Lenovo Device Manager (LDM)
User Guide

Name of Document	LDM User Guide
Version Number	V2.2
Release Date	30 August 2022
Modifications/Additions	1. Remote BIOS Management for Intel vPro® devices 2. Intel vPro Statistics-Exporting device details 3. Android Device Settings/Restrictions 4. Android Application Management 5. Intel vPro Essentials vs Enterprise functionality

Contents

1 OVERVIEW

As the demand for more devices grows and the move to the cloud continues, Lenovo Device Manager provides a flexible, scalable endpoint and app management solution for any Lenovo Windows or Android device.

LDM features include:

- Robust device details and health status
- Simplified device & cloud-based application updating
- Integration with Intel vPro® EMA
- Quick deployment of software and add-on services
- Better end-user experience
- Safe, secure platform

Lenovo
Device
Manager

Zero-touch device management. Now that's smarter.

As the demand for more devices grows and the move to the cloud continues, Lenovo Device Manager (LDM) was developed to provide a flexible, scalable endpoint and app management solution for any Lenovo Windows or Android device. This cloud-based solution offers a streamlined experience for even the most complex environments, providing faster, less costly, and more flexible device management.

The LDM platform provides IT administrators the ability to easily manage all devices, ensuring the best end-user experience enhanced by Intel vPro® Essentials.

Robust device details and health status reporting

Easy to navigate dashboard to monitor all devices

Quick deployment of software and add-on services

Safe, secure platform for your fleet of devices

Smarter technology for all

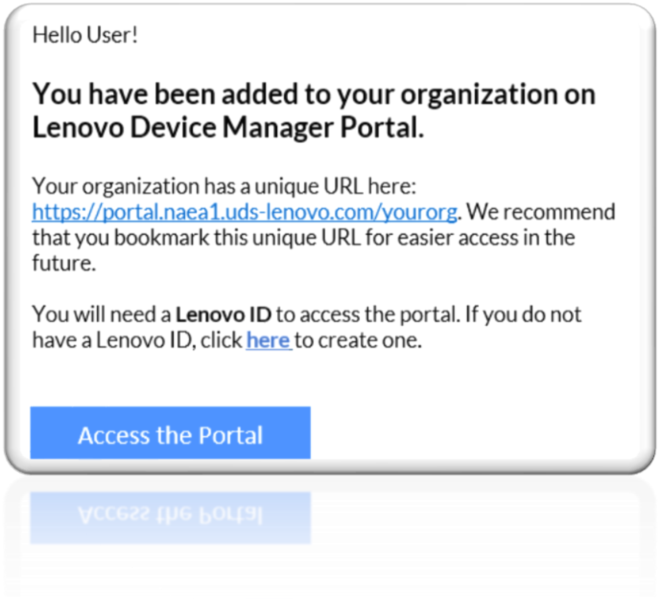
Lenovo

© Lenovo 2022. All rights reserved.

2 Setup & Configuration

2.1 Organization Setup

When your organization's portal is created, a single administrative account will be created. The IT Owner (Org Admin) specified to Lenovo at the time of sale will receive a Lenovo Device Manager e-mail indicating that he or she has been granted access to your organization. Clicking on the link will take you to the Sign on page where you can log in to LDM as an Organization Administrator. With this administrative account, you can: configure the portal, invite users, and add devices.



Hello User!

You have been added to your organization on Lenovo Device Manager Portal.

Your organization has a unique URL here: https://portal.naea1.uds-lenovo.com/yourorg. We recommend that you bookmark this unique URL for easier access in the future.

You will need a **Lenovo ID** to access the portal. If you do not have a Lenovo ID, click here to create one.

Note: As of LDM 2.1, the URL format is: https://portal-platform.naea1-uds.lenovo.com/yourorg

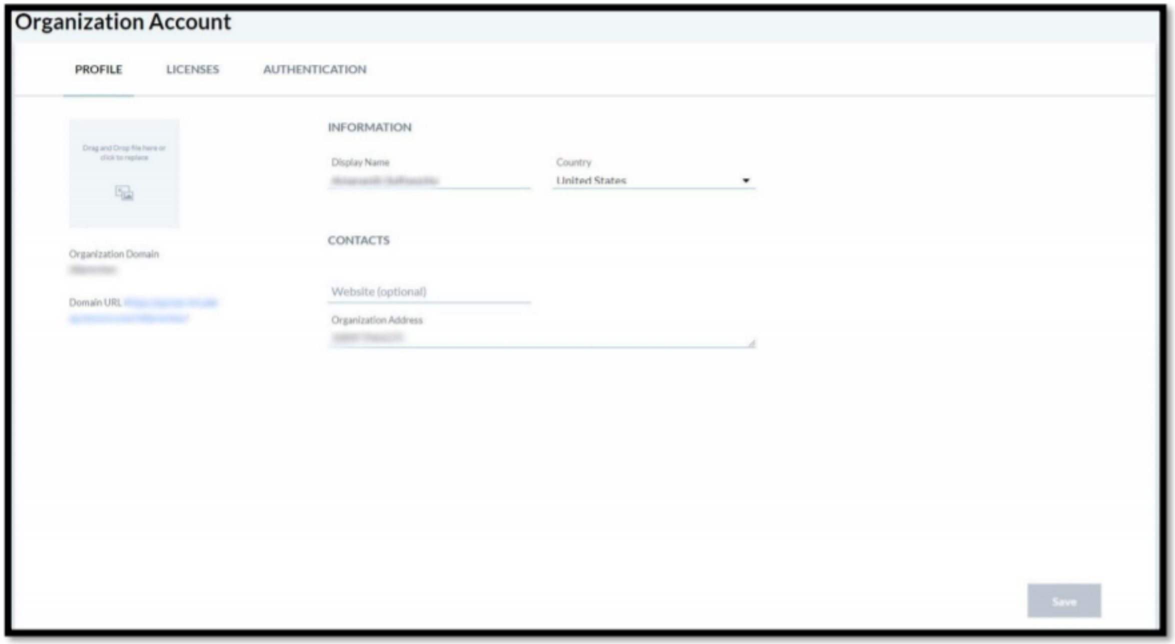
2.2 Manage Organization

2.2.1 Organization Account

Account details for your organization can be accessed by clicking on your **User Icon in the top ribbon > "Organization Account"** option. The following options are available:

- Update Organization Name
- Update Organization Country
- Update Organization Website
- Update Organization Address
- Update Organization Profile Image

Tab / Option	Function
Profile	Manage the profile for your organization • Logo • Organization name • Country • Address
Authentication	View the authentication type for users of the solution in your organization



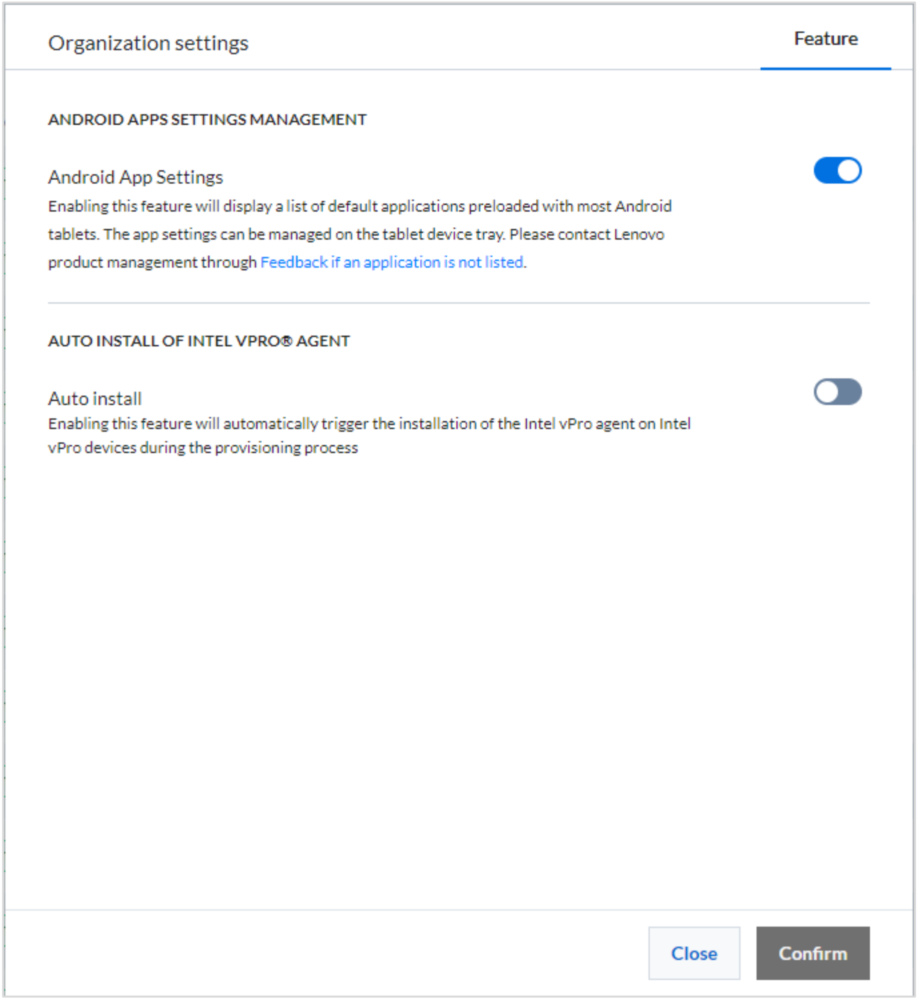
Country: United States

2.2.2 Organization Settings

Customized feature settings configured for your organization's LDM portal clicking on your **User Icon in the top ribbon > "Organization Settings"** option. The following options are available:

- **Android App Settings**: Enables application management functionality from the Device Tray/*Apps/App Restrictions* (Refer to Section 2.3)

- **Auto Install of Intel vPro Agent**: Enables the automatic installation of the Intel vPro agent on eligible devices during the provisioning process.



Organization settings

ANDROID APPS SETTINGS MANAGEMENT

Android App Settings ●

Enabling this feature will display a list of default applications preloaded with most Android tablets. The app settings can be managed on the tablet device tray. Please contact Lenovo product management through Feedback if an application is not listed.

AUTO INSTALL OF INTEL VPRO® AGENT

Auto install ○

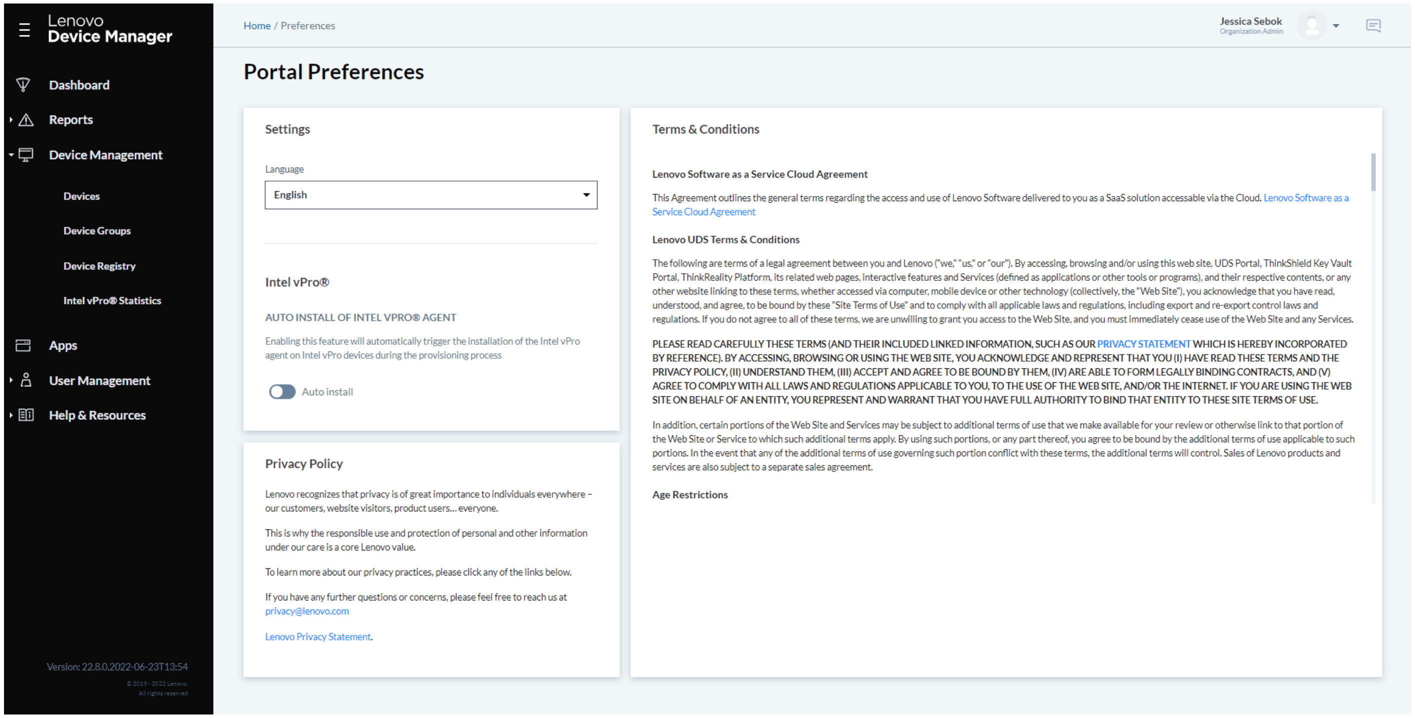
Enabling this feature will automatically trigger the installation of the Intel vPro agent on Intel vPro devices during the provisioning process

2.3 User Preferences

Preferences for your user account in the portal can be accessed by clicking on your **User Icon in the top ribbon > "Preferences"** option.

Preferences page allows you to manage account settings, and view Terms & Conditions with Privacy Policy.

Preference	**Description**
Language	The language that the portal UI is displayed in
Intel vPro® Agent Auto-Installation	Enable/Disable automatic installation of the Intel vPro agent during the provisioning process. When enabled, LDM will automatically identify all devices with the Intel vPro chip and install the required agent to fully manage those devices through the LDM portal. For more information, refer to Section 3.4. **Note**: This feature is set to “Disabled” for all new organizations by default. Even if disabled, the manual installation option via the Device Management/Devices/*Device Tray* is still available.



Portal Preferences

Settings

Language: English

Intel vPro®

AUTO INSTALL OF INTEL VPRO® AGENT

Enabling this feature will automatically trigger the installation of the Intel vPro agent on Intel vPro devices during the provisioning process

○ Auto install

Privacy Policy

Lenovo recognizes that privacy is of great importance to individuals everywhere – our customers, website visitors, product users... everyone.

This is why the responsible use and protection of personal and other information under our care is a core Lenovo value.

To learn more about our privacy practices, please click any of the links below.

If you have any further questions or concerns, please feel free to reach us at privacy@lenovo.com

Lenovo Privacy Statement.

Terms & Conditions

Lenovo Software as a Service Cloud Agreement

This Agreement outlines the general terms regarding the access and use of Lenovo Software delivered to you as a SaaS solution accessable via the Cloud. Lenovo Software as a Service Cloud Agreement

Lenovo UDS Terms & Conditions

The following are terms of a legal agreement between you and Lenovo (“we,” “us,” or “our”). By accessing, browsing and/or using this web site, UDS Portal, ThinkShield Key Vault Portal, ThinkReality Platform, its related web pages, interactive features and Services (defined as applications or other tools or programs), and their respective contents, or any other website linking to these terms, whether accessed via computer, mobile device or other technology (collectively, the "Web Site"), you acknowledge that you have read, understood, and agree, to be bound by these “Site Terms of Use” and to comply with all applicable laws and regulations, including export and re-export control laws and regulations. If you do not agree to all of these terms, we are unwilling to grant you access to the Web Site, and you must immediately cease use of the Web Site and any Services.

