



LDI Plus Quick Start Setup Guide



Copyright/Disclaimer

Copyright © 2023, Lenovo. All rights reserved.

This document contains proprietary information of Lenovo that is protected by copyright and other intellectual property law which restricts its usage. The content in this document is subject to change without notice. If you find any issues in the documentation, please report to us in writing. Lenovo gives no representations or warranties of any kind regarding its content, including accuracy or completeness. Please do not reproduce or transmit any part of this document in any form or by any means, electronic or mechanical, for any purpose, without a written approval from Lenovo.

Contents

Contents	2
1 Onboard Your Fleet	3
1.1 Onboard Your Fleet	3
1.1.1 Software Requirements	3
1.1.2 Download Provisioning Package	4
1.1.3 Install a Physical Device	5
1.1.4 Install Software Agent on Device	6
1.1.5 Track Device on LDI	7
1.1.6 Raise a Ticket	8
1.1.7 Onboard Fleet from Devices Page (Optional)	9
1.1.8 Proxy	9
1.1.9 Current Support Matrix	9
1.1.10 Limitations	9
1.1.11 Troubleshooting	10
1.1.11.1 Pre-install Validation.....	10
1.1.11.2 Troubleshooting Process.....	10
1.1.11.3 Level 1 Troubleshooting.....	11
1.1.11.4 Device Lookup for Remediation Automation	12
1.1.12 Install the Agent to a Virtual Machine	13
1.1.13 Install the Agent to a macOS Device	14
1.1.14 Install the LDI Agent to macOS Devices using MDM / JAMF	14
1.1.15 Check LDI Agent status and restart (macOS)	15
1.1.16 Install the LDI Agent to a Linux Device	15
1.1.17 Uninstall LDI Agent (Windows)	16
1.1.18 Uninstall LDI Agent with scripts (Windows)	17
1.1.19 Uninstall LDI Agent (macOS)	18
1.1.20 Uninstall LDI Agent (Linux)	18
1.1.21 Additional Information	18
1.1.22 Onboard Your Fleet in a Proxy Environment	18

1 Onboard Your Fleet

1.1 Onboard Your Fleet

This chapter helps you smoothly onboard the fleet of devices in your organization to the LDI platform.



This can be installed by running the executable on individual devices or by using an endpoint management utility such as SCCM, Microsoft Intune, or Ivanti that have been tested and approved for LDI deployment. Other endpoint management utilities will likely work as well.

1.1.1 Software Requirements

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

Category	Requirement
Manufacturer	Any device manufacturer is supported, though some features may only be available on the Lenovo devices.
Operating System	Windows: <ul style="list-style-type: none">• Windows 10: 64 bit version 1809 (October 2018 Update) or newer• Windows 11: 64-bit• Windows 10S or 10x editions are not supported.• VMs are supported using alternate installer macOS: <ul style="list-style-type: none">• macOS versions 10.9 and above are supported.• Intel and Apple Silicon CPUs are supported. Linux: <ul style="list-style-type: none">• Red Hat Enterprise Linux version 7 and 8• Amazon Linux version 2• CentOS Version 7 or later• Fedora Version 35• Oracle Linux Version 7 or later• SuSE Enterprise Linux version 12 or later• openSUSE Leap version 15.3• Ubuntu version 14, 18 or later• Debian version 10 or later• Mageia version 8• Mint version 19, 20.2 or later

Category	Requirement
Hardware	<ul style="list-style-type: none"> Trusted Platform Module (TPM) 2.0 enabled Processor supports x86 instruction set architecture
Environment	<ul style="list-style-type: none"> Access to the Internet - *.uds.lenovo.com on port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com on port 443 Proxy is supported in some scenarios. Devices may require additional configuration to support.
Proxy Support	<p>You must configure the proxy through WinINET (WinHTTP or a third-party application/browser extension).</p> <ul style="list-style-type: none"> Proxy server can reach *.uds.Lenovo.com on port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com on port 443 <p>DNS name resolution is available on each managed device. You cannot set an authentication on the proxy server.</p>

