Dell Wyse ThinOS Version 9.1

Security Configuration Guide

March 2022
Rev. A01

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.**

Contents

1

Preface

Topics:

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 ThinOS version 9.1. The document provides guidelines that help you maximize the security of your thin clients in your environment. You will understand the expectations that Dell has of the environment in which the ThinOS product is deployed.

Document references

The following documents provide a comprehensive reference to the ThinOS version 9.1 operating system:

- Dell Wyse ThinOS Version 9.1 Release Notes
- Dell Wyse ThinOS Version 9.1 Administrator's Guide
- Dell Wyse ThinOS Version 9.1 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.com site.

2

Security quick reference

Topics:

Supported platforms

The Dell Wyse ThinOS version 9.1 firmware is supported on the following thin clients:

- Wyse 3040 Thin Client
- Wyse 5070 Thin Client
- Wyse 5470 Thin Client
- Wyse 5470 All-in-One Thin Client
- OptiPlex 3000 Thin Client

Wyse 3040, 5070, 5470, and 5470 All-in-One thin clients—Dell Technologies recommends that you use the Dell Wyse Management Suite version 3.6 to upgrade your ThinOS firmware to 9.1.6108. You can also use the Dell Wyse USB Imaging Tool version 3.4.0 to install the ThinOS 9.1.6108 Merlin image on your thin client.

OptiPlex 3000 Thin Client—Prepare a USB drive to create an installer based on the ThinOS 9.1.6108 ISO image, using the Dell Recovery Tool. Recover ThinOS using the USB drive that you prepared.

Security profiles

By default, ThinOS devices have the highest privilege when you start the thin client for the first time after a factory reset. An administrator can set different privileges to different devices using either Wyse Management Suite or the local Admin Policy Tool.

There are three privilege levels:

- **High**—All the menu options are available to end users.
- **Customize**—Administrator can define which menu options are available to end users.
- **None**—Only VDI connections are available to end users.

ThinOS also supports the administrator mode on the local ThinOS UI. In any privilege level, local users can enter the configured administrator mode username and password to enable the **High** privilege level on your device. Local users should exit the Administrator mode and return to the preset privilege level after completing the task that needs a higher privilege level.

Configure account privileges using Admin Policy Tool or Wyse Management Suite

Steps

1. On the ThinOS client, open the Admin Policy Tool, or go to ThinOS 9.x policy settings on Wyse Management Suite.
   The **Configuration Control || ThinOS** window is displayed.
2. Click the **Standard** tab or the **Advanced** tab.
3. Expand **Privacy & Security**.
4. Click **Account Privileges**.

5. Click the **Enable Admin Mode** slider switch if you want to enable the Administrator mode. When enabled, you must specify the Admin username and password.
6. From the **Privilege Level** drop-down list, select a privilege level—**None**, **Customize**, or **High**.

   When you set the user privilege to **Customize**, you can manually select options that you want to enable or disable in the ThinOS system menu.

7. Click **Save & Publish**.

Flash security

- **Secure Boot**—By default, Secure Boot is enabled on the device to ensure that the system is secure during the boot process.
- **Flash encryption**—The entire disk is encrypted for each individual device except the Extensible Firmware Interface (EFI) system partition. The data on the disk is safe and secure.

USB device security

- **Allow or block access to USB devices**—ThinOS enables you to allow or block access to USB devices that are connected to your device.

  To allow access to USB devices, do the following:

  1. On the ThinOS client, open Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.

  2. On the **Advanced** tab, expand **Privacy & Security**, and click **Device Security**.
  3. From the **Device Security** Type drop-down list, select **Allow**.
  4. In the **Device Security Allow list** section, click **Add Row**.
  5. Enter the vendor ID and product ID of the device. Example—`0xvvvvpppp`, where vvvv is device vendor ID and pppp is device product ID.
  6. Enter the class name or class ID. Example—**Audio** or **0xccsspp**.
  7. Click **Save & Publish**.

  To block access to USB devices, do the following:

  1. On the ThinOS client, open Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.

  2. On the **Advanced** tab, expand **Privacy & Security**, and click **Device Security**.
  3. From the **Device Security** Type drop-down list, select **Deny**.
  4. In the **Device Security Allow list** section, click **Add Row**.
  5. Enter the vendor ID and product ID of the device. Example—`0xvvvvpppp`, where vvvv is device vendor ID and pppp is device product ID.
  6. Enter the class name or class ID. Example—**Audio** or **0xccsspp**.
  7. Click **Save & Publish**.
- **Allow or block access to USB ports**—ThinOS enables you to allow or block access to USB ports of the device.

