Lenovo ThinkServer Operating System-based Platform Update Tool User Guide

ThinkServer

Version 1.1.9

First Edition (September 2014) Revision 1

Table of Contents

1. Introduction

This guide will provide instruction about how to use the features available in the **Lenovo ThinkServer Operating System-based Platform Update Tool (OSPUT)**.

The ThinkServer Operating System-based Platform Update Tool is a command line tool that allows administrators to update the firmware of the Lenovo ThinkServer components, such as TSM, BIOS and others from within the OS installed on the server's operating system.

The next sections will present all commands and options available in the OSPUT.

2. System Requirements

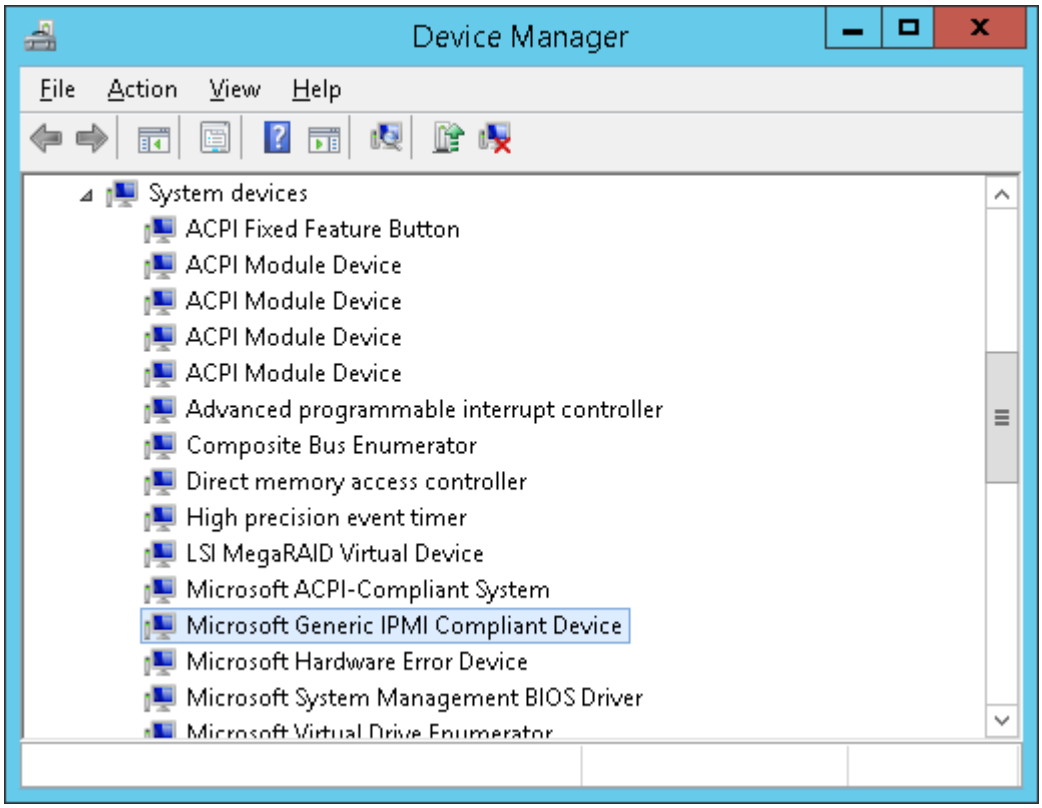
In order to install and execute the OSPUT, your server must meet the following requirements:

- Lenovo ThinkServer RD350, RD450, RD550, RD650 or TD350.
- Microsoft® Windows Server 2008 R2 SP1, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 ,Red Hat Enterprise Linux 6.5, Red Hat Enterprise Linux 6.8,Red Hat Enterprise Linux 7 or SUSE Linux Enterprise Server 11 SP3 and 12 64-bit operating systems.
- Lenovo ThinkServer running TSM firmware 0.84 or later.
- Microsoft® IPMI driver (for Windows only).
- OpenSSL 1.0.1g or later (for Linux only).
- OpenIPMI 2.0.16 or later (for Linux only).

