1. “Perangkat atau pengguna?”

Lansweeper dirancang **utama untuk perangkat / aset IT** — hardware, software, server, workstation, network devices, dll.

Data pengguna juga bisa dicatat (misalnya siapa user di komputer, domain, login, dll) tapi fungsi utamanya adalah aset/perangkat.
Jadi: fokus “perangkat” lebih kuat.

Pertanyaan **“Perangkat atau pengguna?”** maksudnya begini 👇
User ingin tahu **objek utama yang dilacak atau dikelola oleh sistem Lansweeper itu apa** — apakah:

1. **Perangkat (device-based)** → berarti Lansweeper fokusnya pada **hardware atau aset fisik/logis** seperti komputer, server, switch, printer, router, dan VM.
2. **Pengguna (user-based)** → berarti sistem fokusnya pada **siapa yang menggunakan perangkat** (misalnya data karyawan, login user, aktivitas, dsb).

🔍 **Jawaban konteks Lansweeper:**
Lansweeper itu **berbasis perangkat (device-based)**.
Dia memindai (scan) semua perangkat di jaringan — mendeteksi:

- hostname, IP, OS, hardware specs
- software terinstal
- status patch
- siapa user yang login

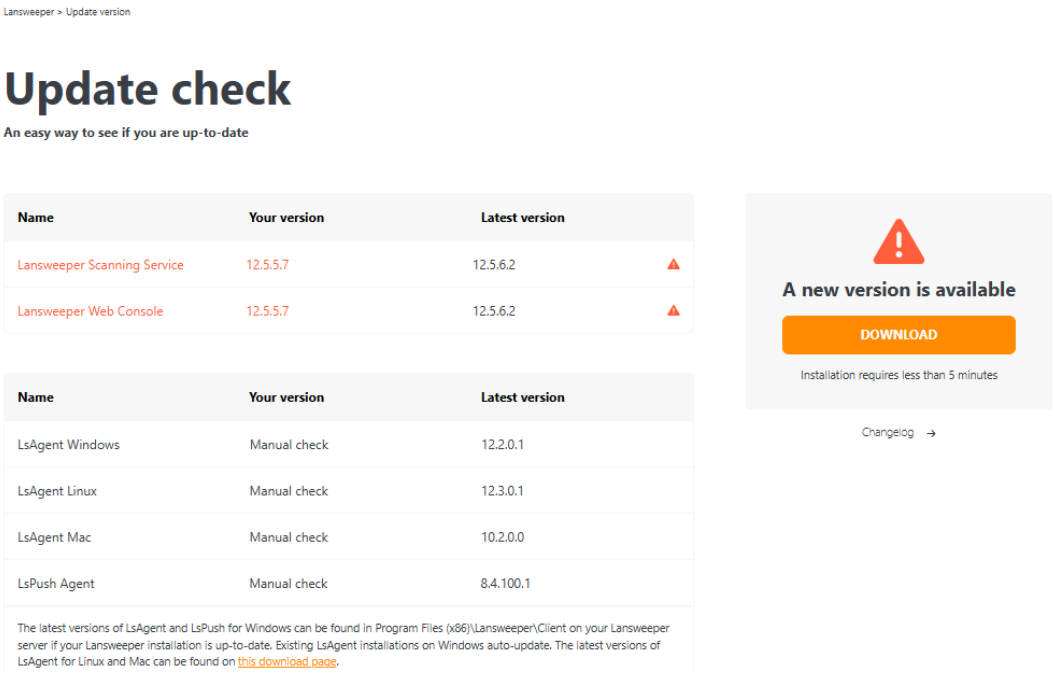
Jadi walaupun Lansweeper bisa menampilkan informasi **pengguna yang login di perangkat**, **fokus utamanya tetap pada perangkat/aset IT**.

🧠 Singkatnya:
Pertanyaan “perangkat atau pengguna?” artinya: *sistem ini memonitor perangkat atau orangnya?*
Jawaban: **Lansweeper fokus memonitor perangkat (asset-based), bukan user activity tracking.**

2. “Apakah tersedia versi terakhir?”

Ya. Versi terbaru disebut dalam wiki bahwa versi terakhir adalah **12.5.6.2**.

