Network tunnels

Network endpoints within the edge installation can be accessed over the internet using Homegear Cloudconnect and C1 Proxy. HTTP, HTTPS and SSH endpoints are supported at the moment. They can be exposed with or without using Sensaru Cloud's authentication.

Cloudconnect configuration

At the bottom of `/etc/homegear/cloudconnect.conf` you can configure network endpoints you want to access over the cloud. All endpoints are accessed using `https://edge.sensaru.cloud` (on port 443). To be able to access different clients, every client has an index assigned which needs to be specified when edge.sensaru.cloud is opened. When no index is specified, index 1 is used.

An example configuration might look like this:

```
[My client]
clientIndex = 2
clientHost = 127.0.0.1
clientPort = 7892
clientSsl = false
clientVerifyCertificate = false
```

A client configuration always starts with the name of the configuration in square brackets. `[My client]` in this case. The name itself can be anything. Just the square brackets are mandatory.

The following parameters are available:

Parameter	Optional	Description
`clientIndex`	no	The index described above. Indexes from 1 to 9999 (inclusive) require the user to be authenticated within Sensaru Cloud (typically using OAuth, i. e. Sensaru Cloud's login page). Indexes from 10000 to 19999 (inclusive) do not require authentication. They can be accessed directly but require some GET parameters for routing information.
`clientHost`	no	The host to forward the requests to. Can be any network device that is reachable from the edge client - even hosts in the internet. IPv4 and IPv6 are supported.
`clientPort`	no	The port to forward the requests to.

Parameter	Optional	Description
`clientSsl`	yes	Set to `true` when the endpoint requires TLS encryption (e. g. for HTTPS)
`clientVerifyCertificate`	yes	Especially local network devices often do not have valid certificates. Set `false` to disable certificate verification for the connection to the specified network endpoint.

Warning

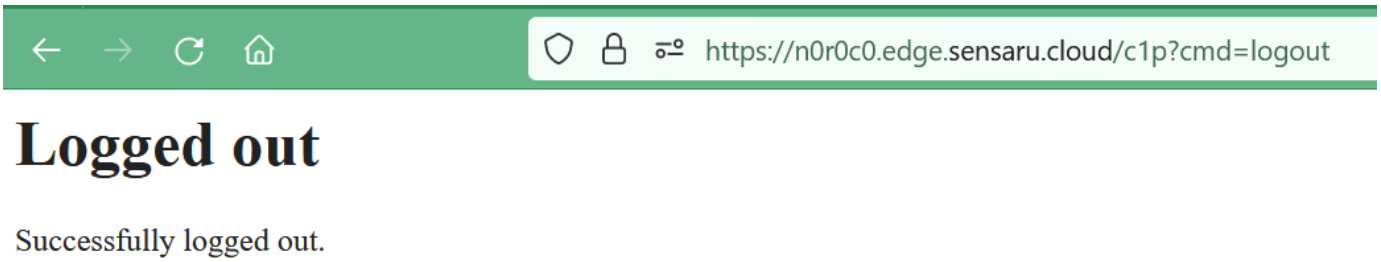
When using client indexes from 10000 to 19999 make sure, the endpoint itself has some form of secure authentication. Otherwise it can be openly accessed by anybody.

Generic commands

Generic commands are executed by accessing the path `/c1p` on edge.sensaru.cloud. The only command right now is `cmd=logout` which is passed as a query parameter:

```
https://edge.sensaru.cloud/c1p?cmd=logout
```

This command destroys the session within C1 Proxy (not in C1 Auth!).



Access web pages

With Sensaru Cloud's login form

Cloudconnect configuration

To access webpages with Sensaru Cloud's authentication, a client index between 1 and 9999 (inclusive) must be used. An example configuration might look like this:

```
[My web page]
clientIndex = 4
clientHost = 192.168.178.12
clientPort = 80
```

When TLS (HTTPS) is used, it might look like this:

```
[My web page]
clientIndex = 4
clientHost = 192.168.178.12
clientPort = 443
clientSsl = yes
clientVerifyCertificate = false
```

When the web page has a valid certificate, use a configuration looking like this:

```
[My web page]
clientIndex = 4
clientHost = my-webpage
clientPort = 443
clientSsl = yes
clientVerifyCertificate = yes
```

Note

The internet part of the connection is always encrypted, regardless wether encryption is used locally or not.