1.1.2 Download Provisioning Package

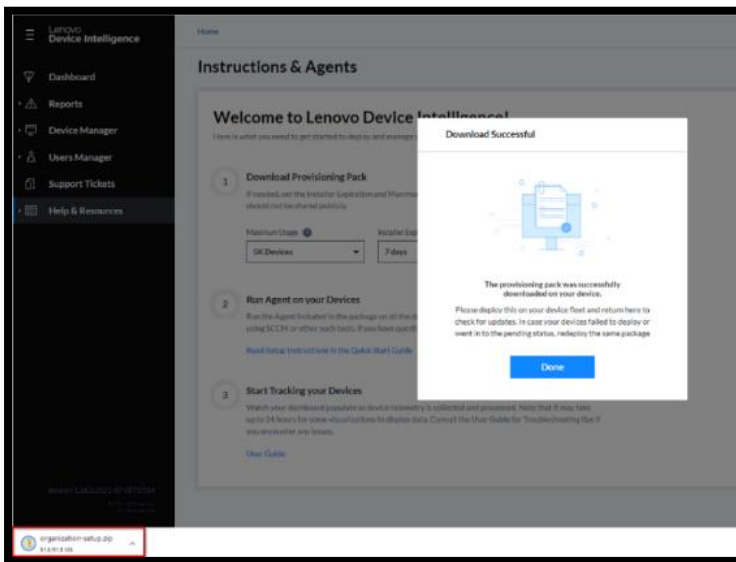
You can onboard fleet of devices to LDI platform through:

- Instructions and Agents (Preferred)
 - Devices page (optional)
- Click **Help & Resources** and then click **Instructions & Agents**. The **Instructions & Agents** page appears.
 - Select **Windows (Physical)** to onboard a physical device. For further details, refer to [Install a Physical Device](#).
 - Select **Windows (Virtual)** to onboard a virtual machine. For further details, refer to [Install the Agent to a Virtual Machine](#).
 - Select **macOS** to onboard a macOS device. For further details, refer to [Install a macOS Device](#).

- Select **Linux** to onboard a Linux device. For further details, refer to [Install a Linux Device](#).

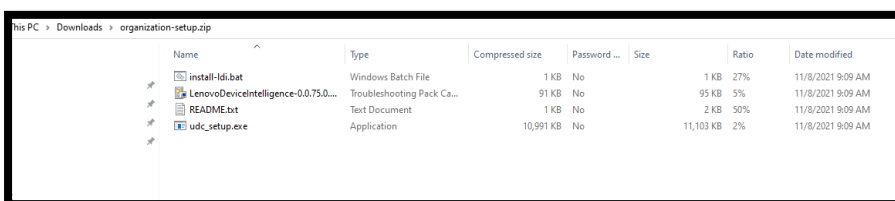
1.1.3 Install a Physical Device

1. Follow the instructions in [Download Provisioning Package](#).
2. Click **Confirm**.
3. In the **Maximum Usage** drop-down list, select the number of devices on which you can download the provisioning package.
4. In the **Installer Expiration** drop-down list, select the days for which the provisioning pack installation is valid.
5. Click **Download Pack**. The pack is downloaded on the device, which access the portal.



The package, organization-setup.zip which has the following components:

- **install-ldi.bat** - A script that has series of commands for installation for LDI software.
1. A Windows-based troubleshooting file package, **LenovoDeviceIntelligence-0.0.75.0.diagcab**. To know more about how to install, run, and create the **LenovoDeviceIntelligence.diagcab** file, refer to [Troubleshooting](#).
 2. README.txt file
 3. **udc_setup.exe** - UDC setup, UDC Service information, and task control settings



1.1.4 Install Software Agent on Device

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

Execute the following steps on every device in the fleet.

1. Copy the following files to an empty folder in the device, e.g., C:\temp\LDItemp
 - udc_setup.exe
 - README.txt
 - install-ldi.bat
2. Execute the batch file as an Administrator.
 - Open the command prompt as an Administrator
 - Execute cd C:\temp\LDItemp
 - .\install-ldi.bat
3. Confirm whether device onboarding was successful or not by checking for an error in the registry.

UDC records the error in the Windows Registry at HKLM\SOFTWARE\LENOVO\UDC\CriticalTranscript when onboarding fails.

