

# SanerNow Software Deployment

---

*Ensure Endpoints are always installed with Approved Software Packages*

## Overview

In this world of complex infrastructure, there are numerous operating systems and different endpoints - laptops, workstations, servers or virtualization, and BYODs. The challenge often is ensuring all these endpoints have common set of approved applications installed and running. We lack visibility and even if device availability is ensured, the process of application deployment is an upheaval task. Organizations look for an intuitive and reliable approach to software deployment.

SanerNow takes a fresh look at how software can be deployed and managed with ease.

## What does SanerNow offer?

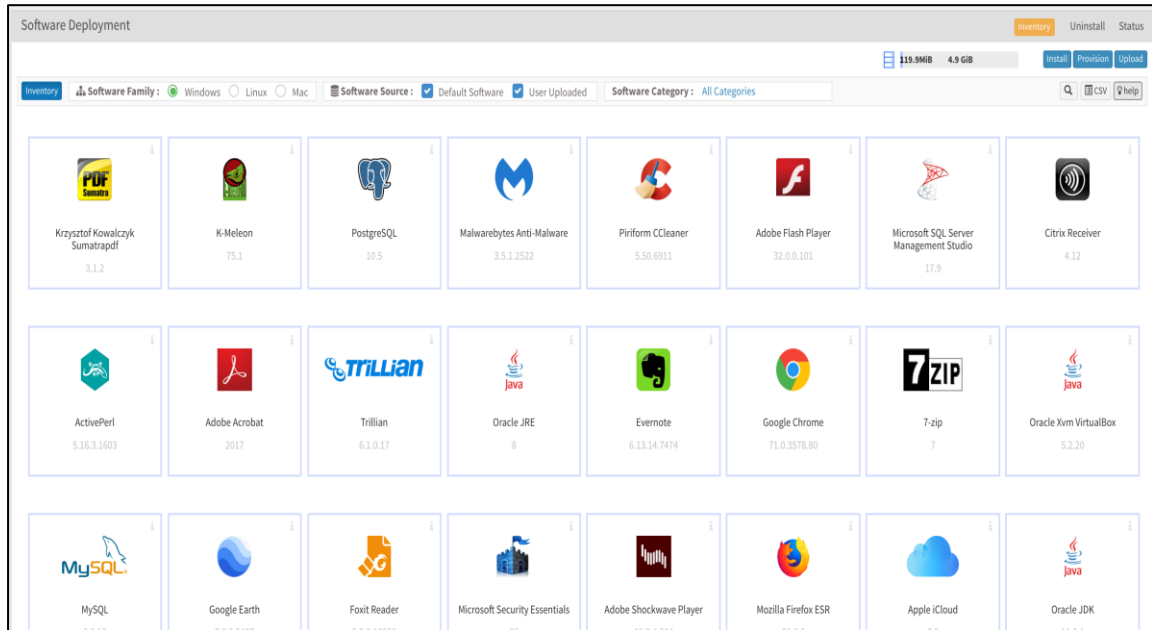
SanerNow has been offering remediation to mitigate known vulnerabilities and safeguard endpoints against attacks. This requires constant tracking and amendment of remediation scripts to provide latest software from time-to-time, ensuring smooth installation. With the release of version 4.1.1.0, SanerNow added numerous ways in which software deployment can be approached and includes latest **vulnerability-free** versions of commonly used software. It also offers customization to diligently handle various operating systems; accepts user inputs such as how to install in silent mode, what to run and where to install.

Three major capabilities were introduced with the release of SanerNow 4.1.1.0,

1. Deployment of Software Applications
2. Provision Applications Deployment
3. Uninstallation of Software Applications

## 1. Deployment of Software Applications

SanerNow supports application deployment from array of pre-defined software packages as well as applications and software packages that can be uploaded into the repository and manage.