  To enable or disable access to USB ports, do the following:

  1. On the ThinOS client, open Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.

  2. On the **Advanced** tab, expand **BIOS**, and select your platform model.
  3. From the **Device Security** Type drop-down list, select **Deny**.
  4. In the **System Configuration** section, click the **Enable Rear USB Ports** toggle switch to enable or disable the rear USB ports. If the USB port is disabled, the operating system cannot detect the device that is attached to this port.
  5. Click the **Enable Front USB Ports** toggle switch to enable or disable the front USB ports. If the USB port is disabled, the operating system cannot detect the device that is attached to this port.
  6. Click **Save & Publish**.

Federal Information Processing Standard (FIPS) compliance

ThinOS allows you to enable or disable the Federal Information Processing Standard (FIPS) Publication 140-2 Level 1 authentication compliance. It is based on OpenSSL (Open Secure Socket Layer). You can configure the option using System Tools on the ThinOS client, local Admin Policy Tool, or Wyse Management Suite.

When you enable FIPS on ThinOS, algorithms that are unapproved by FIPS are not allowed to be used in a wireless connection. If the selected method uses an unapproved algorithm, the wireless connection fails. Example—EAP-MD5, EAP-MSCHAPV2, EAP-FAST, EAP-LEAP methods use MD5 and MD4, which are unapproved by FIPS.

To enable FIPS using either Admin Policy Tool or Wyse Management Suite, do the following:

1. On the ThinOS client, open Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

   The **Configuration Control | ThinOS** page is displayed.
2. On the **Advanced** tab, expand **Privacy & Security**, and click **Device Security**.
3. Click the **Enable FIPS** toggle switch to enable the option.
4. Click **Save & Publish**.

To enable FIPS using System Tools, do the following:

1. Log in to the ThinOS client.
2. From the desktop menu, click **System Tools**.

   The **System Tools** dialog box is displayed.
3. Click the **Certificates** tab.
4. Click the **Enable FIPS** toggle switch to enable the Federal Information Processing Standard (FIPS) Publication 140-2 authentication compliance.
5. Click **OK**.

