


Wyse Management Suite

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.

Chapter 1: Preface.....	4
Legal disclaimer.....	4
Scope of document.....	4
Document references.....	4
Security resources.....	4
Getting help.....	5
Reporting security vulnerabilities.....	5
Chapter 2: Security quick reference.....	6
Deployment models.....	6
Security hardening third-party components.....	6
Security profiles.....	6
Chapter 3: Product and subsystem security.....	7
Product overview.....	7
Authentication.....	7
Login security settings.....	7
User and credential management.....	8
Authentication types and setup.....	8
Authorization.....	9
Network security.....	9
Data security.....	10
Configuring Transport Layer Security.....	10
Cryptography.....	10
Certificate management.....	10
Auditing and logging.....	11
Event audit.....	11
Log management.....	11
Code or product integrity.....	11
Browser support for CSP header.....	11
Chapter 4: Verify code signing.....	12
Chapter 5: Contacting Dell.....	13

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. Dell Technologies recommends 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 Wyse Management Suite. The document provides guidelines that help you maximize the security posture of your environment. You will understand the expectations that Dell has of the environment in which the Wyse Management Suite is deployed.

Document references

The following documents provide a comprehensive reference to Wyse Management Suite:

- [Dell Wyse Management Suite Release Notes](#)
- [Dell Wyse Management Suite Administrator's Guide](#)
- [Dell Wyse Management Suite Migration Guide](#)

You can access the manuals available at www.dell.com/support/manuals.

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.

Getting help

The [Dell support page](#) provides access to licensing information, product documentation, advisories, software downloads, how-to videos, and troubleshooting information.

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.
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:

- [Deployment models](#)
- [Security hardening third-party components](#)
- [Security profiles](#)

Deployment models

You can download Dell Wyse Management Suite from www.dell.com/support.

Dell Wyse Management Suite can be installed using a local path or a network share folder as a package source for installation. For more information, see Dell Wyse Management Suite Installation Guide at www.dell.com/support/manuals.

By default, the on-premise deployment supports HTTPS protocol security configuration.

Following are the recommendations to enable the security options when you deploy Wyse Management Suite on a private cloud:

- Before you install the product in the recommended Windows Server operating system, ensure that the operating system is updated with the latest service packs, patches, and updates.
- Import the SSL certificate to secure the connection to Wyse Management Suite.
- Always enable HTTPS protocol on port 443 for Wyse Management Suite.
- Enable TLS 1.2 version.
- Import trusted certificates and enable CA validation for certificates.
- Harden the third-party components.
- Ensure the security of the SMB protocol by enabling SMB signing on the host Windows server. For information on configuring SMB signing, see *Overview of Server Message Block signing* at <https://docs.microsoft.com/>.

Security hardening third-party components

Wyse Management Suite provides you details to harden the third-party components in order to ensure that the components can be configured to be more secure.

For information about how to harden the following third-party components, see *Hardening Document for Server Security Configuration* at www.dell.com/support/manuals:

- Mongo database
- MySQL database
- JDK
- Tomcat

Security profiles

Dell Wyse Management Suite runs under the default security profile with secure HTTP enabled over TLS version 1.2 and 1.3. It is recommended to use the Certificate Authority (CA) signed certificates for stronger security environments.

Product and subsystem security

Topics:

- [Product overview](#)
- [Authentication](#)
- [Authorization](#)
- [Network security](#)
- [Data security](#)
- [Cryptography](#)
- [Auditing and logging](#)
- [Code or product integrity](#)
- [Browser support for CSP header](#)

Product overview

Dell Wyse Management Suite is the next generation management solution that enables you to centrally configure, monitor, manage, and optimize your Dell Hybrid Client powered endpoints and Dell thin clients. It also offers advanced feature options such as cloud and on-premises deployment, manage-from-anywhere option by using a mobile application, and so on..

