Last updated: January, 2025

INSTALLATION GUIDE

SElink™ | XProtect Essential+ 2024 R1

Prepared by:
Senior Product Leader, R&D Department

Table of Content

Overview

This document serves as an installation manual for integrating ***SElink™*** *with the* ***Milestone XProtect Essential +*** *video management solution. It outlines the key components of both solutions and provides step-by-step guidance on how they work together to form a secure, efficient, and integrated system.*

SElink™ is a versatile and robust solution designed for secure, high-performance networking. It replaces traditional VPNs by leveraging ***Zero Trust Network Access (ZTNA)*** *principles and continuous monitoring to block unauthorized data streams. SElink™ eliminates the need for Public IPs or dedicated SIM plans, simplifying network segmentation without requiring changes to existing infrastructure. By enforcing unidirectional, simultaneous data flows and isolating streams at the application level, SElink™ ensures maximum security while maintaining stability, performance, and availability. Its seamless integration capabilities enable rapid deployment, making it an ideal choice for applications such as IP video surveillance and critical infrastructure. Additionally, SElink™ provides enhanced visibility and auditing features, supporting compliance and accountability requirements.*

This guide covers the following:

- *The components of SElink™ and Milestone XProtect*
- *How SElink™ integrates with Milestone XProtect to enhance security and functionality*
- *Step-by-step instructions for installation and configuration*
- *Best practices for maintaining and optimizing the integrated solution*

While SElink™ is designed to be easy to install and configure, it is important to note proper network preparation and an understanding of the existing network architecture are essential to ensure seamless integration and to fully leverage the capabilities of SElink™. One of the key advantages of SElink™ is its ability to support ***gradual deployment****. It can be applied to specific sections of the network—often the most critical parts—without requiring modifications to the existing infrastructure. Over time, the solution can be extended to additional sections of the network, following a phased roadmap tailored to the organization's needs.*

This guide outlines a specific use case, which may vary depending on the unique requirements and peculiarities of each network. It is intended to demonstrate the simplicity and flexibility of SElink™ integration while highlighting the need for an initial assessment of network requirements to determine the optimal deployment approach. By following this guide, users will gain a clear understanding of how SElink™ can be integrated into their environment, ensuring a secure, efficient, and reliable system tailored to their specific needs.

Copyright, Trademarks and Disclaimers

Licensing

The current integration was executed on a Milestone server running version 2024 R1. However, SElink™ has been extensively tested and validated across multiple server versions, including both earlier and later releases. The integration between Milestone and SElink™ is designed to be version-agnostic, ensuring compatibility without the need for specific version alignment between the two solutions. Below is a detailed list of the software components utilized in this implementation:

	Versions Support Compatibility		
Software Name	Tested Version	Prior Version	Next Version
XProtect Essential+	2024 R1	Any	Any
XProtect Smart Client	2024 R1	Any	Any
XProtect Management Client	2024 R1	Any	Any
SElink™ Gateway	1.2.7	Any	Any
SElink™ Management Suite	1.7.9	Any	Any
SElink™ Agent GUI/M2M	1.8.2	Any	Any

Design

The tested architecture comprised a single server hosting the Milestone VMS, which was interconnected with cameras from multiple manufacturers distributed across various geographical locations. SElink™ facilitated secure communication between the cameras and the Milestone server, leveraging post-quantum encryption to safeguard data in transit and implementing Zero Trust Network Access (ZTNA) principles to manage component accessibility.

This approach significantly strengthened the cybersecurity posture of the architecture, mitigating risks such as traffic hijacking, Man-in-the-Middle (MiTM) attacks, and lateral movement within the network.

The server and select cameras were equipped with an onboard SElink™ agent. For cameras incompatible with direct agent installation, a dedicated device—functioning as an Access Point and running the SElink™ agent—was deployed. While Blu5 supplied the hardware for the Access Point device in this implementation, any compatible device capable of hosting the SElink™ agent could be utilized. This highlights the flexibility and adaptability of the SElink™ solution, which seamlessly integrates into diverse architectures, whether cloud-based or on-premise.