If there is an error during installation, check the following error code table to identify the error and rectify it by following the remedial tips:

UDC Significant Event Codes	Error Name	Remedial Tip
None	Ok	
1016:12007	PortalUnreachable	Ensure you have a proper network connectivity and check the connection to the UDS portal.
1001:80	CertificateMismatch	Portal certificate is not valid. Check for https proxy (like Fiddler) that overrides server certificate. Otherwise, contact Lenovo, because server certificate could have been changed.
1001:85	TokenExpired	LDI portal token has expired, or the device registration limit set for this token is over. Request for a new provisioning package with a new token.
1001:86	TokenNotValidated	UDS does not accept provided token. Create another provision package or contact the administrator.

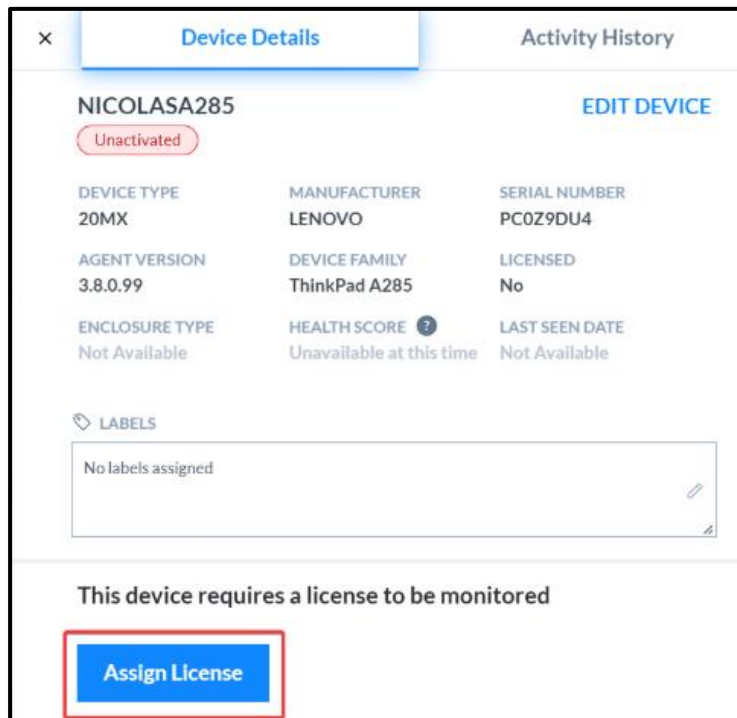
1016	RegisteredToAutomaticOrg	The device was registered to an automatic organization. Restart UDService and log in again. If it fails, contact the administrator.
	DeviceAlreadyRegistered	This device was already registered in the portal. No other action may be needed, but we recommend you follow the uninstallation steps including deletion from the portal before attempting to reinstall and register the device to the portal. Refer to Uninstall UDC .
1016	UnableToRetrieveClaimCode	The script /UDC was unable to retrieve the activation code required for registration of the device in the portal. Restart UDService and try again. If it fails, contact the administrator. To restart the UDC Service, follow these options: Press Windows + R → Enter services.msc → Select UDC Client Service → Restart Restart the device and log in to the LDI Plus portal again.
1011	RegistrationToOrganizationFailed	device_path in the C:\ProgramData\Lenovo\Udc\Shared\ConfigPolicy.json.signed is empty or this file is missing. Check for the UDC Error and UDC log files. Note: Check for the log files in C:\ProgramData\Lenovo\Udc\Log ConfigAgent log file informs you if the config policy has been updated from UDS DeployAgent log file informs you if the package has been installed successfully. Navigate to C:\ProgramData\Lenovo\Udc\Download to see the Provisioning Package ID.

1.1.5 Track Device on LDI

1. Check the **Devices** page to track whether the device has been onboarded to the LDI or not.
2. Check the device status. If the status is:
 - **Pending** - The device could not be onboarded because of an error. Check for the type of error code in the registry and follow the remedy tip provided for it in the error code table. This also includes devices that don't have an assigned license.
 - **Active** – Device has successfully onboarded and is currently online.
 - **Offline** - Device has successfully onboarded and is currently offline.