Authentication

Dell Wyse Management Suite supports the following processes to authenticate the product subsystems:

- Wyse Management Suite console authentication
- Device registration with Wyse Management Suite
- Wyse Management Suite remote repository authentication

Login security settings

- **Administrator console login settings**—By default, you can log in to the console using the registered administrator credentials enabled during installation. The registered administrator can access the product with a registered username and password. After a failed login, you are notified with the text as

```
Your login attempt was un successful, try again. Reason: Invalid username or password
```

HTTPS communication is enabled by default. Security on session is established by enforcing a token authentication for each request to access the console.

You can also configure Active Directory to enable the Domain account to access the product.

NOTE: Secure connection to Active Directory can be established with the use of LDAPS protocol. For more information, see Wyse Management Suite 3.2 or later version *Administrator's guide* at <https://www.dell.com/support/manuals>.

- **Device login security**—Devices are registered with a secured group token. Device check-in and device commands are performed with a unique device authentication code. Device and Wyse Management Suite coordinates using MQTT in a secure way.
- **Remote repository login settings**—Repository is registered with the Wyse Management Suite using the administrator user accounts.
- **Disable auto-complete feature settings**—Ensure that you disable the browser autocomplete feature if the browser is used in shared computing where multiple users use the browser. For more information, see the respective browser documentation for disabling the autocomplete feature settings.

- Wyse Management Suite 3.5 supports concurrent login. From Wyse Management Suite 3.8, concurrent login of a user is not supported and a user can have only one active session.

When you try to log in to the server from another browser or try to log in from another system without logging off from the previous session, then

```
Your login attempt was not successful. Reason: User account already logged in
```

error message is displayed. The same error is displayed if you do not log off from the session from a browser.

The administrator can select the option **Log me out everywhere else** to log in to the portal forcefully. If the option is selected, the previous login session is invalidated. After you deploy on-premises or public cloud version of Wyse Management Suite, all the active sessions are invalidated. The administrator must relogin to Wyse Management Suite to continue accessing the portal.

When the administrator changes the portal administrator role or the username for any other logged in user, then the session of other logged in user gets invalidated. The other administrators must relogin to Wyse Management Suite to continue accessing the portal.

User and credential management

- User account and security credentials
 - Administrator
 - Global administrator who has access to all Wyse Management Suite features.
 - Group administrator who has access to all assets and functions for an assigned group.
 - Custom global administrator who has access to customized Wyse Management Suite features.
 - Viewer who has only read access to all the data and can be assigned permissions to send real-time commands such as shutdown and restart.
 - Unassigned administrators—Users who are imported from the AD server are displayed on the **Unassigned admins** page. You can assign a role to these users from the portal.
 - End users—You can add individual users to Wyse Management Suite using the **End Users** tab. You can configure and deploy settings to an individual user. The settings are applied to the user account and are applied to the thin client when the user logs in. This option is applicable only to thin clients running the ThinOS 9.x operating system and Dell Hybrid Clients.
 - Multi-Tenant users—Multi tenant users can be enabled from the **Portal Administration** page. For more information, see *Wyse Management Suite Administrator's Guide* at <https://www.dell.com/support/manuals>.
- Security credentials—Wyse Management Suite securely communicates to various devices and third party servers including active directory, repository, Edge gateways, and mobile application. The communication protocol is based on proven and safe encryption protocols.
- Password complexity—All passwords to access Wyse Management Suite 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 accepts passwords that meet the new length and complexity requirements. The tooltip on the settings UI displays the complexity and length requirement for each password. If the password does not meet the specified requirement, the field is highlighted in red color to indicate that the entered password is invalid. For third party servers integrated with Wyse Management Suite, the password complexity is managed by the third party server.
- Authentication to external systems—Kerberos based SSO authentication is supported for Active directory.

