Managing Assets Using SanerNow

4.0 User Guide
Asset Management

Asset management allows you to track and manage your organization’s assets, such as:

- Devices (hardware assets)
- OS applications such as Microsoft Office, .NET etc., and their patches (operating system)
- Third-party software such as Skype, Adobe etc. (licensed assets for third party applications)

Asset management includes:

- Installation of assets
- Uninstallation of assets

The SanerNow endpoint security solution helps you to track and manage your assets and their lifecycle within your organization from a centralized location.

To access the Asset Management tool:
1. Logon to SanerNow using your SanerNow credentials.
2. Select an account to manage by clicking the icon at the upper left corner of the window. A dashboard with the summary view of the account is displayed.
3. Click the SanerNow icon on the header. Click the Asset Management icon. The Asset Management Dashboard is displayed, which provides device details, hardware and software asset details, and license information.

Device Distribution

This pane shows the distribution of devices, categorized by operating system. Clicking More Info shows the list of all devices on the network, irrespective of the OS. You can filter this view by a specific OS or you can search for a specific device if the list of devices on your network is very long. You can also download an Excel sheet of the devices by clicking the CSV icon.

Assets based on Publisher

This pane provides a list of assets, categorized by publisher.
Hardware Assets

This pane shows a distribution of all the hardware assets by either the manufacturer or device type. To retrieve a list of all the hardware assets, click the CSV icon in the Hardware Assets pane; a Microsoft Excel file is generated with details for all the assets.

Devices

This pane shows you a list of devices being managed.
Software Assets

This pane shows the software assets being managed. You can choose to filter the list of assets by publisher or by device groups, if you need to traverse a long list of assets. To retrieve a list of all assets in an organization, click the CSV icon in the Software Assets pane; a Microsoft Excel file is generated with details for all assets. You can choose to view 15, 25, 50 or all assets.

Licenses

You can view the licenses that the organization owns in this pane, categorized by Operating System, Applications, and Hardware licenses. This pane helps you track the license details of all assets and optimize asset usage. Details, include the license key (if it is available), devices where it is installed, the remaining number of licenses, the cost of the license, and any duplicate use or violation. Click the expand icon to take action, such as modifying existing or adding new license information.
Out-dated Applications

This pane helps keep track of all assets that are a security risk because of applications and hardware or operating systems that are outdated or have reached end-of-life. The vendor either no longer supports the application or provides patches and fixes. This pane is helpful for making decisions on whether to uninstall or phase out applications based on your organization’s asset needs.

Blacklisted Applications

This pane shows a list of all applications that are blacklisted in the organization but are still in use. Clicking the expand icon allows you to take action such as uploading a .csv file of applications that you want to blacklist or whitelist, adding or modifying blacklisted application details, and filtering the list of blacklisted applications.

Note: Blacklisting applications does not automatically remove applications from devices. That process can be
managed with the SanerNow Endpoint Management tool or by other methods.

Filtering the list of applications allows viewing only blacklisted or whitelisted applications, and to refine the list further by a combination of device groups, operating systems, and asset publishers.
Rarely Used Applications

This pane provides a list of rarely used applications. It shows how assets are distributed across hosts, and how frequently they are used. This helps plan your license distribution, decide on applications to decommission, and reduce cost.

Setting Alerts for Asset Management

You can choose to be alerted when there are changes to assets on your network, or when new assets are added.

To Set Alerts for Asset Management

1. Click Alerts > Asset Management.
2. Set the subscription status to On.
3. Specify the email to which you want the alerts sent.
4. Specify which conditions you want to receive alerts for:
   - New devices – when a new system is added to the network.
   - Rarely used assets – when assets have not been used for a long time.
   - Blacklisted assets – when staff is trying to use an asset blacklisted for use within the organization
   - Software license violations – when the software license of an asset is being used in excess of the total number of licenses, due to any reason.
- Outdated applications – when an application that is no longer supported by the vendor or has no patches or updates is still being used or exists on a device
- New assets – when a new application is installed

5. Click Update to complete.

Asset Management Reports

Asset Reports provide a comprehensive view of the hardware and software assets in the organization, the blacklisted applications, and the license distribution, etc.

To Generate the Asset Management Report

- Click Reports > Asset Report.

To export the report to a PDF
Click Export > PDF

To export the report and send it via email:
1. Click Export > Email.
2. Specify email addresses.

**To Back Up Reports**

The backup settings under Reports allow IT administrators to obtain a backup report showing the history of assets. The backup time should be scheduled. The backup report can be scheduled to run automatically daily or weekly.

**To configure backup settings for reports:**
1. Click **Backup**.
2. Specify the frequency of backup in the **How Often** drop-down. You can back up reports daily, or weekly. If you choose weekly, you can specify the days.
3. Specify the number of days that a backup should be maintained in the **Keep Only the Latest** box. Files older than the specified value will be deleted. You can maintain backups for a maximum of 30 days.
4. Specify the **Backup Time**, that is, the time when SanerNow will create an archive of the report. Specify an **Email** addresses.
5. Click **Save**.

**Uninstalling Blacklisted Applications**

You can uninstall blacklisted or unwanted applications either manually, using a tool your organization already owns, or through SanerNow’s Endpoint Management tool. For details on how to uninstall applications using the SanerNow Endpoint Management tool, see the *Managing Endpoints Using SanerNow 4.0 User Guide*. 
About Us

SecPod Technologies creates cutting edge products to ensure endpoint security. Founded in 2008 and headquartered in Bangalore with operations in USA, the company provides computer security software for proactively managing risks and threats to endpoint computers.

Contact Us

Web: www.secpod.com
Tel: +91-80-4121 4020 | +1-918-625-3023
Email: info@secpod.com

© SecPod Technologies 2018. All Rights Reserved.