External users accessed the camera streams via the Milestone XProtect Client application, with all connections secured through an SElink™ channel installed on the users' laptops. This configuration ensured end-to-end protection and control over all data flows, including Camera-to-Server and User-to-Server communications.

The SElink™ solution is composed of the following elements:

SElink™ Gateway

SElink™ gateway act as communication brokers, providing software-defined connectivity links to services from any location, endpoint, or access point. Implementing techniques for bandwidth optimization and stable connectivity, tunneling segmentation, secure micro-links, all endpoints appear as a single high-performance WAN. Positioned where servers and services are configured (in the same subnet / LAN or in the Cloud), SElink™ gateways can be implemented in cloud data centers or on-premise and are available as virtual or physical hardware appliances.

SElink™ Agents

The SElink™ agent are available for ***Windows OS, Mac OS,*** *and* ***Linux*** *Operating Systems and can be installed on* ***endpoints*** *and* ***access points*** *alike. The agent allows endpoints/access points to access whitelisted services and applications from any location without relying on unreliable VPN connections. The agent integrates protection mechanisms to achieve cybersecurity resilience against various attacks, including viruses, malware, ransomware, and other vulnerabilities that may originate from the operating systems themselves. It supports Client-to-Server, Server-to-Client, Server-to-Server connections, and also Client-to-Client connections (e.g., for field assistance to client devices, troubleshooting, and maintenance). Network devices/access points do not require a public IP, resulting in reduced operational costs and a smaller attack surface.*
SElink™ Agents are available for ***users (GUI)*** *and* ***unattended devices (Machine-2-Machine)****.*

SElink™ Management Suite

Unified dashboard for managing all SElink™ agents, providing visibility and control over the network, including endpoints and services, bandwidth, and service usage (On-Premise and Cloud). The system is designed to fill in the missing elements that ensure full network visibility. Information is accessible to the administrator and any auditors for continuous network monitoring and reporting activities.
Compatibility with third-party SIEM and SOC systems is planned for the integration of customized reporting. When adding a new device, the administrator can define specific criteria such as the MAC address, device name, and so on. These fields are useful not only for identifying each device but also for preventing any 'unidentified' device from accessing without authorization.

