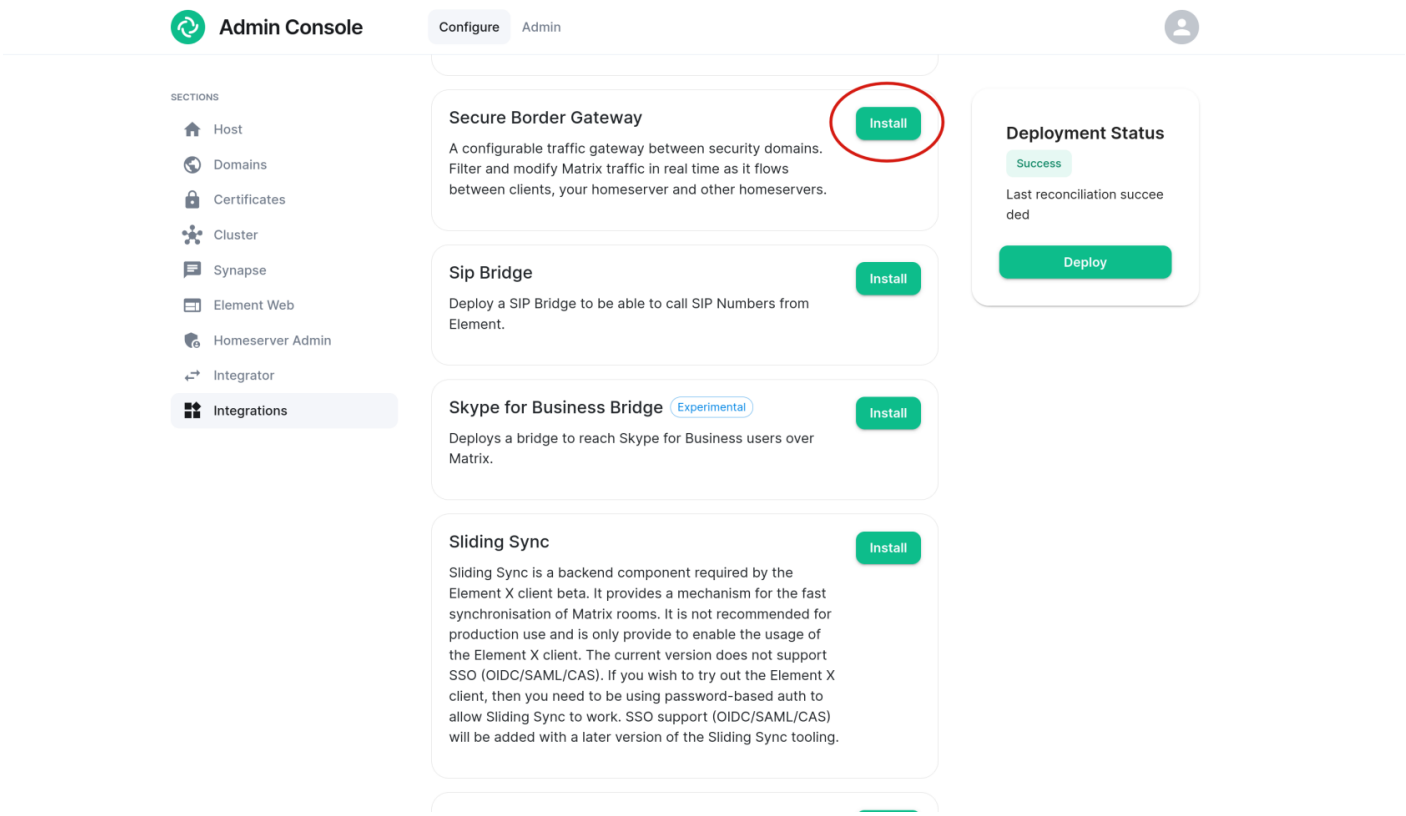
The Secure Border Gateway

The Secure Border Gateway (SBG) is an HTTP proxy designed to filter and analyze Matrix traffic between both clients and the homeserver, as well as between the homeserver and other federating homeservers. This guide outlines the key functionalities and configuration you need to be aware of when using the SBG.

