Dell ThinOS 10.x App Builder

User Guide

February 2026
Rev. A03

DELL Technologies

Notes, cautions, and warnings

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

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

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

Contents

1

Introduction

App Builder is a ThinOS feature that enables the creation, customization, and deployment of Customer-Installed (CI) application packages. It provides a secure and controlled environment for integrating third-party or custom applications into ThinOS 10.x devices (version 2508 or later). App Builder is available exclusively in Enhanced Mode, which unlocks advanced capabilities such as certificate-based security, application packaging, and extended customization options.

CI packages that are created with App Builder can be deployed using Wyse Management Suite (WMS) or Admin Policy Tool (APT), depending on the management strategy. App Builder supports two deployment modes:

- **Isolated Mode (Recommended)**—Runs applications in a sandboxed environment to ensure system stability and security.
- **Native Mode**—Runs applications directly on the ThinOS operating system. This mode requires whitelisting and is appropriate only for trusted, production-ready applications.

Related Links:

Reference materials and supporting documentation

Topics:

About this guide

This guide provides instructions for:

- Enabling Enhanced Mode and activating App Builder.
- Creating CI application packages using App Builder.
- Deploying and managing CI packages on ThinOS devices using WMS or APT.
- Generating and managing certificates for secure application signing.
- Troubleshooting common issues during packaging and deployment.

Intended audience

This guide is designed for:

- Developers creating and packaging CI applications.
- IT administrators deploying and managing CI applications on ThinOS devices in enterprise environments.

2

App Builder enhancements in ThinOS 10.x 2602

This chapter provides an overview of the new App Builder enhancements that are introduced in ThinOS 10.x 2602, including improved application packaging capabilities, expanded configuration options, streamlined deployment workflows, and additional controls for Customer Installed (CI) application behavior and visibility.

It includes:

- Auto-Launch CI applications—Enables Customer Installed (CI) applications to automatically launch at system startup through WMS or APT configuration.
- Support for environment variables—Supports defining app-specific environment variables that remain isolated from system-level variables.
- Export application logs—Provides symbolic link–based log access, allowing export and troubleshooting of application logs.
- Configuration file support for Isolated Mode Apps—Allows uploading and deploying application configuration files for isolated-mode CI apps.
- Access apps from VDI Menu before login—Shows Customer Installed (CI) application icons before login when enabled in WMS or APT, allowing pre-session app visibility.

Topics:

Auto-launch Customer Installed (CI) application

Describes how administrators can configure CI applications in ThinOS 10.x to start automatically at boot using WMS or APT, based on desktop file configuration.

About this task

After configuration, ThinOS 10.x launches the specified Customer Installed (CI) application automatically at every startup or reboot. The application is performed using its associated `.desktop` file, and the auto-launch behavior remains consistent across reboots and software updates.

Steps

1. To configure the auto-launch Customer Installed (CI) application feature, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Desktop Mode** > **System Operating Mode**.
3. Enable **Enhanced Mode** and **App Builder Mode**, then click **Save & Publish**.
4. Open **App Builder** from the taskbar.
5. Select **Isolated Mode** or **Native Mode**, enter the application **Name** and **Version**, and upload the required `.deb` packages. For more information, see Application packaging using Dell App Builder.
6. Select the correct binary path or enter it manually.
7. Click **Next** and review dependency check results.
8. Click **Build** after validation completes.
9. When the build finishes, click **Preview**, verify the UI, and exit.

10. Upload the required `.pem` certificate.
11. Click **Bundle**, then click **Save** (the `.pkg` file is saved to USB).
12. Deploy and select the generated `.pkg` file using WMS or APT.
    For more information, see Deploying CI application packages.
13. Add the application name under **CI Application Configuration** > **CI Apps Auto Launch List**.
14. Click **Save & Publish**, and reboot the device after installation completes.

Results

The configured Customer Installed (CI) application launches automatically at every ThinOS startup.

Configure environment variable handling for CI applications

Explains how to define application-specific environment variables for CI applications in ThinOS 10.x using WMS or APT, ensuring application settings remain isolated from system-level environment variables.

About this task

Custom environment variables are applied only to the targeted application at runtime. System-critical environment variables remain protected, ensuring operating system stability while allowing applications to use their own configurations.

Steps

1. To configure custom environment variables, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Desktop Mode** > **CI Application Configuration** > **Add Row** > **Environment Variables**.
3. Click **Save & Publish**.
4. Build and launch the CI application.
   For more information, see Application packaging using Dell App Builder.

Results

The application uses its defined environment variables without affecting system-wide settings.

Export application logs

Explains how ThinOS 10.x enables exporting CI application logs by creating a symbolic link in /var/log that points to the application's internal log directory.

About this task

ThinOS generates a soft link in `/var/log`, allowing IT administrators to discover, export, and troubleshoot application logs without duplicating files across directories.

Steps

1. To export application logs , do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Desktop Mode** > **CI Application Configuration** > **Add Row**.
3. In **CI application 1**, provide the **App Name** and **Log Path**.
4. Upload the **.pkg** file in WMS or APT.
   For more information, see Deploying CI application packages.

5. Install and launch the CI application.

Results

Application logs are accessible through `/var/log` using the generated symbolic link.

Configure configuration file support for Isolated Mode applications

Explains how to upload and attach configuration files to isolated-mode CI applications in ThinOS 10.x, enabling controlled application behavior using WMS, or APT.

