WHITE PAPER

The Complete Guide to Remote Access

secomea

Table of Contents

The Role of Remote Access

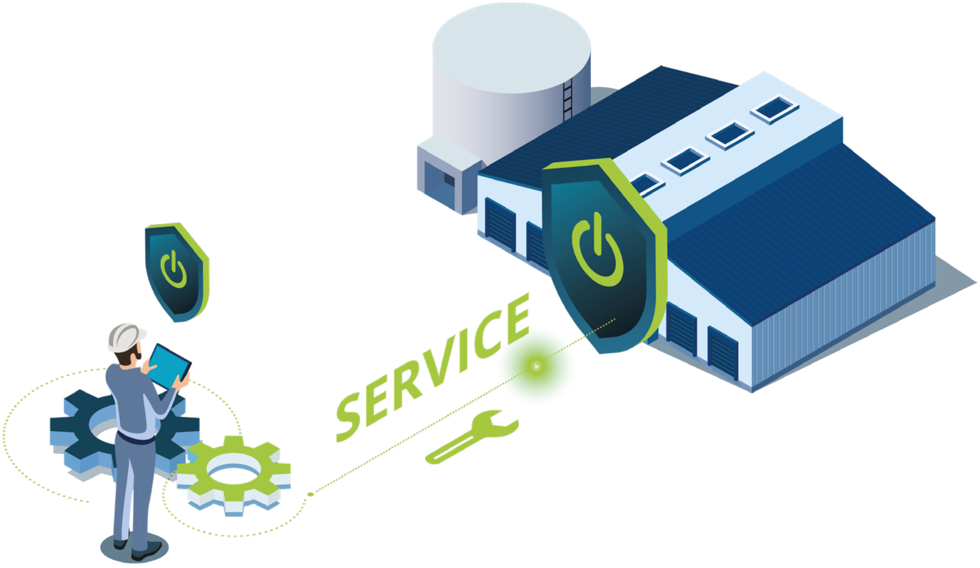
For companies running remote machinery, "safety and security should be paramount in industrial systems to prevent harm and minimize threats to personnel, assets, and the environment." (1)

This is easier said than done. As businesses strive for process optimization, growth, and compliance, the need for a reliable maintenance model grows hand-in-hand. Businesses with intolerant for downtime, such as the medical, metallurgical and food and beverage industries, need maintenance that can react to machine breakdowns in a manner that is safe, expedient, and administratively repeatable.

Why Companies adopt Remote Access to enable Remote Maintenance:

Remote access reduces downtime by digitalizing maintenance tasks otherwise requiring technicians to travel to machinery physically. A study by the university of Dresden notes,
"Remote monitoring leverages available personnel by allowing them to spend more time looking at the condition of the equipment and less time collecting data." (2)

Consequentially, remote access enables technicians to access the status of remote machinery on demand. This access on-demand allows technicians to provide predictive, preventative maintenance before a machine breaks down. Understandably, this shortened turnaround for maintenance tasks leads to less downtime, and increased revenue.



Reducing the impact of Crises:

In 2020 and 2021, the Covid-19 pandemic shocked supply chains across the world, whilst curtailing travel availability. Revenues plunged as business travel declined. The idea of sending an engineer to, for example, board a flight from Germany to service a plant in Chile, became nonviable. Companies reliant on in-person accessibility for off-site talent suffered from project delays, reduced productivity, and increased unplanned downtime.

The pressures of travel lockdowns forced companies to pursue alternatives to manual maintenance. According to studies conducted in Hungary, travel restrictions "had a mostly positive impact on the introduction of Industry 4.0 and industrial digitalization" (3) across sectors. Companies increasingly see remote access as important future-proofing, and remote access is defined as a key component of industry 4.0, under international standard IEC 62443. (4)

All flights cancelled
Bruxelles..............Cancelled
Amsterdam..........Cancelled
Johannesburg.........Cancelled
Oslo........................Cancelled
Copenhagen...........Cancelled

How to Choose a Remote Access System

Interoperability and ease-of-use

Diversity in sites, equipment, staffing and compliance, dictate that an effective that remote maintenance system needs to be adaptable to the needs of the client. Consequentially, "With the trend to just-in-time (JIT) production and flexible, agile manufacturing, it is vital that maintenance management becomes integrated with corporate strategy to ensure equipment availability, quality products, on-time deliveries, and competitive pricing." (5)

Differing remote access products offer a choice of device data collection, directory integration, or remote desktop functionality. Unfortunately, diverse platforms complicate strategic decision-making for OT and IT administrations and technicians alike. Use of multiple tools hampers usability. Consequentially, Companies benefit from remote access products that feature multiple functions on one platform, enabling procedural alignment with corporate strategy through flexible interoperability.

