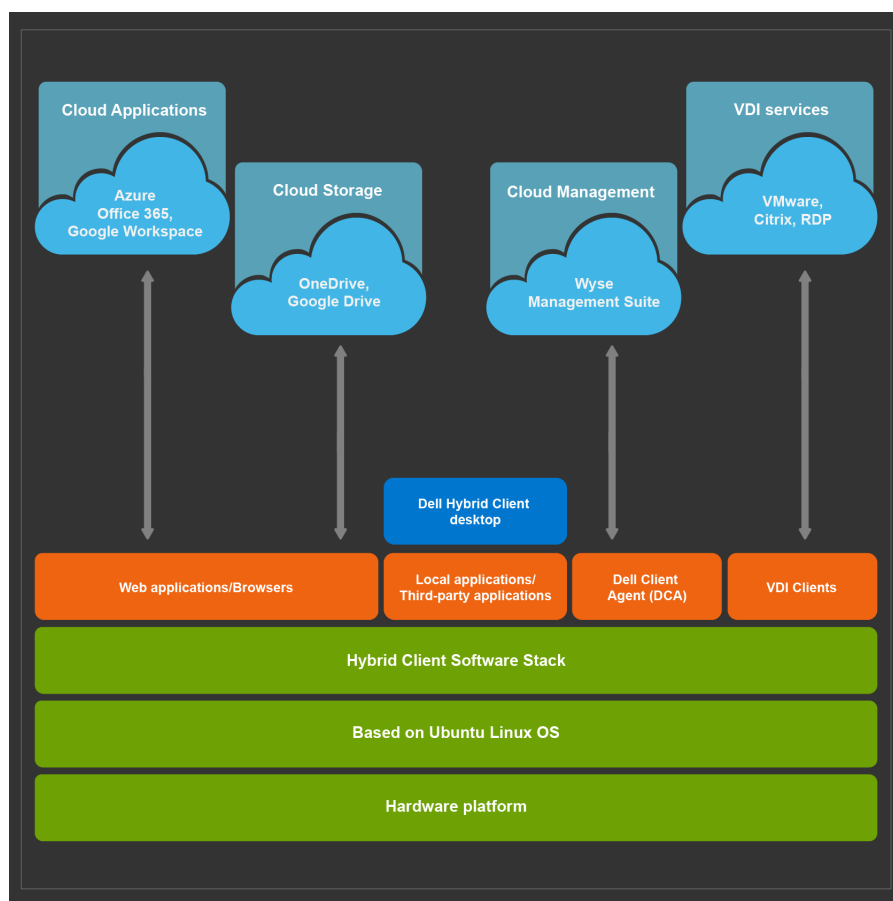


Figure 1. Dell Hybrid Client layered structure

# Authentication

Dell Hybrid Client supports the following configuration options for users or processes to authenticate to the product subsystems:

- **Account privilege levels**—There are two types of user accounts that are enabled for Dell Hybrid Client:
  - **Guest user**—The guest user account is a low-privilege account. It is available for users who do not have an Active Directory 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. Dell Technologies recommends that the guest user password is changed from Wyse Management Suite. By default, the password is not enabled for a guest user.
  - **Domain user**—The domain user account is a high-privilege account where all the configurations are preserved across logins.
  - **Local user**—The local user account is similar to the domain user account. However, a local user needs to be added from Wyse Management Suite. The user details and configurations are preserved only in one system.

**NOTE:** There is no default password for Guest user and Local user. It must be configured using Wyse Management Suite.

For more information about configuring the account settings, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

- **Virtual Desktop Infrastructure (VDI) Broker agent authentication**—AD credentials are used for authenticating users to remote VDI brokers agents. This allows user to access remote sessions and remote resources. Credential type can be a domain username with a password or a smart card. You can also use other authentications that are supported by both remote systems and local devices. User credentials are configured and managed by remote resource systems such as AD controllers and Broker agents. The following are the remote connection deployment options:
  - Citrix Virtual Apps and Desktops
  - VMware Horizon
  - Windows Remote Desktop Services
  - Direct RDP connections
  - Azure Virtual Desktop
  - Teradici (available as add-on)
  - Imprivata (available as add-on)

**NOTE:** Smart card authentication is not supported for RDP, Teradici, and Imprivata connections.

For more information about configuring the Broker agent settings, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

- **Active Directory authentication**—Dell Hybrid Client supports user authentication with Active Directory, both local AD and on-premises user synchronization with Azure AD. Active Directory allows an administrator to enable or disable the user authentication to specific work domains. As a domain user, you can securely connect to the work domain using the Active Directory credentials.