About this task

After configuration, the specified configuration file is bundled with the application and deployed to the correct destination path during installation.

Steps

1. To upload configuration files to isolated-mode CI applications, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Desktop Mode** > **CI Application Configuration** > **Upload Configuration**.
3. Upload and select the application configuration file.
4. Add a row under CI application.
5. Enter **App Name**, **Destination Path**, and optionally define **App Capability**.
6. Click **Save & Publish**.
7. Launch the application and verify that the configuration file is present in the expected folder and functioning.

Results

The configuration file is deployed correctly and applied when the application runs.

Configure application visibility in the VDI Menu before login

Explains how to configure ThinOS 10.x so that CI applications appear in the VDI Menu before user login when the Show Apps Before Login option is enabled using WMS or APT.

About this task

After you enable this option and reboot the device, all installed CI application icons are visible on the ThinOS login screen VDI Menu. This allows administrators to preview available applications without establishing a remote session.

Steps

1. To upload configuration files to isolated-mode CI applications, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Desktop Mode** > **System Operating Mode**.
3. Enable **Enhanced Mode** and **App Builder Mode**, then click **Save & Publish**.
4. Open **App Builder** from the taskbar.
5. Select **Isolated Mode** or **Native Mode**, enter the application **Name** and **Version**, and upload the required `.deb` packages. For more information, see Application packaging using Dell App Builder.

6. Select the correct binary path or enter it manually.
7. Click **Next** and review dependency check results.
8. Click **Build** after validation completes.
9. When the build finishes, click **Preview**, verify the UI, and exit.
10. Upload the required `.pem` certificate.
11. Click **Bundle**, then click **Save** (the `.pkg` file is saved to USB).
12. Deploy and select the generated `.pkg` file using WMS or APT.
    For more information, see Deploying CI application packages.
13. Go to **System Operating Mode** > **Others**.
14. Enable **Show Apps Before Login**.
15. Click **Save & Publish**, and reboot the device after installation completes.

Results

CI application icons appear in the VDI Menu before login when the device restarts.

3

Getting started with App Builder

To begin, enable the Enhanced Mode and install the required packages—CI Software Enabler and App Builder—using WMS or APT. Once activated, App Builder is available for CI application packaging.

Before proceeding with packaging and deployment, ensure that the environment is properly configured by reviewing the following:

- Operating modes
- System prerequisites
- Role-based responsibilities

Topics:

Key concepts and terminology

Learn essential terms that are related to ThinOS application packaging and deployment. It covers operating modes, tools, and components such as ThinOS, Enhanced Mode, Appliance Mode, CI Applications, CI Apps Onboarding, App Builder, WMS, and APT, providing a quick reference for understanding the environment setup.

Table 1. Key concepts and terminology

Term	Definition
ThinOS	Dell lightweight operating system for thin clients.
Enhanced Mode	A privileged ThinOS mode that enables App Builder, CI app support, and certificate-based security.
Appliance Mode	The default ThinOS mode is optimized for security but does not support CI applications.
Customer-Installed (CI) Application	A third-party or custom app that is packaged for ThinOS using `.deb` files or App Builder.
CI Apps Onboarding	Third-party or custom `.deb`-based application that is packaged for ThinOS that must be onboarded by Dell to run in Native Mode. CI Apps Onboarding is the required package that enables such applications to be created, allowlisted, and performed in Native Mode. Any application that is intended for Native Mode must be onboarded by Dell in advance, and once onboarding is complete, installing the CI Apps Onboarding package is sufficient to enable the application to run on ThinOS.
App Builder	A ThinOS feature for creating secure, deployable CI application packages. App Builder supports the following deployment modes: • Isolated Mode—Runs apps in a secure, containerized environment. Prevents conflicts with ThinOS base OS. • Native Mode—Runs apps directly on ThinOS OS with full system access. Higher risk of dependency conflicts and security exposure.
WMS (Wyse Management Suite)	Dell centralized management tool for ThinOS devices.

Table 1. Key concepts and terminology (continued)

Term	Definition
APT (Admin Policy Tool)	A local configuration tool for ThinOS devices.

Understanding ThinOS operating modes

Switch between Appliance and Enhanced Mode in ThinOS to unlock advanced features like App Builder and CI app support.

ThinOS 10.x supports two operating modes:

- Appliance Mode (Default)
  - Optimized for maximum security and system integrity.
  - Does not support CI application deployment.
- Enhanced Mode
  - Unlocks advanced features such as:
    - App Builder
    - CI application support
    - Certificate-based security
  - Must be enabled before packaging or deploying CI applications.

System requirements for App Builder

Check ThinOS version, WMS compatibility, and hardware specs to ensure successful installation and use of App Builder.

Before using App Builder, ensure the following:

- ThinOS version—10.x 2508 (10.0127) or later
- Wyse Management Suite (WMS)—Version 5.3 or later
- Hardware—Devices with at least 4 GB RAM and 32 GB secondary storage
- WMS Setup—Group token that is created and a device that is registered in WMS

Roles and responsibilities in CI application deployment

Dell App Builder supports a role-based workflow for secure and efficient CI application deployment on ThinOS devices. Each role contributes to different stages of the application life cycle.

