



LDI User 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.

Revision History

Version	Published On	Description
1	24 March 2022	A consolidated User Guide comprising all other guides in it.
2	14 April 2022	Updated for 2.14 release
3	10 June 2022	Updated for ServiceNow Integration, Device Lookup and Windows Device Manager Errors sections.
4	8 August 2022	Updated with Ivanti Endpoint Manager Guide and Device / OS Support Matrix
5	25 August 2022	Updated for 2.18 release, notably revised to include new device status and Windows Device Manager Module Error Codes
6	29 September 2022	Updated for 2.19 release
7	8 December 2022	Updated for 2.21 release, notably removed portion inconsistent with LDI version, and revised network port requirements.
8	24 February 2023	Updated for 23.02 release, notably with more uninstallation options.
9	26 April 2023	Updated for 23.04 release, notably with Import Labels feature and ability to subscribe to status page within portal (https://ldistatus.uds.lenovo.com).
10	3 June 2023	Updated for 23.05 release, notably with daily report processing (instead of weekly), permissions consistency, and speed improvements.
11	9/13/2023	Updated to include battery replacement or repair info.

Contents

Contents	3
1 Overview	9
1.1 Use cases	9
1.2 Features and Licenses.....	9
1.3 Get Help When Using Tool	10
2 Onboard Your Fleet.....	11
2.1 Onboard Your Fleet	11
2.1.1 <i>Software Requirements.....</i>	<i>11</i>
2.1.2 <i>Download Provisioning Package.....</i>	<i>12</i>
2.1.3 <i>Install a Physical Device</i>	<i>12</i>
2.1.4 <i>Install Software Agent on Device</i>	<i>13</i>
2.1.5 <i>Track Device on LDI.....</i>	<i>15</i>
2.1.6 <i>Raise a Ticket.....</i>	<i>16</i>
2.1.7 <i>Onboard Fleet from Devices Page (Optional)</i>	<i>16</i>
2.1.8 <i>Proxy.....</i>	<i>17</i>
2.1.9 <i>Current Support Matrix.....</i>	<i>17</i>
2.1.10 <i>Limitations</i>	<i>17</i>
2.1.11 <i>Troubleshooting.....</i>	<i>18</i>
2.1.11.1. Pre-install Validation	18
2.1.11.2. Troubleshooting Process	18
2.1.12 <i>Uninstall UDC</i>	<i>19</i>
2.1.13 <i>Uninstall UDC with scripts.....</i>	<i>20</i>
2.1.14 <i>Onboard Your Fleet in a Proxy Environment.....</i>	<i>20</i>
2.2 LDI SCCM Quick Start Guide.....	21
2.2.1 <i>Overview</i>	<i>21</i>
2.2.2 <i>Purpose</i>	<i>21</i>
2.2.3 <i>Prerequisite</i>	<i>21</i>
2.2.4 <i>Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Application Mode</i>	<i>21</i>
2.2.4.1. Create an Application	21
2.2.4.2. Add Deployment Type to the Application	22
2.2.4.3. Select Deployment Setting	23
2.2.4.4. Specify Content Settings for Delivery to Devices.....	23
2.2.4.5. Specify Detection Rule	24

2.2.4.6.	Configure User Experience Settings	25
2.2.4.7.	Deploy the LDI Provisioning Package in SCCM to the Fleet of Devices	26
2.2.4.8.	Select Application for Deployment to the Device Group	26
2.2.4.9.	Specify Content Destination	27
2.2.4.10.	Known Issues	28
2.2.5	<i>Scheduling</i>	28
2.2.6	<i>User Experience</i>	29
2.2.7	<i>Alerts</i>	29
2.2.8	<i>SCCM Uninstall UDC Client</i>	30
2.2.8.1.	Select the Application to Uninstall	30
2.2.8.2.	Specify Content Destination	31
2.2.9	<i>Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Package Mode</i>	31
2.2.9.1.	Create a Package	31
2.2.9.2.	Create a Program	33
2.2.9.3.	Deploy Provisioning Package	37
2.2.9.4.	Specify Content Destination	39
2.2.9.5.	Deployment Settings	41
2.2.9.6.	User Experience	43
2.2.9.7.	Distributions Points	43
2.3	Microsoft InTune	45
2.3.1	<i>Purpose</i>	45
2.3.2	<i>Prerequisite</i>	45
2.3.3	<i>Configure Microsoft InTune to Deploy LDI Provisioning Package</i>	45
2.3.4	<i>Create .intunewin Package</i>	45
2.3.5	<i>Register an Application</i>	46
2.3.6	<i>Provide a Permission</i>	47
2.3.7	<i>Create and Add Windows Application to InTune</i>	49
2.3.8	<i>Deploy Application</i>	54
2.4	<i>Ivanti</i>	56
2.4.1	<i>Executable Properties</i>	56
2.4.2	<i>Windows Action Properties</i>	56
3	Configure LDI	58
3.1	Manage access	58
3.1.1	<i>User Creation</i>	58
3.1.2	<i>Assign User(s) to a User Group from the Users page</i>	61

3.1.2.1.	User Groups.....	62
3.1.2.2.	Manage User Group	62
3.1.3	<i>Password change</i>	62
3.1.4	<i>Authentication Types</i>	63
3.1.5	<i>Azure Active Directory, Okta and LenovoID</i>	63
3.2	Manage Devices	63
3.2.1	<i>Device manager screens, inspect device fix onboarding issues</i>	63
3.3	Org Settings vs Configuration.....	64
3.3.1	<i>Organization Setup</i>	64
3.3.2	<i>Manage Organization</i>	64
3.3.2.1.	Set Portal Language	65
3.4	Organization Settings.....	66
4	Monitor your fleet	67
4.1	Dashboards	67
4.1.1	<i>Dashboard Enhancements</i>	68
4.1	Issues and Reports.....	69
4.2.1	<i>System Crashes (BSODs)</i>	69
4.1.1.	<i>Mark the Issue as Resolved</i>	76
4.2	Device Lookup.....	77
4.3	Device Manager	78
4.3.1	<i>Add Devices</i>	78
4.3.2	<i>Manage Devices</i>	78
4.3.2.1.	Delete or Remove a Device	79
4.3.2.2.	Rename a Device	79
4.3.3	<i>Notifications</i>	81
4.3.3.1.	Email Notification on Fleet.....	81
4.3.3.2.	Customize Alarms and events	81
4.3.3.3.	Windows Device Manager Errors.....	81
5	Integrate with Outside Systems	83
5.1	RESTful API	83
5.2	Purpose.....	83
5.3	Audience.....	83
5.4	Get API Credentials.....	83
5.5	Learn API Operations.....	86
5.6	Try APIs.....	87

5.7	Examples of API Methods	88
5.7.1.1.	Authentication - API token session	88
5.7.1.2.	HTTP Samples	89
5.8	Negative API Sample.....	90
5.8.1.1.	Groovy ACME Test.....	90
5.9	User Management.....	91
5.9.1	<i>GET Users</i>	93
5.9.2	<i>Create User</i>	94
5.9.3	<i>Delete User</i>	95
5.10	Devices.....	96
5.10.1.1.	ACME Client Code.....	96
5.10.1.2.	HTTP Request Responses.....	97
5.11	Fleet Management	98
5.12	Insights Tests.....	98
5.12.1.1.	Request	99
5.13	Issues Filter	100
5.14	Mark Issue as Resolved.....	101
5.15	Sensors	103
5.16	ServiceNow Integration	104
5.16.1	<i>Audience</i>	104
5.16.2	<i>Prerequisites</i>	104
5.16.3	<i>Import and Install Lenovo XML File in ServiceNow</i>	105
5.16.4	<i>Authenticate LDI API Credentials in ServiceNow</i>	108
5.16.5	<i>Synchronize Assets in ServiceNow and LDI</i>	110
5.16.6	<i>Mandatory Requirements for LDI CSV Format</i>	113
5.16.7	<i>Update Asset Information from ServiceNow to LDI Account</i>	113
5.16.8	<i>Integrate ServiceNow into LDI Tool</i>	115
5.16.9	<i>Create a ServiceNow Incident Rule</i>	116
5.16.10	<i>Handle an Incident in ServiceNow</i>	117
6	Appendix	119
6.1	Remediation Scripts Help.....	119
6.2	Device Support Matrix.....	138
6.2.1	<i>LDI OEM and OS Support Matrix</i>	138
6.3	Windows Device Manager Module Error Codes.....	139
	<i>Code 1 "This device is not configured correctly. (Code 1)"</i>	139

Code 3 "The driver for this device might be corrupted... (Code 3)"	139
Code 9 "Windows cannot identify this hardware... (Code 9)"	140
Code 10 "This device cannot start. (Code 10)"	141
Code 12 "This device cannot find enough free resources that it can use... (Code 12) " ..	141
Code 14 "This device cannot work properly until you restart your computer. (Code 14)" ..	142
Code 16 "Windows cannot identify all the resources this device uses. (Code 16)"	143
Code 18 "Reinstall the drivers for this device. (Code 18)"	143
Code 19 "Windows cannot start this hardware device... (Code 19)"	144
Code 21 "Windows is removing this device...(Code 21)"	145
Code 22 "This device is disabled. (Code 22)"	146
Code 24 "This device is not present, is not working properly... (Code 24)"	146
Code 28 "The drivers for this device are not installed. (Code 28)"	147
Code 29 "This device is disabled... (Code 29)"	147
Code 31 "This device is not working properly... (Code 31)"	147
Code 32 "A driver (service) for this device has been disabled. (Code 32)"	148
Code 33 "Windows cannot determine which resources are required for this device. (Code 33)" ..	149
Code 34 "Windows cannot determine the settings for this device... (Code 34)"	149
Code 35 "Your computer's system firmware does not... (Code 35)"	150
Code 36 "This device is requesting a PCI interrupt... (Code 36)"	150
Code 37 "Windows cannot initialize the device driver for this hardware. (Code 37)" ...	151
Code 38 "Windows cannot load the device driver... (Code 38)"	151
Code 39 "Windows cannot load the device driver for this hardware... (Code 39)."	152
Code 40 "Windows cannot access this hardware... (Code 40)"	152
Code 41 "Windows successfully loaded the device driver... (Code 41)"	153
Code 42 "Windows cannot load the device driver... (Code 42)"	154
Code 43 "Windows has stopped this device because it has reported problems. (Code 43)" ..	154
Code 44 "An application or service has shut down this hardware device. (Code 44)" ...	155
Code 45 "Currently, this hardware device is not connected to the computer... (Code 45)" ..	155
Code 46 "Windows cannot gain access to this hardware device... (Code 46)"	156
Code 47 "Windows cannot use this hardware device... (Code 47)"	156
Code 48 "The software for this device has been blocked... (Code 48)."	157
Code 49 "Windows cannot start new hardware devices... (Code 49)."	157

<i>Code 50 "Windows cannot apply all of the properties for this device... (Code 50)"</i>	<i>158</i>
<i>Code 51 "This device is currently waiting on another device... (Code 51)."</i>	<i>159</i>
<i>Code 52 "Windows cannot verify the digital signature for the drivers required for this device. (Code 52)"</i>	<i>159</i>
<i>Code 53 "This device has been reserved for use by the Windows kernel debugger... (Code 53)"</i>	<i>159</i>
<i>Code 54 "This device has failed and is undergoing a reset. (Code 54)"</i>	<i>160</i>

1 Overview

Lenovo Device Intelligence (LDI) is an enhanced predictive and proactive SaaS tool for the smarter PC fleet management. Lenovo Device Intelligence Plus gives enterprise IT Administrators advanced predictive insights to help pinpoint hardware and systemic issues before they occur.

Delivering in-depth device and business insights, the LDI solution is an AI-powered SaaS PC health management tool. The solution identifies critical issues across the fleet, both current and potential, monitors for hardware failures, Blues Screen of Death (BSODs), and system and software applications causing performance degradation. For the organization requiring smarter insights into PC health, LDI features a deeper level of analytics such as persona analysis, digital user experience scoring, asset optimization, productivity impact assessments, root cause analysis, sector benchmark comparisons, remediate issues, and more. This enables customers to monitor, analyse, predict, prevent, and optimize their IT environments for better business outcomes.

1.1 Use cases

LDI software through its predictive analytics of device functioning and issue detection capability helps the organization to:

- Reduce support calls
- Reduce breakdowns and increase device uptime and productivity
- Improve customer experience

An IT Manager, Analyst, or Administrator can use this tool to predict, detect, and resolve issues before they negatively impact employees' productivity.

Features and tools are available to address use cases in LDI. For more details, refer to [LDI Test Drive](#).

1.2 Features and Licenses

LDI enables you to proactively support the system users through AI and ML techniques to predict the failures that might occur in users' devices.

Besides, you can monitor device performance in real-time, detect, and report the issues when they occur.

LDI also provides:

- Options to execute issue fixes
- Root cause and correlation analysis capabilities
- Application comparative and trend analytics
- Assessment of IT's impact on employee productivity
- Digital UX scoring to quantify end-user experience with their IT resources
- External and internal data benchmarking
- Employee workstyle personas mapped to IT resources

- Asset optimization analytics to help size hardware and software investments

1.3 Get Help When Using Tool

This chapter provides you valuable information about how to put the product to use.

You can reach out to LDI support in multiple ways to get help if you face any issues in using the tool:

- Report the problem to the support team. Send an email to LDI support@lenovo.com.
- Report the problem in the interface. Refer to [Raise a Ticket](#).

2 Onboard Your Fleet

2.1 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.

2.1.1 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 or verified on the Lenovo devices.
Operating System	Windows 10 version 1809 (October 2018 Update) or newer Windows 11 64-bit OS Special editions such as 10S or 10x are not currently supported
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 ports 443 <ul style="list-style-type: none"> Port 8883 needed for devices with UDC agent older than 22.10.0.5 Proxy is supported in some scenarios. Devices may require additional configuration to support.

Category	Requirement
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 ports 443 <ul style="list-style-type: none"> Port 8883 needed for devices with UDC agent older than 22.10.0.5 <p>DNS name resolution is available on each managed device. You cannot set an authentication on the proxy server.</p>

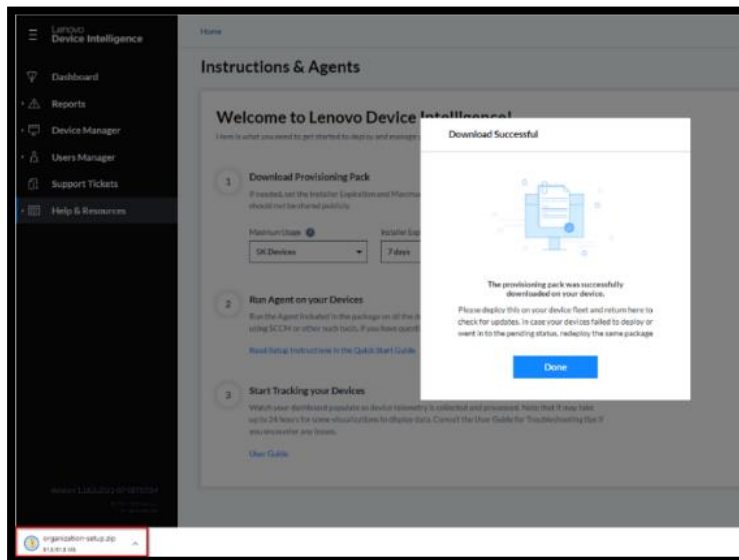
2.1.2 [Download Provisioning Package](#)

You can onboard fleet of devices to LDI platform through:

- Instructions and Agents (Preferred)
 - Devices page (optional)
1. 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](#).

2.1.3 [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

This PC > Downloads > organization-setup.zip

Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
install-Ldi.bat	Windows Batch File	1 KB	No	1 KB	27%	11/8/2021 9:09 AM
LenovoDeviceIntelligence-0.0.75.0...	Troubleshooting Pack Ca...	91 KB	No	95 KB	5%	11/8/2021 9:09 AM
README.txt	Text Document	1 KB	No	2 KB	50%	11/8/2021 9:09 AM
udc_setup.exe	Application	10,991 KB	No	11,103 KB	2%	11/8/2021 9:09 AM

2.1.4 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\LDI temp
 - 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\LDI temp`
 - `.\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 UDC Service 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

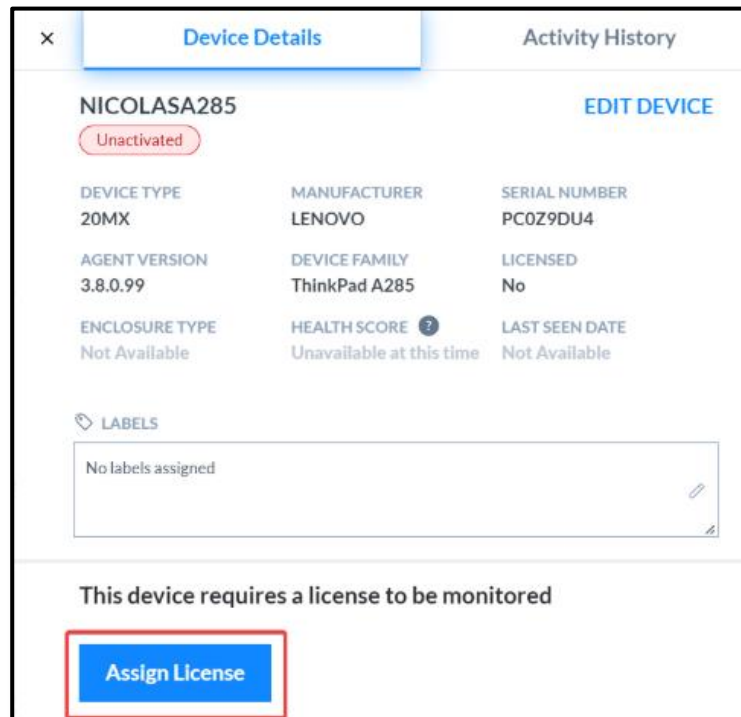
		<p>portal. Restart UDService and try again. If it fails, contact the administrator.</p> <p>To restart the UDC Service, follow these options: Press Windows + R → Enter services.msc → Select UDC Client Service → Restart</p> <p>Restart the device and log in to the LDI portal again.</p>
1011	RegistrationTo Organization Failed	<p>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.</p> <p>Note: Check for the log files in C:\ProgramData\Lenovo\Udc\Log</p> <p>ConfigAgent log file informs you if the config policy has been updated from UDS</p> <p>DeployAgent log file informs you if the package has been installed successfully.</p> <p>Navigate to C:\ProgramData\Lenovo\Udc\Download to see the Provisioning Package ID.</p>

2.1.5 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'

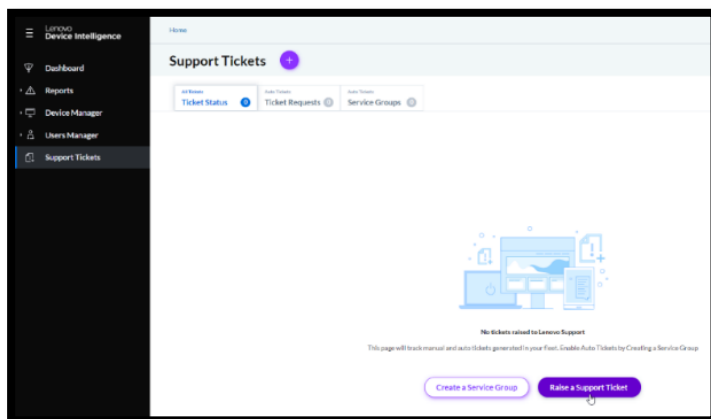


3. Click **Assign License**.

- **Offline** - Devices that do not send data to the system for 1 hour. These devices are moved from Active Status to Offline Status. If the device does not have a license, it becomes Unactivated with status Pending.

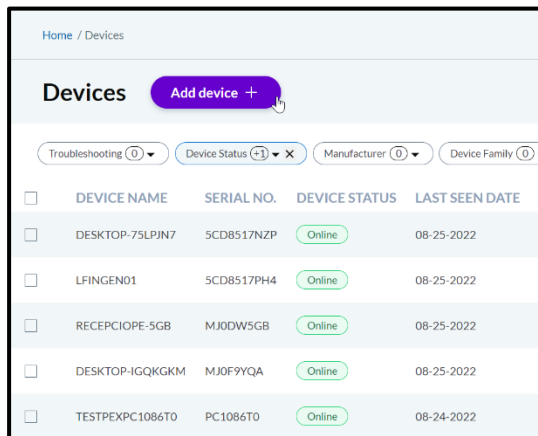
2.1.6 Raise a Ticket

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



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

2.1.8 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.

2.1.9 Current Support Matrix

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

2.1.10 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.

2.1.11 Troubleshooting

When you are unable to register your device in the LDI 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.

2.1.11.1. Pre-install Validation

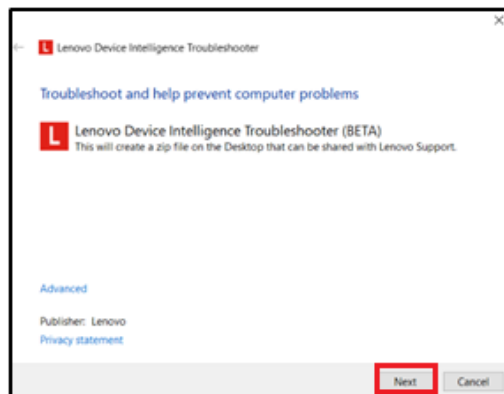
Note the following information for the API accessibility in different settings:

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

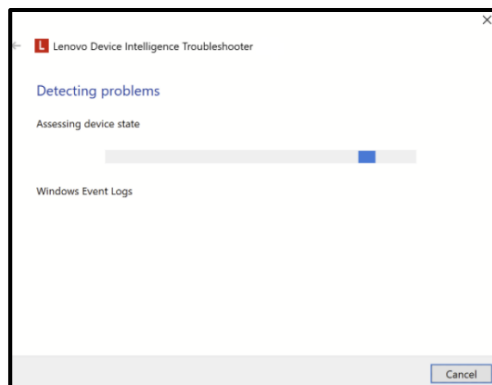
2.1.11.2. Troubleshooting Process

Follow these steps to troubleshoot:

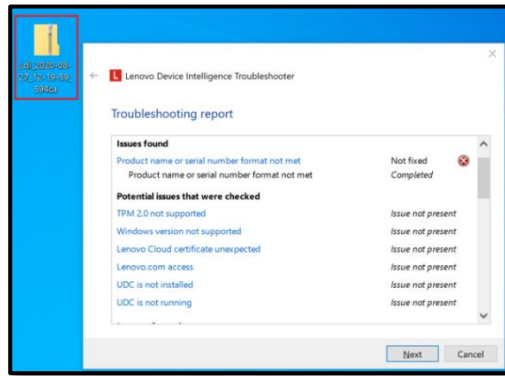
1. Double-click the `LenovoDeviceIntelligence.diagcab` file. The following window appears.



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



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



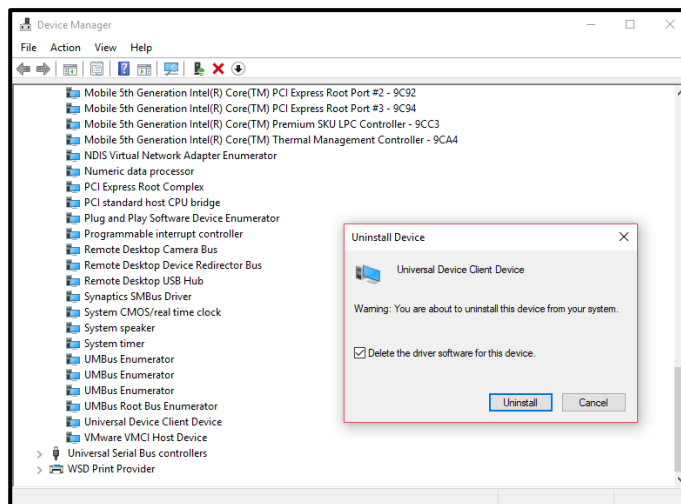
Note: By default, the output is a zip file, and it also displays the location where the file is saved.

2.1.12 Uninstall UDC

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.

1. In the device, open the **Device Manager** page.
2. Select **System devices** and right-click **Universal Device Client Device**.
3. Select **Uninstall**.

Note: Select the **Delete the driver software for this device** check box.