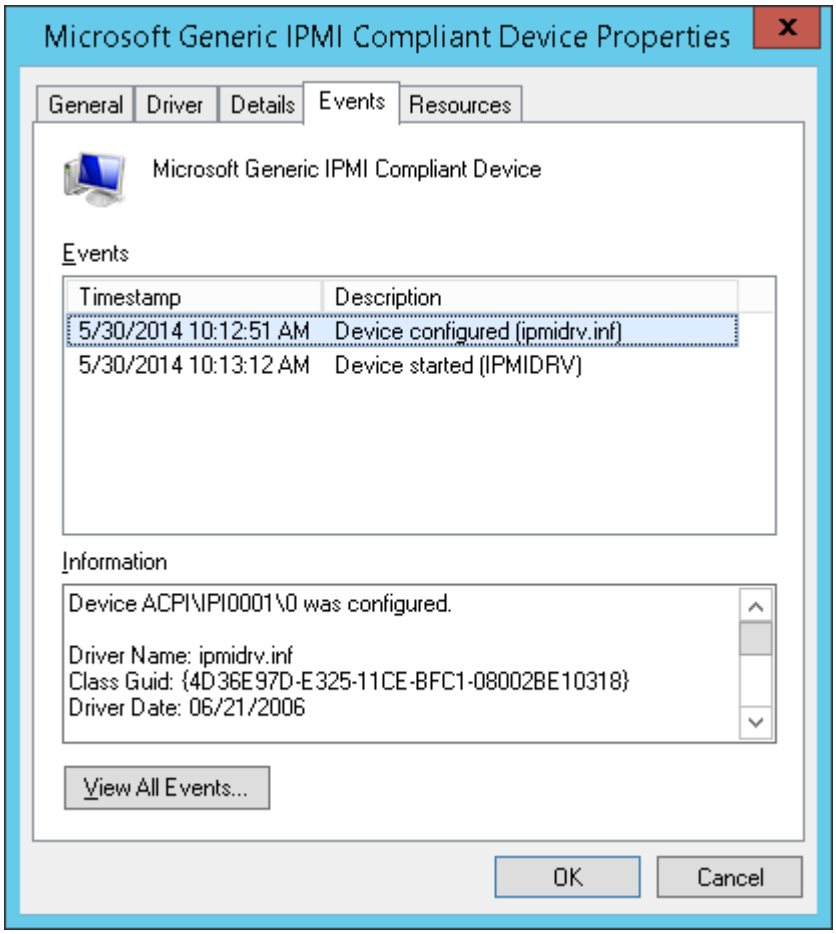
3. OSPUT Install Procedure for Microsoft® Windows Operating Systems

OSPUT must be installed on the server's operating system.
In order to install the OSPUT follow the instructions below:

1. Detect IPMI support:
   - You can verify if the device has been detected and that the driver is properly installed by checking if the "Microsoft Generic IPMI Compliant Device" device is listed on the System Devices within Device Manager:



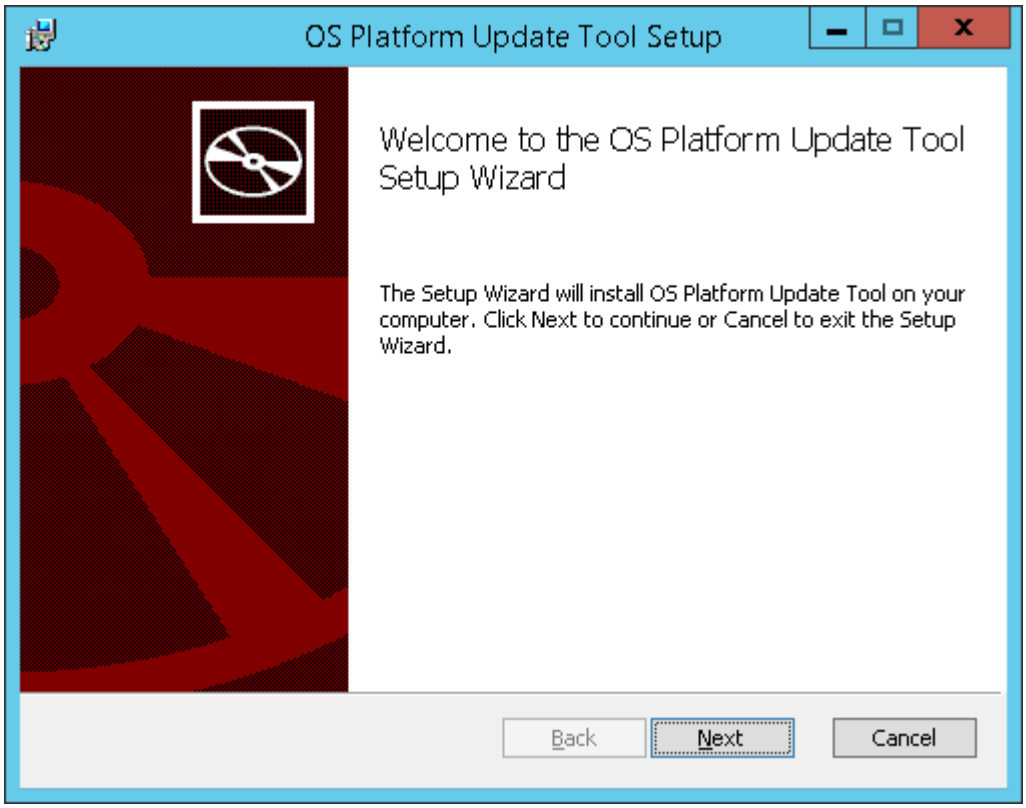
• Then, on device "Microsoft Generic IPMI Compliant Device" properties, you can check if the driver is correctly installed and configured.