Table 2. Roles and responsibilities in CI application deployment

Role	Responsibilities
Developer	• Prepare application files (.deb or custom). • Use App Builder to package and configure. • Test the application on Ubuntu 24.04 before packaging.
IT Administrator	• Enable Enhanced Mode on ThinOS devices. • Upload required packages using WMS or APT. • Enable App Builder Mode on ThinOS devices. • Use App Builder to package and configure. • Deploy applications and verify installation.

4

Environment setup for CI application deployment

Before deploying CI applications on ThinOS devices, you must prepare the environment by enabling Enhanced Mode, installing the required packages, and activating App Builder.

Topics:

Enable Enhanced Mode

By default, Dell ThinOS operates in **Appliance Mode** to provide the highest level of security. **Enhanced Mode** is a privileged operating mode in ThinOS 10.x that enables access to advanced features such as the App Builder and supports the installation and execution of Customer Installed (CI) or custom applications.

Steps

1. To enable **Enhanced Mode** on the device, use any of the following methods:
   - Using WMS:
     a. Log in to WMS as an administrator.
     b. Go to **Groups & Configs** and select a group.
     c. Go to **Edit Policies** > **ThinOS10.x** > **Advanced** > **Desktop Mode**, and click **System Operating Mode**.
   - Using Admin Policy Tool:
     a. Open APT on the device.
     b. Go to **Advanced** > **Desktop Mode**, and click **System Operating Mode**.
2. Click **Enable Enhanced Mode**.

   NOTE: Enhanced Mode reduces overall system security. Use it only in trusted or controlled environments.

   For more information about **Enhanced Mode** and **Appliance Mode**, see *Dell ThinOS 10.x 2502,, 2505, and 2508 Administrator's Guide* at Support | Dell.

   For more information about disabling the **Enhanced Mode**, see Disable Enhance Mode.

Installing CI Software Enabler, CI Apps Onboarding, and App Builder packages

Explains how to install the CI Software Enabler, CI Apps Onboarding, and App Builder packages on ThinOS devices. The CI Software Enabler and CI Apps Onboarding package enables the installation and functionality of Customer Installed (CI) applications when Enhanced Mode is enabled, while the App Builder is used to create, customize, and package CI applications for deployment.

Install CI Software Enabler and CI Apps Onboarding package using WMS or APT

CI Software Enabler and CI Apps Onboarding package allows the installation and execution of Customer Installed (CI) applications on ThinOS devices when Enhanced Mode is enabled. Explains how to install the CI Software Enabler package using WMS or APT on the ThinOS device.

Prerequisites

- ThinOS 10.x 2508 (10.0127) or later version must be running on your device.
- A group must be created in Wyse Management Suite with a group token.
- The device must be registered to Wyse Management Suite.

Steps

1. Download the **CI Software Enabler** and **CI Apps Onboarding** package from Support | Dell.
2. Upload the **CI Software Enabler** and **CI Apps Onboarding** package using any of the following methods:
   - Using WMS:
     a. Log in to WMS as an administrator.
     b. Go to **Groups & Configs** and select a group.
     c. Go to **Edit Policies** > **ThinOS10.x**, and click **Standard**.
   - Using Admin Policy Tool:
     a. Open APT on the device.
     b. Click **Standard**.
3. From the **Standard** menu, expand **Firmware**.

   NOTE: If you cannot locate the **Application Package Updates** option under the **Standard** tab, use the **Advanced** tab.

4. Click **Application Package Updates**.
5. Click **Browse** and select the CI Software Enabler and CI Apps Onboarding package to upload.
6. Ensure the switch option of **Application Package Updates** is set to **Install** under the **Dell** category.
7. Expand the **Dell** dropdown list, and select the uploaded package.
8. Click **Save & Publish**.
   The device downloads the package, installs it, and then restarts.

Install the App Builder package using WMS or APT

The App Builder package can be installed on ThinOS devices using Wyse Management Suite (WMS) or Admin Policy Tool (APT). Once installed, the package enables administrators to create, customize, and package Customer Installed (CI) applications for deployment. App Builder works in Enhanced Mode, allowing organizations to tailor applications to specific requirements and deliver them efficiently across ThinOS environments.

Prerequisites

- ThinOS 10.x 2508 (10.0127) or later version must be running on your device.
- A group must be created in Wyse Management Suite with a group token.
- The device must be registered to Wyse Management Suite.
- The CI Software Enabler package must be installed.

Steps

1. Download the App Builder package from Support | Dell.
2. Upload the App Builder package using any of the following methods:
   - Using WMS:
     a. Log in to WMS as an administrator.
     b. Go to **Groups & Configs** and select a group.
     c. Go to **Edit Policies** > **ThinOS10.x**, and click **Standard**.
   - Using Admin Policy Tool:

a. Open APT on the device.
b. Click **Standard**.

3. From the **Standard** menu, expand **Firmware**.

   NOTE: If you cannot locate the **Application Package Updates** option under the **Standard** tab, use the **Advanced** tab.

4. Click **Application Package Updates**.
5. Click **Browse** and select the App Builder package that you want to upload.
6. Ensure the switch option of **Application Package Updates** is set to **Install** under the **Dell** category.
7. Expand the **Dell** dropdown list, and select the uploaded package.
8. Click **Save & Publish**.
   The device downloads the package, installs it, and then restarts.

Enable App Builder

To activate the App Builder package on ThinOS devices, install it using Wyse Management Suite (WMS) or Admin Policy Tool (APT). After the package is activated, you can select the appropriate deployment mode to create, customize, and package Customer Installed (CI) applications for deployment.