Responsiveness and Security

According to IBM, 95% of workplace cybersecurity incidents start with human error. Common errors include "system misconfiguration, poor patch management, use of default usernames and passwords or easy-to-guess passwords, lost laptops or mobile devices and disclosure of regulated information". (6) With ease-of-operations critical to minimizing incidents, industries managing complex networks need remote access solutions that are expedient to configure, set up, and patch.

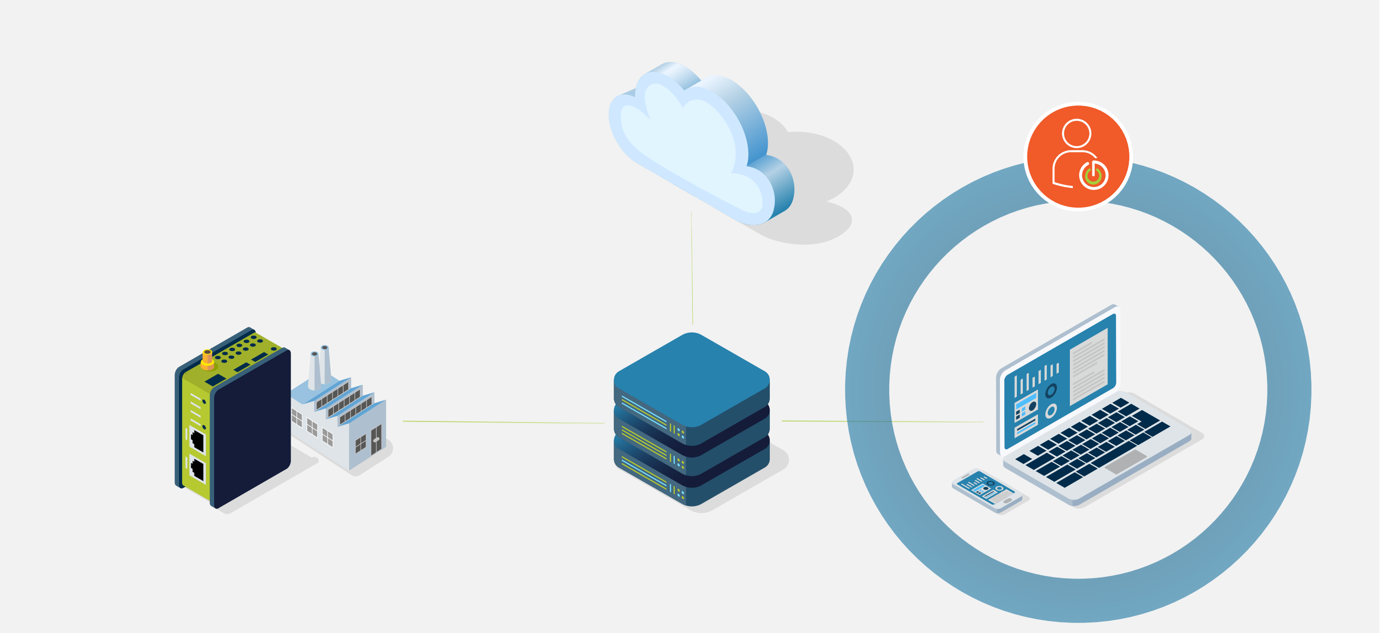
For administrators, a secure remote maintenance platform offers centralized management of endpoints, devices, users, and authentication, on an interface that is easy to operate, reducing the prevalence of human error, and, therefore, improving cybersecurity.

How to Service Machinery With Remote Support

Using Secomea LinkManager

What is LinkManager

LinkManager is the client program technicians use to access machines and services interlinked over a machine operator's Secomea Remote Access network.
The LinkManager client program runs from a dedicated installation on a technician's work PC.



Why do technicians use LinkManager

LinkManager is designed for ease-of-use by industrial service professionals, displaying only pre-provisioned devices and connections. This prevents confusion and minimizes human error, while keeping the accessed network secure.