PLEASE READ CAREFULLY THESE TERMS (AND THEIR INCLUDED LINKED INFORMATION, SUCH AS OUR PRIVACY STATEMENT WHICH IS HEREBY INCORPORATED BY REFERENCE). BY ACCESSING, BROWSING OR USING THE WEB SITE, YOU ACKNOWLEDGE AND REPRESENT THAT YOU (I) HAVE READ THESE TERMS AND THE PRIVACY POLICY, (II) UNDERSTAND THEM, (III) ACCEPT AND AGREE TO BE BOUND BY THEM, (IV) ARE ABLE TO FORM LEGALLY BINDING CONTRACTS, AND (V) AGREE TO COMPLY WITH ALL LAWS AND REGULATIONS APPLICABLE TO YOU, TO THE USE OF THE WEB SITE, AND/OR THE INTERNET. IF YOU ARE USING THE WEB SITE ON BEHALF OF AN ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND THAT ENTITY TO THESE SITE TERMS OF USE.

In addition, certain portions of the Web Site and Services may be subject to additional terms of use that we make available for your review or otherwise link to that portion of the Web Site or Service to which such additional terms apply. By using such portions, or any part thereof, you agree to be bound by the additional terms of use applicable to such portions. In the event that any of the additional terms of use governing such portion conflict with these terms, the additional terms will control. Sales of Lenovo products and services are also subject to a separate sales agreement.

Age Restrictions

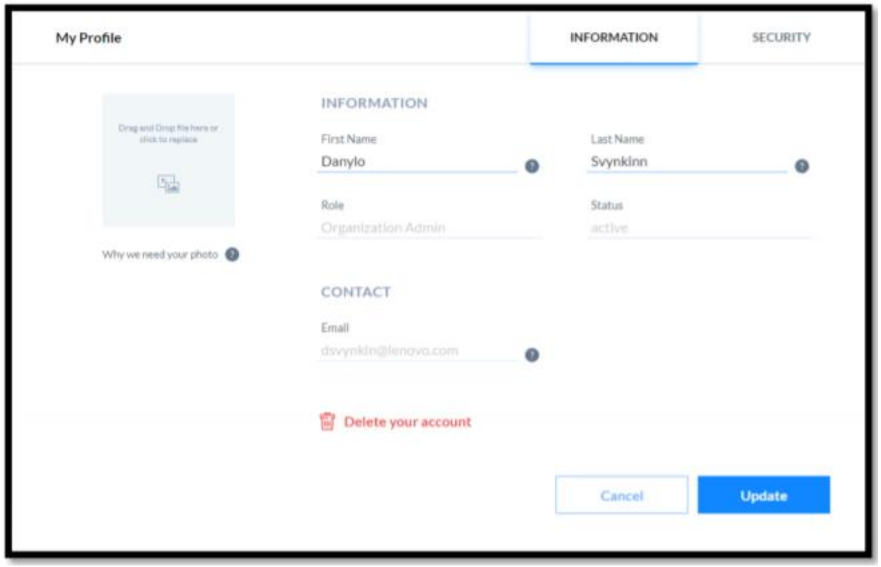
2.4 User Management

2.4.1 User Roles & Permissions

Profile info can be accessed by clicking on your **user icon in the top ribbon > "My Profile"** option. The following options are available:

- Update your First Name
- Update your Last Name
- Update your Profile Image
- Enable/disable Multi-Factor Authentication.
- Delete your account
- When adding users to your portal, there are two role types to assign: Organization Admin and IT Admin. Below is a table contrasting the functionality of these roles.

Functionality	Role	
	Org Admin	IT Admin
Dashboard	🟢	🟢
View Devices	🟢	🟢
Manage Devices	🟢	🟢
Factory Reset Devices	🟢	🔴
View Device Groups	🟢	🟢
Manage Device Groups	🟢	🟢
View Device Licenses	🟢	🟢
Assign Device Licenses	🟢	🟢
View Users	🟢	🔴
Manage Users	🟢	🔴
View User Groups	🟢	🔴
Manage User Groups	🟢	🔴
Manage Org Settings	🟢	🔴



INFORMATION

First Name: Danylo

Last Name: Svynkinn

Role: Organization Admin

Status: active

CONTACT

Email: dsvynkin@lenovo.com

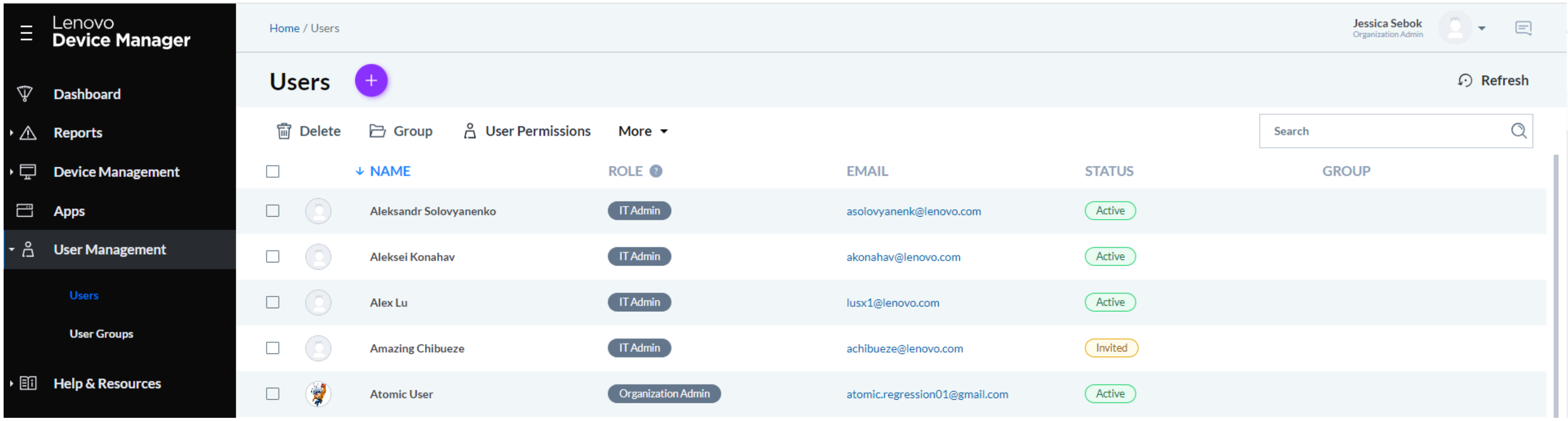
Delete your account

Lenovo ID

Lenovo ID is the secure and trusted mechanism providing authentication & identity management for Lenovo Client Remote Management. It offers single sign on as well as integration with other Lenovo solutions. Lenovo ID accounts can be freely created at passport.lenovo.com. It is not necessary to create the Lenovo ID accounts before, users can be invited to join and create an account.

View Organization Users

Users can be managed in your portal by accessing **Users Manager → Users**. To understand the differences between User Roles, click on the "User Permissions" button.



	NAME	ROLE	EMAIL	STATUS	GROUP
□	Aleksandr Solovyanenko	IT Admin	asolovyanenk@lenovo.com	Active	
□	Aleksei Konahav	IT Admin	akonahav@lenovo.com	Active	
□	Alex Lu	IT Admin	lusx1@lenovo.com	Active	
□	Amazing Chibueze	IT Admin	achibueze@lenovo.com	Invited	
□	Atomic User	Organization Admin	atomic.regression01@gmail.com	Active	

On the Users page, you can:

- Invite users
- Delete users
- Group users
- Update users
- Perform Bulk updates for users
- Export a list of users to CSV
- View User status

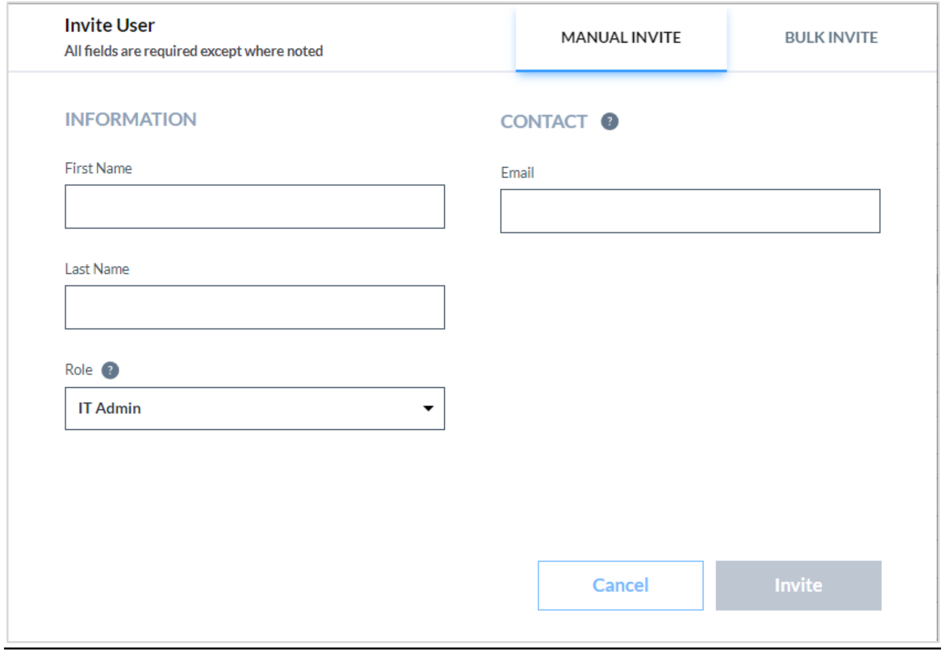
2.4.2 Adding, Updating & Deleting Users on an Organization

Invite Individual User(s)

Users can be added to your portal by accessing **Users Manager → Users → ✚ (add)** button. You can invite users individually, or in bulk by uploading a CSV file containing user details for each invitee.

To add users individually (manually):

1. Click on button "+"
2. Input all the required info
3. Click on the button "Invite"
4. The user will receive an email invitation with a link to sign in and/or create a Lenovo ID account using the same email address



Invite User

All fields are required except where noted

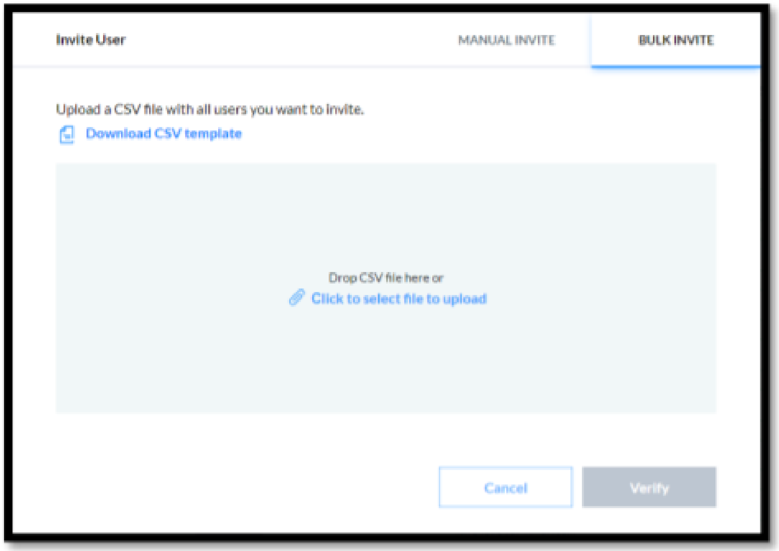
Role: IT Admin

<u>To add user(s) in bulk:</u>

1. Click on button "+"
2. Select "Bulk Invite" tab
3. Download CSV template by clicking on "Download CSV template" button
4. Populate CSV file with required info for each user - First Name, Last Name, Role and Email

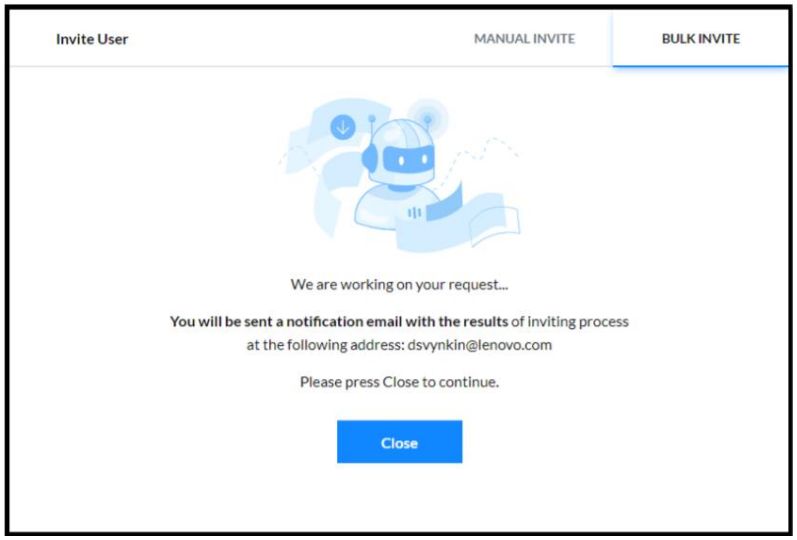
Example CSV for Bulk User Invite:

```
First Name,Last Name,Role,Email
Bill,Lumbergh,Organization Admin,wlumberg@company.com
Peter,Gibbons,IT Admin,pgibbons@company.com
```



Upload a CSV file with all users you want to invite.

Drop CSV file here or



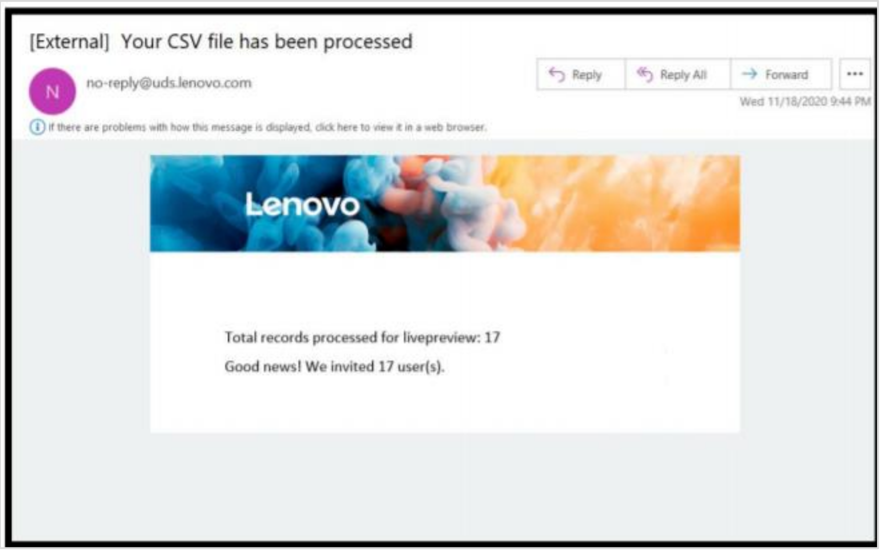
We are working on your request...

You will be sent a notification email with the results of inviting process at the following address: dsvynkin@lenovo.com

Please press Close to continue.

5. Drop CSV file to the modal window and click on button "Verify"
6. When uploading a CSV file, the file will be processed and any errors with the upload will be displayed in a feedback screen

7. You will receive an e-mail confirmation from the portal when the upload completes
8. If a user loses their invitation email, you can resend the invitation by clicking on the user in the Users Table


[External] Your CSV file has been processed

no-reply@uds.lenovo.com

Wed 11/18/2020 9:44 PM

If there are problems with how this message is displayed, click here to view it in a web browser.

Total records processed for livepreview: 17

Good news! We invited 17 user(s).