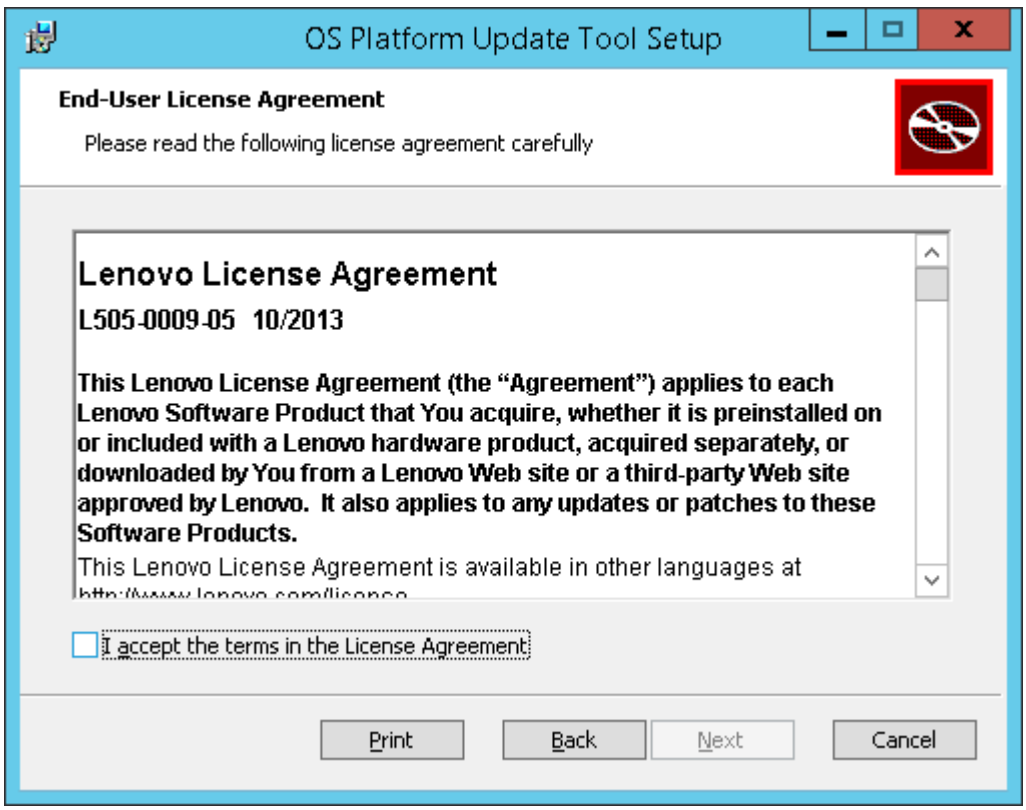
• If you did not find the device, it means that the system was unable to automatically detect TSM and install the IPMI Driver.

2. Download the latest OSPUT installer package from the Lenovo support website.

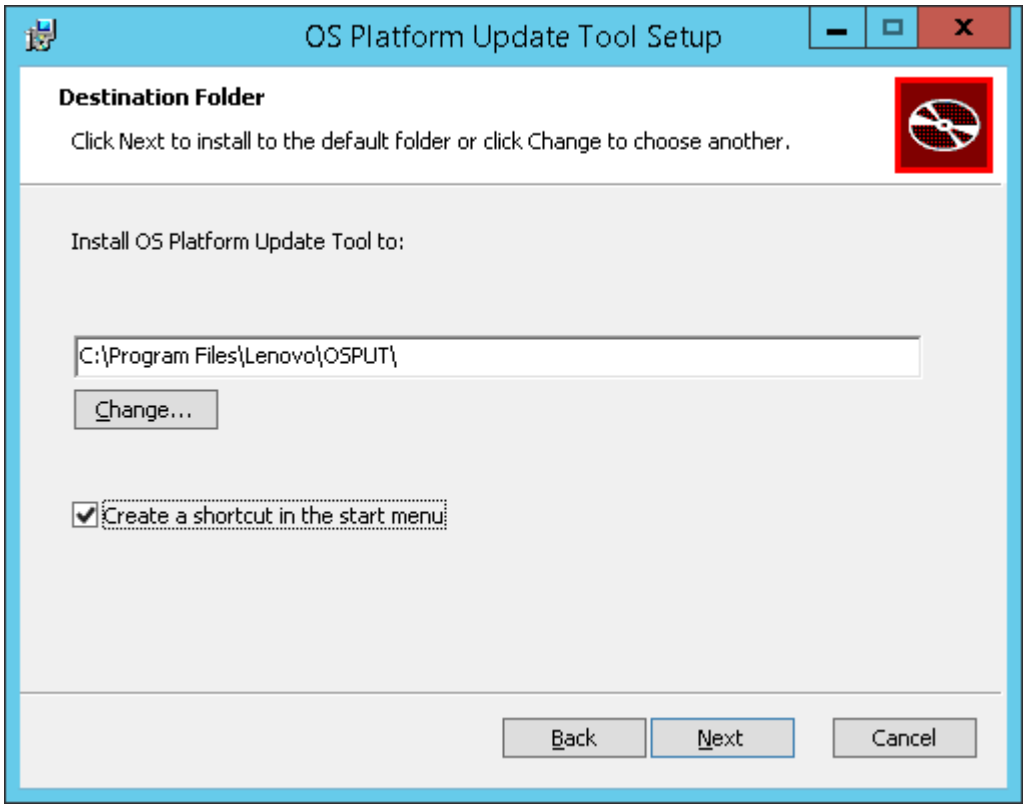
3. Execute the installer with **Administrator Privileges**



