Lenovo Device Manager (LDM)
User Guide

Name of Document	LDM User Guide
Version Number	V2.1
Release Date	28 July 2022
Modifications/Additions	1. Org Setup: Updated portal URL format 2. Org Settings section added under Manage Organization 3. Intel vPro® Agent Installation • Device Claiming process: Automatic installation of Intel vPro Agent (Quick Start Guide) • Account Preferences/Org Settings: Enabling/Disabling automatic install of Intel vPro Agent • Intel vPro Section 4. Automated App Package Creation 5. Claiming Process updated for Android Devices (Quick Start Guide) 6. Updated User role permissions (IT Admin) for license assignments 7. UX enhancements (images updated) on: • Device Management/Devices/Device Tray/*Device Info* • User Management/Users/*List* & Users/*Add User*

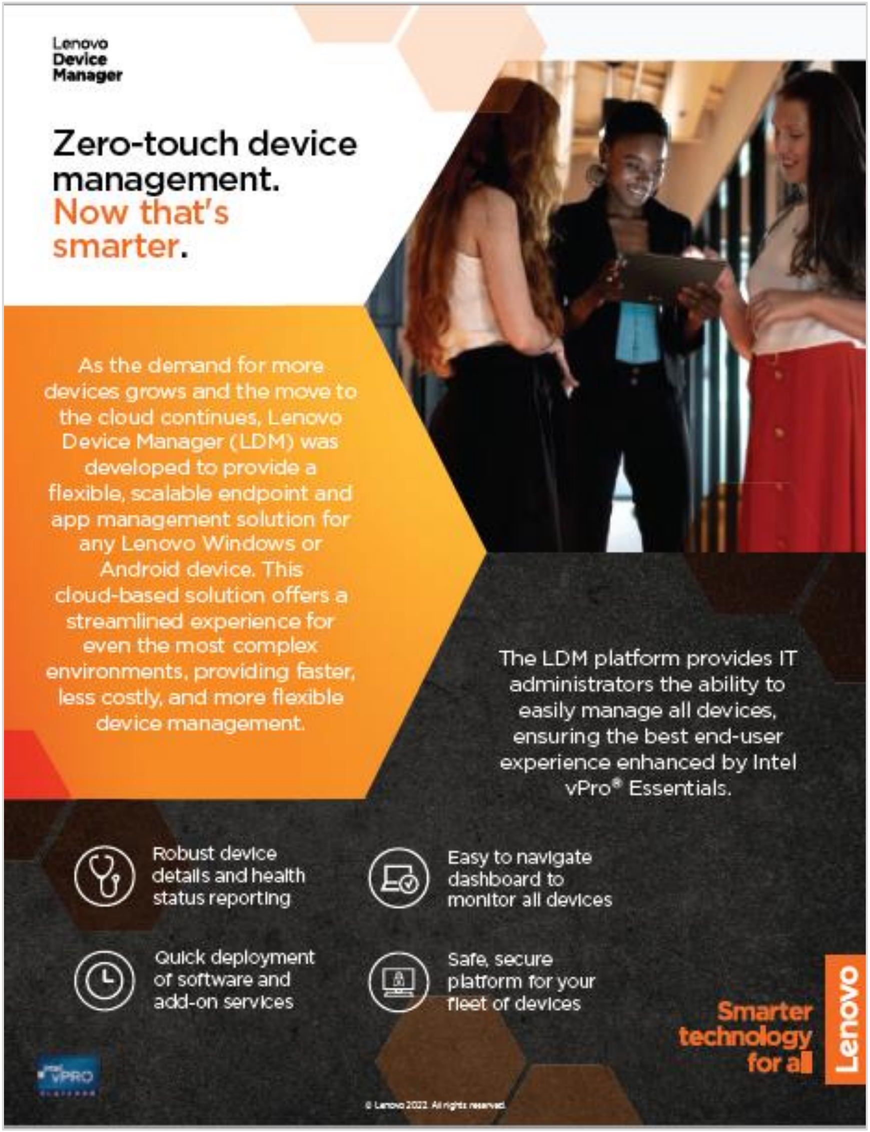
Contents

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

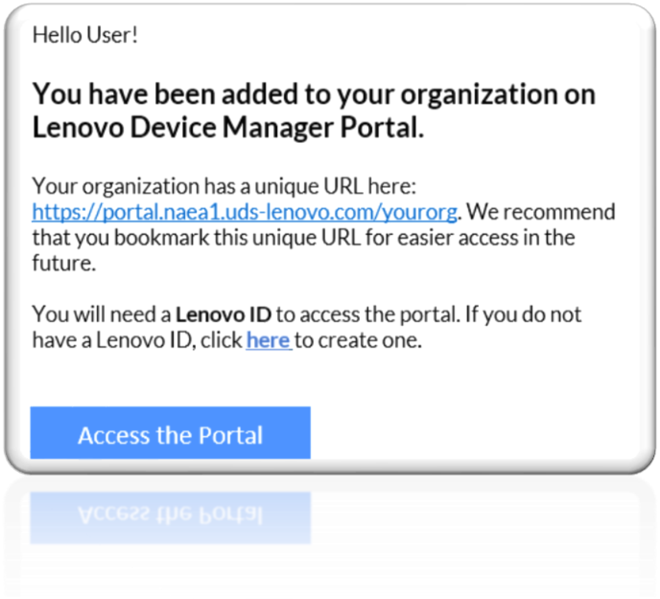
Lenovo

© 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

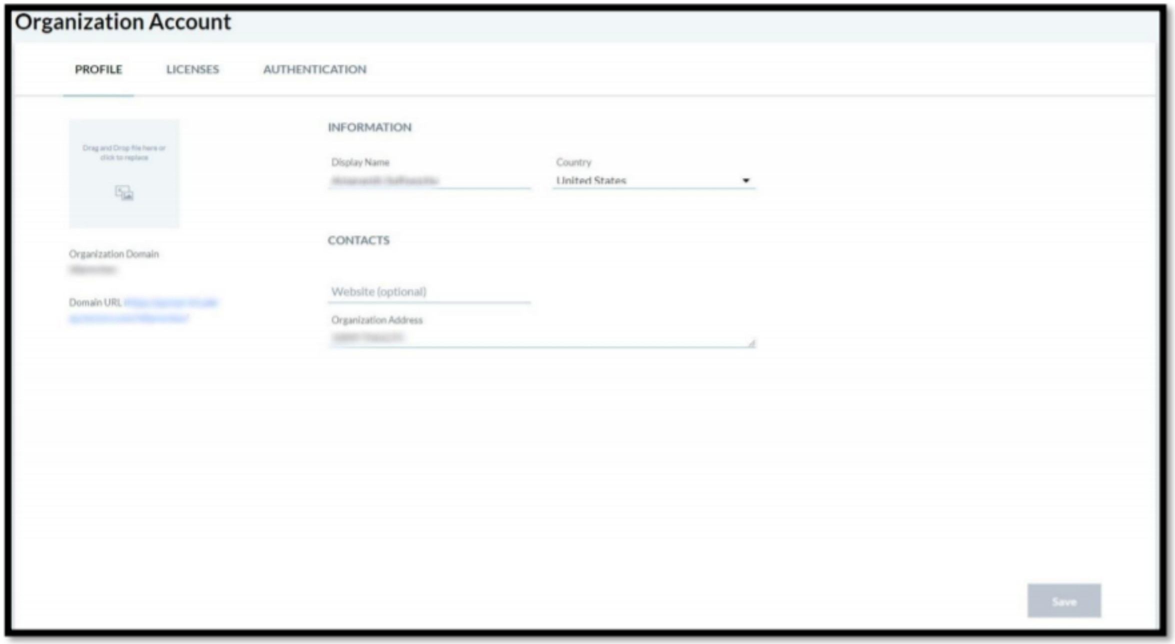
2.2 Manage Organization

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



Organization Account

INFORMATION

Display Name: [redacted]

Country: United States

Organization Domain: [redacted]

Domain URL: [redacted]

CONTACTS

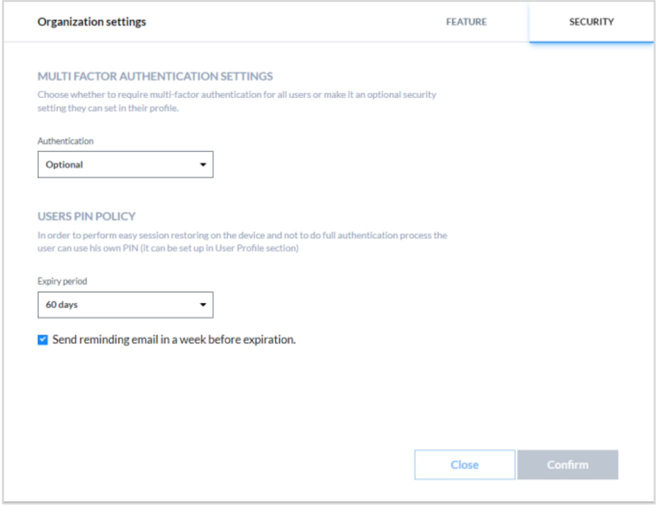
Website (optional)

Organization Address: [redacted]

2.2.2 Organization Settings

Customized feature and security 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:

- Security Settings
  - Multi-factor Authentication
  - User PIN Policy
- Feature Settings
  - *Coming in LDM 2.2*



MULTI FACTOR AUTHENTICATION SETTINGS

Choose whether to require multi-factor authentication for all users or make it an optional security setting they can set in their profile.

Authentication: Optional

USERS PIN POLICY

In order to perform easy session restoring on the device and not to do full authentication process the user can use his own PIN (it can be set up in User Profile section)

Expiry period: 60 days

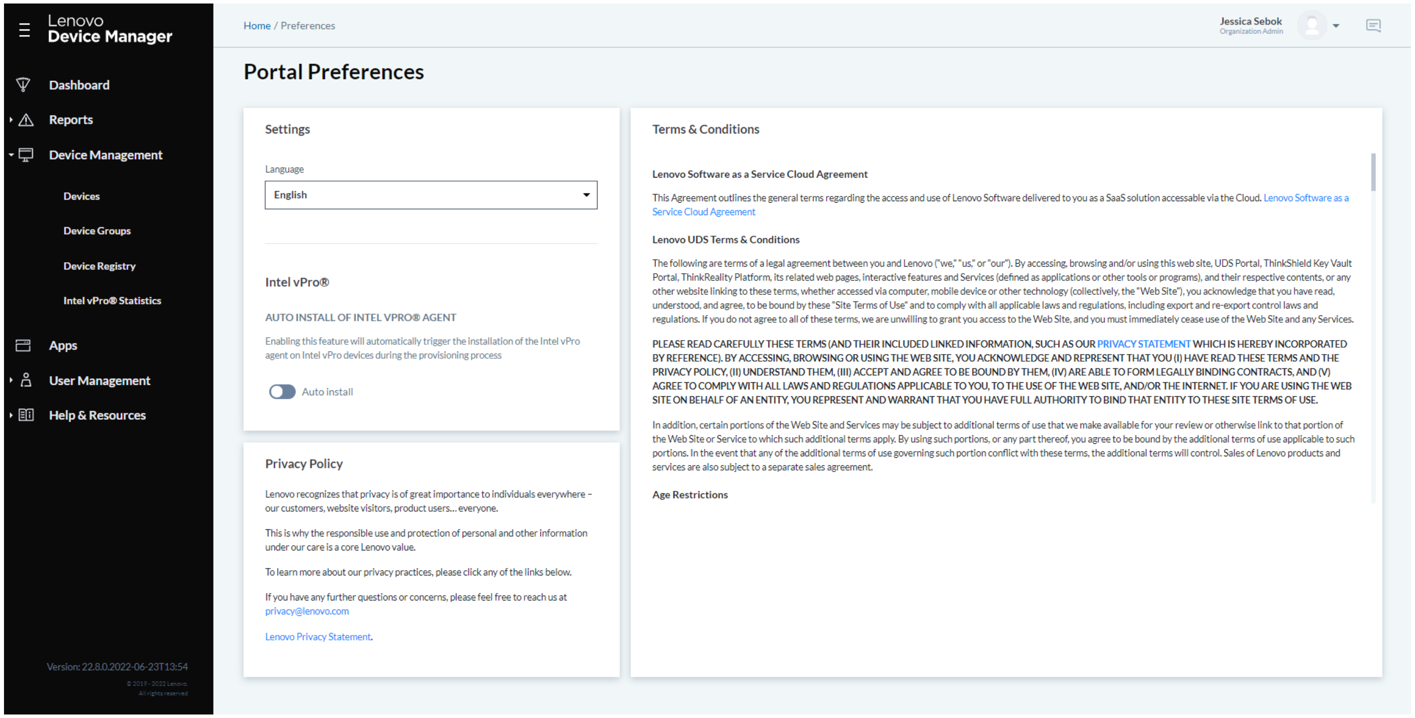
☑ Send reminding email in a week before expiration.