Note: To get a license, follow these steps:

1. Select Device Manager → Devices.
2. Search for the device with 'Unassigned License'

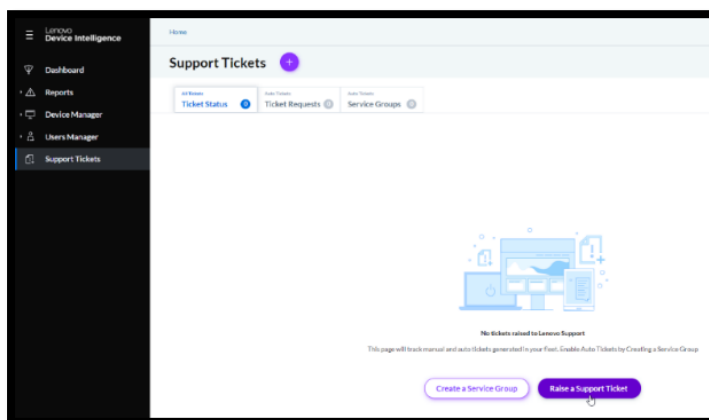


3. Click Assign License.

- **Offline** - Devices that do not send data to the system for 5 minutes. These devices are moved from Active Status to Offline Status. If the device does not have a license, it becomes Unactivated with Pending status.

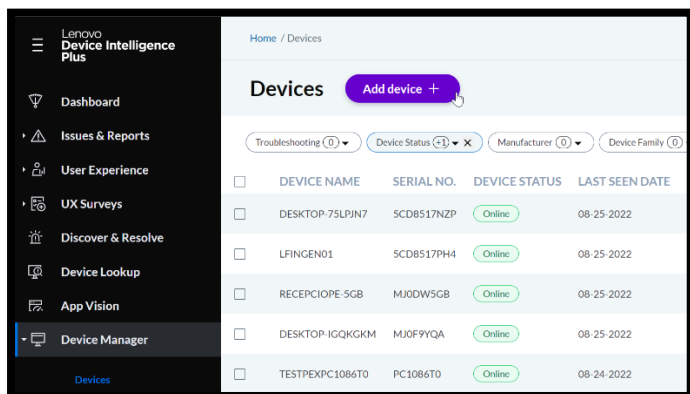
1.1.6 Raise a Ticket

Raise a ticket if the error persists even after following the remedial tip from the error code table.



1.1.7 Onboard Fleet from Devices Page (Optional)

You can also onboard the fleet of devices in your organization to LDI platform from the **Devices** page.



In the **Devices** page, click **Add device +**. The **Instructions & Agents** window appears. For more details, refer to [Download Provisioning Package](#).

1.1.8 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 permanently for that endpoint. Please refer to your proxy service documentation for how to achieve this.

1.1.9 Current Support Matrix

- Leverages OS level proxy configuration
- Usage: Configure proxy information in OS using pac file or manual proxy setup

1.1.10 Limitations

Scenario	Configure UDC to use proxy	For UDC to work and if TLS inspection is enabled
Reaching to internet requires proxy	Use the OS level configuration * Pac file as well as manual proxy setup	In proxy server, whitelist *.uds.lenovo.com: 443 (include port 8883 if UDC agent older than 22.10.0.5)
Internet is reachable but proxy is also required to be setup	Use the OS level configuration * Pac file as well as manual proxy setup	Whitelist *.uds.lenovo.com at device level OR Whitelist *.uds.lenovo.com at proxy server

Note: The UDC agent installation is not supported on virtual machines, hence Type 1 hypervisors and type 2 hypervisors are not supported.

1.1.11 Troubleshooting

When you are unable to register your device in the LDI Plus tool, you can run a tool that executes some routine checks, collect logs, and other device information that can be used to analyse the problem offline. Use the `LenovoDeviceIntelligence.diagcab` file for troubleshooting, which you get with the Provisioning Package.