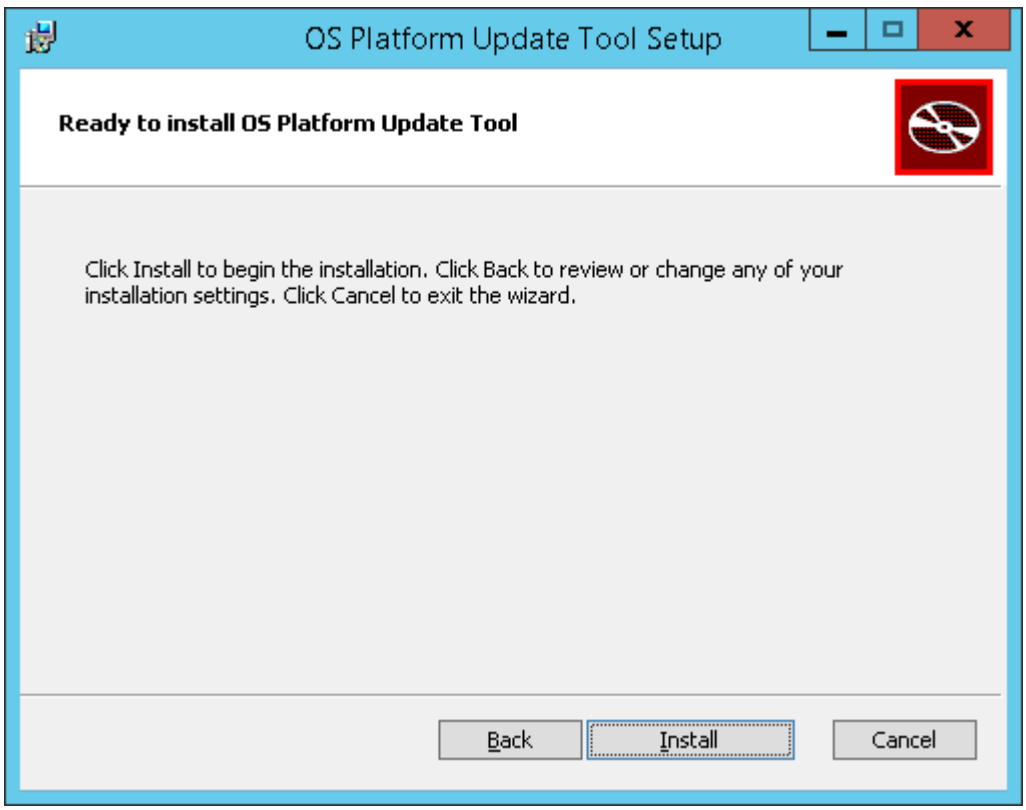
4. Read and accept the EULA for the OSPUT