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

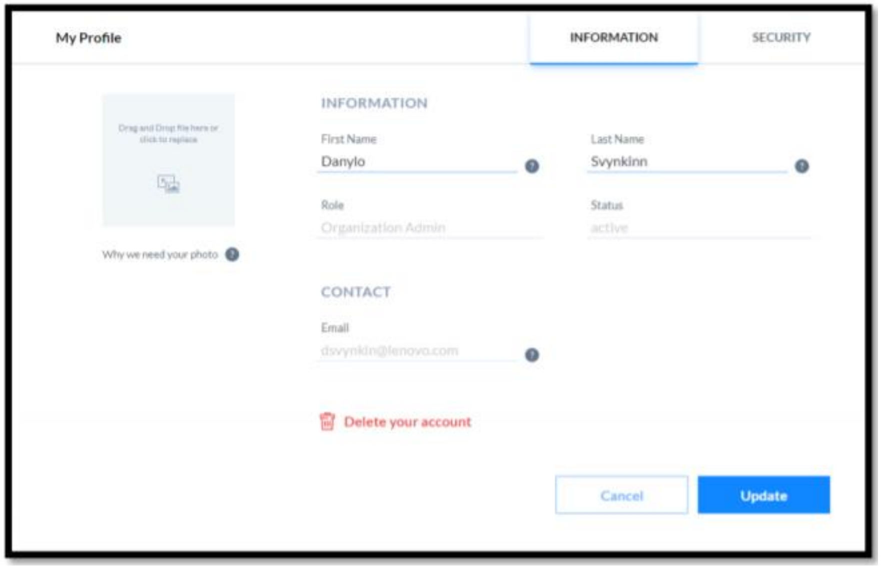
2.4 User Management

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

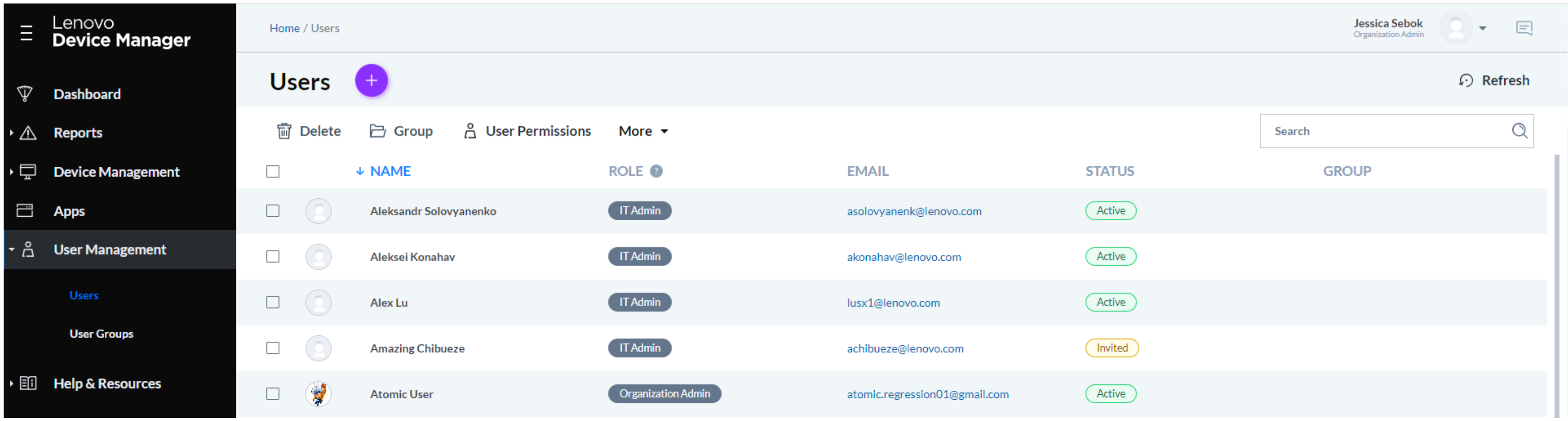
Delete your account

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

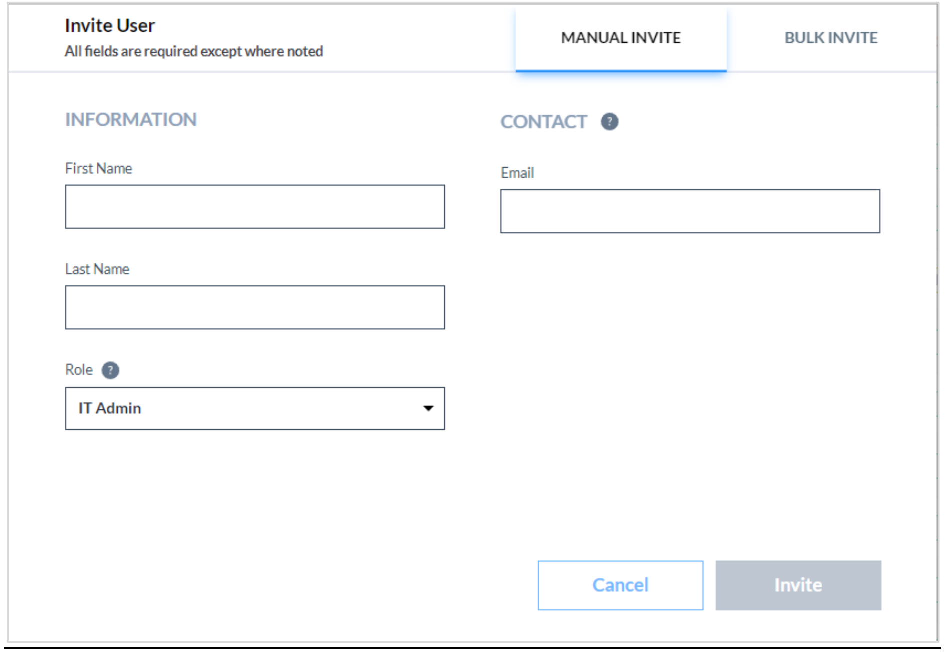
2.4.2 Adding, Updating & Deleting Users on an Organization

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

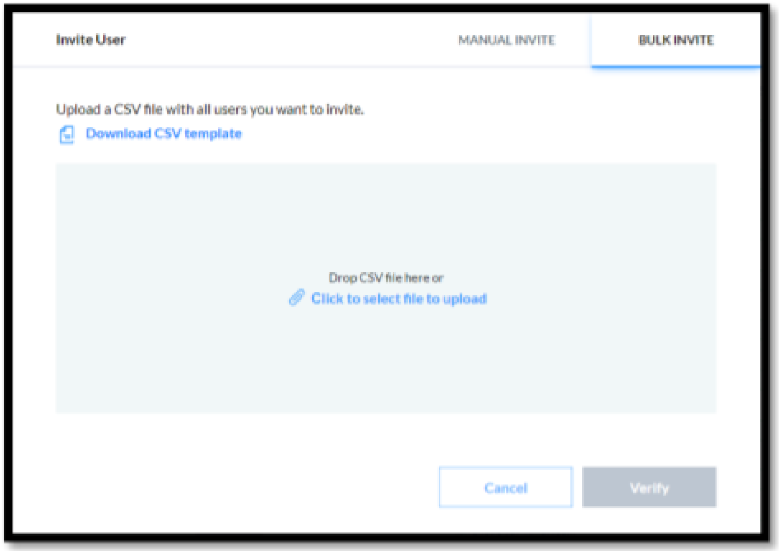
IT Admin

To add user(s) in bulk:

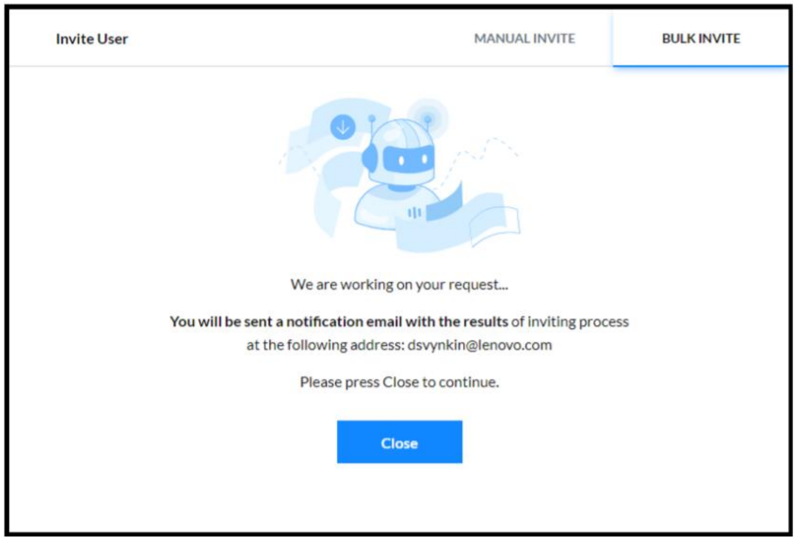
1. Click on button "+"
2. Select "Bulk Invite" tab
3. Download CSV template by clicking on "Download CSV template" button
4. Populate CSV file with required info for each user - First Name, Last Name, Role and Email

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.



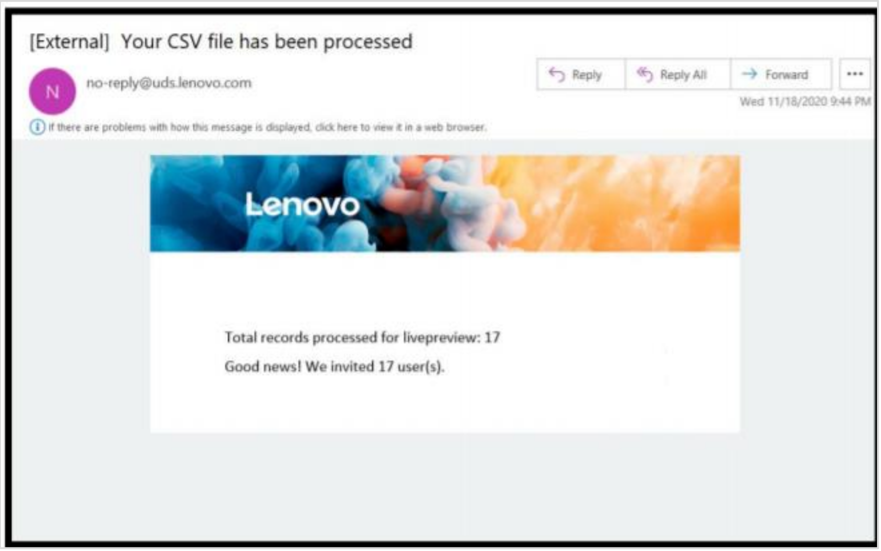
We are working on your request...

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**)

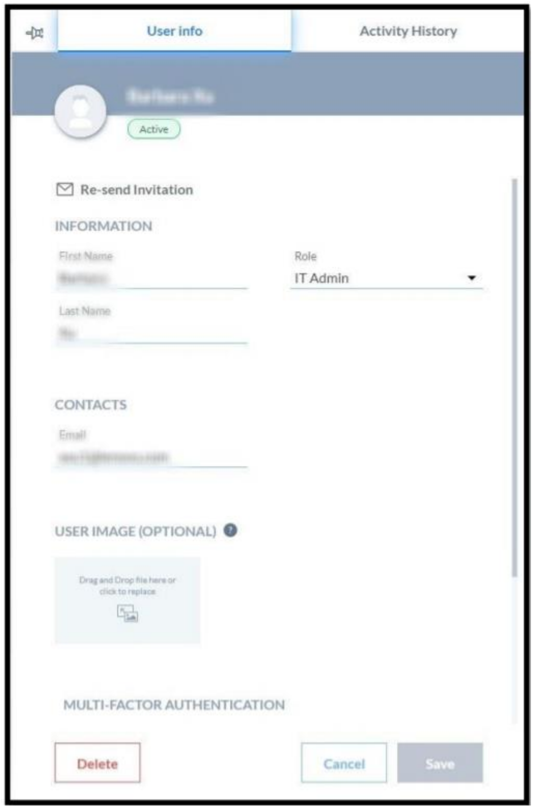
Each user must select the checkbox and accept each agreement before gaining access to the LDM portal.

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]

Active

INFORMATION

First Name: [redacted]

Role: IT Admin

Last Name: [redacted]

CONTACTS

Email: [redacted]

USER IMAGE (OPTIONAL)

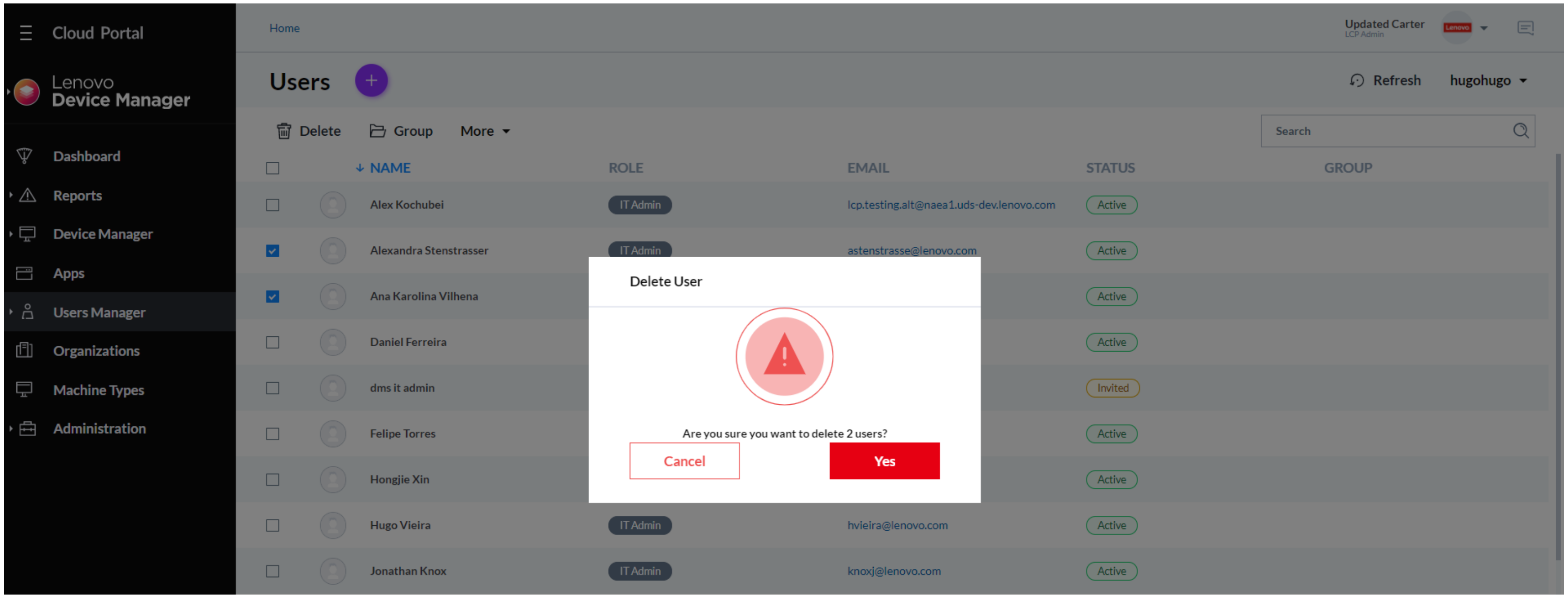
Drag and Drop file here or click to replace

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

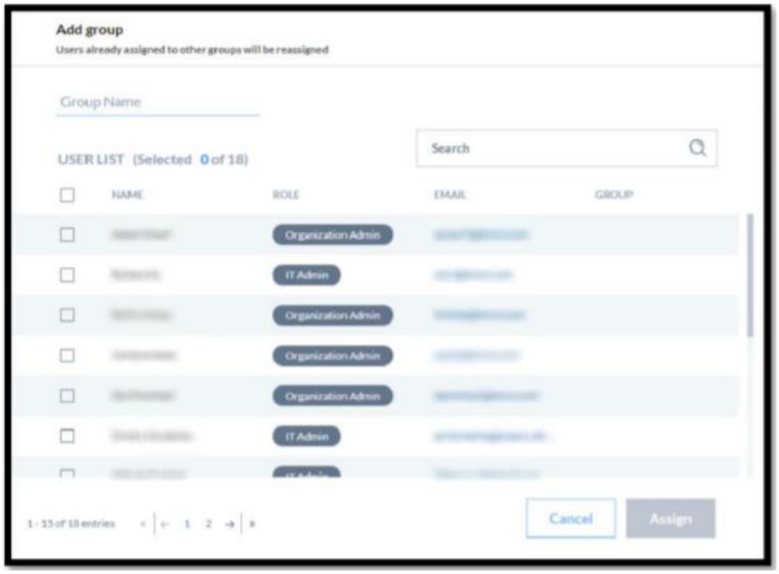
User Groups

Grouping users is helpful for managing a large number of users - typically by geography, department, or role. User groups can be managed in your portal by accessing **Users Manager → User Groups**.