Access the web page

To access the web page with authentication a few parameters must be passed to select the client to access and to set the correct principal for the login page:

Parameter	Optional	Description
`c1pdeviceid`	yes	The device ID to access (e. g. `5628.102.1`). Normally consists of economic unit ID, property ID and administration unit ID seperated by dots. For edge clients associated to buildings and not administration units, just omit the administration unit ID including the leading dot. For edge clients associated to economic units, just specify the economic unit ID without any dots. This parameter only has to be set when logging in as a system provider, system distributor or business partner user, because these user types do not have an associated edge client.

Parameter	Optional	Description
`c1psubid`	yes	The sub ID of the client. Only used when there are multiple clients with the same device ID. Defaults to `1`. This parameter only has to be set when logging in as a system provider, system distributor or business partner user, because these user types do not have an associated edge client.
`c1pusp`	no	The system provider ID of the logged in user. Required to preselect the correct principal on the login page.
`c1pusd`	no	The system distributor ID of the logged in user. Required to preselect the correct principal on the login page.
`c1pubp`	no	The business partner ID of the logged in user. Required to preselect the correct principal on the login page.

To access the webpage, use the following URL:

```
https://edge.sensaru.cloud.com
```

For all client indexes other than 1, the index needs to be specified:

```
https://edge.sensaru.cloud/?c1pclientindex=4
```

Without Sensaru Cloud's login form

Warning

The web page specified here mandatorily must implement authentication by itself. Otherwise it can be accessed by anybody over the internet!

Cloudconnect configuration

To access webpages without Sensaru Cloud's authentication, a client index between 10000 and 19999 (inclusive) must be used. An example configuration might look like this:

```
[My web page]
clientIndex = 10002
clientHost = 192.168.178.12
clientPort = 80
```

When TLS (HTTPS) is used, it might look like this:

```
[My web page]
clientIndex = 10002
clientHost = 192.168.178.12
clientPort = 5001
clientSsl = yes
clientVerifyCertificate = false
```

When the web page has a valid certificate, use a configuration looking like this:

```
[My web page]
clientIndex = 10002
clientHost = my-webpage
clientPort = 5001
clientSsl = yes
clientVerifyCertificate = yes
```

Note

The internet part of the connection is always encrypted, regardless wether encryption is used locally or not.