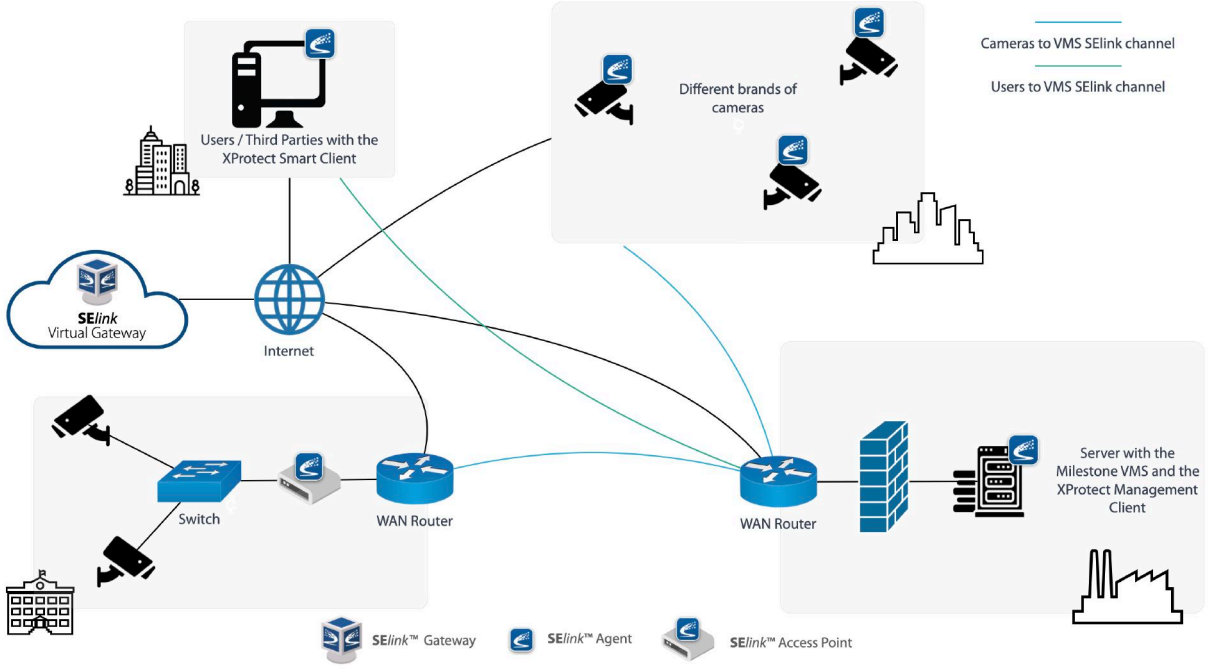
SElink™ Network Configurator

SElink™ is designed to provide a flexible, reliable, and scalable network architecture. Based on a cluster architecture, the Network Configurator is the tool for configuring and managing geographically deployed SElink™ gateways (nodes).

SElink™ Licenses

Endpoint licenses are associated with users or specific devices. Each device/user is assigned a license. Access Point licenses, installed on custom or generic hardware, can manage multiple users and devices. In this case, there is no need for an endpoint license on each individual device or for each user in the network.
The network administrator assigns a valid license to each new user/device in the SElink™ network so that the new user/device can access authorized applications or services. Devices or Access Points without a valid license will no longer be able to access the SElink™ network and services. Different types of licenses are available according to use and Agent installed.

Below is a schematic representation of the architecture:



Requirements and Considerations

The proposed architecture has only one fundamental requirement: SElink™ Agents must maintain communication with the SElink™ Gateway, irrespective of whether the Gateway is deployed in the cloud or on-premises. This is because the Gateway serves as the central broker for all communications within the system. With this single requirement satisfied, a wide range of architectural deployments can be realized, significantly reducing network complexity. Devices equipped with SElink™ can establish communication even with all inbound ports closed, drastically minimizing the attack surface and mitigating the risk of cyberattacks from external threats. Furthermore, since each device operates as a client (SElink™ Agent) connecting to a broker (SElink™ Gateway), it can be physically relocated without disrupting communication with other devices. This flexibility eliminates the need for network reconfiguration and ensures continuous, high-level operability.

Installation

The installation process integrating SElink™ with Milestone XProtect is designed to be simple and user-friendly.

It involves two steps:

1. ***Installation of the SElink™ Gateway:*** *The Gateway serves as the central communication hub, enabling secure and efficient data flow between connected devices and users. It is the core component that orchestrates the SElink™ solution.*
2. ***Installation of the SElink™ Agents on Endpoints/Devices:*** *Agents are deployed on endpoints such as cameras, servers, and user devices to facilitate secure communication with the Gateway. These agents ensure that all data exchanges adhere to Zero Trust principles and are protected by SElink™'s advanced security features.*

The following sections provide detailed instructions for each step, ensuring a smooth and successful deployment of the SElink™ solution within your Milestone XProtect environment.

Installation of the SElink™ Gateway

It can be deployed either ***on-premise*** *or in the* ***cloud****, depending on the customer's specific requirements and network architecture. The installation is performed using a customized image file, tailored to the customer's network specifications, ensuring optimal compatibility and performance.*

Installation of the SElink™ Agent

For ***Windows*** *(Widows 10 and above) and* ***MacOS environments*** *(Mac OS 10.10 and above), executable installation files are provided for both the* ***SElink™ GUI*** *and the* ***SElink™ Management Suite****.*

In cases of IoT devices and Unix environments, ***SElink™ M2M Agents*** *are available. These agents need to be placed on the device and executed via the command line. SElink™ supports the major Windows, Unix, and MacOS releases, and as a fully proprietary solution, it offers the versatility to be installed on custom devices by the company's R&D team. The M2M Agent is available on multiple platforms, such as Windows, Linux, MACOS, Android and on several architectures such as x86, x64, arm32, arm64.*