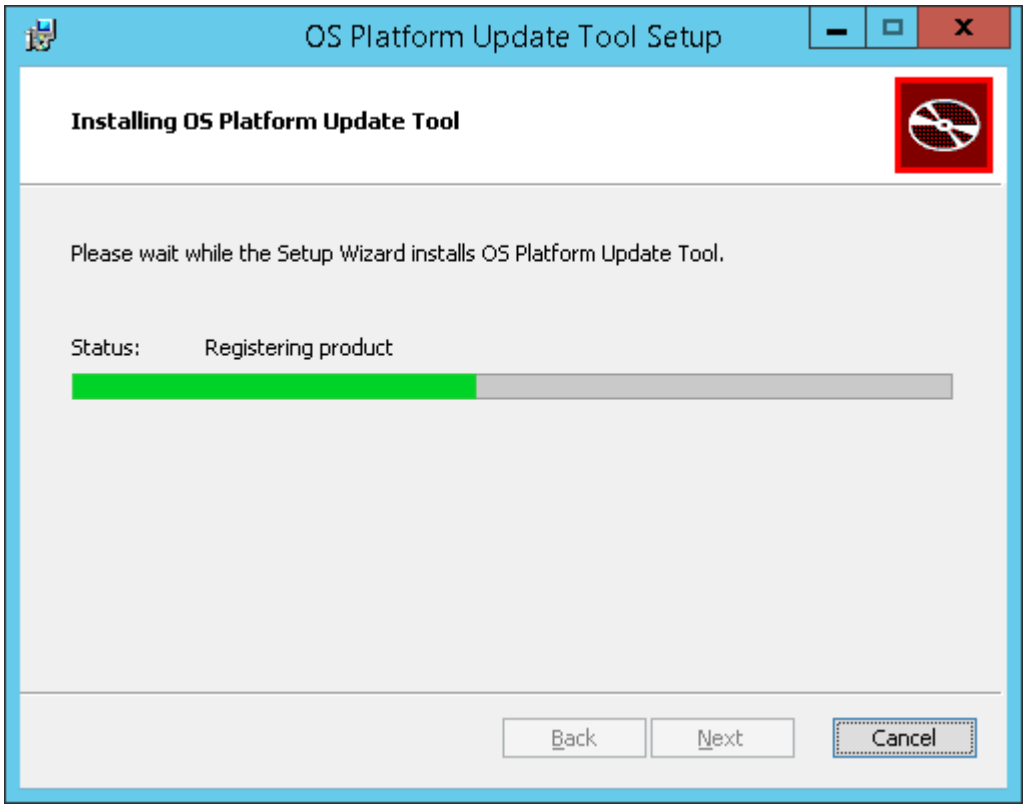
5. Select the location where the OSPUT will be installed and also if shortcuts will be created



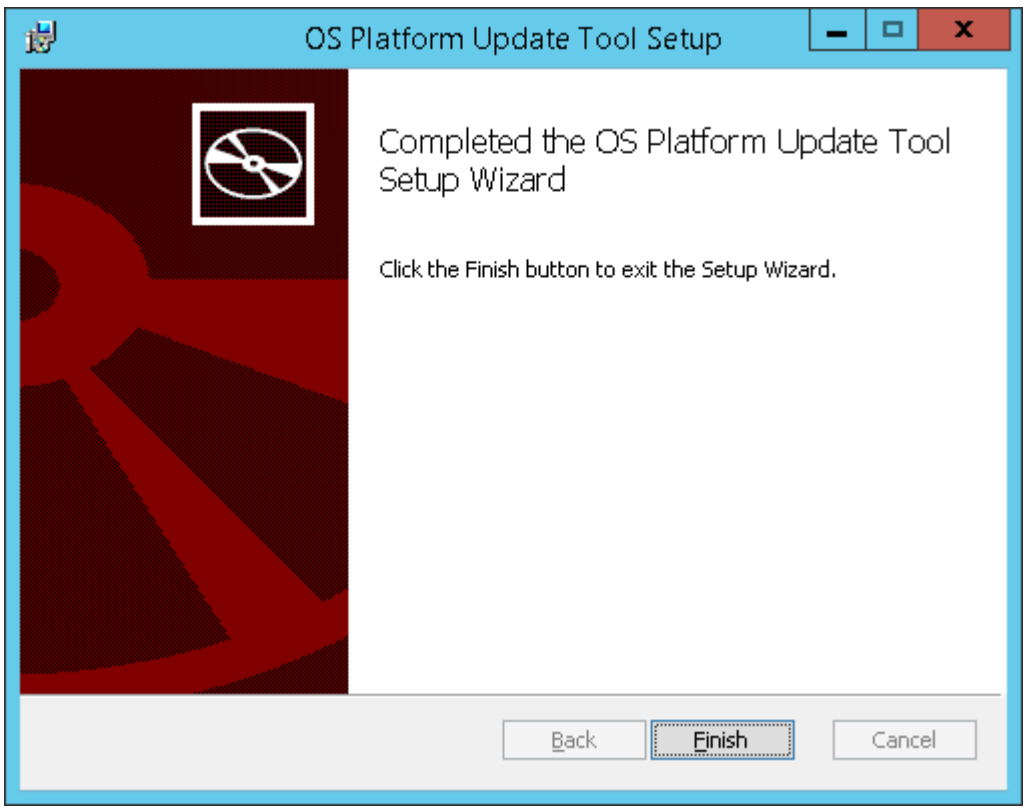
6. Click **Install** to confirm your preferences and install the OSPUT