Pastikan selalu cek di situs resmi Lansweeper untuk rilis patch/versi terkini sebelum implementasi.



Oke, gini penjelasannya 👇
Pertanyaan **“Apakah tersedia versi terakhir?”** maksudnya adalah:
➡️ **Apakah produk Lansweeper yang kamu pakai itu sudah versi terbaru (latest version) atau masih versi lama?**

💡 **Tujuan pertanyaan ini:**
User ingin tahu:

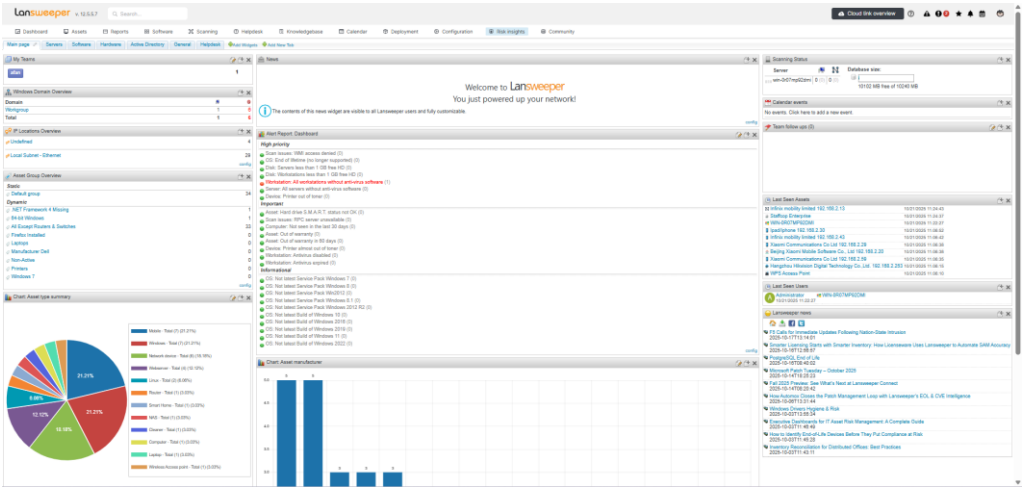
- Apakah **Lansweeper masih aktif dikembangkan** (ada update rutin).
- Apakah **fitur dan keamanannya up to date**.
- Versi berapa yang saat ini **terbaru di situs resminya**.

“Ya, Lansweeper memiliki versi terbaru yang terus diperbarui oleh vendor. Versi terakhir saat ini adalah **12.5.6.2**, dengan berbagai peningkatan fitur dan keamanan. Update bisa dilakukan otomatis maupun manual tergantung apakah kita pakai versi on-premise atau cloud.”

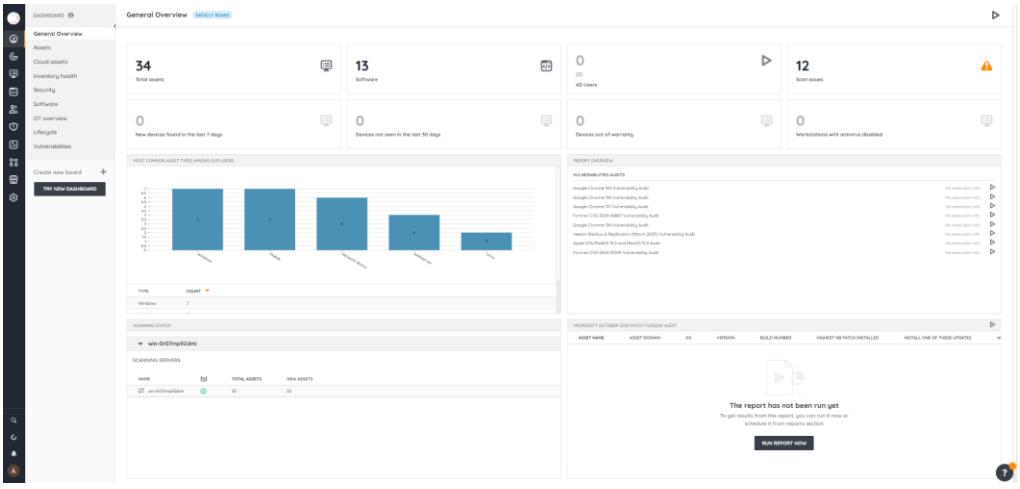
3. “Apakah bisa on-premise / cloud?”