For more information about AD joining, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

- **Smart card-based authentication**—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.

For more information about how to log in as a domain user using a smart card, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

- **Unauthenticated Interfaces**—Dell Hybrid Client supports guest user login without a password. Dell Technologies recommends that as an administrator, you must set a password for the guest user account from Wyse Management Suite.
- **Wyse Management Suite server authentication**—Dell Hybrid Client-based device is registered to the Wyse Management Suite server through a valid group registration token. The server authentication is based on the group token and the device or user group to which the device is registered on Wyse Management Suite.

For more information about registering the device to Wyse Management Suite, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

## Login security settings

- **Device login security**—Device login is enabled for temporary guest users, domain users, and local users. A guest user can access Dell Hybrid Client with or without a password as configured by the administrator on the Wyse Management Suite console. A domain user is a registered user with valid credential details. A local user is a user created from Wyse Management Suite by the administrator for logging into the device without domain registration.
- **End User License Agreement (EULA) acceptance**—When you start a device that is powered by Dell Hybrid Client-based device for the first time, the End-User License Agreement (EULA) screen is displayed. EULAs must be read and accepted to continue using the Dell Hybrid Client software. EULA must be accepted first when using the DHCP or DNS method for automatic device enrollment.
- **Failed Login behavior and user account lockout**—During login authentication failures, a message **Please try again** is displayed on the login screen. Dell Hybrid Client reloads the login user interface when you enter incorrect login credentials. You can log in to Dell Hybrid Client only if the authentication is successful. However, you can configure the user account lockout for remote Broker agent or domain controller using the AD group policies.  
**i** **NOTE:** If incorrect login credential is entered for more than three attempts, then the account is locked for 60 s.
- **Security configurations**—The following are the security options that can be configured using Wyse Management Suite:
  - Configure the BIOS password for Dell Hybrid Client.
  - Add or modify Group Token for the device group.
  - Install a certificate on Dell Hybrid Client.
  - Configure USB lockdown settings to allow or block certain USB ports.
  - Configure the GRUB password for Dell Hybrid Client.
  - Enable or disable the VNC connection on Dell Hybrid Client.
  - Enable or disable the SSH connection on Dell Hybrid Client.
  - Set a password for Guest user on Dell Hybrid Client.
  - Enable or disable the installation of unsigned third-party applications.
  - Enable or Disable the security profiles by setting security profile as **Open Box**.
  - To access **Advance Settings** under **Device Settings**, GRUB password is required.

## User and credential management

- **User accounts and default credentials**
  - **Guest**—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. As an administrator, you can enable or disable the guest user account using Wyse Management Suite. The Guest user is the default user without a password. As an administrator, you can configure the password for the guest user account. 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. You can configure a password for the guest user from Wyse Management Suite.
  - **SSH**—The SSH user account is activated when the SSH add-on is deployed to Dell Hybrid Client from Wyse Management Suite. The default username is `sshuser`. The password is configured using the Wyse Management Suite console. As an IT administrator, you can grant elevated privileges to the SSH-enabled user from Wyse Management Suite. However, use this option with caution as granting elevated privileges to an SSH-enabled user may lead to inappropriate use of access on device.
  - **Admin**—The administrator's account is activated only when dev mode is enabled on Dell Hybrid Client. As an administrator, you can use the account to manage sudo or elevated privileges. In Dell Hybrid Client version 1.1, you must use the administrator's password to access the account. In Dell Hybrid Client 1.5 onwards, you can use the GRUB password to access the administrator's account. The administrator's account gets activated when you open the terminal from **Advanced settings** in **Device settings**.
  - **GRUB**—GRUB is the default boot loader for Dell Hybrid Client. GRUB password is unique to each device. As an administrator, you can set a password for the GRUB boot menu to restrict user access to the following operations:
    - Enabling dev mode to access the terminal.
    - User access to the GRUB boot menu.
- **Security profiles**—Security profiles can be set to **High**, **Medium**, **Low**, or **Open Box** based on the type of third-party applications that are being deployed—See [Security profiles](#).
- **BIOS admin credentials**—Dell Technologies recommends that as a Wyse Management Suite administrator, you must change the BIOS password from the Wyse Management Suite console—See, [BIOS security](#).