Create User Group:

To create user group:

1. On the User Groups page click on ✚ ("Create group") button.
2. Fill in field "Group Name" in the opened window.



Add group

Users already assigned to other groups will be reassigned

Group Name

USER LIST (Selected 0 of 18)

Search

□	NAME	ROLE	EMAIL	GROUP
□	[illegible]	Organization Admin	[illegible]	
□	[illegible]	IT Admin	[illegible]	
□	[illegible]	Organization Admin	[illegible]	
□	[illegible]	Organization Admin	[illegible]	
□	[illegible]	Organization Admin	[illegible]	
□	[illegible]	IT Admin	[illegible]	

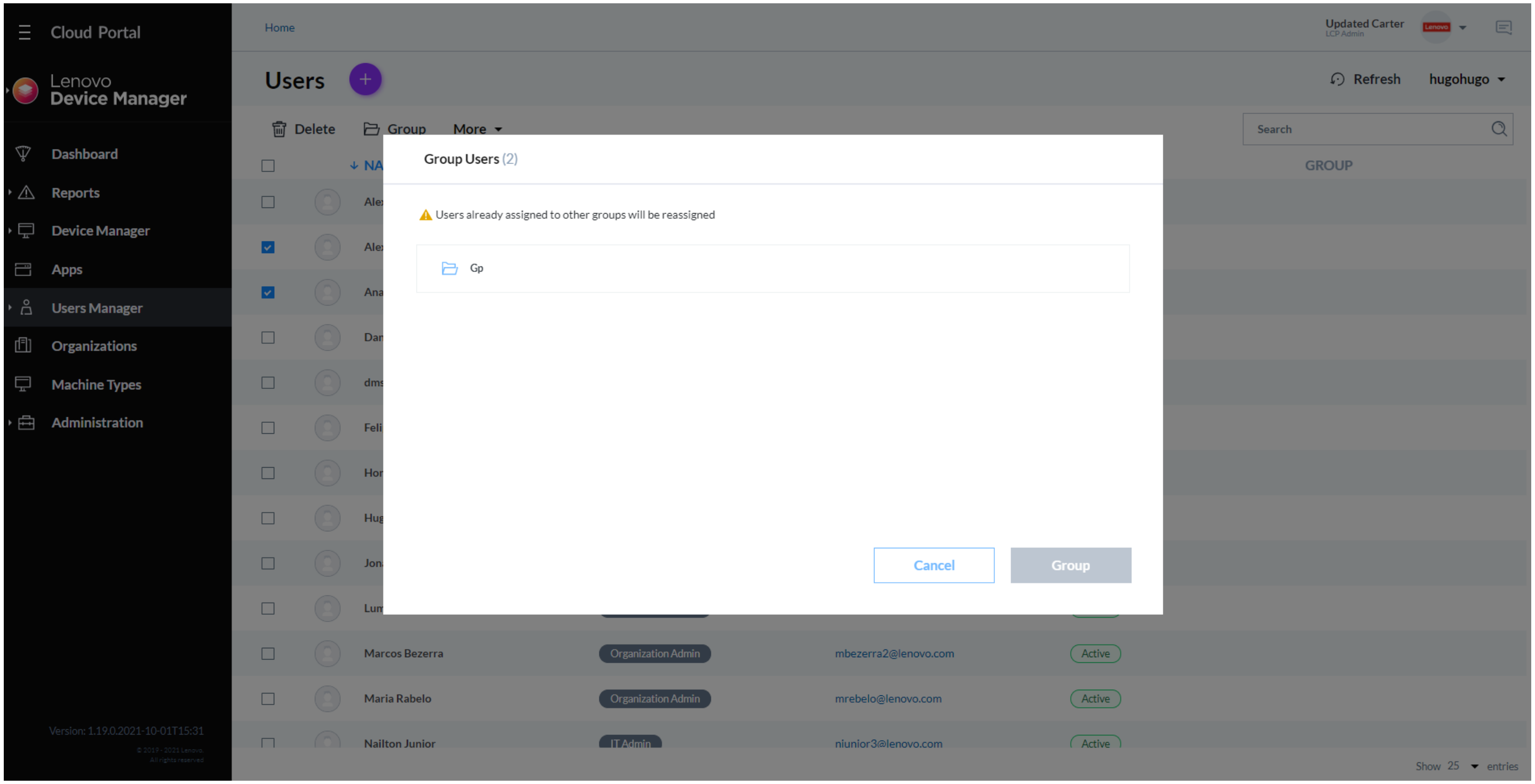
1 - 15 of 18 entries

3. Select users you want to assign to this group (not required step).
4. Click on button “Assign”

Assign User(s) to a User Group from the Users page

To assign a User to a User Group you need to:

1. Add a Check next to the User(s) which you want to assign to a User Group and click on button "Group" at the top of the page.
   Note: A User can be assigned to an existing group only. Please see the User Groups section for more information on how to create a group.
2. Select the group you want to assign the user(s) to and click on button "Assign".
   Note: Any users already assigned to other groups will be reassigned to the current group as a result of this action.



Group Users (2)

⚠ Users already assigned to other groups will be reassigned

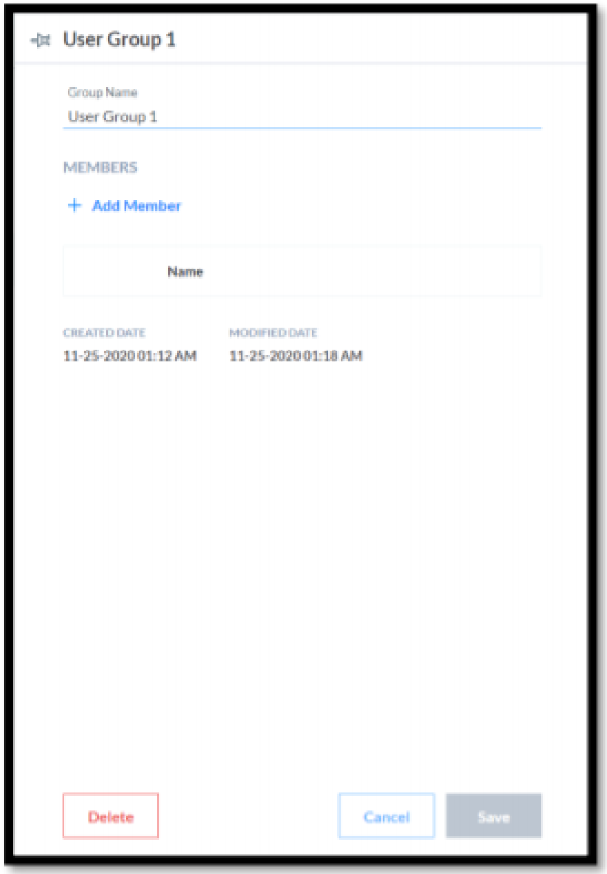
	NA				GROUP
□	Marcos Bezerra	Organization Admin	mbezerra2@lenovo.com	Active	
□	Maria Rabelo	Organization Admin	mrebelo@lenovo.com	Active	
□	Nailton Junior	IT Admin	njunior3@lenovo.com	Active	

Managing User Groups

To manage or update group info, click on a group to open user group tray.

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

- Update group name
- Add new user(s) to the group
- Delete user(s) from the group
- Delete a group



User Group 1

Group Name: User Group 1

MEMBERS

Name

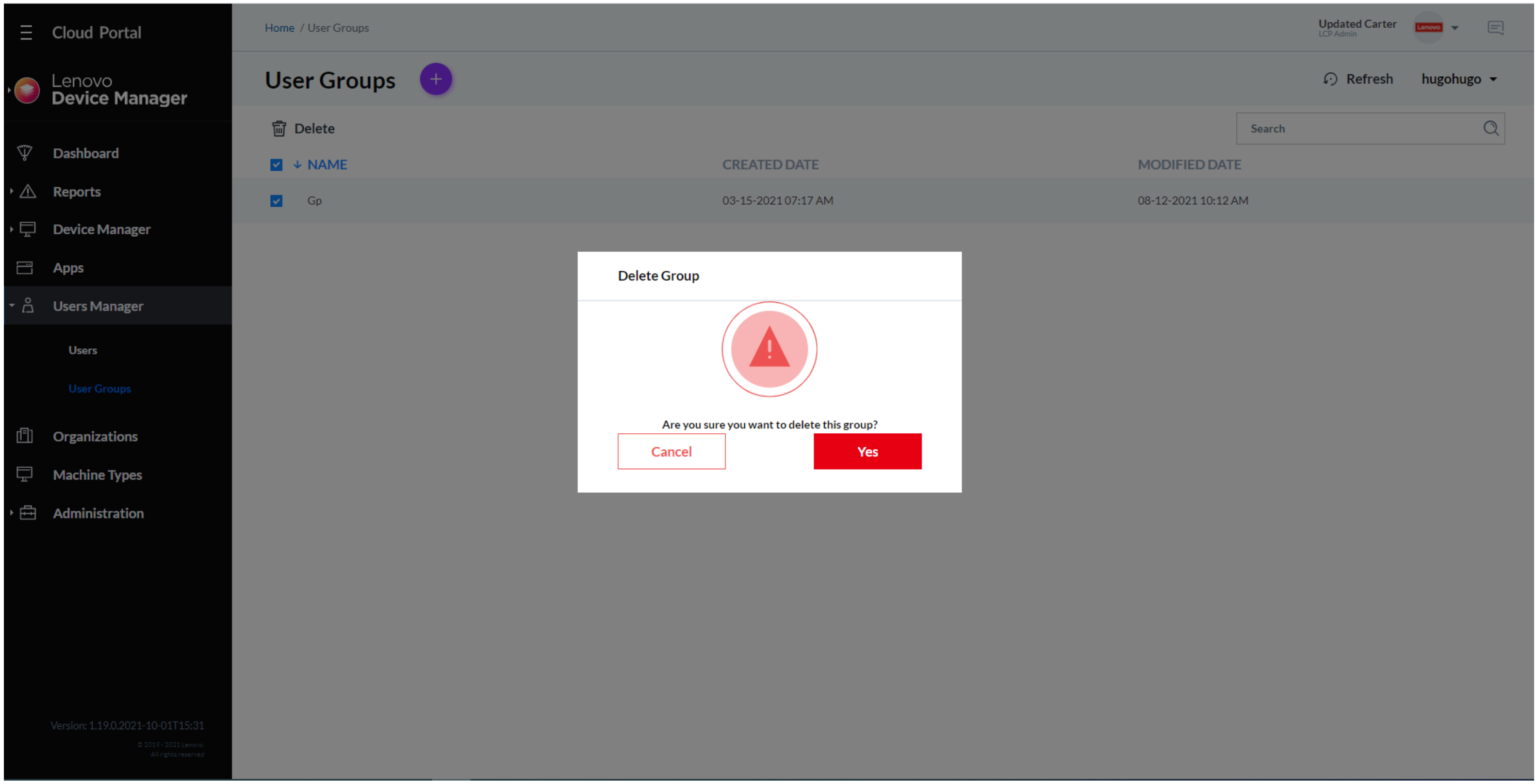
CREATED DATE: 11-25-2020 01:12 AM

MODIFIED DATE: 11-25-2020 01:18 AM

Deleting User Group(s)

To delete a User Group:

1. Select the groups you want to delete.
2. Click on "Delete" and confirm the deletion.



NAME	CREATED DATE	MODIFIED DATE
Gp	03-15-2021 07:17 AM	08-12-2021 10:12 AM

Delete Group

Are you sure you want to delete this group?

You may also delete a group directly from the User Group tray.

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.

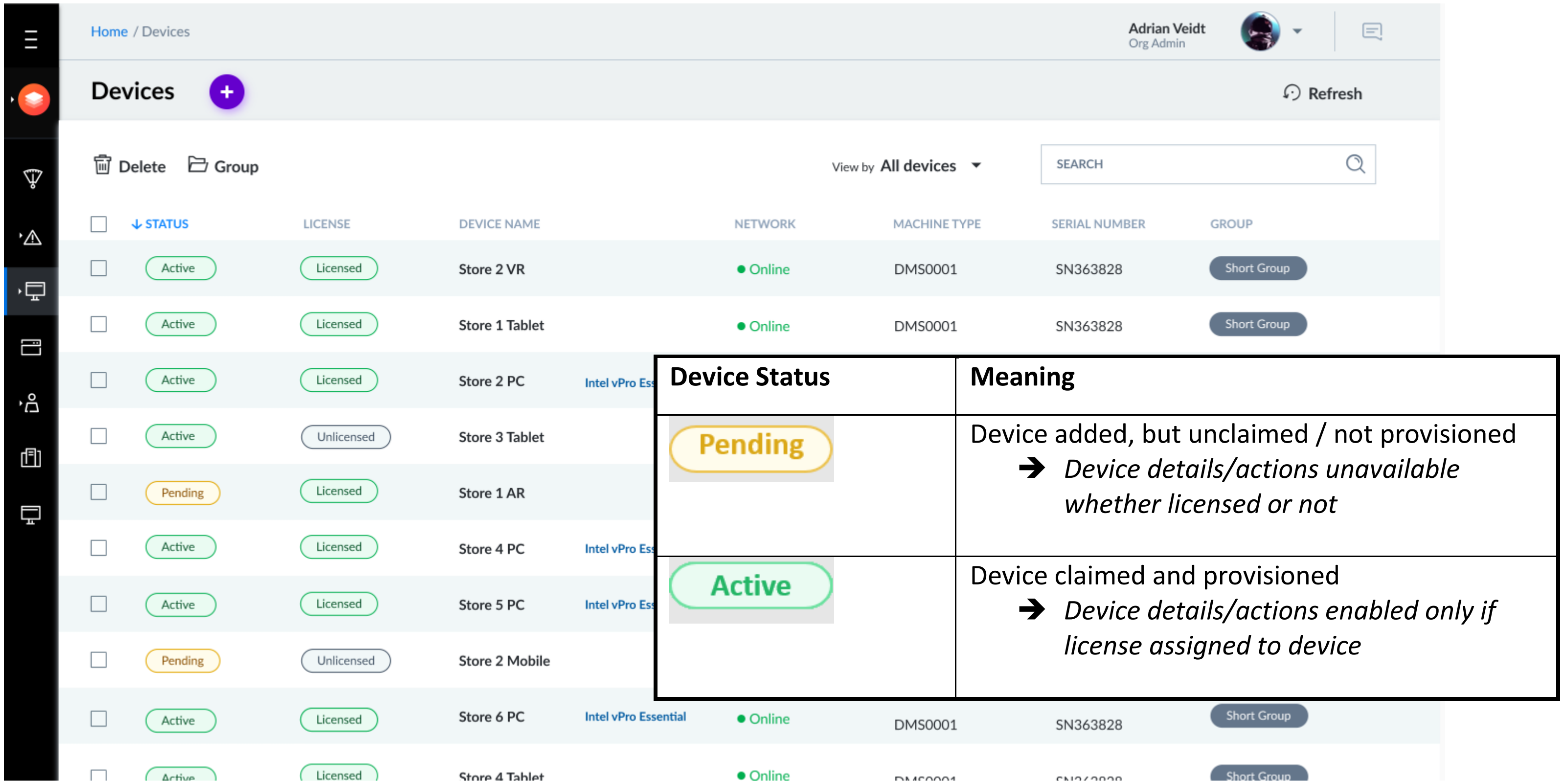
3.2 Manage Devices

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
- 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.