Saner Default Software Repository

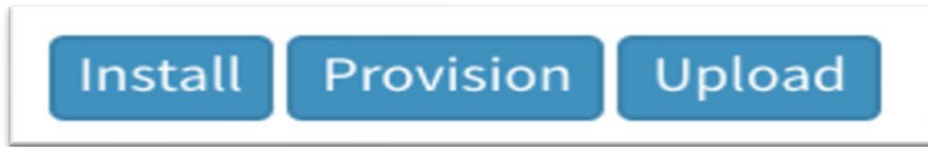
Software installers differ based on operating systems; it may differ from a usual installation routine, may require configuration changes during installation and may require additional support for legacy software. SanerNow allows users and administrators to upload software onto the platform and create tasks to install them during a stipulated time. It also renders different ways to install software on endpoints. Let's take a deeper look into each of them.

There are three main ways to upload software and Saner agents are equipped to handle these cases below

1. **Installer Packages.** Upload a single installer or a group of software applications combined into a single compressed ZIP file
2. **Compressed Installer Packages.** Upload a ZIP/GZIP/TAR file and provide customization pointers
3. **External Software Repository URL.** Provide a link to download installers from vendor or organizations' repositories

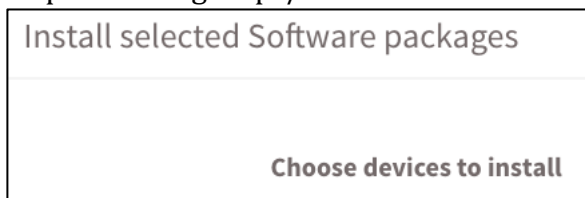
## Getting Started

Go to EM > Actions > Software Deployment, click on **Upload** on right hand side tool bar to start.

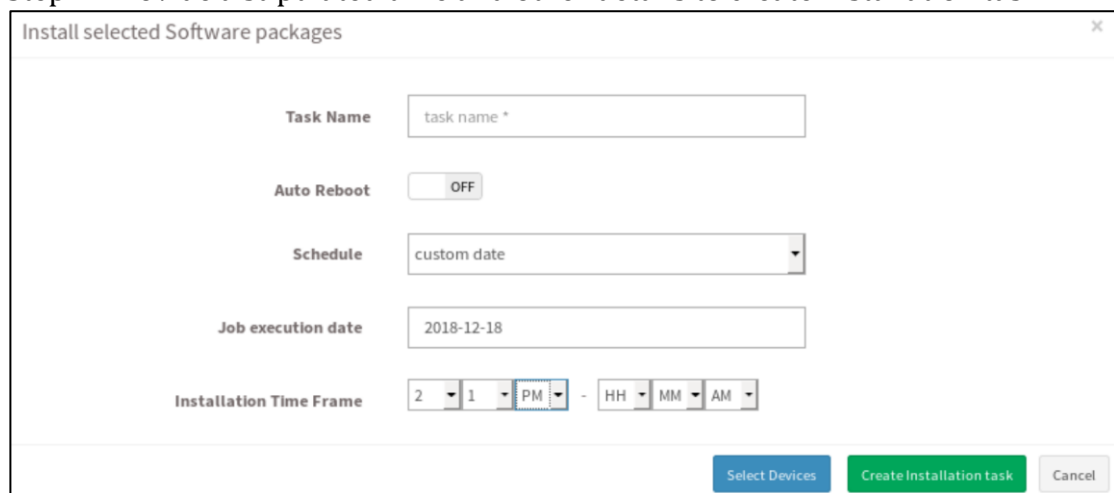


Select multiple software and click on **Install** to send deployment tasks to Saner agents.

Step 1: Select groups/devices



Step 2: Provide a stipulated time and other details to create installation task.