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

2.1.13 Uninstall UDC with scripts

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
```

2.1.14 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 *.uds.lenovo.com
2. In the **Port** field, enter **443**.

Edit proxy server

Use a proxy server

☒ On

Proxy IP address: proxy.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 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 (include port 8883 if UDC agent older than 22.10.0.5)
- 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.

2.2 LDI SCCM Quick Start Guide

2.2.1 Overview

The LDI SCCM QSG chapter explains how to use System Center Configuration Manager (SCCM) to deploy the LDI Provisioning Package on the fleet of devices in your organization.

You can use following methods to deploy the package:

- Configure SCCM to deploy LDI Windows (Physical) Package on the Devices in the **Application Mode**
- Configure SCCM to deploy LDI Windows (Physical) Package on the Devices in the **Package Mode**

2.2.2 Purpose

You can configure SCCM to install the LDI Provisioning Package on all the devices in your organization and register them as per the Service License Agreement between your organization and LDI Solutions. Instead of installing the provisioning package on each device, you can use SCCM to run it on the entire fleet of device.

2.2.3 Prerequisite

Download the LDI Provisioning Package on the device on which you want to configure SCCM and deploy the package on the entire fleet of devices in your organization. To know how to download and install the package, refer to [Onboard Your Fleet](#).

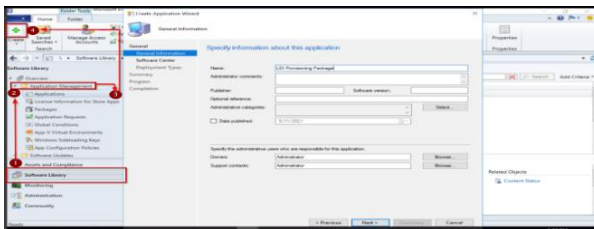
2.2.4 Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Application Mode

2.2.4.1. Create an Application

Copy the following files downloaded from the LDI Windows (Physical) package to a folder in the computer with an account of the site server that has READ permission.

- Udc_setup.exe
- LenovoDeviceIntelligence-0.0.75.0.diagcab
- README.txt

- install-LDI.bat



In the SCCM account:

1. Click the **Software Library** tab. The Software Library window appears.
2. Click the **Applications Management** folder. The Application window appears.
3. Click **Applications**.

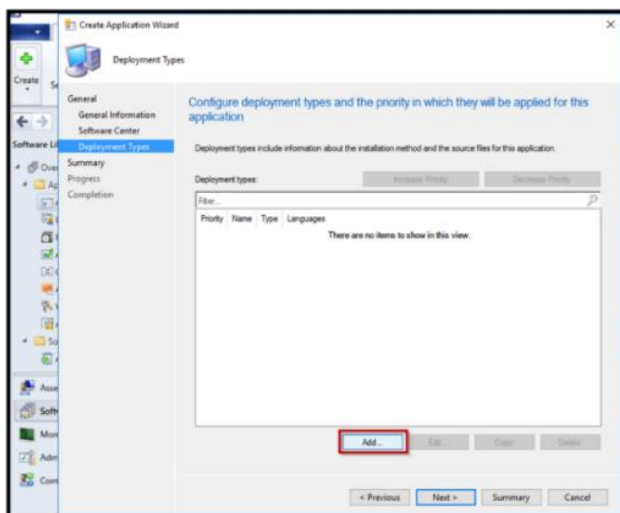
Create Application Wizard

Enter information about a new application in the SCCM. Fill-in the name, version, and publisher of the application. You can also select the administrative owners (users) and category of the application.

4. Click **Create**. The **Create Application** window appears.
5. Click **Next**. The **Deployment Types** page appears.

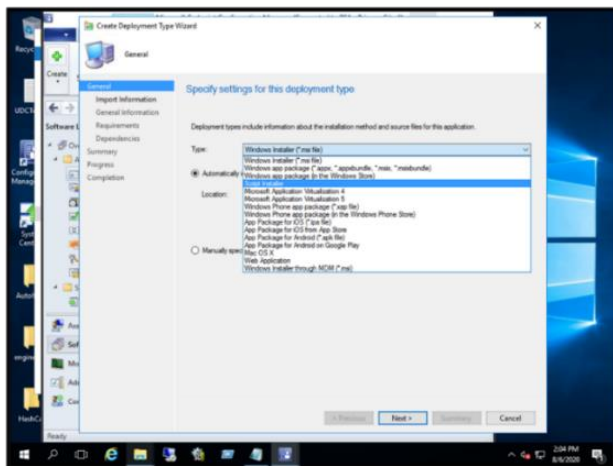
The new application is registered in SCCM. The next section **Deploy the Application** describes the steps to deploy the new application.

2.2.4.2. Add Deployment Type to the Application



In the **Deployment Types** page, click **Add** and then click **Next**. A window appears that shows a list of options.

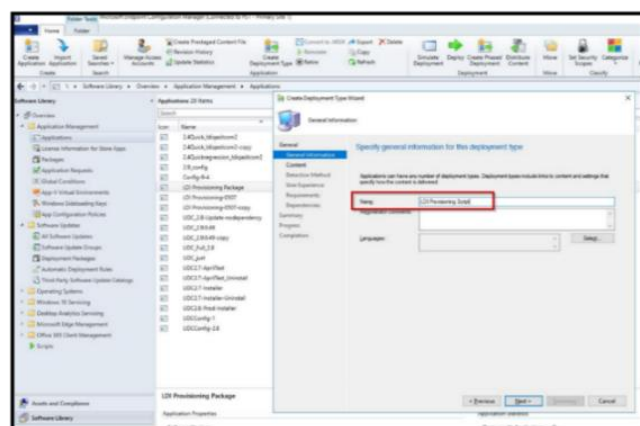
2.2.4.3. Select Deployment Setting



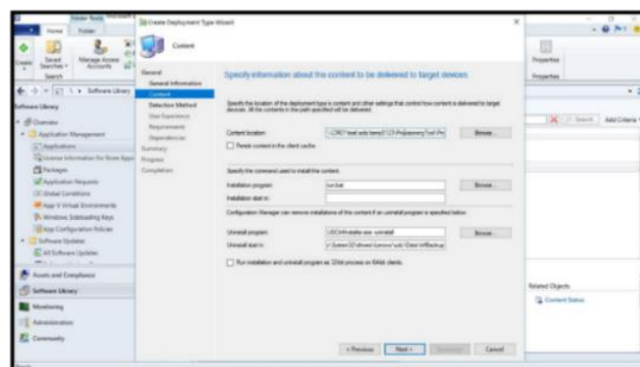
1. Select **Script Installer**.
2. Click **Next**.

2.2.4.4. Specify Content Settings for Delivery to Devices

3. Enter **Name** of the application. For example, LDI Provisioning Script.
4. Click **Next**. The **Content - the Create Deployment Type** window appears.

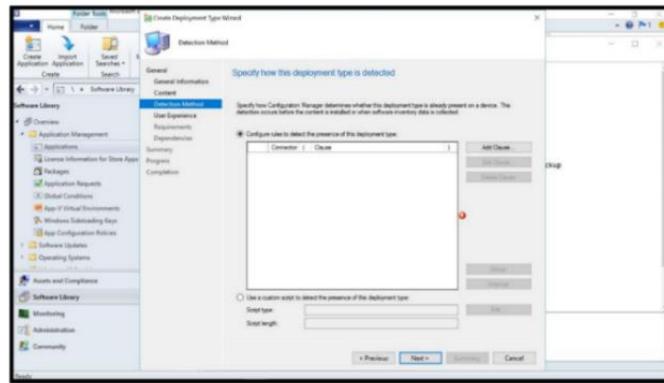


5. In the **Content** page, specify the path of the folder that has all files.



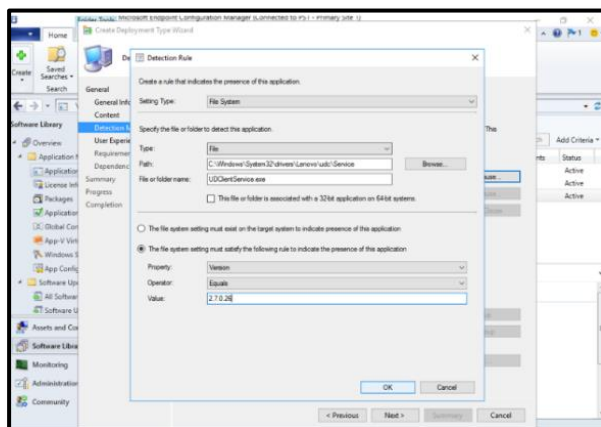
6. In the **installation program** field, enter the command - **install-LDI.bat**. If the target device is a virtual machine, then enter the command **Setup.exe /VERYSILENT**.
7. In the **Uninstall program** field, enter the command - **UDCInflInstaller.exe -uninstall**.

8. In the Uninstall start field, enter the command
- **C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup**
9. Click **Next**. A window appears.
10. In the window, specify how the deployment type is detected.
11. Click **Add Clause**.



12. Click **Next**. The **Detection Rule** window appears.

2.2.4.5. Specify Detection Rule



In the **Detection Rule** window, configure the detection rules as follows:

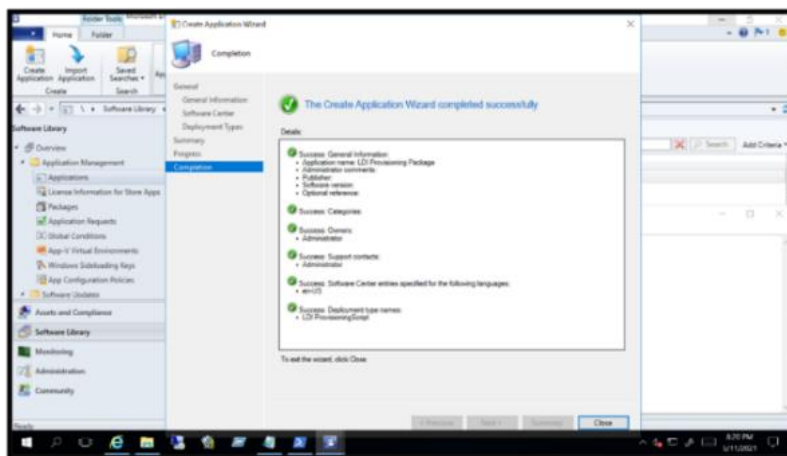
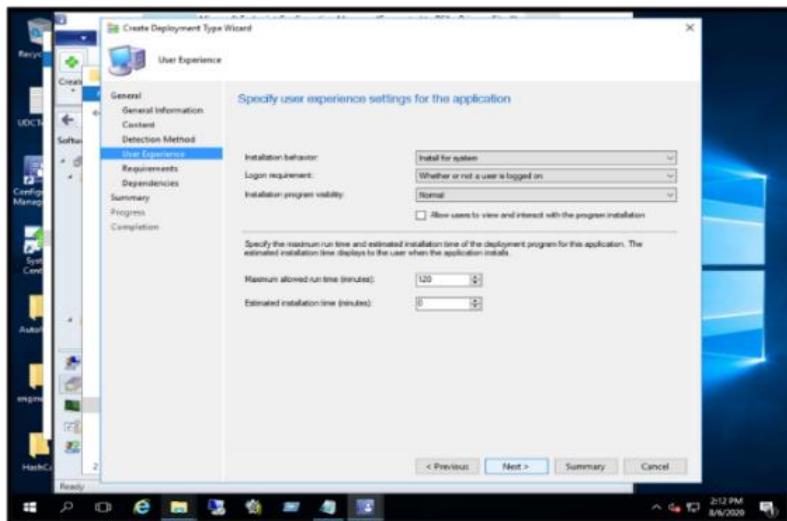
1. In the **Setting Type** field, select **File System**.
2. In the **Path** field, enter C:\Windows\System32\drivers\Lenovo\udc\Service.
3. In the **File or folder name** field, enter UDClientService.exe
4. Note: De-select the This file or folder is associated with a 32-bit application on 64-bit system checkbox.
5. Select The file system setting must satisfy the following rule to indicate the presence of this application radio button.
6. In the **Property** drop-down list, select **Version**.

7. In the **Operator** drop-down list, select **Equals**.
8. In the **Value** field, enter the current UDC version.
9. Click **OK**.
10. Click **Next**.

2.2.4.6. Configure User Experience Settings

In the **User Experience** page, follow these steps:

1. In the Installation behavior field, select **Install for a system**.
2. In the Logon requirement field, select **Whether or not a user is logged on**.
3. In the Installation program visibility field, select **Normal**.
4. Click **Next**.

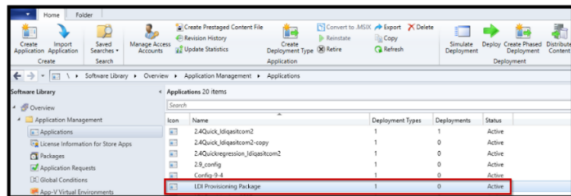


Complete the rest of the wizard to create the deployment type for the application.

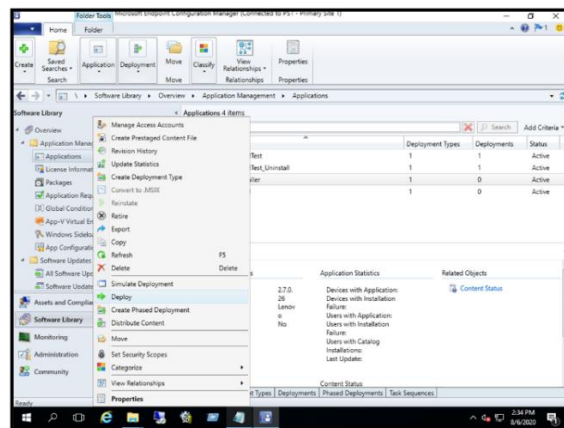
2.2.4.7. Deploy the LDI Provisioning Package in SCCM to the Fleet of Devices

After you register the LDI provisioning pack and configure the deployment settings in the SCCM account, you must deploy or assign the application to a group or fleet of devices in the organization.

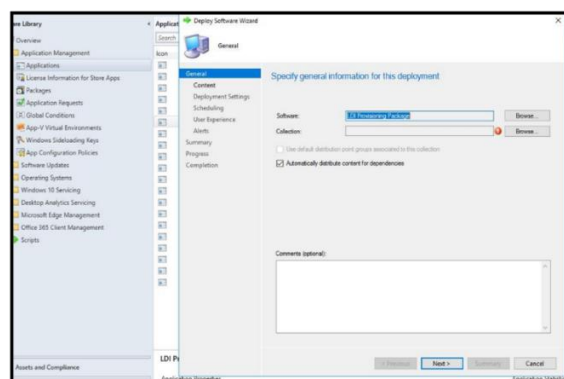
2.2.4.8. Select Application for Deployment to the Device Group



5. Select the application. For example, LDI Provisioning Package.
6. Right-click the selected application. A pop-up window appears.



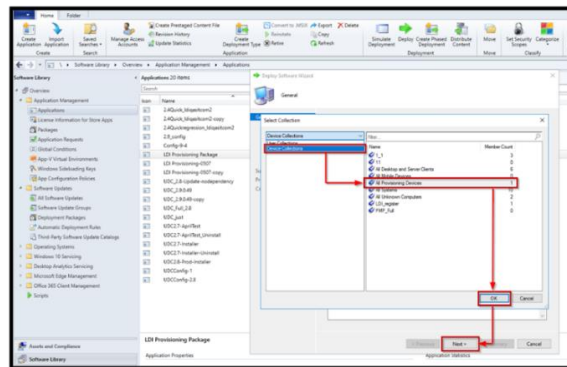
7. Click **Deploy**.



In the **General** page in the **Deploy Software Wizard**:

8. Click **browse** to select the software package. For example, LDI Provisioning Package.

9. In the **Collection** field, click **browse**. The **Select Collection** window appears.



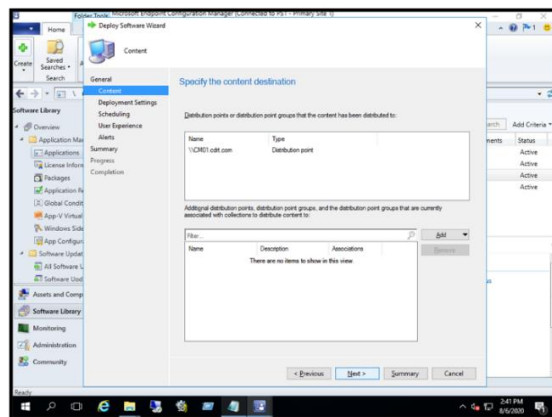
10. In the **Select Collection** window, click **Device Collections**. A list of device collections appears.

Device Collection

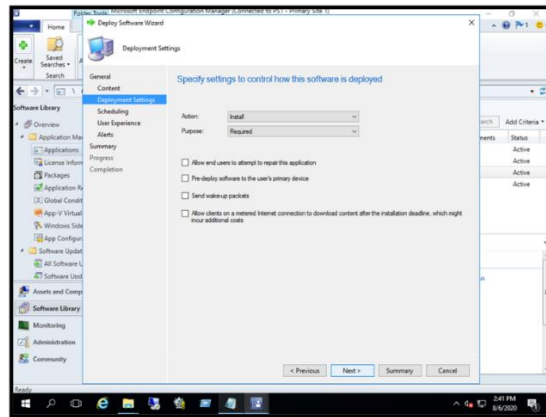
The fleet or group of devices. For example, the fleet of devices in your organization that is to be onboarded to the LDI platform.

2.2.4.9. Specify Content Destination

1. Specify the distribution point where the collection of devices is to be deployed.
2. Click **Next**.



3. Select the deployment settings for the software. For example, LDI Provisioning Package.



4. In the **Action** field, select **Install**.
5. in the **Purpose** field, select **Required**.

Mandatory

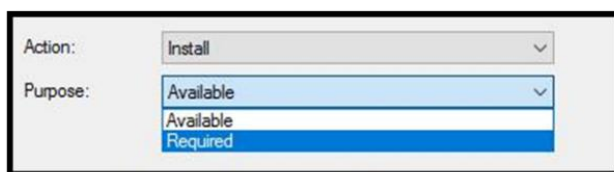
Select the **Required** option to install UDC Installer software.

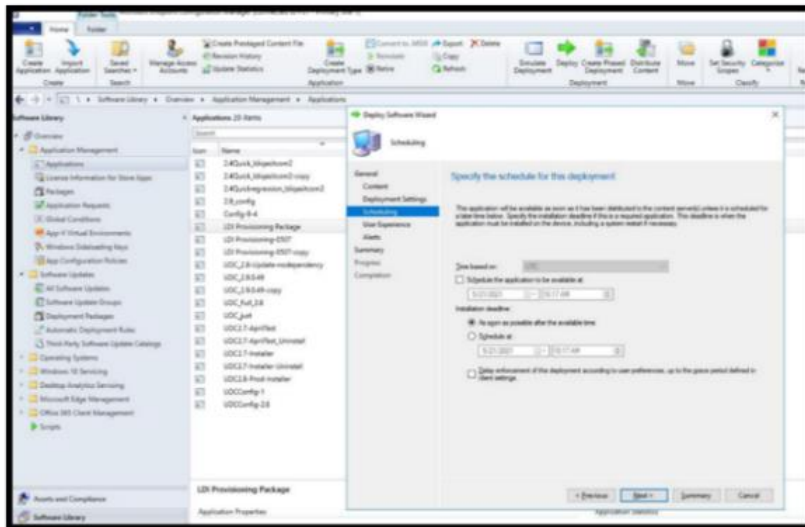
2.2.4.10. Known Issues

Error Code	Error Description	Root Cause	Workaround
0x87D00324	When you test the SCCM deployment, a notification Installation Failed appears on end user's desktop, however the package is installed successfully.	The software detection rule was not found.	In the Deploy Software Wizard page, select User Experience . Then, in the User notifications drop-down list, select Hide in Software Center and all notifications .

2.2.5 Scheduling

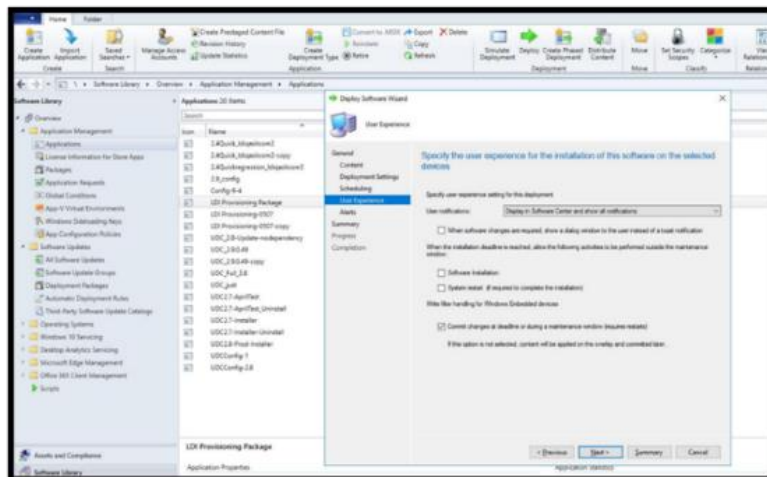
Leave the Scheduling settings as default.





2.2.6 User Experience

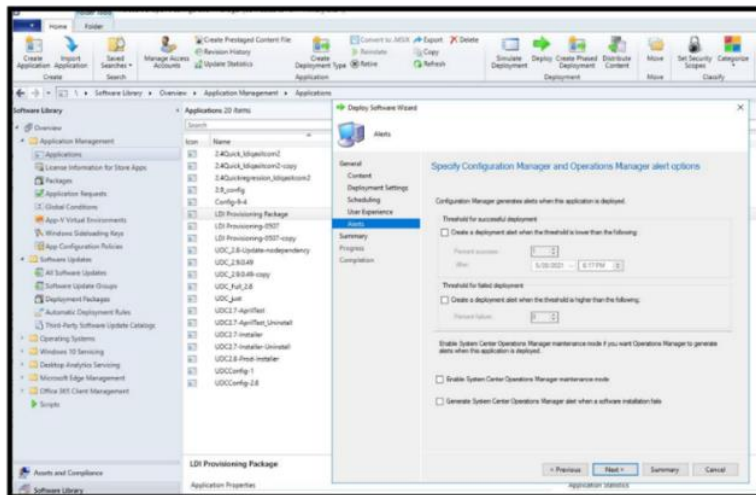
You are advised to leave the User Experience settings as default.



2.2.7 Alerts

You are advised to leave the Alerts settings as default.

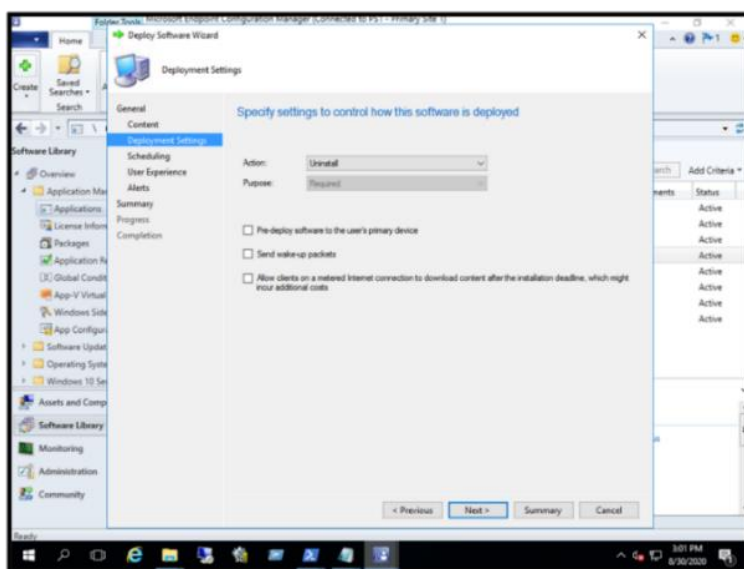
Complete the rest of the wizard to complete the deployment.



Verify if the devices in the Device Collection that are deployed with this application can successfully finish the installation.

Verify in the LDI portal if the devices are successfully activated.

2.2.8 SCCM Uninstall UDC Client



To uninstall the LDI Agent, for example, UDC service, follow these steps:

2.2.8.1. Select the Application to Uninstall

1. In the **Applications** tab, select the application.
2. Right-click the application.
3. Click **Deploy**.
4. Select the Group of Device.
5. Click Device Collection.
6. Select the Automatically distribute content for dependencies checkbox.

2.2.8.2. Specify Content Destination

Specify Settings to Control Software Deployment

Action: **Uninstall**

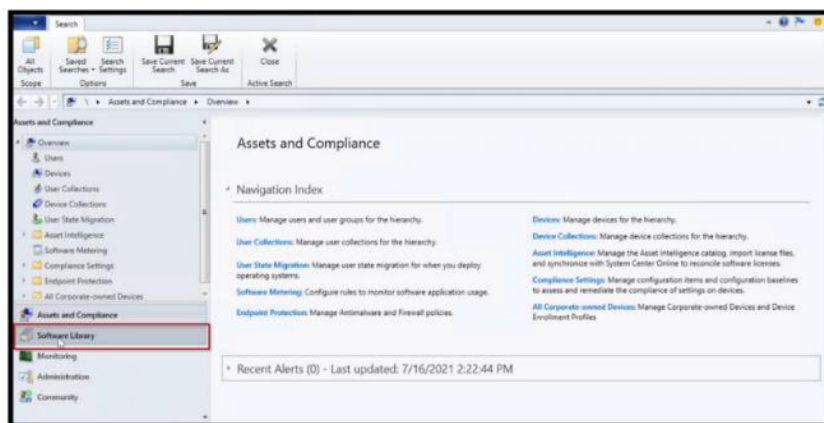
Purpose: **Required**

1. Complete the Uninstall Process.
2. Verify if the devices in the Device Collection that are deployed with this uninstall deployment, have UDC software uninstalled from them.
3. In the LDI portal, delete the devices before running the provisioning tool again.

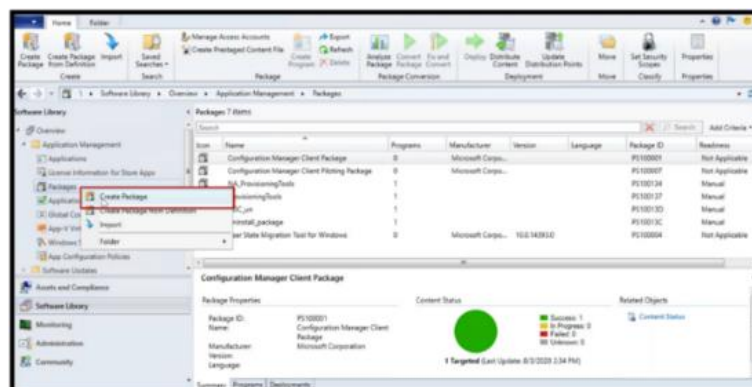
2.2.9 Configure SCCM to Deploy LDI Windows (Physical) Package on the Devices in the Package Mode

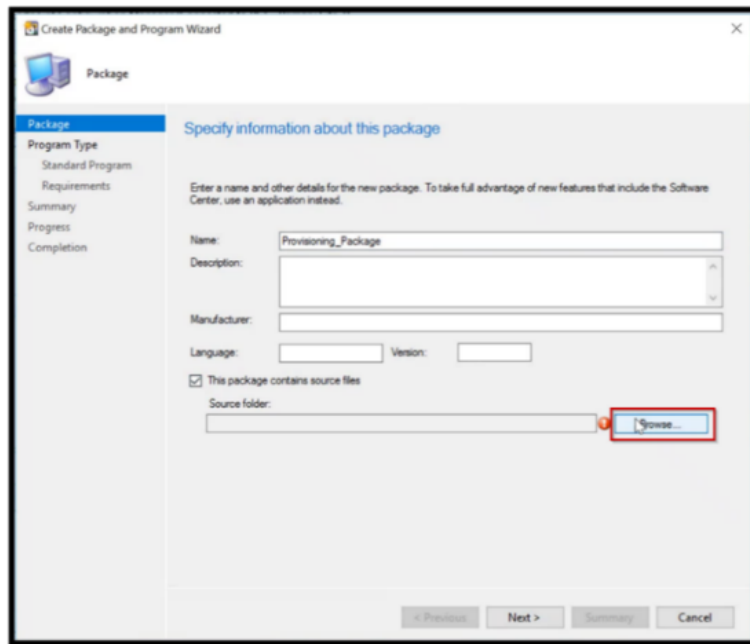
2.2.9.1. Create a Package

1. Log in to the SCCM Account.
2. In the navigation menu, click **Software Library**. The **Software Library** window appears.

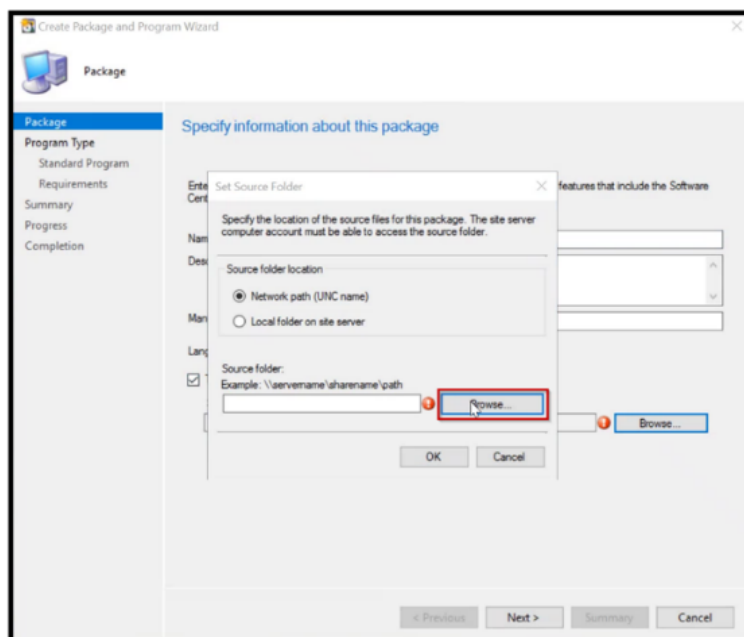


3. Click **Application Manager** folder to view the sub menu.
4. Right-click **Packages**.
5. Right-click **Create Package**. The form field appears where you can enter details about the package.

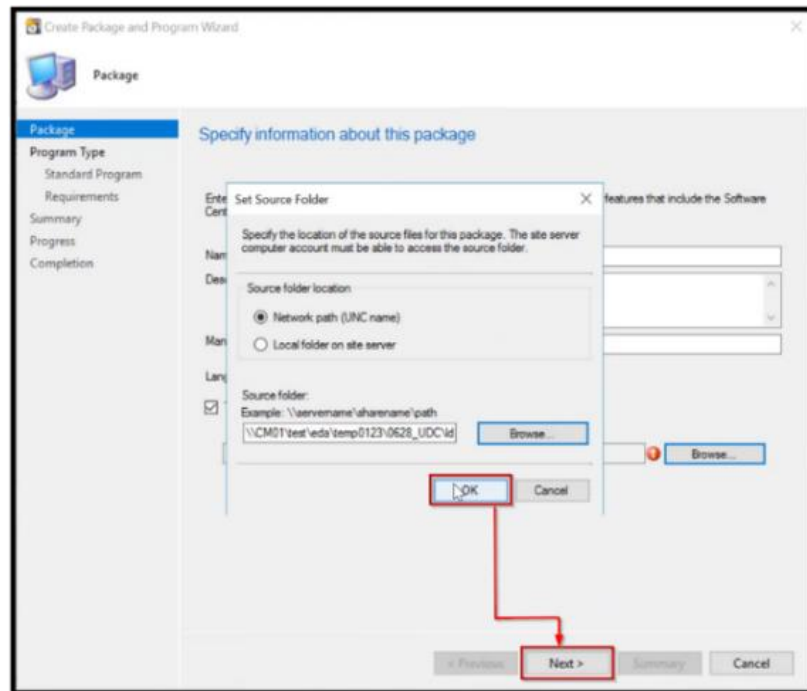




6. Enter the **name** of the package. For example, Provisioning Package.
7. Select the **checkbox**. This package contains the source file.
8. Click **Browse**.



9. In the Create Package and Program Wizard window, click Browse.
10. Select the **folder**. For example, LDI26_UDC.
11. Click **Select Folder**. A pop-up window appears.



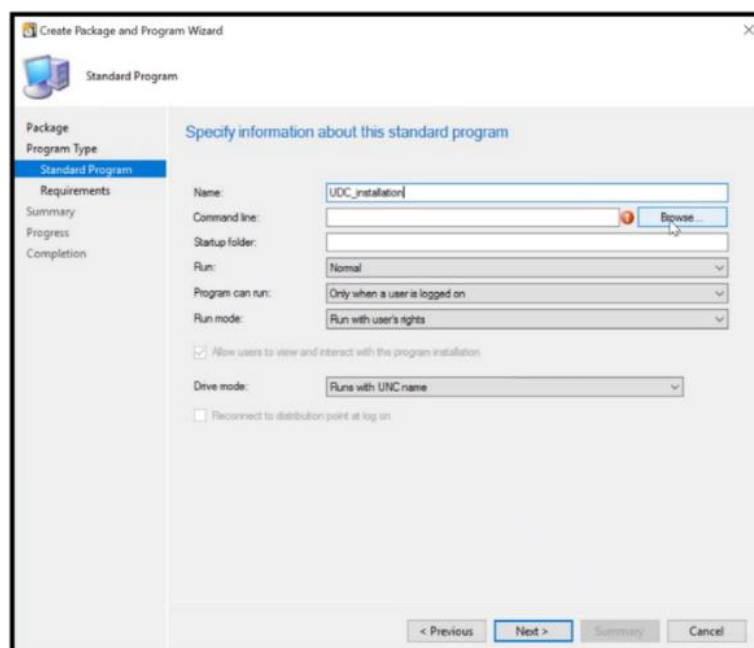
The window shows the path of the selected folder.

12. Click **OK**.

13. Click **Next**. In the **Program Type** section, select the type of program you want to create.

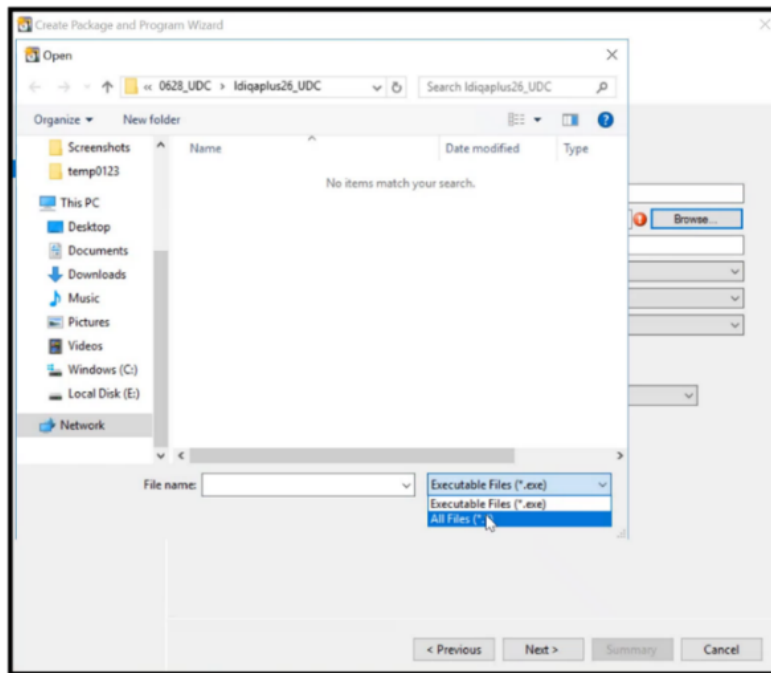
2.2.9.2. Create a Program

1. Select Standard program.
2. Select **Next**. You see form field for the creating the program.

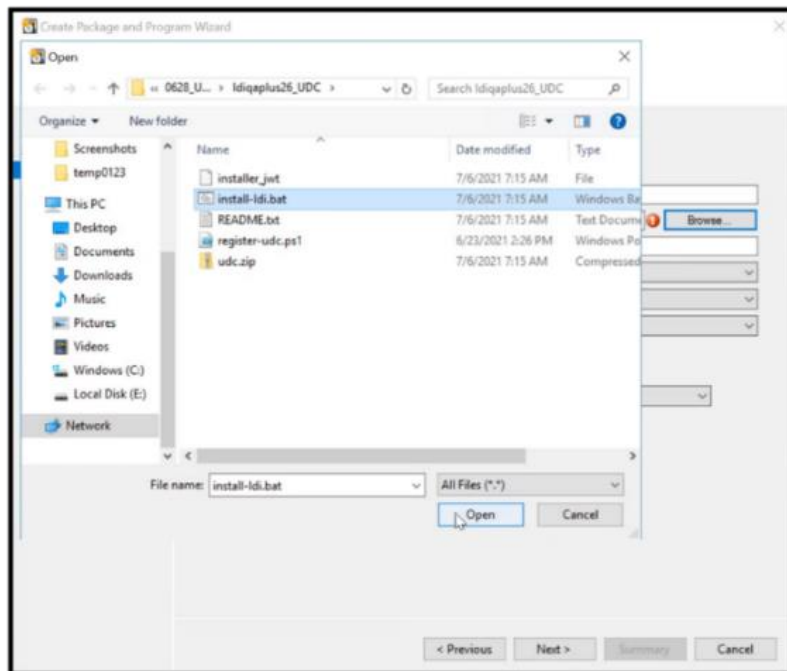


3. Enter the name of the program. For example, UDC_Installation.

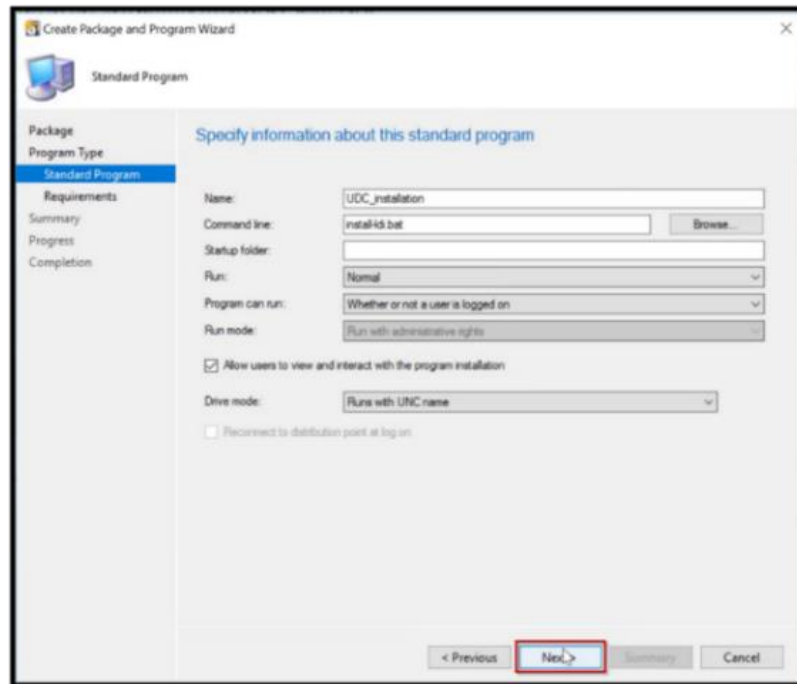
4. In the **Command line** field, click **Browse**. You see the following pop-up window.



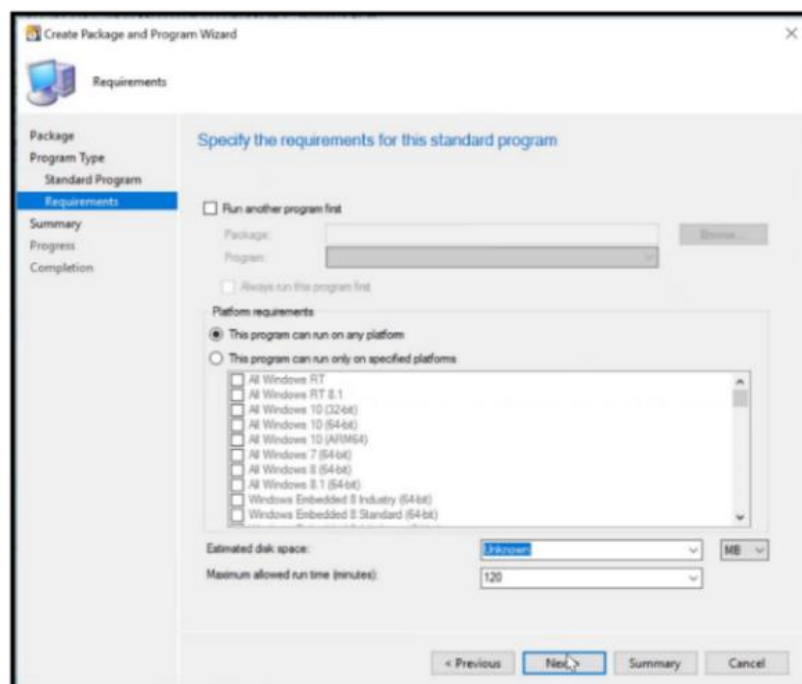
5. Select **All Files**. You see all the files.



6. Select **install-LDI.bat**.
7. Select **Open**.

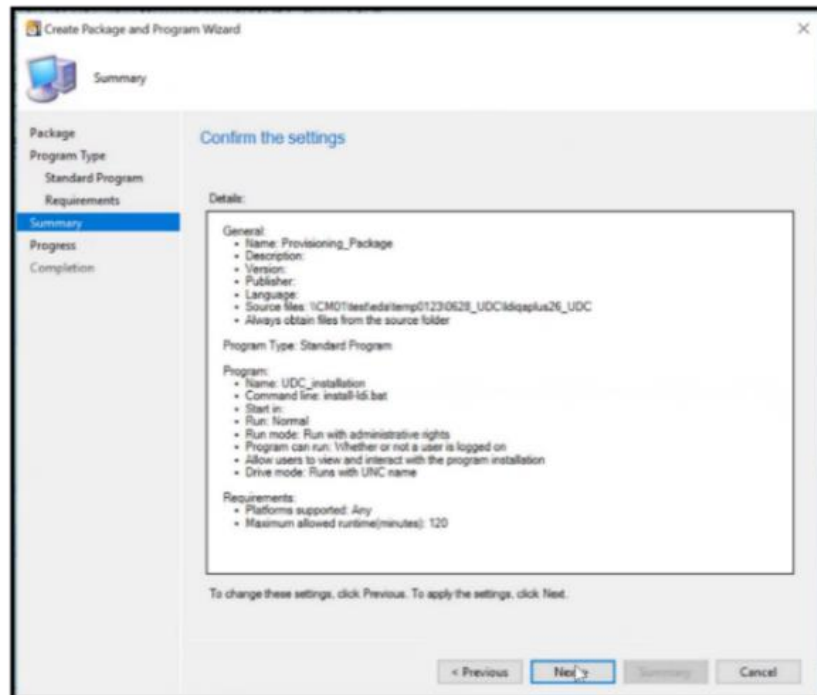


8. In the Program can run field, select Whether or not a user is logged on.
9. Select the checkbox - Allow users to view and interact with the program installation.
10. Click **Next**.

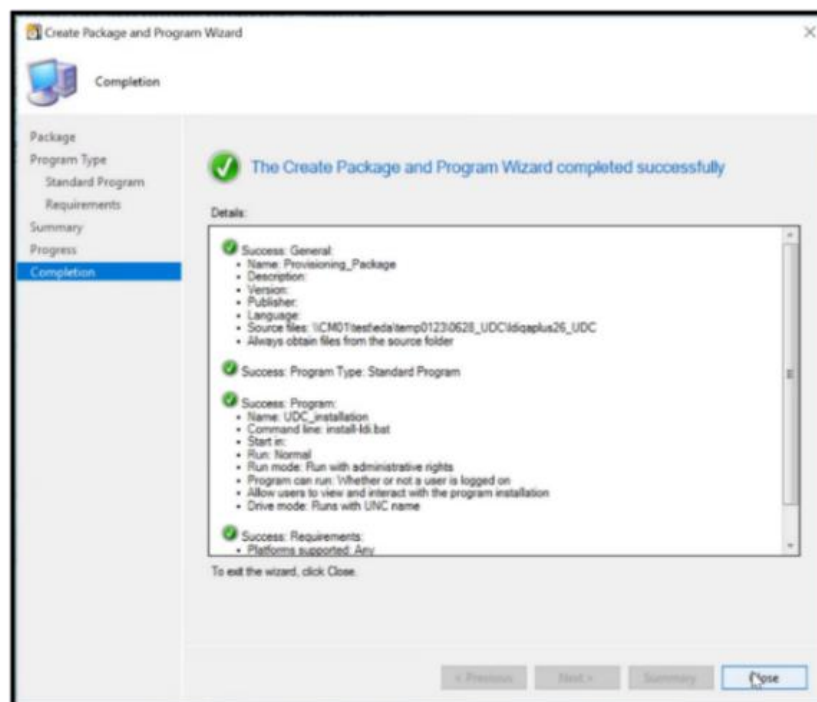


Note: In the **Requirements** section, keep the default settings, as shown in the screenshot.

11. Click **Next**.

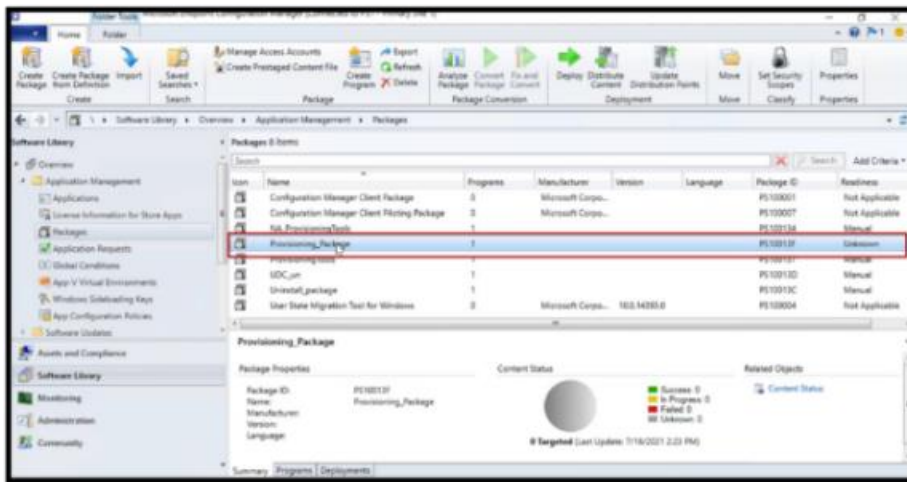


12. In the **Confirm settings** section, click **Next**, to confirm settings selected for creation of package and program.



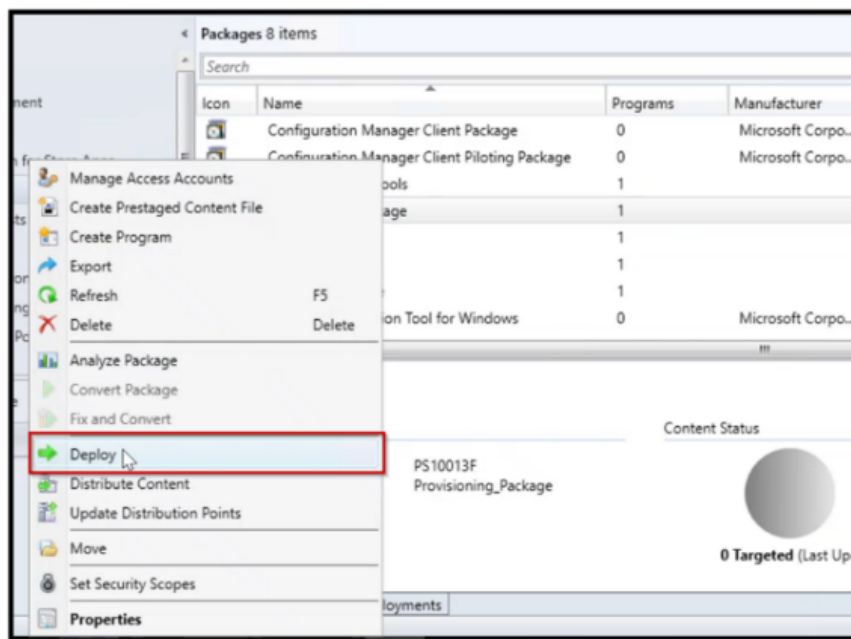
13. Click **Close** to close the wizard.

2.2.9.3. Deploy Provisioning Package

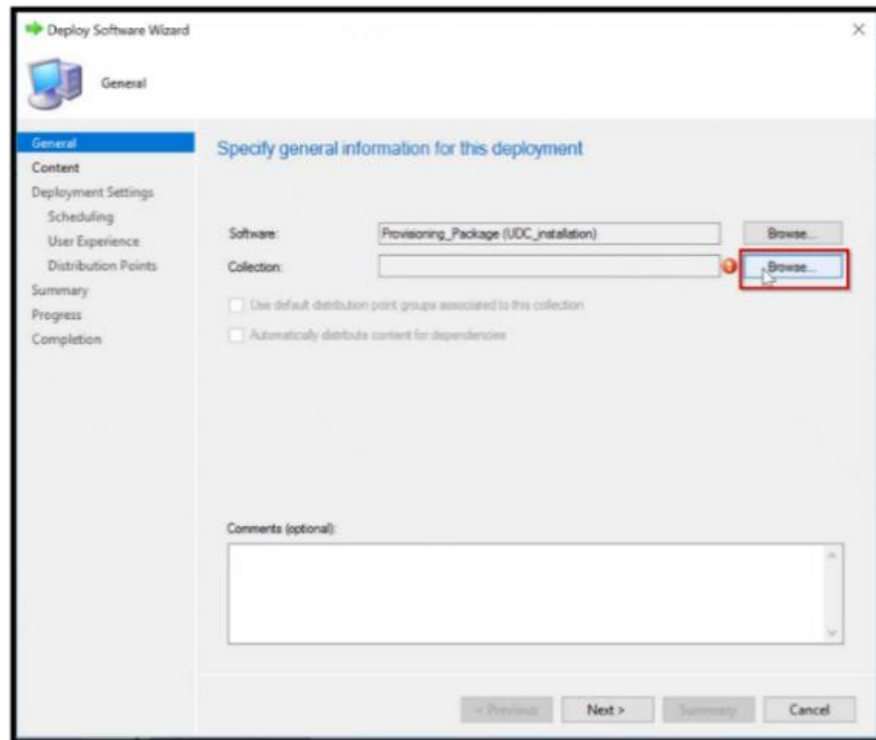


14. Select **Packages** in the navigation menu.

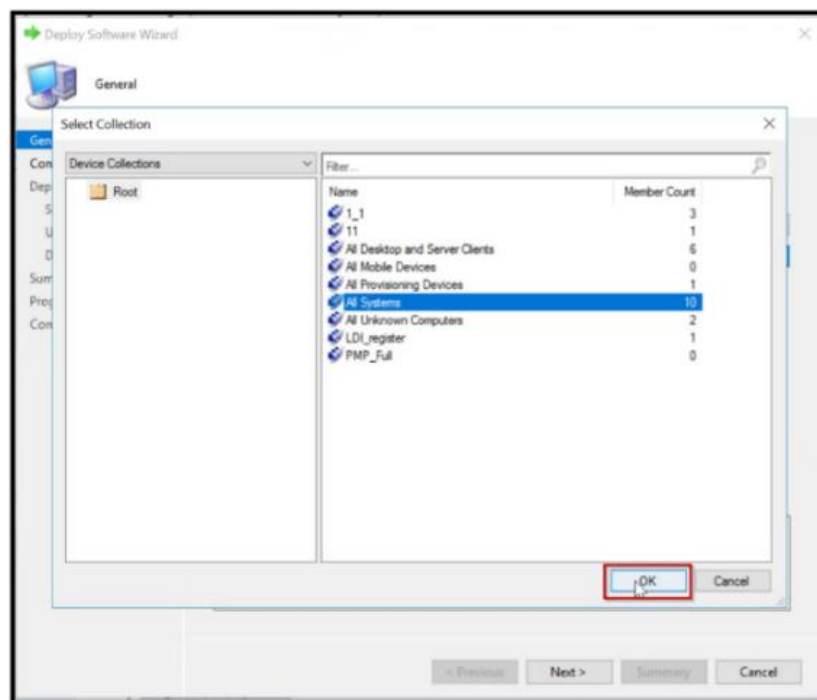
15. Right-click on the **package**. For example, Provisioning Package. A pop-up window appears.



16. Click **Deploy**. You see the General section where you can specify the type of deployment.

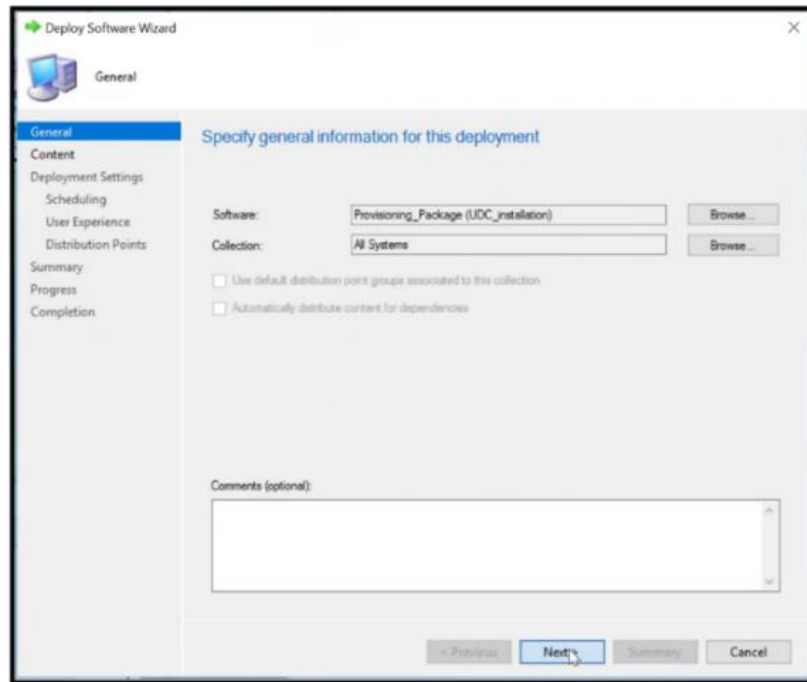


17. In the **Collection** field, click **Browse**. A pop-up window appears.



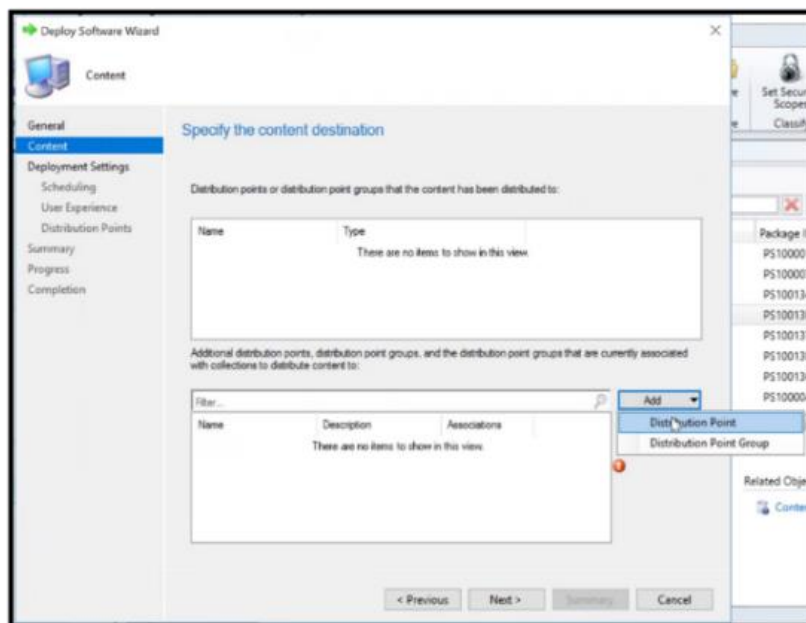
18. Select an option from the context menu in the pop-up window, e.g., All Systems.

19. Click **OK**.



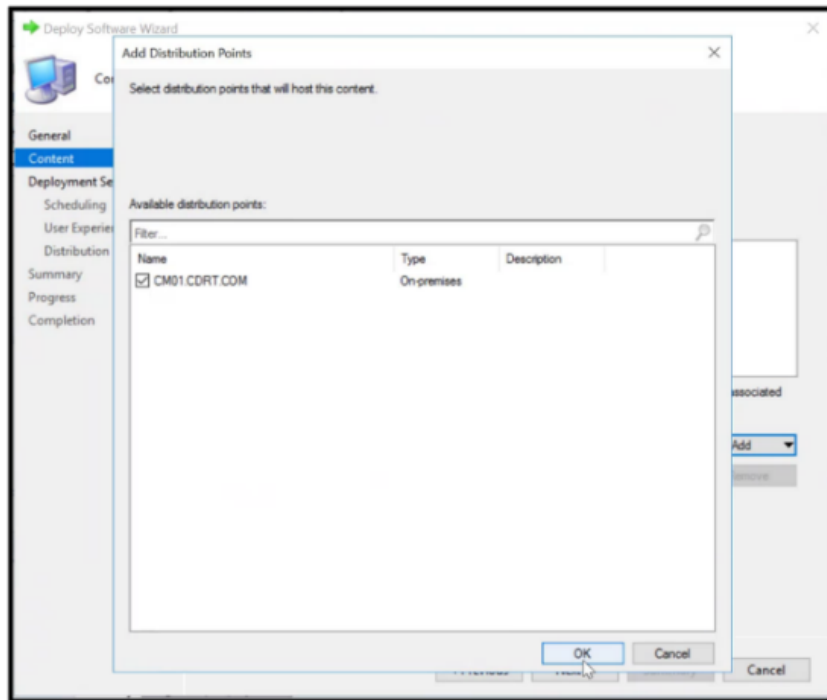
20. Click **Next**. The **Content** section appears.

2.2.9.4. Specify Content Destination



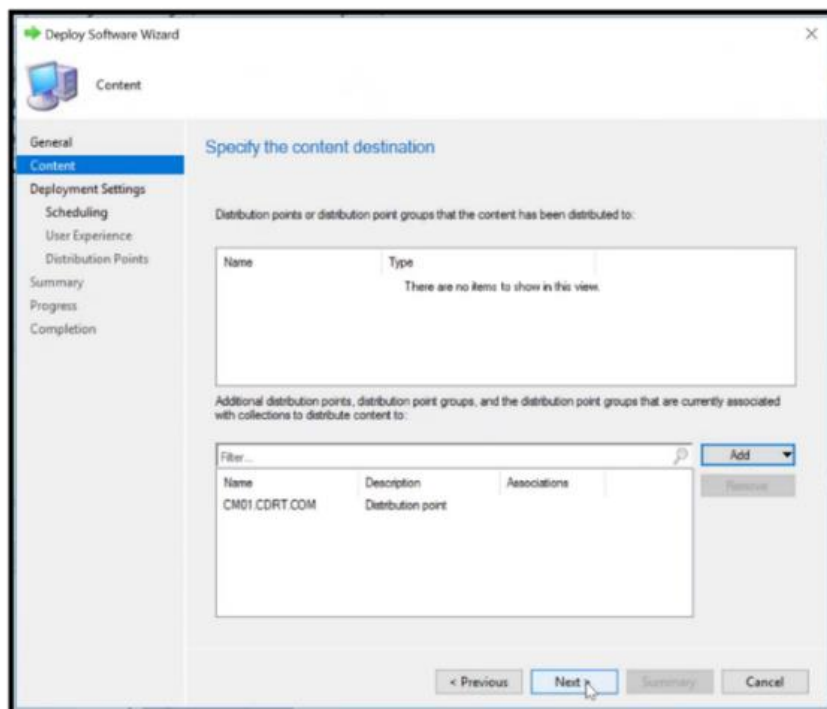
21. Click **Add** to view a drop-down menu.

22. Click **Distribution Point**. A pop-up window appears.



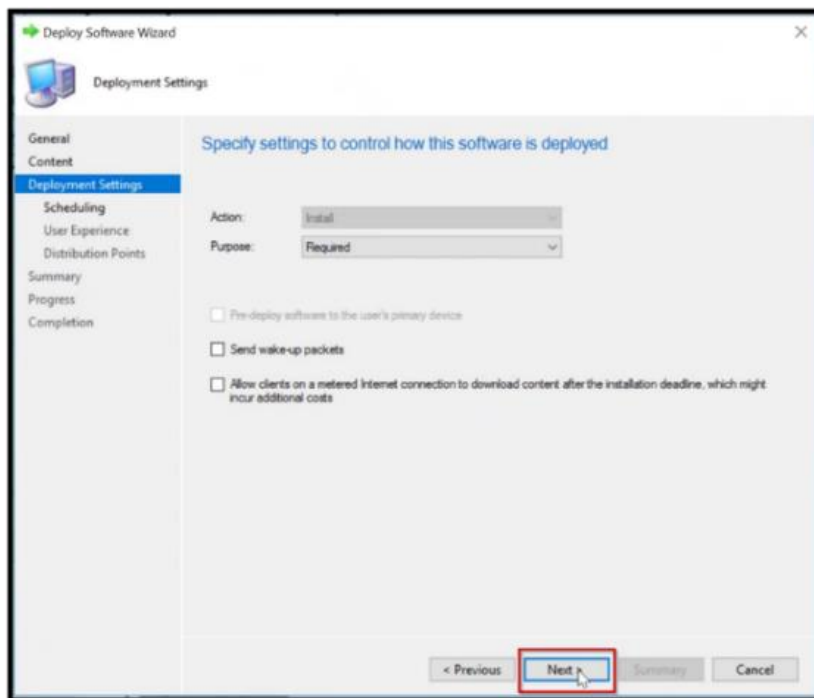
23. Select the **CM01.CRDT.COM** checkbox.

24. Click **OK**.



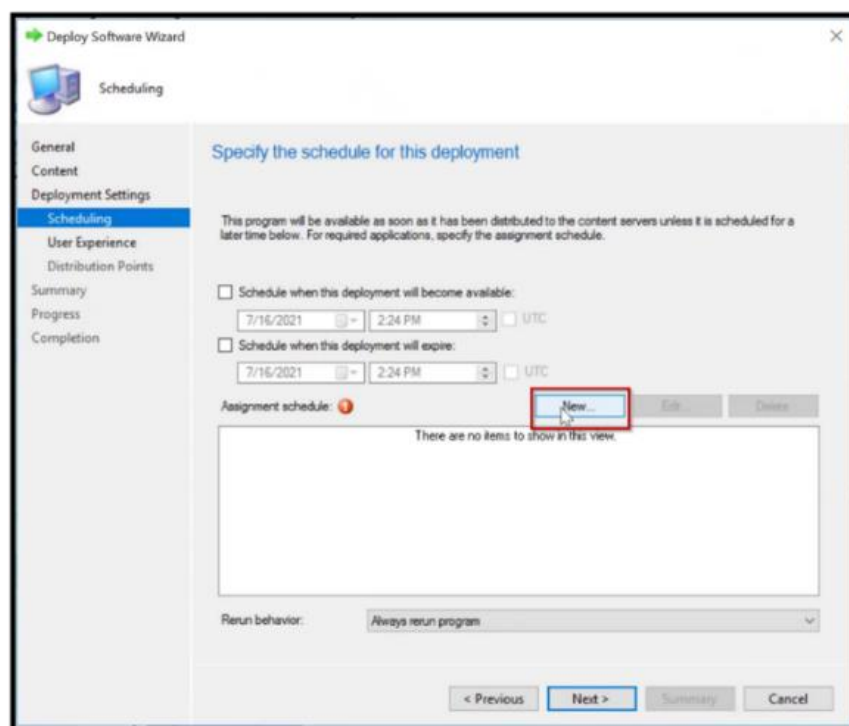
25. Click **Next**. The **Deployment Settings** section appears.

2.2.9.5. Deployment Settings

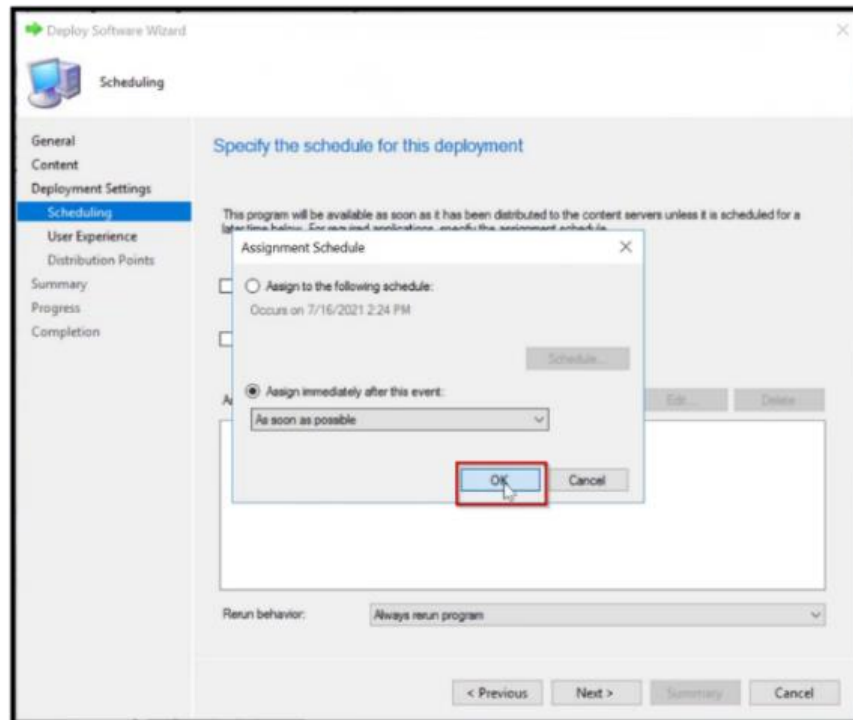


26. In the **Purpose** field, select **Required**.

27. Click **Next**. The Scheduling section appears.



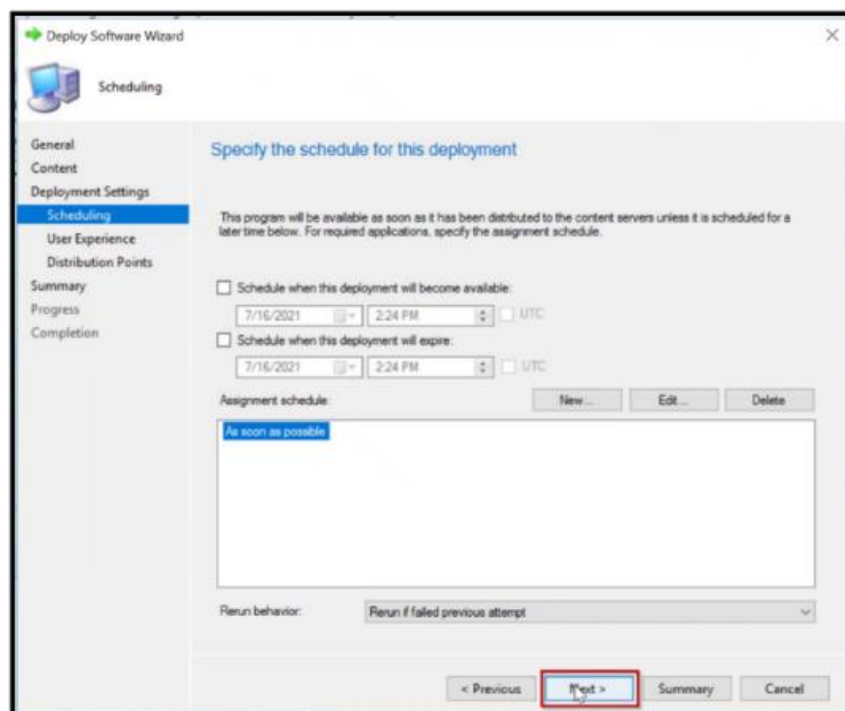
28. Click New. The Deploy Software Wizard appears.



29. Select Assign immediately after this event.

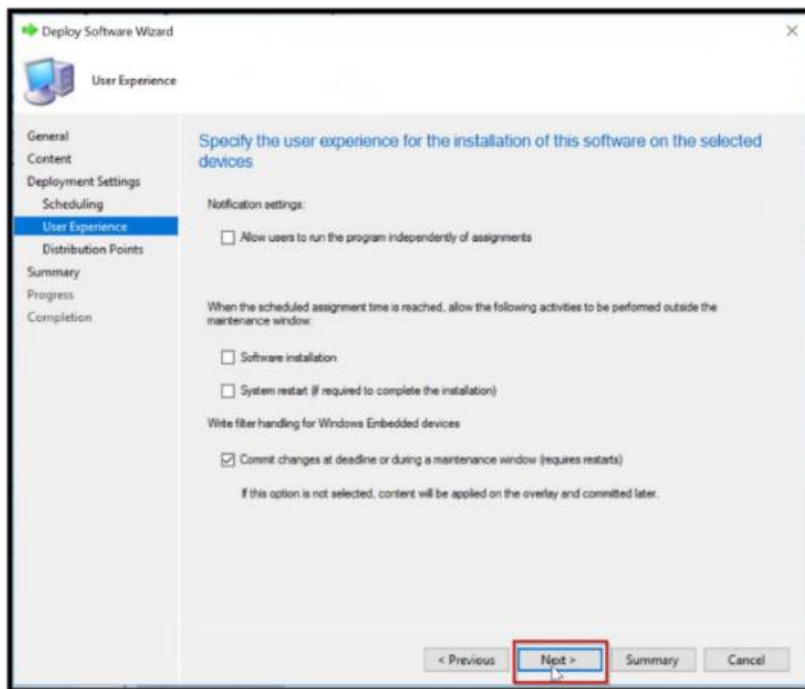
30. Select **As soon as possible** from the drop-down list.

31. Click **OK**.



32. Click **Next**.

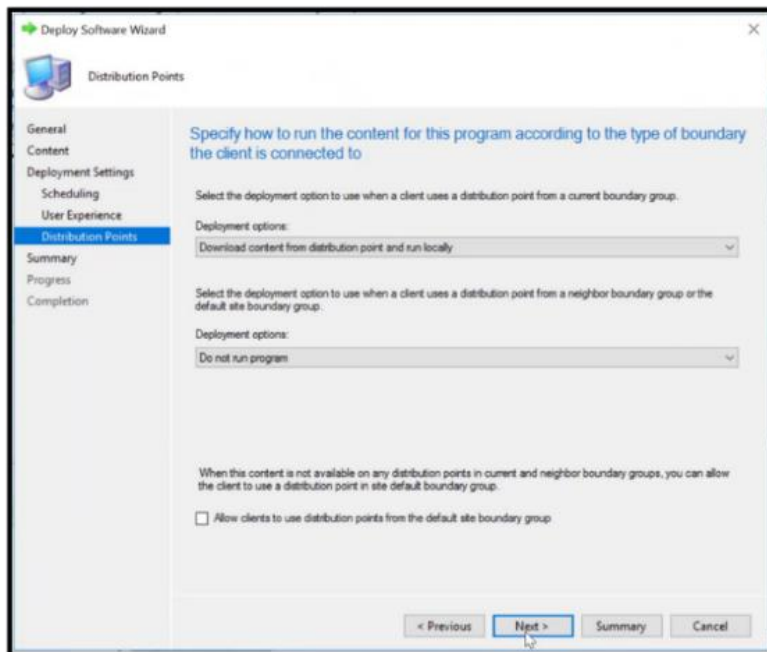
2.2.9.6. User Experience



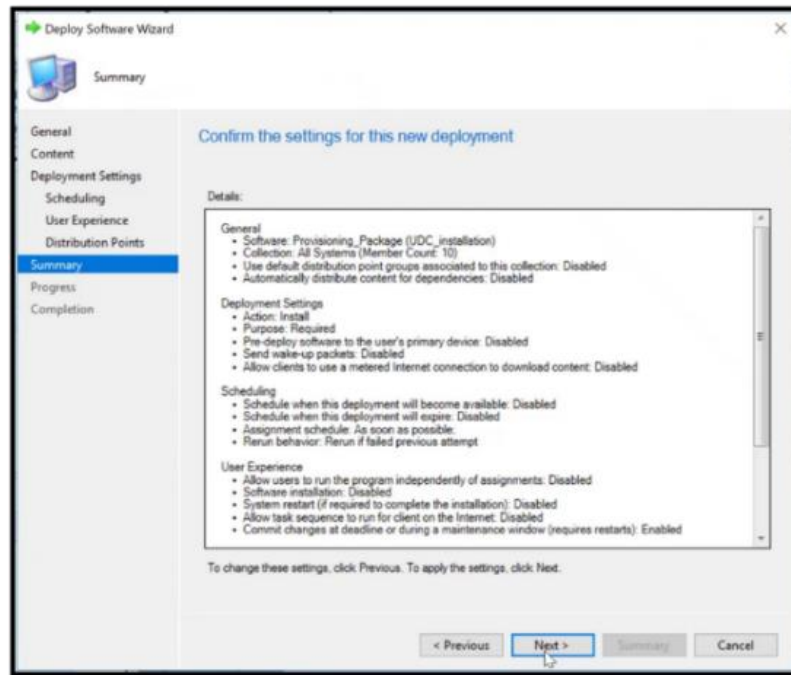
Keep user experience settings as default settings.

33. Click **Next**. You see the **Distribution Points** section.

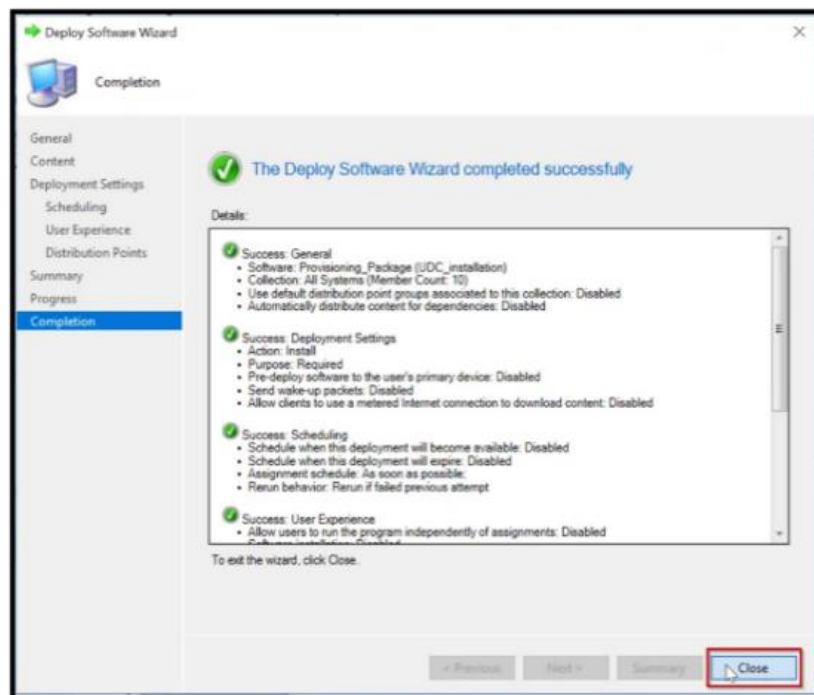
2.2.9.7. Distributions Points



34. Keep the Distribution Points settings as the default settings and click **Next**.



35. Click **Next** to confirm General, Deployment, Scheduling and User Experience settings.

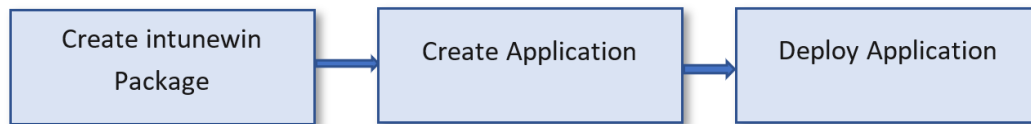


36. Click **Close** to exit the wizard.

2.3 Microsoft Intune

This chapter allows you to enroll your device in LDI using Microsoft Intune. For this, it provides you an overview of steps to follow to enroll devices.

Note: You must have an Azure Active Directory (AAD) account to enroll your device in Intune.



2.3.1 Purpose

You can configure Microsoft Intune to install the LDI Provisioning Package on all the devices in your organization and register them as per Service License Agreement between your organization and LDI Solutions. Instead of downloading Provisioning package on each device you can use Microsoft Intune to run it on the entire fleet of device. This saves your time and effort.

2.3.2 Prerequisite

Download the LDI Provisioning Package on the device you want to configure Microsoft Intune onto and deploy the package on the entire fleet of devices in your organization. Refer to [Onboard your fleet](#) to download and install the package.

2.3.3 Configure Microsoft Intune to Deploy LDI Provisioning Package

LDI agent is distributed as a single exe InnoSetup file or as a zip archive with Universal Device Client (UDC) agent and jwt client. Once you create the .intunewin package, you can upload and deploy/assign the application using Intune console.

2.3.4 Create .intunewin Package

1. Log in to LDI.
2. Select **Help & Resources** → **Instructions & Agents**.
3. From the **Select System** drop-down list, select **Windows (Physical)**.
4. For the onboarding method, select **Microsoft Intune**.
5. Click **Confirm**.

Note: If you're not connected to the Azure ID, select Organization Settings → Connectors to set the values of Directory (Tenant) ID, Application (Client) ID, and App Secret fields.

6. In the **Instructions for Windows Intune Devices Onboarding** page, select the permissions. Refer [Provide a Permission](#).
7. Click **Next**.
8. Select **Maximum Usage** and **Installer Expiration** values from the respective drop-downs.
9. Click **Download**.
10. Upload the .intunewin into Applications.
11. Enter the application ID from the Intune URL in the **Application ID** field. Refer [Register an Application](#) to get the Application ID.

12. Unzip the udc_setup.exe file.

13. Convert exe file into .intunewin package. Create a new folder and copy the received installer file in that folder. Then, install and run IntuneWinAppUtil tool with the following parameters: IntuneWinAppUtil -c <created input folder with exe file> -s <exe installer> -o <output_folder>. This command generates .intunewin file in the output folder. For example:

.\IntuneWinAppUtil.exe -c .\udc_setup\ -s .\udc_setup\udc_setup.exe -o .\output