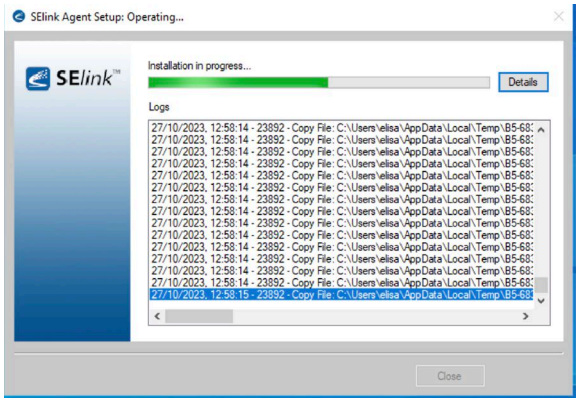
Note on Agent Software Versions
The list of Agent software provided here is not exhaustive. New versions are continually released to incorporate new integrations and improvements. To ensure you have access to the latest version, please always contact your local Milestone Partner.

SElink™ GUI Agent Installation

The system requirements for the GUI include 160MB free disk space, and about 200MB RAM.

Run the executable file to install the SElink™ GUI and then follow the Setup Wizard guided procedure.

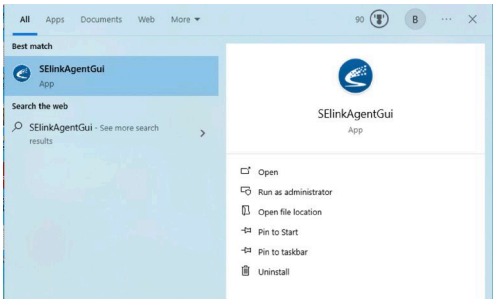
*Read and accept the End User License agreement prior to installing the software. The installation process may require a few minutes. You will see that a green progress bar is advancing, whilst the various files are deployed and the SElink™ service is being created (**Error! Reference source not found.**). You may click on the "Details" button to follow the progress and view the output logs.*



Installation Wizard progress

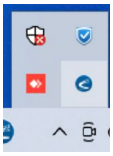
***Note**: In a few cases, it can happen that the SElink™ GUI might depend on standard application modules that are not yet activated on your pc that require a restart. Depending on the missing modules, there is therefore a chance that your pc is restarted in this phase and the installer could be prevented from running automatically. Kindly run the installer again in the event that the installer does not reinitiate the process automatically after a reboot.*

At the end of a successful installation, the Close *button is activated and the GUI Agent is ready to be used.*



SElink™ Agent GUI Windows Application

You may now find the SElink™ Agent GUI *application in the list of your installed applications and the SElink™ GUI icon*  *within the system tray.*



SElink™ GUI- System Tray icon

SElink™ Admin Agent Installation

Installation is easy and straight forward; the user being guided through the procedure by a setup wizard.

Copy the SElink™ installer on your PC and run it to start the guided procedure.

In case a user requires to log on different computers for his daily work, a separate installation of SElink™ is necessary on each computer.

When the installation is completed, the system will prompt you to create an Admin Account. Refer to section "Configuration – SElink™ Admin Agent Configuration" to add a new Admin Account and start making Zero Trust configurations for your SElink™ network.

SElink™ M2M Agent Installation

The system requirements for the M2M Agent include 10MB free disk space and about 32MB RAM.

Connect to the Endpoint and create a folder for the SElink™ Agent. In case of a ***Windows installation****, it is requested that the folder is created as* C:\SElink*.*

In case of a ***Linux installation****, make sure that the folder is in a position where no other applications can erase its contents.*

Two files need to be placed inside the SElink™ *folder:*

- *The* ***M2M Agent****, as appropriate for the operating system. The Agent must be granted administrative privileges*
- *The* ***configuration file****, named* om.b5

The configuration file must include the connection string to the SElink™ Gateway in the correct format: ***hostname:port****. Ensure that the SElink™ Gateway is reachable from the endpoint where the agent is installed.*

For SElink™ services to function, the agent must be running. Upon startup, the agent typically becomes operational after establishing its initial connection to the SElink™ Gateway and completing mutual authentication.

