

FOR EXTERNAL USE

Synergis Cloud Link

Frequently Asked Questions

Synergis Product Group

July 2022

Genetec[™]

Contents

1. What is Synergis Cloud Link?	1
2. What is Softwire?	1
3. What makes Synergis Cloud Link unique?	2
4. What are the scalability benefits of Synergis Cloud Link architecture?	3
5. Does Synergis software directly manage access control system controllers?	3
6. What is unique about the architecture that Genetec proposes?	4
7. Is communication between Synergis Cloud Link and third-party hardware, encrypted?	4
8. How does Synergis Cloud Link gateway help lower the total cost of ownership (TCO)?	4
9. Is Synergis Cloud Link easy to maintain?	5
10. How do Synergis and Synergis Cloud Link ensure maximum uptime and security?	5
Appendix 1 – Synergis Cloud Link scalability table	6

This document is designed to empower customer-facing staff to respond to all possible questions about Security Center Synergis™ architecture and the Synergis Cloud Link gateway. This is an external document that can be used for both new (greenfield) and migration projects.

1. What is Synergis Cloud Link?

Synergis Cloud Link is an intelligent IoT gateway engineered to address the longstanding customer demand for non-proprietary access control. It is an industrial micro-server running Linux and Synergis Softwire integration services. The purpose of Synergis Cloud Link is that it allows organizations to benefit from a wide scale of access control hardware, improve the reliability of access control systems and make them less dependent on connectivity to the access control server.

Now, when customers migrate to the Synergis IP access control system, they can leverage the Synergis Cloud Link gateway to maintain their existing hardware, wiring, and infrastructure while taking advantage of all Synergis capabilities. The device supports non-proprietary access control modules from the industry's most established manufacturers such as HID Global, Axis Communications, ASSAABLOY, Mercury Security, Allegion, SimonsVoss, STid, and others.

2. What is Softwire?

Softwire is the software running inside Synergis Cloud Link. The Softwire integration service is advantageous to be running on this micro-server because having the access control decision processing unit closer to the edge increases the resilience to diverse types of failure, such as network failures or server disruptions.

Softwire is an integration layer that allows us to bridge multiple APIs into a universal interface that is simple to manage. That software layer is decoupled from the main system to allow us to deliver outcomes at a faster rate without being bound to the release of the main solution.

Softwire is not necessarily bound to proprietary hardware, but it relies on peripherals not commonly found on general-purpose servers:

- A combined hardware-watchdog and a battery backup to create resilience to environmental circumstances such as power glitches.
- RS-485 serial ports to communicate to third-party hardware such as readers, wireless locks, and controllers without ethernet capability.

3. What makes Synergis Cloud Link unique?

- Synergis Cloud Link is a new technology gateway that allows on-premises devices to securely connect to Genetec cloud services. It provides an asynchronous and encrypted communication channel to the server. These capabilities are what make the Synergis Cloud Link device so unique.
- Synergis Cloud Link is flexible as it allows users to leverage their current access control infrastructure and upgrade to an IP-based solution thanks to its open architecture. It also reduces the number of IP connections between remote sites and a central site. As technology evolves and cloud adoption in the security industry accelerates, both on-premises and cloud-enabled access control will converge. Synergis Cloud Link bridges the gap between these two systems. Should the customer need a fully cloud-enabled access control device, or a hybrid device with both on-premises and cloud capabilities, they can be confident that Synergis Cloud Link will offer them the flexibility to adapt to their emerging needs.
- Synergis Cloud Link is an intelligent IoT gateway that customers can deploy at all remote sites instead of a server. One of its many embedded features is threat level management, which simplifies customer responses to potential threats. This allows operators to quickly restrict specific areas and activate a threat level state through Synergis.
- Peer-to-peer (P2P) communications between multiple Synergis Cloud Link devices enable communications between devices. Through this connection, end users can leverage global input/output linking and global anti-passback (APB) across devices, regardless of connectivity to the main server¹.
- Genetec controls the logic running within Synergis Cloud Link and the associated software release. As the dependency on third-parties slows down, we can deliver business outcomes to our customers and control the logic closer to the edge.
- Synergis Cloud Link uses strong encryption between remote and central sites through Synergis Cloud Link devices and Synergis servers, and between Synergis Cloud Link devices and third-party hardware. It also increases overall security of your system by reducing the surface of attack for hackers, given that there are fewer devices connected over a WAN or the internet.

¹ P2P communications will be available in Security Center 5.11 in Summer 2022

4. What are the scalability benefits of Synergis Cloud Link architecture?

For small to mid-sized installations, the all-in-one Genetec Streamvault™ Series 300 appliance supports the Synergis Softwire workload. It can manage up to 100 readers and record/decode up to 32 IP or analog cameras on a single device, serving both as a server and a workstation. Therefore, it maintains two levels in its architecture, all while benefiting from an ecosystem of access control hardware.

For larger scale or multi-site installations, Synergis Cloud Link allows users to scale their access control system, locally or at remote sites, to meet customers' growing needs and to benefit from an unmatched choice of third-party access control hardware. Larger sites can leverage a mix of popular hardware from HID Global, Axis Communications, ASSA ABLOY, Mercury Security, Allegion, SimonsVoss, STid, and more. Also, for multi-site deployments, Synergis Cloud Link can be installed instead of an off-the-shelf server to benefit from savings in server hardware and lifetime maintenance. Up to 2,048 readers are supported per Synergis Access Manager server when paired with Synergis Cloud Links. Equipped with native IP and PoE capabilities – and encrypted to provide highly secure network communications – the gateway itself can support up to 256 readers and electronic locks, as well as monitor hundreds of zones and alarm points.