```
C:\>.\IntuneWinAppUtil.exe -c .\udc_setup\ -s .\udc_setup\udc_setup.exe -o .\output
The output folder '.\output' does not exist. Do you want to create it (Y/N)?y
INFO Validating parameters
INFO Validated parameters within 14 milliseconds
INFO Compressing the source folder '.\udc_setup\' to 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO Calculated size for folder '.\udc_setup\' is 10314460 within 13 milliseconds
INFO Compressed folder '.\udc_setup\' successfully within 337 milliseconds
INFO Checking file type
INFO Checked file type within 6 milliseconds
INFO Encrypting file 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin' has been encrypted successfully within 83 milliseconds
INFO Computing SHA256 hash for C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\0787d135-3c90-4d71-8c8b-3aaf2a57b9d6
INFO Computed SHA256 hash for 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\0787d135-3c90-4d71-8c8b-3aaf2a57b9d6' within 150 milliseconds
INFO Computing SHA256 hash for C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin
INFO Computed SHA256 hash for C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin within 142 milliseconds
INFO Copying encrypted file from 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\0787d135-3c90-4d71-8c8b-3aaf2a57b9d6' to 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO File 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Contents\IntunePackage.intunewin' got updated successfully within 24 milliseconds
INFO Generating detection XML file 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage\Metadata\Detection.xml'
INFO Generated detection XML file within 450 milliseconds
INFO Compressing folder 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage' to '.\output\udc_setup.intunewin'
INFO Calculated size for folder 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage' is 10196164 within 1 milliseconds
INFO Compressed folder 'C:\Users\ \AppData\Local\Temp\278d1ab9-b47c-4c34-a21d-fbfa1e08e2c1\IntuneWinPackage' successfully within 371 milliseconds
INFO Removing temporary files
INFO Removed temporary files within 8 milliseconds
INFO File '.\output\udc_setup.intunewin' has been generated successfully