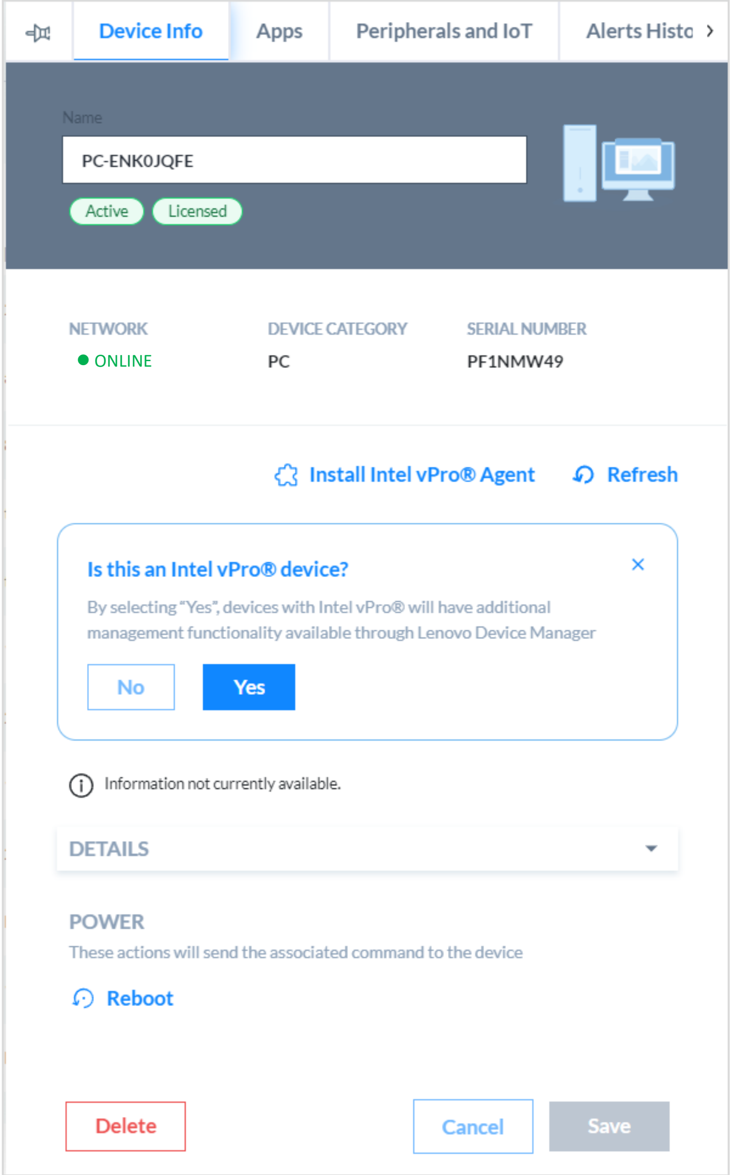
The following features are available on the device tray - ***Device Info*** tab:

- 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: PC-ENK0JQFE

NETWORK: ● ONLINE

DEVICE CATEGORY: PC

SERIAL NUMBER: PF1NMW49

Is this an Intel vPro® device?

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

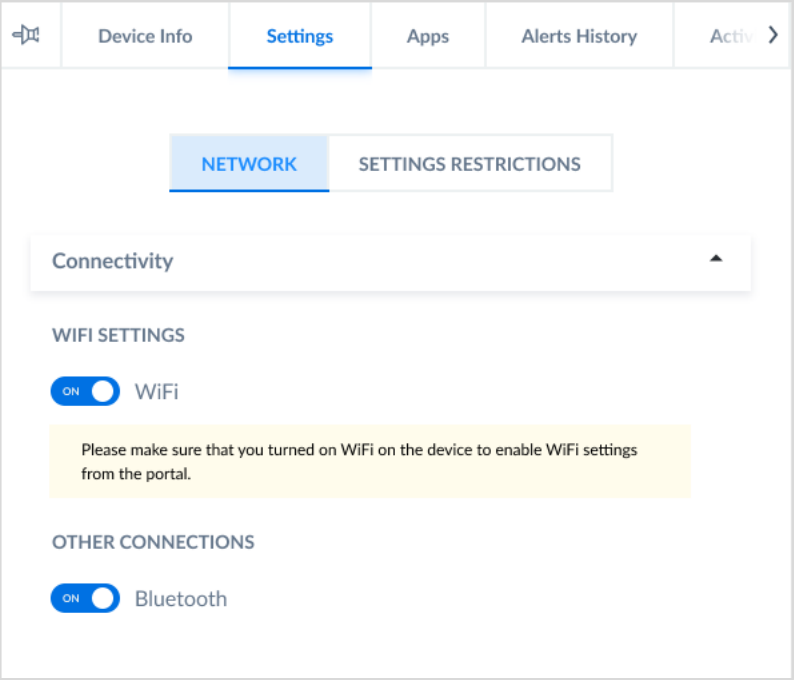
Information not currently available.

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):

- ***Network*** 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

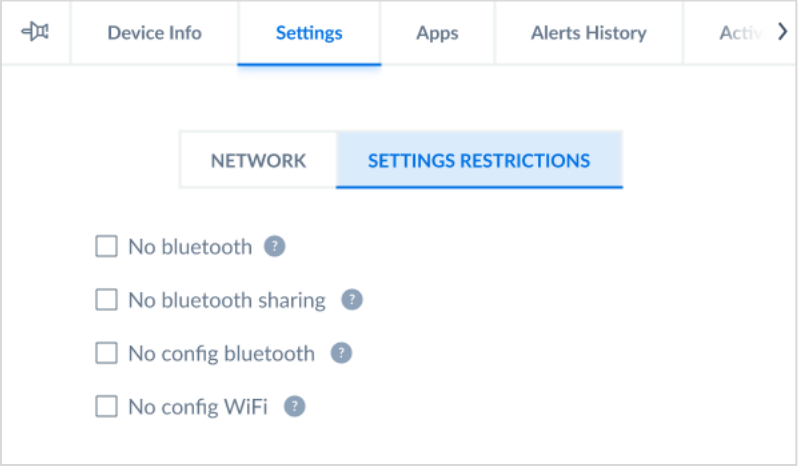


ON WiFi

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

ON Bluetooth

- ***Settings Restrictions*** tab (restricts settings allowed to be changed directly on device)
  - No Bluetooth
  - No Bluetooth sharing
  - No config Bluetooth
  - No config WiFi



□ No bluetooth

□ No bluetooth sharing

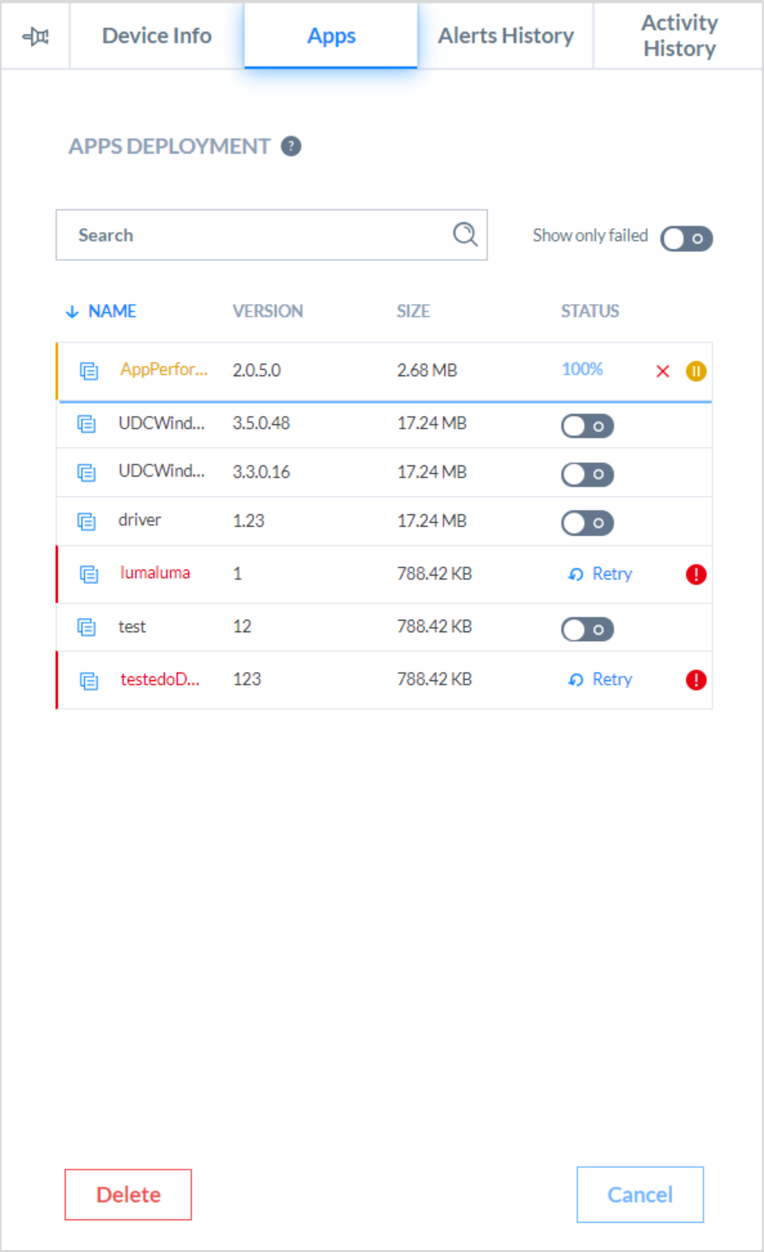
□ No config bluetooth

□ No config WiFi

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

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

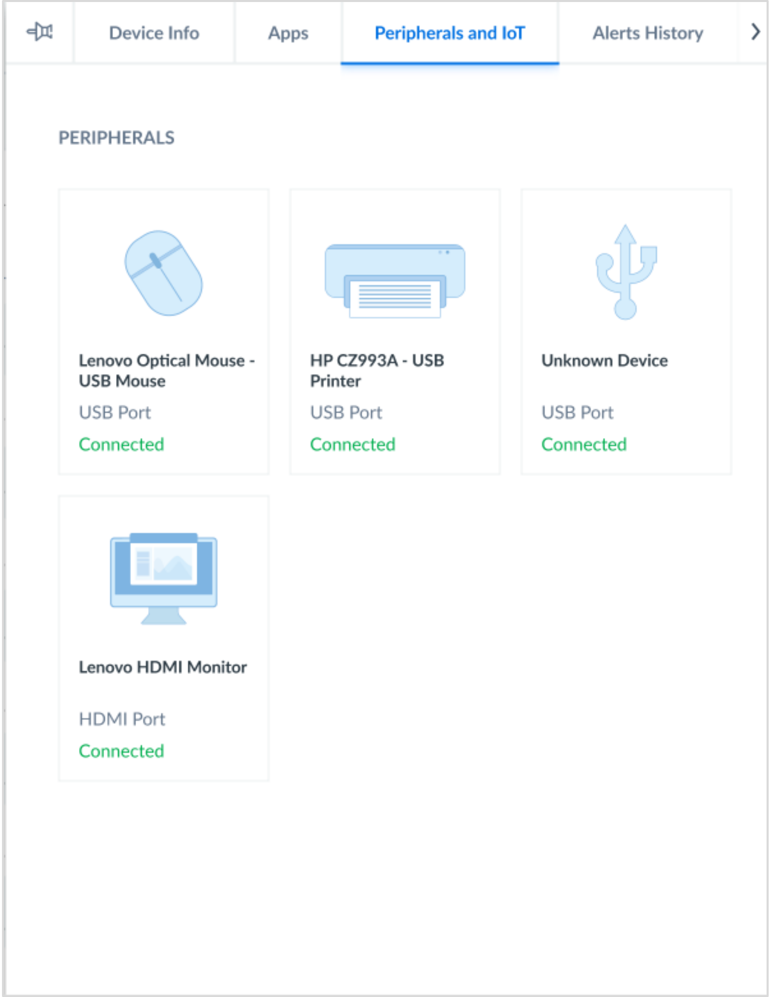
- View LDM-managed applications (software, firmware, driver) on device
- Deploy application updates to the device
- Uninstall applications from the device
- View deployment status
- Delete device



NAME	VERSION	SIZE	STATUS
AppPerfor...	2.0.5.0	2.68 MB	100%
UDCWind...	3.5.0.48	17.24 MB	
UDCWind...	3.3.0.16	17.24 MB	
driver	1.23	17.24 MB	
lumaluma	1	788.42 KB	Retry
test	12	788.42 KB	
testedoD...	123	788.42 KB	Retry