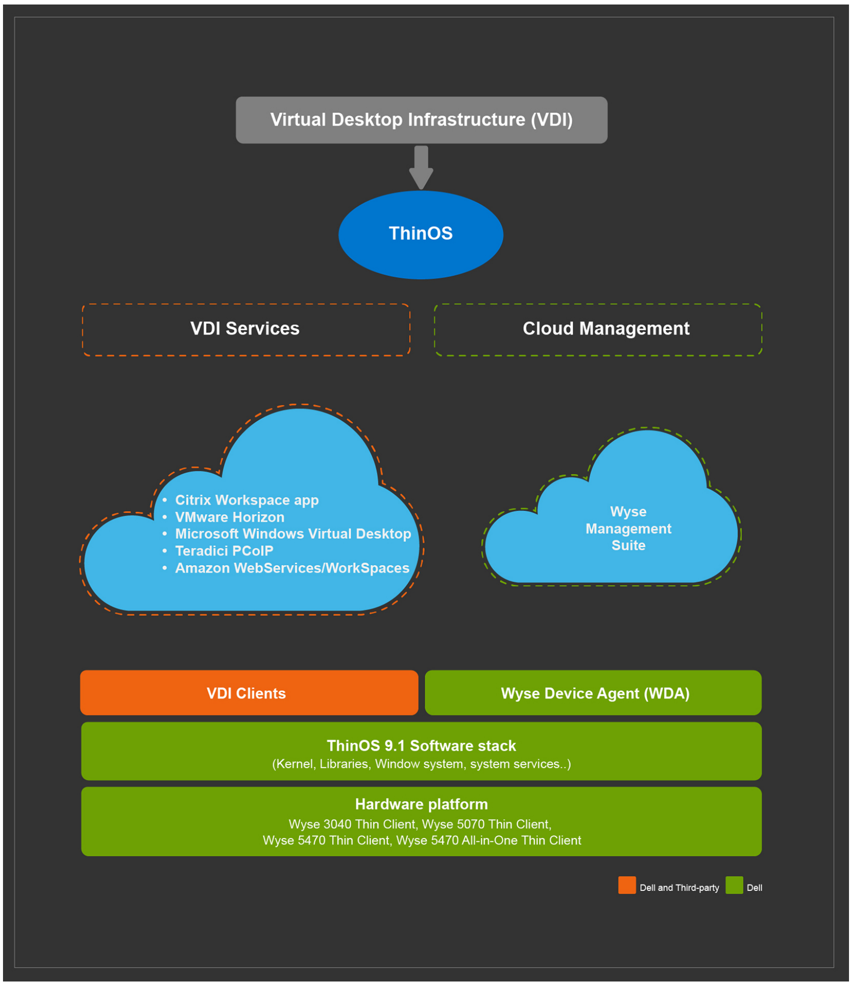
3

Product and subsystem security

Topics:

Product overview

ThinOS is a highly secure, deployment-ready operating system for endpoints that connect to virtual workspaces.



Virtual Desktop Infrastructure (VDI)
ThinOS
VDI Services
Cloud Management
• Citrix Workspace app
• VMware Horizon
• Microsoft Windows Virtual Desktop
• Teradici PCoIP
• Amazon WebServices/WorkSpaces
Wyse Management Suite
VDI Clients
Wyse Device Agent (WDA)
ThinOS 9.1 Software stack
(Kernel, Libraries, Window system, system services..)
Hardware platform
Wyse 3040 Thin Client, Wyse 5070 Thin Client,
Wyse 5470 Thin Client, Wyse 5470 All-in-One Thin Client
🟧 Dell and Third-party
🟩 Dell

Figure 1. ThinOS layered structure

Authentication

ThinOS supports the following configuration options for users or processes to authenticate to the product subsystems.

- Account privilege levels
- VDI broker agent authentication
- Active domain authentication
- Multifactor, token, and certificate-based authentication
- Authentication application support
- Unauthenticated authentication support
- Wyse Management Suite server authentication

For more information about the authentication types, see Authentication types and setup.

Login security settings

- **Login banner configuration**—ThinOS enables you to configure the banner or logo for the login window. Use the local Admin Policy Tool or Wyse Management Suite to upload your preferred login banner or logo image.
  1. On the ThinOS client, open Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.
  2. On the **Advanced** tab, expand **Login Experience**, and click **Login Settings**.
  3. In the **Login Experience** section, browse and select a logo that is to be displayed in the login window.
  4. Click **Save & Publish**.
- **Legal notice configuration**—ThinOS enables you to configure a legal notification file to be displayed in the login window. Use the local Admin Policy Tool or Wyse Management Suite to configure the legal notification file.
  1. On the ThinOS client, open Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.
  2. On the **Advanced** tab, expand **Login Experience**, and click **Login Settings**.
  3. In the **Login Experience** section, browse and select a legal notification file to be displayed during sign-on. User must accept the legal notification to continue the sign-on process.
  4. In the **Notice File Title** field, enter the title for the notification dialog box.
  5. In the **Notice File Title Button Caption** field, specify the name for the button that is displayed in the notification dialog box.
  6. Click **Save & Publish**.
- **End User License Agreement (EULA) acceptance**—When you start the ThinOS client for the first time or perform a factory reset, the End-User License Agreement (EULA) screen is displayed. EULAs must be read and accepted to continue using ThinOS. By default, the Dell EULA and HID EULA are displayed. The third-party EULAs are displayed on the EULA screen depending on the ThinOS application packages that you install on the thin client.
- **Failed Login behavior and user account lockout**—ThinOS reloads the login UI when you enter incorrect login credentials. You can log in to ThinOS 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.

Authentication types and setup

- **Local UI privilege level and Administrator mode**—Local UI privilege level can be set to **None**, **Customized**, or **High**. You can enable or disable the local UI Administrator mode using either the local Admin Policy Tool or Wyse Management Suite. For more information about account privileges and administrator mode, see Security profiles.
- **Networks and VPN authentication**—ThinOS supports authentication to both wired and WiFi network connections. Supported authentication types include **Open**, **WPA/WPA2 Personal**, **WPA/WPA2 Enterprise**, **OWE**, **WPA3 Personal**, and **802.1x** authentication. You can configure the authentication settings using either the local Admin Policy Tool or Wyse Management Suite. If your privilege level allows you to access the local UI, you can configure the authentication settings from the local ThinOS client.