[=====] 100%
INFO Done!!!
```

2.3.5 Register an Application

1. Open Manage Azure Active Directory.
2. Select **App Registrations**.
3. Click **New Registration**.

Register an application

Name
The user-facing display name for this application (this can be changed later).
test

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (Lenovo only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 Select a platform: e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#).

Register

4. Enter a name for the application and click **Register**. The Application ID and the Directory ID are created.

2.3.6 Provide a Permission

You need to provide certain permissions to an application to work with InTune.

Note: Before providing permissions, you need to create a secret ID.

To create a secret ID

1. [Register an Application](#).
2. Click **Certificates & Secrets**.

test | Certificates & secrets

Search (Ctrl+F) Get feedback?

Overview Quickstart Integration assistant

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Add a client secret

Description: Enter a description for this client secret

Expires: Recommended 6 months

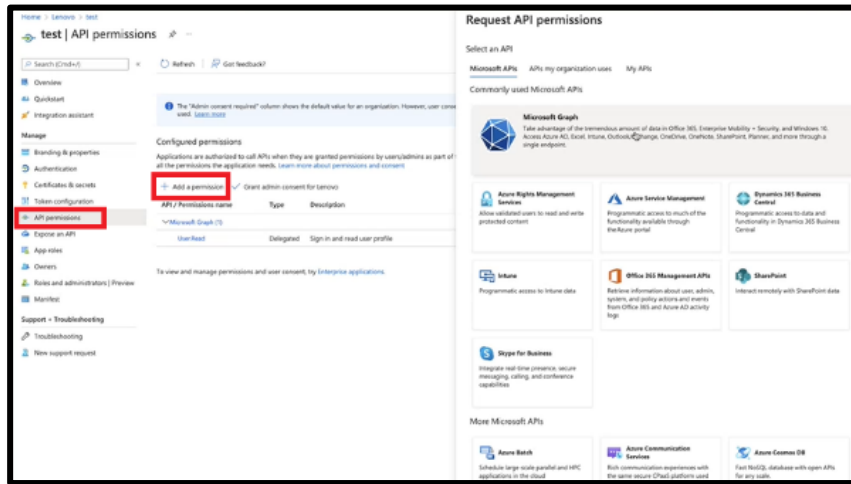
Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Add **Cancel**

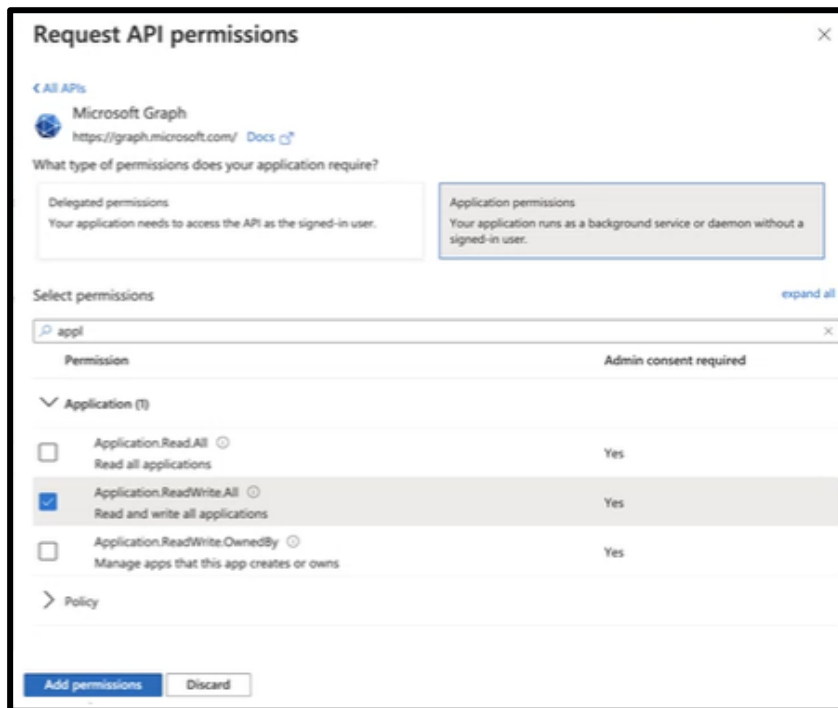
3. Enter a secret ID in the **Description** field and click **Add**.

To provide a permission

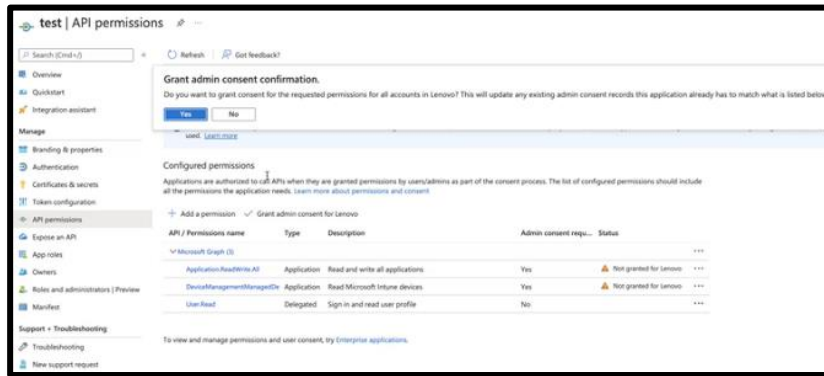
1. Click **API Permissions** and then click **Add a permission**.



2. Select **Microsoft Graph** and then select **Application permissions**. The **Select permissions** window appears.



3. Search for the required permissions, select the respective check boxes, and then click **Add permissions**.

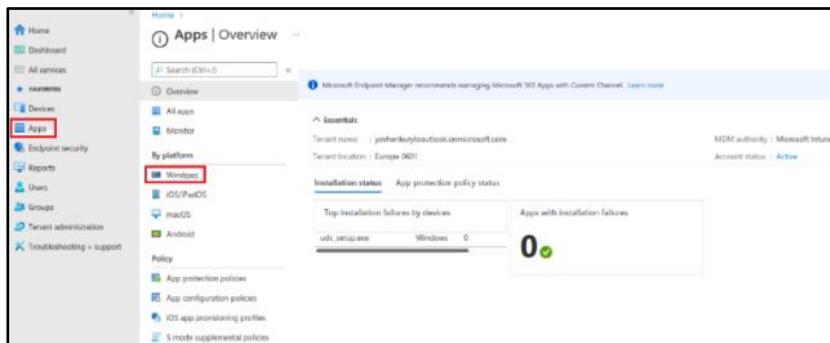


- Click **Grant admin consent for Lenovo**. The **Grant admin consent confirmation** window appears.

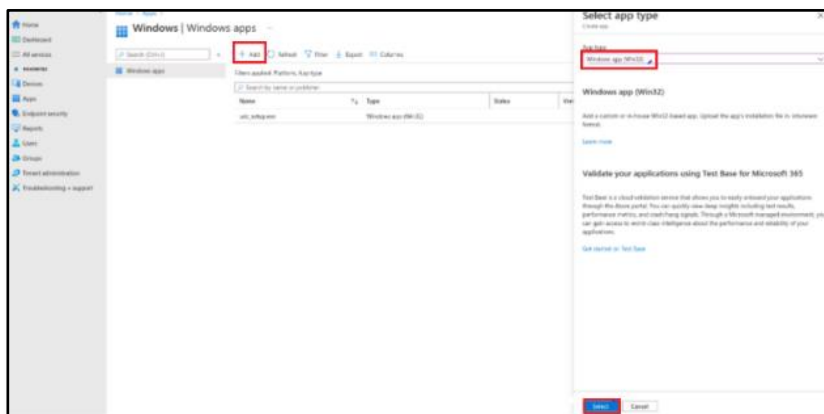
- Click **Yes**.

2.3.7 Create and Add Windows Application to Intune

- Log in to Intune console and select **Apps**, then select **Windows** platform.



- Click **Add** and select **Windows app (Win32) App** type, and then click **Select**.



- Select **.intunewin** package file.



- Provide required app information.

Add App ...

Windows app (Win32)

1 App information 2 Program 3 Requirements 4 Detection rules 5 Dependencies 6 Supersedence

Select file * ⓘ [udc_setup.intunewin](#)

Name * ⓘ

Description * ⓘ

[Edit Description](#)

Publisher * ⓘ

App Version ⓘ

Category ⓘ

Show this as a featured app in the Company Portal ⓘ ☒ Yes ☐ No

Information URL ⓘ

Privacy URL ⓘ

Developer ⓘ

Owner ⓘ

Notes ⓘ

Logo ⓘ [Select image](#)

[Previous](#) [Next](#)

5. Provide application install and uninstall commands.

Install command: `udc_setup.exe /VERYSILENT /NORESTART`

Uninstall command:

`C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe -uninstall`

Microsoft Intune admin center

Home > Apps | All apps >

Add App

Windows app (Win32)

App information Program Requirements Detection rules Dependencies

Specify the commands to install and uninstall this app:

Install command *

Uninstall command *

Install behavior ☒ System ☐ User

Device restart behavior

Specify return codes to indicate post-installation behavior:

Return code	Code type
<input type="text" value="0"/>	<input type="text" value="Success"/>
<input type="text" value="1707"/>	<input type="text" value="Success"/>
<input type="text" value="3010"/>	<input type="text" value="Soft reboot"/>
<input type="text" value="1641"/>	<input type="text" value="Hard reboot"/>
<input type="text" value="1618"/>	<input type="text" value="Retry"/>

+ Add

Previous Next

6. Provide requirements for the application.

Note:

- Operating system architecture requirement is 64-bit. Minimum operating system is Windows 10 1809.
- You can also provide optional requirements such as disc space, number of processors, etc.

Microsoft Intune admin center

Home > Apps | All apps >

Add App

Windows app (Win32)

App information Program Requirements Detection rules Dependencies

Specify the requirements that devices must meet before the app is installed:

Operating system architecture *

Minimum operating system *

Disk space required (MB)

Physical memory required (MB)

Minimum number of logical processors required

Minimum CPU speed required (MHz)

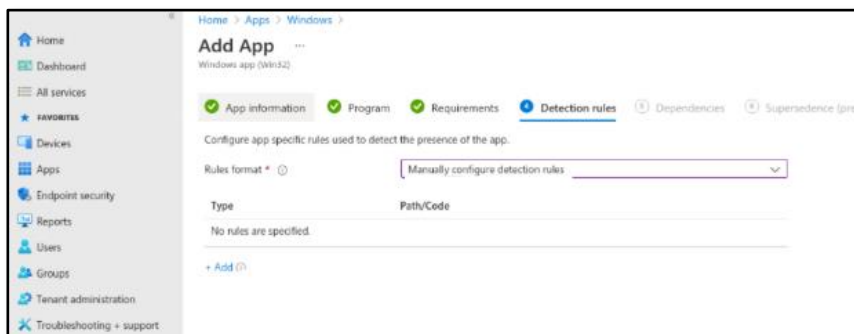
Configure additional requirement rules

Type	Path/Script
No requirements are specified.	

+ Add

Previous Next

7. Select a detection rule from the **Rules format** drop-down list. These rules allow you to detect if application is installed or not. You can select manually configured rules or custom detection script.

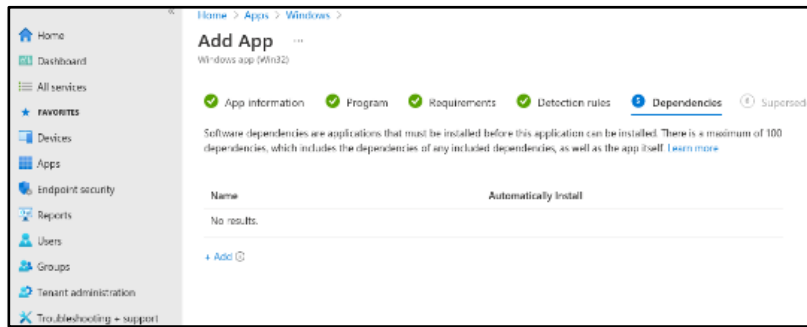


Note: The following are manually detection rules:

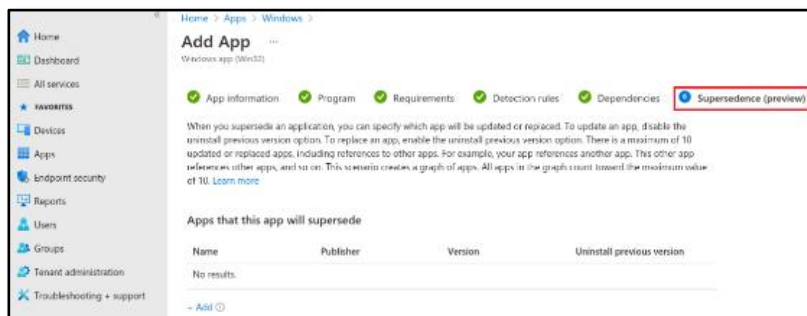
- **MSI** - Detects by MSI product code
- **File** - This rule allows to detect app based on filesystem information: file or folder exists, created/modified date, file size
- **Registry** - The rule allows to detect app based on registry information: key exists, key doesn't exist, value comparison

Note: UDC agent is installed as a driver to
 Path: C:\Windows\System32\drivers\Lenovo\udc\Service.
 File: UDClientService.exe
 Detection method: File or folder exists

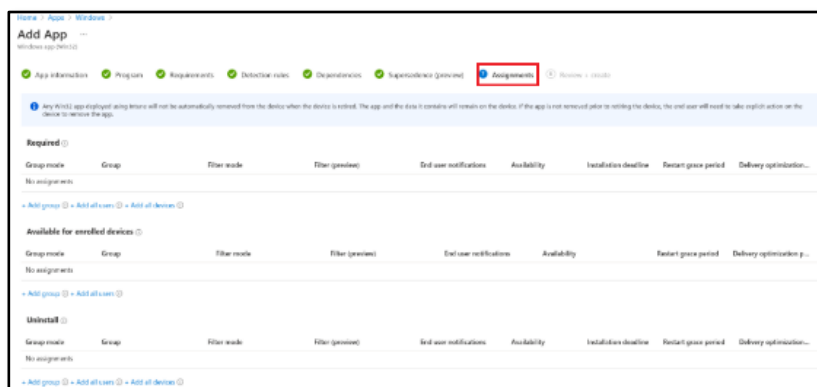
Optional Step 1: Click **Dependencies**, if required.



Optional Step 2: Click **Supersedence**, if required.

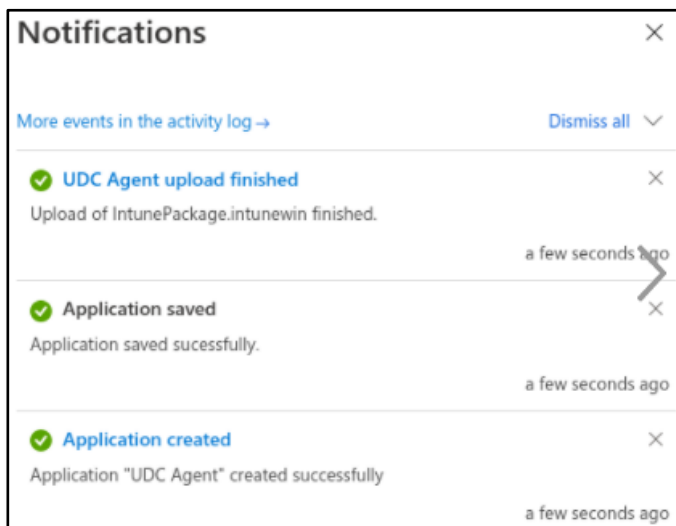


Optional Step 3: Click **Assignments** to deploy the application to the selected device or a group of devices. You can skip this step for creating an application.



8. Click **Review + create**. If the review summary is correct, click **Create**.

Note: When the application is created and uploaded to the system, the following **Notifications** window appears. This process might take an hour or so.



Note:

- Now when the LDI agent is installed successfully, you can search for your device in the **Devices** page under the **Device Manager** module.
- Refer to [Onboard your fleet](#) for the troubleshooting process.

2.3.8 Deploy Application

You can deploy an application to managed devices, users, or groups.

Note: The deployment process might take between five minutes and an hour to complete.

Following types of deployment are available:

- **Required** – Indicates that the application is required for selected enrolled devices and gets installed automatically. Usually, it happens when you log in to the device.

- **Available for enrolled devices** – Indicates that the application is not required, and you can decide whether to install this application or not. In this case, the application remains in the company portal, and you can install it there.
- **Uninstall** – You can select users or groups for which you want to uninstall the application. The application is uninstalled for the selected managed devices.

2.4 Ivanti

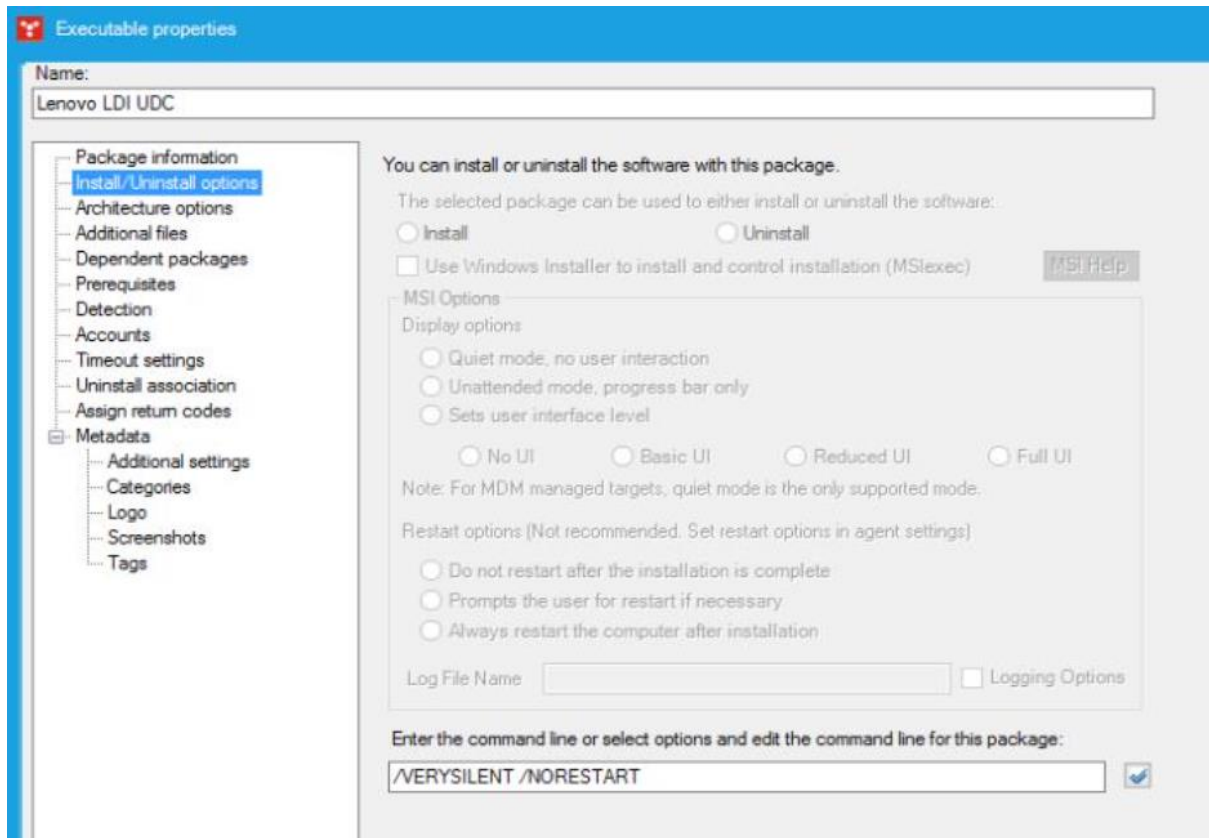
This chapter allows you to enroll your device in LDI Plus using Ivanti. For this, it provides you an overview of steps to follow to enroll devices.

2.4.1 Executable Properties

Install `udc_setup.exe` as an executable using the parameters `"/VERYSILENT /NORESTART"`

Uninstall command:

`C:\Windows\System32\drivers\Lenovo\udc\Data\InfBackup\UDCInfInstaller.exe -uninstall`



2.4.2 Windows Action Properties

Run the registry export as a PowerShell snippet.

Here we assume that the folder `c:\temp` already exists.

Windows Actions properties

Name: LDI registry export

Package actions are used to perform custom operations during package installation. (Note: All actions will be combined and run in the order specified as a single PowerShell script)

Description: export registry

Actions

Type	Description	Continue on failure
Launch an executable		<input type="checkbox"/>

Add Remove Edit Use variable

Arguments (Note: [] indicates an optional field)

Note: Click the value field to edit (for cmdlets that contain a path, environment variables such as %windir% are supported)

Name	Value
Executable	%windir%\system32\reg.exe
[Parameters]	export HKLM\Software\Lenovo\UDC C:\temp\ldi_snapshot_udc-registry.txt /reg:64

PowerShell cmdlet preview