When a technician logs into LinkManager, they are presented with a list of accessible devices. This list is curated by the device network's administrators, provisioned over the GateManager access server. Therefore, there is no danger of a technician accidentally accessing a device which has not been provisioned for maintenance. All actions made over LinkManager are fully visible to network administrators.

Link Manager enables technicians to service devices listed as agents over a SiteManager IoT Gateway.

Through LinkManager, technicians can securely access device programs, for example, Siemens PLC software, over Secomea Remote Access.

LinkManager is adaptable:

LinkManager supports tunneling of UDP/TCP, USB and Serial connections and Layer2 communication, providing a range of options for remote maintainers.

LinkManager Mobile:

For situations when technicians need to monitor remote hardware on the go, LinkManager mobile enables technicians to remotely access to equipment via a web browser.

When to use LinkManager Mobile:

LinkManager Mobile is designed for accessing the GUIs of PLCs and HMIs. This is useful, for example, for operations monitoring and helpdesk services.

How LinkManager Mobile Works:

LinkManager Mobile's in-browser VNC feature enables desktop connections to the full range of approved devices. All technicians need to get started is a LinkManager mobile account.

How to Equip Machinery With Remote Access

Using Secomea SiteManager

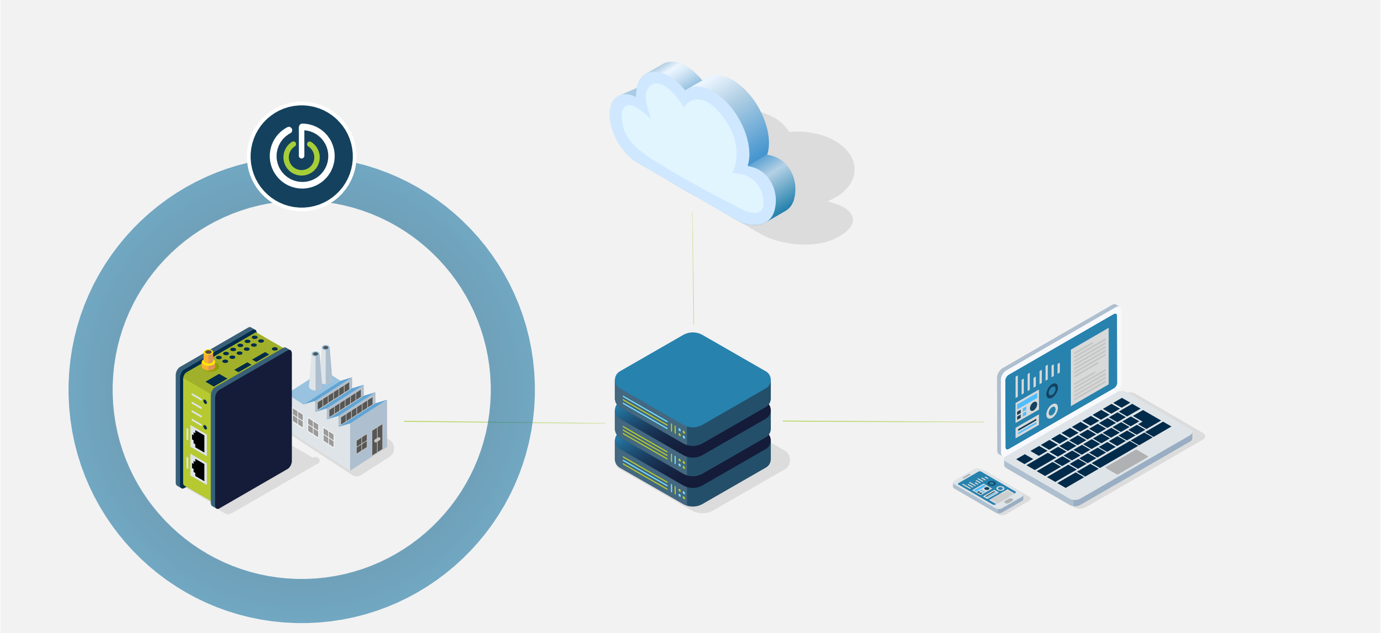
What is SiteManager?

SiteManager is an IIoT gateway that can connect to multiple machines in a plant as a standalone hardware unit, or as run as a software package embedded into a host device.

What can SiteManager do?