Synergis Cloud Link also brings advanced access control logic closer to the door with functionalities such as global I/O or global anti-passback based on peer-to-peer communications between Synergis Cloud Links. The device can also be leveraged as a gateway to easily secure a connection to the Cloud and provide a hybrid architecture.

5. Does Synergis software directly manage access control system controllers, or is this achieved through Synergis Cloud Link?

Communications with HID Mercury LP controllers are handled through Softwire, which can run on different types of devices. For small to mid-sized installations, customers can deploy the all-in-one Streamvault Series 300 appliance with Softwire firmware embedded to communicate directly to HID Mercury LP controllers, without the need for a Synergis Cloud Link gateway.

For larger deployments, Synergis Cloud Link is better suited as it allows organizations to easily scale across single or multiple locations. Each Synergis Cloud Link supports up to 32 HID Mercury LP panels (or 256 readers). For additional scalability features, please see appendix 1. When the installation calls for a centralized or several decentralized Security Center Synergis servers and devices in remote locations, Synergis Cloud Link acts as a gateway device that consolidates connectivity between HID Mercury intelligent controllers and centralized Access Manager servers.

6. What is unique about the architecture that Genetec proposes?

This is what makes our architecture unique:

- Synergis Cloud Link is an integration entry that centrally manages a variety of third-party intelligent controllers and sensors, allowing customers to mix and match different brands of access control hardware that are often already existing on site. As an intelligent gateway device, it consolidates connectivity between third-party devices and Security Center.
- Synergis Cloud Link is a PoE-enabled IoT gateway, engineered to provide greater flexibility and security with the latest encryption standards. This results in activating stronger encryption between Synergis Cloud Link and Access Manager, as well as between Synergis Cloud Link and third-party hardware.
- Through peer-to-peer communications that are not typically found in traditional door controllers, Synergis Cloud Link ensures connectivity and communication between devices without relying on Security Center. In addition, with P2P enabling global anti-passback, peer appliances can track cardholder movement and coordinate to enforce anti-passback rules across areas and locations. This results in a more secure organization.
- Synergis Cloud Link supports native threat level management capabilities through security clearances, allowing organizations to quickly change the behavior of the system – such as restricting access or locking down an entire facility. This also enables the ability to proactively prepare for handling different scenarios.
- Most high-end controllers have arbitrary limitations such as only supporting a few card formats. However, as our customers grow, so does their cardholder population. They may need additional card formats and to retire legacy card formats. Synergis Cloud Link becomes a perfect solution, as the most popular formats are programmed in the door controllers – and Synergis Cloud Link makes the access decision for the other less-popular formats. The cardholder won't even be bothered by the changes being made in the system.

7. Is communication between Synergis Cloud Link and third-party hardware, encrypted?

Synergis Cloud Link establishes secure communication with all third-party hardware, Security Center, and other Synergis Cloud Link gateways using TLS, up to version 1.3.

8. How does Synergis Cloud Link gateway help lower the total cost of ownership (TCO) of security systems?

Synergis architecture lowers the total cost of ownership by deploying the Synergis Cloud Link gateway as opposed to off-the-shelf servers locally or at remote sites. Users benefit from the upfront savings and reduced server maintenance costs. Moreover, with Synergis Cloud Link, customers avoid the need for periodic operating system (OS) and database updates, anti-virus, and other updates. It enables the customer to move to a truly cloud-based solution, reducing the cost of deployment and maintenance of servers.

9. Is Synergis Cloud Link easy to maintain?

Synergis Cloud Link is an embedded device that offers advanced functionality without the maintenance hassle and cost of a traditional server. Given its small size, there is no need for a server room and associated costs. There are no Windows users, an operating system, or a SQL database to manage. Since it's fully tested in factory, no third-party applications conflict with the core firmware. Customers can update their operating systems with secure packages that are managed centrally through Security Center. Synergis Cloud Link is easily maintained through simple firmware updates that can be run in parallel and only take a few minutes.

10. How do Synergis and Synergis Cloud Link ensure maximum uptime and security?

Synergis Cloud Link ensures maximum uptime and security as it is not the only device in the access control architecture where the offline logic resides. When pairing the intelligent Synergis Cloud link gateway with HID Mercury, Axis Communications, or ASSA ABLOY IP lock hardware, the door logic, including cardholder (credentials), schedules, and access rights are synchronized with these third-party devices – so access control decisions can occur offline.

11. Appendix 1 – Synergis Cloud Link scalability table

Synergis Cloud Link managing	Supported downstream modules	Max readers or locks per appliance
VertX Interface Modules	32 V100, V200, or V300	64 readers
HID Mercury LP controllers	32 Mercury LP Panels	256 readers or Allegion Schlage or SimonsVoss or BEST Wi-Q locks
Axis A1601	30 Axis A1601	60 readers
ASSA ABLOY Aperio	64 ASSA ABLOY Aperio Hubs	64 ASSA ABLOY Aperio locks
ASSA ABLOY PoE and Wi-Fi locks	N/A	128 ASSA ABLOY PoE and Wi-Fi locks
Allegion ENGAGE IP	32 Allegion ENGAGE IP Gateways	200 Allegion NDE or LE or FE410 or BE467F