```
<#
Launch an executable
#>
Start-Executable -Executable "%windir%\system32\reg.exe" -Parameters "export HKLM\Software\Lenovo\UDC C:\temp\ldi_snapshot_udc-registry.txt /reg:64" -ErrorAction Stop
if ($? -ne $true)
{
    exit 1
}
```

Executable: %windir%\system32\reg.exe

Parameters: export HKLM\Software\Lenovo\UDC C:\temp\ldi_snapshot_udc-registry.txt /reg:64

3 Configure LDI

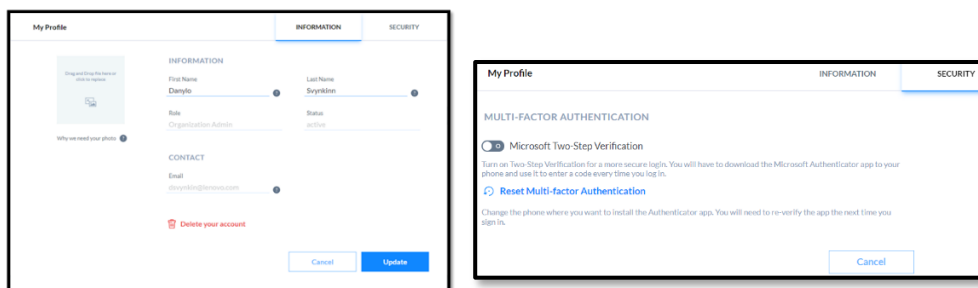
3.1 Manage access

3.1.1 User Creation

Click 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 or disable Multi-Factor Authentication.
- Delete your account



User Role Types

When you add users to your portal, following role types are available to assign:

- Organization Administrator
- IT Administrator
- IT Analyst

The IT Analyst role can be assigned to a Lenovo Support agent if you would like assistance with an issue.

Lenovo Device Intelligence ROLES & PERMISSIONS			
ROLES FEATURES	IT ADMIN Will manage the entire diagnostic and remediation processes	ORGANIZATION ADMIN Will manage Org level functions and be able to play an IT Admin in the system	IT ANALYST Will be available as a support role from the Lenovo team. Will have no system function privileges
Users & Groups Add & Manage	✗	✓	✗
Devices & Groups Add & Manage	✓	✓	✗
Issues & Remediations Create & Remediate	✓	✓	✓
Support Tickets Create & Manage	✓	✓	✓
Auto-Tickets A user will need to be selected as a Service Group Admin to Add and Manage Auto Tickets	✓	✓	✓
License Management Manage & Assign	✓	✓	✗

View Organization Users

You can manage the users in the portal by selecting **Users Manager → Users**. A table depicts name, role, email, status, and group for each user.

Lenovo Device Intelligence		Home / Users			
		Users			
		Delete	Group	More	Refresh
		NAME	ROLE	EMAIL	STATUS
		Adrian Admin	Organization Admin	adrian@lenovo.com	Active
		Andrew Bessone	Organization Admin	andrew@lenovo.com	Active
		Caroline Kraft	Organization Admin	caroline@lenovo.com	Active
		Steve Smith	Organization Admin	steve@lenovo.com	Active

In 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
- Invite user(s)

You can add users by accessing **Users Manager → Users → +**. You can invite users individually, or in bulk by uploading a CSV file containing user details for each invitee.

To add users individually

1. Click **+**.
2. Enter all the required details.
3. Click **Invite**.

The user receives an email invitation with a link to sign in and/or create a Lenovo ID account using the same email address.

To add users in bulk

1. Click **+**.
2. Select the **Bulk Invite** tab.
3. Click **Download CSV template** to download CSV template.
4. Populate CSV file with required details for each user - First Name, Last Name, Role, and Email.

For Example: CSV for bulk user invite:

First Name, Last Name, Role, Email

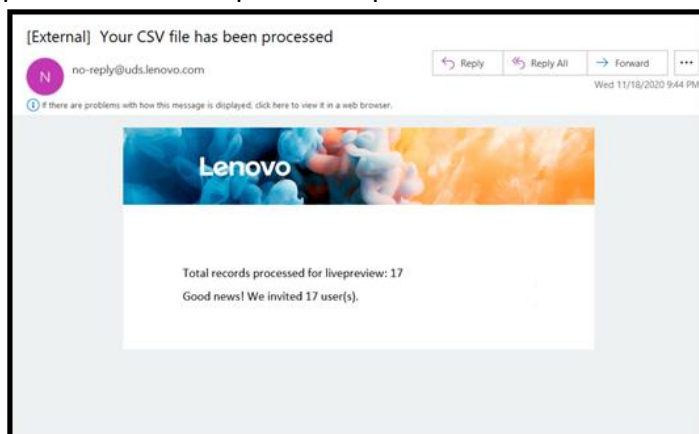
Bill, Lumbergh, Organization Admin, wlumberg@initech.com

Peter, Gibbons, IT Admin, pgibbons@initech.com

Milton, Waddams, Lenovo Device Intelligence Support, mwaddams@initech.com

5. Drop CSV file to the modal window and click **Verify**.

When you upload a CSV file, the file is processed and if there are any errors with the upload, that are displayed in the feedback screen. You receive an e-mail confirmation from the portal when the upload completes.



Note: If a user loses the invitation email, click the user in the Users table to resend the invitation by:

Update User(s)

To manage user information, click 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 or update a user's profile image
- Delete a user.

Note: You can also enable multi-factor authentication for a user, if required. By default, it is disabled.

Bulk Updates

Organization or Subscription Admins have the option to Export or Import users in the Users list.

To export user(s) to the .CSV file

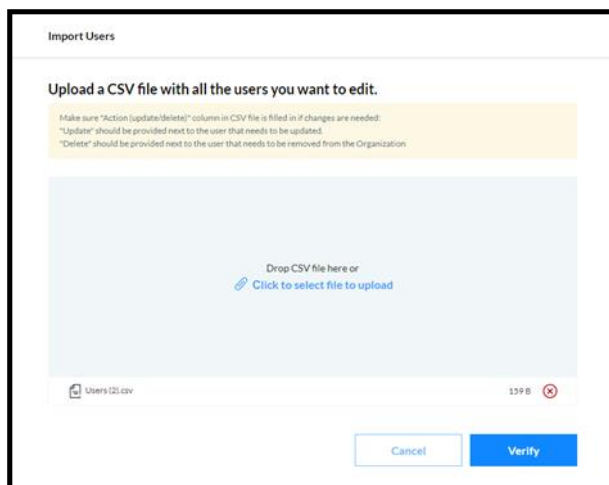
1. Select user(s) you want to export (to export all users, make no selection).
2. In the More drop-down list, click **Export**.

To edit multiple user(s)

Update user fields in the exported users' file.

Note: Make sure **Action** (update/delete) column in the CSV file is filled-in if changes are needed.

- Update should be provided next to the user that needs to be updated.
 - Delete should be provided next to the user that needs to be removed from the Organization.
1. In the **More** drop-down list, click **Import**.
 2. Drop CSV file to the modal window and click **Verify**.



The system validates the uploaded data, and an e-mail confirmation is triggered from the portal when the upload completes.

Use the **Import Results** option to review the results of the import process.

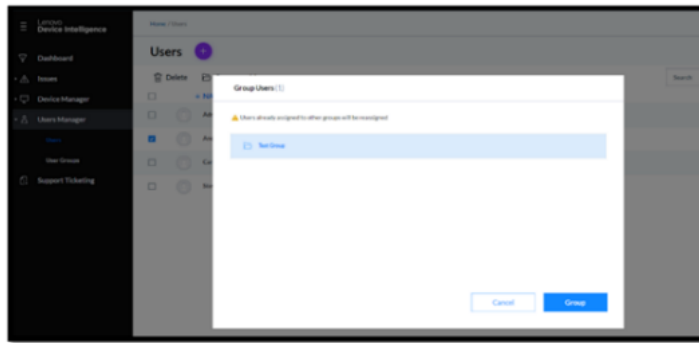
Delete User(s)

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

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

1. Select the User(s) you want to assign to a user group and click **Group** at the top of the page.

Note: You can assign a user to an existing group only.



2. Select the group you want to assign the user(s) to and click **Assign**.
Note: Any users already assigned to other groups will be reassigned to the current group as a result of this action.

3.1.2.1. User Groups

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

Create user group

1. In the **User Groups** page, click **+**.
2. Enter the name of the group in **Group Name**.
3. Select users you want to assign to this group.
4. Click **Assign**.

3.1.2.2. Manage User Group

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

The following options are available:

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

Delete User Group(s)

1. Select the groups you want to delete.
2. Click **Delete**.

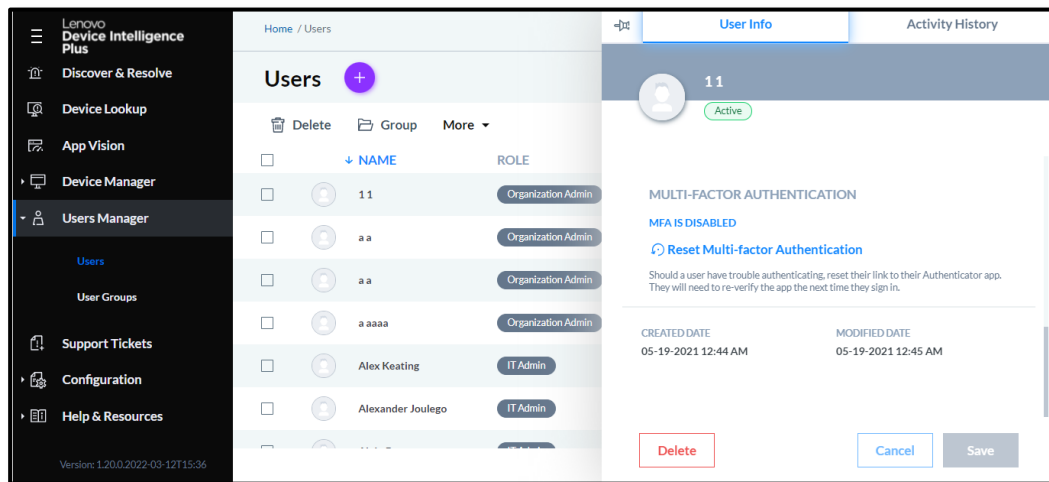
You may also delete a group from the **User Group** tray.

3.1.3 Password change

1. Log in to LDI portal.
2. Click **Forgot Password**. The Reset Password window appears.
3. Enter a new password and click **Next**.
4. Verify your security code. Use the new password to log in to the LDI portal.

3.1.4 Authentication Types

Select **User Manager** → **Users** → **User Info** to view the authentication type for users of the solution in your organization.



3.1.5 Azure Active Directory, Okta and LenovoID

Azure Active Directory

Azure Active Directory (AAD) registration is supported for several use cases, such as integration with InTune for fleet deployment.

Okta

LDI supports Okta Single Sign On.

Lenovo ID

Lenovo ID is the secure and trusted mechanism providing authentication and identity management for Lenovo Device Intelligence Plus. 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 are invited to join by creating an account.

3.2 Manage Devices

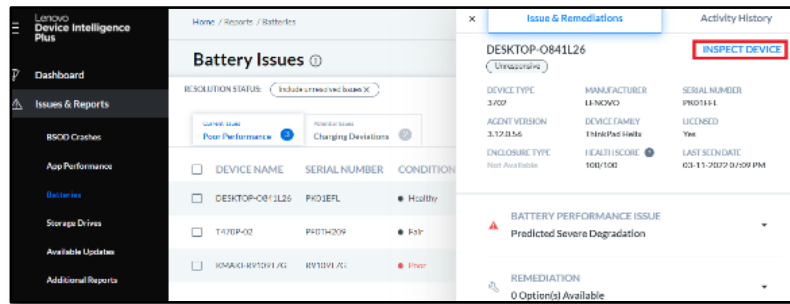
3.2.1 Device manager screens, inspect device fix onboarding issues

For manage devices, refer to [Manage Devices](#).

Inspect Device

You can use Inspect Device to fix the onboarding issues.

1. Click **Inspect Device**.



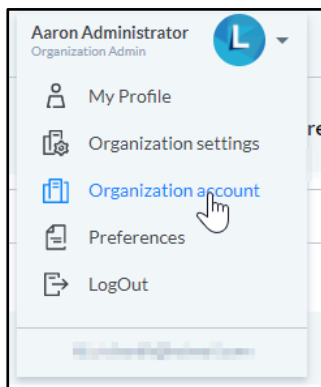
The Battery Issues page appears that shows all the details of the device, issues, sensors, health analysis, installed application, and hardware component related issues. Based on the details, you can fix the issues.

3.3 Org Settings vs Configuration

3.3.1 Organization Setup

When your organization's portal is created, a single administrative account is also created. The IT Owner specified to Lenovo at the time of sale receives a Lenovo Device Intelligence Plus e-mail regarding access to your organization. When you click the link, you are taken to the **Sign on** page log in to LDI as an Organization Administrator.

With this administrative account, you can configure the portal, invite users, and add devices.



3.3.2 Manage Organization

Important Note: Some of the following settings may not appear if your organization is in a Trial program.

Profile

Manage the profile for your organization, including logo, organization name, country, and address.

Licenses

View the licenses assigned to your organization, their quantities, and usage. A link is available to manage license assignment on a per-device basis.

When a device is unlicensed due to assignment or expiration, you can expect the following:

- Data from the device is not collected or processed

- Previous data for the device is preserved
- The device is excluded from reports and intelligence

Authentication

View the authentication type for users of the solution in your organization. You can view the settings for your organization when you click on the 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

User Preferences

You can access the preferences for your user account when you click on the user Icon in the top ribbon Preferences option.

Preferences page allows you to manage portal language, email frequency, and view Terms & Conditions with Privacy Policy.

Language

The language that the portal UI is displayed in.

[3.3.2.1. Set Portal Language](#)

You can configure the portal language in the Portal Preferences page.

1. In the LDI portal, click the User drop-down list.
2. Select Preferences.
3. In the **Settings** section, select a desired language in the **Language** drop-down list.
4. Click **OK**.

Note: Wait for approximately 30 minutes to reflect the change.

You can configure the following languages:

- Deutsch (DE)
- English (EN)
- Español (ES)
- Français (FR)
- 日本語 (JA)
- Português (PT)
- 中文 (ZH)

Email Frequency

Daily Email Summary: Start your day with an update of a daily snapshot of all the current and potential issues in your fleet.

3.4 Organization Settings

Before you use LDI APIs, you must generate API credentials in the LDI account.

1. Click **Organization Settings** in the **Organization Admin** window.
2. Click **API Credentials** in the **Organization Settings** window. The **API Credentials** pane appears. If there are no API credentials, click **Generate** to create the credentials.

Note: A Client ID and Secret key are generated. You can copy them to the clipboard. If you want to change the existing API credentials, you can generate a new one.

3. Click **Regenerate**. The **Regenerate** pop-up window appears.
4. Click **Regenerate**. A new Client ID and Secret key is generated.

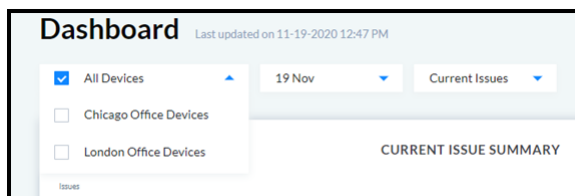
4 Monitor your fleet

4.1 Dashboards

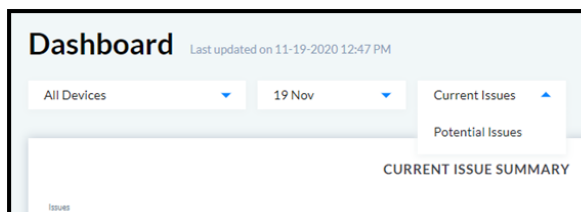
Dashboard is the home page for Lenovo Device Intelligence Plus and offers an overview of the devices in your organization. The Dashboard consists of several cards, where each card represents one or many insight categories. Issues are how items are tracked for each insight category; clicking on metrics displayed on a chart or below a particular widget navigates the user to the corresponding Issue Report Page, which provides a device-by-device list of issues. All widgets are of the same size to allow continuity with the dashboard.

Note: Issue data is displayed for the last 24 hours by default. Facets are available at the top of the dashboard to filter by:

Device Groups



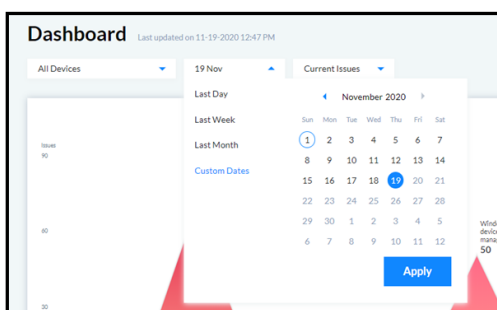
Detected and predicted issues



Date range filter

Selecting a date range filter causes the Dashboard to refresh with the data associated with the selected date range.

Note: The following Dashboard widgets are not affected by the Date Filter: Health Score, Device Counts, and Licensing (if available).



Filtering by date provides a historical view of your devices fleet in each insight category that allows you to view and analyses how the state of your devices has changed over time.

Filtering by a date range causes some Dashboard charts to transform into a trend line to display issues over time.

Date/Time Refresh now corresponds to when the data was last refreshed in the organization.

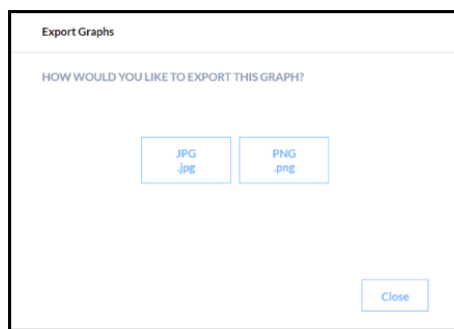
Dashboard Last updated on 01-27-2021 11:44 AM

4.1.1 Dashboard Enhancements

Expanded Dashboard Widgets

Dashboard widgets can be exported.

1. Click the ellipsis found on the upper right-hand corner of the widget.
2. Select Export Graphs.



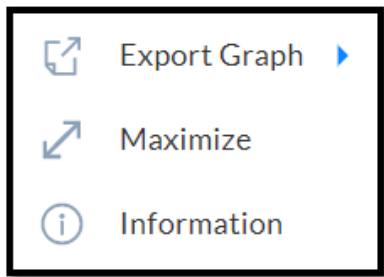
You can select JPG or PNG file types.

Maximize Widgets

Dashboard widgets that contain information may be expanded.

1. Click on the ellipsis found on the upper right-hand corner of the widget.
2. Choose **Maximize**.

Note: If there is no data in a widget, the Maximize option is not available for that widget.



3. Click **Close** to return to the dashboard.

4.1 Issues and Reports

Reports help you identify and act on issues that may result from BSOD crashes, app performance, batteries, storage drives, and device errors. By categorizing these problems in an easy-to-read layout, this module provides a way to view current and potential future issues briefly, giving the IT personnel an opportunity to be proactive instead of reactive.

4.2.1 System Crashes (BSODs)

System crashes for Windows devices are commonly referred to as **Blue Screen of Death**. LDI uses artificial intelligence to analyse device hardware, drivers, and OS events to highlight crashes that are currently occurring or likely to occur in the future.

Detected Crashes

This report provides details about crashes that have recently occurred on devices within your organization.

Frequently Crashing

This report can identify trending crashes on device within your organization. This can help you tackle the most troublesome crashes that may be impacting the device experience.

Predicted Crashes

This report uses AI to identify crash trends and predict which devices are likely to encounter similar crashes. Responding to predictions in this report enables you to fix problems before they occur.

Date filtering provides a historical view of the issues that affected devices fleet before. You can filter BSOD Issues by various columns.

When you click a device, the system displays the Issue Tray, which provides details about the findings and remediations.

Application Performance Insights

A process can be a driver, UI application, or background service, and an average PC may have 100 - 200 processes running at a time. Each process consumes from a limited resource pool of memory, disk I/O, network, and most importantly, CPU. LDI uses on-device AI to identify processes that are exhibiting abnormal resource usage that may be impacting the performance of the whole PC and may be an early indicator for further issues that could be observed in your fleet.

Batteries

Batteries enables you to work while on a plane, in a meeting, or on the couch. A computer user with a poor performing battery experiences a diminished work experience, and may be limited regarding how, where, and when they work. All batteries naturally degrade over time, but some batteries may degrade faster than others due to user behaviour, environment conditions, or manufacturer quality defects.

Replacement and repair of devices or parts of devices is available pursuant to the terms of an applicable Lenovo warranty.

Poor Performance

This report can identify devices with batteries that are under performing into their expected charge. Devices marked as poor condition are unable to remain unplugged for long.

Charging Deviations

AI-based anomaly detection that detects devices who are experiencing charging behaviour that is irregular when compared to normal charging trends. A change in the charging characteristics may be indicative of a new or recent change on the device that could induce irregular power consumption.

Storage Drives

Storage reports aggregate data from storage drives such as Hard Disk Drive (HDD), Solid State Drive (SSD), and Non-Volatile Memory Express (NVME) within your organization and highlight concerning issues using factors such as drive capacity, S.M.A.R.T monitoring, temperature, and firmware. A problematic storage device may result in frequent crashing, loss of time, or permanent loss of work.

All Detected

You can use this report to identify devices with storage drives that are currently problematic. This report also helps you to identify user devices that may need a drive replacement or clean-up.

High Risk

This report uses AI to identify storage failure trends and **predict** which devices may soon have a high-risk issue. Responding to predictions in this report enables you to fix problems before they occur.

Medium Risk

This report uses AI to identify storage failure trends and **predict** which devices may soon have a medium-risk issue. Responding to predictions in this report enables you to fix problems before they occur.

Out of Capacity

This report displays the devices that run out of capacity in next 30 days.


Available Updates

This report displays the devices that have BIOS and Thunderbolt-related updates available in the tool.

Additional Reports

This feature allows you to analyse reports and select their different download format.

Report Filtering


Report filtering  functionality allows you to filter the list of issues by filter criteria (defined columns by which the list can be filtered - unique for each issue report and its tab) displayed in the **Filter Data** modal window.

You can use following types of filtering:

Multi-Select filtering: Available for qualitative filter criteria to group by unique items represented in the issue list. Filter criteria list contains the list of unique filter criteria items that are presented in the history of the defined issues list.

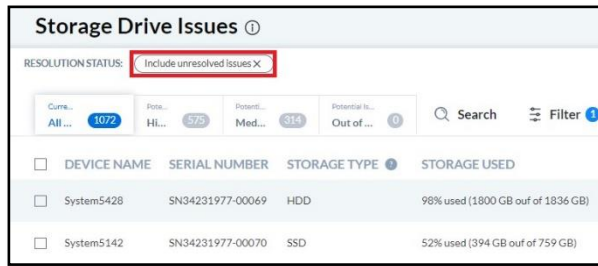
Range filtering: Available for numeric filter criteria to filter by a specific range of numeric values. Filter criteria range slider allows selecting the range within the min and maximum filter criteria numeric values that are presented in the history of the defined issues list.

Exporting Reports to CSV

To perform Issues List export, click the  **Export List** icon to export the selected BSOD crashes report in the .csv file format. If there were filters applied, then confirm if you want to export with or without filters applied.

Note: You must apply filters before exporting report/reports. Otherwise, you get the details of all the devices' issues.

To remove the filter, click .



Issue Tray

When you click a particular device row in an Issue Report, the Issue Tray window is displayed as a slide-in from the right side of the window.

The Issue Tray contains two tabs:

- **Issue & Remediations** - Information about the device that experienced the selected issue, the issue details, and the remediations.
- **Activity History** - Feedback for a remediation or issue itself to improve the remediations that are shown for issues.

Click [Raise a Lenovo Support Ticket](#) to raise a support ticket.

Other Features

Searching Functionality

Click [Search](#) to find a device or issue in a list or report table. Search supports single and multiple character wildcard searches using ? and *.

- The single character wildcard search (?) looks for terms that match that with the single character replaced. For example, to search for **text** or **test**, you can input **te?t**.
- Multiple character wildcard search (*) looks for 0 or more characters. For example, to search for Windows, Windows95, or WindowsNT, enter **win***.

Issues Feedback

This data is gathered and used to prioritize the remediations shown for a given issue in the future.

To send feedback positive or negative for a particular issue, click **Yes** or **No** in the issue tray. The system displays the feedback modal window with the list of options for selection. Enter details to the displayed text area if any, then click **Send**.

To provide a comment regarding your experience with the tool, enter text in the box comment text and click **Save**.

Was this helpful? [Yes](#) [No](#)

0 Comment(s) on this Issue

Write a comment

[Cancel](#) [Save](#)

Snooze

The Snooze feature allows you to snooze not-so-important issues so that you can focus on more important ones that need attention/remediation on a priority basis. You can use this feature to:

- Snooze a specific issue on one or more device, or all devices in the organization
- Create a rule, which is a set of issues or a single issue and apply it on specific devices or entire fleet of devices.
- Select the duration for which the device(s) can be snoozed. It can be for a day, week, month, or year.
- Snooze feature is available for Organization Admin, IT Admin, and IT Analyst accounts.

BSOD Crashes

Current Issues: Detected Crashes (1) | Frequently Crashing (0) | Potential Issues: 0 | Predicted Crashes (0)

DEVICE NAME	SERIAL NUMBER	CRASH CODE
Laptop_40	SNQ7278940	0x00000002
Laptop_33	SNQ7278833	0x00000005
Laptop_41	SNQ7278940	0x00000004
Laptop_40	SNQ7278940	0x00000004
Laptop_40	SNQ7278940	0x00000003
Laptop_40	SNQ7278940	0x00000003

Note: The issue is snoozed. Your alerts won't be shown until it expires.

The snooze icon shows that the device has been snoozed for a specific issue. Name or type of issue for which the device has been snoozed. A device can be snoozed for multiple issues.

You can use the snooze feature in different ways. They are:

Snooze an Issue on a Single Device

1. Click **Snooze** icon in the device row. You see a modal window.

Applications Impacting Performance

Search Filter Export

DEVICE NAME	SERIAL NUMBER	APPLICATION	AVG CPU USAGE	DEVICE GROUP	LAST DETECTED
Laptop_24	SNQ7278834	chrome.exe	40	Not Available	03-01-2023 07:00
Laptop_25	SNQ7278835	chrome.exe	35	Not Available	03-01-2023 07:00
Laptop_100	SNQ7278836	chrome.exe	75	Not Available	03-01-2023 07:00

2. Select the duration from the available options.
3. Click **Snooze**. The device is snoozed. You can see that snooze icon appears before the device name.

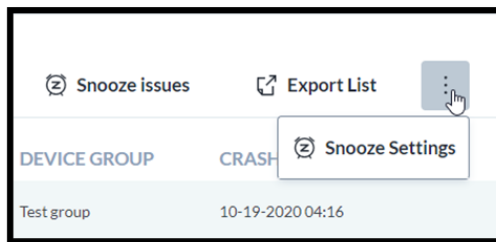
Snooze Same Issue(s) on Multiple Devices

DEVICE NAME	SERIAL NUMBER	APPLICATION	AVG CPU USAGE	DEVICE GROUP	LAST DETECTED
Device_01	INVT278901	Application	80	Test group	10-30-2020 07:00
Device_02	INVT278902	Application	59	Test group	10-30-2020 07:00
Device_03	INVT278903	Application	73	Test group	10-30-2020 07:00
Device_04	INVT278904	Application	82	Test group	10-30-2020 07:00
Device_05	INVT278905	Application	93	Test group	10-30-2020 07:00
Device_06	INVT278906	Application	80	Test group	10-30-2020 07:00

1. Select the checkboxes against the device names with same issue(s).
2. Click **Snooze Issues**. You see a modal window.
3. Select the duration to snooze the devices.

If you mark the checkbox then all devices in the organization will be snoozed for the specific issue(s).

4. Mark the checkbox- Apply to any device with the same issue(s).
5. Click **Snooze**. Both devices with same issue are snoozed.
6. Create a Snooze Rule and Implement on Selected Device(s)



7. Click **Ellipsis**. You see the **Snooze Settings** button.
8. Click **Snooze Setting**. The **Snooze Settings** pop-up window appears.

ADD A RULE is the default tab and on the default pane you can:

9. Select the issue to snooze in the **Snooze By** drop-down list.
10. Select the duration for which device is to be snoozed.

11. Click **Snooze**.

You can select multiple issues from the **Snooze By** drop-down list for specific duration.

You can create new rules by using the ADD A RULE tab. All the rules created can be viewed in the ACTIVE RULES tab.

12. Click Ellipsis.

13. Click Snooze Settings. The Snooze Settings window appears.


14. Select the issues from the drop-down list in **Snooze By** field. The device(s) is snoozed for selected issues.

15. Select duration. It is the time for which the device is snoozed for the selected issue(s).

16. Click **Snooze**. All devices are snoozed for the selected issues.

Unsnnooze the Snoozed Issues

You can unsnooze the snoozed devices in three different ways:

1. Click  from the device row. You see a modal window.
2. Select the Only for this Device option.

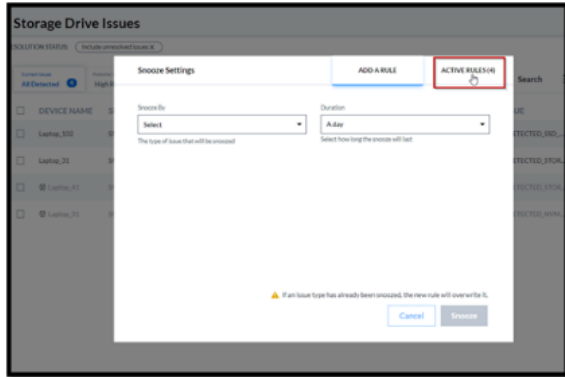
If you select the radio button – For any device - then all devices which were snoozed for specific issue(s), will be unsnoozed.

3. Click **Unsnnooze**. The device is unsnoozed.

Unsnnooze from the Device Tray

1. Click the device row. The device tray window appears.
2. Click the downward arrow in the **Actions** tab. A menu pops up.
3. Click **Unsnnooze** issue. You see a modal window.
4. Select the Only for this device option.
5. Click **Unsnnooze**. The issue is unsnoozed on the device.

Unsnnooze from the Active Rules tab




6. Click **Active Rules** tab. The **Snooze Settings** window appears.
7. Select the **Snoozed Issue** type checkbox in header of the table. All issue types are marked.
8. Click **Unsnnooze**. All the issue types on all devices are unsnoozed.

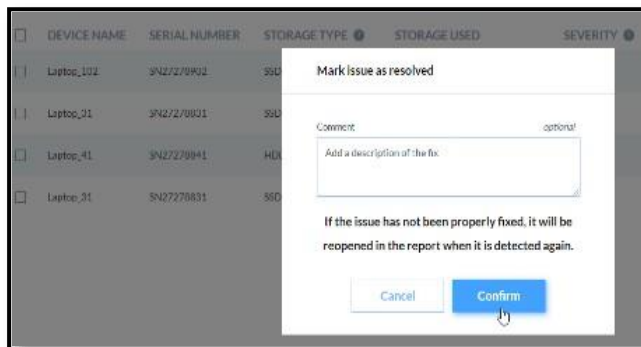
In the Active Rules Tab, following are the headers:

1. **Snoozed Issue Type** – Lists different types of issues that are snoozed
2. **Applied To** - Mentions the serial number of the device(s) on whom issue(s) have been snoozed. When “Any Device” is mentioned then it means that all devices in the organization or fleet having the same issue type(s) will be snoozed for that issue(s).
3. **Except** - Mentions the serial number(s) of the device(s) on which snooze rule is not applied.
4. **Expires At** – Indicates the time and date of expiry of the snooze rule.

Note:

You can now mark an issue on a device as resolved. A green-colored Right icon  appears before the name of the device. If you hover the cursor on the icon a message box pops up. The row is greyed out.

4.1.1. Mark the Issue as Resolved



1. Click on Right Icon. You see a modal window.
2. Enter comment in the comment box (optional).

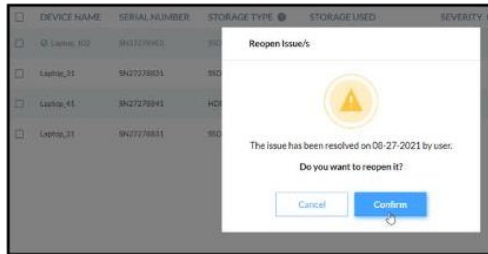
3. Click **Confirm**.

Reopen the Resolved issue

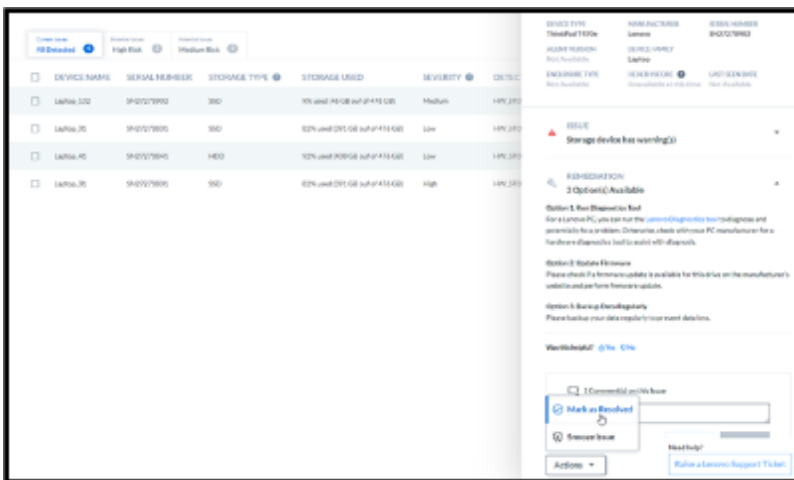


DEVICE NAME	SERIAL NUMBER	STORAGE TYPE	STORAGE USED	SEVERITY	DETECTED ISSUE	DEVICE GROUP	DETECTED ON
Laptop_302	SN27278902	SSD	9% used (46 GB out of 476 GB)	Medium	HW_STORAGE_DETECTED_SRD...	1	11-04-2020 06:02
Laptop_31	SN27278931	SSD	82% used (391 GB out of 476 GB)	Low	HW_STORAGE_DETECTED_STOR...	Test group	11-04-2020 06:02

4. Click on the Right Icon. A window appears.

5. Click **Confirm** to reopen the issue.

You can also resolve and reopen the resolved issue from the device tray.

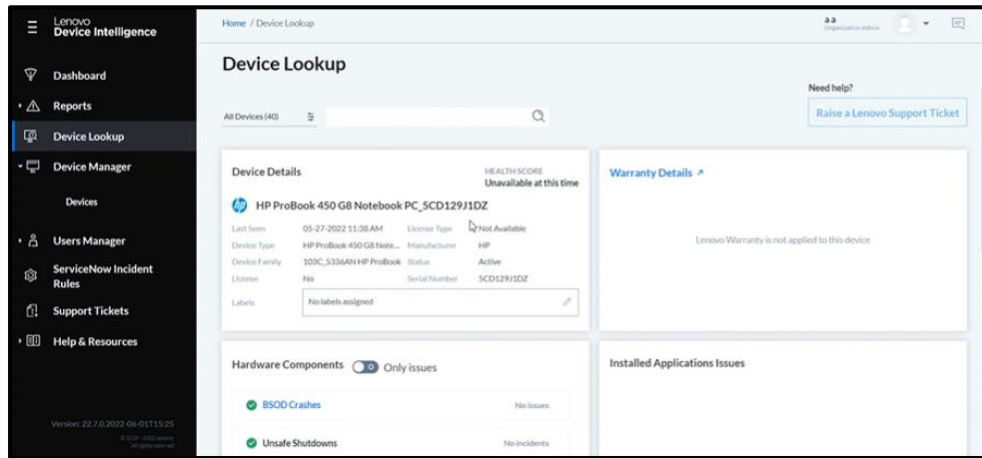


4.2 Device Lookup

Built for use by Service or Help Desk personnel, Device Lookup provides heightened visibility into physical and virtual user desktops to enable IT quickly diagnose problems, enhancing end user experience and productivity while reducing IT personnel involvement. Device Lookup empowers technicians to diagnose user service issues using powerful features to analyse between the problem system and all physical and virtual user systems or any subset to identify and learn where behavior diverges from the normal ones.

Device Lookup reduces the amount of time each service technician spends per call, reduces the number of call escalations, and increases the call resolution ratio. Device Lookup continuously monitors literally hundreds of performance objects on every user system in the environment –

tracking application behavior, system performance, and changes to the user system configuration. Alerted as specified thresholds are exceeded, technicians can make the necessary adjustments to proactively correct the problem.



Key Features:

- Displays last viewed devices
- Health Score
- Hardware components related issues
- Installed applications issues
- [Windows Device Manager Errors](#)

4.3 Device Manager

Overview

Devices represent the PC devices that are in your organization and typically used by employees. A device can be a tablet, notebook, desktop, workstation, or more.

4.3.1 Add Devices

Adding a device requires providing details to the portal about the device (serial number, model, etc.) and provisioning the device with configuration and a software agent.

4.3.2 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. For the device status, refer to [Track Device on LDI](#).

View Devices

Device Tray

From the Devices page, click on any device to open its corresponding *Device Tray*. The Device Tray contains following tabs:

- Device details
- Activity History

The following options are available for a user on the Device Tray:

- View device details
- View hardware and software details about this device
- Delete the device
- Raise a support ticket
- Crashes & Unsafe Shutdowns
- Installed Components & Versions

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

Installed Components and Versions (BIOS, Drivers, Firmware)

- Current BIOS Version
- List of device drivers loaded in last 7 days including current version
- Firmware
- Operating System

[4.3.2.1. Delete or Remove a Device](#)

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

1. Select the devices in the devices list.
2. Click **Delete** and confirm.

The device is no longer accessible in your portal. We recommend you uninstall the LDI Agent from the device if you do not want to use the device in the portal.

[4.3.2.2. Rename a Device](#)

1. Select Device Manager → Devices.
2. Search the device by name or by label.
3. Select More → Export Device List. The Export Devices window appears.
4. Click **Yes**.
5. Open the downloaded CSV file and make the desired changes.

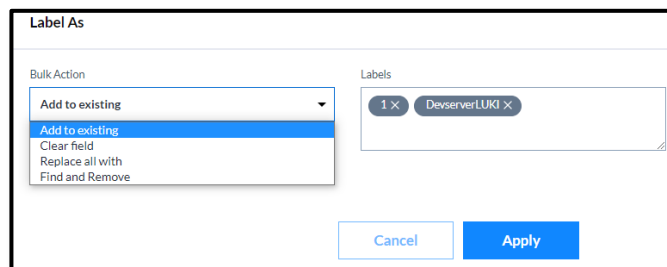
6. Select **More → Import Device Changes**. The **Import Device Changes** window appears.
7. Select the file to import and click **Verify**. The **Import Devices** window appears.
8. Click **Yes**. The **Import Device Changes** notification window appears stating that the details are sent to your email ID.
9. Click **Close**.

Note: Once you receive an email, confirm the change.

Device Labels

To group the devices based on department, location, or device type, you label them using the Label As feature.

1. Select Device Manager → Devices.
2. Select one or more devices and click **Label As**.

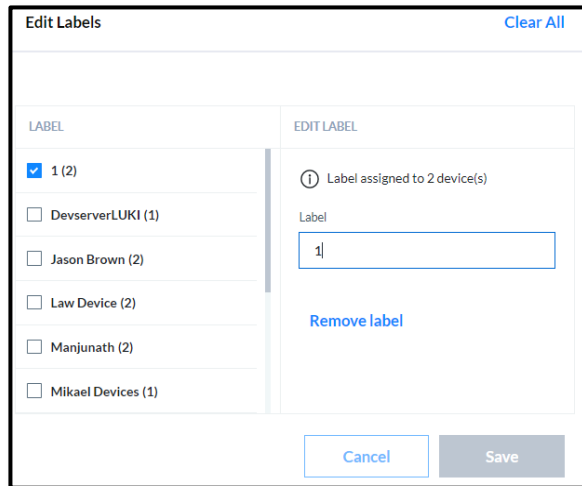


3. Select a value from the **Bulk Action** drop-down list and click in the **Labels** field to select an existing label or create a new one.
4. Click **Apply**. The label/labels are assigned to the device/devices.

Edit Labels

You can edit or delete a label using the Edit Labels feature.

1. Select Device Manager → Devices.
2. Select More → Edit Labels.



3. To remove a label, select one or more labels and click **Remove label**.


Note: From any of the pages that have the filtering widget, you can filter the devices based on label.

4.3.3 Notifications

4.3.3.1. Email Notification on Fleet

The portal sends daily email reports summarizing the issues that are reported in the Dashboard to all users enrolled in your organization. By default, the **Daily Email Summary** report is enabled. Preferences for E-mail Notifications can be configured by selecting User Icon → **Preferences** in the top ribbon.

Feedback

We value all feedback from users. A feedback form can be accessed by clicking on the Messaging Icon () in the top ribbon.



4.3.3.2. Customize Alarms and events

When you select an alarm category button from the Alarm Dashboard, the table displays data for the category's alarms that were active at the Focus Time. Active alarms are those with critical (red) or warning (yellow) severity levels.

When you select the Alarms category, data for the last alarm category button selected displays.

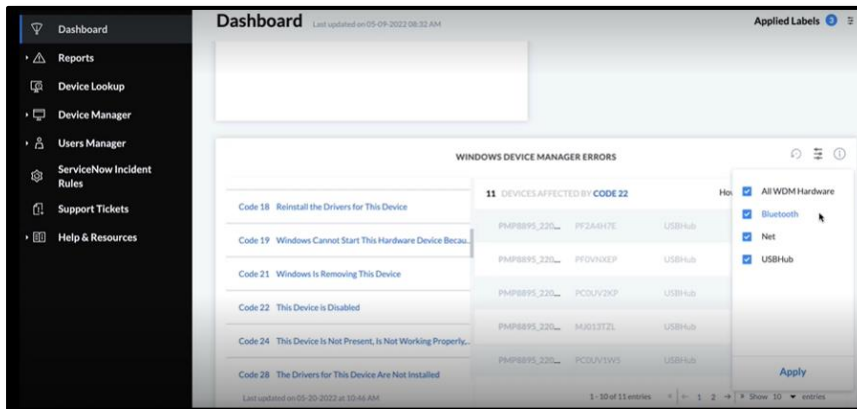
4.3.3.3. Windows Device Manager Errors

This feature allows you to get the device error codes and their details.

-  - Filters the device details based on the error code
-  - Refreshes the device error details

Monitor your fleet

- 1-10 of 200 entries << | < 1 2 3 4 5 ... 8 > | >> - Uses Pagination to navigate to the desired page
- Last Detected at 07-20-2025 at 20:25 PM - Gets the Last Updated details
- ⓘ - Tooltip to know the usage of Windows Device Manager Errors



When you click a device which has an error, the Device Lookup page opens where you can see the complete error details and the error resolution options too.

Note: If the Detected On value is not equal to the Last Updated On value, it means that the Detected On is outdated. It might be the case that the issue is resolved but the system is not synchronised.

5 Integrate with Outside Systems

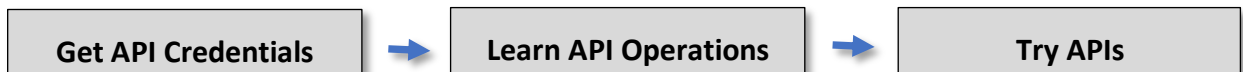
5.1 RESTful API

5.2 Purpose

The purpose of this guide is to inform you how to generate API credentials from your organization admin account, authenticate APIs and use them to integrate LDI with external platforms or applications.

5.3 Audience

This guide is for IT Administrators, Managers, and Developers.

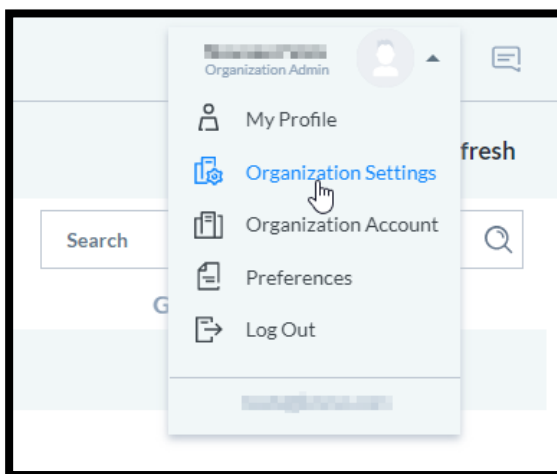


5.4 Get API Credentials

Note: You must have an Organization Administration account in LDI portal to generate API credentials.

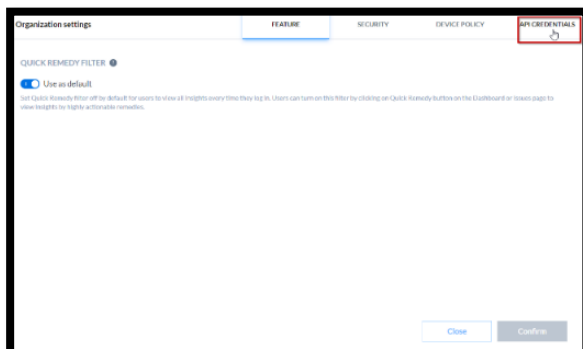
Before you use LDI APIs, you must generate API credentials in the LDI account.

1. Click **Organization Settings** in the Users drop-down list.

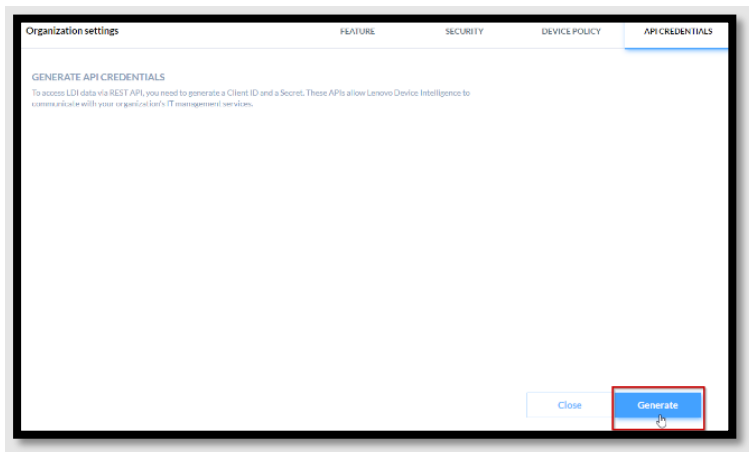


2. Click **API Credentials**. You see API Credentials pane.


Note: If there are no API credentials, you must generate them.



3. Click **Generate**.

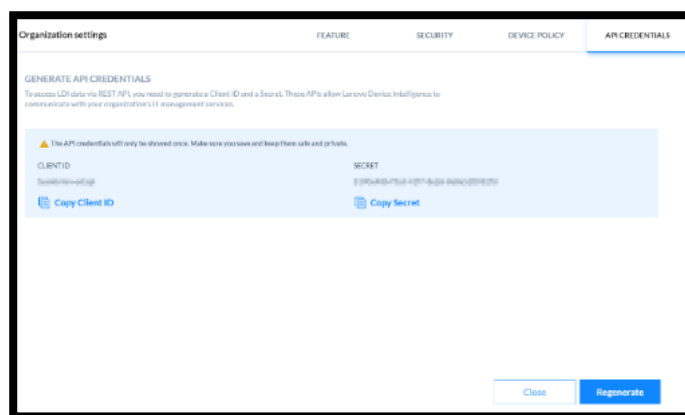


Note: A Client ID and Secret key are generated. You can copy them to the clipboard.

WARNING  **Keep the API credentials in a secure place and regenerate them over the time in accordance with business policies of your organization.**

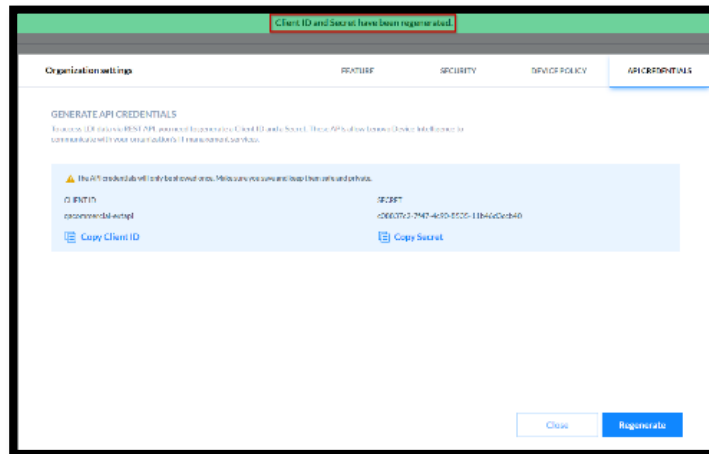
If you want to change the existing API credentials, you must generate a new one.

4. Click **Regenerate**.



5. In the **Regenerate Secret** window, click **Regenerate**.

6. A new Client ID and Secret key is generated.



The Client ID and Secret key do not expire until you regenerate a fresh pair.

After you have generated API credentials, you can use the following URLs to access different API endpoints.

Type the URL : <https://auth.naea1.uds.lenovo.com> or <https://auth.euwe1.uds.lenovo.com>, depending upon the organization region the devices are located.

[Generate LDI API credentials](#) (Client ID and Secret).

LDI API URLs

1. NA

External API: <https://api.naea1.uds.lenovo.com>

Authentication: <https://auth.naea1.uds.lenovo.com>

2. EU

External API: <https://api.euwe1.uds.lenovo.com>

Authentication: <https://auth.euwe1.uds.lenovo.com>

NA is North American Region and EU is European Union Region.

Note: After you generate a new pair of Client ID and Secret key, the older pair gets invalid.

The bearer token is a type of an access token that uses Auth 2.0 and expires within 30 minutes. You use the bearer token to get a new Access token. To get an access token you send the Authentication server this bearer token along with your client id. This way the server knows that the application using the bearer token is the same application that the bearer token was created for.

Generate API bearer token using External API.

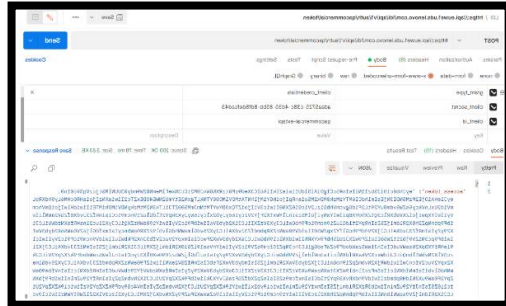
The URL - Base URL + /api/v1/auth/<organization_name>/token

Note: The Base URL depends on your region whether NA or EU.

Body should be x-www-form-urlencoded and should contain:

- grant_type: client_credentials
- client_secret: secret (from api credentials page)
- client_id: id (from api credentials page)

Note: Generate a new bearer token when it expires after 30 minutes.