1.1.11.1. Pre-install Validation

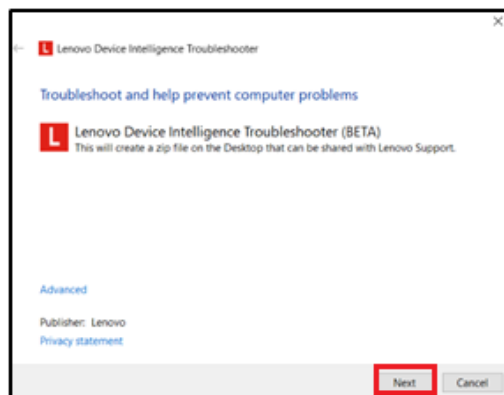
Note the following information for the API accessibility in different settings:

API	Test-NetConnection-Port 443
Reachability	api.naea1.uds.lenovo.com
	Test-NetConnection-Port 443
	api.euwe1.uds.lenovo.com

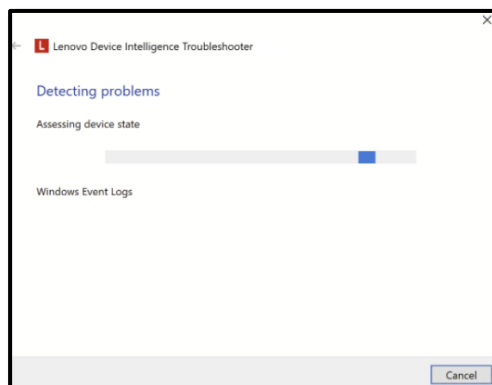
1.1.11.2. Troubleshooting Process

Follow these steps to troubleshoot:

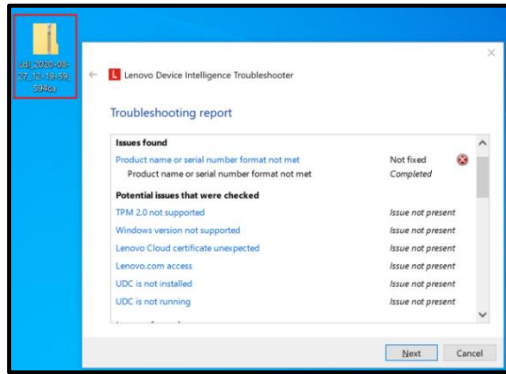
1. Double-click the `LenovoDeviceIntelligence.diagcab` file. The following window appears.



2. Click **Next** to complete the installation.



4. After successful installation, the **Troubleshooting report** window appears.



Note: By default, the output is a zip file, and it also displays the location where the file is saved.

1.1.11.3. Level 1 Troubleshooting

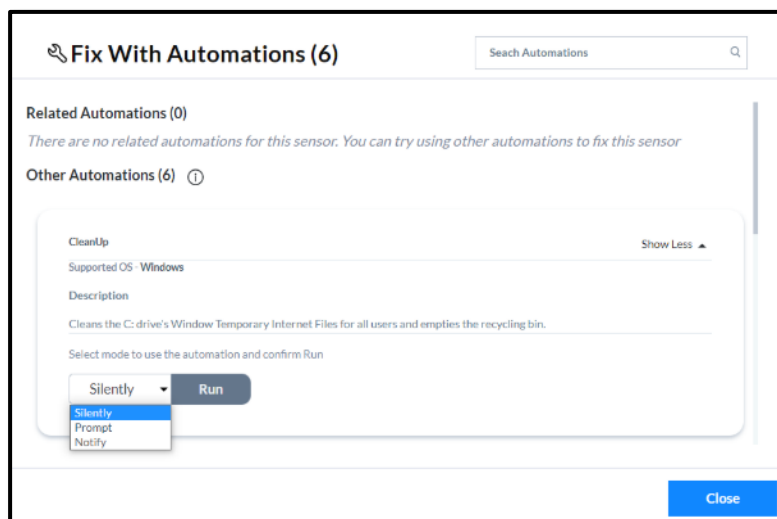
Issue Description	Troubleshooting Process
<p>Device Status - Pending</p>	<p>After onboarding your LDI Plus device if you see the device status is Pending, we recommend you restart the Universal Device Client service or your LDI Plus device.</p> <p>To restart the UDC client, select Services, search for Universal Device Client Service, and then Restart.</p> <p>Ensure that you have an active internet connection with access to *.uds.lenovo.com ports 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com port 443.</p> <p>You see the Device Status as Pending, if there is no license assigned to it or if the license for your device is expired, you will need to assign a license:</p> <ul style="list-style-type: none"> Click the Unactivated link and then click Assign License. <p style="text-align: center;">or</p> <p>Click your profile image and select Organization Account → Licenses → Assignments.</p>
<p>Device Status - Offline</p>	<p>You see the Device Status Offline if the device is unable to reach the cloud for more than 5 minutes.</p> <p>Ensure that your LDI Plus device has an active internet connection with access to *.uds.lenovo.com port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com port 443.</p>