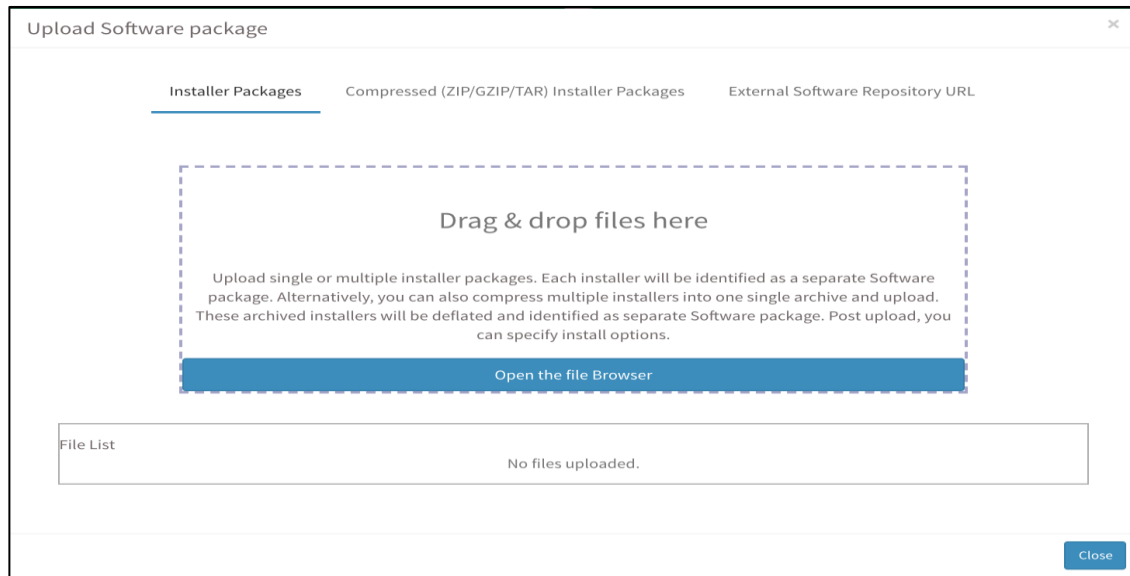
**Provision** is a tool that is described in [System Provisioning](#) section below.

Let's take a look at each of the cases,

### Case 1: Installer Packages

Upload a single installer or a group of software applications combined into a single compressed ZIP file. Users can simply drag and drop file/files or open file browser to select files and upload. Once the file is uploaded, metadata of files

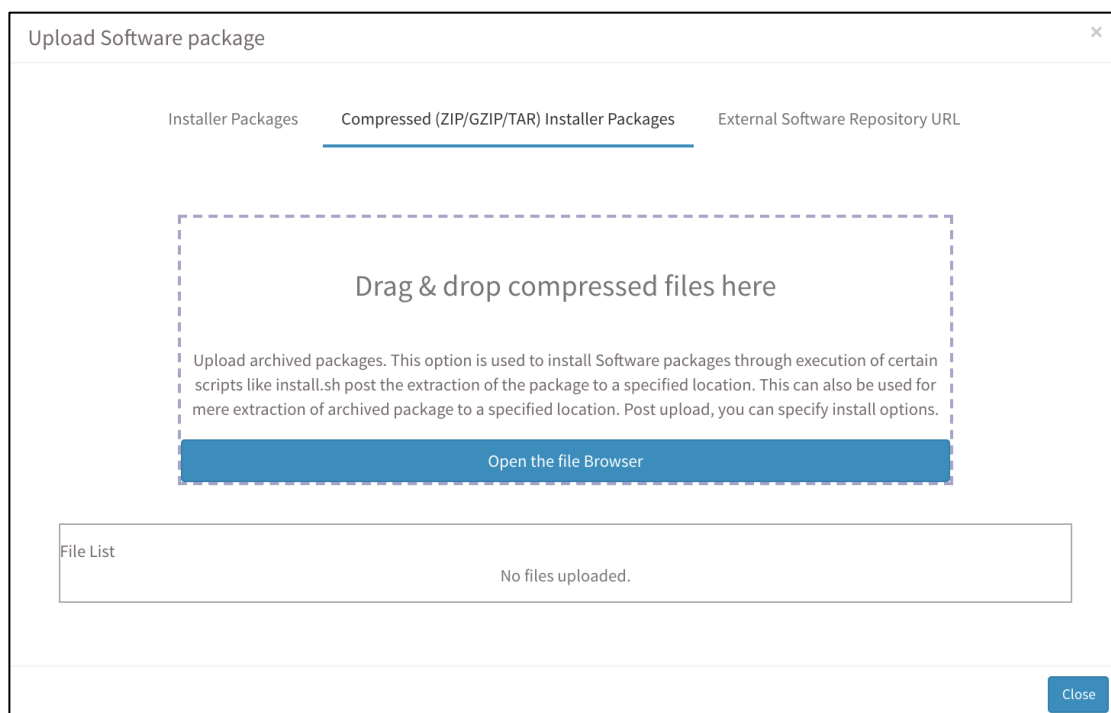
need to be edited to provide a mandatory silent installation option for better user experience at endpoints.