User Agreements / Terms & Conditions Acceptance for New Users

The first time a new user logs into LDM, three user agreements will be presented:

- Lenovo Software as a Service Cloud Agreement
- Lenovo UDS Terms & Conditions (also available under **User Account > Preferences**)
- Lenovo Privacy Policy (also available under **User Account > Preferences**)

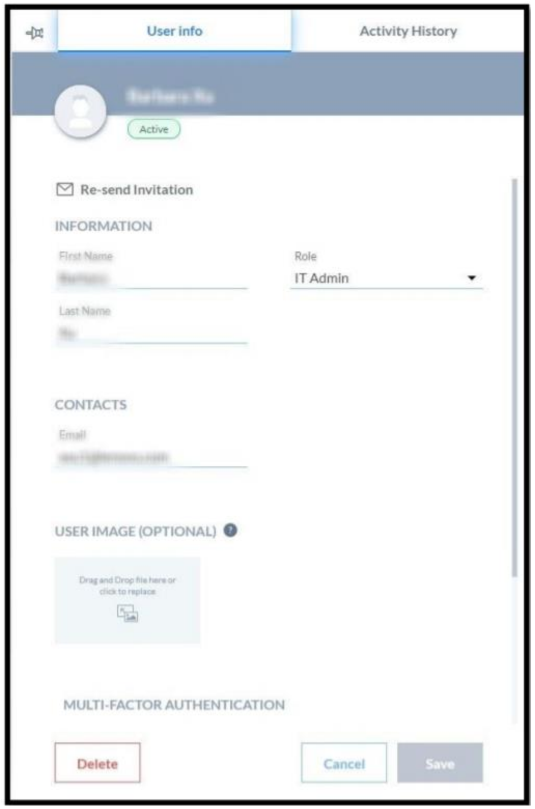
Each user must select the checkbox and accept each agreement before gaining access to the LDM portal.

Update User(s)

To manage user information, click on a user to open the user tray.

The following options are available for a user on the user tray:

- Update user’s information and contact details (First Name, Last Name, Email, User Role)
- Upload/update a user’s profile image
- Delete a user



[redacted]

INFORMATION

First Name
[redacted]

Role
IT Admin

Last Name
[redacted]

CONTACTS

Email
[redacted]

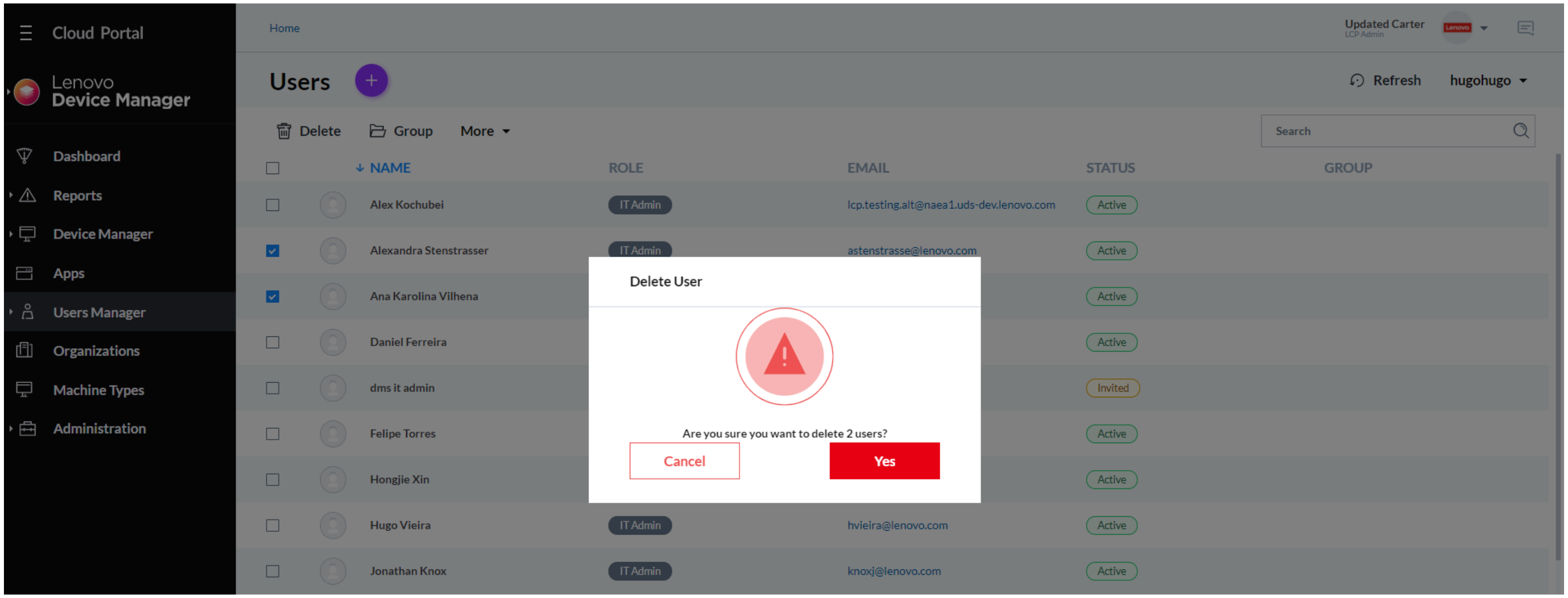
USER IMAGE (OPTIONAL)

MULTI-FACTOR AUTHENTICATION

Deleting User(s)

To delete user(s) from your organization:

1. Select the User(s) you want to delete.
2. Click on the button "Delete" and confirm the deletion.



□	NAME	ROLE	EMAIL	STATUS	GROUP
□	Alex Kochubei	IT Admin	lcp.testing.alt@naea1.uds-dev.lenovo.com	Active	
☑	Alexandra Stenstrasser	IT Admin	astenstrasse@lenovo.com	Active	
☑	Ana Karolina Vilhena			Active	
□	Daniel Ferreira			Active	
□	dms it admin			Invited	
□	Felipe Torres			Active	
□	Hongjie Xin			Active	
□	Hugo Vieira	IT Admin	hvieira@lenovo.com	Active	
□	Jonathan Knox	IT Admin	knoxj@lenovo.com	Active	

Delete User

Are you sure you want to delete 2 users?

Cancel Yes

2.5 User Groups

3 MANAGE DEVICES

Devices represent the various device types that are in your organization and typically used by employees. A device type can fall under any of the following categories:

	Current Device Type Categories			
	PCs	**SmartEdge**	**Tablet / Mobile**	**AR / VR**
Examples	Any Lenovo notebook, desktop, workstation, etc	Any Lenovo edge appliance and servers	Any Lenovo tablets or mobile device	Any Lenovo AR or VR appliance

3.1 Add Devices

Adding a device to LDM requires provisioning the device with a configured client agent from Device Management / Devices / *Claim a device*.

NOTE: A dedicated guide exists for the device enrollment and activation process. Please refer to the Quick Start Guide for detailed steps.

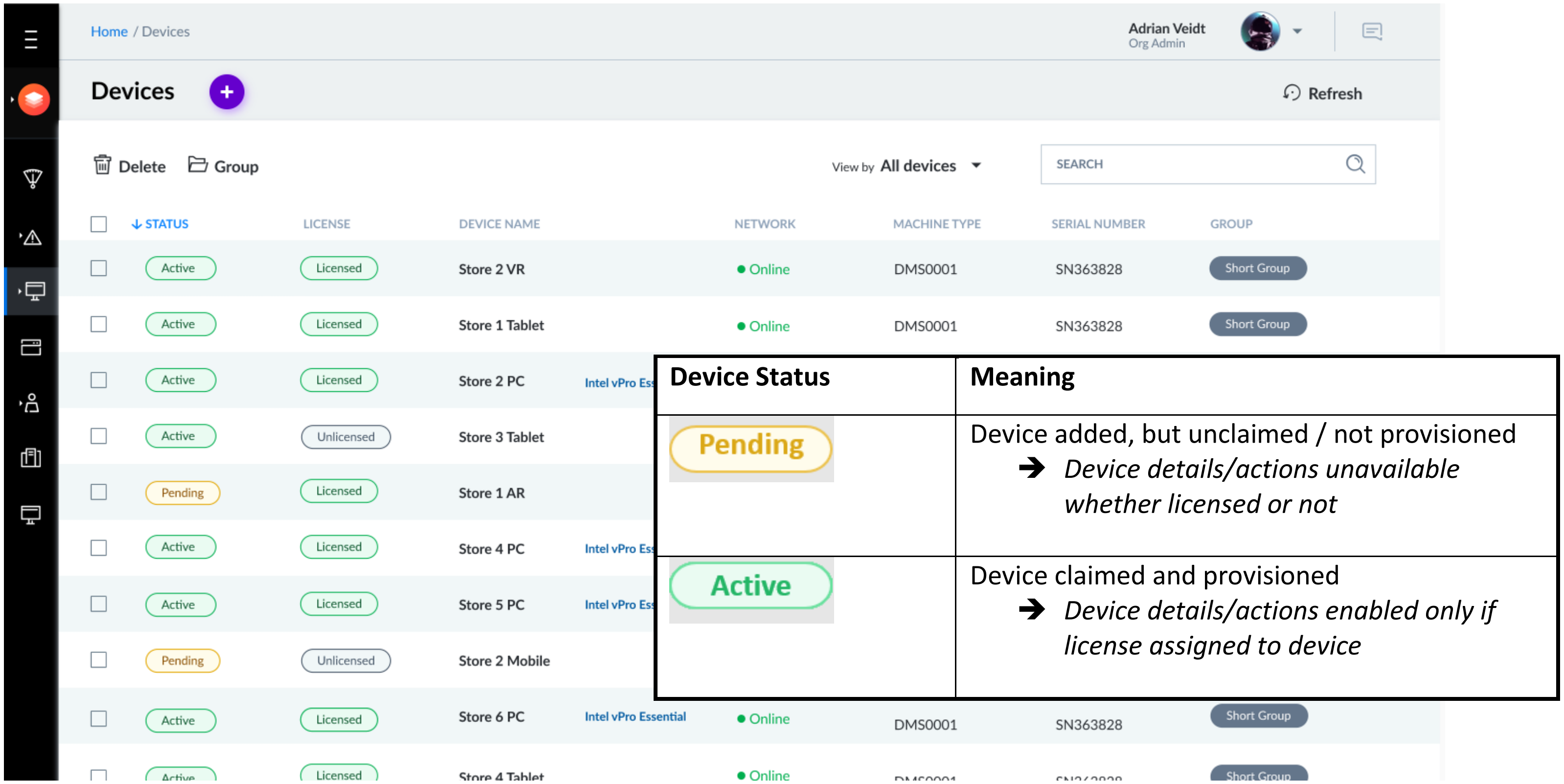
3.2 Manage Devices

Devices in your organization's portal can be accessed via **Device Manager → Devices**.

Each device in the table represents a device that was added into your portal, including devices that have not yet completed registration. The Status for each device is helpful for identifying the expected functionality for the device. Only devices that have an “Active” status and have been assigned a license, “Licensed”, can be fully managed through LDM. To assign a license to a device, refer to the *Licensing* section of this document.

Android devices that have been factory reset are removed from this list automatically and added to the “Decommissioned” Report. See *Reports* for more information.

Devices that have the Intel vPro® agent installed, will be designated by the “Intel vPro®” label. For more information, see Section 3.4.



□	↓ STATUS	LICENSE	DEVICE NAME		NETWORK	MACHINE TYPE	SERIAL NUMBER	GROUP
□	Active	Licensed	Store 2 VR		● Online	DMS0001	SN363828	Short Group
□	Active	Licensed	Store 1 Tablet		● Online	DMS0001	SN363828	Short Group
□	Active	Licensed	Store 2 PC	Intel vPro Ess				
□	Active	Unlicensed	Store 3 Tablet					
□	Pending	Licensed	Store 1 AR					
□	Active	Licensed	Store 4 PC	Intel vPro Ess				
□	Active	Licensed	Store 5 PC	Intel vPro Ess				
□	Pending	Unlicensed	Store 2 Mobile					
□	Active	Licensed	Store 6 PC	Intel vPro Essential	● Online	DMS0001	SN363828	Short Group
□	Active	Licensed	Store 4 Tablet		● Online	DMS0001	SN363828	Short Group

Device Status	Meaning
Pending	Device added, but unclaimed / not provisioned ➔ *Device details/actions unavailable whether licensed or not*
Active	Device claimed and provisioned ➔ *Device details/actions enabled only if license assigned to device*

3.3 View Device Information and Perform Basic Actions

Standard Device Tray:

From the Devices page, click on any device to open its corresponding *Device Tray*.

The *Device Tray* may contain up to six tabs, depending on the device type:

- Device Info
- Device Settings (currently only available for Android devices)
- Apps
- Remote Management (currently only available for Windows devices)
- Peripherals & IoT (HDMI & USB connectivity details)
- Alerts History
- Activity History

NOTE: Use the forward and back arrows at each end of the tab selector to access additional items.

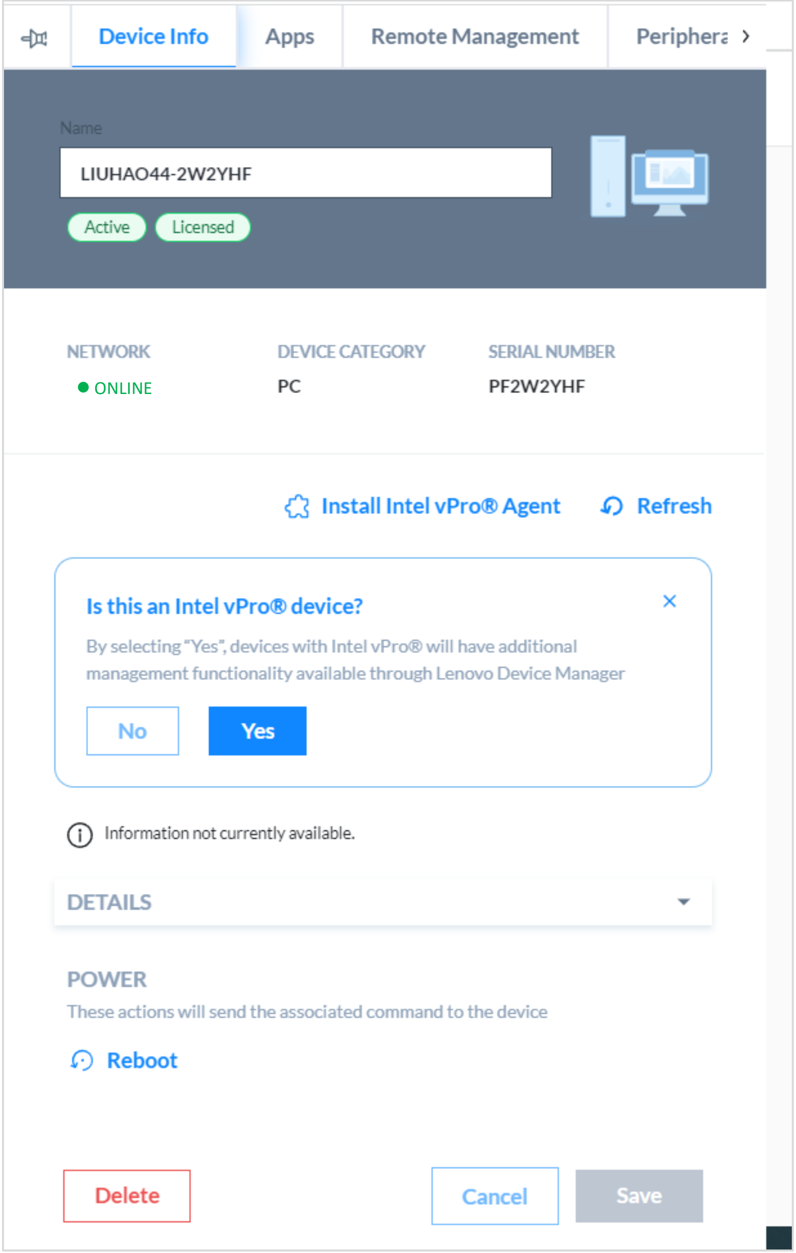
The following features are available on the device tray - ***Device Info*** tab:

- View device hardware and software details
- Manually install the Intel vPro® Agent
- Delete the device from the portal
- Remotely Reboot the device
- Configure device name
- Remotely factory reset the device (for Android only)

The **name of the device** on the Device List can be configured by:

1) Type the new name in the field at the top of the Device Tray
2) Click "Save"

NOTE: If a device has not been fully registered or is not licensed, neither data nor action functionality will be available in the Device Tray



Name: LIUHAO44-2W2YHF

NETWORK	DEVICE CATEGORY	SERIAL NUMBER
● ONLINE	PC	PF2W2YHF

Is this an Intel vPro® device?