Prerequisites

Ensure that you have enabled the **Enhanced Mode** using WMS or APT. For more information about enabling Enhanced Mode, see Enable Enhanced Mode.

Steps

1. Enable **App Builder** using any of the following methods:
   - Using WMS:
     a. Log in to WMS as an administrator.
     b. Go to **Groups & Configs** and select a group.
     c. Go to **Edit Policies** > **ThinOS10.x** > **Advanced** > **Desktop Mode**, and click **System Operating Mode**.
   - Using Admin Policy Tool:
     a. Open APT on the device.
     b. Go to **Advanced** > **Desktop Mode**, and click **System Operating Mode**.
2. Enable **App Builder**.
   After successful installation, the App Builder icon appears on the ThinOS taskbar of the endpoint device.

   NOTE: It is recommended to use **Isolated Mode** for app deployment, as **Native Mode** may make the system vulnerable and cause existing applications to malfunction due to conflicting libraries.

5

Application packaging using Dell App Builder

Dell App Builder enables you to create Customer-Installed (CI) application packages for ThinOS devices. These packages include application binaries, metadata, dependencies, and permissions, ensuring secure and consistent deployment.

Topics:

Packaging prerequisites

Ensure that all system, application, and environment prerequisites are met before creating CI application packages. This includes ThinOS version, WMS compatibility, hardware specifications, and required packages.

- ThinOS 10.x 2508 (10.0127) or later.
- Wyse Management Suite (WMS) 5.3 or later.
- Enhanced Mode is enabled.
- CI Software Enabler, CI Apps Onboarding, and App Builder packages installed.
- App Builder is enabled.
- Minimum recommended requirement is 8 GB RAM and 64 GB storage.
- Select an Ubuntu 24.04 (x86_64) compatible third-party application that includes a Debian installation package and meets all licensing requirements.
- It is recommended to test the application on Ubuntu 24.04 before packaging.
- Verify the allowed CI application package details before packaging. For more information, see Customer Installed (CI) application package details.

Deployment modes

App Builder supports two deployment modes for CI applications. Each mode determines how the application interacts with the ThinOS operating system and impacts security and stability.

Table 3. Supported deployment modes

Mode	Description	Recommended Use
Isolated Mode	Runs apps in a secure, containerized environment. Prevents conflicts with ThinOS base OS.	The default choice for most deployments. Enhances security and stability.
Native Mode	Runs apps directly on ThinOS OS with full system access. Higher risk of dependency conflicts and security exposure.	Only for trusted, production-ready apps. Requires `.deb` packages to be added to the Native Mode allowlist. Here is an example of how to add an application to the allowlist using ThinOS App Builder.

NOTE: It is recommended using **Isolated Mode** for app deployment to avoid system vulnerabilities or library conflicts.

NOTE: Previewing or building native applications directly impacts the underlying operating system. Use these features with caution, as any misconfiguration or error may affect OS stability or functionality.

Create CI application packages

Build CI application packages by adding app details, resolving dependencies, setting permissions, previewing builds, and signing for deployment.

Steps

1. Open **App Builder** from the ThinOS taskbar of the endpoint device.
2. In **Files & details** tab:
   a. Go to **Application Deployment Mode**, and select **Isolated** mode.
   b. Enter the required inputs:
      - **Application Name**: Enter the application name.

        NOTE: Do not rename the application name. If you rename it, ensure that you close App Builder and repeat the process again.

      - **Version**: Enter the version.
      - **Debian Packages**: Upload the supported `.deb` files that are downloaded from trusted sources using USB device.
      - **Executable Path**: Enter the binary path to launch the app (For example: `/usr/bin/<appname>`). This field is autopopulated if the binary is detected, but you can also manually specify a custom path if needed.
      - **App Icon**: Upload the required icon for the application. Supported file types: .png, .jpg, .jpeg, and .ico.

      NOTE: To find the executable binary path from a `.deb` file, run `dpkg -c <appname>.deb` and to list only file paths, run `dpkg -c <appname>.deb | awk '{print $6}'`. You can use the output paths `/usr/bin/appname` to identify the executable binary path for launching the application. Alternatively, unpack the `.deb` file and check the `.desktop` file to locate the binary path.
3. Click **Next**.
4. In the **Dependencies** tab, verify the details.

   NOTE: A listed missing dependency may not indicate that the file is absent, it can result from a name or version mismatch with the expected dependency.

   NOTE: Dependencies are categorized as **Available** (already on the ThinOS client), **Downloadable** (from Ubuntu repositories), and **Missing (Custom)** (must be manually uploaded by returning to Step 1).

   NOTE: You can view the dependency report and download the log and report using the **Save Report** button.
5. Click **Next**.
6. In **Permissions** tab, upload a configuration file type `.txt`, `.ini`, `.config`,`.properties`, `.cfg`, or `.conf`, and set application-level permissions.
   Modify the permission as per your requirement.
   - USB Access: Enable/Disable
   - Webcam: Enable/Disable
   - Network: Configuration
   - Microphone: Enable/Disable
   - Printing: Enable/Disable
   - Bluetooth: Enable/Disable
   - Persistent Storage

   NOTE: In Isolated Mode, peripherals must be manually enabled or disabled, whereas in Native Mode, they are automatically allowed to access it.
7. Click **Next**.
8. In **Preview** tab, you can verify the build process and validate the application.
9. Launch the application and verify it by validating peripheral access configurations.
   Once the build process begins, the admin or user can monitor the logs, and a report is generated automatically upon completion.