Authentication types and setup

Dell Technologies enables secure HTTPS communication between the device and Wyse Management Suite. The following three types of authentications are supported:

- Device authentication—Devices are registered to Wyse Management Suite with a secure group token.
- User authentication—During installation, a user with global administrator privileges must be created. Using the global administrator user, other users and roles can be created. You can also configure active directory users and roles.
- Third-party components authentication—Active directory can be integrated with Wyse Management Suite by using LDAP or LDAPS. A global administrator can import and configure active directory users and their roles. It is recommended to use the LDAPS protocol to integrate the active directory in a secure way.

Authorization

- **Product services**—All Windows product services are provided with limited privileges to ensure security.
- **Console**—Console authorization for Wyse Management Suite users have the following groups:
 - Administrator
 - Global administrator who has access to all Wyse Management Suite features.
 - Group administrator who has access to all assets and functions for an assigned group.
 - Custom global administrator who has access to customized Wyse Management Suite features.
 - Viewer who has only read access to all the data and can be assigned permissions to send real-time commands such as shutdown and restart.
 - Unassigned administrators—Users who are imported from the AD server are displayed on the **Unassigned admins** page. You can assign a role to these users from the portal.
 - End users—You can add individual users to Wyse Management Suite using the **End Users** tab. You can configure and deploy settings to an individual user. The settings are applied to the user account and are applied to the thin client when the user logs in. This option is applicable only to thin clients running the ThinOS 9.x operating system and Dell Hybrid Clients.
 - Multi-Tenant users—Multi tenant users can be enabled from the **Portal Administration** page. For more information, see *Wyse Management Suite Administrator's Guide* at <https://www.dell.com/support/manuals>.
- **Device**—Device configuration in Wyse Management Suite has following authorization steps:
 - Device Registration
 - Device check-in

You can also enable or disable **Device Enrollment Validation** from **Portal Administration** page.

Network security

Default installation of Wyse Management Suite establishes HTTPS protocol communication.

- **Network exposure**—The following table lists the network ports that are supported on Wyse Management Suite. The ports are open by default when you install Wyse Management Suite.

Table 1. Network exposure

Service name	Port	TCP or UDP	Summary
Dell On-Premises Private Cloud	443(Recommended), 8080	TCP	Security recommendation is to enable the 443 port to ensure the secure way of communication.
Dell Secure MQTT Service	8443	TCP	By default 8443 port is open with the installation to ensure a secure connection with MQTT.
MQTT Broker agent Service	1883	TCP	This port is also open post installation. NOTE: Ensure that you disable 1883 port message when Secure MQTT is enabled.
EMSDK	5172, 49159	TCP	Optional and enabled only to manage Teradici devices.

Network vulnerability scanning is performed on Wyse Management Suite and there are no security issues on the networked subsystems or interfaces. If you discover a security issue, you are encouraged to report it to Dell immediately. See, [Reporting security vulnerabilities](#).


- **Communication security settings**—By default Wyse Management Suite enables HTTPS protocol for communication. Additionally, you can enable the following secure communications:
 - Secure communication to MQTT using port 8443.
 - LDAPS protocol for AD integration. For more information, see *Dell Wyse Management Suite 3.2 or later version Administrator's Guide* at <https://www.dell.com/support/manuals>.

Data security

- **Data at Rest**—The data is encrypted and stored in a database. Access to the database is restricted and you cannot access the database remotely. Also, passwords or any secure information is not displayed.
- **Data in Flight**—In order to ensure the security, regular updates to the cipher's enablement and disablement must be adhered for Wyse Management Suite. The following list of ciphers can transmit secrets securely:
 - TLS 1.2
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_DHE_RSA_WITH_AES_256_CCM
 - TLS_DHE_RSA_WITH_AES_256_CCM_8
 - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
 - TLS 1.3
 - TLS_AES_256_GCM_SHA384
- **Data integrity**—Wyse Management Suite does not allow you to publish or expose user data or sensitive data in logs or in any format. Wyse Management Suite ensures to send sensitive data either in Post Request body or in Request headers. But does not allow in HTTP GET query strings.