By selecting "Yes", devices with Intel vPro® will have additional management functionality available through Lenovo Device Manager

Information not currently available.

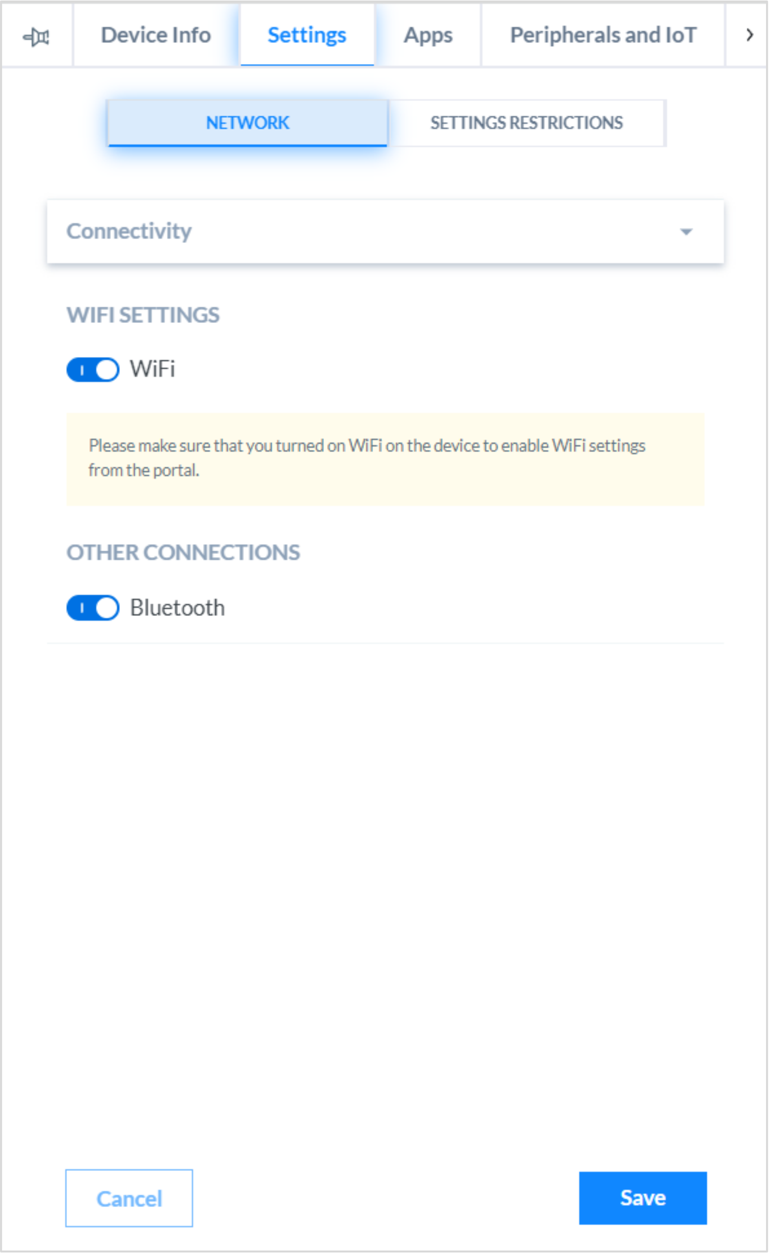
POWER

These actions will send the associated command to the device

The following options are available for a user on the device tray – ***Settings*** tab (currently available for Android devices only):

Note: This option is currently only available for Android devices (tablets).

- ***Network*** sub-tab (remotely configures the device, but could still be changed by device user)
    - Enable/disable WiFi connectivity on the device
    - Enable/disable Bluetooth connectivity on the device

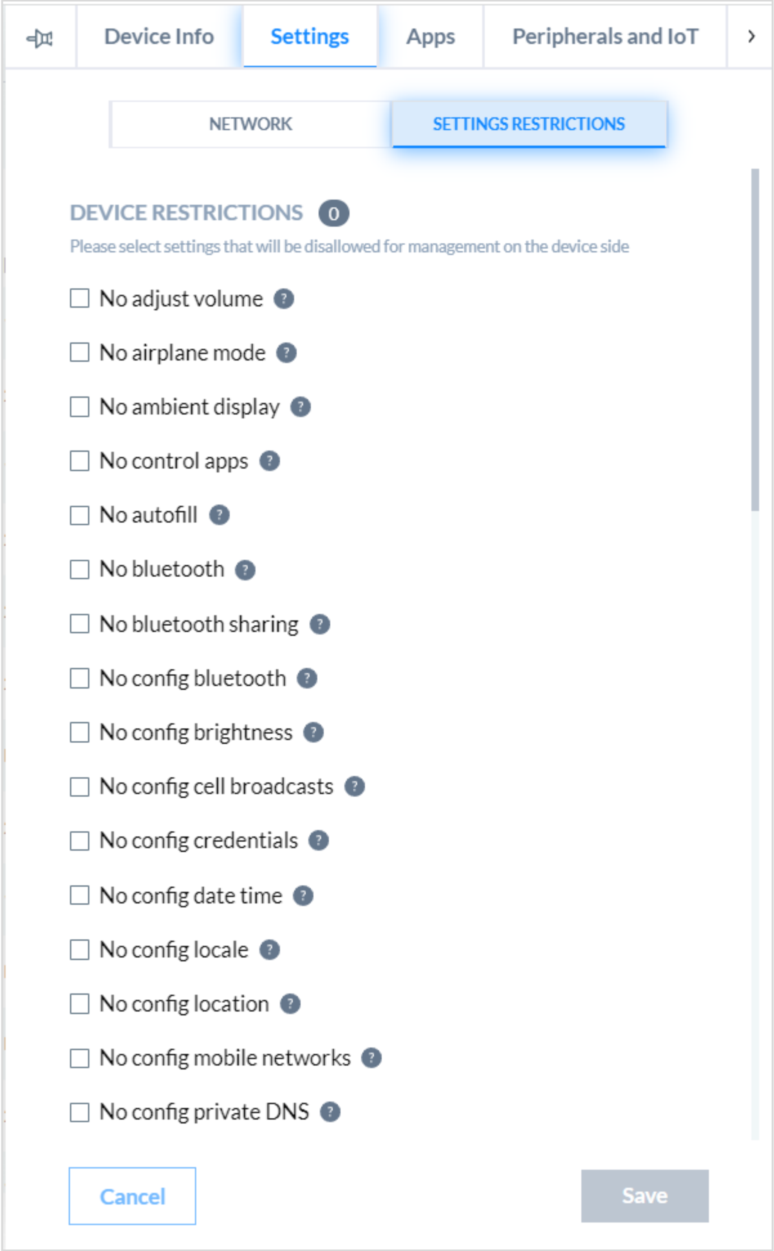


Please make sure that you turned on WiFi on the device to enable WiFi settings from the portal.

- ***Settings Restrictions*** sub-tab (restricts settings allowed to be changed directly on device)

IT Admins can limit how an end user interacts with their device by setting the restrictions defined on the next page.

1. Select one or more restrictions
2. Click “Save”
3. Restrictions will be applied to the device



DEVICE RESTRICTIONS 0

Please select settings that will be disallowed for management on the device side

□ No adjust volume

□ No airplane mode

□ No ambient display

□ No control apps

□ No autofill

□ No bluetooth

□ No bluetooth sharing

□ No config bluetooth

□ No config brightness

□ No config cell broadcasts

□ No config credentials

□ No config date time

□ No config locale

□ No config location

□ No config mobile networks

□ No config private DNS

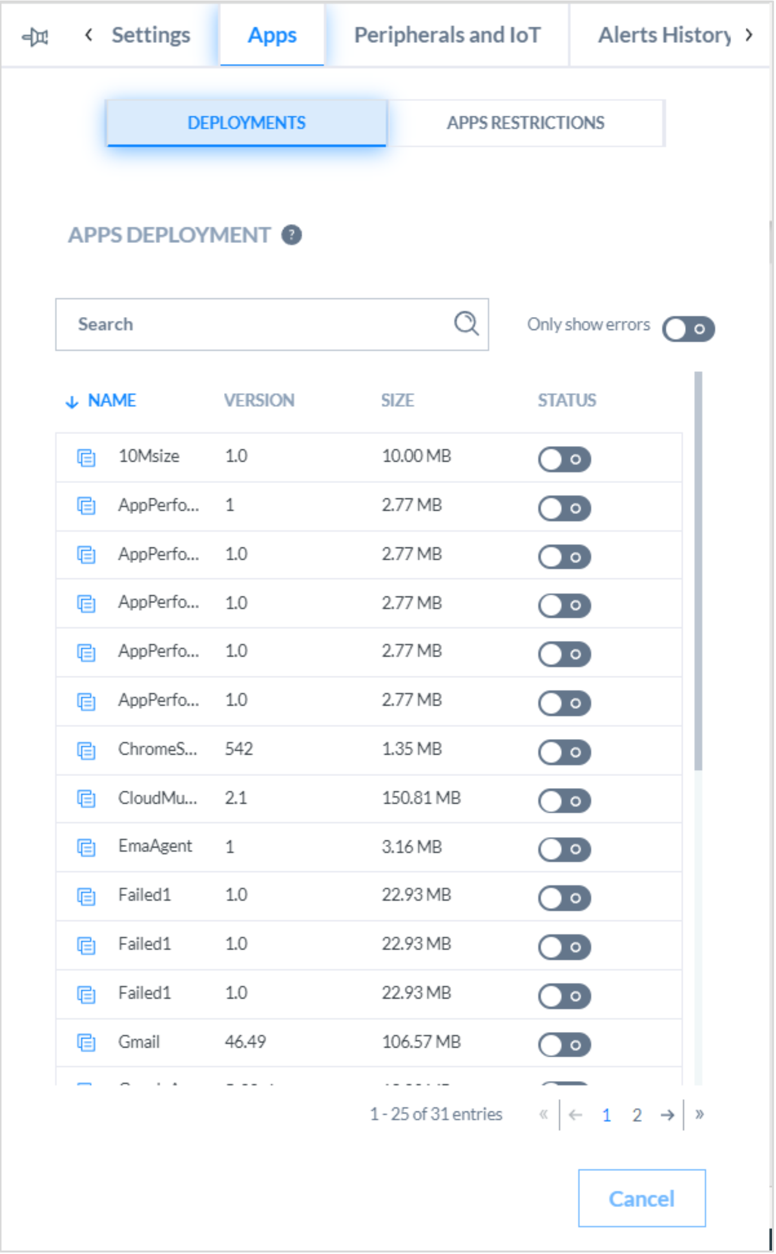
Android Device Restrictions Defined:

- No adjust volume
- No airplane mode
- No ambient display
- No control apps
- No autofill
- No Bluetooth
- No Bluetooth sharing
- No config Bluetooth
- No config brightness
- No config cell broadcasts
- No config credentials
- No config date time
- No config locale
- No config location
- No config mobile networks
- No config private DNS
- No config screen timeout
- No config tethering
- No config VPN
- No config WiFi
- No content capture
- No content suggestions
- No create windows
- No cross-profile copy-paste
- No factory reset
- No fun
- No install apps
- No install unknown sources
- No install unknown sources globally
- No modify accounts
- No physical media
- No network reset
- No outgoing beam
- No outgoing calls
- No printing
- No remove user
- No safe boot
- No set user icon
- No set wallpaper
- No sharing into profile
- No share location
- No SMS
- No system error dialogs
- No unified password
- No uninstall apps
- No unmute microphone
- No file transfer through USB
- No user switch
- No apps verification

***Note**: In LDM, hovering over tool tip next to each Restriction provides its definition*

The following options are available for a user on the device tray – ***Apps*** tab:

- ***Deployments*** sub-tab:
  - View LDM-managed applications (software, firmware, driver) on device
  - Deploy application updates to the device
  - Uninstall applications from the device
  - View deployment status



APPS DEPLOYMENT

NAME	VERSION	SIZE	STATUS
10Msize	1.0	10.00 MB	○
AppPerfo...	1	2.77 MB	○
AppPerfo...	1.0	2.77 MB	○
AppPerfo...	1.0	2.77 MB	○
AppPerfo...	1.0	2.77 MB	○
AppPerfo...	1.0	2.77 MB	○
ChromeS...	542	1.35 MB	○
CloudMu...	2.1	150.81 MB	○
EmaAgent	1	3.16 MB	○
Failed1	1.0	22.93 MB	○
Failed1	1.0	22.93 MB	○
Failed1	1.0	22.93 MB	○
Gmail	46.49	106.57 MB	○

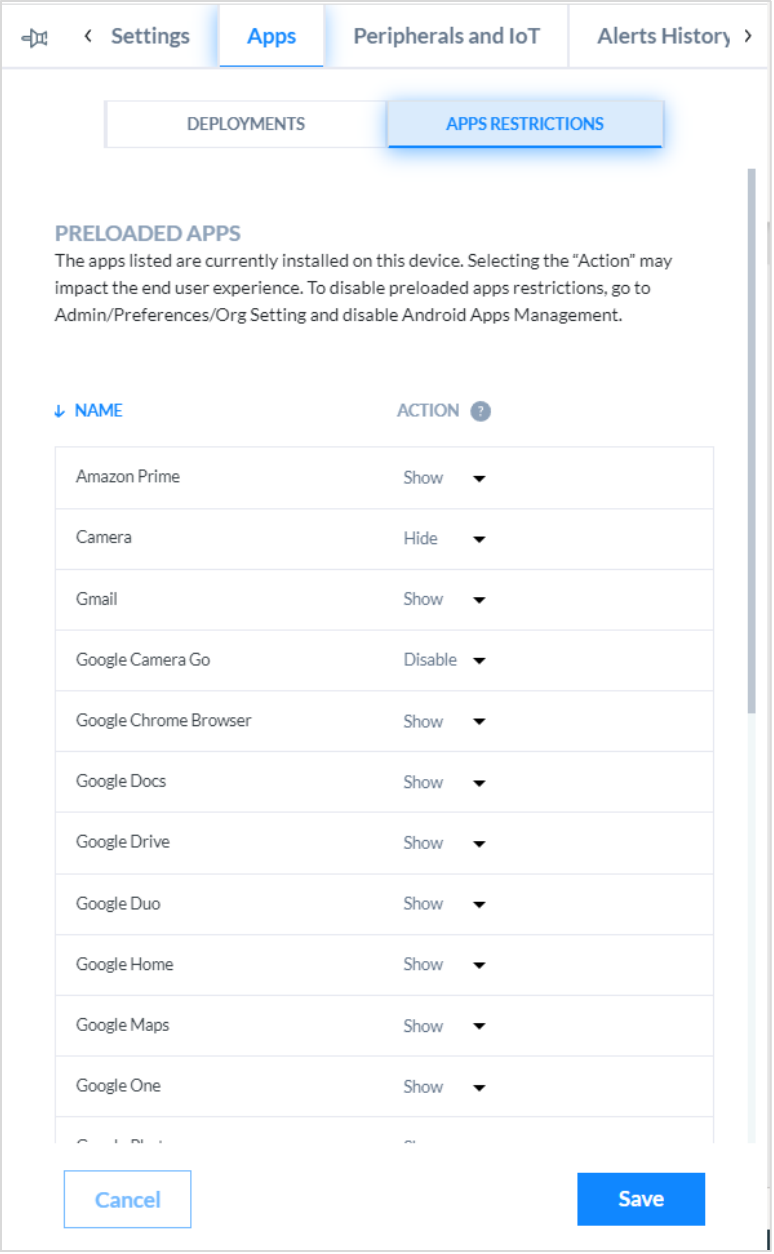
1 - 25 of 31 entries « ← 1 2 → »

- ***App Restrictions*** sub-tab:

  Note: This feature is currently only available for Android devices (tablets) and **MUST BE ENABLED** in Org Settings (see Section 2.2.2 for more information)

  - Displays list of standard pre-loaded Android apps
  - Allows end user app experience to be controlled remotely

  1. Find the App to be managed
  2. Under "Action", click the drop down to select from the following Actions:
     - ○ **Show** (default) – allows app to be visible and usable on the device
     - ○ **Hide** – app will be hidden on the device and unusable
     - ○ **Disable** – app will be seen, but will be disabled and unusable



PRELOADED APPS

The apps listed are currently installed on this device. Selecting the "Action" may impact the end user experience. To disable preloaded apps restrictions, go to Admin/Preferences/Org Setting and disable Android Apps Management.