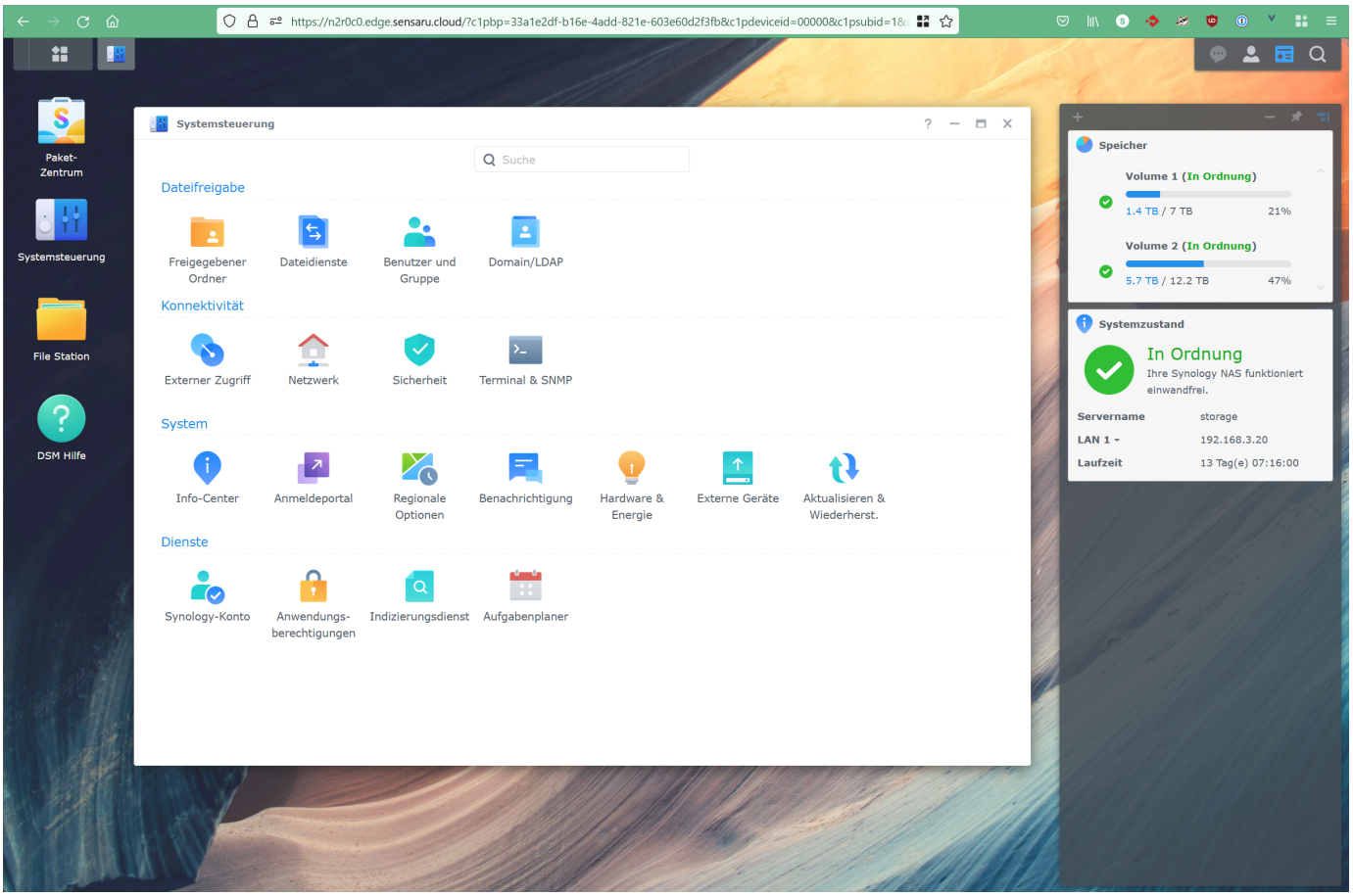
Access the web page

Parameter	Optional	Description
`c1pclientindex`	no	The client index to access.
`c1pbp`	no	The business partner ID the edge client is associated to.
`c1pdeviceid`	no	The device ID to access (e. g. `5628.102.1`). Normally consists of economic unit ID, property ID and administration unit ID seperated by dots. For edge clients associated to buildings and not administration units, just omit the administration unit ID including the leading dot. For edge clients associated to economic units, just specify the economic unit ID without any dots.
`c1psubid`	no	The sub ID of the client. Only used when there are multiple clients with the same device ID. Defaults to `1`.
`c1pcreatecookie`	no	Setting this parameter to `true` or `1` creates a session. Always required when accessing web pages.

So an example URL might look like this:

```
https://edge.sensaru.cloud/?c1pbp=c1-ssh root@33a1e2df-
b16e-4add-821e-603e60d2f3fb_00000_1_10000&c1pdeviceid=00000&c1psubid=1&c1pclientindex=10002&c1pcr
```

Like this you can for example access Synology's DSM over Sensaru Cloud:



Access APIs

APIs normally do not load additional content and do not use redirects. They are typically accessed using client indexes between 10000 and 19999 to circumvent authentication. In this case no session needs to be created (and shouldn't). To access these APIs follow the instruction for web pages but set `c1pcreatecookie` to `0` or `false`. If you are unsure if that works, just try it out. If it does not work, you can still reenable the session cookie.

SSH and SCP

An example configuration to expose SSH over Sensaru Cloud looks like this:

```
[SSH]
clientIndex = 10000
```

```
clientHost = ::1
clientPort = 22
```

To access this SSH endpoint the tools "c1-ssh" and "c1-scp" must be used. See the SSH section.

Access other protocols

Homegear Cloudconnect and C1 Proxy can tunnel pretty much all TCP connections. To do that, the following must be done (programatically):

1. Open a socket connection and send a `GET` request to edge.sensaru.cloud using `c1pclientindex` (10000 to 19999), `c1pbp`, `c1pdeviceid` and `c1psubid` and additionally pass the query parameter `c1pproxymode` set to `true` or `1`. `c1pproxymode` makes C1 Proxy and Homegear Cloudconnect keep the socket connection open and bidirectionally pass through anything that comes in.
2. The first response you get is a 302 redirect. Close the first socket connection and open a socket connection to the redirect URL. Send the `GET` request again. Set `Connection: keep-alive` in the HTTP header.
3. Read the HTTP response and check for response code `200`. `200` is returned on success, all other response codes are returned on error (`503` when the specified edge client was not found or is not connected).
4. Do not close this socket connection.
5. Now the tunnel is open and you can initiate TCP communication (including TLS-encrypted communication) with the underlying service.