Ya — Lansweeper mendukung dua skenario utama:

- **On-premises**: instalasi internal, database SQL sendiri.



- **Cloud / hybrid**: ada solusi “Sites” yaitu Lansweeper Sites yang memungkinkan manajemen dari cloud.
  – Contoh: Perbandingan antara “Lansweeper Sites” (cloud) dan “Lansweeper On-premises” ada di dokumentasi.
  → Jadi jawabannya: **ya bisa on-premise ataupun cloud**.



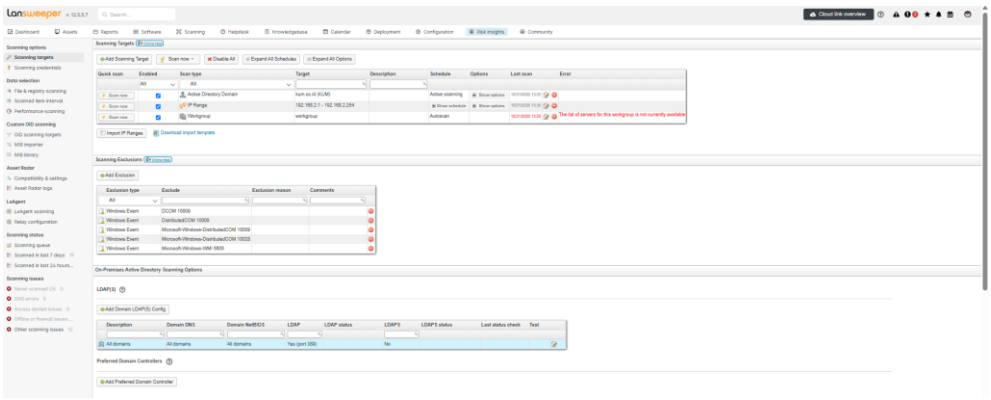
4. “Agentless atau agent-based atau keduanya?”

Keduanya: Lansweeper mendukung **agentless** dan **agent-based** discovery/scanning.

1. Agentless scanning
langsung dari server Lansweeper-nya.
Server Lansweeper akan melakukan **network scan** ke perangkat menggunakan protokol standar:

- **WMI** untuk Windows
- **SSH** untuk Linux/Mac
- **SNMP** untuk network device (switch, router, printer, dll)
- **HTTP/HTTPS** untuk perangkat web-enabled

➡️ Jadi **nggak perlu instal apa-apa di device**.
Cukup kasih Lansweeper akses (IP range & kredensial admin), dia otomatis deteksi hardware, OS, software, IP, user login, dll.



🧠 **2. Agent-based scanning**
ada 2 jenis utama agent-based di Lansweeper:

🟢 **a. LsAgent (modern agent)**

- Bisa di-install di **Windows, macOS, Linux**
- Mengirim data ke server Lansweeper (on-prem atau cloud)
- Cocok buat laptop / PC yang **sering di luar jaringan kantor** (misalnya WFH)
- Komunikasi lewat **internet (port 443, TLS-encrypted)**

🟢 **b. Legacy agent (Lspush)**

- Tools lama, **ngirim data manual atau via file ke server**
- Tidak realtime seperti LsAgent
- Masih bisa dipakai untuk environment tertentu, tapi lebih disarankan pakai LsAgent sekarang.

Agent-based Scanning with LsAgent

TRY NOW

No credit card required

ℹ️ This page discusses LsAgent. If you are working in Lansweeper Sites you now have access to the new IT Agent in preview. For more information check out the preview page, or follow the installation process here.

Discover Hard-to-Reach Devices

Lansweeper usually scans your entire IT environment completely Agentless. However, with networks becoming increasingly mobile and complicated, certain assets become harder to reach. Think for example of laptops out on the road, devices at remote locations or machines in protected zones (DMZs).

LsAgent is a small, lightweight application that gathers data locally from Windows, Mac & Linux devices and sends it back to your Lansweeper installation. It is Lansweeper's answer to increased network mobility and complexity.