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

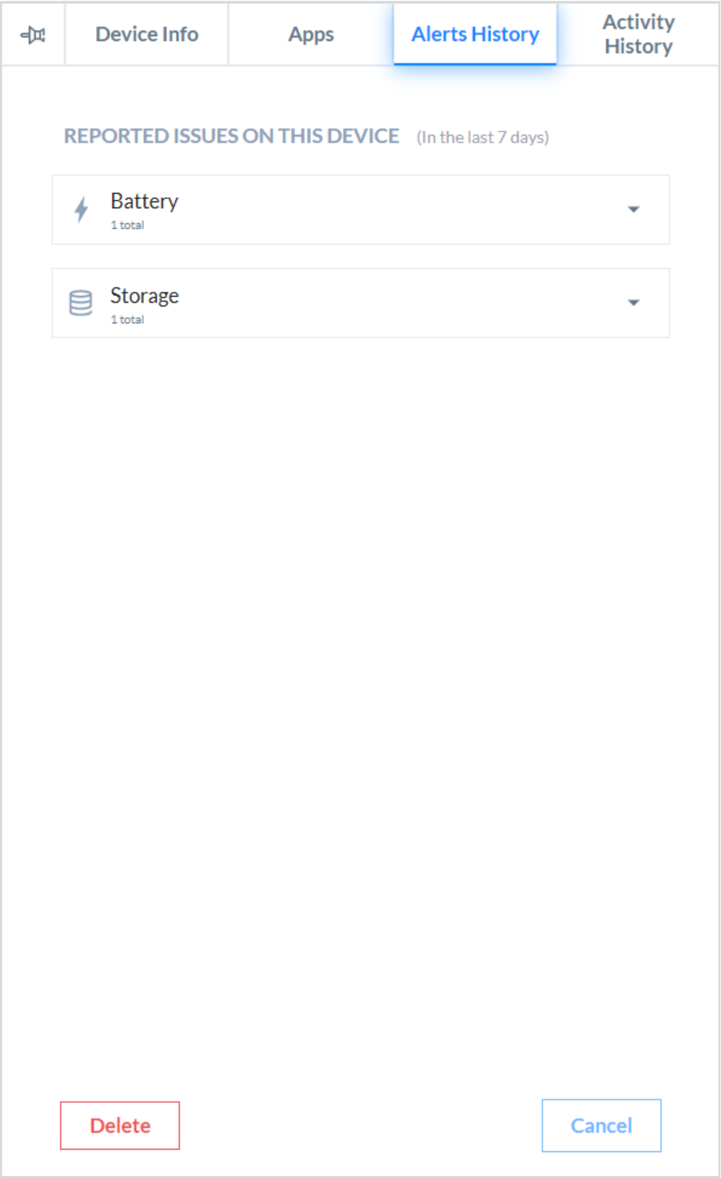
Unknown Device
USB Port
Connected

Lenovo HDMI Monitor
HDMI Port
Connected

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

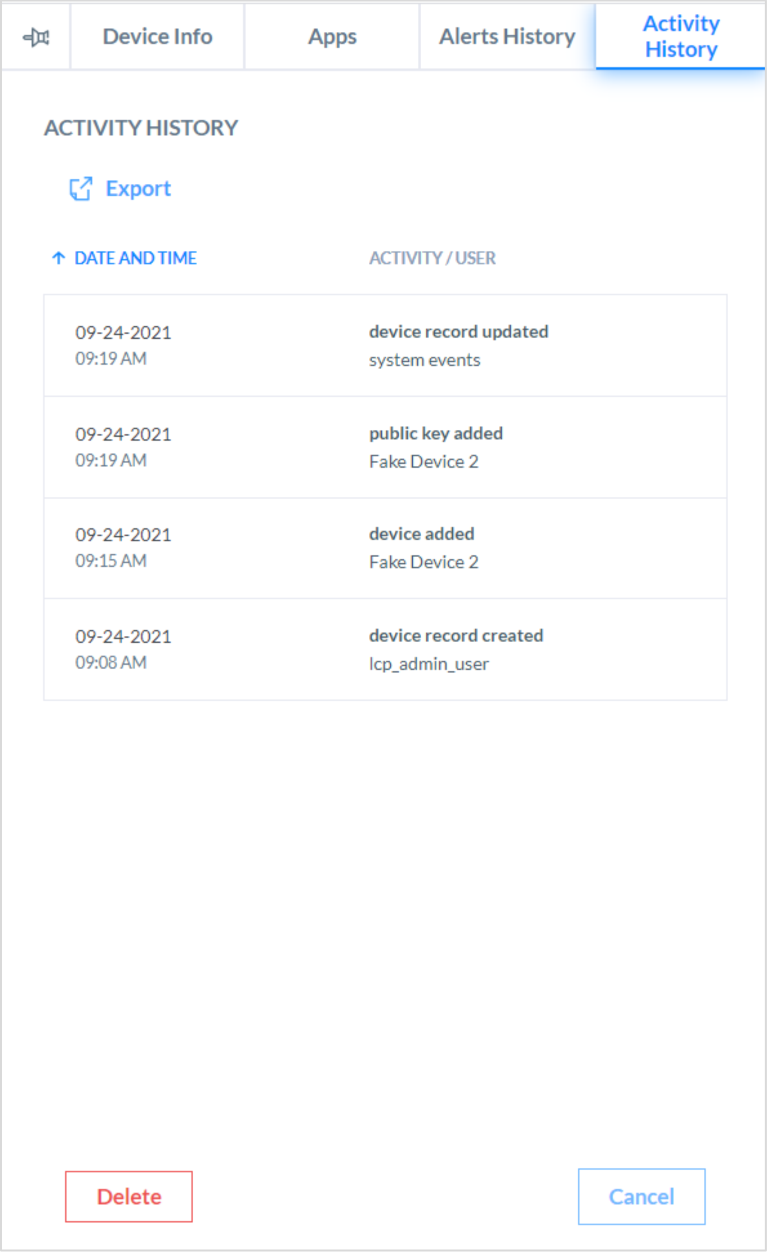
- View any "Low Battery" alert
- View any "Storage" alert
- View any "OTA Deployment" alert
- Delete device

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



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

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.

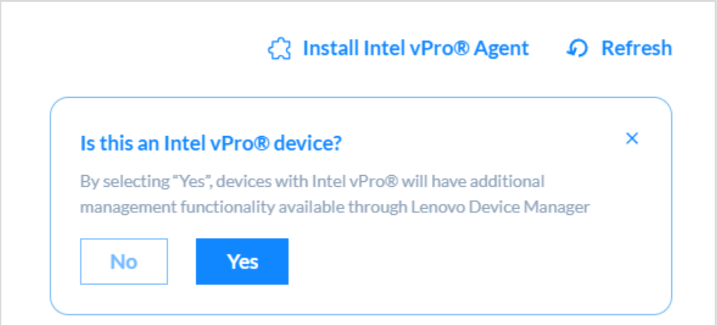
Org Admins can enable or disable this feature for all devices claimed under their organization in Org Settings/*Preferences* (see Section 2.3 for more information).

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.



Is this an Intel vPro® device?

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

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.*

Uninstalling the Intel vPro® Agent

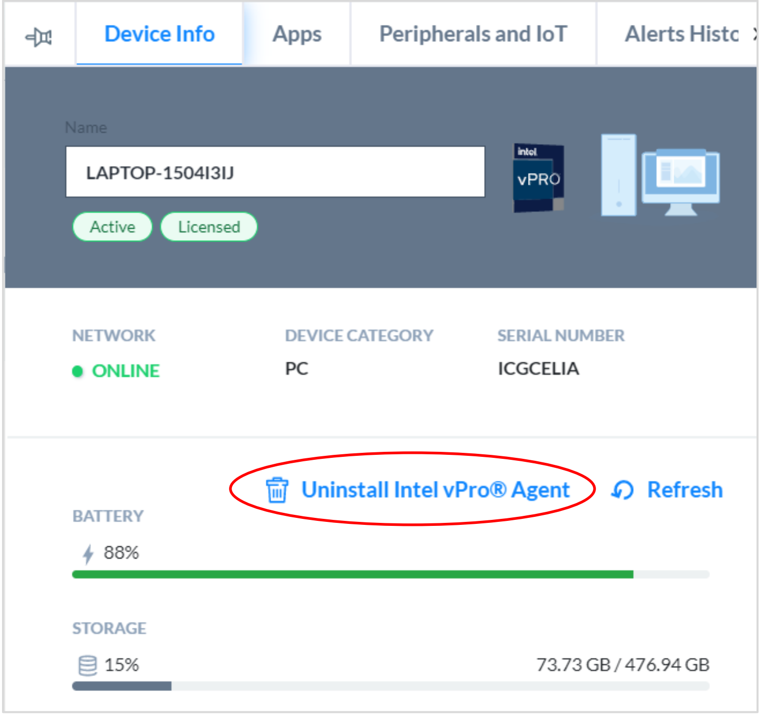
If, for any reason, the Intel vPro agent needs to be removed from a device, IT Admins can easily do so by:

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.*



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

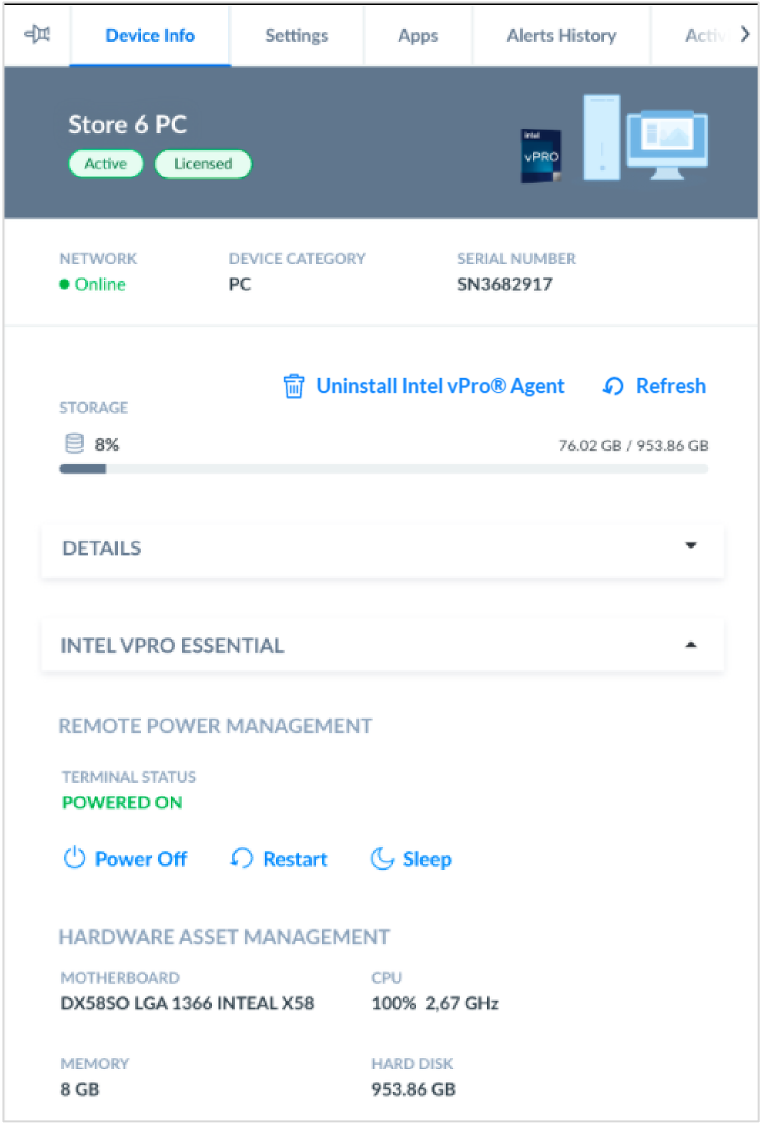
Power Management Added with Intel vPro®:

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.