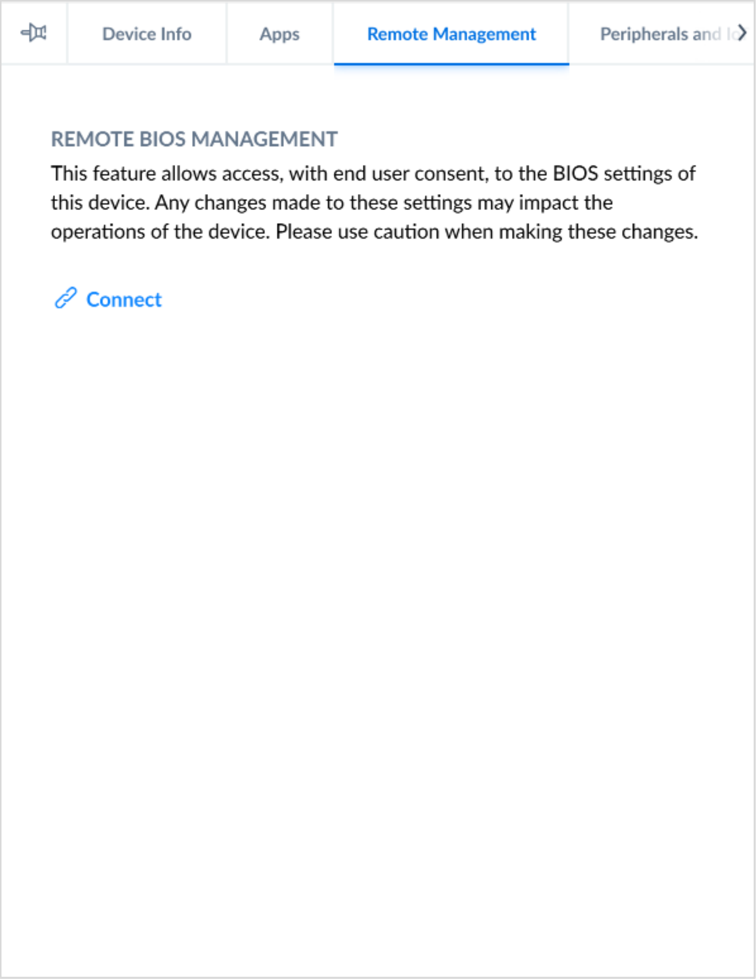
↓ NAME	ACTION
Amazon Prime	Show ▾
Camera	Hide ▾
Gmail	Show ▾
Google Camera Go	Disable ▾
Google Chrome Browser	Show ▾
Google Docs	Show ▾
Google Drive	Show ▾
Google Duo	Show ▾
Google Home	Show ▾
Google Maps	Show ▾
Google One	Show ▾

The following options are available for a user on the device tray – ***Remote Management*** tab:

Note: This feature is currently only available for Windows devices (with Intel vPro agent installed)

- Remote BIOS Management: Allows IT Admins to access the device's BIOS settings
- Requires Intel vPro agent installed on the device

For more information on Remote BIOS Management, see Intel vPro Support, section 3.4

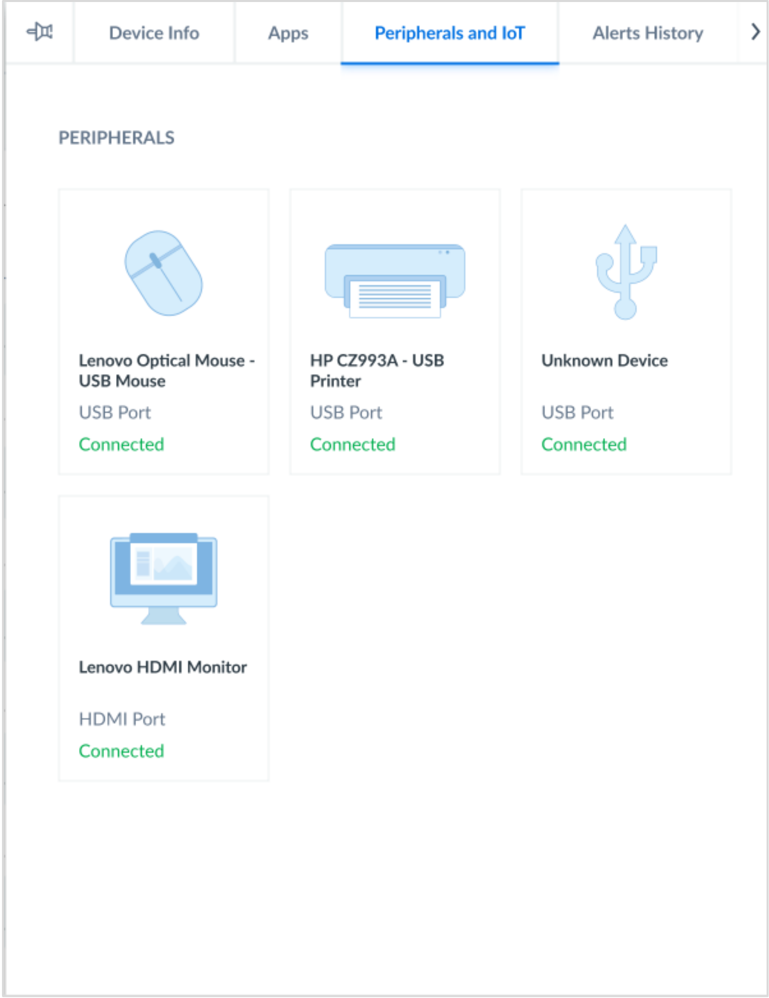


REMOTE BIOS MANAGEMENT

This feature allows access, with end user consent, to the BIOS settings of this device. Any changes made to these settings may impact the operations of the device. Please use caution when making these changes.

The following options are available for a user on the device tray – ***Peripherals and IoT*** tab:

- View any USB or HDMI connected peripheral connected to the device
- See port type in use



PERIPHERALS

Lenovo Optical Mouse - USB Mouse
USB Port
Connected

HP CZ993A - USB Printer
USB Port
Connected

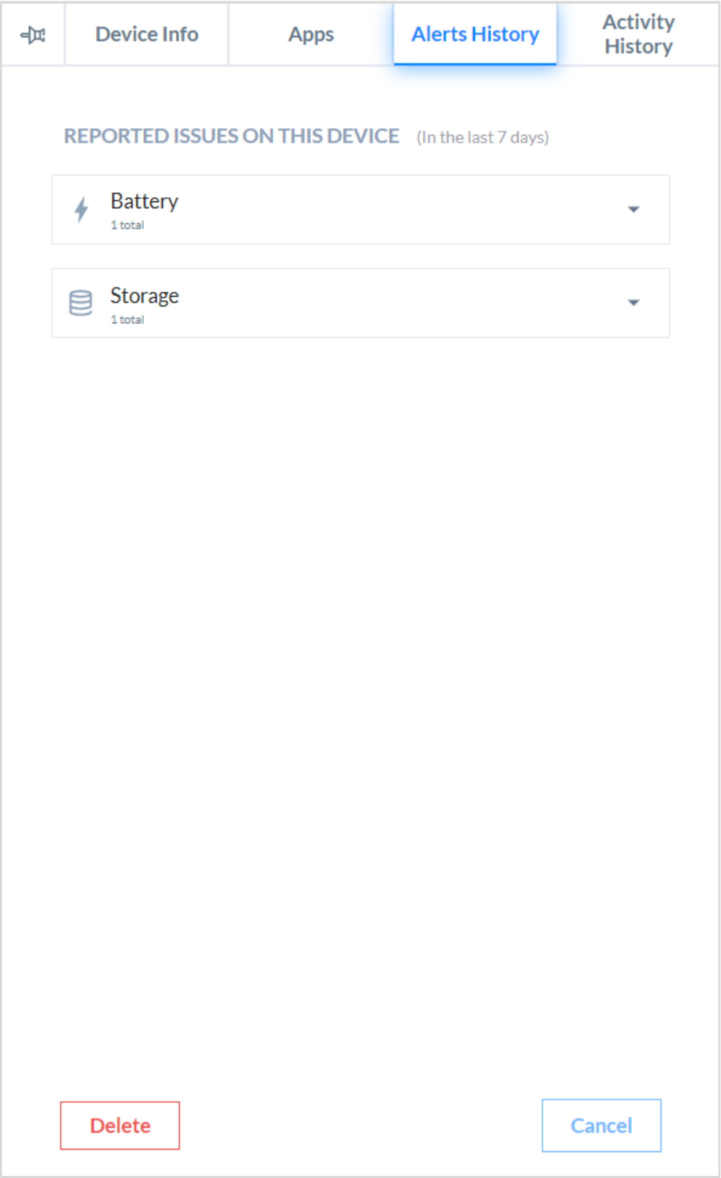
Unknown Device
USB Port
Connected

Lenovo HDMI Monitor
HDMI Port
Connected

The following options are available for a user on the device tray – ***Alert History*** tab:

- View any “Low Battery” alert
- View any “Storage” alert
- View any “OTA Deployment” alert
- Delete device

NOTE: Alert status is reflective over a rolling seven-day period.



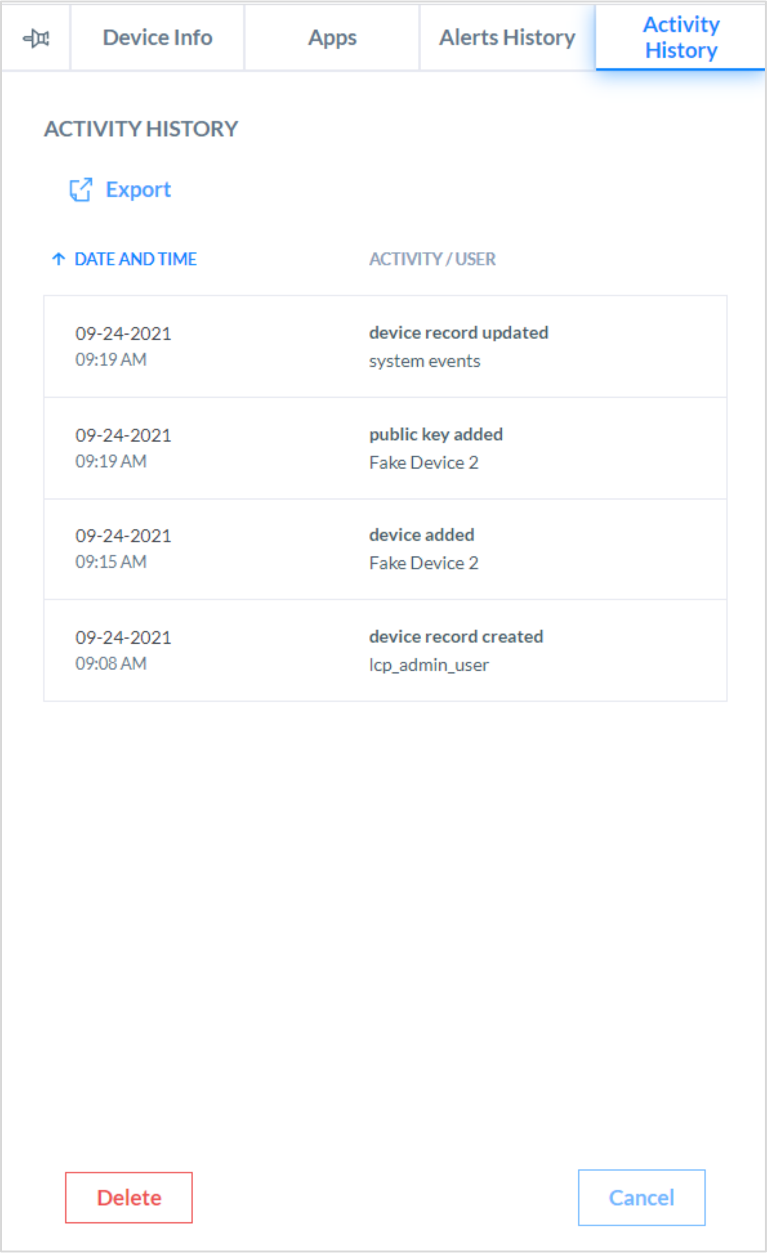
REPORTED ISSUES ON THIS DEVICE (In the last 7 days)

Battery
1 total

Storage
1 total

The following options are available on the device tray - ***Activity History*** tab:

- View the device Activity History
- Export device Activity History to CSV file
- Delete device



↑ DATE AND TIME	ACTIVITY / USER
09-24-2021 09:19 AM	**device record updated** system events
09-24-2021 09:19 AM	**public key added** Fake Device 2
09-24-2021 09:15 AM	**device added** Fake Device 2
09-24-2021 09:08 AM	**device record created** lcp_admin_user

3.4 Intel vPro® Support

Lenovo Device Manager support Intel vPro EMA functionality with the installation of the Intel vPro agent during LDM provisioning. Certain LDM features may be available differently for devices with Intel vPro Essentials and Intel vPro Enterprise chipsets. The following guide should help clarify the Intel vPro features supported from LDM:

Features Currently Supported on LDM	Intel® Standard Manageability for Intel vPro® Essentials	Intel® Active Management Technology (Intel® AMT) for Intel vPro® Enterprise
Device Hardware Inventory Information: Device component details, statistics and change alerts	●	●
Remote power management Power on, off, restart, sleep, wake, hibernate	●	●
Remote BIOS Management	●	●
Hardware manageability over Wi-Fi	●	●

3.4.1 Managing Individual Intel vPro® Devices

Automatic Installation of the vPro® Agent

During the provisioning process, LDM can identify devices with the Intel vPro chip installed and will automatically install the Intel vPro Agent. When enabled, this automatic feature will allow Intel vPro devices to be managed quickly and easily without any additional effort.

Org Admins can enable or disable this feature for all devices claimed under their organization in Org Settings/*Preferences* (see Section 2.3 for more information).

Manually Installing the Intel vPro® Agent

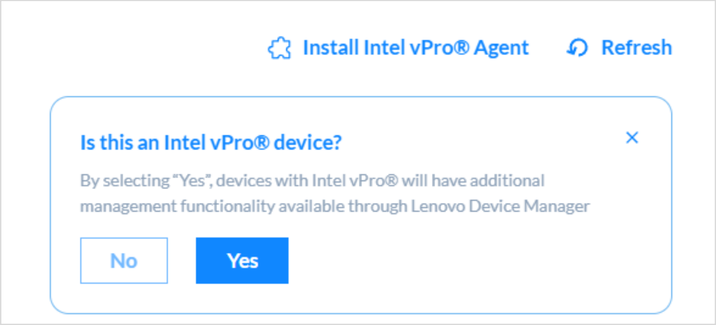
If a device was not initially identified as an Intel vPro device during the claiming/provisioning process, but can be identified as having Intel vPro, IT Admins can deploy the Intel vPro® Agent manually through Device Management / Devices / *Device Tray*. Once installed, the additional Intel EMA features and functionality will be available for the device.

To do this:

1. Select the device from the “Devices” list and open the *Device Tray*
2. Answer “Yes” to the “Is this an Intel vPro® device” question
3. The Intel vPro® agent will be deployed to the device automatically upon the next UDC check in.

Note:

- *If the question does not immediately appear or it had previously been answered with “No”, simply click on the “Install Intel vPro® Agent” option at the top of the device tray.*
- *If it is not an Intel vPro® device, or you want to wait to install the Agent on the device, select “No” or click on the “x” to close the question box. You can always go back later and select “Install Intel vPro® Agent” at the top of the device tray.*



Is this an Intel vPro® device?