Secure and Reliable Inventory

LsAgent helps you keep track of those difficult to scan devices without snagging on credentials, requirements or firewalls. It gathers the asset data locally and then sends it back to your Lansweeper installation.

The data can be sent back either by using a direct push or through Lansweeper's cloud-hosted relay service. The relay encrypts and stores your data in a hyper-secure environment, where your Lansweeper installation can come and fetch it. Get started with LsAgent now and download your installer here.

5. “Jenis server yg bisa melalui Lansweeper?”

➡️ **Server apa saja yang bisa dideteksi, di-scan, atau dimonitor oleh Lansweeper.**
Artinya, mereka mau tahu **apakah Lansweeper cuma bisa untuk Windows Server aja**, atau juga bisa buat **Linux, Mac, virtual machine, cloud server, atau bahkan network device.**

💡 **Penjelasan sederhananya:**
Lansweeper itu **alat asset discovery & inventory**, jadi dia bisa memindai **berbagai jenis server dan device** di jaringan — bukan cuma Windows.

🖥️ **Jenis server yang bisa dideteksi oleh Lansweeper:**

Jenis Server	Dukungan	Keterangan
Windows Server (2008, 2012, 2016, 2019, 2022)	✅	Paling lengkap, bisa scan lewat **WMI**, baca hardware, software, service, patch, user login.
Linux Server (Ubuntu, CentOS, Debian, RedHat, dsb)	✅	Scan via **SSH**, bisa baca hostname, IP, CPU, RAM, storage, package, kernel version.
macOS Server / mac device	✅	Scan via **SSH** atau **LsAgent**.
Virtual Server (VMware, Hyper-V)	✅	Lansweeper bisa integrasi dan baca VM host & guest info.
Cloud Server (AWS, Azure, GCP)	✅	Melalui fitur **Cloud Asset Discovery**, dia bisa tarik data instance dari akun cloud.
Network Device (Router, Switch, Firewall, Printer)	✅	Scan via **SNMP**, bisa baca vendor, model, firmware, port, MAC, dll.

6. “Apakah API possible terbuka?”

💬 **Maksud pertanyaan**
“Apakah API possible terbuka?”
artinya:
➡️ Apakah **Lansweeper punya API yang bisa diakses / digunakan pihak lain** (terbuka untuk integrasi)?
Dalam bahasa gampangnya:
“Apakah data dari Lansweeper bisa diambil atau dihubungkan ke sistem lain — misalnya ke dashboard internal, helpdesk, CMDB, atau aplikasi buatan sendiri — lewat API?”

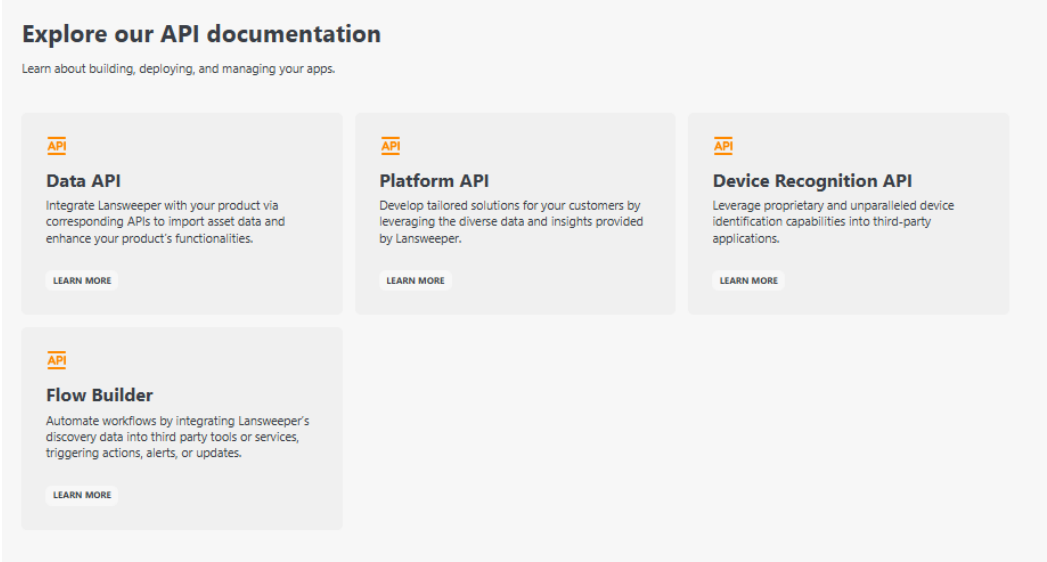
🔍 **Penjelasan teknis singkat**
API (Application Programming Interface) itu semacam **jembatan komunikasi antar sistem**.
Contohnya:

- Kamu punya **sistem helpdesk (misal Odoo, Freshservice, ServiceNow)**
- Kamu mau **otomatis ambil data aset dari Lansweeper** (misal nama PC, IP, OS, user, dll)
  → Nah, lewat **API**, sistem kamu bisa “minta data” langsung dari database Lansweeper tanpa perlu buka manual.

💡 **Jawaban konteks Lansweeper**
Ya, **Lansweeper punya API terbuka**.
Bahkan mereka punya portal developer resmi: developer.lansweeper.com
Jenis API yang tersedia:

1. **Data API** – untuk ambil data aset, software, warranty, dan inventory.
2. **Device Recognition API** – buat identifikasi otomatis perangkat.
3. **Platform API** – untuk integrasi dengan aplikasi lain (misal ServiceNow, Jira, Microsoft Power BI, dsb).

Jawabannya: **Ya, bisa. Lansweeper menyediakan API terbuka yang bisa digunakan untuk integrasi dan automasi data aset.**



🔶 **1. Data API**

➡️ **Fungsinya:**

Untuk **mengambil (read)** data aset dari database Lansweeper. Kamu bisa ambil data seperti:

- daftar perangkat, IP, hostname, OS
- software yang terinstal
- user login
- status warranty atau hardware
- lokasi aset

🧠 Cocok buat:

Integrasi ke dashboard internal, CMDB, Power BI, ServiceNow, atau sistem monitoring lain.

📘 Contoh penggunaan:

GET https://api.lansweeper.com/data/v2/assets
Authorization: Bearer <your_token>

🔶 **2. Platform API**

➡️ **Fungsinya:**

Untuk **mengembangkan solusi yang lebih kompleks dan custom** di atas platform Lansweeper — misalnya bikin aplikasi tambahan, portal pelanggan, atau sistem manajemen aset versi perusahaan kamu sendiri.

Platform API biasanya punya akses **lebih luas** ke fitur internal Lansweeper, bukan cuma data aset.

🧠 Cocok buat:

- Vendor atau developer yang mau bikin produk integrasi
- Perusahaan besar yang mau otomasi alur kerja antar sistem ITSM

🔶 **3. Device Recognition API**

➡️ **Fungsinya:**

Untuk **mengenali jenis perangkat (device identification)** berdasarkan fingerprint, MAC address, vendor, dan atribut jaringan.

Lansweeper punya database raksasa untuk mengenali jutaan jenis perangkat dari berbagai vendor.

Jadi kalau kamu kirim data identifikasi (misalnya: MAC, OUI, atau SNMP sysObjectID), API ini akan kasih tahu **perangkat itu merek dan model apa**.

🧠 Cocok buat:

- Integrasi dengan sistem keamanan jaringan, NAC, CMDB, atau IoT inventory
- Developer yang butuh otomatis deteksi jenis device baru

🔶 **4. Flow Builder**

➡️ **Fungsinya:**

Untuk **otomasi alur kerja (workflow automation)** antara Lansweeper dan sistem lain.

Misalnya:

- Kalau ada server baru terdeteksi → otomatis kirim notifikasi ke Teams/Slack.
- Kalau ada PC belum update Windows → otomatis buat tiket di helpdesk.
- Kalau ada asset tertentu offline → trigger webhook ke sistem monitoring lain.