Case 1: Installer Packages

## Case 2: Compressed Installer Packages

Upload a ZIP/GZIP/TAR file and provide customization pointers such as appropriate location to decompress in an endpoint, file/script to run that eventually installs the software. User can create customized scripts i.e. lineated steps for installation such as change configuration settings, move/copy files before running the actual installer.



Case 2: Compressed Installer Packages



Software deployment is achievable using internal repositories hosted by an organization or external repositories such as OneDrive. Users can render a script to download files with or without credentials and this script can be compressed and uploaded onto the platform. Users can specify such a script as 'File to run' which will be executed after decompressing the downloaded zip file on the endpoints.

A typical example of a script could contain lines such as below,

```
wget -- no-check-certificate --post-  
data='resIds=xxx&canary=yyy&authkey=zzz '  
'https://onedrive.live.com/downloadfiles/V1/Zip?authKey=zzz '
```

Once the software installer is downloaded, next lines in the script can provide configuration (if any) and run the installer with silent option for uninterrupted deployment.

### Case 3: External Software Repository URL

Users may provide a link to download installers from vendor or organizations' repositories. Saner agents will initially download the software and recognize the installer file to be EXE/MSI in case of Microsoft Windows, DPKG/RPM files for Linux based operating systems or DMG/PKG for Mac operating systems. The silent option provided will be considered during installation.

Upload Software package


Installer Packages    Compressed (ZIP/GZIP/TAR) Installer Packages    External Software Repository URL

URL to download Software package

Software package name  [Fetch info](#)

[Close](#)

Case 3: External Software Repository URL

In case your deployment file appears with  sign, it indicates that mandatory input is missing and requires your attention. Click on the deployment file to edit those fields. Software installation task can only be created when these fields are specified with appropriate data.

## 2. Provision Applications Deployment

Standard Applications can be provisioned for deployment as part of system preparedness for use. This will ensure standard applications are deployed and the endpoints are ready for use.

Users can easily provision newly added devices or existing devices with essential software. System provisioning interface is very similar to 'Install', but it creates a rule for all devices under a specific group. Users can select several software installers and click on **Provision** from top right menu bar to install on a group of devices. Existing devices in the group receive the task immediately.

In case of new agent installation, once the device activates, it is assigned to the group. After initial download and scan, devices execute the System Provision task; it installs all the required software one after another. Once the task is complete, it eventually re-scans the system to report vulnerabilities and compliance deviations.