If the device needs a VPN or proxy configuration	<p>Ensure that your LDI plus device allows the following domains and ports:</p> <ul style="list-style-type: none"> *uds.lenovo.com port 443 (include port 8883 if UDC agent older than 22.10.0.5) and *lakesidesoftware.com port 443
Other Installation Issues	<p>Provisioning Packs have a limited number of installations and expiration time.</p> <p>If you face an issue after using the same installation files for a while, select Help & Resources à Instructions and Agents to create a new Provisioning Pack for installations.</p>

1.1.11.4. [Device Lookup for Remediation Automation](#)

You can use the **Fix with Automations** feature for remediation automation.

1. Log in to LDI Plus.
2. Create your automations in Configuration → Insights & Automations.
3. Select **Device Lookup** → **Overview** and search for a device which has an issue.
4. In the Critical Sensors section, click the Fix with Automations link.



Related Automations section displays the sensor-related automations whereas **Other Automations** section displays other automation besides the sensor ones.

5. Click the **Run** drop-down list.

Note: You can select one of the following modes:

Silently – You can run the automation without sending any notifications to the user’s device. You see the message **Automation run successfully** in end. Select **Device Lookup** → **Tools** →

Automation History to see the details of the execution of the remediation automation such as run from, run by, automation time, related sensors, etc.

Prompt – You send a notification to the device and the device user needs has the option to select the prompt message to start the execution of remediation automation. Select **Configuration → Insights & Automations → Automations → Automations**. In the **Prompt** text box, enter the message that you want to notify the user.

Notify - You send a notification to the device about the execution of the remediation automation. The device user has no option to cancel the notification message.

Note: This feature is available for Virtual Machines and Windows (Physical) devices only and not for macOS devices as of now.

1.1.12 Install the Agent to a Virtual Machine

1. Follow instructions in [Download Provisioning Package](#).
2. Click **Confirm**. The **Instructions & Agents** page appears.
3. Click **Download**.
4. Copy the following files to an empty folder in the virtual device, e.g., C:\temp\LDI
 - Install-ldi.bat
 - README.txt
 - Install-ldiagent.ps1
 - Setup.exe
 - SysTrackCloudEdition.msi
 - VC_redist.x64.exe
 - VC_redist.x86.exe
5. Execute the batch file as an Administrator.
 - Open the command prompt as an administrator and execute `cd C:\temp\LDItemp`
 - Execute `.\Install-ldi.bat`

Note: Restart the device and wait for six hours for the device sync up and remain connected to network.

6. In the **Device Lookup** page, enter the virtual machine name in the **Search** text box to see the details.

1.1.13 Install the Agent to a macOS Device

Note: You can bulk deploy macOS LDI Plus devices using an endpoint manager tool.

1. Follow instructions in [Download Provisioning Package](#).
2. Click **Confirm**. The Instructions & Agents page appears.
3. Click Download.

Note: Once downloaded, complete the following additional steps to onboard device.

4. Run Install-Ldiagent.pkg.
5. Run the below command to complete the install.

```
sudo /Library/Application Support/Lakeside Software/Isiagentctl setup
```
6. Restart the device and wait for six hours for the device sync up.
7. In the **Device Lookup** page, enter the macOS device name in the **Search** text box to see the details.

1.1.14 Install the LDI Agent to macOS Devices using MDM / JAMF

1. Follow instructions in [Download Provisioning Package](#).
2. Click **Confirm**. The Instructions & Agents page appears.
3. Click Download.