🧠 Cocok buat:

- Otomasi integrasi antar aplikasi (tanpa coding berat)
- Trigger event & alert otomatis

Kesimpulan singkat

API	Fungsi utama	Contoh penggunaan
Data API	Ambil data aset	Integrasi CMDB, dashboard, report
Platform API	Bangun solusi custom di atas Lansweeper	Portal pelanggan, sistem internal
Device Recognition API	Identifikasi otomatis jenis perangkat	IoT, NAC, asset detection
Flow Builder	Otomasi workflow antar sistem	Trigger alert, buat tiket otomatis

7. “Kalau di cloud apakah data aman dan tidak bocor?”

💬 **Maksud pertanyaannya**
“Kalau di cloud apakah data aman dan tidak bocor?”
artinya:
➡️ *Kalau kita pakai Lansweeper versi cloud (bukan yang diinstal di server lokal / on-premise), apakah data perusahaan kita — seperti nama perangkat, IP, user, software, dll — dijamin aman dan tidak bisa diakses orang lain?*

🧠 **Konteks teknis**
Lansweeper ada dua versi utama:

1. **On-Premise** → semua data disimpan di server lokal kamu.
   Keamanan tergantung kamu sendiri (firewall, backup, enkripsi, dll).
2. **Cloud (Lansweeper Sites)** → data dikirim ke server cloud milik Lansweeper, supaya kamu bisa akses dashboard dari mana saja.

Nah, user yang nanya itu khawatir:
“Kalau data dikirim ke cloud, berarti data perusahaan saya (nama PC, IP internal, user, software, dll) disimpan di servernya Lansweeper. Apakah itu aman?”

🔒 **Jawaban dan penjelasan profesional**
Secara resmi, **Lansweeper Cloud** menggunakan **standar keamanan enterprise**, termasuk:

- **Data terenkripsi** saat dikirim (TLS/HTTPS) dan saat disimpan (encryption at rest).
- **Autentikasi aman (SSO, MFA)** untuk user yang login.
- **Access control**: kamu bisa atur siapa yang boleh lihat aset mana.
- **ISO 27001 certified hosting provider** — artinya infrastruktur mereka mengikuti standar keamanan internasional.
- **Tidak ada akses langsung ke aset di jaringan kamu** — Lansweeper Cloud hanya menerima data hasil scan, bukan remote control ke perangkat kamu.

Jadi secara umum, **aman**, asalkan:

- kamu atur role permission dengan benar,
- pakai password kuat / MFA,
- dan pastikan agent/relay hanya mengirim ke endpoint resmi Lansweeper.

Jawaban: **Ya, aman**, karena Lansweeper Cloud sudah menggunakan enkripsi, kontrol akses, dan standar keamanan internasional seperti ISO 27001.
Tapi tanggung jawab keamanan tetap dibagi dua — sebagian di vendor (Lansweeper), sebagian di pengguna (konfigurasi & akses user).

Security

Lansweeper manages the data of over 20,000 companies worldwide, and with this responsibility, we are committed to providing our customers with the highest standards of security.

We understand our responsibility when you, our customers, entrust us with a significant amount of data. To maintain customer confidence in our security posture and the security features we provide, we work diligently to continuously improve security processes and controls and provide our customers with the highest transparency they need.

Below this page you can request access to our security documentation.

1. Our SOC 2 Type II report
2. ISO 27001 Certification
3. CSA STAR self-assessment
4. Security & Compliance Policies
5. CAIQ Questionnaire
6. Penetration Test Attestation
7. TX-RAMP Certification
8. Security Incident Response Plan
9. NIST CSF 2.0 Mapping
10. Certificate of Insurance

Lansweeper recently introduced the Cloud version of its IT asset management platform, providing a new and enhanced way to know your IT. Lansweeper Cloud features a modern interface, data federation capabilities and API-based integrations that empower distributed multi-location organizations with centralized access to IT asset data.

Using Lansweeper Cloud, you can sync data from multiple local Lansweeper installations to a cloud account for a global view of your organization's IT estate. Customers who deploy Lansweeper Cloud benefit from enhanced security features to protect their IT asset data across multiple sites, including:

- Multi-factor authorization (MFA)
- Single sign-on (SSO)
- Multiple Manager SSO
- Granular permissions and scopes
- The ability to add multiple site owners

In this post we'll take a closer look at each of these features in greater depth.