```
private synchronized Tuple2<String, Instant> fetchNewToken() {
    Instant now = Instant.now();
    var response = authClient
        .POST_FORM("/api/v1/auth/" + realm + "/token",
            Map.of("grant_type", "client_credentials",
                "client_id", clientId,
                "client_secret", clientSecret));

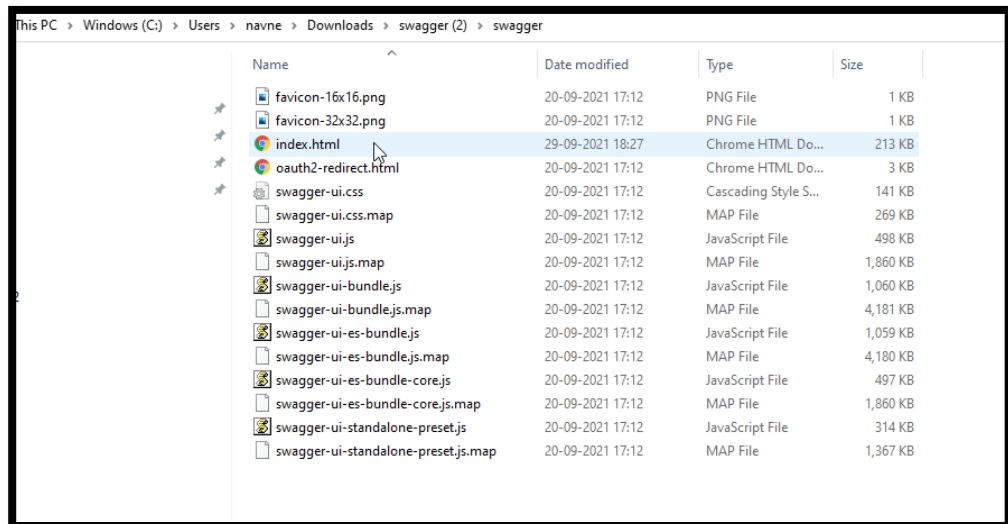
    if (response.code >= 400) throw new RuntimeException("Token not
retrieved: " + response.asString());
    var body = response.asMap();
    String accessToken = (String) body.get("access_token");
    int expiresIn = ((Number) body.get("expires_in")).intValue();
    return new Tuple2<>(accessToken, now.plusSeconds(expiresIn - 15));
}

public synchronized String getToken() {
    if ((token == null) || (token.getV2().isAfter(Instant.now())))
```

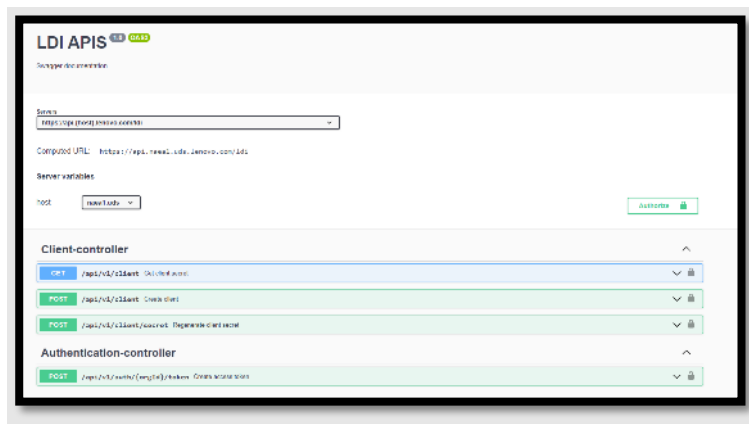
5.5 Learn API Operations

Swagger specification archive contains a folder with an index.html file and some other JavaScript files.

1. Download Swagger Specification zip file from the [support site](#) which provides you details about each API.
2. Extract the files in the folder.



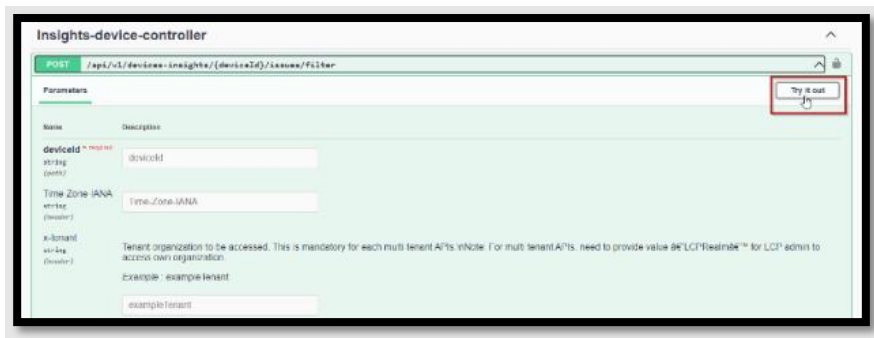
3. Double-click to open the index.html. You see the LDI APIs home page in Swagger.



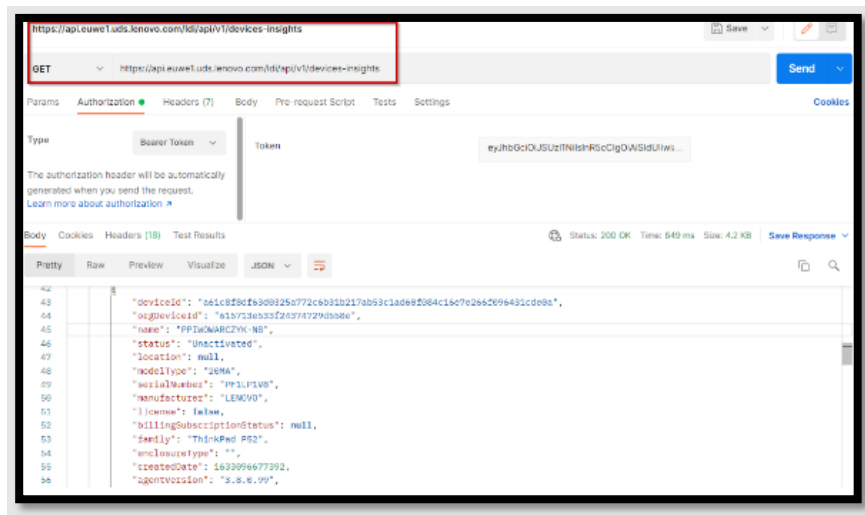
4. Generate a bearer token (Refer [Get API Credentials](#) and Postman example).

5.6 Try APIs

1. Select an API method in Swagger.



2. Use the bearer token in the call.
3. Click Try it out.



5.7 Examples of API Methods

5.7.1.1. Authentication - API token session

ACME JAVA CODE

```

package com.acme.ldi.test;

public class LdiClientTest {

    @org.junit.Test
    void tokenTest() {
        // parameters depends on geography
        String authUrl = "https://api.uds-qa.lenovo.com";
        String apiUrl = "https://api.uds-qa.lenovo.com";
        // realm name supplied by sales team
        String realm = "autoticketing";
        // client id to be supplied by integration support team
        String clientId = "autoticketing-extapi";
        // client secret gotten via UI self-service
        String clientSecret = "0bf4c041-a9b1-4133-9045-73795a254439";

        LdiClient client = new LdiClient(apiUrl, realm, clientId,
clientSecret);
    }
}

```


Lenovo SDK snapshot

POST <https://api.uds-qa.lenovo.com/ldi/api/v1/auth/autoticketing/token>

Content-Type: application/x-www-form-urlencoded

client_id=autoticketing-extapi&client_secret=0bf4c041-a9b1-4133-9045-73795a254439&grant_type=client_credentials

```
private synchronized Tuple2<String, Instant> fetchNewToken() {
    Instant now = Instant.now();
    var response = apiClient
        .POST_FORM("/ldi/api/v1/auth/" + realm + "/token",
            Map.of("grant_type", "client_credentials",
                "client_id", clientId,
                "client_secret", clientSecret));
    if (response.code >= 400) throw new RuntimeException("Token not
retrieved: " + response.asString());
    var body = response.asMap();
    String accessToken = (String) body.get("access_token");
    int expiresIn = ((Number) body.get("expires_in")).intValue();
    return new Tuple2<>(accessToken, now.plusSeconds(expiresIn - 15));
}

public synchronized String getToken() {
    if ((token == null) || (token.getV2().isAfter(Instant.now())))
        token = fetchNewToken();
    return token.getV1();
}
```

date: Tue, 28 Sep 2021 11:47:12 GMT

pragma: no-cache

referrer-policy: no-referrer

server: Lenovo

set-cookie: KC_RESTART=; Version=1; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Max-Age=0; Path=/auth/realms/autoticketing/; Secure; HttpOnly

strict-transport-security: max-age=31536000; includeSubDomains

x-content-type-options: nosniff

x-frame-options: SAMEORIGIN

```
x-xss-protection: 1; mode=block
{"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41
R
...(truncated text)
zU0Nk1CX0RB0FJU0yKRZ-H716fnlFWk54eCn2vouFmKFz2frAuR9kE-
bgp3AhTSOuT6nlb4HGmSrMNNkYbg","expires_in":15552000,"refresh_expires_in":0,"to
ken_type":"Bearer","not-before-policy":0,"scope":"email profile"}
```

5.8 Negative API Sample

5.8.1.1. Groovy ACME Test

```
@Test
void tokenNegativeTest() {
    var client = new com.lenovo.lidi.client.LdiClient(authUrl, apiUrl, realm,
clientId, clientSecret + "_INVALID");
    var response = client.authClient
        .POST_FORM("/auth/realms/" + realm + "/protocol/openid-
connect/token",
            [grant_type : "client_credentials",
             client_id   : clientId,
             client_secret: clientSecret])
    assert response.code == 401
```

POST https://auth.uds-qa.lenovo.com/auth/realms/autoticketing/protocol/openid-
connect/token

Content-Type: application/x-www-form-urlencoded

grant_type=client_credentials&client_secret=0bf4c041-a9b1-4133-9045-
73795a254439-INVALID&client_id=autoticketing-extapi

HTTP Response

401

```
access-control-allow-credentials: true
cache-control: no-store
content-length: 75
content-security-policy: frame-src 'self'; frame-
ancestors 'self' https://portal.uds-
qa.lenovo.com https://developer.naea1.uds-qa.lenovo.com; object-src 'none';
content-type: application/json
date: Tue, 28 Sep 2021 13:29:06 GMT
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
```

5.9 User Management

```
package com.acme.LDI .test
import org.junit.jupiter.api.Test
class UserTests extends BaseLDI TestClass {
    @Test
    void createNewUser() {
        var response = this.client.authenticatedRestConnector.POST("/LDI
/api/v1/users",
            [loginId      : "ccretoiu@lenovo.com",
             compositeRoleName: "pm_org_admin",
             firstName      : "ABC",
             creatorId      : "autoticketing",
             country        : "USA",
             email          : "ccretoiu@lenovo.com",
             lastName       : "ABC"])
        assert response.code == 409 // Expected conflict
    }
    @Test
    void getAllUsers() {
```

```

        var response = this.client.authenticatedRestConnector.GET("/LDI
/api/v1/users")
        assert response.code == 200
        var body = response.asMap()
        assert body.keySet() == ['_embedded', 'page', 'responseType'] as Set
        var usersList = body._embedded.userList
        var loginIds = usersList*.loginId
        println "${loginIds.size()} users found: ${loginIds}"
    }
    @Test
    void createAndDeleteUser() {
        var seed = Math.random().toString().replaceAll(/[^\d]/, '')
        var response = this.client.authenticatedRestConnector.POST("/LDI
/api/v1/users",
            [loginId          : "sdragos.${seed}@lenovo.com",
             compositeRoleName: "pm_org_admin",
             firstName       : "ABC",
             creatorId       : "autoticketing",
             country         : "USA",
             email           : "sdragos.${seed}@lenovo.com",
             lastName        : "ABC"])
        assert response.code == 201
        var searchResult = this.client.authenticatedRestConnector.GET("/LDI
/api/v1/users", [freeText: "sdragos.${seed}@lenovo.com"])
        assert searchResult.asMap()._embedded.userList*.loginId ==
["sdragos.${seed}@lenovo.com"]
        var userDetails = searchResult.asMap()._embedded.userList[0]

        var deleteResponse =
this.client.authenticatedRestConnector.PATCH("/LDI /api/v1/users",
            ["userList" : [userDetails.userId],
             "operation": "DELETE"]
        )
        var secondSearchResult =
this.client.authenticatedRestConnector.GET("/LDI /api/v1/users",
[freeText: "sdragos.${seed}@lenovo.com"])
        var usersList=secondSearchResult.asMap()?._embedded?.userList

```

```
        assert (usersList?.collect { it['loginId'] } ?: []).empty
    }
}
```

5.9.1 GET Users

HTTP Request

```
GET https://api.uds-qa.lenovo.com/LDI /api/v1/users

Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
... (truncated text) vxilXFgr4gKVbCfnnVUScQXPkcGF2aqifGEQNaLiIXsBWM8iAX8smq-
2YNZdY509LuBw
```

API Response

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json
date: Wed, 29 Sep 2021 10:31:13 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
transfer-encoding: chunked
x-content-type-options: nosniff
x-envoy-upstream-service-time: 349
x-frame-options: DENY
x-xss-protection: 1; mode=block

{"_embedded":{"userList":[{"userId":"7204a566-1495-4be8-8c76-19899adf508d"...
(truncated
text)...{"number":0,"size":8,"totalElements":8,"totalPages":1},"responseType":"P
AGE"}
```

Stdout

```
8 users found: [shuma@lenovo.com, sdragos@lenovo.com, penghong2@lenovo.com, penghong221062911034172@lenovo.com, penghong2+21063007144784@lenovo.com, otsiupa@lenovo.com, ccretoi@lenovo.com, ladamestean1@lenovo.com]
```

5.9.2 Create User

POST <https://api.uds-qa.lenovo.com/LDI/api/v1/users>

Authorization: Bearer

eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW...(truncated text).... -4NQ

Content-Type: application/json; charset=utf-8

```
{
  "loginId": "ccretoiu@lenovo.com",
  "compositeRoleName": "pm_org_admin",
  "firstName": "ABC",
  "creatorId": "autoticketing",
  "country": "USA",
  "email": "ccretoiu@lenovo.com",
  "lastName": "ABC"
}
```

409

cache-control: no-cache, no-store, max-age=0, must-revalidate

content-length: 99

content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com; style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-src 'self' 'unsafe-inline'; object-src 'none';

content-type: application/json

date: Wed, 29 Sep 2021 10:31:15 GMT

expires: 0

pragma: no-cache

referrer-policy: no-referrer

server: Lenovo

strict-transport-security: max-age=31536000; includeSubDomains

x-content-type-options: nosniff

x-envoy-upstream-service-time: 54

x-frame-options: DENY

x-xss-protection: 1; mode=block

```
{"messages":["User with login id ccretoiu@lenovo.com already exist in organization autoticketing"]}]}
```

Email

```
GET https://api.uds-qa.lenovo.com/LDI  
/api/v1/users?freeText=sdragos.02879781611736808%40lenovo.com
```

```
Authorization: Bearer  
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW  
...(truncated text)... SMHqjNONc5SeugT5C4dINKENr0Mlh933i6qw
```

200

```
cache-control: no-cache, no-store, max-age=0, must-revalidate  
content-length: 1269  
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;  
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-  
src 'self' 'unsafe-inline'; object-src 'none';  
content-type: application/json  
date: Wed, 29 Sep 2021 10:31:18 GMT  
expires: 0  
pragma: no-cache  
referrer-policy: no-referrer  
server: Lenovo  
strict-transport-security: max-age=31536000; includeSubDomains  
x-content-type-options: nosniff  
x-envoy-upstream-service-time: 183  
x-frame-options: DENY  
x-xss-protection: 1; mode=block  
{"_embedded":{"userList":[{"userId":"555fcf91-9dca-4fc6-9df5-...(truncated  
text)...number":0,"size":1,"totalElements":1,"totalPages":1},"responseType":"PAG  
E"]}
```

5.9.3 Delete User

```
PATCH https://api.uds-qa.lenovo.com/LDI /api/v1/users
```

```
Authorization: Bearer  
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW  
...(truncated text)... KBLewSCisibDjTmr8RNt4w  
Content-Type: application/json; charset=utf-8
```

```
{
  "userList": [
    "555fcf91-9dca-4fc6-9df5-4d9f38841e2d"
  ],
  "operation": "DELETE"
}
```

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 95
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data;; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json
date: Wed, 29 Sep 2021 10:31:20 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 601
x-frame-options: DENY
x-xss-protection: 1; mode=block
{"operationSuccessfulUsers":["555fcf91-9dca-4fc6-9df5-
4d9f38841e2d"],"operationFailedUsers":[]}
```

5.10 Devices

5.10.1.1.ACME Client Code

Acme Groovy Code

```
package com.acme.LDI .test

import org.junit.jupiter.api.Test

class DevicesTests extends BaseLDI TestClass {
    @Test
    void getDevices() {
```



```

        var response = client.authenticatedRestConnector.GET("/LDI
/api/v1/devices/")
        assert response.code == 200
        var body = response.asMap()
        assert body.keySet() ==
['content', 'pageable', 'last', 'totalElements', 'totalPages', 'sort', 'first'
, 'number', 'numberOfElements', 'size', 'empty'] as Set
        assert body['content'] instanceof List
    }
    @Test
    void export() {
        var deviceId = client.authenticatedRestConnector.GET("/LDI
/api/v1/devices/").asMap()['content'][0]['deviceId']
        var response = client.authenticatedRestConnector.POST("/LDI
/api/v1/devices/bulk/export",
            [ids: [deviceId]])
        assert response.code == 200
        var file = response.asFile()
        assert file.name =~ /\.*.csv/
        assert file.text.split(/\v/)[0] == 'DEVICE NAME,MACHINE TYPE,SERIAL
NUMBER,GROUP'
    }
}

```

5.10.1.2. HTTP Request Responses

Get Devices

Request

```
GET https://api.uds-qa.lenovo.com/LDI /api/v1/devices/
```

```
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50b3RhdGEiLCJ1aWQiOiJhICJwZG1iME41RzU0Nk1CX0RBOFJUOW
...(truncated text)...N0LFHsvE7Q09QXeGzoU0IS86PlDF16BhEEcXzN5Pow
```

200

```

cache-control: no-cache, no-store, max-age=0, must-revalidate
content-security-policy: default-src 'self'; connect-src *.uds-qa.lenovo.com;
style-src 'self' 'unsafe-inline'; img-src 'self' data:; script-
src 'self' 'unsafe-inline'; object-src 'none';
content-type: application/json

```

```
date: Tue, 28 Sep 2021 15:37:56 GMT
expires: 0
pragma: no-cache
referrer-policy: no-referrer
server: Lenovo
strict-transport-security: max-age=31536000; includeSubDomains
transfer-encoding: chunked
x-content-type-options: nosniff
x-envoy-upstream-service-time: 543
x-frame-options: DENY
x-xss-protection: 1; mode=block

{"content":[{"orgDeviceId":"6112d2990e9e6a202b99effc","deviceId":""},"orgId":
...(truncated
text)...{"sorted":true,"unsorted":false,"empty":false},"number":0,"first":true,"
numberOfElements":20,"size":20,"empty":false}
```

5.11 Fleet Management

ACME Code

Fleet Status

```
package com.acme.LDI .test

import org.junit.jupiter.api.Test

class FleetManagement extends BaseLDI TestClass {

    @Test
    void fleetStatus() {
        var response = client.authenticatedRestConnector.GET("/LDI
/api/v1/fleethealth")

        assert response.asMap().keySet() ==
["latestJobRuntime", "timestamp", "fleetHealthScore", "fleetBsodScore", "fleet
StorageScore", "fleetBatteryScore", "fleetWdmScore", "fleetPerformanceScore"]
as Set
    }
}
```

5.12 Insights Tests

```
package com.acme.LDI .test

import org.junit.jupiter.api.Test

class InsightsTests extends BaseLDI TestClass {
```

```

@Test
void insightsTest() {
    var devices = client.authenticatedRestConnector.GET('/LDI
/api/v1/devices').asMap().content
    var deviceId = devices[0].deviceId
    var response = client.authenticatedRestConnector.POST("/LDI
/api/v1/devices-insights/$deviceId/issues/filter", [:])
    var body = response.asMap()
    assert body.keySet() ==
['content', 'pageable', 'last', 'totalElements', 'totalPages', 'sort', 'first'
, 'number', 'numberOfElements', 'size', 'empty'] as Set
    assert body['size'] == 20
}
}

```

5.12.1.1. Request

```
GET https://api.uds-qa.lenovo.com/LDI /api/v1/fleethealth
```

```

Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpzZW50b3R0IiwiaWF0IjoiYXZlICJwZG1iME41RzU0Nk1CX0RBOFJUOW
...(truncated
text)...SWWahdAVE1lOwYgQRmbPNnDEoAq_ajmCyTPDb3SRR2C1JqIjF0za2Yr796vj5xgoyycLOL1
4ydadQ

```

Response

```

200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 223
content-type: application/json
date: Wed, 29 Sep 2021 10:30:58 GMT
expires: 0
pragma: no-cache
server: Lenovo
strict-transport-security: max-age=31536000 ; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 314
x-frame-options: DENY
x-xss-protection: 1; mode=block

```

```
{"latestJobRuntime":"2021-09-24T07:49:42.196","timestamp":"2021-09-10T05:06:01.585638","fleetHealthScore":98,"fleetBsodScore":100,"fleetStorageScore":91,"fleetBatteryScore":94,"fleetWdmScore":99,"fleetPerformanceScore":100}
```

5.13 Issues Filter

Issues Tests

```
package com.acme.LDI .test
import org.junit.jupiter.api.Test
class IssuesFilter extends BaseLDI TestClass {
    @Test
    void filterIssues() {
        var response = client.authenticatedRestConnector.POST('/LDI
/api/v1/issues/filter')
        assert response.code == 200
        var body = response.asMap()
        assert body.keySet() ==
['content', 'pageable', 'last', 'totalElements', 'totalPages', 'sort', 'number
', 'first', 'numberOfElements', 'size', 'empty'] as Set
        assert body['pageable']['pageNumber'] == 0
        assert body['pageable']['pageSize'] == 20
        assert body['content'] instanceof List
        println "Found ${body['content'].size()} issues."
    }
    @Test
    void markIssueAsResolved() {
        var response = client.authenticatedRestConnector.POST('/LDI
/api/v1/issues/mark-as-resolved',
            ["issuesUids": ["fake-issue-uid"],
            "comment"    : "Would like to resolve an issue that does NOT
exist."
            ])
        assert response.code == 404
    }
}
```

Request

```
POST https://api.uds-qa.lenovo.com/LDI /api/v1/issues/filter
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
...(truncated text)...
bzhfSJCvsw8pTti6yVbvHLJVaw1eNkqVkVXJ2DXwDMoAyibXc7OCUmLX0JfH2fU9tfERhYWwd7A
```

Response

```
200
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-type: application/json
date: Wed, 29 Sep 2021 10:31:07 GMT
expires: 0
pragma: no-cache
server: Lenovo
strict-transport-security: max-age=31536000 ; includeSubDomains
transfer-encoding: chunked
x-content-type-options: nosniff
x-envoy-upstream-service-time: 2066
x-frame-options: DENY
x-xss-protection: 1; mode=block
{"content":[{"bucketId":"app_performance_impact","category":"Excel.exe","code
":null...(truncated text)...
2,"first":true,"numberOfElements":20,"size":20,"empty":false}
```

5.14 Mark Issue as Resolved

```
@Test
void markIssueAsResolved() {
    var response = client.authenticatedRestConnector.POST('/LDI
/api/v1/issues/mark-as-resolved',
        ["issuesUids": ["fake-issue-uuid"],
        "comment"      : "Would like to resolve an issue that does NOT
exist."
        ])
    assert response.code == 404
}
```

Request

```
POST https://api.uds-qa.lenovo.com/LDI /api/v1/issues/mark-as-resolved
```

```
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSldUIiwia2lkIiA6ICJwZG1iME41RzU0Nk1CX0RBOFJUOW
...(truncated text)...
_ZD3p_pmiikTMzOJyQQ64CDSxE7DmRjS_zirs0XAnDQ5nIm716XVxn9bqgCriHNoqSERg8CyRWJixL
BRPIe1P5K6Zd184A
Content-Type: application/json; charset=utf-8
{
  "issuesUids": [
    "fake-issue-uuid"
  ],
  "comment": "Would like to resolve an issue that does NOT exist."
}
400
cache-control: no-cache, no-store, max-age=0, must-revalidate
content-length: 1355
content-type: application/json
date: Wed, 29 Sep 2021 10:31:03 GMT
expires: 0
pragma: no-cache
server: Lenovo
strict-transport-security: max-age=31536000 ; includeSubDomains
x-content-type-options: nosniff
x-envoy-upstream-service-time: 71
x-frame-options: DENY
x-xss-protection: 1; mode=block
{"timestamp":"2021-09-29T10:31:03.761+00:00","status":400,"error":"Bad
Request","message":"400 BAD_REQUEST \"JSON parse error: Cannot deserialize
value of type `java.util.UUID` from String `fake-issue-uuid`: UUID has to be
represented by standard 36-char representation; nested exception is
com.fasterxml.jackson.databind.exc.InvalidFormatException: Cannot deserialize
value of type `java.util.UUID` from String `fake-issue-uuid`: UUID has to be
represented by standard 36-char representation\\n at [Source:
(PushbackInputStream); line: 3, column: 9] (through reference chain:
com.lenovo.iss.graphql.rest.request.MarkAsResolvedRequest[\\issuesUids\\]-
>java.util.HashSet[0])\\\", \"path\":\"/iss-insights-api/api/issues/mark-as-
resolved\", \"errors\": {\"defaultMessage\": \"400 BAD_REQUEST \"JSON parse error:
Cannot deserialize value of type `java.util.UUID` from String `fake-issue-
uuid`: UUID has to be represented by standard 36-char representation; nested
exception is com.fasterxml.jackson.databind.exc.InvalidFormatException: Cannot
```

```
deserialize value of type `java.util.UUID` from String \"fake-issue-uuid\":
UUID has to be represented by standard 36-char representation\n at [Source:
(PushbackInputStream); line: 3, column: 9] (through reference chain:
com.lenovo.iss.graphql.rest.request.MarkAsResolvedRequest[\"issuesUuids\"]-
>java.util.HashSet[0])\""}}
```

Response

Assertion failed:

```
assert response.code == 404
|           |           |
|           400 false
com.lenovo.LDI .util.RestResponse@f6497e3
at
org.codehaus.groovy.runtime.InvokerHelper.assertFailed(InvokerHelper.java:436)
at
org.codehaus.groovy.runtime.ScriptBytecodeAdapter.assertFailed(ScriptBytecodeA
dapter.java:670)
at com.acme.LDI
.test.IssuesFilter.markIssueAsResolved(IssuesFilter.groovy:25)
at java.base/java.lang.Thread.run(Thread.java:834)
```

5.15 Sensors

```
package com.acme.LDI .test
import org.junit.jupiter.api.Test
class SensorsTest extends BaseLDI TestClass {
    @Test
    void getDefinedSensors() {
        // Test not functional, it's expected to fail
        var response =
client.authenticatedRestConnector.GET("/api/v1/LDI/definedsensors?descriptionA
pp=1")
        assert response.code == 200 // Test not implemented
    }
    @Test
    void getSensorActions() {
        // Test not functional, it's expected to fail
    }
}
```

