

# HaloITSM

Asset Discovery



# Halo Asset Discovery

Powered by **Lansweeper**

## HaloITSM Asset Management Software - Build your centralised IT Asset Inventory and gain complete visibility across your entire IT estate.

With IT popping up in every shape, anywhere and anytime, the pressure is as high as it has ever been on IT processes to ensure stability, continuity, and productivity for an organization. An asset discovery tool can achieve this by providing complete visibility across your entire IT estate and centralising your whole inventory of IT Assets. This will allow IT managers to be able to make accurate decisions as they are able to rely on data sources which are up to date, organised and complete. Using an effective asset discovery tool in addition to HaloITSM will result in effective management of the IT within the organisation as it will be clear what assets you have to manage.

Rather than collecting IT asset data to meet the criteria of specific IT scenarios, we believe ITAM should be a scenario-independent endeavour, with the goal of creating a single source of truth. Centralized IT Asset Data enables every stakeholder who needs insights into your company's IT landscape to speak the same language. Connecting and centralizing IT Asset Data to collaborate across silos, locations, and departments is essential.



**“Life before HaloITSM was frustrating. HaloITSM is now the keystone to our IT department.”**

- Max Maticchioni, Software Systems and Projects Coordinator, Toowoomba Grammar School.

Create a complete and up-to-date inventory with Halo Asset Discovery. Scan Windows, Linux, Unix, and MAC devices. Find and organise printers, routers, switches and track assets not yet deployed or disconnected from your network. Discover SNMP-enabled devices on your network to create a detailed network inventory.



Get your IT discovery up and running in no time with HaloITSM's advanced scanning methods, and discover your IT without having to install any software on your machines. Eliminate one of the biggest hurdles in IT Asset Management, and save valuable time and resources.



Halo ITSM's Asset Radar detects assets the moment they connect to the network, enabling complete coverage and eliminating blind spots across your IT environment. Combined with our advanced, AI-powered Credential-free Device Recognition technology to recognize and identify these assets, this delivers unmatched inventory accuracy across the entire IT estate — IT, OT and IoT.



Configure your network discovery to match your needs: scan your network by IP range, set critical servers to be scanned, or use active scanning and integrate Active Directory to continuously keep your inventory up to date.



Consider HaloITSM Asset Discovery your single source of truth on hardware, software, and users. Rely on a complete and up-to-date overview to spearhead and support all network-related tasks, projects, and decisions. Analyse your IT and answer questions no one can.



When HaloITSM Asset Discovery scans your Windows-based assets, it will query the WMI service and retrieve most of its information from the framework. Additional information will be retrieved from the Windows registry and also from active directory when using active scanning. When scanning an asset via AD, information like status (enabled or disabled), OU, AD groups, BitLocker recovery key, manager, location, company and more are retrieved.



HaloITSM Asset Discovery scans a Linux or Unix asset through the Secure Shell or SSH protocol. Depending on your Linux distribution, it will run a selection of Linux commands in order to retrieve information from the asset. As long as your Linux distribution can understand the Linux commands as used by HaloITSM, it will be able to capture information from them. When scanning your active directory using active scanning, additional AD information like status (enabled or disabled), OU, AD groups, BitLocker recovery key, manager, location, company and more are retrieved.



HaloITSM Asset Discovery scans Mac computers through the Secure Shell or SSH protocol, similar to other Unix based assets. When you enable SSH, a cryptographic network protocol, HaloITSM can run the system profiler command on the asset. This System Profiler or System Information tool is a software utility which can gather technical data about installed hardware, devices, system settings and more. When Spotlight is enabled, HaloITSM can also retrieve information about the software that is installed on the asset. Spotlight is a system-wide search feature of Apple's operating systems.



Network device management is a manual and bulky process without an automated tool. Apart from scanning Linux, Mac and Windows computers, Halo Asset Discovery is also capable of scanning network devices. This includes cameras, firewalls, mail servers, music systems, NAS devices, printers, routers, switches, UPS devices, VOIP phones and web servers.

HaloITSM sorts scanned devices into categories based on their device type, which is extremely helpful in large and dynamic networks. Locating devices and checking configuration is quite straightforward through a filtered search in the web console.