MFA permissions

MFA helps to increase the overall security of your Lansweeper Cloud site, enhancing data protection by adding a layer of security on top of your login credentials. Administrators who are authorized to configure site settings can set up MFA as a requirement for site access, so that if the credentials of an account are compromised, the site – and the data – remains secure and protected.

You can implement MFA in your Lansweeper Cloud instance in two ways: Enable SSO (see below) or use the built-in MFA configuration provided by Lansweeper. Learn more on how to set up MFA in Lansweeper Cloud.

SSO

Lansweeper provides SSO capabilities so you can centrally manage accounts in your existing third-party authentication system, eliminating the need for your users to have multiple sets of credentials.

SSO enables secure user access and the ability to add or delete accounts from a central location, which comes in handy when someone joins or leaves the company. This also makes it easier to enforce your organization's security policies, simplifying management tasks.

Lansweeper Cloud supports OpenID Connect (OIDC) and SAML for SSO, which means you can use popular SSO solutions such as Active Directory, Google and Okta with your Lansweeper Cloud deployment. Once it's set up, domain users will be able to access Lansweeper using their SSO credentials.

> **You can find detailed instructions on how to set up SSO for your Lansweeper Cloud account here.**

Multiple SSO Managers

Another security feature Lansweeper offers is the ability to add multiple Cloud SSO managers, which is an ideal solution when redundancy is critical. This way, you're not dependent on a single person for managing SSO configuration. This feature removes some of the frustration of limited SSO management capabilities and further strengthens security, while ensuring users have uninterrupted access to their Lansweeper account.

Lansweeper allows for up to 10 managers, who can be named an Admin or an Owner:

- Admins can edit SSO settings.
- Owners can edit SSO settings, add domains, and manage other owners and admins.

Learn how to add multiple managers to SSO here.

Granular permissions

Lansweeper Cloud allows you to define which parts of your site users can access. Additionally, you can define asset scopes to allow specific users to access specific segments of the asset inventory based on the domain, asset type, installation or IP location. Watch this video to learn how to configure granular permissions.

Add multiple site owners to a site

By default, the creator of a Lansweeper site is the only owner of that site. Lansweeper has added functionality to its Cloud offering to enable multiple owners to be added to a site and share the same privileges as the site's creator.

Having multiple owners is important for redundancy purposes – you're not dependent on a single person to manage the site. It's also often a security requirement for enterprise organizations in which multiple people are supporting teams and employees.

With this feature, if an owner is fired from or leaves your company, you can easily continue to manage the site without having to collaborate with that employee or call Lansweeper Support for help. Additionally, you can more easily comply with legislation around data privacy and security.

Find out how to add multiple owners to your site here.

8. “Task management : apakah bisa update Windows?”

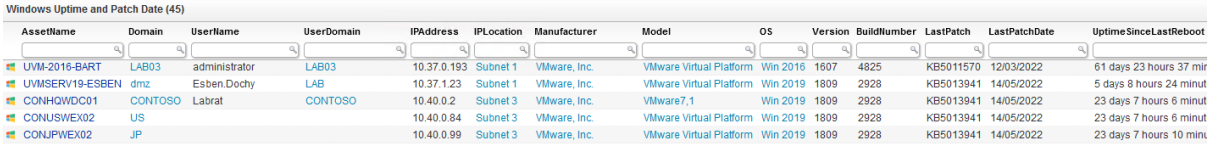
Jadi, pertanyaannya bisa diterjemahkan jadi:
“Apakah Lansweeper bisa menjalankan task untuk update sistem Windows di perangkat yang dikelola?”

💡 **Jawaban profesional:**
Tidak secara langsung.
Lansweeper **tidak berfungsi sebagai patch management tool** atau Windows Update manager.
Tapi dia **bisa mendeteksi status patch/update**, misalnya:

- apakah Windows-nya up-to-date,
- patch keamanan mana yang belum terpasang,
  karena Lansweeper melakukan *scan vulnerability & update status.*

Kalau kamu mau **melakukan update otomatis**, biasanya Lansweeper diintegrasikan dengan:

- **Microsoft WSUS / SCCM**, atau
- **intune / PDQ Deploy / ManageEngine / Atera / NinjaOne**,
  yang memang punya fungsi patching.