By selecting "Yes", devices with Intel vPro® will have additional management functionality available through Lenovo Device Manager

Uninstalling the Intel vPro® Agent

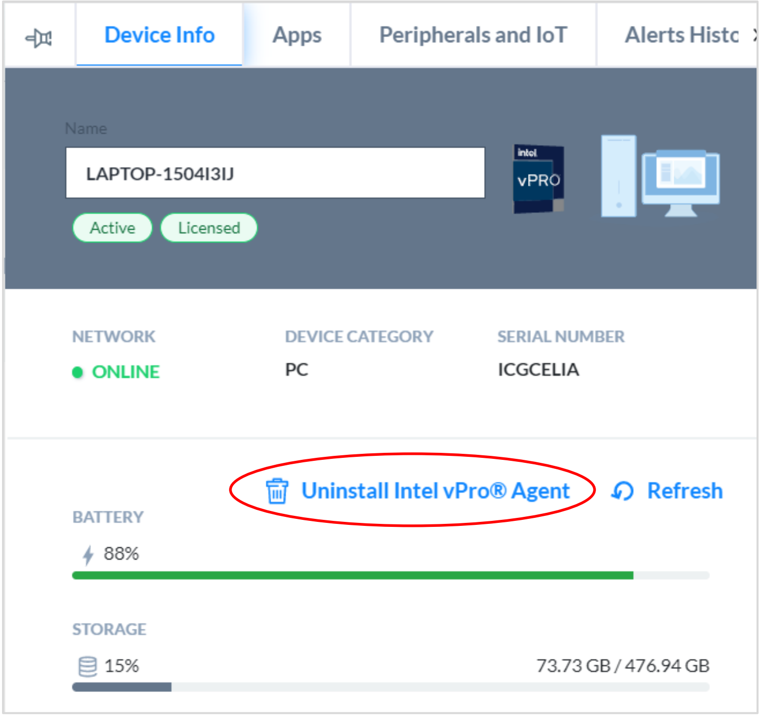
If, for any reason, the Intel vPro agent needs to be removed from a device, IT Admins can easily do so by:

1. Clicking on the **“Uninstall Intel vPro Agent”** button at the top of the device tray.

2. Confirm the uninstall. The agent will then be removed with the next device update.

Note:

- *Once uninstalled, LDM will no longer display the Intel vPro features and functionality for the device.*
- *The Intel vPro agent can be reinstalled on the device later if desired.*



Name: LAPTOP-1504I3IJ

NETWORK: ONLINE

DEVICE CATEGORY: PC

SERIAL NUMBER: ICGCELIA

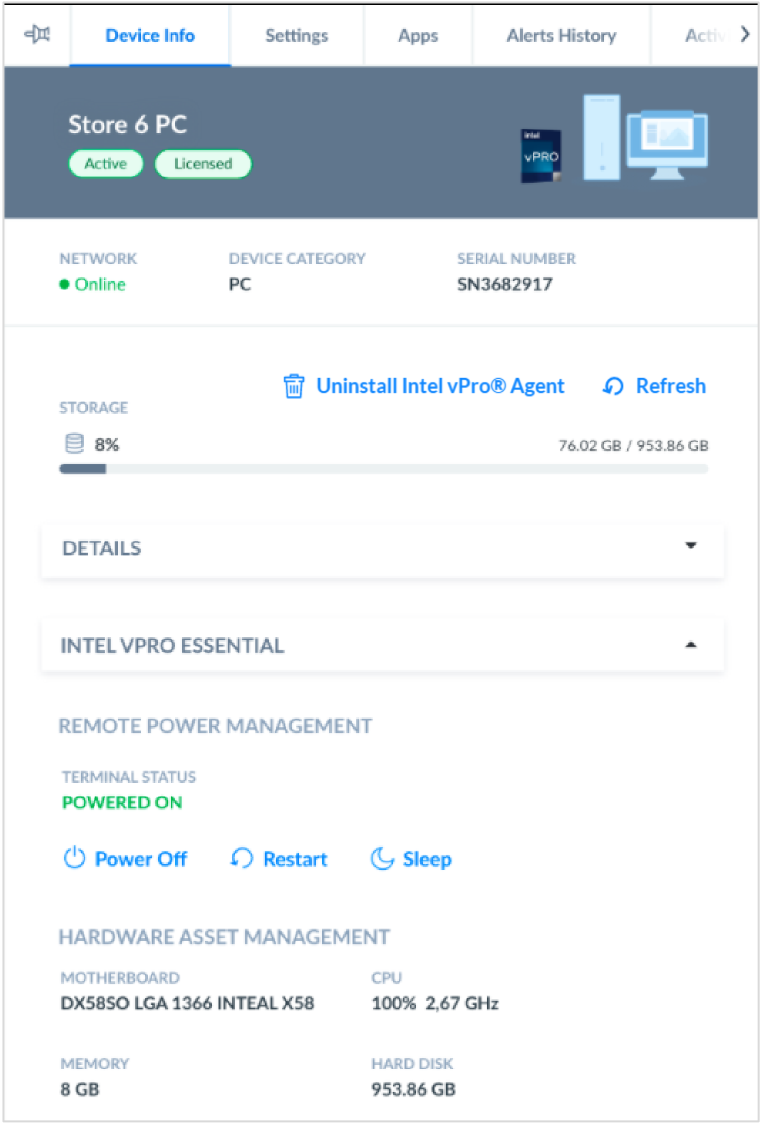
BATTERY: 88%

STORAGE: 15% 73.73 GB / 476.94 GB

Device Tray for Devices with Intel vPro® Agent Installed

Once the Intel vPro® Agent is installed on a device with the Intel vPro® chip, users will see a new section added to the Device Tray, "Intel vPro®". From here additional device information can be found on the following components:

- Motherboard
- CPU
- Memory
- Storage/HD



Store 6 PC

NETWORK: ● Online

DEVICE CATEGORY: PC

SERIAL NUMBER: SN3682917

STORAGE: 8% — 76.02 GB / 953.86 GB

REMOTE POWER MANAGEMENT

TERMINAL STATUS: POWERED ON

HARDWARE ASSET MANAGEMENT

MOTHERBOARD: DX58SO LGA 1366 INTEAL X58

CPU: 100% 2,67 GHz

MEMORY: 8 GB

HARD DISK: 953.86 GB

Power Management Added with Intel vPro®:

By selecting one of options below on the Intel vPro® section of the *Device Tray*, users can quickly and easily perform remote power management actions.

Users will be shown the progress and success or failure of an action at the top of the LDM page as well as in the "Terminal Status" on the Device Tray.

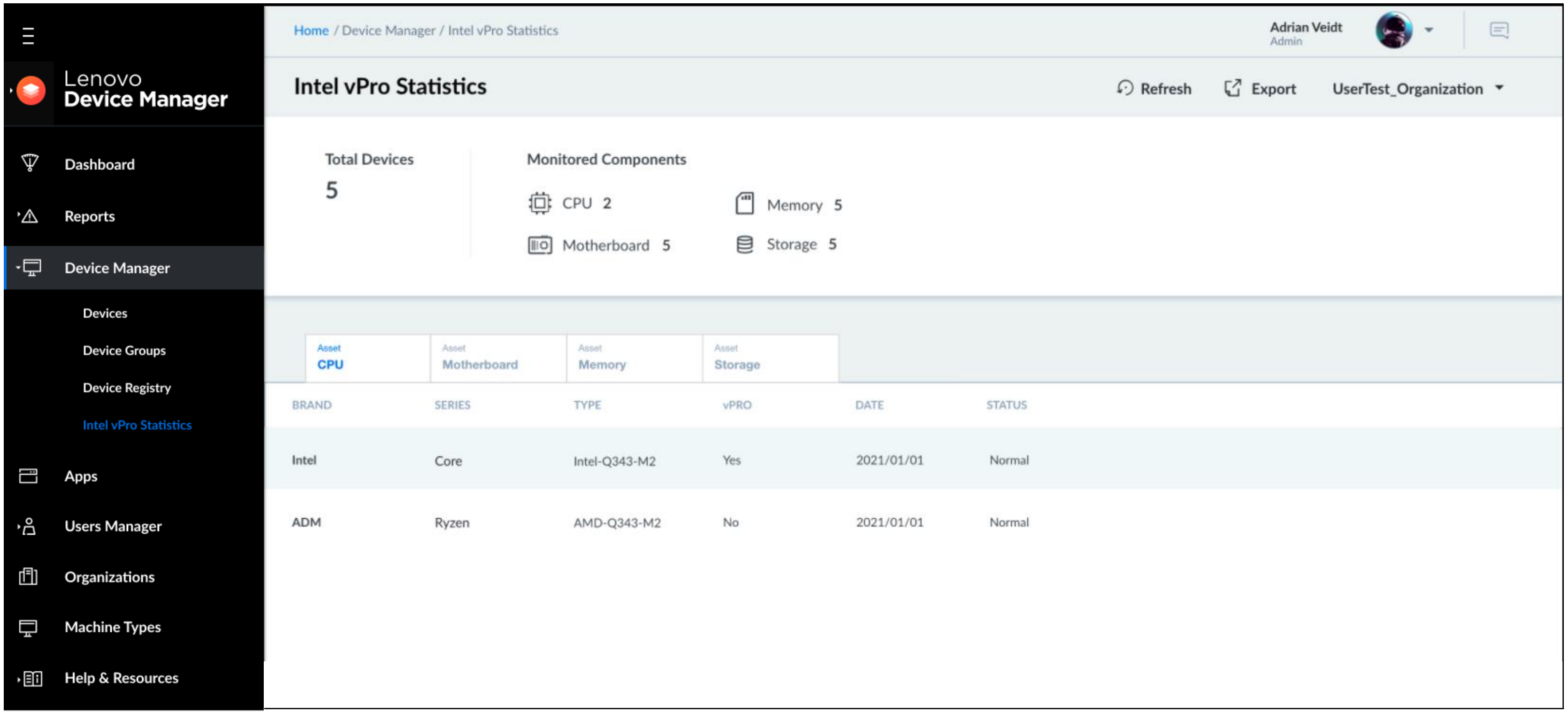
- Power On/Off
- Restart
- Sleep/Wake

Note: some power management actions may require the end user to agree to proceed with the function and may only be supported by Intel Gen 12 and above devices.

3.4.2 Intel vPro® Statistics

The Intel vPro® Statistics page summarizes the information for each Intel vPro® device and the monitored components within those devices, giving IT Admins the ability to quickly track assets and proactively manage changes. Details include the specific types and versions of the CPU, Motherboard, Memory and Storage assets currently in use within the Intel vPro® inventory. This view allows IT Admins to see which specific assets are in use in which devices. So, if an upgrade is necessary, a quick report can be pulled to schedule the change.

1. Go to Device Manager → Intel vPro® Statistics
2. Select the component type by selecting one of the tabs (CPU, Motherboard, Memory or Storage)
3. Select the asset type and a new window will display the Intel vPro® devices that have the asset
4. Select "Export" from the devices list to export the device details in a .CSV file



Intel vPro Statistics

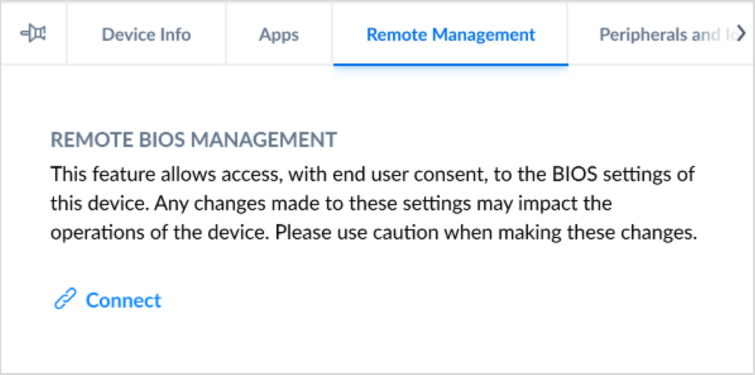
Total Devices
5

Monitored Components
CPU 2
Motherboard 5
Memory 5
Storage 5

Asset CPU | Asset Motherboard | Asset Memory | Asset Storage

BRAND	SERIES	TYPE	vPRO	DATE	STATUS
Intel	Core	Intel-Q343-M2	Yes	2021/01/01	Normal
ADM	Ryzen	AMD-Q343-M2	No	2021/01/01	Normal

3.4.3 Remote BIOS Management on Intel vPro® Devices



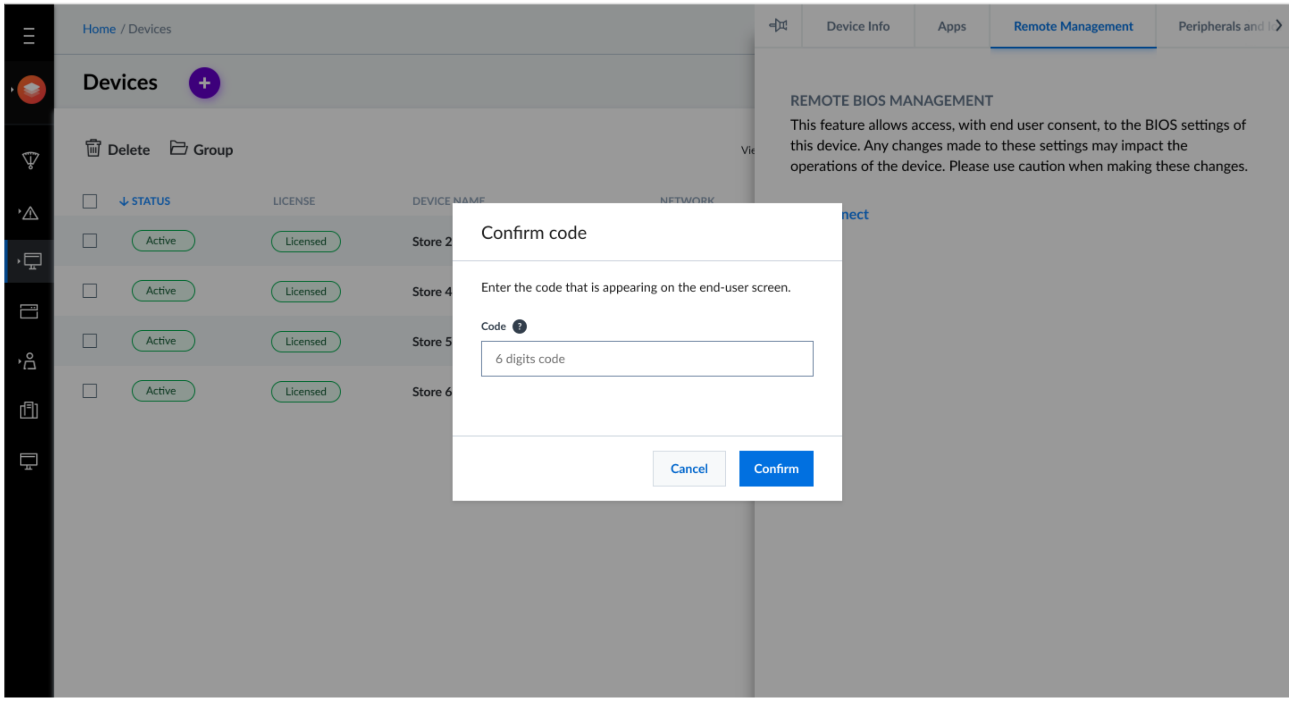
REMOTE BIOS MANAGEMENT

This feature allows access, with end user consent, to the BIOS settings of this device. Any changes made to these settings may impact the operations of the device. Please use caution when making these changes.

IT Admins can connect to an eligible end user's device through **Device Manager→Device List/*Device Tray*/Remote Management**.

The device must be online, licensed and have the Intel vPro agent installed AND it **must be attended** as a consent code must be shared between the device user and the IT Admin to gain access.

1. Click on the "Connect" button to access the device
2. Once connected, LDM will require a 6-digit consent code be entered. The IT Admin should obtain this code directly from the device end user.