The exact data returned depends on the protocols enabled on the device, as well as the device type. As a rule, SNMP provides HaloITSM with the most detailed device information. Many network devices have SNMP enabled by default. Each device has its own webpage listing device details such as name, MAC, IP address, vendor, model and serial number. Device specific information includes a complete network interface for switches and routers or toner information for printers. When IP address changes occur, your device entries are simply updated. Annoying duplicates will not clutter your database!

While HaloITSM scans most of the information by itself, editing and adding entries is possible as well. Edit a single asset or change the information for many devices at a time. You can surf to any device's webpage to edit its scan results or submit extra device information such as purchase and warranty date. On top of that, there are up to 20 custom fields that can hold information specific to your organization.

## Brands using Halo Asset Discovery include:



Through integration with Lansweeper, Halo is providing its customers with easy one-click access to detailed, complete and accurate IT asset data, reducing manual tasks while accelerating ticket resolution and enabling self-service capabilities to improve service delivery.

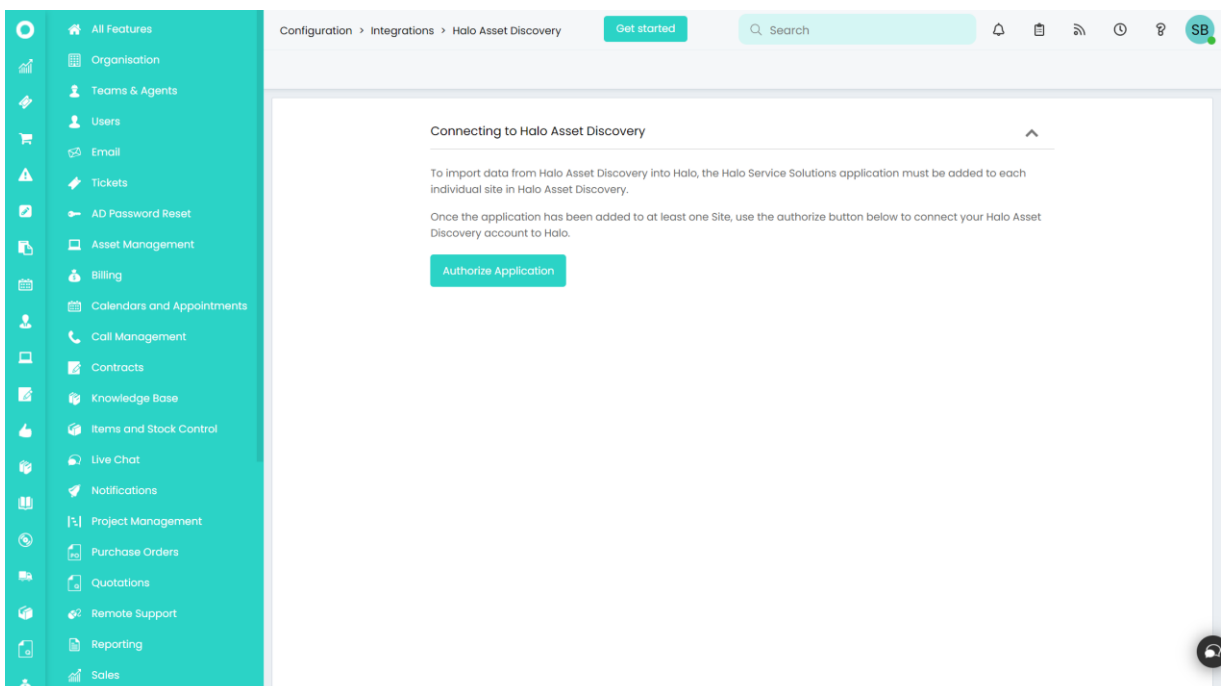
## Benefits of the integration

- Seamless asset discovery pushed into the HaloITSM CMDB
- Supports the development of self-service offerings, lightening the load on Service Desk Team
- Provides an easy-to-use, intuitive interface while supporting complex functionality
- Aligns with ITIL processes “Out-of-the-box” and simplifies data governance
- Easy-to-use and customisable

## General Configuration

To enable the integration in Halo, go to Configuration > Integrations, and enable the ‘Halo Asset Discovery’ module. Once the module has been enabled, click the icon for the module to begin configuring it.