- **Broker, domain, and remote session credentials**—Remote session broker agent, active domain, remote desktop, and remote application credentials are configured by administrators of the respective remote resources. Remote resources include cloud, or hosts and virtual machines that are organized in domains. There is no local default credential for remote desktops or remote application users. User must use the credential that is configured on the remote site. Example—A domain user with remote desktop access privilege must enter domain credentials to access remote resources.
- **Managing credentials**—Account credentials can be managed by deploying the configuration from Wyse Management Suite to Dell Hybrid Client.
- **Securing credentials**—Dell Hybrid Client transmits and receives encrypted data from various servers including AD Server, RDP Server, Cloud Server, and Wyse Management Suite server for information related to user authentication and user data. The communication protocol is based on proven and safe encryption protocols. All credentials are stored in encrypted form in the device, or transmitted between the client and the server using encrypted keys that are unique to each device.
- **Password complexity**—Password complexity for remote desktop, remote application, session broker agent, and session gateway is managed by a remote system administrator. Example—Administrator can configure the settings using AD domain policies and apply the settings to all domain users for remote desktop access. Some passwords for device management require you to create a password according to the complexity and strength rules, including password length and password strength. When a new password is set, Wyse Management Suite only accepts passwords that meet the new length and complexity requirements. The tooltip on the Wyse Management Suite password setting UI displays the complexity and length requirement for each password. If the password complexity does not meet the device criteria, an error is displayed in the Wyse Management Suite event list.

## Authentication to external systems

The following authentication types are supported on Dell Hybrid Client for accessing the external systems:

- Kerberos-based SSO authentication is supported for Dell RDP and Active Directory.
- Azure and Google Cloud server authentication (with or without SSO) is supported using username, password, or smart card.
- Box.com server authentication is supported using username and password.
- Citrix authentication is supported with or without SSO. A valid certificate is used to validate the server. Citrix uses a domain registered username and password, or a smart card for authentication.
- VMware authentication is supported without SSO. VMware uses a valid username and password, or a smart card for authentication.
- Windows Virtual Desktop without SSO is supported using username and password.
- Wyse Management Suite server authentication is based on Unique ID (UID). A random UID is generated for each device that is registered to Wyse Management Suite.

## Authorization

- **Guest user authorization**—A guest user is authorized to access all system configurations without SSO. The guest user needs credential details to access all VDI and cloud infrastructure. The Wyse Management Suite administrator can enable the guest user account with or without password using the Wyse Management Suite console.
- **Domain user authorization**—A registered domain user is authorized to access all system configurations with or without SSO.
- **Local user authorization**—A registered local user is authorized to access all system configurations without SSO.
- **Remote authorization settings**—The following are the supported remote authorization options for accessing Dell Hybrid Client remotely:
  - **VNC access**—Dell Hybrid Client can be accessed remotely using VNC. As an administrator, you must deploy the VNC add-on using Wyse Management Suite to enable the VNC access on Dell Hybrid Client.
  - **SSH access**—Using the SSH protocol, you can connect securely to Dell Hybrid Client from a remote device. As an administrator, you must deploy the SSH add-on using Wyse Management Suite to enable the SSH access on Dell Hybrid Client.
- **External authorization associations**—When you access the VDI resources, user credentials are configured from remote resource systems, and the authorization is processed on the remote resource systems. Authorization is configured on VDI Broker agents, gateways, and remote session hosts.
- **Advanced setting authorization**—In **Device Settings** there are certain configurations that require elevated authentication. The random GRUB password is to be used for first time to unlock these Advanced settings. However, once the Wyse Management Suite administrator changes the GRUB password (post Wyse Management Suite registration), the same can be used to unlock these settings from there onwards.
- **Dell Client Agent authorization**—You must authenticate to open Dell Client Agent and register the client using Wyse Management Suite. The default password to access the Dell Client Agent UI is the Device Serial Number. Once the device is

registered using the Wyse Management Suite and is compliant, the Dell Client Agent password remains the same as GRUB password set using Wyse Management Suite. However, if the device is noncompliant, the password remains the same as the random password which can be generated through Wyse Management Suite.