	STATUS	LICENSE	DEVICE NAME	NETWORK
□	Active	Licensed	Store 2	
□	Active	Licensed	Store 4	
□	Active	Licensed	Store 5	
□	Active	Licensed	Store 6	

REMOTE BIOS MANAGEMENT

This feature allows access, with end user consent, to the BIOS settings of this device. Any changes made to these settings may impact the operations of the device. Please use caution when making these changes.

Confirm code

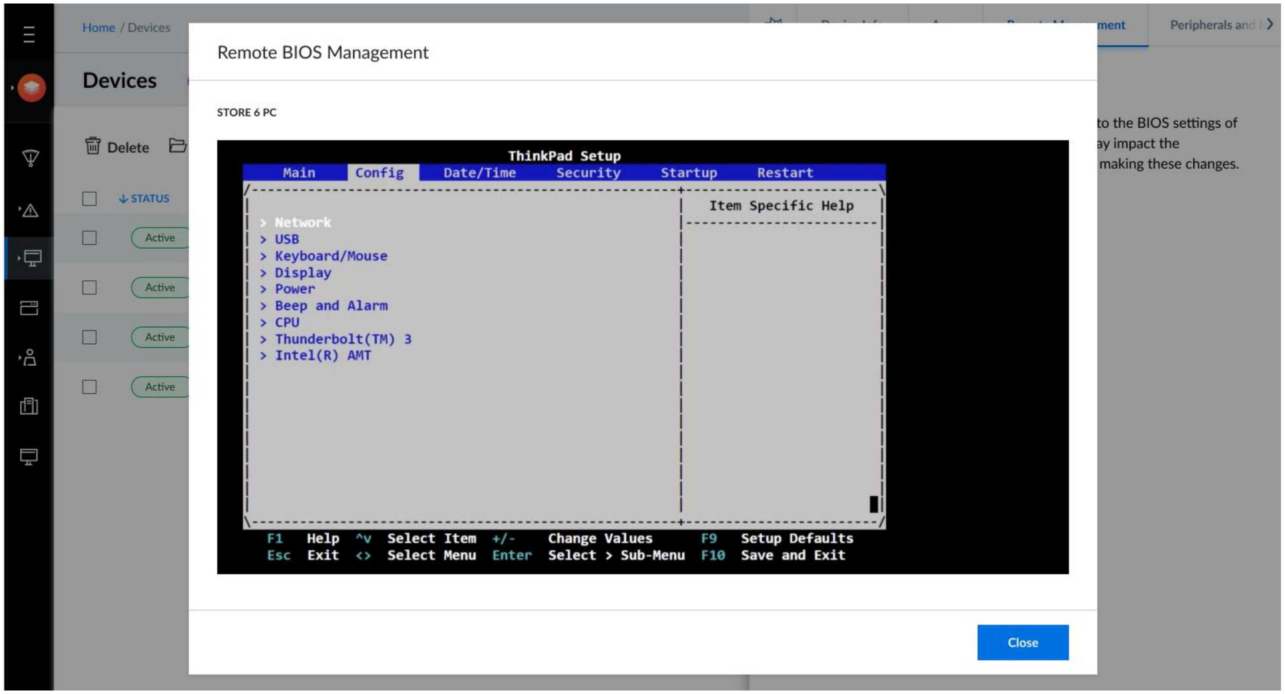
Enter the code that is appearing on the end-user screen.

Code ?

6 digits code

3. Once consent code is confirmed, LDM will access the device’s BIOS Settings via the Intel vPro EMA server.

4. BIOS Settings can then be remotely viewed and modified as needed.



Remote BIOS Management

STORE 6 PC

to the BIOS settings of
ay impact the
making these changes.

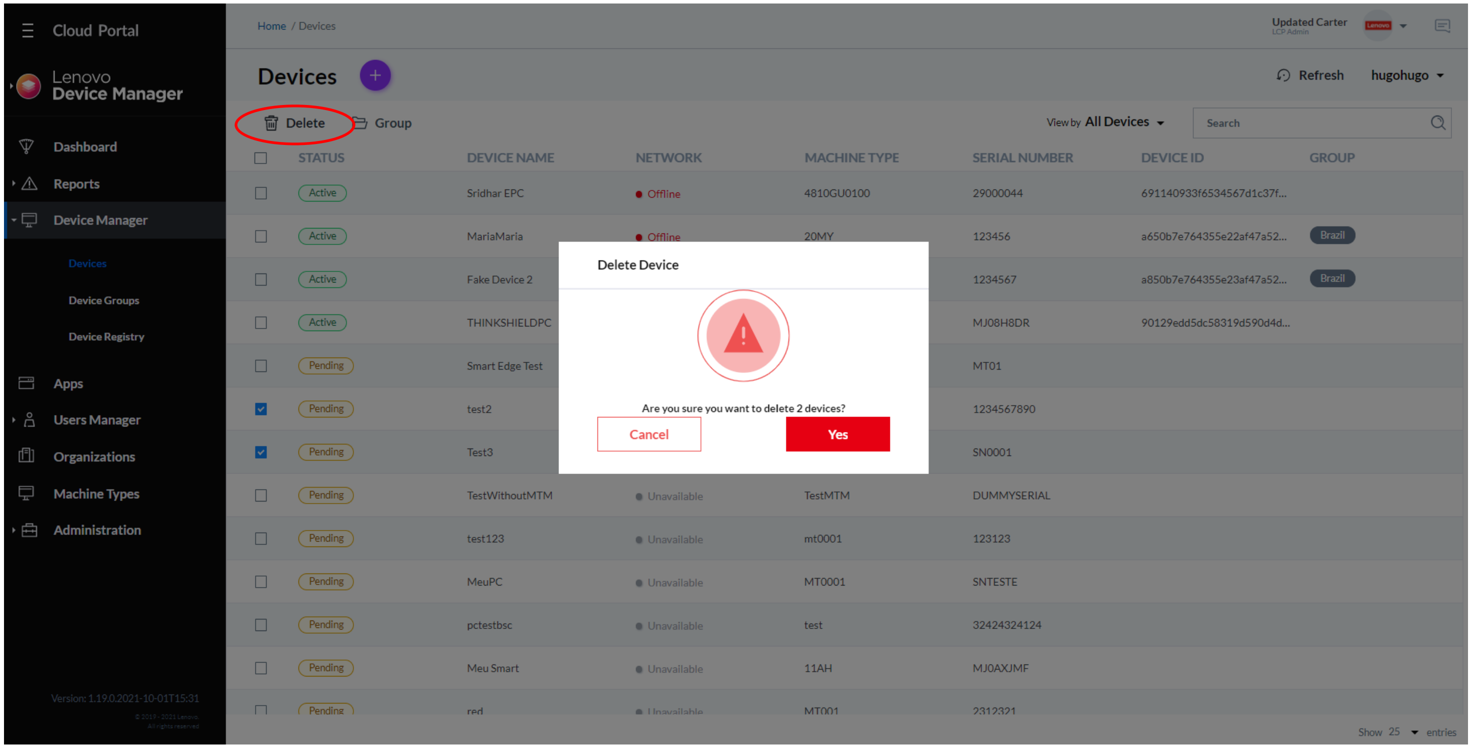
```
                         ThinkPad Setup
   Main      Config     Date/Time     Security     Startup     Restart

 > Network                                         Item Specific Help
 > USB
 > Keyboard/Mouse
 > Display
 > Power
 > Beep and Alarm
 > CPU
 > Thunderbolt(TM) 3
 > Intel(R) AMT

 F1   Help  ^v Select Item  +/-    Change Values       F9   Setup Defaults
 Esc  Exit  <> Select Menu  Enter  Select > Sub-Menu   F10  Save and Exit
```

3.5 Deleting or Removing a Device

A device should be deleted if you want to remove it from your portal, especially when ownership of the device will be transferred outside of your company.

To delete one or more devices:

1. Select the devices in the devices list
2. Click on the "Delete" button and confirm.



☐	STATUS	DEVICE NAME	NETWORK	MACHINE TYPE	SERIAL NUMBER	DEVICE ID	GROUP
☐	Active	Sridhar EPC	● Offline	4810GU0100	29000044	691140933f6534567d1c37f...	
☐	Active	MariaMaria	● Offline	20MY	123456	a650b7e764355e22af47a52...	Brazil
☐	Active	Fake Device 2			1234567	a850b7e764355e23af47a52...	Brazil
☐	Active	THINKSHIELDPC			MJ08H8DR	90129edd5dc58319d590d4d...	
☐	Pending	Smart Edge Test			MT01		
☑	Pending	test2			1234567890		
☑	Pending	Test3			SN0001		
☐	Pending	TestWithoutMTM	● Unavailable	TestMTM	DUMMYSERIAL		
☐	Pending	test123	● Unavailable	mt0001	123123		
☐	Pending	MeuPC	● Unavailable	MT0001	SNTESTE		
☐	Pending	pctestbsc	● Unavailable	test	32424324124		
☐	Pending	Meu Smart	● Unavailable	11AH	MJ0AXJMF		
☐	Pending	red	● Unavailable	MT001	2312321		

Delete Device

Are you sure you want to delete 2 devices?

Cancel Yes

After being deleted, the device will no longer be accessible in your portal. It is recommended that you uninstall the Lenovo UDC Agent (Universal Device Client) from the device if you do not intend on using the device in the portal. For instructions on how to uninstall UDC, please refer to the Device Setup Guide for uninstall instructions.

3.6 Grouping Devices

3.7 Device Registry

4 LICENSING

Lenovo Device Manager operates on a device-based SaaS model. Licenses can be purchased through standard Lenovo channels and applied to UDS / LDM. Within the LDM portal, administrators may view the licenses purchased for the organization and easily assign the licenses to devices. Devices can be claimed and provisioned but can only be fully managed through LDM once a license has been applied.

4.1 Managing Licenses

4.2 Managing License Purchases

5 APPS

5.1 App Management

5.2 Adding an Application

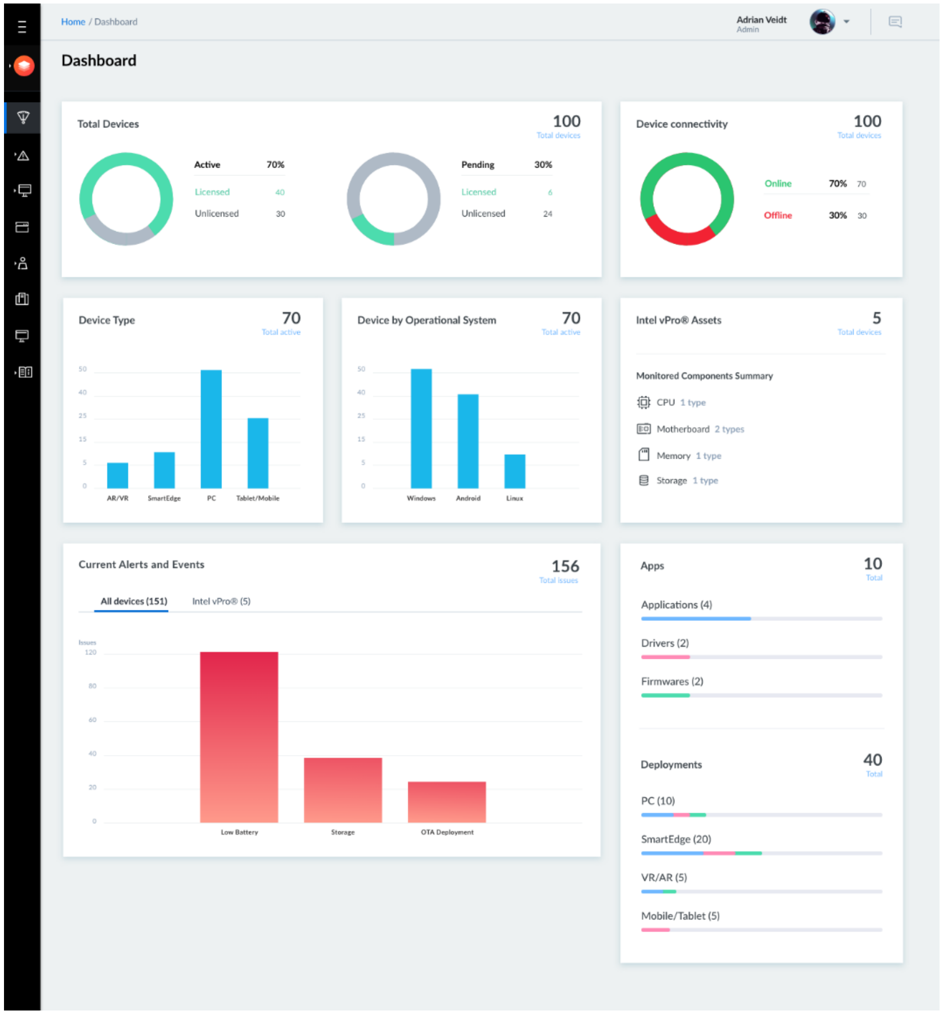
5.3 Deploying an Application

5.4 Removing an Application

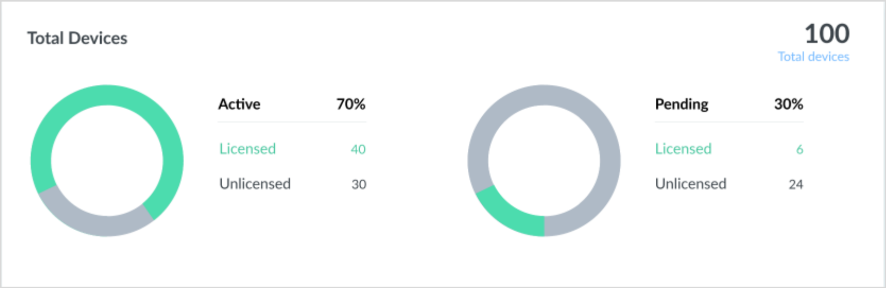
6 Lenovo Device Manager Dashboard

The Dashboard is the home page for Lenovo Device Manager and offers an at-a-glance overview of the devices in your organization. The Dashboard consists of several widgets, where each widget represents different device management categories.

Clicking on metrics displayed on a chart will typically navigate the user to the corresponding detail pages throughout the portal. This data is updated throughout the day.



Dashboard Widgets



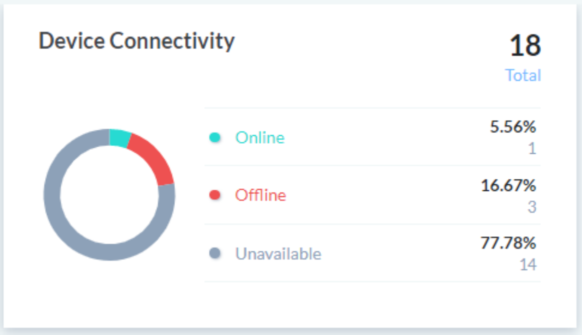
Total Devices

100
Total devices

Active	70%
Licensed	40
Unlicensed	30

Pending	30%
Licensed	6
Unlicensed	24

The total devices claimed on Lenovo Client Remote Management, highlighting licensing status. Clicking on Active or Pending charts will automatically take you to the Device list, filtered by the status selected.

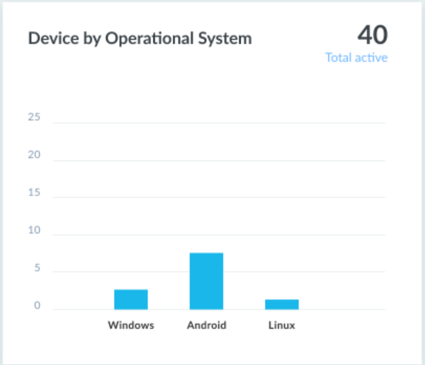


Device Connectivity

18
Total

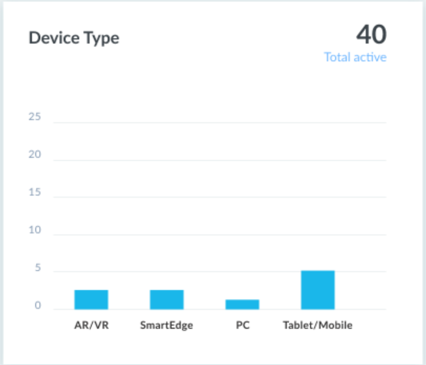
● Online	5.56% 1
● Offline	16.67% 3
● Unavailable	77.78% 14

Current connectivity status, highlighting devices that are currently online or offline. Unavailable devices have not yet been fully claimed on LDM.