   NOTE: In **Isolated Mode**, if you encounter issues with peripherals during application preview (such as webcam or audio access), return to **Step 3** and enable the required access by selecting the appropriate checkboxes.
10. Click **Exit Preview**, and then click **Next**.
11. In **Bundle** tab, click **Browse File(s)** to add the signed certificate. Supported file type: `.pem`.

NOTE: You can upload an existing certificate if you have already generated one.

12. Click **Bundle & Sign**.
    Once **Bundle and Sign** is complete, you can save the created application package and either upload it using WMS or APT, or copy it to a USB.
13. Click **Save Application**.
    The application is saved successfully and moved to USB successfully. To upload the application package to WMS or APT, see Upload package using WMS or APT.

    NOTE: Save the application before closing the App Builder to prevent loss of any unsaved changes.

    For more information about enabling Auto-launch CI application and Show Apps Before Login, see Auto-Launch CI applications and Application visibility before login in to the VDI Menu.

6

Deploying CI application packages

You can deploy CI application packages to ThinOS devices using Wyse Management Suite (WMS) or Admin Policy Tool (APT). Deployment ensures secure and consistent delivery of applications across managed devices.

Topics:

Deploy CI application package using WMS or APT

You can deploy a Customer Installed (CI) application package that is created using App Builder to ThinOS devices using WMS or APT.

Prerequisites

- Enable Enhance Mode.
- Install the CI Software Enabler package.
- Test the CI application on Ubuntu standalone Ubuntu setup before packaging.

Steps

1. To upload the **CI Certificate** of the CI application package created using App Builder, use any of the following methods:
   - Using WMS:
     a. Log in to WMS as an administrator.
     b. Go to **Groups & Configs** and select a group.
     c. Go to **Edit Policies** > **ThinOS10.x** > **Advanced** > **Desktop Mode** > **CI Certificates**, and click **Import CI Certificate**.
   - Using Admin Policy Tool:
     a. Open APT on the device.
     b. Go to **Advanced** > **Desktop Mode** > **CI Certificates**, and click **Import CI Certificate**.
2. Click **Browse** and select the corresponding public certificate for the CI application package.
3. Click **Save & Publish**.
4. Go to **Configuration Control | ThinOS** > **Advanced** > **Firmware** > **Application Package Updates**.
5. Click **Browse** and upload the customer installed (CI) application package.
   The EULA and vendor details are displayed.
6. Verify the vendor names and license agreement and then click **Accept** to upload the package.
   Once the package is uploaded, it appears under the **Customer Apps** section.
7. Go to **Customer Apps** > **App Builder packages** section and select the application package.
8. Click **Save & Publish**.
   The device reboots, and an application icon is added to the apps list for quick access and launch.

   NOTE: CI Software Enabler is not required for Native Mode applications.

7

How to build and Allowlist an Onboarded CI Application using ThinOS App Builder

This section outlines how to add a Customer Installed (CI) application to the allowlist in ThinOS Native Mode using ThinOS App Builder. The FabulaTech USB for Remote Desktop plugin is used as an example to demonstrate the process of enabling Enhanced Mode, packaging the `.deb` file, generating the CI package, and allowlisting it so it can run on the ThinOS client. The same workflow applies to any third-party CI application.

Steps

1. To install FabulaTech USB plugin as Customer Installed (CI) application into ThinOS devices, do any of the following:
   - Log in to WMS as an administrator, go to **Groups & Configs**, select a group, click **Edit Policies**, and go to **ThinOS10.x** > **Advanced**.
   - Open APT on the device and select **Advanced**.
2. Go to **Desktop Mode** > **System Operating Mode**.
3. Enable **Enhanced Mode** and **App Builder Mode**, then click **Save & Publish**.
   NOTE: Ensure that the Enhanced Mode is enabled first, and then proceed to install the required packages and activate the App Builder-generated package. For more information, see Environment setup for CI application deployment.
4. Open **App Builder** from the taskbar.
5. Select **Native Mode**, enter the application **Name** and **Version**, and upload the required `.deb` packages.
   For more information, see Application packaging using Dell App Builder.
6. Select the correct binary path or enter it manually.
7. Click **Next** and review dependency check results.
8. Click **Build** after validation completes.
9. When the build finishes, click **Preview**, verify the UI, and exit.
10. Upload the required `.pem` certificate.
11. Click **Bundle**, then click **Save** (the `.pkg` file is saved to USB).
12. Deploy and select the generated `.pkg` file using WMS or APT.
    For more information, see Deploying CI application packages.
13. Configure the FabulaTech USB for Remote Desktop Integration with ThinOS 10.x.
    For more information, see FabulaTech USB for Remote Desktop Integration with ThinOS 10.x.

Results

The device reboots, and the FabulaTech CI Software icon is added to the apps list for quick access and launch.

8

Uninstalling Packages

Explains how to remove CI application packages from ThinOS devices using the Admin Policy Tool (APT) for local removal or Wyse Management Suite (WMS) for centralized management.

Topics:

Uninstall CI application package in client device

This topic explains how to uninstall the customer installed (CI) application package from the ThinOS device.

