

# Deploying a managed SCION AS in the cloud supported by Cyberlink and cloudscale

The SCION production network has seen significant growth in recent years. Notable examples of its deployment include the **Secure Swiss Finance Network (SSFN)** [<https://www.six-group.com/en/products-services/banking-services/ssfn.html>] and the **Secure Swiss Health Network (SSHN)** [<https://support.hin.ch/de/scion/scion-technologie/was-ist-der-hvr-mit-scion/>], both of which support critical infrastructure and are tailored to members of their respective ecosystems.

Recently, our team at **ETH Zurich** received exciting news about SCION's expansion into the cloud. In a joint effort, **cloudscale** [<https://www.cloudscale.ch/>] and **Cyberlink** now offer **native SCION connectivity** to the production network for all customers [<https://www.cyberlink.ch/die-scion-cloud>]. This marks a major milestone: Now, anyone can take advantage of SCION's advanced networking features directly from their servers at cloudscale, without being part of a larger consortium.

In this post, we will walk you through the steps we followed to deploy a SCION Autonomous System (AS) in the cloud supported by Cyberlink and cloudscale —exactly as any customer could.

## Your very own SCION Cloud – managed

The first step is to get in touch with **cloudscale and Cyberlink**, who provided us with detailed information about their SCION offering [<https://www.cyberlink.ch/scion>]. As of the time of writing, they support two types of SCION connectivity:

1. **Non-managed SCION access:** This option provides a direct SCION link to Cyberlink's SCION Border Router at cloudscale within the requested SCION ISolation Domain (ISD). Customers choosing this approach are responsible for deploying and managing their own SCION AS services within their **Virtual Data Center (VDC)**.

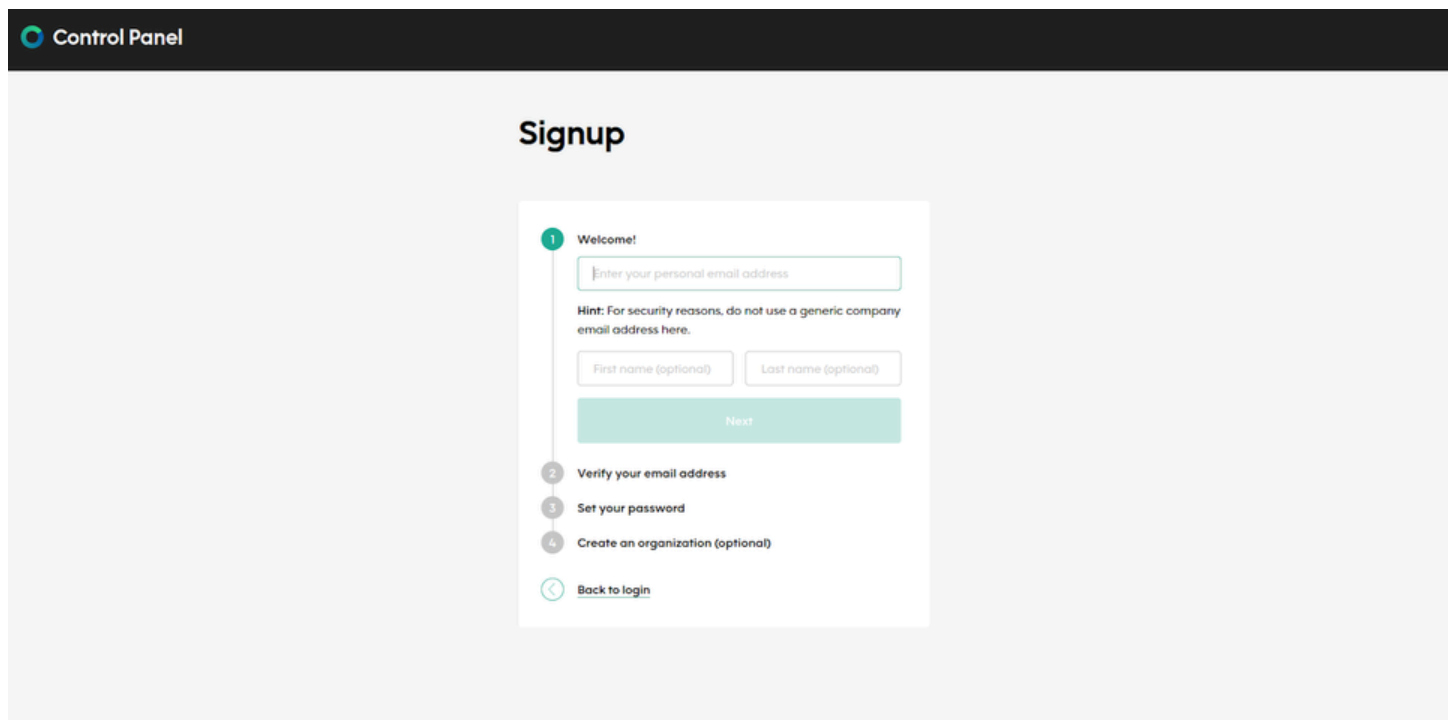
2. **Managed SCION access:** In this setup, **Cyberlink** handles the deployment and management of SCION services on behalf of the customer, offering a more hands-off experience. The managed access makes use of the Anapaya EDGE appliance.