Store 6 PC

NETWORK: Online
DEVICE CATEGORY: PC
SERIAL NUMBER: SN3682917

STORAGE
8% 76.02 GB / 953.86 GB

INTEL VPRO ESSENTIAL

REMOTE POWER MANAGEMENT

TERMINAL STATUS: POWERED ON

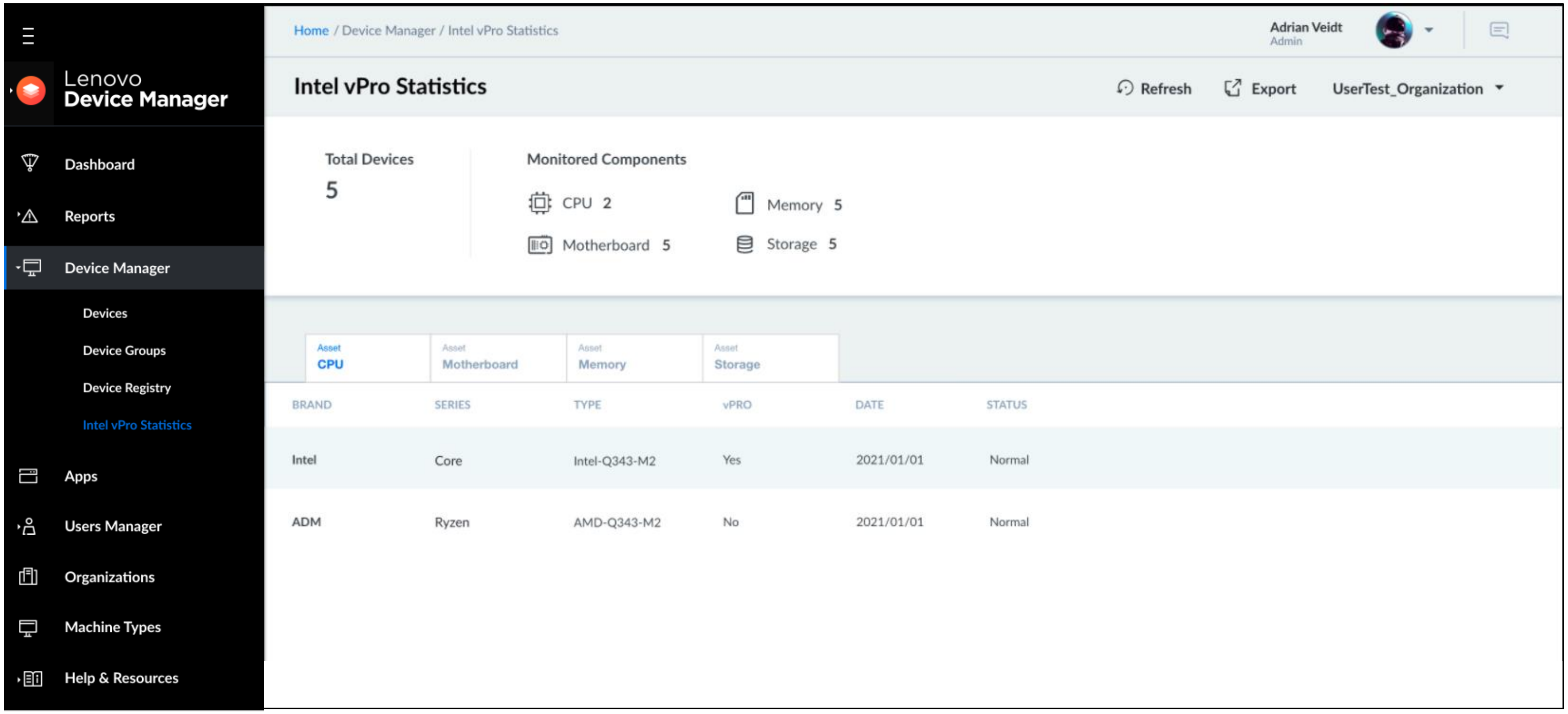
HARDWARE ASSET MANAGEMENT

MOTHERBOARD: DX58SO LGA 1366 INTEAL X58
CPU: 100% 2,67 GHz
MEMORY: 8 GB
HARD DISK: 953.86 GB

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



Intel vPro Statistics

Total Devices 5

Monitored Components

CPU 2

Memory 5

Motherboard 5

Storage 5

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

3.5 Deleting or Removing a Device

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

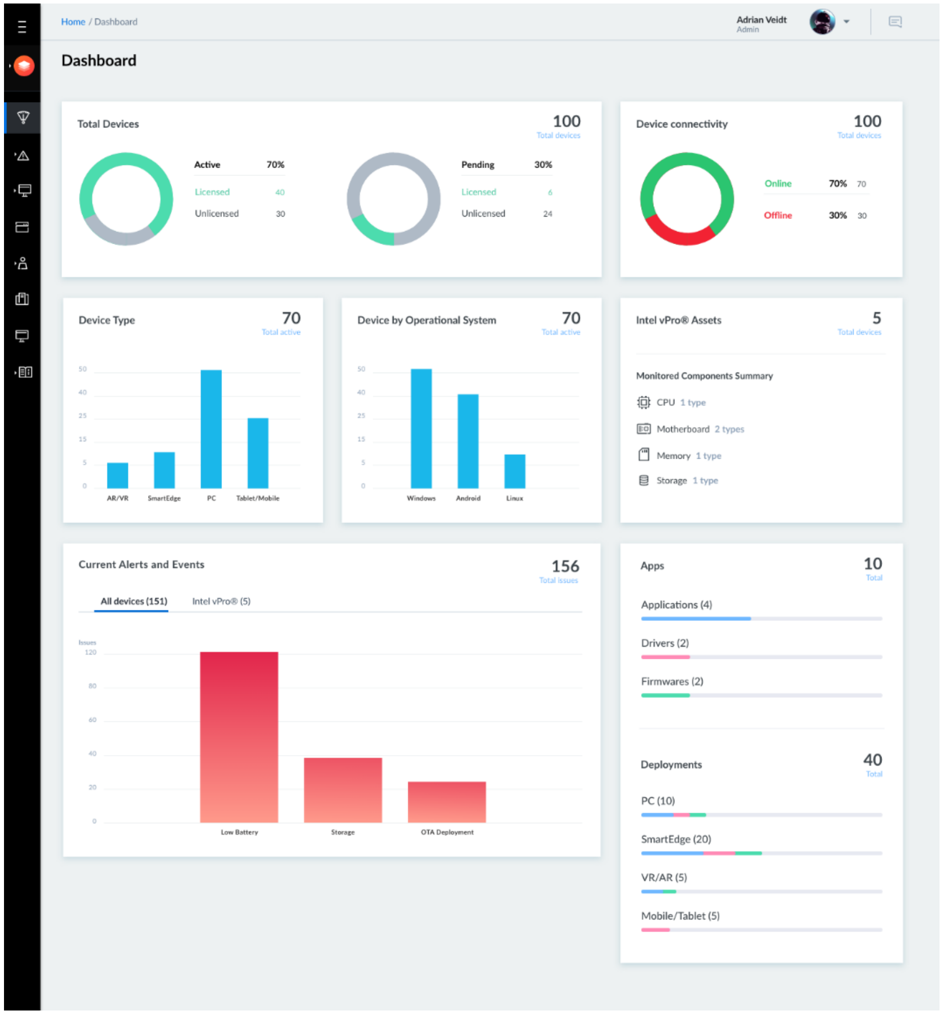
5.3 Deploying an Application

5.4 Removing an Application

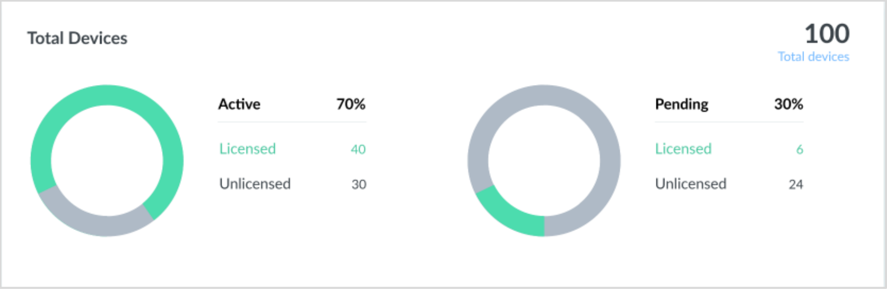
6 Lenovo Device Manager Dashboard

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



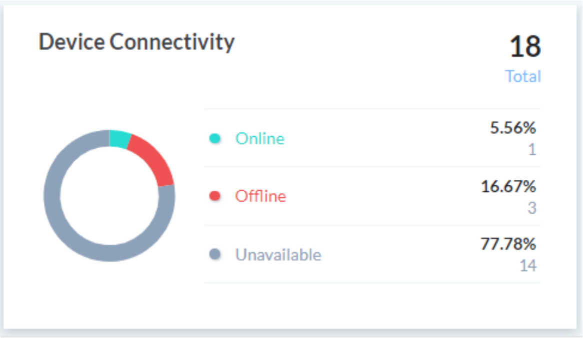
Total Devices

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.

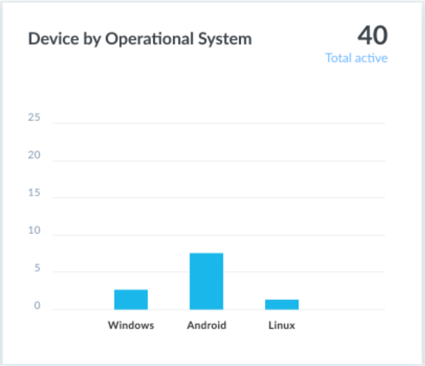


Device Connectivity

18
Total

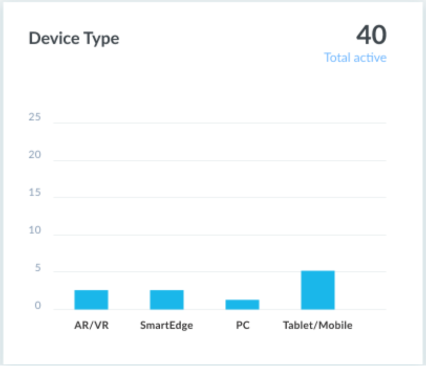
● Online	5.56%	1
● Offline	16.67%	3
● Unavailable	77.78%	14

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

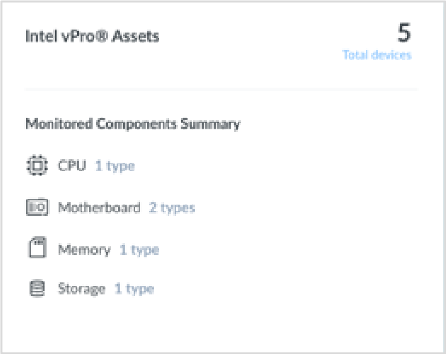
40
Total active



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.



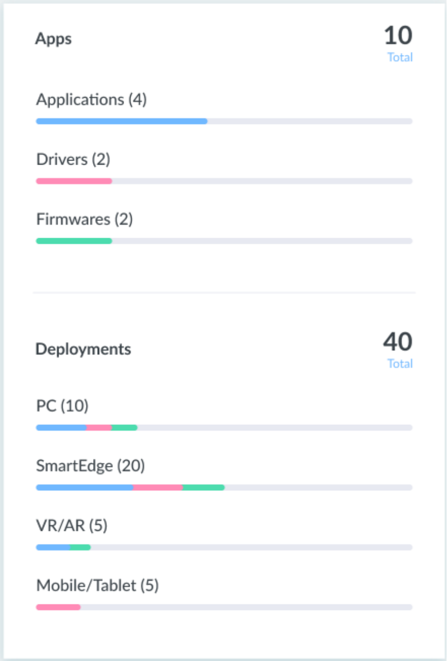
Intel vPro® Assets

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

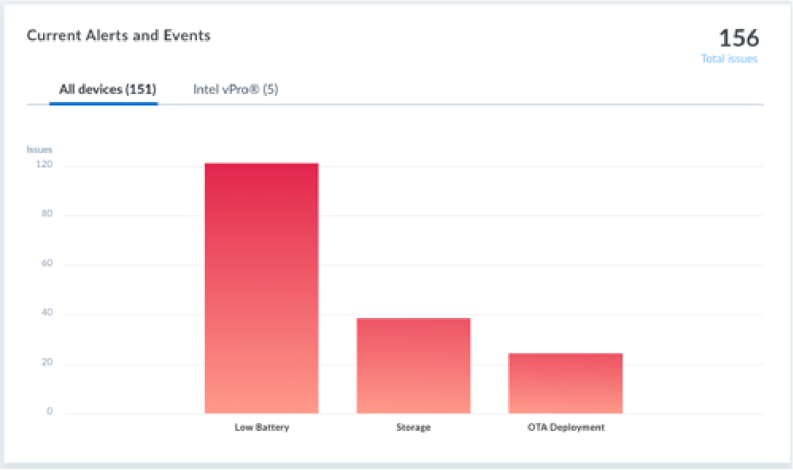
- Applications (4)
- Drivers (2)
- Firmwares (2)

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”

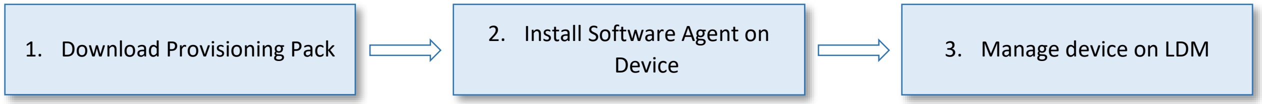
Lenovo Privacy Policy

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

Lenovo Device Manager supports an automated process that simplifies the onboarding of Windows devices by providing a .zip file with the necessary files to be easily downloaded and applied to devices. Any Lenovo Windows device can be automatically claimed on the LDM platform by installing the LDM Provisioning Pack to the device.

The provisioning package is a zip file - organization-setup.zip. It has:

1. Installer_jwt file - A JSON Web Token (JWT) format for secure exchange of the information between LDM server and organization devices.

2. Install-ldm.bat – A script that has series of commands for installation for LDM software.

3. README.txt file

4. register-udc-ldm.ps1 - PowerShell script for the registration of Universal Device Client (UDC).

5. Udc.zip - A compressed zip folder that has UDC setup and UDC Service information, task control settings, device parameters to be fetched when the provisioning pack is run on it.

6. config_policy & bridge_config_policy files – These are the encrypted files contains the policy configuration of the organization.

> The setup is unique for the organization and must not be shared.

To automatically claim a Windows device:

1. Go to **Device Manager → Devices** and click on **✚** ("Claim Device") button

2. Select the *Device Type* that fits the device to be added: “PC” or “Smart Edge” (*Note: Windows tablets are not currently supported)*

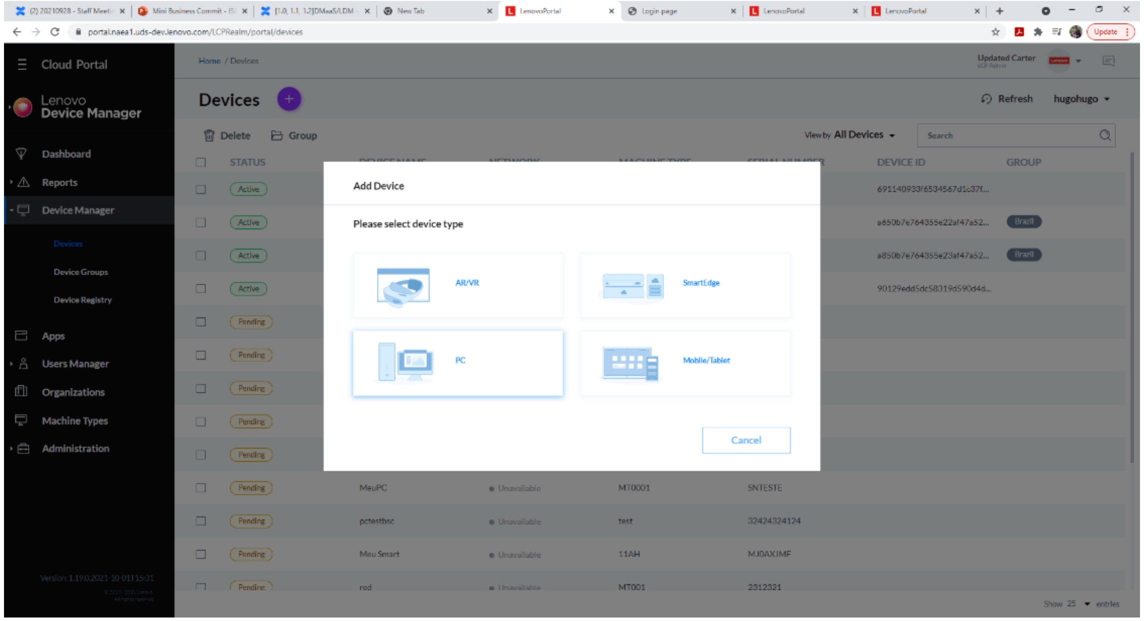
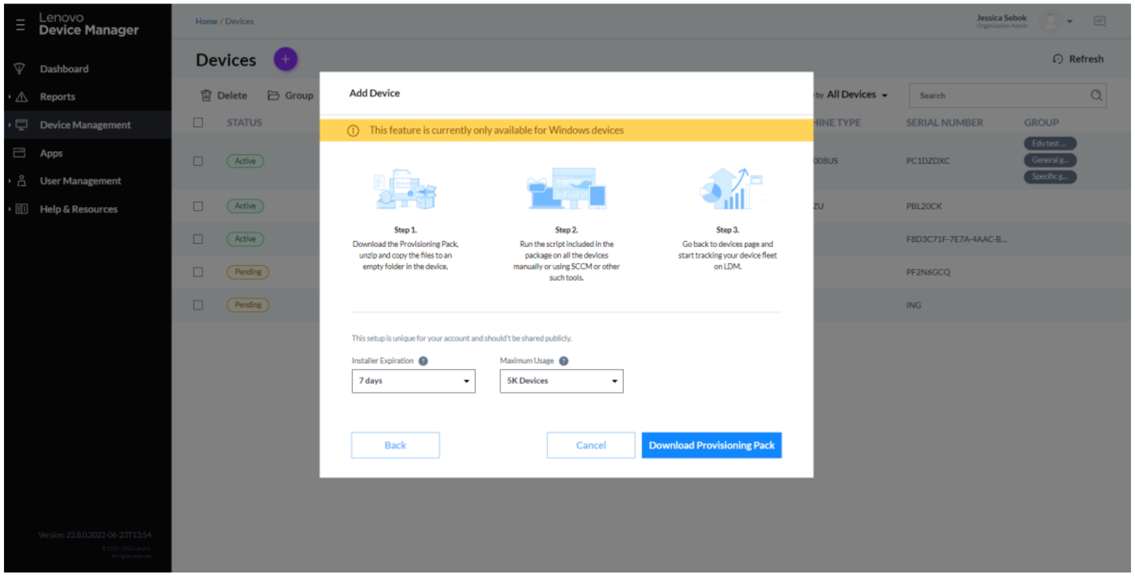