Steps

1. Open **Settings** on the device.
2. Go to **System Tools**.
3. Go to **Packages** tab.
   This section lists all installed packages on the device.
4. Select the customer installed (CI) application package that you want to uninstall.
5. Select the customer installed (CI) application package, and click **Delete**.

Uninstall CI application package using WMS

This topic explains how to uninstall the customer installed (CI) application package from the ThinOS device using Wyse Management Suite (WMS).

Prerequisites

- Register the device to WMS.
- Create a group in WMS with a group token.

Steps

1. Go to the **Groups & Configs** page, and select the target group.
2. From the **Edit Policies** drop-down menu, click **ThinOS 10.x**.
   The **Configuration Control | ThinOS** window is displayed.
3. In the left pane, click **Standard**.

   NOTE: If you cannot locate the Application Package option under the **Standard** tab, use the **Advanced** tab.

4. From the **Standard** menu, expand **Firmware**, and click **Application Package Updates**.
5. Select the customer installed (CI) application package that you want to uninstall.
6. For the customer installed(CI) application package, ensure that the switch is set to **UNINSTALL**. You can select only one version in the list for each category.
7. Click **Save & Publish**.

9

Certificate management for CI application signing

This chapter explains how to generate an SSL certificate and private key for customer installed (CI) application packages, which are required for creating and deploying customer installed (CI) application packages.

Topics:

Generating Certificates on Windows Using IIS

This topic outlines the steps to generate a Certificate Signing Request (CSR) and private key using Internet Information Services (IIS) on Windows.

Steps

1. Generate a CSR and Private key using IIS on Windows.
2. Extract Certificate and Private key from a `.pfx` file using OpenSSL.

   NOTE: A `.pfx` (PKCS#12) file contains both a private key and public key.
3. Extract the Public Certificate:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out public_key.crt
   ```

   - `-in <filename.pfx>`: Specifies the input PFX file.
   - `-clcerts`: Extracts only the client certificate (excludes CA certificates).
   - `-nokeys`: Excludes the private key.
   - `-out public_key.crt`: Output file for the public key.
4. Extract the Private Key:

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out private_key.pem
   ```

   - `-nocerts`: Excludes all certificates, extracts only the private key.
   - `-nodes`: Outputs the private key-in plain text (not encrypted).
   - `-out private_key.pem`: Output the file for the private key.

   The private key is stored in plain text. Handle and store securely.
5. After running the commands, you obtain:
   - **public_cert.crt**–the public key certificate.
   - **private_key.pem**–the private key in PEM format.

   These files are used to create customer installed (CI) application packages.

Generating certificates manually on Ubuntu 24.04 for Managed Clients using OpenSSL

This sections explains how to manually generate an RSA private key and a self-signed certificate on Dell client devices with Ubuntu 24.04 for Managed Clients.

Prerequisites

Ensure that the following requirements are met:

- System requirements: OpenSSL package installed.
- Permissions: User account with sudo privileges.
- Information needed:
  - Common Name (CN) for the certificate (for example, domain name).
  - Wanted certificate validity period (in days).
- Security considerations: Choose a secure location for storing your private key and certificate.

Steps

1. Open **Terminal**.
2. Run the OpenSSL command to generate the Private Key:

```
openssl genpkey -algorithm RSA -out "$PRIVATE_KEY" -pkeyopt rsa_keygen_bits:3072
```

3. Run the OpenSSL command to generate a Self-Signed Certificate:

```
openssl req -new -x509 -key "$PRIVATE_KEY" -out "$PUBLIC_CERT" -days "$VALIDITY_DAYS"
-subj "/CN=$COMMON_NAME"
```

4. Verifying the Certificate and Key:

```
openssl dgst -verify "$PUBLIC_KEY_PATH" -keyform PEM -sha256
```

NOTE: Replace the environment variables `$PRIVATE_KEY`, `$PUBLIC_CERT`, `$VALIDITY_DAYS`, `$COMMON_NAME`, `$PUBLIC_KEY_PATH` with values before running the commands.

10

Frequently Asked Questions

What are the prerequisites before using App Builder?

- Enable Enhanced Mode on ThinOS.
- Install CI Software Enabler and App Builder packages.
- Ensure that the device meets system requirements (ThinOS 10.x 2508+, WMS 5.3 or later, 4 GB RAM, 32 GB storage

How can I prevent runtime conflicts caused by dependencies?

- Avoid multiple versions of the same dependency.
- Avoid multiple versions of the same dependency.
- Use Isolated Mode to minimize dependency-related issues.

What should I do if the App Builder shows missing dependencies in the Dependencies tab?

- Check if the dependency is already present but mismatched in version.
- Reupload the correct version of the missing dependency.
- Use the Dependency Report in App Builder to identify and resolve issues.

How can I avoid binary path detection errors?

- Maintain a consistent folder structure for application files.
- Verify the autofilled executable path in App Builder.
- If incorrect, manually specify the correct path (for example, /usr/bin/<appname>).

How can I ensure my app installs successfully without certificate issues?

- Use a valid, nonexpired certificate for signing.
- Verify certificate integrity before bundling.
- If the certificate is expired, regenerate and resign the package.

What should I do if my build fails silently?

- Check logs in the Preview and Build Report tabs for error details.
- Resolve any dependency or permission errors that are indicated in the logs.
- Rerun the build after fixing issues.

Why is my application failing to run after deployment?