SiteManager is designed for the requirements of operational technology environments. Typical IoT gateways function either as a VPN router or as a data collector. SiteManager is a dedicated IIoT (Industrial internet of things) gateway, fulfilling both data collection and routing functions simultaneously.

SiteManager is preconfigured for PLCs, and, consequentially, OT staff can get SiteManager up and running without spending downtime configuring the solution, compromising the factory firewall through port forwarding, or altering the existing operational technology network.



How to connect Machinery with Hardware Gateways:

SiteManager hardware gateways connect up to one hundred machines to the Secomea remote maintenance platform. Machinery can communicate to the SiteManager over most industrial protocols, including ethernet, serial, Modbus and more.

All an engineer needs to set up SiteManager are credentials, a secure connection, and a bundle of cables, or a Wi-Fi connection.

Connecting Machinery with Software Gateways:

Software gateways are alternatives to IIoT gateway hardware.

SiteManager software is optimized for installation onto machinery and thus can run on most platforms. Supported platforms include ARM architectures, like the Raspberry Pi, Docker containers, BeagleBone, or most PCs, Macs, and PLCs.

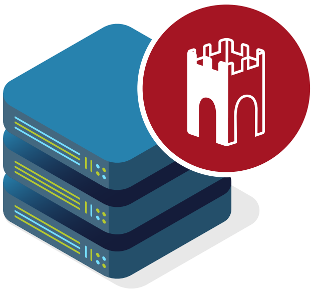
Why companies use Software Gateways:

Software gateways are adaptable, enabling companies to install IIoT gateway functionality to machines in field. Furthermore, software gateways give companies the option for gateway functionality in high-hazard environments that may not accommodate a hardware gateway.

How to Administrate Remote Access

Using Secomea GateManager

What is GateManager:

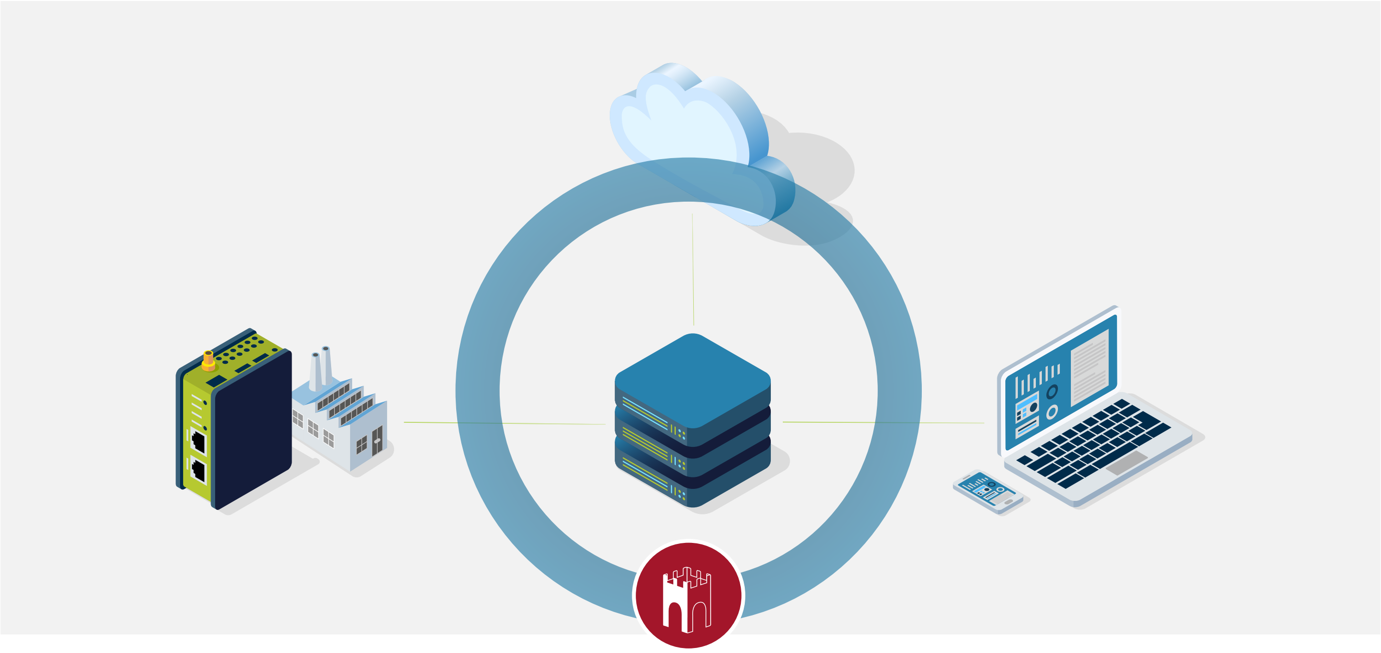


GateManager is range of access and device management servers. GateManager unifies the functions of an Identity Access Management system (IAM) and device management tool, into a single system.