Note: Once downloaded, complete the following additional steps to deploy using JAMF

4. Create a new flat package file (i.e. SysTrack.pkg) containing the agent installation Install-SysTrack.pkg file and the Isiagent.cfg file.
5. Create a preinstall script that expands the new package:

```
pkgutil --expand SysTrack.pkg /tmp/Lakeside
```
6. Add the silent install as a part of the preinstall script:

```
sudo installer -pkg /tmp/Lakeside/Install-SysTrack.pkg -target /
```
7. Copy the CFG file as a part of the preinstall script:

```
cp "/tmp/Lakeside/Isiagent.cfg" "/Library/Application Support/Lakeside Software/Isiagent.cfg"
```
8. Add a post-install script to delete the installation files:

```
sudo rm -rf /tmp/Lakeside
```

1.1.15 Check LDI Agent status and restart (macOS)

The control script must be run as root or with sudo.

Check usage options:

```
root# ./lsiagentctl
```

```
Usage: ./lsiagentctl {start|stop|restart|status}
```

Check the status of the agent:

```
root# ./lsiagentctl status
```

```
lsiagentd (pid 999) is running...
```

Restart the agent:

```
root# ./lsiagentctl restart
```

```
Restarting lsiagentd... done!
```

1.1.16 Install the LDI Agent to a Linux Device

Note: You can bulk deploy Linux LDI Plus devices using an endpoint manager tool.

1. Follow instructions in [Download Provisioning Package](#).
2. Click **Confirm**. The Instructions & Agents page appears.
3. Click Download.

Note: Once downloaded, complete the following additional steps to onboard device.

4. Navigate to the extracted location and change the rights of *SystemsManagementAgentLinux.sh* to all read, write, and executable.

The control script must be run as root or with sudo.

```
sudo chmod ugo=wrx ./SystemsManagementAgentLinux.sh
```

Note: *ls -lg* will allow you to check the current rights for that file

5. Install the Agent by running the *SystemsManagementAgentLinux.sh* script with the below parameters as needed.

The control script must be run as root or with sudo.

```
sudo ./SystemsManagementAgentLinux.sh install [proxy_params]
```

Script Parameters	Description	Example
install	Required – Must be first parameter	N/A
--config	Optional – Default SysTrack Configuration	SysTrack Test Config
--proxyconnectionhub	Optional – The name of their ProxyConnectionHub system (if applicable)	test.lakesidesoftware.org
--autodetectproxy	Optional – Preferred proxy setting: whether or not to use autodetect	N/A
--autoconfigscript	Optional – Preferred proxy setting: the address of a .pac file from which to get proxy information	http://test.lakesidesoftware.org/test.pac
--httpproxy	Optional – Preferred proxy setting: the address for the preferred HTTP proxy	127.0.0.1:80
--httpsproxy	Optional – Preferred proxy setting: the address for the preferred HTTPS proxy	127.0.0.1:443
--ftpproxy	Optional – Preferred proxy setting: the address for the preferred FTP proxy	127.0.0.1:21
--socketproxy	Optional – Preferred proxy setting: the address for the preferred Socket proxy	127.0.0.1:443

6. Restart the device and wait for six hours for the device sync up.
7. In the **Device Lookup** page, enter the Linux device name in the **Search** text box to see the details.

1.1.17 Uninstall LDI Agent (Windows)

Note: We recommend you use the Device Manager option to uninstall Universal Device Client (UDC) that ensures removal of UDC from both Windows and Driver Store.