- Common causes:
  - Conflicting libraries in Native Mode.
  - Missing permissions for peripherals.
- Recommended actions:
  - Use Isolated Mode for better stability.
  - Reconfigure permissions in App Builder and redeploy.

11

Appendix

Topics:

Disable Enhance Mode

This topic outlines the process of disabling Enhanced Mode to restore ThinOS to its default secured Appliance Mode for maximum security.

Reset methods

- **Hard Reset**
  - Performs a complete system wipe and restores the device using the factory recovery image (similar to BIOS-level recovery).
  - Recommended when returning devices to production or decommissioning.
- **Soft Reset**
  - Removes only Customer-Installed (CI) applications while retaining system settings and user configurations.
  - Recommended when removing CI applications but preserving existing configurations and policies.

NOTE: Use **Hard Reset** when returning devices to production or decommissioning to ensure a clean, secure state. By default, **Soft Reset** is enabled. If WMS groups are switched, a **Soft Reset** of the devices occurs. Use **Soft Reset** when removing CI applications but preserving existing configurations and policies.

Customer Installed (CI) application package details

Outlines the supported CI applications for ThinOS 10.x, including version details, allowlist status, package names, and checksum information.

Table 4. Native Mode—allowed CI application packages for ThinOS 10.x

CI application	Version	Allowlist status	Package details (file name—SHA256)
AuthX	43.4	Allowed	authx-authenticator_dell_43.4.deb— 12cfdb8f90bc82bd83c788da4d8459842219ceb44fcc770483c5a251 03352511f96dd2b715851fa52c972d0f21a7c2d2
	2.3.0		Authx-Secure_dell_2.3.0.deb — cd08919c9505174e81b9b0e95acdfa8bf109ffdb6a9fc78b7014e2e27 84df1b83f9116cc02e103bc24beecb69e4e27e4
Avaya agent	2.0.6.26.3001	Allowed	avaya-agent_2.0.6.26.3001_amd64.deb— 43d45753a3eaf00dd465ca902ef05d27dbf64faa4701146cc3af79a0a 9b70ca5ef083e155bfa7d7ae5a5094a9f73813e
Dizzion Client	7.9.4	Allowed	frame_7.9.4_amd64.deb— 188f2cfa80a2ba757febc3689f23cf4ebdce4144c9f5474f5b230616e 6102edf6c0b80aab77973719419ab588ee6ef70
	7.9.8		frame_7.9.8_amd64.deb— 66d450a124596546e3ed3d29b632d21fc70d8ba39da40c73aba9454 2e54cad2f81567eb4467c893a63ae6904df047391

Table 4. Native Mode—allowed CI application packages for ThinOS 10.x (continued)

CI application	Version	Allowlist status	Package details (file name—SHA256)
FabulaTech	• ftplugins:4.2.0.3 • ftplugins:4.2.0.7 • Ftusbrdp:6.2.2.2 • ftscan:3.8.4.1	Allowed	• ftplugins-4.2.0.3-amd64.deb—1918dc485e5673586bc7aa7c5d43f3cb3e2bf77cdfd9c3deb59cc91bc90a60e1de954cd58a7cbc975eeb4595ba230b17 • ftplugins-4.2.0.7-amd64.deb—2db46af52548e732b80cdab8e06e436b0fcc40948c966aa296e88d69c0c19c389b64efaab642f9881a69df677e40aaba • ftusbrdp-6.2.2.2-amd64.deb—50759ff3176119cf21606e353636dfc88a8579cb922f907ea2c08634668f94c2e213be068c3324db52f7ee2cc63e9ed2 • ftscan-3.8.4.1-amd64.deb—7e842e59b522430b5fef28ce17ab2ef853384929eca4530eac3827c435ef6d0355bd0d3e6c59121a89a0f618a1f8edb0
Crowdstrike	1.0.1	Allowed	falconcid-1.0.1.deb—b51329a39cd061bf74c0017235ce119d565c822abc313d8767286db01dceb16af60a26233bff5859ee36af7de1fe4ff9
	7.30.0-18306	Allowed	falcon-sensor-7.30.0-18306_amd64.deb—2472f6880426c3d8170902e7edd17c448ffa21c2156696a289615dcf775fc43112288753b0f2438cbcfe24798728067c
IDMelon	1.0.0.8	Allowed	IDmelonVDIAgent-all-1.0.0.8.deb—2343c9eb689f542491b6b5d7bf6f0b3db626b2871504d4f0da86a1159961679b13d94d656790608342e9fc48cdbcb35c
	1.0.0.10		IDmelonVDIAgent-all-1.0.0.10.deb—7aba3312ac9450f6fce7a9c62d20f42d6b9c2bc053d49230fc52191e5541647a8a8f64393f5b6d01d0b94ed7f1cf8242
	1.0.0.23		IDmelonVDIAgent-all-1.0.0.23.deb—ba7b62977c4f8b1cb73154a39585cf5fdfe30d1ba68adc31c1bdf139072316405f7de7bb035f5f68ae3ed228cc3b8402
HP Anywhere (PCoIP)	25.03.3-22.04	Allowed	• pcoip-client_25.03.3-22.04_amd64.deb—a41c4663fd3e7468277b03b123aebaebb0929bce89159f0ad2e13f1bac2316a107a805c15344d987991a2171faefb0fd • pcoip-client_25.03.2-22.04_amd64.deb—c6dc6dd471216a5e19b3a06476b1c9bcf0d2ac22ff7befe3d6d6d2eb38ac70e38610c033e0a60d82bf52490710e19cca
Parallel RAS	20.2.25997	Allowed	RASClient20.2.25997_x86_64.deb—e7f251688de53c7db4d9038d07847453eebfad29978a6bee03be85b13689a399c87b6d4e98aa7622b8a4360de8fc9be9
Thales SDK	5.2.2	Allowed	Thales-SDK-5-2-2.deb—a3bc10b567025a7df6e5d90d99291506fa5e87d84779e9652f08857cbec71122510d7c402304ea61821092326b295c12
Printer logic (Accession Health)	25.2.0.51	Partially allowed	printerinstallerclient_amd64.deb—e7a9fa3dcfe0a75f5206cc83b142ad2e349f830f3ec85b434c4fb0f66751e5b49cf6698f55f6ced40d2c12250012eafe