- **Log files authorization**—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.

## Network security

- **Network exposure**—The following table lists the network ports that are used for HTTP and HTTPS communications between different services.

**Table 3. Network exposure**

Service name	Port	Summary
DNS Service	50	Used for DNS services
Citrix	80, 443, 8100, 1433,1434, 135, 3389, 389, 2598, 1494, 8008, 16500–16509, and 9001	Used for connecting to Citrix desktop and published applications
VMware	55000, 4172, 3389, 9427, 32111, 22443, 389, 80, 443, 8443, 48080, 4100, 4101, 8472, and 22389	Used for connecting to VMware desktop and Published applications
RDP	3389	Used for connecting to RDP desktop and published applications
Kerberos	88 and 464	Used for SSO-based authentication
WMS	443 and 1883	Used for connecting to the Wyse Management Suite server.
SSH	22	Used for Secure Shell (SSH) connections.
VNC	5900	Used for VNC connections.

- **Communication security settings**—Dell Hybrid Client supports the following access methods:
  - Use the Wyse Management Suite server to configure and manage the device settings.
  - Use the VNC connection to remotely control the device.
  - Use the SSH connection to remotely access the device.

All access methods must be configured from Wyse Management Suite before use.

- **Firewall settings using Uncomplicated Firewall (UFW)**—This feature is enabled when the security level is set to **High**. By default, the firewall is disabled on the device. When the firewall is enabled, the following actions take place:
  - Denies incoming packets with exception for ports utilized for Dell Hybrid Client features.
  - Allows all the outgoing packets.
  - Disables routed packets.

## Data security

- **Data at Rest**—The home folder of an AD user is encrypted and secured using the ZFS encryption. All the user-level data and device-level data are protected with approved encryption mechanisms. All encryption keys are stored securely. All the DBs are encrypted and stored in the system.
- **Data in Flight**—All data communication that is transmitted to and from the device uses a standard TLS encryption mechanism—TLS version 1.2 and later. When the user logs off, the user-specific configurations is encrypted and backed up in the Wyse Management Suite server or a cloud server.

# Cryptography

- AES 256 algorithm is used to encrypt user data at rest.
- TLS version 1.2 and later are used for remote communications—VDI, cloud, and Wyse Management Suite.

## Auditing and logging

Table 4. Auditing and logging

Component	Summary
Log protection	To comply with the security standards, Dell Hybrid Client system does not log any sensitive data in the log file. The log files are locked with the current GRUB password when exported out of the system. The password can be changed by the Wyse Management Suite administrator.
Logging format	Log format includes <time stamp> <Type> <Service> <log message>. <b>Type</b> specifies whether the log is an INFO, ERROR, or a DEBUG log.
Alerting	Alert logs are displayed on the system as notifications.

## 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

### 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.

## Code or product integrity

Dell Hybrid Client enables you to install Dell-signed, custom-signed, and unsigned third-party applications. As an administrator, you must use the Wyse Management Suite console to deploy application packages to devices powered by Dell Hybrid Client. All files that are distributed by Dell are signed applications. To get your application signed by Dell, contact your Dell Sales Representative and submit the Debian file that needs to be signed. Once the signing process is complete, the Dell Sales Representative will deliver the signed application. Alternatively, you can also install custom-signed and unsigned applications on Dell Hybrid Client. For more information about installation of third-party applications on Dell Hybrid Client, see the *Dell Hybrid Client Version 1.x Administrator's Guide* at [www.dell.com/support](http://www.dell.com/support).

# Contacting Dell

## Prerequisites

 **NOTE:** If you do not have an active internet connection, you can find contact information on your purchase invoice, packing slip, bill, or Dell product catalog.

## About this task

Dell provides several online and telephone-based support and service options. Availability varies by country and product, and some services may not be available in your area. To contact Dell sales, technical support, or customer service issues:

## Steps

1. Go to [www.dell.com/support](http://www.dell.com/support).
2. Select your support category.
3. Verify your country or region in the **Choose a Country/Region** drop-down list at the bottom of the page.
4. Select the appropriate service or support link based on your need.