```

        var response =
client.authenticatedRestConnector.GET("/api/v1/LDI/sensoractions?descriptionAp
p=1")
        assert response.code == 200 // Test not implemented
    }
}

```

5.16 ServiceNow Integration

The Lenovo Device Intelligence (LDI) ServiceNow Integration section helps you setup LDI ServiceNow Plugin so that ServiceNow platform can connect to device(s) in the LDI organization account through LDI external API.

5.16.1 Audience

IT Administrators, Analysts, and Managers.

5.16.2 Prerequisites

- Establish parity between LDI and ServiceNow Platforms.

Note:

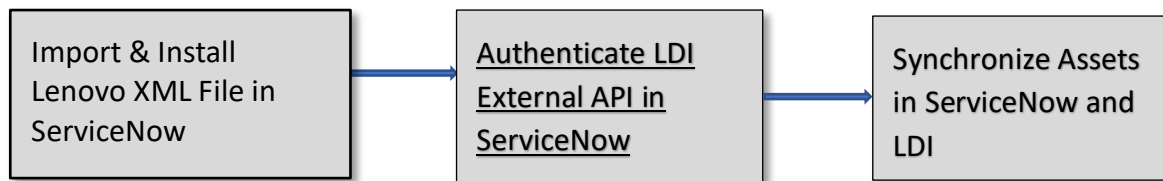
A physical device like laptop, desktop, server, etc. is referred to as a Device in LDI application and as an Asset in the ServiceNow application.

You must synchronize devices in LDI with the Assets or configuration items in the ServiceNow application for the proper working of the LDI ServiceNow plugin. Therefore, you must fulfil the following conditions:

- The name of the LDI device must be the same as the name of the Asset in the ServiceNow application
- The Serial number of the LDI device and Asset serial number must be the same.
- Requisite Roles and Rights required for LDI and ServiceNow accounts.

Application	Roles and Rights
Lenovo Device Intelligence (LDI)	You must have an Organization Administrative account to generate API credentials - Client ID and Secret. The API credentials are required for API integration between LDI and ServiceNow so that the LDI ServiceNow plugin can work.
ServiceNow	Administrator account

Disclaimer – The LDI ServiceNow plugin was developed and tested in a clear and empty ServiceNow Instance. Any change done by ServiceNow in their platform can affect the LDI ServiceNow plugin.



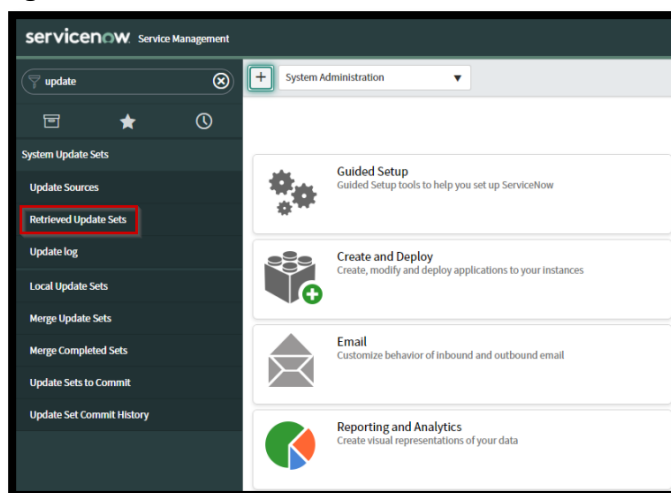
5.16.3 Import and Install Lenovo XML File in ServiceNow

Application Remote Update Set is an XML file that you can import into ServiceNow Instance. The file contains configuration and scripts developed by Lenovo.

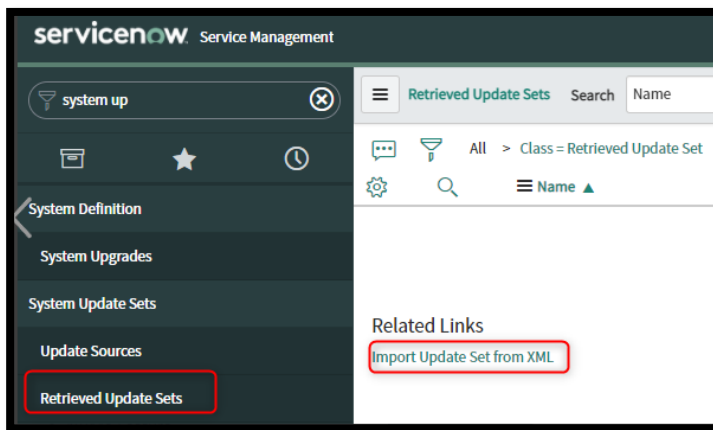
Note: It is mandatory to have an administrative account in ServiceNow application.

Follow these steps to import and install Lenovo XML file:

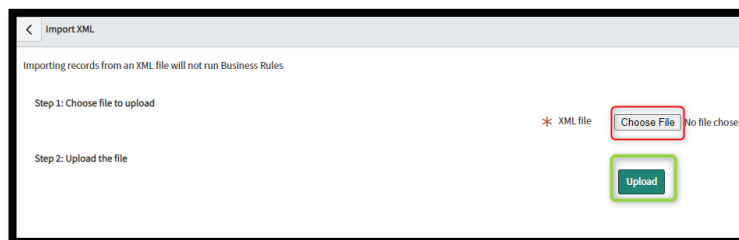
1. Sign in to the ServiceNow dashboard.



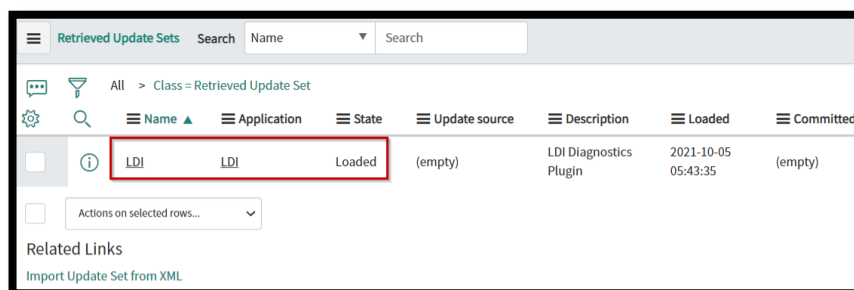
2. Enter **update** in the search box. The **System Update Sets** menu appears.
3. Click **Retrieved Update Sets**. In the Related Links, Import Update Set from XML link appears.



4. Click Import Update Set from XML.



5. Click **Choose file**, and then click **Upload**. After the file is imported, the LDI application appears in the list.



6. Click **LDI**. The LDI record appears in the ServiceNow application.

Retrieved Update Set
LDI

Name: LDI

Application: LDI

Update source:

Parent:

State: Loaded

Loaded: 2021-10-05 05:43:35

Description: LDI Diagnostics Plugin

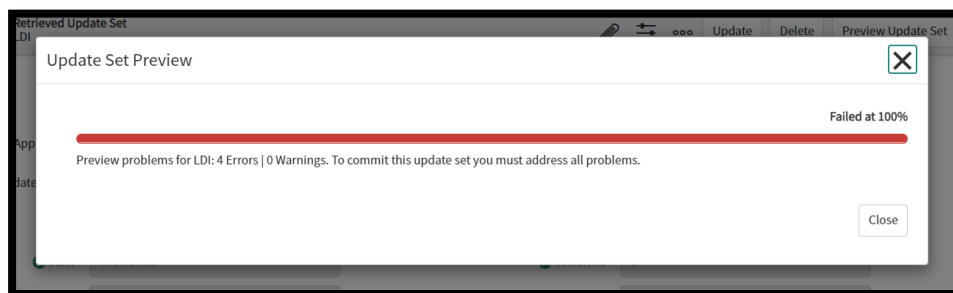
Application name: LDI

Update Delete **Preview Update Set**

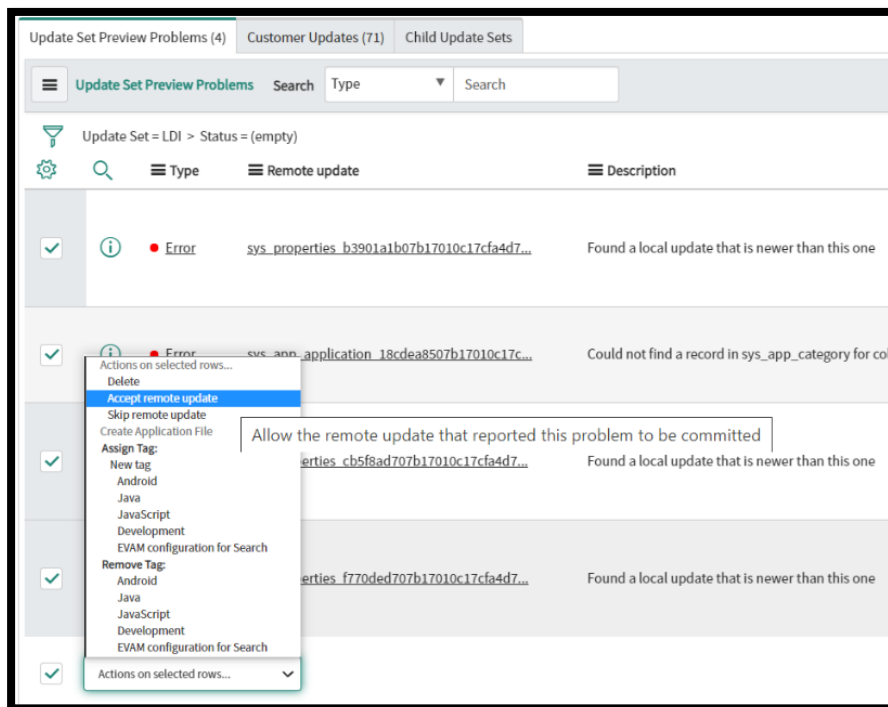
Note: You can update, delete, or get a preview of the LDI update sets.

7. Click **Preview Update Set**.

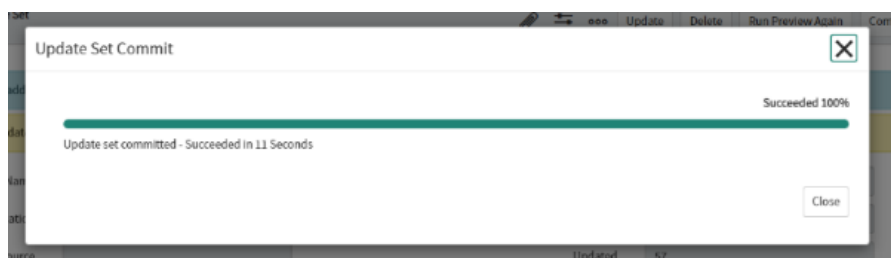
Note: The preview fails if there are errors during import of LDI XML file.



8. To resolve the errors, select all errors in the tab, click **Update Set Preview Problems**.



9. Click **Accept remote update**.

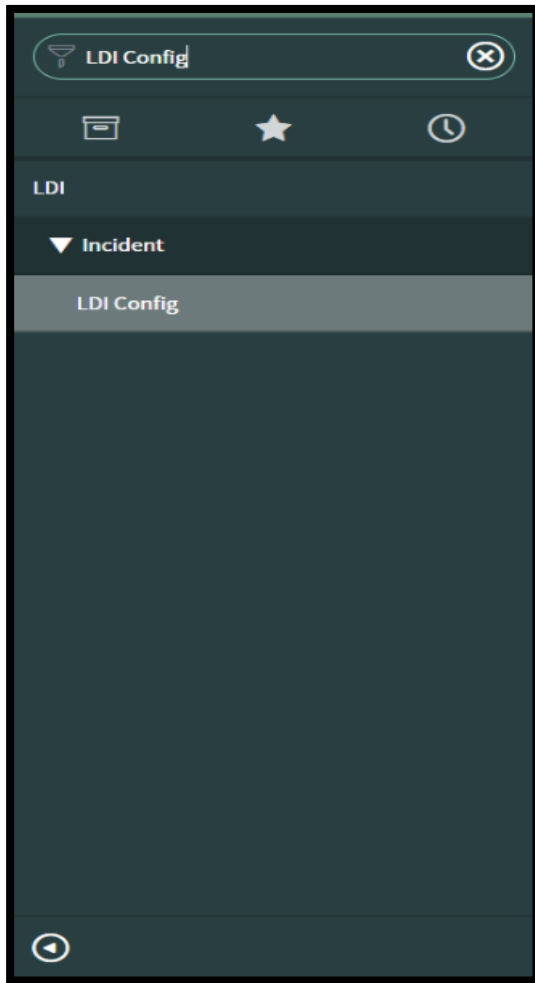


10. Click **Commit**. The update set is successfully committed.

5.16.4 Authenticate LDI API Credentials in ServiceNow

This section explains how to add the LDI API credential in the ServiceNow instance to setup LDI ServiceNow plugin.

1. In the search box, enter **LDI Config**. The **LDI Config** tab appears.



2. Click **LDI Config**. The **Properties** page appears. In this page, enter credentials of LDI API to establish connection between ServiceNow and LDI platform.

3. Enter LDI API Client ID.

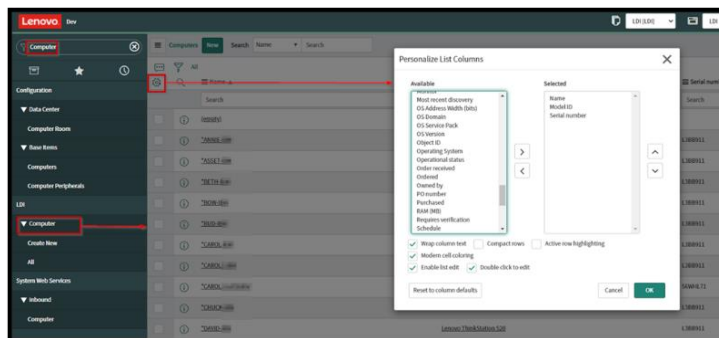
Note: To generate LDI API credentials, refer to [Get API Credentials](#).

5.16.5 Synchronize Assets in ServiceNow and LDI

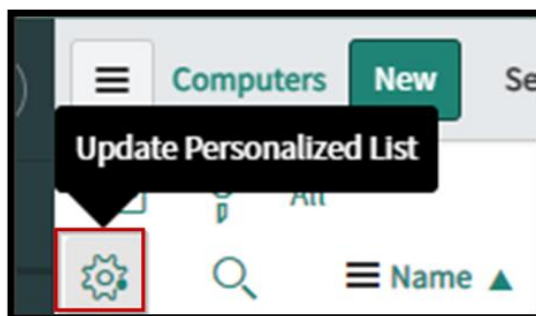
Refer [Prerequisites](#) section before proceeding ahead.

11. Log in to ServiceNow instance.

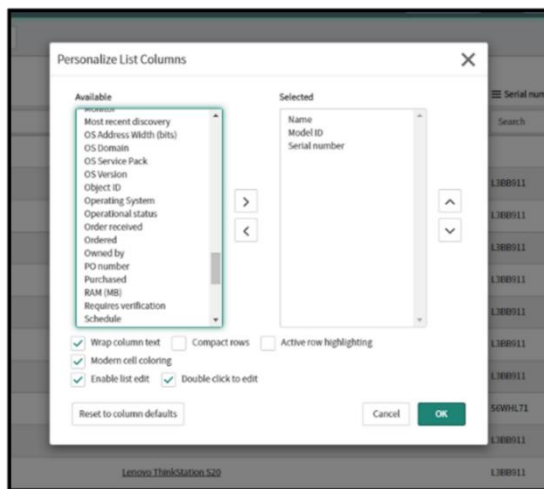
12. In the search box, enter **computer**. The **Computer** tab appears in the navigation menu.



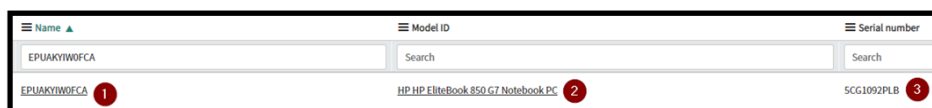
13. Click **Computer** in the navigation menu. The list of Assets appears in the pane.



14. Click the **Settings**  icon. The **Personalize List Columns** window appears.



Note: The checkboxes shown in the screenshot are marked by default.

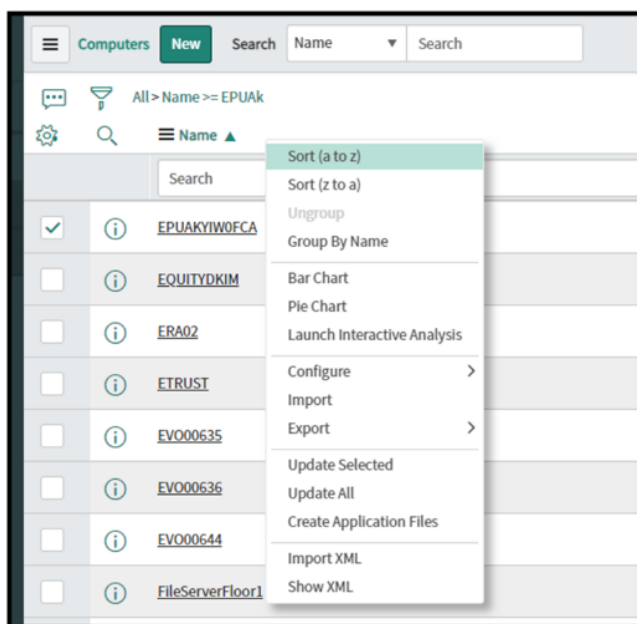


1. Name of the Asset. For example, EPUAKYIW0FCA
2. Model ID of the Asset – HP EliteBook 850G7 Notebook
3. Serial Number of the Asset – 5CG1092

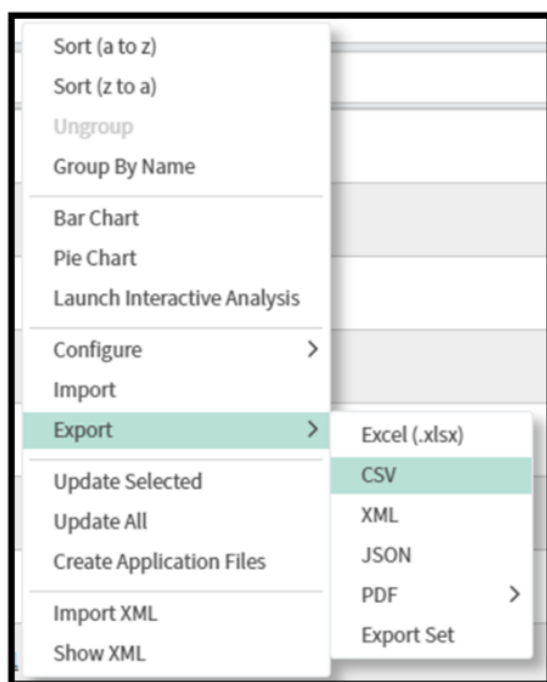
You can search an asset by the Name, Model ID, or Serial Number. Choose assets you want to synchronize by using filters.

Important Note: Do not apply filter if you want to synchronize all.

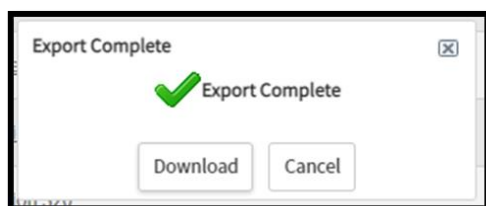
4. Mark the checkboxes to select Assets(s) that you want to synchronize with LDI platform.



5. Right-click the **Export** tab. A side menu appears. In the context menu, choose **Export** → **CSV**.



6. Select the type of format of the file to be exported. For example, CSV.



7. Click **Download**. The file is downloaded on the device.

The format of the ServiceNow file is:

```
"name","model_id","serial_number"
```

```
"EPUAKYIW0FCA","HP HP EliteBook 850 G7 Notebook PC","5CG1092PLB"
```

```
DEVICE NAME, MACHINE TYPE, SERIAL NUMBER, GROUP
```

```
EPUAKYIW0FCA, HP EliteBook 850 G7 Notebook PC,5CG1092PLB,
```

```
EPBYMINW150E,HP EliteBook 850 G7 Notebook PC,5CG1092PMP,Office1
```

5.16.6 Mandatory Requirements for LDI CSV Format

If the name of a device in LDI and ServiceNow is different, then the device name can be changed automatically using the CSV file.

Important Notes:

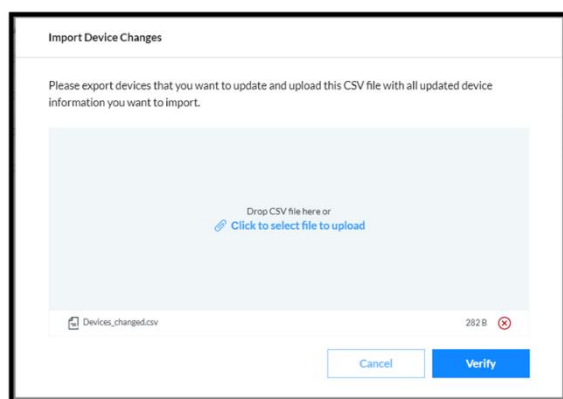
- Only underscore (_) and dash (-) symbols are allowed.
- To upgrade DEVICE NAME automatically, MACHINE TYPE must be model_id, and SERIAL NUMBER must be equal to serial_number.

5.16.7 Update Asset Information from ServiceNow to LDI Account

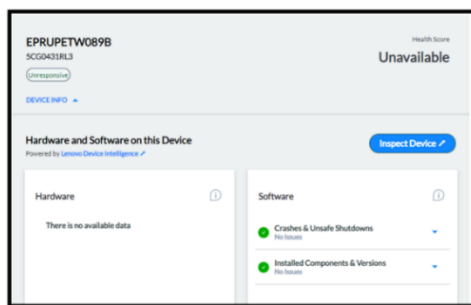
1. Log in to LDI account.
2. Click **Devices** in the navigation menu. The **Devices** pane appears.

3. Click **More**. The drop-down window appears.

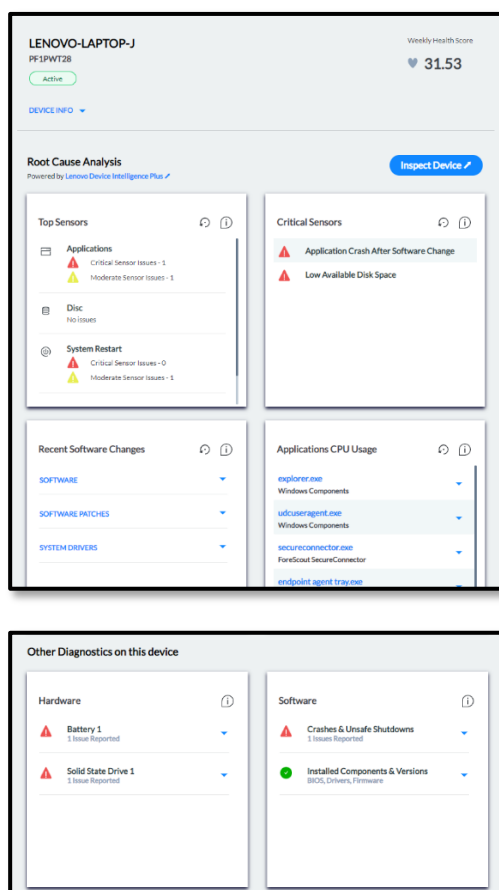
4. Click **Import Device Changes**.



5. Select the file. For example, the CSV file of Assets exported from ServiceNow.
6. Click **Verify**. The file is verified.



7. Click **Yes**. The device information is updated in LDI, and you receive a confirmation email at your registered email ID. ServiceNow receives data of specific device(s) and renders it in the Plugin tab. The LDI ServiceNow plugin is set up.



5.16.8 Integrate ServiceNow into LDI Tool

This feature allows the system to raise a ticket and assign it to the LDI Support team when an incident occurs. It includes tasks such as configuring connection to ServiceNow portal, creating rules that includes sensor management, etc.

Communication between servicenow-integration-service and ServiceNow API occurs using basic authentication. Thus, ServiceNow user credentials are stored in the servicenow-integration-service database and provided each time the API is called.

There is a possibility to use a more secure mechanism - OAuth authentication, when a limited-time token is obtained from OAuth API by credentials and is used in the API calls.

Follow this procedure to support the OAuth authentication:

1. Log in to the ServiceNow portal.
2. Fill-in **Instance URL**.
3. Enter the values for these fields:
 - User ID or Admin Credentials
 - Password
 - Client ID
 - Client Secret

Note:

- The Organization Admin must create a user in ServiceNow for User ID and Password and a client for Client ID and Client Secret.
 - The roles must be specified: Admin, Asset, App_service_user, etc. With this set of roles, there is an issue with setting high impact and urgency through the API. When High is requested, Medium is set in the incident.
4. Click **Connect to ServiceNow**. All the filled-in credentials are stores in the database afterward. This way it's possible to receive tokens whenever it's needed.
- Note:** This option requires saving user and password, but this user can be controlled at ServiceNow side.





Note: You must have an LDI Admin access privileges to configure and create a rule.


1. Log in to LDI portal.
 2. Select **Configuration → Insights & Automations → ServiceNow Incident Rules**. The **SNOW Incident Rules** page appears.
 3. Click the **Config Status** drop-down on top-right in the page.
 4. Select **Edit Configuration**. The **Configure Connection to ServiceNow** page appears.
 5. In the **Add Instance Credentials** section, enter the ServiceNow Instance URL, ServiceNow User ID, and ServiceNow Password.
 6. In the **Add Client Credentials** section, enter the ServiceNow Client ID and ServiceNow Client Secret.
- Note:** All are mandatory fields.
7. Click **Connect ServiceNow**.

5.16.9 Create a ServiceNow Incident Rule


Note: You need to configure ServiceNow in LDI before creating an incident rule. Refer to [Integrate ServiceNow Into LDI Tool](#) for more details.

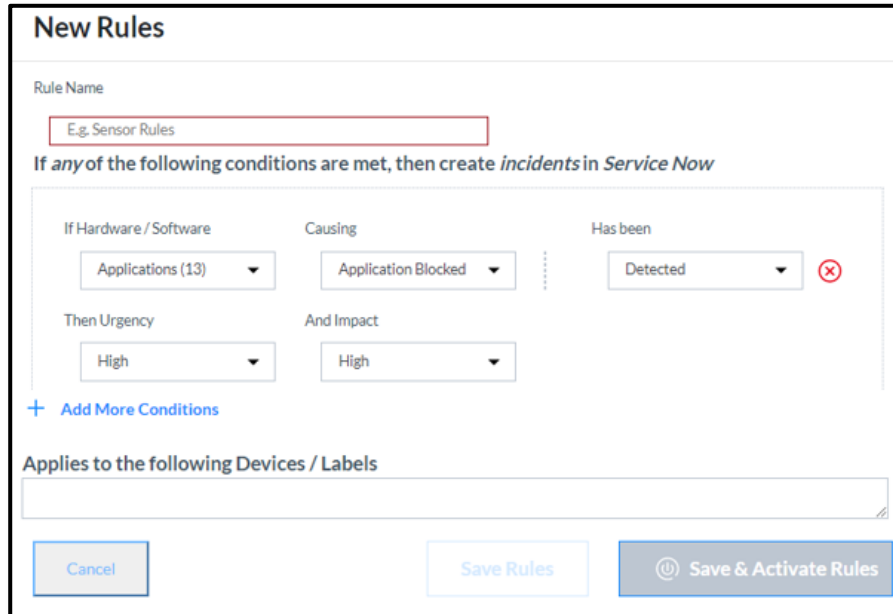
The following table displays the fields in the SNOW Incident Rules page:

Field Name	Field Description
Rule Name	The Name of the ServiceNow rule.
Activities Synced	The activities logged by LDI automation. Activities synced displays the number of incidents created when this rule is applied. When the rule is deactivated, this field is not updated.
Actions	<ul style="list-style-type: none">• Click the  icon to edit a rule.• Click the  icon to activate a rule.• Click the  icon to deactivate a rule.• Click the  icon to delete a rule.

Note: You can also click the  Show Active Rules toggle button on top of the page to display all the active rules for the ServiceNow devices.

To create a rule:

1. In the **SNOW Incident Rules** page, click the  icon. The **New Rules** page appears.
2. Enter the name you want to give to a new rule.
3. Select the conditions from the dropdowns.



4. Enter the device name or label to which the new rule is applicable.
5. Click **Save Rules**.

5.16.10 Handle an Incident in ServiceNow

The following page displays all the related details of an event created due to occurrence of an incident.

5.

The screenshot displays the 'Incident' management interface for incident INC0010688. The interface is divided into several sections for data entry and viewing.

Header: Incident INC0010688. Action buttons: Follow, Update, Resolve, Update LDI Diagnostics, Delete.

Form Fields:

- Number:** INC0010688
- Caller:** LDI Platform
- Category:** Inquiry / Help
- Subcategory:** -- None --
- Service:** (empty)
- Service offering:** (empty)
- Configuration Item:** EPRUPETW089B
- Contact type:** -- None --
- State:** New
- Impact:** 1 - High
- Urgency:** 2 - Medium
- Priority:** 2 - High
- Assignment group:** (empty)
- Assigned to:** Recent selections, Hardware
- Short description:** 2: Application Crash After Software Change, Major Latency Issues
- Description:**

The following 2 sensors have been triggered in 1 sensor categories by Lenovo Device Intelligence Automation.

Sensor: Application Crash After Software Change
Severity: 7
Triggered: 1 time(s)
Details:
APPNAME : OPSWATClientUI.exe
FLTCOUNT : 2.0
LS_ID : APPNAME-OPSWATClientUI.exe
MOD_DATE : 1.648722124E9

Sensor: Major Latency Issues
Severity: 8

Note: When you create an incident, the details are updated in the **LDI Diagnostics** tab. You can see this tab at the bottom of page. This tab helps you to take appropriate actions.

6 Appendix

6.1 Remediation Scripts Help

LDI provides you the following out-of-the-box scripts to get you started.

Script Category	Script Name	Help
Citrix Service Actions	Service_Enable_Citrix_AD_Identity	Enables the Citrix AD Identity Service
Citrix Service Actions	Service_Enable_Citrix_Broker	Enables the Citrix Broker Service
Citrix Service Actions	Service_Enable_Citrix_CDF	Enables the Citrix CDF Service
Citrix Service Actions	Service_Enable_Citrix_Configuration	Enables the Citrix Configuration Service
Citrix Service Actions	Service_Enable_Citrix_Credential_Wallet	Enables the Citrix Credential Wallet Service
Citrix Service Actions	Service_Enable_Citrix_Desktop_Service	Enables the Citrix Desktop Service
Citrix Service Actions	Service_Enable_Citrix_Device_Redirector	Enables the Citrix Device Redirector Service

Citrix Service Actions	Service_Enable_Citrix_Encryption_Service	Enables the Citrix Encryption Service
Citrix Service Actions	Service_Enable_Citrix_EUEM	Enables the Citrix EUEM Service
Citrix Service Actions	Service_Enable_Citrix_Group_Policy_Engine	Enables the Citrix Group Policy Engine Service
Citrix Service Actions	Service_Enable_Citrix_Host	Enables the Citrix Host Service
Citrix Service Actions	Service_Enable_Citrix_Location_and_Sensor_Virtual_Channel	Enables the Citrix Location and Sensor Virtual Channel Service
Citrix Service Actions	Service_Enable_Citrix_Machine_Creation	Enables the Citrix Machine Creation Service
Citrix Service Actions	Service_Enable_Citrix_MultiTouch_Redirection	Enables the Citrix MultiTouch Redirection Service
Citrix Service Actions	Service_Enable_Citrix_Personal_vDisk	Enables the Citrix Personal vDisk Service
Citrix Service Actions	Service_Enable_Citrix_Print_Manager	Enables the Citrix Print Manager Service
Citrix Service Actions	Service_Enable_Citrix_Profile_Management	Enables the Citrix Profile Management Service
Citrix Service Actions	Service_Enable_Citrix_PVS_2StageBoot	Enables the Citrix PVS 2StageBoot Service
Citrix Service Actions	Service_Enable_Citrix_PVS_API	Enables the Citrix PVS API Service
Citrix Service Actions	Service_Enable_Citrix_PVS_BNPXE	Enables the Citrix PVS BNPXE Service

Citrix Service Actions	Service_Enable_Citrix_PVS_BNTFTP	Enables the Citrix PVS BNTFTP Service
Citrix Service Actions	Service_Enable_Citrix_PVS_BOOTP	Enables the Citrix PVS BOOTP Service
Citrix Service Actions	Service_Enable_Citrix_Pvs_for_VMs_Agent	Enables the Citrix Pvs for VMs Agent Service
Citrix Service Actions	Service_Enable_Citrix_PVS_Soap	Enables the Citrix PVS Soap Service
Citrix Service Actions	Service_Enable_Citrix_PVS_Stream	Enables the Citrix PVS Stream Service
Citrix Service Actions	Service_Enable_Citrix_Services_Manager	Enables the Citrix Services Manager Service
Citrix Service Actions	Service_Enable_Citrix_Smart_Card	Enables the Citrix Smart Card Service
Citrix Service Actions	Service_Enable_Citrix_Stack_Control	Enables the Citrix Stack Control Service
Citrix Service Actions	Service_Enable_Citrix_Storefront	Enables the Citrix Storefront Service
Citrix Service Actions	Service_Enable_Citrix_Telemetry	Enables the Citrix Telemetry Service
Citrix Service Actions	Service_Enable_HDX_MediaStream	Enables the Citrix HDX MediaStream Service
Citrix Service Actions	Service_Restart_Citrix_Configuration	Restarts the Citrix Configuration Service
Citrix Service Actions	Service_Restart_Citrix_Credential_Wallet	Restarts the Citrix Credential Wallet Service
Citrix Service Actions	Service_Restart_Citrix_Desktop_Service	Restarts the Citrix Desktop Service

Citrix Service Actions	Service_Restart_Citrix_Device_Redirector	Restarts the Citrix Device Redirector Service
Citrix Service Actions	Service_Restart_Citrix_Encryption_Service	Restarts the Citrix Encryption Service
Citrix Service Actions	Service_Restart_Citrix_EUEM	Restarts the Citrix EUEM Service
Citrix Service Actions	Service_Restart_Citrix_Group_Policy_Engine	Restarts the Citrix Group Policy Engine Service
Citrix Service Actions	Service_Restart_Citrix_Host	Restarts the Citrix Host Service
Citrix Service Actions	Service_Restart_Citrix_Location_and_Sensor_Virtual_Channel	Restarts the Citrix Location and Sensor Virtual Channel Service
Citrix Service Actions	Service_Restart_Citrix_Machine_Creation	Restarts the Citrix Machine Creation Service
Citrix Service Actions	Service_Restart_Citrix_Mobile_Receiver_Virtual_Channel	Restarts the Citrix Mobile Receiver Virtual Channel Service
Citrix Service Actions	Service_Restart_Citrix_MultiTouch_Redirection	Restarts the Citrix MultiTouch Redirection Service
Citrix Service Actions	Service_Restart_Citrix_Personal_vDisk	Restarts the Citrix Personal vDisk Service
Citrix Service Actions	Service_Restart_Citrix_Print_Manager	Restarts the Citrix Print Manager Service
Citrix Service Actions	Service_Restart_Citrix_Profile_Management	Restarts the Citrix Profile Management Service
Citrix Service Actions	Service_Restart_Citrix_PVS_2StageBoot	Restarts the Citrix PVS 2StageBoot Service

Citrix Service Actions	Service_Restart_Citrix_PVS_API	Restarts the Citrix PVS API Service
Citrix Service Actions	Service_Restart_Citrix_PVS_BNPXE	Restarts the Citrix PVS BNPXE Service
Citrix Service Actions	Service_Restart_Citrix_PVS_BNTFTP	Restarts the Citrix PVS BNTFTP Service
Citrix Service Actions	Service_Restart_Citrix_PVS_BOOTP	Restarts the Citrix_PVS_BOOTP Service
Citrix Service Actions	Service_Restart_Citrix_Pvs_for_VMs_Agent	Restarts the Citrix Pvs for VMs Agent Service
Citrix Service Actions	Service_Restart_Citrix_PVS_Soap	Restarts the Citrix PVS Soap Service
Citrix Service Actions	Service_Restart_Citrix_PVS_Stream	Restarts the Citrix PVS Stream Service
Citrix Service Actions	Service_Restart_Citrix_Services_Manager	Restarts the Citrix Services Manager Service
Citrix Service Actions	Service_Restart_Citrix_Smart_Card	Restarts the Citrix Smart Card Service
Citrix Service Actions	Service_Restart_Citrix_Stack_Control	Restarts the Citrix Stack Control Service
Citrix Service Actions	Service_Restart_Citrix_Storefront	Restarts the Citrix Storefront Service
Citrix Service Actions	Service_Restart_Citrix_Telemetry	Restarts the Citrix Telemetry Service
Citrix Service Actions	Service_Restart_HDX_MediaStream	Restarts the Citrix HDX MediaStream Service

Device Configuration Actions	DongleMeteredConnectionSet2Off	This script is used to set DongleOrAny Wireless with meteredconnection property to off
Device Configuration Actions	fixDNSCache	This script will fix the DNS Cache
Device Configuration Actions	GPUpdate-Computer	Runs a computer Group Policy Update with force parameter - run this as the System
Device Configuration Actions	GPUpdate-Full	Runs a full Group Policy Update with force parameter - run this as the System
Device Configuration Actions	GPUpdate-User	Runs a user Group Policy Update with force parameter - run this as the user
Device Configuration Actions	ReRunLogonScript	Finds the location of the user's login script and runs it again if available
Device Configuration Actions	SystemFileCheck	Scans the integrity of all protected system files and repairs files problems when possible - run this as system
Microsoft Office Actions	ClearCachedOfficeCredentials	Clears the cached credentials for Office using the cmdkey command and matching credentials with MicrosoftOffice16_Data in the name - run this as the User
Microsoft Office Actions	ClearSkypeCachePassword	Removes skype cached password

Microsoft Office Actions	ClearSkypeforBusinessCache	Clears the Skype for Business Cache - run as the user
Microsoft Office Actions	DisableOutlookAutoComplete	Disables outlook auto complete
Microsoft Office Actions	Enable_OutlookSearch	Enables outlook search
Microsoft Office Actions	Excel_Enable_All_Macros	Changes the users registry value to enable all macros in Excel updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	Excel_Enable_Developer_Tools	Changes the users registry value to enable the developer tools in Excel updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Options - DeveloperTools for the user - run this as the user
Microsoft Office Actions	Excel_Enable_Signed_Macros	Changes the users registry value to enable signed macros in Excel updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	Office16ClearDocCache	Clears the Office 16 Document cache - run as the user
Microsoft Office Actions	Office16SetClearDocCacheOnExit	Sets the Office 16 Document cache to be cleared on document closure - runs as the user

Microsoft Office Actions	OneDriveReset	Resets Microsoft OneDrive this can sometimes resolve sync issues and resets all OneDrive settings. OneDrive performs a full sync after the reset. You won't lose any data by resetting OneDrive. - runs this as the user
Microsoft Office Actions	OST_RemoveUserProfileGT60	Removes 60 days old ost file from profile
Microsoft Office Actions	OST_RepairRemoveRestartOutlook	Removes problemOrtroubled ost file and restart the outlook
Microsoft Office Actions	PowerPoint_Enable_All_Macros	Changes the users registry value to enable all macros in PowerPoint updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	PowerPoint_Enable_Developer_Tools	Changes the users registry value to enable the developer tools in PowerPoint updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Options - DeveloperTools for the user - run this as the user
Microsoft Office Actions	PowerPoint_Enable_Signed_Macros	Changes the users registry value to enable signed macros in PowerPoint updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\PowerPoint\Security:vbawarnings for the user - run this as the user
Microsoft Office Actions	WindowsDefenderFullScan	Runs a Windows Defender Full Scan

Microsoft Office Actions	WindowsDefenderQuickScan	Runs a Windows Defender Quick Scan
Microsoft Office Actions	WindowsDefenderUpdateDefinitions	Updates the Windows Defender Signatures - this can be useful in troubleshootoing - run as the System
Microsoft Office Actions	WindowsHardwareDiagnostic	Runs the Windows Hardware Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsInternetDiagnostic	Runs the Windows Internet Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsNetworkDiagnostic	Runs the Windows Network Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsPrinterDiagnostic	Runs the Windows Printer Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsUpdateDiagnostic	Runs the Windows Update Diagnostic wizard - run this as the user
Microsoft Office Actions	WindowsUpdateResetDownloadFolders	Stops the Windows update services and renames the download folders then restarts the services - run this as the system
Microsoft Office Actions	Word_Enable_All_Macros	Changes the users registry value to enable all macros in Word updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security:vbawarnings for the user - run this as the user

Microsoft Office Actions	Word_Enable_Developer_Tools	Changes the users registry value to enable the developer tools in Word updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Options - DeveloperTools for the user. This action needs to be run this as the user.
Microsoft Office Actions	Word_Enable_Signed_Macros	Changes the users registry value to enable signed macros in Word updates HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security:vbawarnings for the user. This action needs to be run this as the user.
Microsoft SCCM Actions	SCCM-Agent-repair	Runs the SCCM Agent repair program.
Microsoft SCCM Actions	SCCM-Agent-restart	Runs the SCCM Agent restart program.
Microsoft SCCM Actions	SCCM-ClearCache	Clears the SCCM Agent cache by default this is the directory %windir%\ccmcache
Microsoft SCCM Actions	SCCM-Client-AppDeployEvalCycle	Trigger an SCCM Client Application Deployment Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-DiscoveryDataCollectionCycle	Triggers an SCCM Client Discovery Data Collection Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-FileCollectionCycle	Triggers an SCCM Client File Collection Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-HardwareInventoryCycle	Triggers an SCCM Hardware Inventory Cycle - run this as system

Microsoft SCCM Actions	SCCM-Client-MachinePolicyEvaluationCycle	Triggers an SCCM Machine Policy Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-MachinePolicyRetrievalCycle	Triggers an SCCM Machine Policy Retrieval Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SftwrMeteringRptCycle	Triggers an SCCM Software Metering Usage Report Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SftwrUpdateAssgnmtEval	Triggers an SCCM Software Updates Assignments Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SoftwareInventoryCycle	Triggers an SCCM Software Inventory Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-SoftwareUpdateScanCycle	Triggers an SCCM Software Update Scan Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-StateMessageRefresh	Triggers an SCCM State Message Refresh - run this as system
Microsoft SCCM Actions	SCCM-Client-UserPolicyEvaluationCycle	Triggers an SCCM User Policy Evaluation Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-UserPolicyRetrievalCycle	Triggers an SCCM User Policy Retrieval Cycle - run this as system
Microsoft SCCM Actions	SCCM-Client-WindowsSrcListUpdate	Triggers an SCCM Windows Installers Source List Update Cycle - run this as system

Microsoft SCCM Actions	SCCM-Set-Site	Changes the local machine registry value to update the SCCM site updates HKLM\SOFTWARE\Microsoft\CCM\CcmEval:LastSiteCode HKLM\SOFTWARE\Microsoft\SMS\DP:SiteCode and HKLM\SOFTWARE\Microsoft\SMS\MobileClient:AssignedSiteCode
Remote Sessions Actions	Service_Enable_HDX_MediaStream	Enables the Citrix HDX MediaStream Service
Remote Sessions Actions	Service_Restart_HDX_MediaStream	Restarts the Citrix HDX MediaStream Service
Remote Work Actions	Service_Enable_Zoom_Sharing	Enables the Zoom Sharing Service
Remote Work Actions	Service_Restart_Zoom_Sharing	Restarts the Zoom Sharing Service
Security Actions	Service_Enable_1EClient	Enables the 1E Client Service
Security Actions	Service_Enable_Bitlocker	Enables the Bitlocker Service
Security Actions	Service_Enable_Cisco_acumbrella	Enables the Cisco acumbrellaagent Service
Security Actions	Service_Enable_Cisco_Umbrella	Enables the Cisco Umbrella_RC Service
Security Actions	Service_Enable_ClearPass_Agent	Enables the ClearPass Agent Controller Service
Security Actions	Service_Enable_ClearPass_OnGuard	Enables the ClearPass OnGuard Agent Service

Security Actions	Service_Enable_CrowdStrikeFalcon	Enables the CrowdStrike Falcon Service
Security Actions	Service_Enable_DefenderATP	Enables the Windows Defender ATP Service
Security Actions	Service_Enable_Defender_Firewall	Enables the Windows Defender Firewall Service
Security Actions	Service_Enable_Defender_NIS	Enables the Windows Defender Antivirus Network Inspection Service
Security Actions	Service_Enable_FortiClient_VPN	Enables the Fortinet SslvpnDaemon Service
Security Actions	Service_Enable_iDAppsService	Enables the iDAppsService Service
Security Actions	Service_Enable_McAfeeFramework	Enables the McAfee Agent Backwards Compatibility Service
Security Actions	Service_Enable_McAfee_AgentService	Enables the McAfee Agent Service
Security Actions	Service_Enable_McAfee_macmnsvc	Enables the McAfee Agent Common Services Service
Security Actions	Service_Enable_NomadBranch	Enables the NomadBranch Service
Security Actions	Service_Enable_Symantec_Broker	Enables the Symantec Privilege Broker Service
Security Actions	Service_Enable_Symantec_EP	Enables the Symantec Endpoint Protection Service
Security Actions	Service_Enable_Symantec_EPLP	Enables the Symantec Endpoint Protection Local Proxy Service

Security Actions	Service_Enable_Symantec_EPWSC	Enables the Symantec Endpoint Protection WSC Service
Security Actions	Service_Enable_Symantec_IDS	Enables the Symantec IDS Service
Security Actions	Service_Enable_Symantec_IPS	Enables the Symantec IPS Service
Security Actions	Service_Enable_Symantec_Util	Enables the Symantec Util Service
Security Actions	Service_Enable_Tanium_Client	Enables the Tanium Client Service
Security Actions	Service_Enable_Trend_CCSF	Enables the Trend Micro Common Client Solution Framework Service
Security Actions	Service_Enable_Trend_Firewall	Enables the Trend Micro Security Agent Firewall Service
Security Actions	Service_Enable_Trend_Listener	Enables the Trend Micro Security Agent Listener Service
Security Actions	Service_Enable_Trend_NTRTScan	Enables the Trend Micro Security Agent Real-time Scan Service
Security Actions	Service_Enable_Trend_TMBM	Enables the Trend Micro Unauthorized Change Prevention Service
Security Actions	Service_Restart_1EClient	Restarts the 1E Client Service
Security Actions	Service_Restart_Bitlocker	Restarts the Bitlocker Service

Security Actions	Service_Restart_Cisco_acumbrella	Restarts the Cisco acumbrellaagent Service
Security Actions	Service_Restart_Cisco_Umbrella	Restarts the Cisco Umbrella_RC Service
Security Actions	Service_Restart_ClearPass_Agent	Restarts the ClearPass Agent Controller Service
Security Actions	Service_Restart_ClearPass_OnGuard	Restarts the ClearPass OnGuard Agent Service
Security Actions	Service_Restart_CrowdStrikeFalcon	Restarts the CrowdStrike Falcon Service
Security Actions	Service_Restart_DefenderATP	Restarts the Windows Defender ATP Service
Security Actions	Service_Restart_Defender_Firewall	Restarts the Windows Defender Firewall Service
Security Actions	Service_Restart_Defender_NIS	Restarts the Windows Defender Antivirus Network Inspection Service
Security Actions	Service_Restart_iDAppsService	Restarts the iDAppsService Service
Security Actions	Service_Restart_McAfeeFramework	Restarts the McAfee Agent Backwards Compatibility Service
Security Actions	Service_Restart_McAfee_AgentService	Restarts the McAfee Agent Service
Security Actions	Service_Restart_McAfee_macmnsvc	Restarts the McAfee Agent Common Services Service
Security Actions	Service_Restart_NomadBranch	Restarts the NomadBranch Service

Security Actions	Service_Restart_Symantec_Broker	Restarts the Symantec Privilege Broker Service
Security Actions	Service_Restart_Symantec_EP	Restarts the Symantec Endpoint Protection Service
Security Actions	Service_Restart_Symantec_EPLP	Restarts the Symantec Endpoint Protection Local Proxy Service
Security Actions	Service_Restart_Symantec_EPWSC	Restarts the Symantec Endpoint Protection WSC Service
Security Actions	Service_Restart_Symantec_IDS	Restarts the Symantec IDS Service
Security Actions	Service_Restart_Symantec_IPS	Restarts the Symantec IPS Service
Security Actions	Service_Restart_Symantec_Util	Restarts the Symantec Util Service
Security Actions	Service_Restart_Tanium_Client	Restarts the Tanium Client Service
Security Actions	Service_Restart_Trend_CCSF	Restarts the Trend Micro Common Client Solution Framework Service
Security Actions	Service_Restart_Trend_Firewall	Restarts the Trend Micro Security Agent Firewall Service
Security Actions	Service_Restart_Trend_Listener	Restarts the Trend Micro Security Agent Listener Service
Security Actions	Service_Restart_Trend_NTRTScan	Restarts the Trend Micro Security Agent Real-time Scan Service

Security Actions	Service_Restart_Trend_TMBM	Restarts the Trend Micro Unauthorized Change Prevention Service
Sensor Actions	Disk Cleanup	Cleans the C: drive's Window Temporary Internet Files for all users and empties the recycling bin.
Sensor Actions	Rebuild WMI	<p>Goes through the recommended WMI rebuild actions as described by Microsoft. If no parameter is passed, the script defaults to its Alarm only setting and a log is generated in the location the script is run.</p> <p>Note: This script restarts the WMI service as part of its operation. This results in a service that depends on WMI restarting which as well can result in problems such as VDI session disconnects.</p>
Sensor Actions	Restart Base Filtering Service	Restarts the Base Filtering Service, which is responsible for managing firewall and IPSec policies and user mode filtering.
Sensor Actions	Restart Computer	Restarts the computer.
Sensor Actions	Restart Cryptographic Service	Restarts the Cryptographic Service which controls the certificates that are trusted as well as confirming the signatures of Windows files.
Sensor Actions	Restart DCOM Service	Restarts the DCOM Service which controls the launch of COM and DCOM servers in response to object activation requests.

Sensor Actions	Restart DHCP Service	Restarts the DHCP Service which registers and updates IP addresses and DNS records for the computer.
Sensor Actions	Restart DNS Client Service	Restarts the DNS Client Service which cache DNS names and registers the full name for the computer.
Sensor Actions	Restart Event Broker Service	Restarts the Event Broker Service which coordinates the execution of background work for WinRT applications.
Sensor Actions	Restart LAN Manager Service	Restarts the LAN Manager Service which creates and maintains connections to remote servers.
Sensor Actions	Restart Local Session Manager Service	Restarts the Local Session Manager Service which manages local user sessions.
Sensor Actions	Restart Netlogon Service	Restarts the Netlogon Service which maintains a secure channel to the domain controller for authentication.
Sensor Actions	Restart NIC	Restarts the Network Adapters on the system.
Sensor Actions	Restart NLA Service	Restarts the NLA Service which collects and stores configuration information for the network.
Sensor Actions	Restart Plug and Play Service	Restarts the Plug and Play Service which enables the computer to recognize and adapt to hardware changes.

Sensor Actions	Restart Printer Spooler Service	Restarts the Printer Spooler Service which spools print jobs and handles interactions with the printer.
----------------	---------------------------------	---

Appendix

6.2 Device Support Matrix

6.2.1 LDI OEM and OS Support Matrix

Module	Sub-Module	Win10 & 11		Manufacturer				
				Agnostic	Lenovo	HP	Dell	MS Surface
Reports	BSOD Crashes	X			X	X		X
	AppPerformance	X		X				
	Batteries	X			X			
	Storage Drives	X			X	*NVMe	*NVMe	*NVMe
	Available Updates	X			X			
Device Manager	Devices	X		X				
Device Lookup	Device Lookup	X			X	X	X	X

6.3 Windows Device Manager Module Error Codes

The following error codes are sourced from Microsoft and used in relation to Microsoft's Windows Device Manager.

Code 1 "This device is not configured correctly. (Code 1)"

Cause

The device has no drivers installed on your computer, or the drivers are configured incorrectly.

Recommended Resolution

Update the Driver

In the device's **Properties** dialog box, click the **Driver** tab, and then click **Update Driver** to start the **Hardware Update Wizard**. Follow the instructions to update the driver. If updating the driver does not work, see your hardware documentation for more information.

Note: You may be prompted to provide the path of the driver. Windows may have the driver built-in or may still have the driver files installed from the last time that you set up the device. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 3 "The driver for this device might be corrupted... (Code 3)"

Full error message

"The driver for this device might be corrupted, or your system may be running low on memory or other resources. (Code 3)"

Cause

The device driver may be corrupted, or you are running out of memory; the system is running low on system memory and may need to free up or add more memory.

Recommended Resolutions

Close some open applications

If the computer has insufficient memory to run the device, you can close some applications to make memory available. You can also check memory and system resources, and the virtual memory settings.

- To check memory and system resources, open Task Manager. To do this, press CTRL+ALT+DELETE, and then click **Task Manager**.
- To check virtual memory settings, open the **System Properties** dialog box, click the **Advanced** tab, and then click **Settings** in the **Performance** area.

Uninstall and reinstall the driver

The device driver may have become corrupted. Uninstall the driver from Device Manager and scan for new hardware to install the driver again.

1. In the device's **Properties** dialog box, click the **Driver** tab, and then click **Uninstall**. Follow the instructions.
2. Restart your computer.
3. Open Device Manager, click **Action**, and then click **Scan for hardware changes**. Follow the instructions.

Note You may be prompted to provide the path of the driver. Windows may have the driver built-in or may still have the driver files installed from the last time that you set up the device. However, sometimes, it will open the New Hardware Wizard which may ask for the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Install additional RAM

You may have to install additional random-access memory (RAM).

Code 9 “Windows cannot identify this hardware... (Code 9)”

Full error message

"Windows cannot identify this hardware because it does not have a valid hardware identification number. For assistance, contact the hardware manufacturer. (Code 9)"

Cause

Invalid device IDs for your hardware have been detected by your PC.

Recommended Resolutions

Contact the hardware vendor. The hardware or the driver is defective.

Code 10 "This device cannot start. (Code 10)"

Full Error Message

"This device cannot start. Try upgrading the device drivers for this device. (Code 10)"

Cause

Typically, the device's hardware key contains a "FailReasonString" value, and the value string is displaying an error message defined by the hardware manufacturer. If the hardware key does not contain a "FailReasonString" value, the message above is displayed.

Recommended resolutions

Update the driver

In the device's **Properties** dialog box, click the **Driver** tab, and then click **Update Driver** to start the Hardware Update Wizard. Follow the instructions to update the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 12 "This device cannot find enough free resources that it can use... (Code 12) "

Full Error Message

This device cannot find enough free resources that it can use. If you want to use this device, you will need to disable one of the other devices on this system. (Code 12)

Cause

This error can occur if two devices that are installed on your computer have been assigned the same I/O ports, the same interrupt, or the same Direct Memory Access channel (either by the BIOS, the operating system, or both). This error message can also appear if the BIOS did not allocate enough resources to the device.

Recommended Resolution

Windows Vista and later versions of Windows

Use Device Manager to determine the source of and to resolve the conflict. For more information about how to resolve device conflicts, see the Help information about how to use Device Manager. This error message can also appear if the BIOS did not allocate sufficient resources to a device. For example, this message will display if the BIOS does not allocate an interrupt to a USB controller because of an invalid multiprocessor specification (MPS) table.

Windows Server 2003, Windows XP, and Windows 2000

1. Open Device Manager.
2. Double-click the icon that represents the device in the Device Manager window.
3. On the device property sheet that appears, click Troubleshoot to start the hardware trouble-shooter for the device.

This error message can also appear if the BIOS did not allocate sufficient resources to a device. For example, this message will be displayed if the BIOS does not allocate an interrupt to a USB controller because of an invalid multiprocessor specification (MPS) table.

Code 14 "This device cannot work properly until you restart your computer. (Code 14)"

Full Error Message

"This device cannot work properly until you restart your computer. To restart your computer now, click Restart Computer. (Code 14)"

Recommended Resolution

Restart your computer. From Start, click **Shut Down**, and then select **Restart**.

Code 16 "Windows cannot identify all the resources this device uses. (Code 16)"

Full Error Message

"Windows cannot identify all the resources this device uses. To specify additional resources for this device, click the Resources tab and fill in the missing settings. Check your hardware documentation to find out what settings to use. (Code 16)"

Cause

The device is only partly configured and might need additional manual configuration of the resources the device requires.

Recommended Resolution

The following steps might only work if the device is a Plug and Play device. If the device is not Plug and Play, you can refer to the device documentation or contact the device manufacturer for more information.

1. From Start, search for **device manager** and select Device Manager from the results.
2. Double-click the device in the list, and choose the **Resources** tab.
3. In the **Resource Settings** list, check to see if there is a question mark next to a resource. If so, select that resource, and assign it to the device.
4. If a resource cannot be changed, click **Change Settings**. If **Change Settings** is unavailable, try to clear the **Use automatic settings** check box to make it available.

Code 18 "Reinstall the drivers for this device. (Code 18)"

Reinstall the device driver using the Hardware Update wizard

1. From Start, search for **device manager** and select Device Manager from the results.

2. Right-click the device in the list.
3. On the menu that appears, choose **Update Driver** to start the Hardware Update wizard.

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 19 "Windows cannot start this hardware device... (Code 19)"

Full Error Message

Windows cannot start this hardware device because its configuration information (in the registry) is incomplete or damaged. (Code 19)

Cause

This error can result if more than one service is defined for a device, there is a failure opening the service key, or the driver's name cannot be obtained from the service key.

Recommended Resolution

Uninstall and reinstall the driver

1. From Start, search for **device manager** and select Device Manager from the results.

2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select Scan for hardware changes to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Revert to the most recent successful registry configuration

To roll a system back to the most recent successful configuration of the registry, you can restart the computer in Safe Mode and select the Last Known Good Configuration option, or if you've created a system restore point, you can try restoring to it.

[Recovery options in Windows 10](#)

[Backup and restore your PC](#) (Windows 8.1)

[What are the system recovery options in Windows?](#) (Windows 7)

Code 21 "Windows is removing this device...(Code 21)"

Full Error Message

Windows is removing this device. (Code 21)

Cause

This error means that Windows is in the process of removing the device. However, the device has not yet been completely removed. This error code is temporary and exists only during the attempts to query and then remove a device.

Recommended Resolutions

You can either wait for Windows to finish removing the device or restart the computer.

1. Wait several seconds, and then press the F5 key to update the Device Manager view.
2. If that does not resolve the problem, restart your computer. Click Start, click **Shut Down**, and then select **Restart** in the **Shut Down Windows** dialog box to restart the computer.

Code 22 "This device is disabled. (Code 22)"

Cause

The device was disabled by the user in Device Manager.

Recommended Resolution

In Device Manager, click **Action**, and then click **Enable Device**. This starts the Enable Device wizard. Follow the instructions.

Code 24 "This device is not present, is not working properly... (Code 24)"

Full Error Message

This device is not present, is not working properly, or does not have all its drivers installed. (Code 24)

Cause

The device is installed incorrectly. The problem could be a hardware failure, or a new driver might be needed. Devices stay in this state if they have been prepared for removal. After you remove the device, this error disappears.

Recommended Resolution

Remove the device, and this error should be resolved.

Code 28 "The drivers for this device are not installed. (Code 28)"

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 29 "This device is disabled... (Code 29)"

Full Error Message

This device is disabled because the firmware of the device did not give it the required resources. (Code 29)

Recommended Resolution

Enable the device in the BIOS of the device. For information about how to make this change, see the hardware documentation or contact the manufacturer of your computer.

Code 31 "This device is not working properly... (Code 31)"

Full Error Message

This device is not working properly because Windows cannot load the drivers required for this device. (Code 31)

Recommended Resolution

Reinstall the device driver using the Hardware Update wizard

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. On the menu that appears, choose **Update Driver** to start the Hardware Update wizard.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 32 "A driver (service) for this device has been disabled. (Code 32)"

Full Error Message

A driver (service) for this device has been disabled. An alternate driver may be providing this functionality. (Code 32)

Cause

The start type for this driver is set to disabled in the registry.

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.

5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 33 "Windows cannot determine which resources are required for this device. (Code 33)"

Cause

The translator that determines the kinds of resources that are required by the device has failed.

Recommended Resolutions

1. Try using the BIOS setup utility or update the BIOS.
2. Configure, repair, or replace hardware.

Contact the device hardware vendor for more information about updating your BIOS and how to configure or replace the device.

Code 34 "Windows cannot determine the settings for this device... (Code 34)"

Full Error Message

Windows cannot determine the settings for this device. Consult the documentation that came with this device and use the Resource tab to set the configuration. (Code 34)

Recommended Resolution

The device requires manual configuration. See the hardware documentation or contact the hardware vendor for instructions on manually configuring the device. After you configure the device itself, you can use the **Resources** tab in Device Manager to configure the resource settings in Windows.

Code 35 “Your computer's system firmware does not... (Code 35)”

Full Error Message

Your computer's system firmware does not include enough information to properly configure and use this device. To use this device, contact your computer manufacturer to obtain a firmware or BIOS update. (Code 35)

Cause

The Multiprocessor System (MPS) table, which stores the resource assignments for the BIOS, is missing an entry for your device and must be updated.

Recommended Resolution

Contact the manufacturer of your computer to update the BIOS.

Code 36 “This device is requesting a PCI interrupt... (Code 36)”

Full Error Message

This device is requesting a PCI interrupt but is configured for an ISA interrupt (or vice versa). Please use the computer's system setup program to reconfigure the interrupt for this device. (Code 36)

Cause

The interrupt request (IRQ) translation failed.

Recommended Resolution

Change the settings for IRQ reservations in the BIOS.

For more information about how to change BIOS settings, see the hardware documentation or contact the manufacturer of your computer. You can also try to use the BIOS setup tool to change the settings for IRQ reservations (if such options exist). The BIOS might have options to reserve certain IRQs for peripheral component interconnect (PCI) or ISA devices.

Code 37 "Windows cannot initialize the device driver for this hardware. (Code 37)"

Cause

The driver returned a failure when it executed the DriverEntry routine.

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 38 "Windows cannot load the device driver... (Code 38)"

Full Error Message

Windows cannot load the device driver for this hardware because a previous instance of the device driver is still in memory. (Code 38)

Cause

The driver could not be loaded because a previous instance is still loaded.

Recommended Resolution

Restart your computer. From Start, click **Shut Down**, and then select **Restart**.

Code 39 “Windows cannot load the device driver for this hardware... (Code 39).”

Full Error Message

Windows cannot load the device driver for this hardware. The driver may be corrupted or missing. (Code 39)

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor’s website.

Code 40 “Windows cannot access this hardware... (Code 40)”

Full Error Message

Windows cannot access this hardware because its service key information in the registry is missing or recorded incorrectly. (Code 40)

Cause

Information in the registry's service subkey for the driver is invalid.

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 41 "Windows successfully loaded the device driver... (Code 41)"

Full Error Message

Windows successfully loaded the device driver for this hardware but cannot find the hardware device. (Code 41)

Cause

This problem occurs if you install a driver for a non-Plug and Play device, but Windows cannot find the device.

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.

3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 42 "Windows cannot load the device driver... (Code 42)"

Full Error Message

Windows cannot load the device driver for this hardware because there is a duplicate device already running in the system. (Code 42)

Cause

A duplicate device was detected. This error occurs when a bus driver incorrectly creates two identically named sub-processes (known as a bus driver error), or when a device with a serial number is discovered in a new location before it is removed from the old location.

Recommended Resolution

Restart your computer. From Start, click **Shut Down**, and then select **Restart**.

Code 43 "Windows has stopped this device because it has reported problems. (Code 43)"

Cause

One of the drivers controlling the device notified the operating system that the device failed in some manner.

Recommended Resolution

If you have already tried the "Try these steps first" section, check the hardware documentation or contact the manufacturer for more information about diagnosing the problem.

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 44 "An application or service has shut down this hardware device. (Code 44)"

Recommended Resolution

Restart your computer. From Start, click **Shut Down**, and then select **Restart**.

Code 45 "Currently, this hardware device is not connected to the computer... (Code 45)"

Full Error Message

Currently, this hardware device is not connected to the computer. To fix this problem, reconnect this hardware device to the computer. (Code 45)

Cause

This error occurs if a device that was previously connected to the computer is no longer connected. To resolve this problem, reconnect this hardware device to the computer.

Recommended Resolution

No resolution is necessary. This error code is only used to indicate the disconnected status of the device and does not require you to resolve it. The error code resolves automatically when you connect the associated device to the computer.

Code 46 “Windows cannot gain access to this hardware device... (Code 46)”

Full Error Message

Windows cannot gain access to this hardware device because the operating system is in the process of shutting down. The hardware device should work correctly next time you start your computer. (Code 46)

Cause

The device is not available because the system is shutting down.

Recommended Resolution

No resolution is necessary. The hardware device should work correctly next time that you start the computer. This error code is only set when **Driver Verifier** is enabled, and all applications have already been shut down.

Code 47 “Windows cannot use this hardware device... (Code 47)”

Full Error Message

Windows cannot use this hardware device because it has been prepared for safe removal, but it has not been removed from the computer. To fix this problem, unplug this device from your computer and then plug it in again. (Code 47)

Cause

This error code occurs only if you used the Safe Removal application to prepare the device for removal or pressed a physical eject button.

Recommended Resolution

Unplug the device from the computer, and then plug it back in. Restart your computer if that doesn't resolve the error. From Start, click **Shut Down**, and then select **Restart**.

Code 48 “The software for this device has been blocked... (Code 48).”

Full Error Message

The software for this device has been blocked from starting because it is known to have problems with Windows. Contact the hardware vendor for a new driver. (Code 48)

Recommended Resolution

Contact the manufacturer of your hardware device to obtain the latest version or the updated driver. Then, install it on your computer.

Code 49 “Windows cannot start new hardware devices... (Code 49).”

Full Error Message

Windows cannot start new hardware devices because the system hive is too large (exceeds the Registry Size Limit). (Code 49)

Cause

The system hive has exceeded its maximum size and new devices cannot work until the size is reduced. The system hive is a permanent part of the registry associated with a set of files that contains information related to the configuration of the computer on which the operating system is installed. Configured items include applications, user preferences, devices, and so on. The problem might be specific devices that are no longer attached to the computer but are still listed in the system hive.

Recommended Resolution

Uninstall any hardware devices that you are no longer using.

1. Set Device Manager to show devices that are no longer connected to the computer.
 - From Start, click **Run**.
 - In the Open box, type **cmd**. The Command Prompt window opens.
 - At the prompt, type the following command, and then press Enter: **set devmgr_show_nonpresent_devices=1**

2. In Device Manager, click **View**, and then click **Show hidden devices**. You will now be able to see devices that are not connected to the computer.
3. Select a non-present device. On the **Driver** tab, choose **Uninstall**.
4. Repeat step 3 for any non-present devices that you are no longer using. Then restart your computer.
5. Check the device Properties dialog box in Device Manager to see whether the error is resolved.

Code 50 "Windows cannot apply all of the properties for this device... (Code 50)"

Full Error Message

Windows cannot apply all of the properties for this device. Device properties may include information that describes the device's capabilities and settings (such as security settings for example). To fix this problem, you can try reinstalling this device. However, we recommend that you contact the hardware manufacturer for a new driver. (Code50)

Recommended Resolution

Reinstall the device driver manually

1. From Start, search for **device manager** and select Device Manager from the results.
2. Right-click the device in the list.
3. Select **Uninstall** from the menu that appears.
4. After the device is uninstalled, choose **Action** on the menu bar.
5. Select **Scan for hardware changes** to reinstall the driver.

Note You may be prompted to provide the path of the driver. If you are asked for the driver and you do not have it, you can try to download the latest driver from the hardware vendor's website.

Code 51 “This device is currently waiting on another device... (Code 51).”

Full Error Message

This device is currently waiting on another device or set of devices to start. (Code 51).

Recommended Resolution

There is currently no resolution to this problem. To help diagnose the problem, examine other failed devices in the device tree that this device might depend on. If you can determine why another related device did not start, you might be able to resolve this issue.

Code 52 “Windows cannot verify the digital signature for the drivers required for this device. (Code 52)”

Full Error Message

Windows cannot verify the digital signature for the drivers required for this device. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source. (Code 52)

Cause

The driver may be unsigned or corrupted.

Recommended Resolution

Download the latest driver from the hardware manufacturer's website or contact the manufacturer for help.

Code 53 “This device has been reserved for use by the Windows kernel debugger... (Code 53)”

Full Error Message

This device has been reserved for use by the Windows kernel debugger for the duration of this boot session. (Code 53)

Recommended Resolution

Disable Windows kernel debugging to allow the device to start normally.

Code 54 “This device has failed and is undergoing a reset. (Code 54)”

Cause

This is an intermittent problem code assigned while an ACPI reset method is being executed. If the device never restarts due to a failure, it will be stuck in this state and the system should be rebooted.

Recommended Resolution

Restart your computer. From Start, click **Shut Down**, and then select **Restart**.