7. Wait until the installation finishes



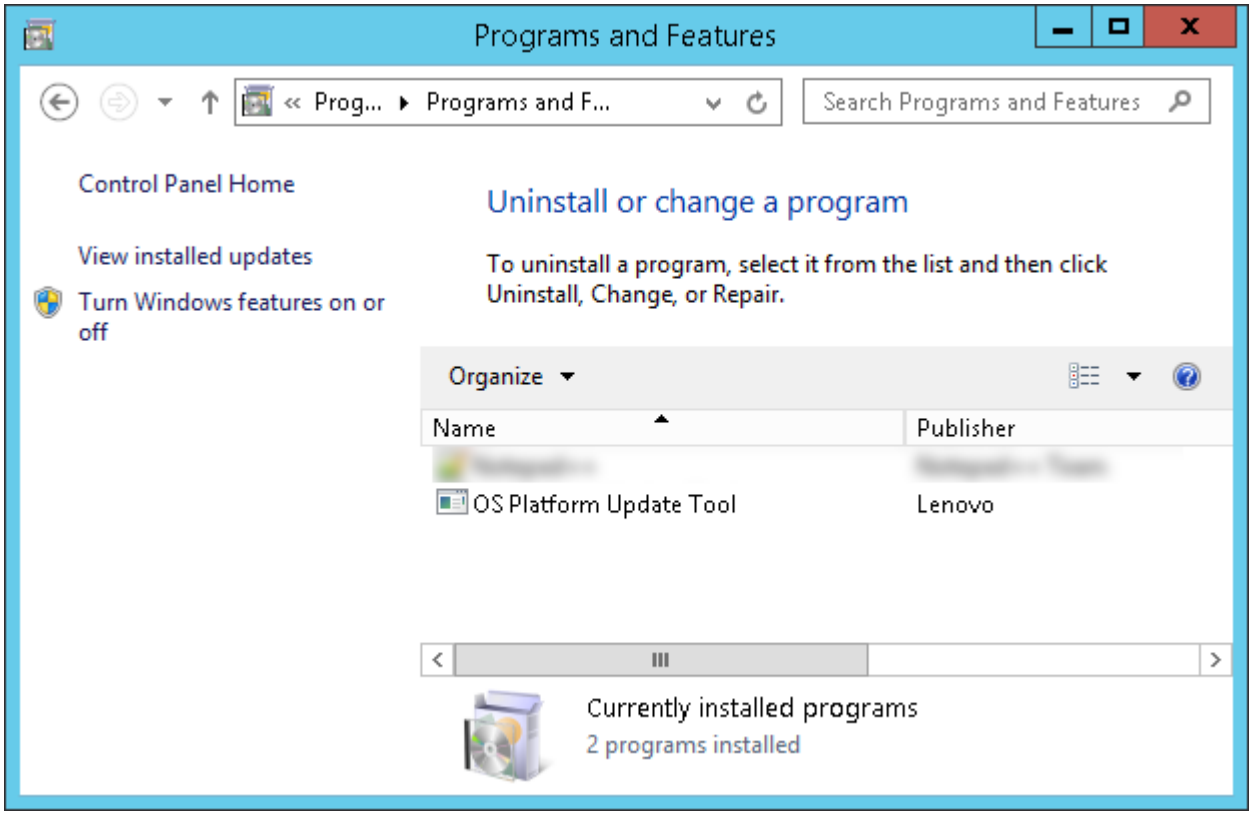
8. Click on **Finish** to close the installer window.



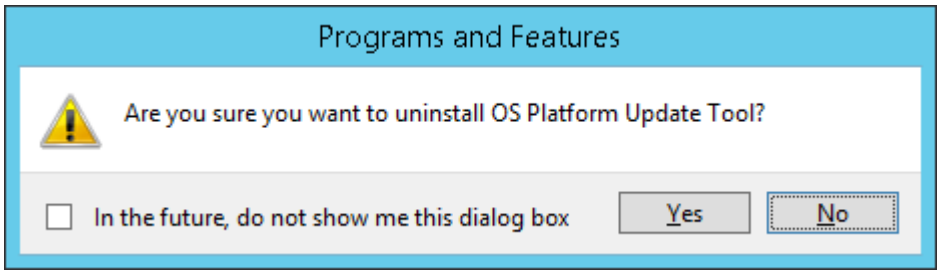
4. OSPUT Uninstall Procedure for Microsoft® Windows Operating Systems

In order to uninstall the OSPUT, make sure you have Windows **Administrator Privileges** and follow the instructions below:

1. Go to **Uninstall a Program** located in the **Control Panel**, search for **OS Platform Update Tool** and click on the **Uninstall** button