The ***M2M Agent*** *is typically configured as a resident service on the endpoint and set to run automatically at startup. During its first connection to a new SElink™ Gateway, the endpoint is registered by the Gateway.*

A connected agent is capable of automated software updates, which are triggered by server-side updates. Changes to services, ports, synthetic IPs, and ZTNA policies are automatically detected and applied by the agent without requiring manual intervention.

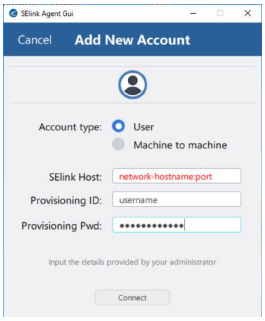
During operation, the agent generates a set of documents and log files within the SElink™ folder. These files contain detailed information about its core functional components (e.g., proxy, gateway, etc.) and can be used for diagnostic purposes if troubleshooting is required for a specific service.

Configuration

SElink™ User/Device Account Creation (GUI)

Upon installation of the SElink™ Agent, you shall proceed to create a user/admin account (called provisioning) to start using the system. Before you start, make sure you have the account information ready. Please refer to your SElink™ administrator for support.

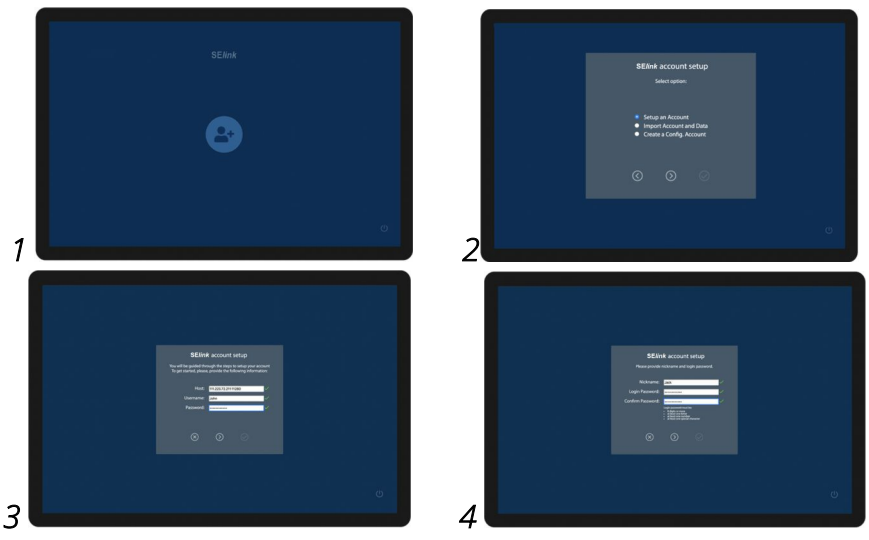
- *How to add a new User:*
  Select the User option. Provide the connection string to the SElink™ Gateway (SElink™ Host). Input the Username and provisioning password and click Connect
  All of this information must be received by your SElink™ administrator
- *How to register a new Device or Access Point:*
  Select a machine-to-machine account (M2M). Only the SElink™ Host provided by your SElink™ Administrator is needed, since the machine account will be automatically identified. Click Connect.



SElink™ User/Device Account Configuration (GUI)

SElink™ Admin Account Creation

Upon installation of the SElink™ Management Suite Agent, the system will prompt to create a new Admin Account. Before you start, make sure you have the account information ready



SElink™ Admin Account Setup – 4 Steps

Upon successful creation of the Admin Account you will be directed to the login page.