A GateManager server is the infrastructure supporting a Secomea Remote Access system– all connections between the LinkManager access clients, and devices connected a SiteManager Gateway pass through GateManager.

What can GateManager do:

With GateManager, companies' fleet-manage their SiteManager IIoT gateways, along with all connections to remote support and LinkManager clients. Administrators use GateManager to provision activity, manage gateways, log user activity, schedule updates, add, time-gate, or remove remote access users and configure devices.



GateManager is interoperable:

GateManager plugs into a host company's IDM via LDAP, preventing redundant approval processes, while keeping user administration simple.

GateManager enables customizable authentication:

No two industrial networks are the same. Adapting to this need, GateManager can operate as a private server, hosted entirely with a company's own network, from a cloud service, or as a server hosted and maintained by Secomea.

GateManager keeps users accountable:

GateManager generates extensive access logs for all remote access actions made by users and devices. Administrators can set conditional alarms for certain actions, along with download caps.

GateManager is easy to administrate:

GateManager features a simple-to-navigate, browser-based UI. Users do not need an IT education to manage an industrial network with GateManager.

A Platform for Industrial Remote Access

For leading companies, a lack of maintenance access is critically costly, as “the average cost of an hour’s unplanned downtime” averages at around half a million dollars for industrial multinationals. (8). Correspondingly, companies need an expedient remote access solution that is demonstratively reliable.

According to a 2021 study drawn from 502 global businesses using Secomea Remote Access, most participants agree, or strongly agree, that Secomea Remote Access is cybersecure, and easy to get up and operational. (9) This assessment is supported by a cybersecurity audit certificate, which states that Secomea Remote Access is “suited to model and provide hierarchical multi-party communication infrastructure in a secure way” (10).

As of August 2022, over 8000 industrial machine networks use Secomea Remote Access to provision remote maintenance. As the manufacturing industry continues to digitalize towards industry 4.0 compliance, it is likely that this number will continue to grow.

sysadvance®

“Secomea brought us the ability to keep a reliable connection to our client’s plants on a 24/7 base. Having LogTunnel allowed us to build a remote turn-key solution to monitor and operate all our plants around the world„

Read their story here.

Citations

1 **The industrial internet of things (IIoT): An analysis framework**
Hugh Boyes, Bil Hallaq, Joe Cunningham, Tim Watson
Cyber Security Centre, WMG, University of Warwick, Coventry, CV4 7AL, UK
Page 10

2 **http://www.sandv.com/downloads/0805bax2.pdf**
Remote Machinery Monitoring – a Developing Industry Nelson Baxter, ABM Technical Services, Inc., Mooresville, Indiana Heather De Jesús, Azima, Inc., Woburn, Massachusetts,
Page 21

3 **The impact of COVID on the digitization of Hungarian maintenance sector**
L Juhász and L Pokorádi 2022 IOP Conference
Page 4

4 **Applicability of the IEC 62443 standard in Industry 4.0 / IIoT**
Björn Leander, Aida Čaušević, Hans Hansson, ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security, August 2019
Article No.: 101Pages 1–8

5 **“Trends and Perspectives in Industrial Maintenance Management.” Journal of Manufacturing Systems 16.6 (1997)**
Luxhøj, James T., Jens O. Riis, and Uffe Thorsteinsson
Page 437

6 **IBM Security Services 2014 Cyber Security Intelligence Index**
Page 3

7 **The True Cost of Downtime: ‘How much do leading manufacturers lose through inefficient maintenance?’**
Senseye, full document

8 **UserTribe study for Secomea A/S, 2021**
Full document

9 **Protect EM, Industry 4.0 Compliance and Enablement Audit Certificate for the Secomea Remote Access Solution**
Prof. Dr. Peter Fröhlich Prof. Dr. Andreas Grzemba, 2015

secomea