Rule for installing Software packages ×

---

**Task Name**

**Auto Reboot**

**Installation Time Frame**

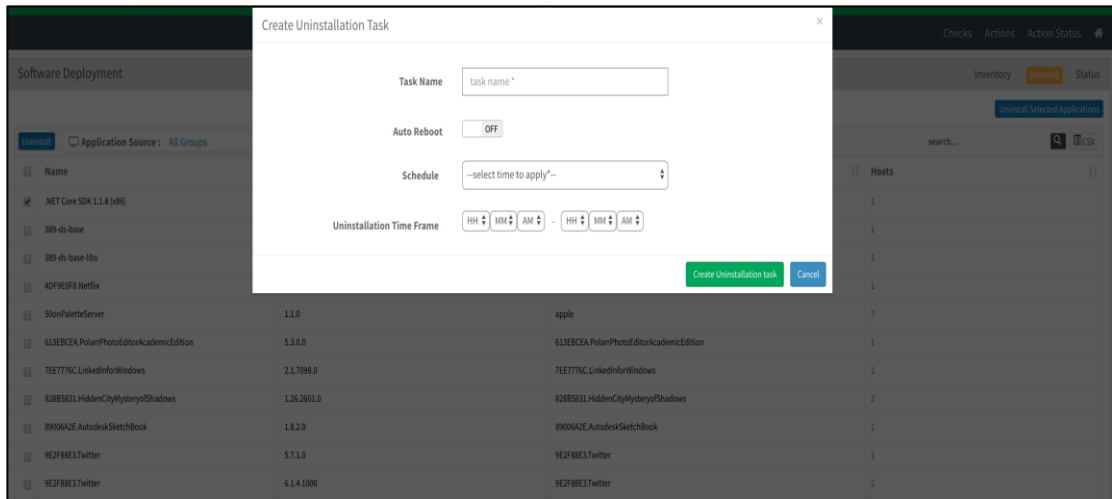
---

### Provision Software Deployment

## 3. Uninstallation of Software Applications

The applications which are unauthorized, blacklisted, unused can be removed from systems as a scheduled cleanup task. Malware and adware embedded applications is one of the causes for concern in dealing with attacks. Organizations invest in procuring licensed software and typically these investments aren't realized effectively. Applications could be underutilized. With ability to remove rogue and under-utilized software, organizations benefit immensely.

Unwanted software can be removed from a device, a set of devices or a group of devices using filters on the top of the menu bar and creating a task. Simply apply filter if necessary, select applications from a list of installed software and click on **Uninstall Selected Applications** to create a task. If filter is not applied, it removes the software from all applicable devices.



Uninstallation of Software Applications



To augment uninstall action, users can block an application using EM > Actions > Application and Device Control > Application Block.

## How to Track Deployment Status

Users get real-time visibility on status of software deployment task against each endpoint. If device has not reported any status, the task is in progress or not yet initiated. A typical status page looks like the image below:

Software Provision Status				
Host Name			Overall Status	
sp-shesh-desktop			partial success	
Name	Action	Status	Reason	
7-zip	Install	success		
PuTTY	Install	success		
WinRAR	Install	success		
WinZIP	Install	fail	Application download failed	

Deployment Status Tracking

This information helps consolidate status of actions with appropriate reasons that helps to take further actions based on results in case of failures, identify newly added devices to System provisioning and ensure that all devices have successfully installed software applications for a given task.

## Usability Notes

- ✓ Select Multiple Applications, hold Ctrl and drag over the items or hold Ctrl and click on items you wish to select.
- ✓ Upload single or multiple files (in compressed format) for deployment.
- ✓ Customize software deployment with compressed upload and indicate the file to run after extraction
- ✓ Provide URL-based software download and deployment
- ✓ Get information and edit metadata of each software asset

- ✓ View assets according to family. Segregate your uploaded assets from SecPod default. Switch between Grid and List view
- ✓ Filter using categories, or search for assets
- ✓ Create software provisioning task and new Saner-enabled devices would automatically install required software
- ✓ View deployment status
- ✓ Uninstall software
- ✓ Generate CSV data to create your own graphs and reports

## What's next?

---

SanerNow intends to increase the coverage scope to bring in more software installers under this hood that are tested in our labs against known vulnerabilities.

In the next releases to come, SanerNow would integrate with other external software repositories to give a combined list of software available.