As the integration is based on the cloud version of Lansweeper, all you need to do is authorize the application with your Lansweeper Credentials. Once completed you’ll be able to configure the application to what is required.



The screenshot displays the Halo ITSM user interface. On the left is a teal sidebar with a navigation menu listing various features such as Organisation, Teams & Agents, Users, Email, Tickets, AD Password Reset, Asset Management, Billing, Calendars and Appointments, Call Management, Contracts, Knowledge Base, Items and Stock Control, Live Chat, Notifications, Project Management, Purchase Orders, Quotations, Remote Support, Reporting, and Sales. The main content area shows the breadcrumb path 'Configuration > Integrations > Halo Asset Discovery'. Below this, there is a 'Get started' button and a search bar. The primary heading is 'Connecting to Halo Asset Discovery'. The text below explains that to import data, the Halo Service Solutions application must be added to each individual site in Halo Asset Discovery. It then instructs the user to use the 'authorize button' to connect their Halo Asset Discovery account to Halo. A prominent blue button labeled 'Authorize Application' is centered on the page.

## How Lansweeper can be deployed

After installing Lansweeper, you'll start on our first run wizard. Here, you'll get the chance to configure your admin account and select your first subnet before scanning commences. Once completed, you'll see the assets overview and thanks to our credential-free scanning, your subnets' assets should already be there with basic data.

## Patch Management

Automatically Deploy Software & Patches - With the Lansweeper deployment module, you can create deployment packages that install, remove or update software, perform command line or registry changes and even run custom scripts. Deploy packages any way you want. Customize your deployments to control how, when and on which machines your custom deployment packages are executed. Deploy your packages using different security contexts to either do a silent deployment or user specific changes.

## Agent and Agentless Discovery protocol

Lansweeper is unique in the world of IT discovery solutions. Our software provides you with advanced IT asset discovery and recognition capabilities that leave no room for blind spots. Our software combines active and passive scanning features, both agent-based and agentless, that are supported by powerful AI and CDR functionalities, to instantly discover, scan and centralize asset data. With Lansweeper you can find devices in and outside the company, in hard-to-reach places and from unexpected sources. The scannable assets include Windows, Linux and Mac devices, but also routers, printers, switches, ports, virtual computers and mobile devices.

## Alerting Function

Ensuring that unknown devices -which are far more likely to become a rogue network device- are detected the moment they enter your organization's network is crucial. Lansweeper's Asset Radar continuously scans and sniffs network packets to detect unknown and potential rogue hosts. It operates in real-time, scanning unobtrusively for connected devices. No matter where and when devices join the network, Asset Radar eliminates the possibility of unnoticed transient devices that quickly connect and disconnect in between regularly planned scans. By setting up email alerts, administrators can be instantly notified about the detection of any unauthorized assets.

## Lansweeper Cloud

Lansweeper Cloud extends our industry-leading IT Asset Discovery Software with a modern, cloud-based interface. With Cloud, we build on our best-in-class discovery by enabling data federation and API-based integrations to support multiple IT scenarios throughout your organization.

# HALOITSM - TRUSTED BY GLOBAL BRANDS



At HaloITSM our solution powers organizations across the globe, driving efficient ticket management and enabling our clients to deliver exceptional service levels. HaloITSM is a leading out-of-the-box platform, enhanced by flexible configuration and development delivered by our experienced team in partnership with our clients. Our partners benefit from the commitment and responsiveness that is the mark of our agile team.

The addition of Halo Asset Discovery allows the seamless flow of data between the software and the HaloITSM platform, allowing our clients to have more visibility and control of their IT estate. Further building on the efficiency and productivity already provided by our HaloITSM platform.

We have implemented our ITSM solution for the below clients and more, with ITIL processes and integrations at the core of the solutions we have built.



## Get In Touch

**Company Name**

Halo Service Solutions Ltd

**Product**

HaloITSM

**Primary Contact**

Paige Woolnough

**Primary Email**

Paige.Woolnough@imaginehalo.com

**Primary Phone**

+44 1449 833 111

**Address**

Halo House, 2 Gipping Way, Stowmarket, Suffolk, IP14 1GJ