  ThinOS uses the OpenConnect client that is based on the SSL protocol for connecting to a VPN. Use a valid username and password to establish a VPN connection. You can configure the VPN settings using either the local Admin Policy Tool or Wyse Management Suite. If your privilege level allows you to access the local UI, you can configure the VPN settings from the local ThinOS client.

For more information about how to configure the network and VPN settings, see the *Dell Wyse ThinOS Version 9.1 Administrator's Guide* at www.dell.com/support.

- **Virtual Desktop Infrastructure (VDI) broker agent authentication**—User can use AD user credentials to authenticate to remote VDI brokers agents 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 types of authentication which are supported by both remote systems and thin client. User credentials are configured and managed by remote resource systems such as AD controllers and broker agents.

  The following are the remote connections deployment options:

  - Citrix Virtual Apps and Desktops
  - VMware Horizon
  - Windows Virtual Desktop
  - Windows Remote Desktop Services
  - Amazon WorkSpaces
  - Teradici Cloud Access
  - Direct RDP connections

  To configure the broker agent settings, do the following:

  1. On the ThinOS client, open the local Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.

  2. On the **Advanced** tab, expand **Broker Settings** and configure your preferred broker agent settings.
  3. Click **Save & Publish**.

  You can also use the local ThinOS UI to configure the broker agent settings. For more information about broker agent settings, see the *Dell Wyse ThinOS Version 9.1 Administrator's Guide* at www.dell.com/support.

- **Active Domain authentication**—User can use AD user credential to authenticate to domain controller (NTLM) and access the AD group of the user from Wyse Management Suite. A username with a valid password is used for authentication. User credentials are configured and managed by remote resource systems such as AD controllers.

  To configure the active domain controller (NTLM) settings, do the following:

  1. On the ThinOS client, open the local Admin Policy Tool, or go to the ThinOS 9.x policy settings on Wyse Management Suite.

     The **Configuration Control | ThinOS** page is displayed.

  2. On the **Advanced** tab, expand **Login Experience**, and click **Login Settings**.
  3. From the **Login Type** drop-down list, select **Authenticate to domain controller**.
  4. Specify the AD group prefix.
  5. Click **Save & Publish**.

     ThinOS authenticates to the domain controller of the active domain to which the user belongs.

- **Multifactor, token, and certificate-based authentication**—Multifactor authentication is configured by remote resource system administrators. ThinOS supports Citrix Application Delivery Controller (ADC), formerly known as Citrix NetScaler. The following authentication methods are supported:

  - LDAP
  - RSA
  - DUO
  - SMS PASSCODE
  - Native OTP
  - Federated Authentication Service with Azure active directory
  - OKTA

  ThinOS supports user authentication using third-party authentication applications. ThinOS supports the following third-party authentication types:

  - **Imprivata**—ThinOS supports Imprivata on Citrix, VMware, and Microsoft VDI solutions in both **Imprivata ProveID Embedded** and **ProveID Web API** modes.
  - **Identity Automation**—ThinOS supports RapidIdentity for Healthcare (formerly HealthCast) SSO solution.

  ThinOS supports smart card or certificate-based authentication to authenticate TLS connections to remote hosts.

For more information about multifactor, token, and certificate-based authentication, see the *Dell Wyse ThinOS Version 9.1 Administrator's Guide* at www.dell.com/support.

- **Unauthenticated Interfaces**—Anonymous authentication can be configured from a remote system. Citrix and VMware workspaces support anonymous authentication to remote broker agents and session hosts. However, thin client users can log in to the broker agent and the remote session using a configured username and password.
- **Wyse Management Suite server authentication**—ThinOS device is registered to the Wyse Management Suite server through a valid Group Registration key. ThinOS verifies the Wyse Management Suite server using a TLS server certificate. The Wyse Management Suite server certificate verification is forcibly enabled when the Wyse Management Suite server is configured as a public cloud service. Dell Technologies recommends that you enable the Wyse Management Suite server certificate verification option when using a local Wyse Management Suite server.

User and credential management

- **Local privilege level and administrator mode**—Local UI privilege level can be set to **High**, **Low**, or **Customize**. For more information about account privileges, see Security profiles.

  ThinOS supports the local administrator mode. Use the local Admin Policy Tool or Wyse Management Suite to enable or disable the local administrator mode. User credentials are authenticated on each thin client locally. By default, the administrator mode is disabled. There is no default credential to enter into the local administrator mode. The thin client administrator must specify the username and password to access the administrator mode.