2. Confirm the uninstall, by selecting **Yes**, to proceed with the uninstall process



3. Wait until the uninstall process finishes

5. OSPUT Install Procedure for Red Hat Enterprise Linux 6.5,6.8 and 7 Operating System

OSPUT must be installed on the server's host. Make sure your Red Hat Enterprise Linux distribution is registered and activated prior to OSPUT installation. Please refer to your distribution documentation to details about how to get it registered and activated.
In order to install the OSPUT follow the instructions below with **Administrator Privileges**:

1. Verify IPMI support:

```
# rpm -qa | grep -i OpenIPMI
```

Expected Output:

```
OpenIPMI-2.0.16-14.el6.x86_64
OpenIPMI-libs-2.0.16-14.el6.x86_64
```

This output can vary depending on your system. If no output is returned then you need to install IPMI support. To install IPMI execute this command:

- `# yum install OpenIPMI`

2. Start the IPMI service:

```
# service ipmi start
```

Note: Every time OSPUT will be used the IPMI service must be running.

3. Download the latest OSPUT installer package

4. Install the package:

```
# rpm -i osput-1.1.9-1.rhel.x86_64.rpm
```

By default OSPUT is not added to your PATH environment variable.

6. OSPUT Uninstall Procedure for Red Hat Enterprise Linux 6.5,6.8 and 7 Operating System

In order to uninstall the OSPUT, make sure you have **Administrator Privileges** and follow the instructions below:

1. Uninstall the package with **Administrator Privileges**

```
# rpm -e osput
```

7. OSPUT Install Procedure for SUSE Linux Enterprise Server 11 SP3 and 12 Operating System

OSPUT must be installed on the server's host. Make sure your SUSE Linux Enterprise Server distribution is registered and activated prior to OSPUT installation. Please refer to your distribution documentation to details about how to get it registered and activated.
In order to install the OSPUT follow the instructions below with **Administrator Privileges**:

1. Verify IPMI support:
```
# rpm -qa | grep -i OpenIPMI
```
Expected Output:
```
OpenIPMI-2.0.16-0.13.48
```
This output can vary depending on your system. If no output is returned then you need to install IPMI support. To install IPMI execute this command:
    - `# zypper install OpenIPMI`

2. Start the IPMI service:
```
# service ipmi start
# modprobe ipmi_devintf
```
Note: Every time OSPUT will be used the IPMI service must be running.

3. Install dependencies:
    - Enable the Security Module repository:
    ```
    # zypper modifyrepo -e "SLE11-Security-Module"
    ```
    - Install OpenSSL:
    ```
    # zypper install OpenSSL1
    ```

4. Download the latest OSPUT installer package

5. Install the package:
```
# rpm -i osput-1.1.9-1.sles.x86_64.rpm
```

By default OSPUT is not added to your PATH environment variable.

8. OSPUT Uninstall Procedure for SUSE Linux Enterprise Server 11 SP3 and 12 Operating Systems

In order to uninstall the OSPUT, make sure you have **Administrator Privileges** and follow the instructions below:

1. Uninstall the package with **Administrator Privileges**

```
# rpm -e osput
```


9. OSPUT Usage

To execute OSPUT on Windows Operating Systems use the shortcut created on "Start Menu" during the install procedure.
On Linux Operating Systems OSPUT can be found in the following directory: `/opt/lenovo/osput`
Note that OSPUT need to be executed in the condition of good network environment with **Administrator Privileges**.

The basic OSPUT command line syntax is the following:

osput [COMMAND_PARAMETERS] [COMMAND_ARGUMENTS] [TSM_ARGUMENTS]

Where:

- `[COMMAND_PARAMETERS]` is one of the following parameters:
  `-h [ --help ]`
  Display help information.

  `-c [ --command ]`
  Specifies the command to be executed. For the complete list of commands available on this version of the OSPUT check the OSPUT Commands Reference section on this document.

- `[COMMAND_ARGUMENTS]` specifies the arguments specific to each OSPUT command. For more information check the OSPUT Commands Reference section on this document.
- `[TSM_ARGUMENTS]` specifies the arguments specific to flash firmware of remote TSM.
  `-H [ --host ]`
  Specifies remote TSM IP address.

  `-P [ --port ]`
  Specifies remote TSM port number.

  `-u [ --user ]`
  Specifies remote TSM username.

  `-p [ --password ]`
  Specifies remote TSM IP password..

Examples for each OSPUT command can be found on the OSPUT Commands Reference section on this document.

10. OSPUT Commands Reference

10.1. getBundleInfo

Get information about the images present in a bundle file.

SYNTAX

```
osput [--command] getBundleInfo [--file] <bundle_file>
```

DESCRIPTION

The getBundleInfo command displays information about all components of the specified bundle file.

COMMAND ARGUMENTS

```
-f [ --file ]
```

Specifies the bundle filename including full path.