Figure 1

4. Follow **Step 1 on screen** (as shown on Figure 2 below)

   a. Select “Download Provisioning Pack”. The Provisioning Pack will download and is now available to use on the current device, distribute to multiple devices, or save to USB for on-prem installation.



Add Device

This feature is currently only available for Windows devices

Step 1. Download the Provisioning Pack, unzip and copy the files to an empty folder in the device.

Step 2. Run the script included in the package on all the devices manually or using SCCM or other such tools.

Step 3. Go back to devices page and start tracking your device fleet on LDM.

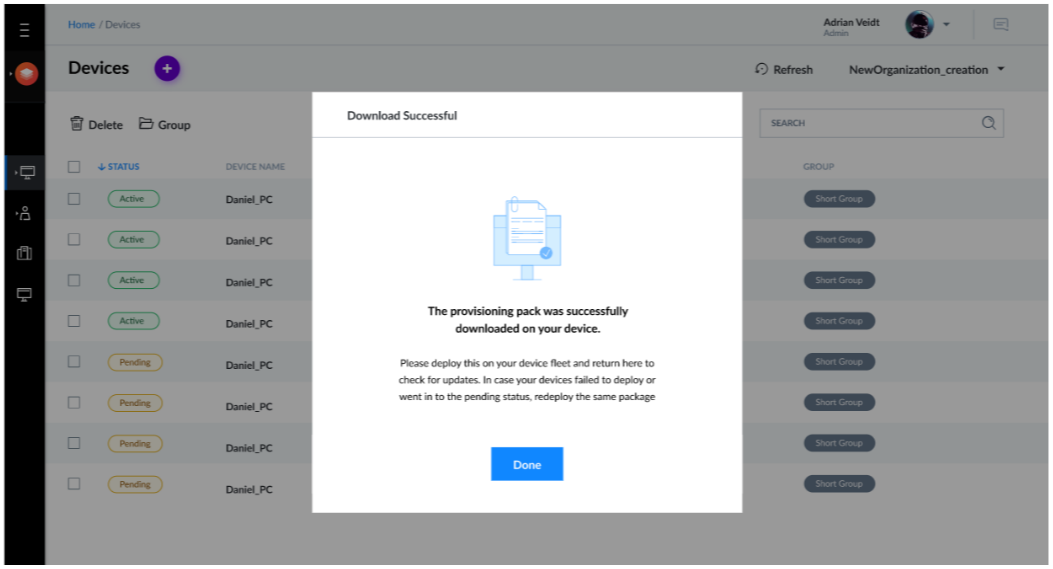
This setup is unique for your account and shouldn't be shared publicly.

Installer Expiration: 7 days

Maximum Usage: 5K Devices

Figure 2

b. Once installed, a “Download Successful” message will appear.



STATUS	DEVICE NAME	GROUP
Active	Daniel_PC	Short Group
Active	Daniel_PC	Short Group
Active	Daniel_PC	Short Group
Active	Daniel_PC	Short Group
Pending	Daniel_PC	Short Group
Pending	Daniel_PC	Short Group
Pending	Daniel_PC	Short Group
Pending	Daniel_PC	Short Group

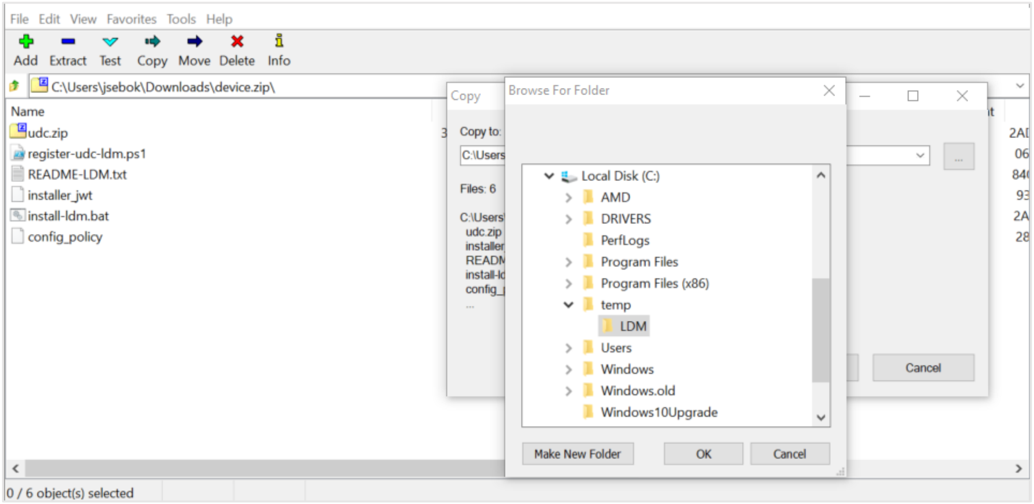
Download Successful

The provisioning pack was successfully downloaded on your device.

Please deploy this on your device fleet and return here to check for updates. In case your devices failed to deploy or went in to the pending status, redeploy the same package

Figure 3

c. Unzip and copy the files to an empty folder in the device. For example, as shown below into C:_temp\LDM.



C:\Users\jsebok\Downloads\device.zip\

Name
udc.zip
register-udc-ldm.ps1
README-LDM.txt
installer_jwt
install-ldm.bat
config_policy

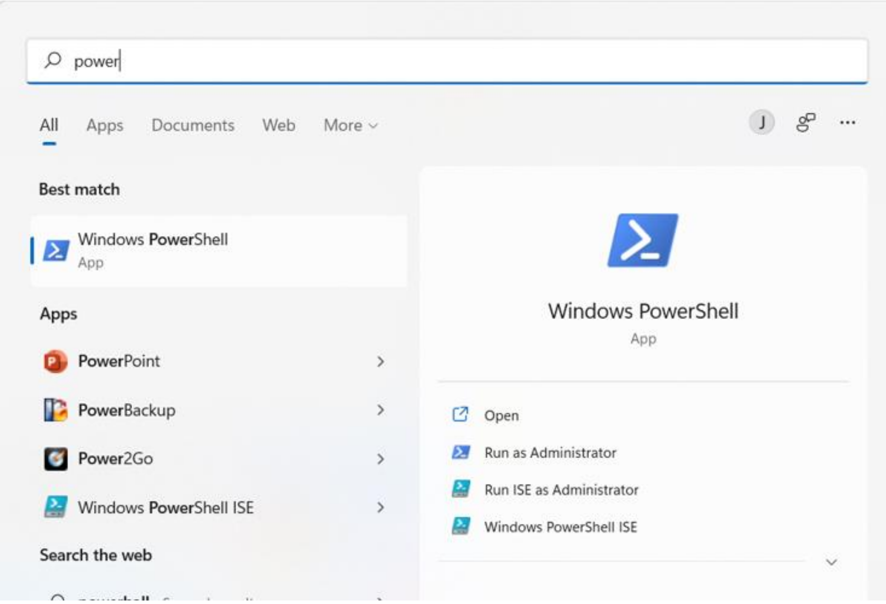
Copy to:
C:\Users
Files: 6

0 / 6 object(s) selected

Figure 4

5. Follow **Step 2 on screen** (as shown on Figure 2)
    a. Execute the PowerShell script as an Administrator:
        - Select the Windows Start icon in the device's toolbar and search for "Windows PowerShell" app
        - Select "Run as Administrator" to open PowerShell command window
        - From PowerShell prompt, enter:

```
> cd C:\temp\LDM\
C:\temp\LDM\>  .\register-udc-ldm.ps1
```



> **Note:** If you get an " UnauthorizedAccess" message, please run the following command to enable the PowerShell script to run without issues: > **Set-ExecutionPolicy Unrestricted**

6. Follow **Step 3 on screen** (as shown on Figure 2)
    b. Check the device list. Once the device status should now be listed as Active .

> **Note:** If onboarding is not successful, check the error listing at the end of this guide for follow up actions.

7. Execute the previous steps on every Windows device in the fleet.

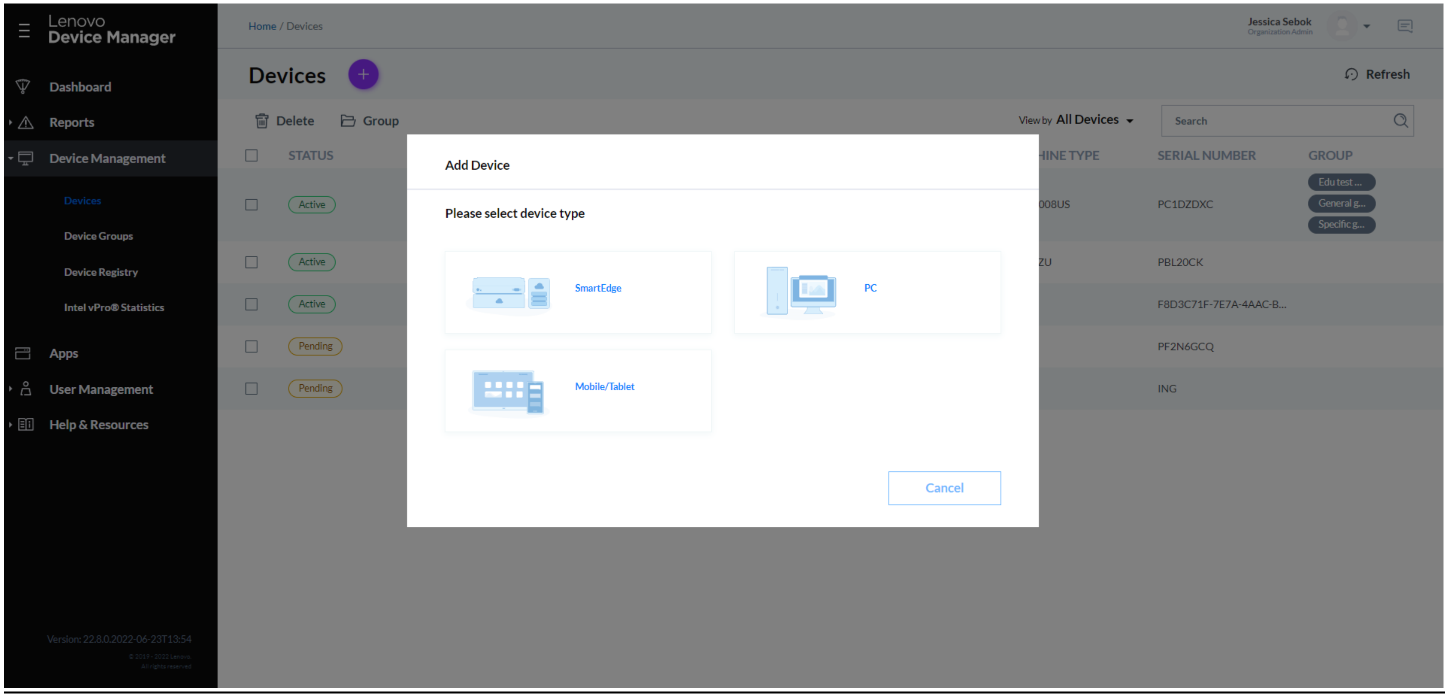
10.2 Add Android Devices

Any Lenovo Android device can be claimed and provisioned by scanning a QR code from the LDM platform.

10.2.1 Claim a device with a QR code:

1. Go to **Device Manager → Devices** and click on **✚** ("Claim Device") button

2. Select the *Device Type* that fits the device to be added: “Mobile/Tablet” (Note: AR/VR devices are not supported in LDM 2.1 but will return in LDM 2.2).