- **VNC shadowing**—ThinOS can be accessed remotely using VNC. VNC service provides user assistance, and is used for remote technical support. The VNC connection is authenticated by each thin client locally. There is no default credential for an account to connect to the VNC service. However, the thin client administrator must enable VNC and set a password using either Wyse Management Suite or the local Admin Policy Tool.
- **BIOS admin credentials**—The default BIOS password is `Fireport`. The thin client administrator can change the BIOS admin password using either Wyse Management Suite or the local Admin Policy Tool. BIOS settings such as boot order and USB port settings are protected by a BIOS password.
- **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.
- **Securing credentials**—All credentials are stored 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.

  All passwords for local ThinOS client 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 and Admin Policy Tool UI only accept 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.

Authorization

- **General authorization settings**—By default, the local UI privilege on ThinOS is set to **High**. Dell Technologies recommends that you set the privilege level to **None** or **Customize** after completing the initial setup of the thin client. ThinOS supports a VNC access with read-only or certain privileges according to the configured settings. By default, VNC is disabled.
- **Remote authorization settings**—Remote resource system administrators can configure the remote resource authorization settings.
- **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.
- **Actions not requiring authorization**—Some of the local system UI including system information dialog box and login dialog box can be accessed without authorization when the privilege level is set as **None**. All local system functionalities including Admin Policy Tool can be accessed when privilege level is set to **High** or when you enable the administrator mode. When the privilege level is set to **Customize**, the thin client administrator can enable or disable the local UI functionalities.

Network security

- **Network exposure**—The following table lists the network ports that are supported on ThinOS.

  Table 1. Network exposure

Service name	Port	TCP or UDP	Summary
`VNCD`	5900	TCP	You can enable or disable the VNC server using Admin Policy Tool or Wyse Management Suite. By default, the option is disabled.
`ntp`	123	UDP	If NTP is not configured, you cannot use the NTP service. You can configure the NTP settings using Admin Policy Tool or Wyse Management Suite.
`syslog`	514	UDP	ThinOS generates service logs. You cannot disable the **syslog** service.
`DNS`	127.0.0.1.53	TCP 4	You cannot disable the DNS service.
`DNS`	0::1.53	TCP 6	You cannot disable the DNS service.
`WMS`	Not available	Not available	Listening port is not available.

  Network vulnerability scanning is performed on ThinOS 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**—ThinOS 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.

  Both access methods must be configured before use.
- **SCEP client settings**— ThinOS supports the following settings:
  - CA certificate hash type, value, and installing the CA certificate after a certificate request. Use the longest hash type for a more secure configuration.
  - SCEPURL and SCEPAdminURL can be configured as http or https. Use https for a more secure configuration.
  - Client certificate RSA key length. Use 4096 instead of 2048 and 1024 for a more secure configuration.
- **Firewall settings**—ThinOS does not support firewall settings.

Data security

System partition, data partition, and swap partition on a ThinOS device are encrypted. Trusted Platform Module (TPM) is used to store keys for encryption or decryption, provided TPM is enabled.

ThinOS does not store any sensitive data. You can export log files from ThinOS with a valid password. All inputs are validated before passing them as parameters to respective scripts.

Cryptography

AES-XTS 128 is used for the disk encryption. TLS 1.1 and 1.2 are used to connect to Citrix, VMware, Windows Virtual Desktop, Amazon WorkSpaces broker agents, and Wyse Management Suite.

Auditing and logging

- **Log management**—Following are the available log levels on ThinOS:
  - Critical
  - Error

    - Info
    - Debug
    - Verbose
- **Log protection**—You must enter a password to export log files.
- **Logging format**—Log file includes `<Type><timestamp><ID>`.
- **Alerting**—Warning logs are displayed on the ThinOS UI as notifications.

Using log files to troubleshoot your thin client

About this task

You can use the troubleshooting options on the ThinOS desktop to troubleshoot your device.