Device by Operational System

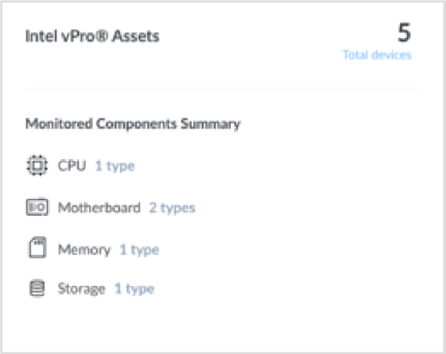
40
Total active



Device Type

40
Total active

Breakdown of devices by “Device Type” and “Operating System” allows you to track the number of each being managed through LDM.



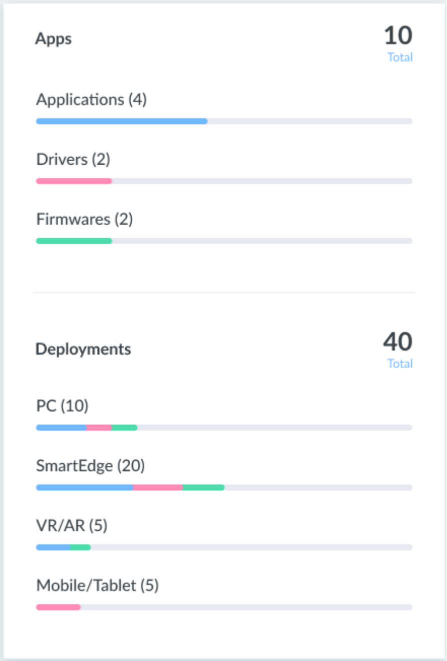
Intel vPro® Assets

5
Total devices

Monitored Components Summary

- CPU 1 type
- Motherboard 2 types
- Memory 1 type
- Storage 1 type

Summarizes the Intel vPro® device assets, including all monitored hardware components.



Apps

10
Total

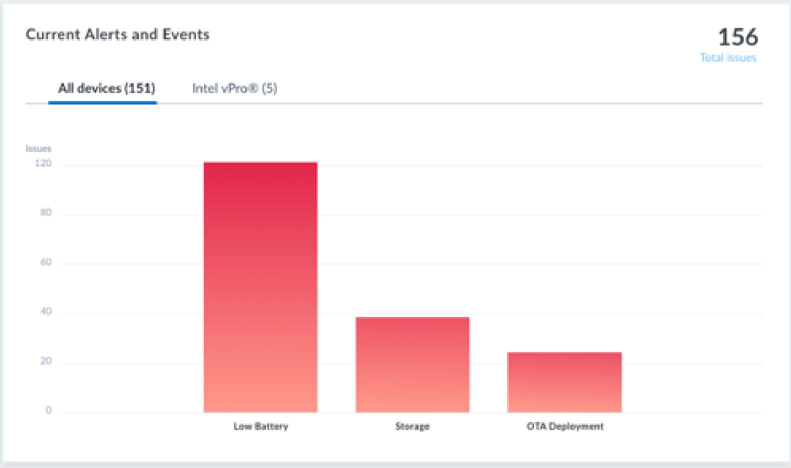
- Applications (4)
- Drivers (2)
- Firmwares (2)

Deployments

40
Total

- PC (10)
- SmartEdge (20)
- VR/AR (5)
- Mobile/Tablet (5)

Provides an overview of the different app types being managed through LDM as well as how those apps are being to deployed.



Provides information on any alerts detected over the last 7 days as of the last data update. Clicking on a category will navigate you to the issue report for that respective category, listing impacted devices. Clicking on the Intel vPro® tab will show asset change alerts. See the “Reports” section for more details on each.

7 REPORTS

7.1 Low Battery Report

7.2 Low Storage Report

7.3 OTA Deployment Report

7.4 Decommissioned Devices Report

7.5 Intel vPro® Asset Changes

8 TROUBLESHOOTING - FAQ

Question: **I am unable to login to the portal; my username or password is incorrect.**

Answer: Your login credentials must match the login setup in Lenovo ID/Lenovo Passport. If you are still having problems logging in, reset the Lenovo ID password and try again.

Question: **During device claiming (provisioning), I am asked to run a 'PowerShell' script. However, I am getting a " UnauthorizedAccess" message. What should I do?**

Answer: To execute the PowerShell script file, please run the following command to enable the PowerShell script to run with out issues:

```
Set-ExecutionPolicy Unrestricted
```

Question: **My LDM portal is not updating with device information, or my device is showing "Offline". What should I do?**

Answer: This typically happens when the Universal Device Client (UDC) has stopped running on the device. To fix:

1. On CMD prompt, run 'services.msc' command
2. When Services application opens, you will see a list of services. Search for 'Universal Device Client'.
3. Check the status column. If status does not show "Running" it needs to be restarted.

4. Highlight the Universal Device Client and right click and select ‘Restart’ to start the service. This is an automatic service so it will start updating the LDM portal soon after.

Question: **I see “Information not currently available. Device network still pending” message on my Device Tray. What should I do?**

Answer: Contact you Org Admin to assign a License to this device. A license may need to be purchased if none are currently available for the organization.

Question: **My device has been in “Pending” state for a long time. Why is it not active?**

Answer: This issue occurs if device has not been provisioned properly and UDC has not been installed. First, check that the serial number and model for the device are correct. If all is correct, contact Lenovo to investigate further.

Question: **I installed the Intel vPro® agent on a device and I want to uninstall it. How can I do this?**

Answer: Remote uninstallation of the Intel vPro® agent is not currently support. This feature will be added in the next release. For now, removing the agent will require manual interaction with the device.

Question: **When claiming a device and “Downloading Provisioning Pack”, I receive the message: “An error occurred. Please try again”. What do I do?**

Answer: Please wait 10 minutes and try again. If the problem persists, contact Lenovo to investigate further.

9 Reference Documents

Terms & Conditions: Available on LDM portal “Preferences”

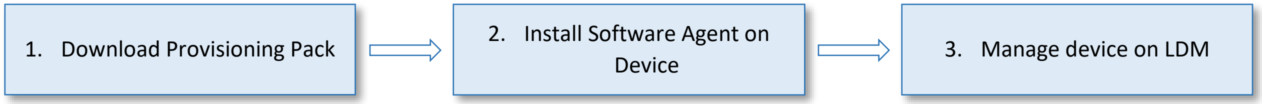
Lenovo Privacy Policy

Lenovo Software as a Service Cloud Agreement

10 LDM Quick Start Guide

Overview

The purpose of this guide is to help you smoothly onboard one or more devices in your organization to the Lenovo Device Manager platform.



1. Download Provisioning Pack
2. Install Software Agent on Device
3. Manage device on LDM

> Note for New User: To set up a new LDM account, it is mandatory to have a Lenovo ID and get an email invitation registered with Lenovo. Once admin account is set up, the administrator can invite other users within the organization to create accounts based on the roles and permissions granted to them.

You can onboard one or more devices to LDM platform through the LDM→Device Management / Devices page. This process may vary based on the device type and operating system as described below. This guide will provide quick instructions for each category type.

	Current Device Type Categories			
	PCs	**SmartEdge**	**Tablet / Mobile**	**AR / VR**
Examples	Any Lenovo notebook, desktop, workstation, etc	Any Lenovo edge appliance and servers	Any Lenovo tablets or mobile device	Any Lenovo AR or VR appliance
Current Install Options	• Automatically with Provisioning Package download	• Automatically with Provisioning Package download	• Automatically with QR code scan	Currently Unavailable in LDM 2.1 *Will return in LDM 2.2*

The UDC software agent bundle includes:

- UDC setup zip file
- Provisioning token
- Provisioning script (ps1)
- Config policy files
- Readme file

10.1 Add Windows Devices

10.2 Add Android Devices

10.3 Installing the Intel vPro® Agent

10.4 Requirements

10.5 Troubleshooting

11 App Package – Example PowerShell Script

Custom package creation allows you to package and deploy applications and policies to your devices using the specifications outlined in Section 5.2.2 of this User Guide. For reference, use the following PowerShell script as an example:

```
Param(
   [string]$command="install"
)
$pathToSelf = Split-Path -Parent -Path $PSCommandPath

$pathToLogFile = "$($env:TEMP)\Lenovo.AppPerformance.Package-$(Get-Date -Format 'yyyy-MM-dd_HH-mm-ss').txt"
$taskName = "Lenovo App Performance Task"
$taskFolder = "Lenovo"
$pathToService = "$($env:ProgramData)\Lenovo\Ldi\Performance"
$pathToServiceParent = Split-Path -Parent $pathToService
$pathToRegistry = "HKLM:\Software\Lenovo\Ldi"
$relativePathToLog = "Lenovo\Ldi"

function Write-Log
{
   Param(
      [string]$logString,
      [switch]$isError
   )

   $log = (Get-Date -Format s).ToString() + ": " + $logString
```

```
    Add-Content $pathToLogFile -value $log

    if($isError.IsPresent) {
        Write-Error $log
    }else{
        Write-Host $log
    }
}

function Assert-Elevation()
{
    $isAdminOrSystem = ([Security.Principal.WindowsPrincipal] `
      [Security.Principal.WindowsIdentity]::GetCurrent() `
    ).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)

    if(-not ($isAdminOrSystem))
    {
        Write-Log "Error: This script requires elevation" -isError
        exit 1
    }
}

function Set-FolderSecurity {
    Param(
        [Parameter(Mandatory = $true)]
        [string]$path
    )
    $fullControlEnum = [System.Security.AccessControl.FileSystemRights]::FullControl
    $readExecuteEnum = [System.Security.AccessControl.FileSystemRights]::ReadAndExecute
    $allowEnum = [System.Security.AccessControl.AccessControlType]::Allow
    $inheritanceFlag = [System.Security.AccessControl.InheritanceFlags]::ObjectInherit -bor
[System.Security.AccessControl.InheritanceFlags]::ContainerInherit
    $propagationFlag = [System.Security.AccessControl.PropagationFlags]::None

    if (-not (Test-Path $path -PathType Container)) {
        New-Item -Path $path -ItemType Directory
    }
    $acl = Get-Acl -Path $path

    # takeown
    $adminGroup = New-Object System.Security.Principal.NTAccount("Builtin", "Administrators")
    $acl.SetOwner($adminGroup)

    # disable inheritance from parent folder
    $isProtected = $true
    $preserveInheritance = $false
    $acl.SetAccessRuleProtection($isProtected, $preserveInheritance)

    # set permission for different user and group
    $adminAccessRule = New-Object -TypeName System.Security.AccessControl.FileSystemAccessRule -ArgumentList "BUILTIN\Administrators",
$fullControlEnum, $inheritanceFlag, $propagationFlag, $allowEnum
    $systemAccessRule = New-Object -TypeName System.Security.AccessControl.FileSystemAccessRule -ArgumentList "NT AUTHORITY\SYSTEM",
$fullControlEnum, $inheritanceFlag, $propagationFlag, $allowEnum
    $userAccessRule = New-Object -TypeName System.Security.AccessControl.FileSystemAccessRule -ArgumentList "BUILTIN\Users",
$readExecuteEnum, $inheritanceFlag, $propagationFlag, $allowEnum

    $acl.AddAccessRule($adminAccessRule)
    $acl.AddAccessRule($systemAccessRule)
    $acl.AddAccessRule($userAccessRule)

    Set-Acl -Path $path -AclObject $acl

    # Grant permission to avoid no enough permission when uninstall
    $acl.SetAccessRuleProtection($false, $true)
    Get-ChildItem $path -Recurse -Force | ForEach-Object { Set-Acl -Path $_.FullName -AclObject $acl }
}

function Install()
{
    Uninstall
    Copy-Service
    Add-ScheduledTask
}

function Copy-Service()
```

```
{
    Set-FolderSecurity $pathToServiceParent
    Copy-Item $pathToSelf\bin\ai\ $pathToService -Force -Recurse
    if(-not (Test-Path $pathToService -PathType Container))
    {
        Write-Log "Error: Can not copy service to $pathToService" -isError
        exit 1
    }
}

function Add-ScheduledTask()
{
    $triggerTime = "12:00"
    $taskCommand = Join-Path $pathToService 'Lenovo.AppPerformance.exe'
    $taskParameter = ' '
    $settings = New-ScheduledTaskSettingsSet -DontStopIfGoingOnBatteries
    $principal = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Users"

    $action = New-ScheduledTaskAction -Execute $taskCommand -Argument $taskParameter -WorkingDirectory $pathToService
    $triggers =  @(
        $(&{
            $dailyTrigger = $(New-ScheduledTaskTrigger -Daily -At $triggerTime)
            $dailyTrigger.StartBoundary = [DateTime]::Parse($dailyTrigger.StartBoundary).ToLocalTime().ToString("s")
            $dailyTrigger
        }),
        $(&{
            $logonTrigger = $(New-ScheduledTaskTrigger -AtLogon)
            $logonTrigger.delay = 'PT15M'
            $logonTrigger
        })
    )

    if(-not (Test-path $taskCommand)) {
        Write-Log "Error: Can not find necessary task target $taskCommand " -isError
        exit 1
    }

    Remove-ScheduledTask
```

```
   Register-ScheduledTask -TaskName $taskName -TaskPath $taskFolder -Action $action -Trigger $triggers -Settings $settings -Principal $principal

   if (-not ($(Get-ScheduledTask -TaskName $taskName -ErrorAction SilentlyContinue).TaskName -eq $taskName)) {
      Write-Log "Error: Can not create scheduled task." -isError
      exit 1
   }
}

function Uninstall()
{
   Remove-ScheduledTask
   Remove-RegistryKey
   Remove-LogFile

   Set-FolderSecurity $pathToServiceParent
   if (Test-Path $pathToService)
   {
      Remove-Item $pathToService -Recurse -Force
   }
   if (-not (Test-Path (Join-Path $pathToServiceParent "*")))
   {
      Remove-Item $pathToServiceParent -Recurse -Force
   }
}

function Remove-ScheduledTask()
{
   if ($(Get-ScheduledTask -TaskName $taskName -ErrorAction SilentlyContinue).TaskName -eq $taskName) {
      Unregister-ScheduledTask -TaskName $taskName -Confirm:$False
   }
}

function Remove-RegistryKey()
{
   if (Test-Path $pathToRegistry)
   {
      Remove-Item $pathToRegistry -Recurse -Force
   }
```

```
}

function Get-AppDataFolderForAllUsers()
{
  $folderName = "Local Appdata"

  $userProfileList = Get-ItemProperty "Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\*" -Name
"ProfileImagePath" `
  | Where-Object PsChildName -Match "^S-1-5-21.*" `
  | Select-Object PSChildName, ProfileImagePath

  return $userProfileList | ForEach-Object {
    $userShellFoldersKey = "Registry::HKEY_USERS\" + $_.PSChildName + "\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders";
    if (Test-Path $userShellFoldersKey) {
      $unexpandedFolderPath = (Get-Item $userShellFoldersKey).GetValue($folderName, `
          [System.String]::Empty, `
          [Microsoft.Win32.RegistryValueOptions]::DoNotExpandEnvironmentNames)
      return $unexpandedFolderPath -replace "%USERPROFILE%", $_.ProfileImagePath
    }
  }
}

function Remove-LogFile()
{
  Get-AppDataFolderForAllUsers | ForEach-Object {
    $userLogFolder = Join-Path $_ $relativePathToLog
    if (Test-Path $userLogFolder) {
      Remove-Item $userLogFolder -Recurse -Force
    }
  }
}

if($command -eq "install")
{
  Assert-Elevation
  Install
}
```

```
if($command -eq "uninstall")
{
   Assert-Elevation
   Uninstall
}
```