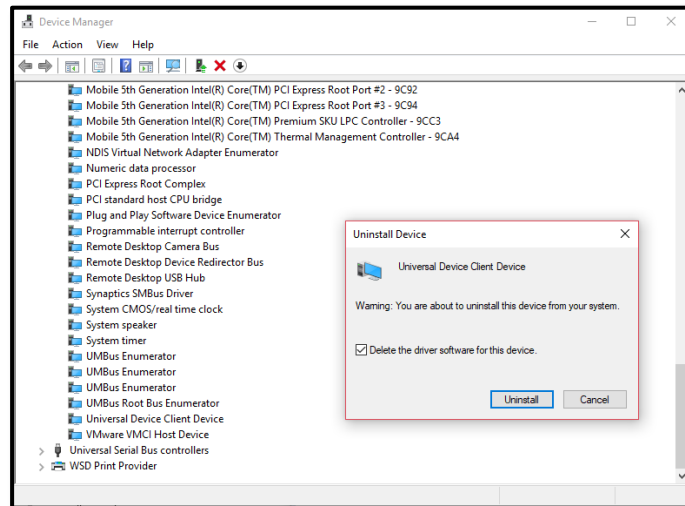
8. In the device, open the **Device Manager** page.
9. Select **System devices** and right-click **Universal Device Client Device**.
10. Select **Uninstall**.

Note:

- Select the **Delete the driver software for this device** check box.
- Continue to remove SysTrack as described below if the device is an LDI Plus.

11. Open Settings or Control Panel in your system to uninstall Systems Management Agent.

- **Settings → Add or Remove Programs → Systems Management Agent → Uninstall**
- **Control Panel → Programs and Features → Systems Management Agent → Uninstall**



12. Verify that there is no Universal Device Client Service in Device Manager or running service.
13. Restart the device.
14. In the LDI Plus portal, select **Device Manager → Devices**, search for that device and click **Delete**.

1.1.18 Uninstall LDI Agent with scripts (Windows)

Automated uninstall using Powershell

```
# This will uninstall UDC device, service, driver, & data
# Ensure running with elevated privileges
$udcInstall = Get-Item (Join-Path ([System.Environment]::SystemDirectory)
"drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe")
if($null -eq $udcInstall) { throw "Unable to locate UDC install files" }
Push-Location $udcInstall.Directory.FullName
& $udcInstall.FullName -uninstall
Pop-Location
```

Automated uninstall using Cmd

```
:: This will uninstall UDC device, service, driver, & data
:: Ensure running with elevated privileges
PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\
.\UDCInfInstaller.exe -uninstall
POPD
```

1.1.19 Uninstall LDI Agent (macOS)

To uninstall the LDI agent from a macOS device, run the below script in the macOS terminal
The control script must be run as root or with sudo.

```
sudo /Library/Application\ Support/Lakeside\ Software/uninstall_systrack.sh
```

1.1.20 Uninstall LDI Agent (Linux)

To uninstall the LDI agent from a Linux device, run the below script in the Linux terminal
The control script must be run as root or with sudo.

```
sudo ./SystemsManagementAgentLinux.sh remove
```

1.1.21 Additional Information

Following are some of the issues and their resolutions regarding virtual machine and macOS device installation:

Issue 1: Virtual machine/macOS is not onboarded to LDI Plus device.

Resolution: Verify that the correct version of installer is downloaded from the LDI Plus portal.

Issue 2: Virtual Machine/macOS is not found in the Device Lookup page.

Resolution: Wait for six hours after restarting your machine.

1.1.22 Onboard Your Fleet in a Proxy Environment

You can onboard your device using proxy setups.

Manual Proxy Setup section:

1. In the **Address** field, enter `https=exampleproxy.company.com:8888`
2. In the **Port** field, enter **8888**.

Edit proxy server
Use a proxy server

On

Proxy IP address: roxy.company.com:8888 Port: 8888

Use the proxy server except for addresses that start with the following entries.
Use semicolons (;) to separate entries.

*.uds.lenovo.com:443;
*.lakesidesoftware.com:443

Don't use the proxy server for local (intranet) addresses

Save Cancel

UDC and LDI Plus support the following proxy configurations:

- You must configure proxy through WinINET (vs WinHTTP or a 3rd party application / browser extension)
- Proxy server can reach *.[uds.lenovo.com:443](https://uds.lenovo.com) (include port 8883 if UDC agent older than 22.10.0.5) and *.lakesidesoftware.com:443
- Proxy server does DNS resolving for client
- Proxy server does NOT support authentication.

Note: UDC can register and sync telemetry on proxy environment by auto-detect the browser proxy settings (except if a user/password is required for such proxy access, which it is not supported).

UDC always imports whatever is configured in the browser settings (WinINET) automatically, though manual setting is done for WinHTTP.