In this post, we focus on the **Managed SCION Access** option, more concretely, on deploying a SCION-enabled endhost within the Managed SCION Access setup. It is particularly well-suited for customers who require performant connectivity and prefer to offload operational overhead. With this approach, customers are not responsible for configuring SCION infrastructure services or managing certificates to keep the SCION AS running.

In a companion post, we explore the Non-managed SCION Access option in more detail.

## Walkthrough

First, we proceeded to create an account and register our organization <https://control.cloudscale.ch/signup>.

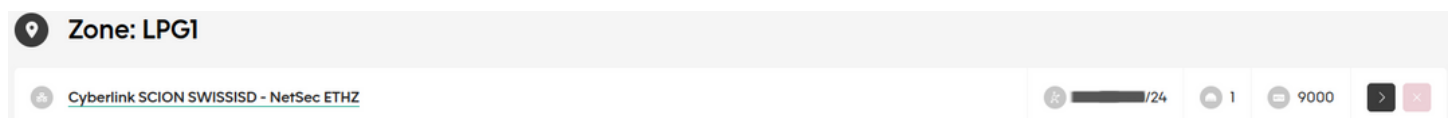


The screenshot shows the 'Control Panel' header in a dark bar. Below it, the 'Signup' section features a multi-step form. Step 1, 'Welcome!', includes a text input for 'Enter your personal email address', a hint about not using generic company emails, and optional inputs for 'First name' and 'Last name'. A 'Next' button is at the bottom of the first step. To the left of the form is a vertical progress indicator with steps 1 through 4: 'Verify your email address', 'Set your password', and 'Create an organization (optional)'. A 'Back to login' link is at the bottom of the indicator.

We created a **project** within cloudscale to host our SCION-enabled Virtual Data Center (VDC).

In parallel, Cyberlink reached out to confirm which cloudscale project should be linked to the SCION access. They also asked if we had any preferences regarding the subnet to be used—specifically, the subnet where we plan to deploy the SCION endhost nodes. By default, Cyberlink assigns a private /24 subnet. Later, we added this private network to the endhost node Virtual Machine (see below).

cloudscale then requested our authorization via email to proceed with linking the SCION access to our project. Once we confirmed, the SCION access appeared in the **Networking>Networks** section of the cloudscale dashboard.



The screenshot shows a dashboard header with 'Zone: LPG1'. Below it, a configuration bar for 'Cyberlink SCION SWISSISD - NetSec ETHZ' is visible. On the right side of this bar, there are several status indicators: a CPU usage bar at 1/24, a cloud icon with the number '1', a message icon with '9000', and a close button with a red 'X'.

With the network details in place, we proceeded to install and configure the first SCION endhost node. To do this, we deployed a **virtual machine (VM)** within our cloudscale VDC. For our setup, we selected the **Flex 4-2** instance type, running **Ubuntu 22.04 LTS**—a recommended operating system for SCION deployments (Ubuntu 22.04 LTS or newer is advised by the SCION implementation guidelines).

The screenshot displays the CloudScale VM selection interface. At the top, there are three tabs: 'Shared vCPUs', 'Dedicated CPU Cores', and 'Dedicated GPUs'. Below these, a grid of VM instance types is shown. The 'Flex-4-2' instance is highlighted with a green 'active' badge. Each instance card lists its memory, vCPUs, and daily cost in CHF, along with a 'Change vCPUs' button.

Instance Type	Memory	vCPUs	Cost (CHF/day)
Flex-4-2	4 GB	2	1.65
Flex-8-4	8 GB	4	3.30
Flex-12-6	12 GB	6	4.95
Flex-16-8	16 GB	8	6.60
Flex-24-12	24 GB	12	9.90
Flex-32-16	32 GB	16	13.20
Flex-48-24	48 GB	24	19.80
Flex-64-32	64 GB	32	26.40
Flex-96-48	96 GB	48	39.60
Flex-128-64	128 GB	64	52.80
Flex-160-80	160 GB	80	66.00
Flex-192-96	192 GB	96	79.20

Finally, we add the private SCION network on the **Network Management** options. The endhost is configured with an address within that range automatically using DHCP.

The screenshot shows the 'Network Management' configuration panel. It includes a 'Public Network Interface' section with checkboxes for 'Enable IPv4' and 'Enable IPv6'. Below this is a 'Private Network "Cyberlink SCION SWISSISD - NetSec ETHZ" (LPGI)' section with a link to 'Attach server to a new private network'.

At this stage, Cyberlink provided the interconnection details for the managed SCION node—specifically, the configuration information required on our endhost.

As of the time of writing, the SCION edge appliance does not support a bootstrapping service for native SCION applications running locally. This means the SCION endhost must be configured manually. Fortunately, the process is straightforward. We're currently working on a seamless and generalizable integration method for SCION endhosts across all existing SCION ecosystems.