FabulaTech USB for Remote Desktop Integration with ThinOS 10.x

This section explains how to configure FabulaTech USB for Remote Desktop on ThinOS 10.x endpoints and supported VDI environments. The FabulaTech USB for Remote Desktop Plugin must be installed on the ThinOS 10.x client, and the server component must be installed inside the VDI session to enable end-to-end USB device redirection.

Configuring FabulaTech USB with ThinOS client

Describes how to prepare ThinOS endpoints by installing the FabulaTech USB redirection plugin using the ThinOS 10.x App Builder and deploying it using WMS or APT.

Steps

1. Download the latest FabulaTech Plugin package version 4.2.0.7 from the FabulaTech official website.
2. Use the ThinOS App Builder to convert the downloaded `.deb` installer into a ThinOS-compatible CI software package.
   For more information, see Create CI application packages.
3. Deploy the generated CI software package through WMS or the APT.
   For more information, see Deploy CI application package using WMS or APT.

Results

Once installation completes, the FabulaTech CI Software icon appears in the ThinOS VDI Menu.

Configuring FabulaTech with VDI sessions

This chapter outlines how to install and configure the FabulaTech USB for Remote Desktop server component inside VDI sessions (Citrix, Horizon, AVD).

Configure Citrix session

Expains how to enable USB redirection inside Citrix VDI sessions using FabulaTech's server software.

Steps

1. Install the USB for Remote Desktop (Server) component inside the Citrix session.
2. Reboot the Citrix VDI session.

Results

After the reboot, the FabulaTech USB redirection icon appears in the system tray, indicating successful installation.

Configure Omnissa Horizon

Explains how to enable it using a registry change as FabulaTech redirection is disabled by default in Omnissa Horizon session.

Steps

1. Install the USB for Remote Desktop (Server) component inside the Horizon session.
2. Open **Registry Editor** (regedit).
3. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\FabulaTech\Netlink 3`.
4. Create a new **DWORD** entry named rdpvcbridge.
5. Set the value to **1** to enable redirection.
6. Restart the **FabulaTech Netlink 3 Supervisor** service or reboot the server.

Results

After the restart, the FabulaTech USB redirection icon appears in the system tray.

Configure Azure Virtual Desktop (AVD)

Explains how to install and enable FabulaTech USB redirection in Azure Virtual Desktop using the custom AVD build provided.

Steps

1. Download the custom AVD-supported version 3.3.375.
2. Install the USB for Remote Desktop (Server) component in the AVD session.
3. Reboot the AVD session.

Results

After the reboot, the FabulaTech USB redirection icon appears in the system tray.

12

Support Resources

This chapter provides FAQs, and support resources for resolving ThinOS 10.x migration issues, including DHCP/DNS setup and log collection.

Topics:

Resources and support

Accessing documents using product selector

1. Go to Support | Dell.
2. Click **Browse All Products**.
3. Click **Computers**.
4. Click **Thin Clients**.
5. Click **Wyse Software**.
6. Click **Dell ThinOS** .
7. Click **Select This Product**.
8. Click **Support Resources** > **Manuals & Documents**.

Reference materials and supporting documentation

This chapter serves as a centralized repository of official Dell ThinOS 10.x documentation. It enables administrators to quickly access key resources for deployment, configuration, compatibility validation, and customization. It provides direct access to key Dell ThinOS 10.x documents that assist IT administrators in various aspects of endpoint management.

Table 5. Document index

Document title	Description	Go to
Dell ThinOS 10.x Administrator Guide	Provides IT administrators with instructions for configuring, managing, and troubleshooting the system.	Dell ThinOS documentation page
Dell ThinOS 10.x Migration Guide	Provides IT administrators with procedures for migrating data, applications, or systems from one environment to another.	
Dell ThinOS 10.x 2602 Release Notes	Provides users with a summary of new features, bug fixes, and known issues for a software release.	
Dell ThinOS 10.x Hardware Compatibility List	Provides IT administrators with details on compatible hardware, software, and supported configurations for the software.	
Dell ThinOS 10.x Compatibility Checker User Guide	Provides IT administrators with the details to repurpose any Dell or non-Dell	

Table 5. Document index (continued)

Document title	Description	Go to
	hardware for ThinOS 10.x using a USB imaging method.	
Dell ThinOS 10.x App Builder User's Guide	Provides users with instructions for using the software, including setup and features.	

Contacting Dell

If you do not have an active Internet connection, you can find contact information about your purchase invoice, packing slip, bill, or Dell product catalog.

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

1. Go to Support | Dell.
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.