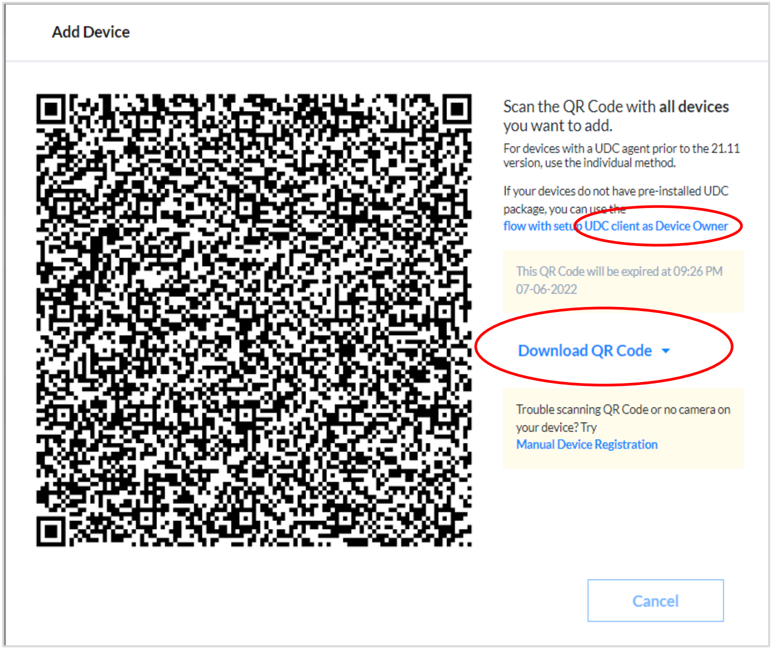
Add Device

Please select device type

□	STATUS	HINE TYPE	SERIAL NUMBER	GROUP
□	Active	008US	PC1DZDXC	Edu test ... General g... Specific g...
□	Active	ZU	PBL20CK	
□	Active		F8D3C71F-7E7A-4AAC-B...	
□	Pending		PF2N6GCQ	
□	Pending		ING	

3. **Scan the QR Code using the camera on the device** to register the device to the LDM organization, install the UDC agent AND provision all device configurations automatically.

4. **If the device is not immediately available to scan the QR code** or you need to distribute it to multiple devices, you can also select "Download the QR Code" to download it in the following formats:
    - PNG
    - JPEG
    - SVG
    - PDF



Add Device

Scan the QR Code with **all devices** you want to add.

For devices with a UDC agent prior to the 21.11 version, use the individual method.

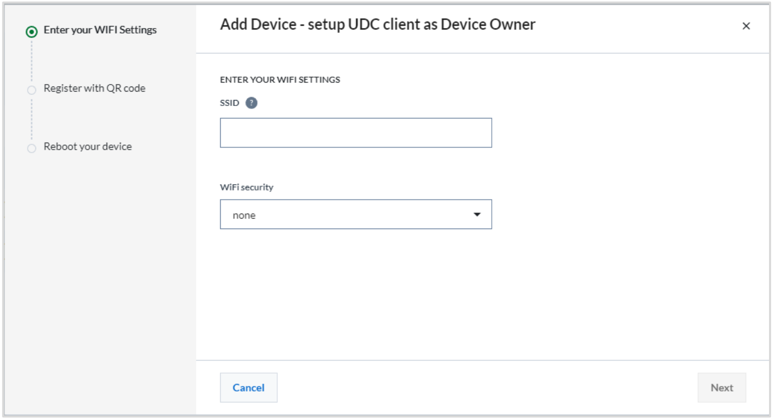
If your devices do not have pre-installed UDC package, you can use the flow with setup UDC client as Device Owner

This QR Code will be expired at 09:26 PM 07-06-2022

Trouble scanning QR Code or no camera on your device? Try Manual Device Registration

5. **To set up the UDC client as Device Owner**, select the "Setup UDC client as Device Owner" option

    a. Add WIFI information:
    - Enter SSID
    - Select WIFI security from dropdown (wpa, wep, or eap)
    - Click "Next" button



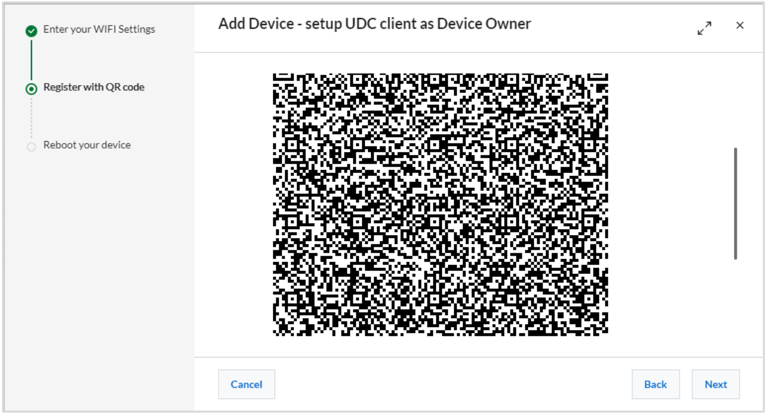
Add Device - setup UDC client as Device Owner

ENTER YOUR WIFI SETTINGS

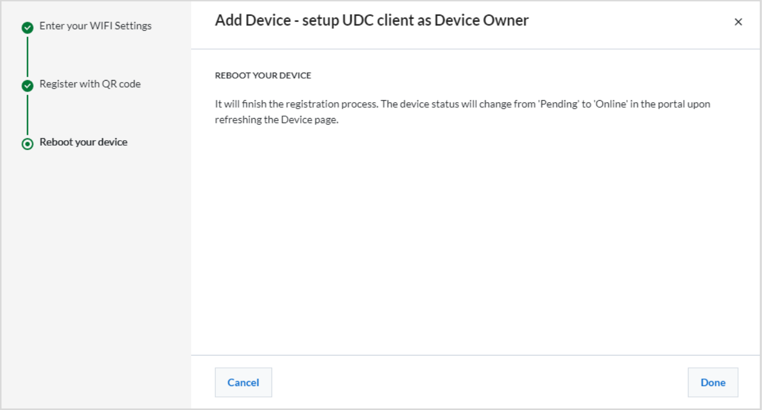
SSID

WiFi security: none

b. Scan QR Code with device and click “Next”



c. Reboot your device to finish the registration process.



REBOOT YOUR DEVICE

It will finish the registration process. The device status will change from 'Pending' to 'Online' in the portal upon refreshing the Device page.

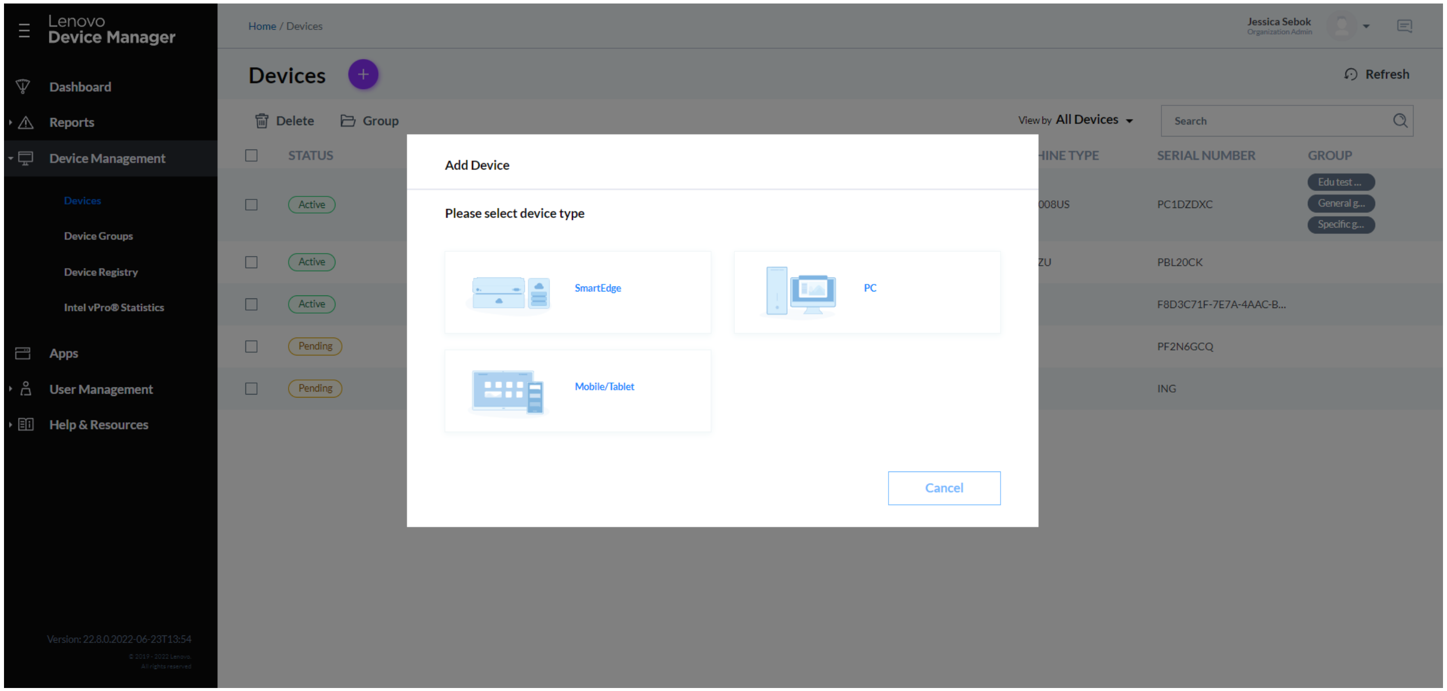
6. Check/refresh the device list. Once the device status should now be listed as Active .

10.2.2 Manually register an Android device

If the device does not have a camera or there are issues scanning the QR code, you can manually register device:

1. Go to **Device Manager → Devices** and click on ✚ ("Claim Device") button

2. Select the *Device Type* that fits the device to be added: “Mobile/Tablet” (Note: AR/VR devices are not supported in LDM 2.1 but will return in LDM 2.2).

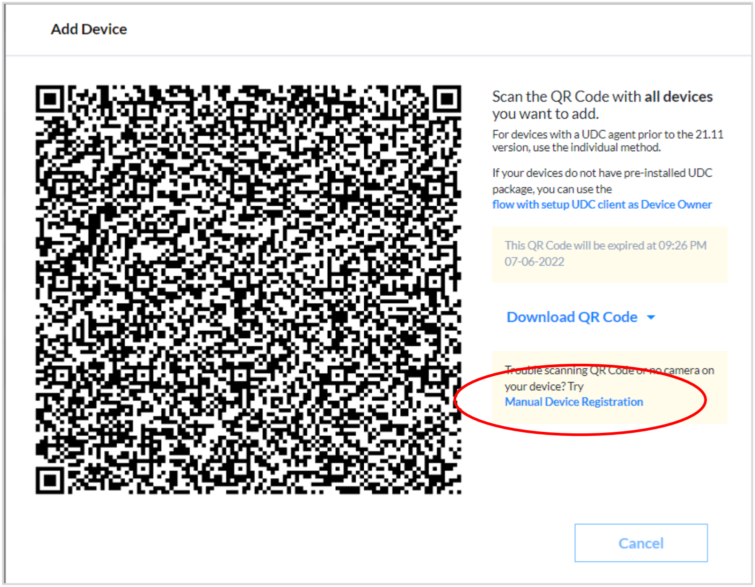


Add Device

Please select device type

STATUS	HINE TYPE	SERIAL NUMBER	GROUP
Active	008US	PC1DZDXC	Edu test ... General g... Specific g...
Active	ZU	PBL20CK	
Active		F8D3C71F-7E7A-4AAC-B...	
Pending		PF2N6GCQ	
Pending		ING	

3. Select the **"Manual Device Registration"** option from the "Add Device screen



Add Device

Scan the QR Code with **all devices** you want to add.

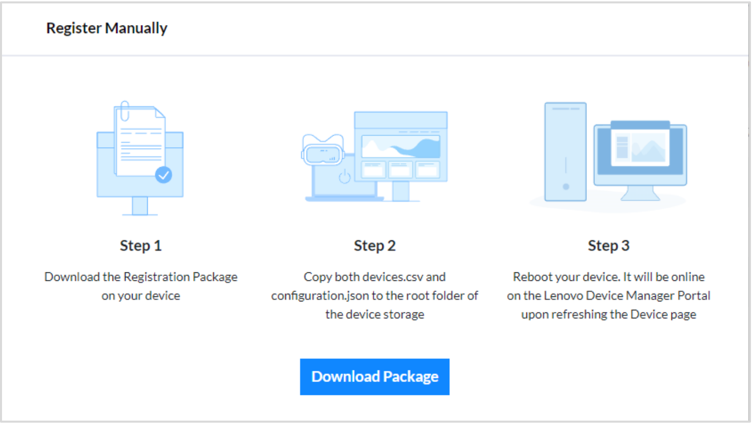
For devices with a UDC agent prior to the 21.11 version, use the individual method.

If your devices do not have pre-installed UDC package, you can use the flow with setup UDC client as Device Owner

This QR Code will be expired at 09:26 PM 07-06-2022

Trouble scanning QR Code or no camera on your device? Try Manual Device Registration

4. Follow the instructions to manually install the Provisioning Package on the device:
    a. Click on "Download File" to download the .json file
    b. Copy the .json file to your device
    c. Reboot your device



Register Manually

Step 1

Download the Registration Package on your device

Step 2

Copy both devices.csv and configuration.json to the root folder of the device storage

Step 3

Reboot your device. It will be online on the Lenovo Device Manager Portal upon refreshing the Device page

5. Check/refresh the device list. Once the device status should now be listed as Active .

10.3 Installing the Intel vPro® Agent

The Intel vPro® agent can be installed to devices with the Intel vPro® chip automatically during provisioning or manually after the devices are claimed on LDM. To install the Intel vPro® agent, follow the steps found in the LDM User Guide, section *3.4 Intel vPro® Support.*

10.4 Requirements

Client software for this solution has a few requirements that the device must meet

Category	Requirement
Manufacturer	Currently any Lenovo device (Windows or Android) is supported
Operating System	Windows 10 version 1809 ("October 2018 Update") or higher • 64-bit OS • Special editions such as "10 S" or "10x" are not currently supported Android version 10 or higher
Hardware	• Trusted Platform Module (TPM) 2.0 enabled • Processor supports x86 instruction set architecture
Environment	• Access to the Internet - specifically *.uds.lenovo.com on ports 80, 443 & 8883 • Proxy is supported in some scenarios. Devices may require additional configuration to support. Refer to Using the Troubleshooter Section for details
UDC Agent	For support of all defined functionality within this document, the following UDC agent versions are required: • Windows 22.2.0.101 / Android 21.11.0.50

> Note: Intel vPro® functionality may vary based on the version of vPro installed on the device. Devices with versions prior to Intel Gen 15 may not have full remote management capabilities.

> Note: Virtual machines and virtual machine hypervisors are not supported

> **Important Note on Proxy**
> UDC uses a security feature called certificate pinning. UDC does not support the scenario where a proxy service in your environment performs TLS inspection (decrypting and re-encrypting traffic using an alternate certificate). You must completely exclude the traffic for *.uds.Lenovo.com from the proxy or disable TLS inspection for that endpoint. Please refer to your proxy service documentation for how to achieve this.

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
}
```