SElink™ Admin Account Login

SElink™ Endpoints Configuration

All SElink™ configurations are centrally managed through the ***Management Suite****, a unified control panel accessible via the SElink™ Admin interface. As SElink™ is a transparent and non-intrusive solution, no additional configurations are required on the Milestone side.*

The ***Management Suite*** *serves as the primary interface for system administrators to interact with the SElink™ Gateway. It provides comprehensive capabilities to monitor system status, perform maintenance, and manage SElink™ processes. Key functionalities include:*

- ***Account Creation and Provisioning****: Create and provision accounts for devices and users.*
- ***ZTNA Policy Definition****: Define and enforce Zero Trust Network Access (ZTNA) policies to ensure robust security rules.*
- ***Service Creation****: Establish SElink™ services to enable secure communication between registered devices and users based on predefined policies. SElink™ supports the rapid creation of:*
    - *Client-to-Server*
    - *Server-to-Client*
    - *Client-to-Client*
    - *Site-to-Site services*

  These services require no additional configuration on other network components, ensuring seamless operability and efficiency. Each service features granular controls, with unidirectional traffic flow for enhanced security and control.
- ***Dashboards and Reporting****: Access real-time dashboards and detailed reports for system monitoring and analysis.*
- ***Gateway Status Monitoring****: Continuously monitor the SElink™ Gateway's operational status to ensure optimal performance.*

SElink™ Agents, assigned to specific devices or user accounts, inherit only the configurations explicitly defined for them. In the event of a security compromise, adhering to ZTNA principles, the affected agent is immediately isolated, blocking potential attack vectors and maintaining system integrity, efficiency, and operability.

Optimization

SElink™ does not require any network modifications; it is flexible and capable of adapting to various scenarios without the need for additional actions. When structured correctly, an SElink™ network allows for a reduction in the number of subnets in use, as devices can communicate with each other using localhost or VIPs (virtualized fake IPs). Additionally, it provides a level of segregation and control between devices, even when they are on the same LAN.

SElink™ helps eliminate unnecessary technologies and reduces reliance on costly, layered multi-vendor solutions.

Being SElink™ able to communicate with all inbound ports closed, it does not require public IP addresses. Consequently, the number of network hardware in the network can be reduced since there are no public IPs to protect.

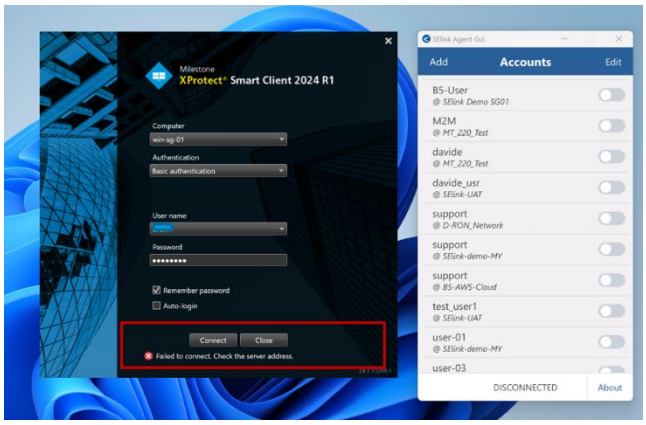
By streamlining infrastructure, it also cuts Capex by minimising hardware sprawl, eliminating the need for expensive dedicated connectivity contracts, and reducing subscriptions to unnecessary security software