Configuring Transport Layer Security

The Wyse Management Suite on-premise installer is improved to select the Transport Layer Security (TLS) version 1.2 and 1.3 during the installation or upgrade. You can also enable the TLS versions using the **Portal Administration** page.

 **NOTE:** From Wyse Management Suite 3.5, the recommended version of Transport Layer Security is 1.2 and 1.3. Ensure that you select all the appropriate versions of TLS based on the device agent and the merlin image. Older versions of Windows Embedded System, Wyse Device Agent (versions below WDA_14.4.0.135_Unified), and 32-bit merlin image versions are only compatible with TLS version 1.0.

Cryptography

AES-256 is used for encryption in Wyse Management Suite. TLS 1.1 is disabled and TLS 1.2 is enabled by default with on-premise installation. Dell Technologies recommends that you use the TLS 1.2 protocol.

Certificate management

You can import your SSL certificate to secure communications with the Wyse Management Suite server. You can import the console by logging in to the Wyse Management Suite private cloud and importing from the **Portal Administration** page.

By default, the Wyse Management Suite imports the self-signed SSL certificate that is generated during the installation to secure communication between the client and the Wyse Management Suite server. If you do not import a valid certificate for your Wyse Management Suite server, a warning message is displayed when you access the Wyse Management Suite from a device other than the server where it is installed.

A warning message is displayed if the self-signed certificate that is generated during installation is not signed by a Certificate Authority such as [geotrust.com](https://www.geotrust.com). You can either import a .pem or .pfx certificate.

Wyse Management Suite provides a provision to enable the CA validation. Enabling it ensures that the transactions such as file operations, image push or pull with the clients work in a secure way and with certificate signature validation.

Auditing and logging

Event audit

Wyse Management Suite manages events by event types such as group creation, device registration, configuration modification, and file upload.

For each event, a static audit message is generated. Go to **Events > Audit** to view the event audit messages. They can be exported from **Portal Administration > Reports**.

Log management

By default, Wyse Management Suite manages logs with the default configuration. You must have sufficient disk space to store the logs. The log levels are categorized into INFO, WARN, DEBUG, and ERROR.

Wyse management suite provides event logs in the console for the events that are related to device, configurations, and other required events.

Log protection

Dell Wyse Management Suite product does not share sensitive information in logs, and users outside the cluster cannot access these logs. Only authenticated and authorized users can access the logs.

Logging format

Logs from Wyse Management Suite include timestamp and log levels consistently. A new line separates each log entry. Some log entries such as exception stack traces may span multiple lines. The timestamp indicate the start of a new entry, and the entries usually include origination information to distinguish similar entries.

Code or product integrity

Dell Wyse Management Suite enables you to update system packages and install third-party applications. All firmware and application packages that are used in Wyse Management Suite are Dell-signed packages. All files that are distributed by Dell are signed applications. You can download the packages from www.dell.com/support and deploy the packages from Wyse Management Suite. EULA must be accepted for all the packages of Wyse Management Suite. Wyse Management Suite does not accept the package if:

- The package does not have a valid signature.
- The package has fake signature.
- The package is altered.

Browser support for CSP header

For enhanced security, CSP headers are added in Wyse Management Suite 3.8. Dell Technologies recommends that you use the following browsers to access Wyse Management Suite 3.8, as they take advantage of this added security layer by processing the CSP headers appropriately:

- Edge 79 or later
- Mozilla Firefox 58 or later
- Chrome 59 or later


Verify code signing

Steps

1. Right-click the **WMS.exe** installer.
2. Click **Properties**.
3. From **WMS.exe Properties** window, click **Digital Signatures** tab.
4. Select **Dell Inc** from the **Signature list** and click **Details**.
5. Click **View Certificate** and a new window is displayed with certificate details.
Ensure that **Issued to**, **Issued by**, and **Valid from** details are validated on the certificate to verify code signing.

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.
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.