We began by installing the SCION endhost stack. You can refer to the official SCION documentation (<https://docs.scion.org/en/latest/manuals/install.html#debian-packages>) to install the necessary components, i.e., `scion-dispatcher`, `scion-daemon` and `scion-tools`.

Next, we downloaded the latest release of the SCION bootstrapperless configuration tool (<https://github.com/netsec-ethz/bootstrapperless-endhost-configurator/releases>). After unzipping the archive, we ran the executable from the command line:

```
██████████@██████████-1:~/endhost-configurator$ sudo ./endhost-configurator
SCION Endhost Configurator
=====

Enter Local ISD-AS number (e.g., 64-1): 64-2:0:a8
Enter Control Service address (IP:port, e.g., 192.168.1.1:30256): 1██████████96:30252
Enter Border Router address (IP:port, e.g., 192.168.1.1:30042): 1██████████96:30042
How many interfaces should be configured? 2
Enter Interface number 1 on the Border Router (e.g., 1): ██████████
Enter Interface number 2 on the Border Router (e.g., 2): ██████████
Generated topology.json from template with 2 interfaces
Copied topology.json to /etc/scion/topology.json
Copied certs directory to /etc/scion/certs

Configuration completed successfully!
Files installed to: /etc/scion
```

We completed the configuration using the interconnection details previously provided by Cyberlink.

Finally, we started the SCION daemon and SCION dispatcher services. To verify connectivity, we used the `scion showpaths` utility, which confirmed that our endhost could successfully retrieve paths to the SCION production network.

```
██████████@██████████-1:~/endhost-configurator$ scion showpaths 64-2:0:9 -n 20
Available paths to 64-2:0:9
# Hops:
[ 0] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 5>34 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 1] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 5>34 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 2] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 6>33 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 3] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 6>33 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 4] Hops: [64-2:0:a8 -- 4>39 64-59414 -- 5>34 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 5] Hops: [64-2:0:a8 -- 4>39 64-59414 -- 5>34 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 6] Hops: [64-2:0:a8 -- 4>39 64-59414 -- 6>33 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 7] Hops: [64-2:0:a8 -- 4>39 64-59414 -- 6>33 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
# Hops:
[ 8] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 3>24 64-15623 -- 8>21 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[ 9] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 3>24 64-15623 -- 8>21 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[10] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 3>24 64-15623 -- 9>22 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[11] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 3>24 64-15623 -- 9>22 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[12] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 7>34 64-2:0:13 -- 31>31 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[13] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 7>34 64-2:0:13 -- 31>31 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[14] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 8>33 64-2:0:13 -- 15>4 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[15] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 8>33 64-2:0:13 -- 15>4 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[16] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 8>33 64-2:0:13 -- 16>20 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[17] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 8>33 64-2:0:13 -- 16>20 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[18] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 8>33 64-2:0:13 -- 31>31 64-559 -- 5>1 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
[19] Hops: [64-2:0:a8 -- 3>38 64-59414 -- 8>33 64-2:0:13 -- 31>31 64-559 -- 6>2 64-2:0:9 --] MTU: 1452 NextHop: Status: alive LocalIP:
```

With just a few simple steps, we've successfully set up a SCION production-ready environment in minutes. This setup enables secure, high-performance connectivity—established within milliseconds—to any entity in the SCION ecosystem, offering reliability comparable to a leased line.

In this post, we focused on deploying a SCION-enabled endhost on the Managed SCION setup. However, SCION unaware applications can also benefit from the SCION connectivity. One advantage of using the managed deployment with the Anapaya Edge is the fact that traditional SCION unaware applications can communicate with other remote SCION unaware applications over SCION-protected communication. In essence, the Edge announces the configured network prefix to other Edges in the SCION network, and if traffic is sent with a destination address that is reachable via this SCION network, then the Edge encapsulates the packet into a SCION packet and sends it over the best path to the destination Edge, where the IP packet is decapsulated and transparently forwarded to the SCION-unaware destination. This setup achieves several advantages over a traditional Internet connection:

- Protection from routing attacks

- Fast failover in case of network outages
- Dynamic path optimization across all available paths to the destination, which can result in a lower-latency, lower-loss, and lower-jitter connection than over the Internet.
- Geo-fencing through path policy definitions on the Edge.

Try it out yourself and experience the benefits of a production-ready SCION environment. Our companion post dives into the **Non-managed SCION Access** setup.

Congrats to cloudscale and Cyberlink for this exciting offering!

About cloudscale:

cloudscale is a leading technology company specializing in cloud infrastructure, with a strong focus on security, performance and scalability. With data centers in Switzerland and ISO 27001 certification, cloudscale supports its customers in meeting compliance requirements.

About Cyberlink:

Cyberlink is a Swiss managed service provider based in Zürich that specializes in the development and provision of state-of-the-art IT solutions. Cyberlink's core competencies are innovative cloud solutions, site interconnection and customized business Internet solutions.