Windows Uptime and Patch Date (45)

AssetName	Domain	UserName	UserDomain	IPAddress	IPLocation	Manufacturer	Model	OS	Version	BuildNumber	LastPatch	LastPatchDate	UptimeSinceLastReboot
UVM-2016-BART	LAB03	administrator	LAB03	10.37.0.193	Subnet 1	VMware, Inc.	VMware Virtual Platform	Win 2016	1607	4825	KB5011570	12/03/2022	61 days 23 hours 37 mir
UVMSERV19-ESBEN	dmz	Esben.Dochy	LAB	10.37.1.23	Subnet 1	VMware, Inc.	VMware Virtual Platform	Win 2019	1809	2928	KB5013941	14/05/2022	5 days 8 hours 24 minut
CONHQWDC01	CONTOSO	Labrat	CONTOSO	10.40.0.2	Subnet 3	VMware, Inc.	VMware7,1	Win 2019	1809	2928	KB5013941	14/05/2022	23 days 7 hours 6 minut
CONUSWEX02	US			10.40.0.84	Subnet 3	VMware, Inc.	VMware Virtual Platform	Win 2019	1809	2928	KB5013941	14/05/2022	23 days 7 hours 6 minut
CONJPWEX02	JP			10.40.0.99	Subnet 3	VMware, Inc.	VMware Virtual Platform	Win 2019	1809	2928	KB5013941	14/05/2022	23 days 7 hours 10 minu

Jadi kalau ditanya user:
“Apakah Lansweeper bisa menjalankan task untuk update sistem Windows di perangkat yang dikelola?”
“Ya, Lansweeper bisa mendeteksi dan melaporkan status update Windows (versi OS, build, patch yang terinstall) dengan sangat baik. Namun, jika yang dimaksud adalah **otomatis-push update Windows ke semua perangkat hanya dari Lansweeper**,
maka jawabannya: **tidak langsung secara out-of-the-box** — fitur deployment ada, namun perlu konfigurasi/paket custom agar update Windows bisa dijalankan melalui Lansweeper.”

Fungsi Lansweeper terkait Windows Update:

Kemampuan	Bisa / Tidak	Penjelasan
🔍 **Scan & deteksi status update Windows**	✅ Bisa	Lansweeper bisa lihat versi OS, build number, patch KB mana yang sudah/belum terpasang.
📊 **Bikin laporan update Windows (Windows Patch Level Report)**	✅ Bisa	Ada dashboard & report khusus untuk lihat patch status tiap device.
⚙️ **Menjalankan Windows Update otomatis**	❌ Tidak bisa	Lansweeper bukan patch management tool, tidak bisa push update ke client.
🔗 **Integrasi ke tool patch management (WSUS, SCCM, Intune, dll)**	⚙️ Bisa	Lansweeper bisa kasih data ke tool lain yang meng-handle update otomatis.

9. “Target troubleshooting berapa lama biasanya?”

Nah, pertanyaan **“Target troubleshooting berapa lama biasanya?”** maksudnya begini 👇
User itu sedang **menanyakan estimasi waktu yang dibutuhkan untuk menyelesaikan masalah** kalau ada kendala saat pakai **Lansweeper** — entah masalah instalasi, scanning, agent, database, atau cloud sync.

Jadi intinya mereka ingin tahu:
“Kalau ada error atau problem, biasanya tim kamu atau sistem Lansweeper butuh waktu berapa lama untuk menyelesaikannya?”

🧩 **Tujuan pertanyaan ini:**
Untuk menilai:

- Seberapa **responsif dan cepat support** Lansweeper atau tim IT yang kelola,
- Seberapa **stabil dan mudah di-troubleshoot** sistemnya.

Jenis Kendala	Estimasi Waktu
Agent / scanning tidak muncul	30–60 menit
Error pada koneksi database / service	1–2 jam
Integrasi Cloud / API error	3–4 jam
Kendala berat (misal bug sistem)	1–3 hari kerja (via support resmi Lansweeper)

Lansweeper juga menyediakan **documentation dan support ticket resmi** yang sangat lengkap, sehingga rata-rata issue umum bisa selesai **di hari yang sama**.”