EXAMPLES

```
osput --command getBundleInfo --file bundle.bdl
```

10.2. getServerInfo

Get information about the components present in the server.

SYNTAX

```
osput [--command] getServerInfo
```

DESCRIPTION

The getServerInfo command lists current firmware versions installed on the server.

EXAMPLES

```
osput --command getServerInfo
```


10.3. getUpdateInfo

Lists which components can be updated using the specified bundle.

SYNTAX

```
osput [--command] getUpdateInfo [--file] <bundle_file>
```

DESCRIPTION

The getUpdateInfo consolidates information read from the specified bundle with the firmware versions installed on the server, listing which components can be updated using that bundle along with their current and new version numbers, dependencies and reboot requirements.

COMMAND ARGUMENTS

```
-f [ --file ]
```

Specifies the bundle filename including full path.

EXAMPLES

```
osput --command getUpdateInfo --file bundle.bdl.
```


10.4. update

Start a firmware update on the server.

SYNTAX

```
osput [--command] update [--file] <bundle_file> [--noRebootAfterUpdate]
[--force]
```

DESCRIPTION

The update command starts firmware update to update components available on a bundle. This command displays how many pending updates remain and the completion status of the current component being updated. If the user presses `Ctrl+C` a command to cancel the all pending updates is sent to the server. Note that this does not guarantee that updates will be cancelled.

COMMAND ARGUMENTS

`-f [ --file ]`

Specifies the bundle filename including full path.

`--noRebootAfterUpdate`

The update process for some components involves a TSM or Host reboot. In some of these cases, the reboot is needed during the update operation, and cannot be avoided. In some other cases, however, even though the update will take place only after rebooting, the reboot can be deferred by specifying the '--noRebootAfterUpdate' option, and will not happen automatically. Later on, when a reboot happens, the update is automatically applied. The reboot requirements for a component update can be verified with the 'getUpdateInfo' command.

`--force`

Update to the same version is not allowed. Use this argument to force the update in this situation.

EXAMPLES

```
osput --command update --file bundle.bdl --noRebootAfterUpdate
```

```
osput --command update --file bundle.bdl --noRebootAfterUpdate --force
```


OSPUT Return Codes

Below is the list of codes returned by OSPUT:

- **0x000000 - Success**
  Return when operation succeeded.

- **0x000001 - Invalid Command Options**
  Return when command line has invalid options or arguments.

- **0x000002 - Operation Failed**
  Return when command operation failed.

- **0x800000 - Out of memory**
  Return when OSPUT cannot allocate necessary memory.

- **0x810000 - IPMI Open Interface Failure**
  Return when OSPUT cannot open the IPMI interface.

- **0x810001 - IPMI Access denied**
  Return when user don't have necessary permission to execute the commands.

- **0x810002 - IPMI Send Request Failure**
  Return when OSPUT can not send the IPMI request.

- **0x810003 - IPMI Send Request Timeout**
  Return when an IPMI request didn't return in an expected time interval.

- **0x820000 - IPMI Session Creation Failure**
  Return when OSPUT can not create an IPMI session.

- **0x820001 - IPMI Session Closing Failure**
  Return when OSPUT can not close an IPMI session.

- **0x830000 - Firmware Update Command Failure**
  Return when firmware update command fail.

- **0x830001 - Cancel Firmware Update Command Failure**
  Return when cancel firmware update command fail.

- **0x840000 - Firmware Update In Progress**
  Return when a firmware update is already in progress.

- **0x840001 - TSM In Update Mode**

Return when the TSM is in update mode by another user.

- **0x840002 - Invalid Unique Update ID**
  Return when the update ID is invalid or expired.

- **0x840003 - No Firmware Image Available**
  Return when no firmware image is available.

- **0x840004 - No Firmware in Cancel State**
  Return when no firmware image is in pending state.

- **0x840005 - Invalid IPMI Command**
  Return when an invalid IPMI command is received.

- **0x840006 - Bundle Upload Failure**
  Return when upload a bundle fail.

- **0x850000 - Bundle Parsing File Opening Failure**
  Return when fail to open a bundle file.

- **0x850001 - Bundle Parsing Invalid Extension**
  Return when the specified bundle has an invalid extension.

- **0x850002 - Bundle Parsing Reading Failure**
  Return when fail to read the specified bundle file.

- **0x850003 - Bundle Parsing Invalid XML File**
  Return when the specified bundle has an invalid catalogue.

- **0x850004 - Bundle Parsing No Image Element**
  Return when the specified bundle don't contains an image element.

- **0x850005 - Bundle Parsing No Device Element**
  Return when the specified bundle don't contains an device element.

- **0x860000 - Bundle Upload Rejected**
  Return when upload occurs while there are updates still pending.

