About Device Assets

https://campus.barracuda.com/doc/89620850/

When you install Onsite Manager at a customer site, it automatically begins:

- scanning assets within the IP addresses you have defined
- discovering new devices
- collecting detailed data

The asset scan on newly discovered devices is performed automatically and does not wait for a predefined interval.

Data is collated and summarized on the **Central Dashboard**, so you can drill down to details as required.

Use the **Managed Windows Inventory** and **Managed SNMP Inventory** views to see assets by site. You can get a quick view of the operating systems, CPU, hard drives and so on at each site. You can then drill down to the actual devices to see more detail.

Notes

- Only asset information that has changed is sent to Service Center. For example, if Microsoft Office is installed on a device, this information is detected by the first asset scan of the device. This information is not resent each subsequent asset scan. However, if Microsoft Office is subsequently updated or uninstalled, this new information is detected by an asset scan and sent to Service Center.
- If a device reboots in between Onsite Manager discovery scans, then Onsite Manager still considers it up and continues incrementing the discovered time (**UP/DN** on device lists). The **Device Overview** page displays a value for time since last reboot, which is reported by the device operating system. Device availability alert thresholds are based on the discovered time and not the last operating system reboot.

What You Can Do

You can:

- perform a device asset scan on demand
- search for a specific asset, such as the CEO's laptop, or search for a set of devices that meet your criteria
- identify versions and licensing across each customer site
- use reports to discover the presence of unauthorized or illegal software, such as peer-to-peer

file sharing applications that rob bandwidth
- monitor and manage any hardware with an IP address and an active management protocol, including:
  - desktops
  - laptops (onsite and offsite)
  - servers
  - managed switches
  - routers
  - firewalls
  - gateways
  - **VoIP** switches and phones
  - printers
  - faxes or scanners
  - specialized equipment and environmental control devices
  - virtual machines and more
- identify inefficient, overloaded and unsupported devices
- automate collection of vendor-assigned asset tags
- track warranty and inventory tag information
- create device aliases to suit customer needs and streamline the support process
- view software assets based on:
  - applications
  - Windows services
  - hot fixes
  - service packs
- view product keys (for the operating system, Microsoft Office and **SQL**) for a device
- view last boot time for a device

  Windows does not treat a computer coming back from sleeping or hibernating as a reboot.

See Also

- For information about the network scan for devices, see Running a Scan Manually.
- For information about using reports to create summary and detail asset reports, see Reporting.