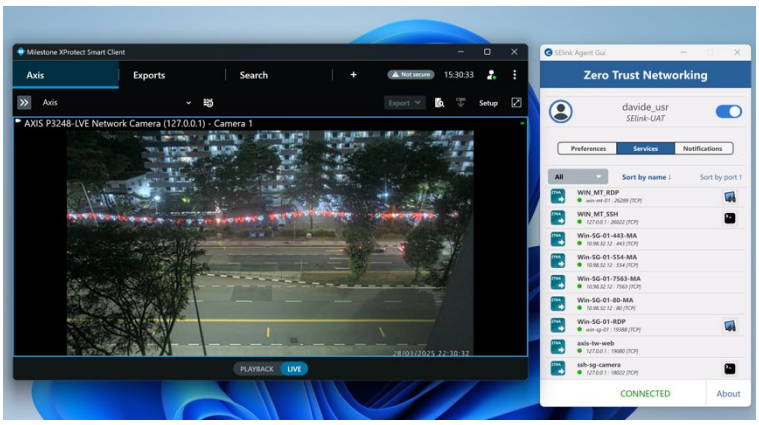
Operations

From an end user's perspective, using SElink™ is simple to learn and operate, with no impact on usability. A SElink™ agent can be configured to activate automatically upon the startup of a laptop/server or can be manually managed by the end user. Once connected to the SElink™ network, the agent automatically updates according to the policies for each specific service assigned to the user, without requiring any action or awareness from them.

Access to services is created only when the user needs to access an external resource, further limiting attack vectors. Controls are performed on each individual service almost in real-time, rather than only at authentication, like other technologies do. This ensures that if, for any reason, a policy is not complied with, the service is interrupted, increasing network control and security.

Below is a practical example:



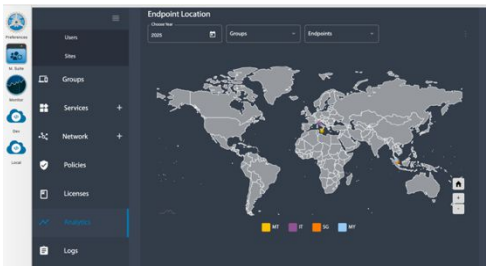


Reducing the need for specialized tools, SElink™ empowers the lowering of cost and time required to train personnel on dedicated systems, improving operational efficiency.

Maintenance

From the Management Suite, administrators can monitor the status of the solution in several ways:

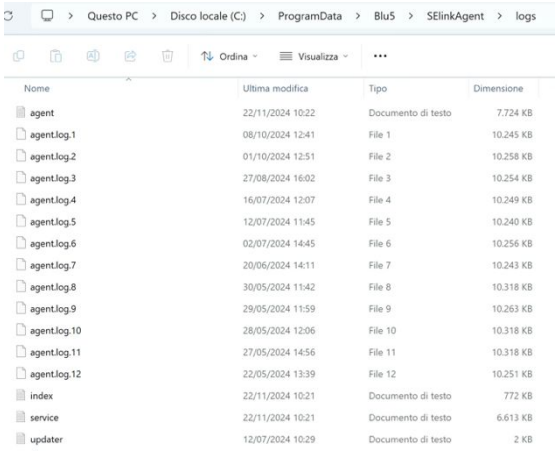
- *Checking the status of server components and their performance from a dedicated panel.*
- *Monitoring the presence of connected endpoints, indicated by a green dot next to the name of a device or user.*
- *Assessing the solution's operability through various analytics dashboards. The results can also be exported as PDF reports for further analysis or sharing.*



Examples of SElink™ Analytics

Troubleshooting

SElink™ manages logs comprehensively across all components of the solution, including both client-side (whether a graphical agent or a command-line agent) and Gateway-side operations. Logs are generated during the use of the solution, but they do not reveal any of the data being transferred. Instead, they consist of various operational files that are crucial for debugging and tracking errors or malfunctions on both the server and client sides.



ABOUT BLU5 GROUP

Leveraging Zero Trust strategies and Secure Virtual Networking principles, Blu5 empowers industries to create secure, manageable, and cost-effective infrastructures that meet dynamic hybrid networking demands. With deep expertise in security architectures, mobile networks, and communications — all based on proprietary intellectual property — Blu5 solutions enable sectors like IoT, Critical Infrastructures, Finance and Banking, Retail, Government, and Space to continuously deliver services and maintain operations, even amidst cyberattacks. Founded in 2007, Blu5 Group has a strong international presence with headquarters in Singapore, an Innovation Centre in Europe, and Manufacturing in the Asia-Pacific. Its expanding Partners' Sales and Support networks, across three continents, scales with the company's growth.

https://www.blu5group.com

ABOUT MILESTONE

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.

https://www.milestonesys.com/partners/technology-partners/technology-partner-finder/

milestone