Steps

1. From the desktop menu, click **Troubleshooting**.
   The **Troubleshooting** dialog box is displayed.
2. Click the **General** tab, and do the following:
    - Click the **Extract CMOS** option to extract the CMOS settings and certain BIOS settings to the USB drive or file server based on your target device selection.
    - Click the **Restore CMOS** option to write the CMOS settings and BIOS settings from the USB drive to the target thin client.
    - Click the **Performance Monitor** option to display the CPU usage history with the Memory, and Networking information. The graphs display on top of all windows.
    - Click the **Force Coredump** option to forcibly generate the debug information for technical investigation when your system is not responding. Both the coredump file and the trap information image are saved to the local drive.
      After you restart the thin client, both the coredump file and trap issue screenshot file are uploaded to the `/wnos/troubleshoot/` directory of the file server or a USB drive.
    - Click the **Export System Setting** option to export the system settings file to the USB drive that is connected to the thin client. A password is mandatory for the exported file. The file is stored in the `/wnos/trouble_shoot/` folder of the USB drive.
    - Click the **Export Screenshot** option to export the system screenshots to the USB drive that is connected to the thin client. The file is stored in the root folder of the USB drive.
    - Click the **Export logs** option to export the system log files to the USB drive that is connected to the thin client. The file is stored in the root folder of the USB drive—`system_log_201910107_125610.tgz`.
    - Click the **Import System Setting** option to import the system settings file from the USB drive that is connected to the thin client. The file is stored in the `/wnos/trouble_shoot/` folder of the USB drive.
3. Click the **Capture** tab, and do the following:
    - **Capture Network Packets**—Use this option to capture network-related logs.
        a. Connect a USB drive to the thin client.
        b. To start logging the unexpected error messages, enable the **Capture Network Packets** option, and click **OK**.
        c. To stop logging the unexpected error messages, disable the **Capture Network Packets** option, and click **OK**.
        d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.tgz`.
        e. Extract the `tgz` file. The log files are available at `./var/log/netmng/`.
    - **Capture Wireless Packets**—Use this option to capture wireless network-related logs.
        a. Connect a USB drive to the thin client.
        b. To start logging the unexpected error messages, enable the **Capture Wireless Packets** option, and click **OK**.
        c. To stop logging the unexpected error messages, disable the **Capture Wireless Packets** option, and click **OK**.
        d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.tgz`.
        e. Extract the `tgz` file. The log files are available at `./var/log/netmng/`.
    - **Capture USB Packets**—Use this option to capture USB packets.
        a. Connect a USB drive to the thin client.
        b. To start logging the unexpected error messages, enable the **Capture USB Packets** option, and click **OK**.
        c. To stop logging the unexpected error messages, disable the **Capture USB Packets** option, and click **OK**.
        d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.tgz`.

    e. Extract the `tgz` file. The log files are available at `./compat/linux/var/usbdump/`.

- **Capture User Coredump**—Use this option to capture coredump files.
    a. Connect a USB drive to the thin client.
    b. To start logging the unexpected error messages, enable the **Capture User Coredump** option, and click **OK**.
    c. To stop logging the unexpected error messages, disable the **Capture User Coredump** option, and click **OK**.
    d. Open the **Troubleshooting** window, and click **Export Logs** on the **General** tab. The log file is stored in the root folder of the USB drive—`system_log_201910107_125610.tgz`.
    e. Extract the `tgz` file. The log files are available at `./compat/linux/var/usbdump/`.

4. Click the **Ping** tab, and do the following:
    a. Enter the IP address, DNS-registered hostname, or WINS-registered hostname of the target device.
    b. 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**.

    ⓘ **NOTE:** Not all network equipment responds to ping packets. This is attributed to Denial-of-Service (DoS) attacks. Lack of response does not necessarily indicate that the target of the ping is unusable for other purposes.

5. Click the **Trace Route** tab, and do the following:
    a. Enter the IP address, DNS-registered hostname, or WINS-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 thin client 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 (routers and computers) in the path. The round-trip response time and the identifier information are displayed in the message box.

6. Click the **Telnet** tab, and do the following:
    a. Click **Telnet**.
    b. Enter the hostname.
    c. Enter a port number.
    d. Select a color theme.
    e. Click **Connect** to connect to a remote host or device.
7. Click the **Network** tab, and view detailed information related to your network connection.
    - Click the **Diagnostics** button to run a diagnostic test on your network connection.
    - Click the **Export log** button to export the network logs to the target device.
8. Click **OK** to save your settings.

Code or product integrity

ThinOS enables you to update system packages and install third-party applications on the ThinOS client. All firmware and application packages that are deployed to ThinOS are Dell-signed packages.

You can download the required packages from www.dell.com/support, and deploy the packages to ThinOS using either Wyse Management Suite or the local Admin Policy Tool. Each package that is deployed using Wyse Management Suite or Admin Policy Tool is checked for a valid signature by the ThinOS device. ThinOS discards the package if:

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

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.