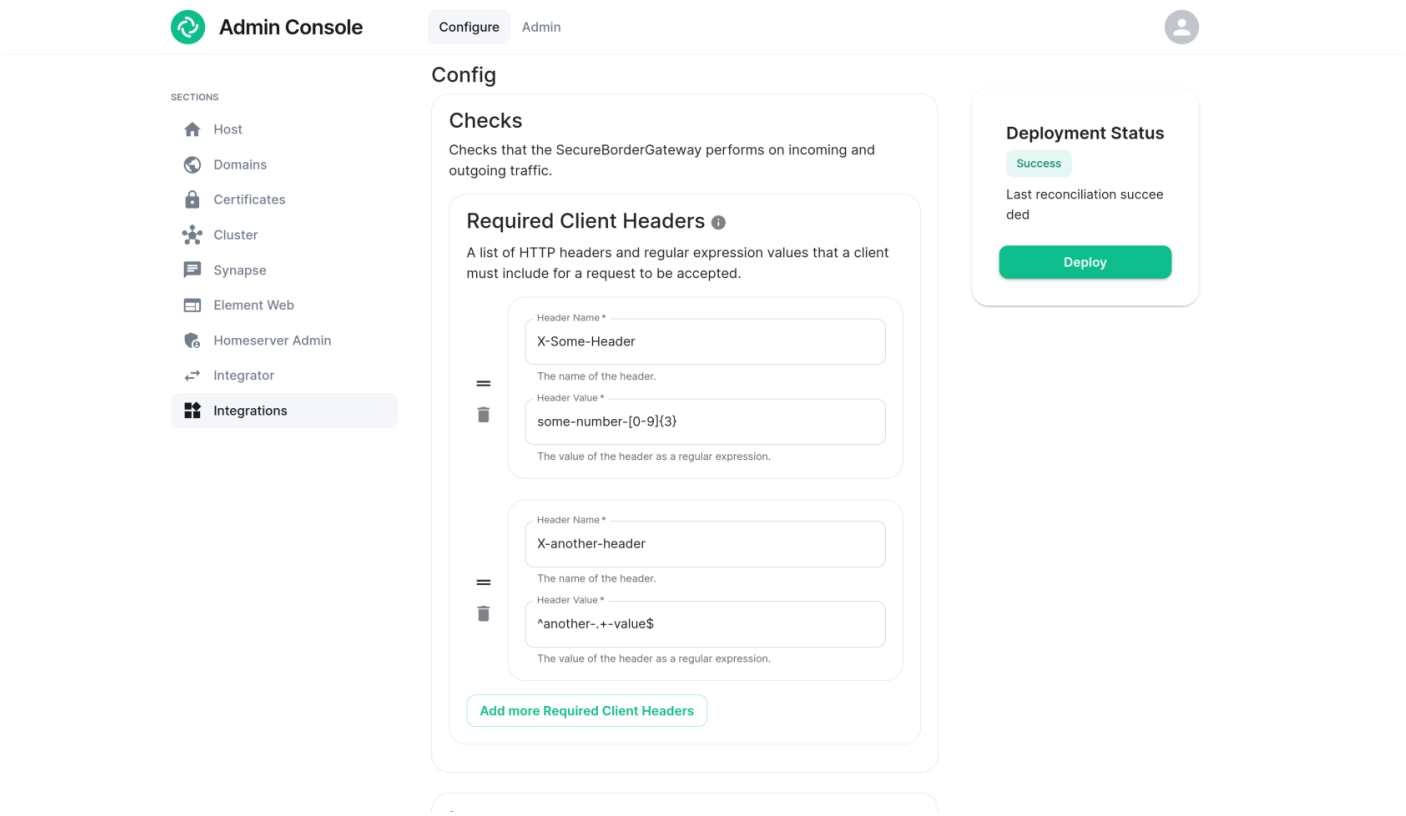
Enable the Secure Border Gateway



On the Integrations page, locate the Secure Border Gateway add-on and select `Install`. Once installed, you can access its configuration.

Configuration

Required Client Headers

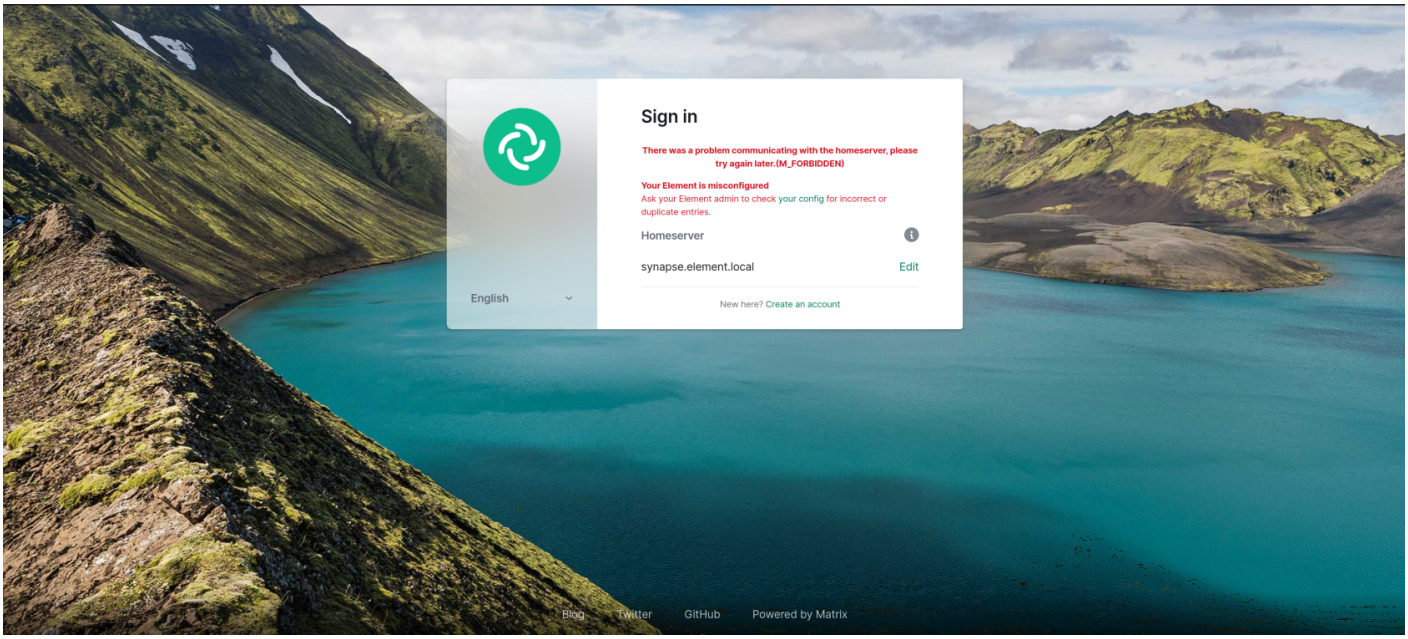


A set of headers can be configured such that a Matrix client must supply *at least one* of in order to access the homeserver.

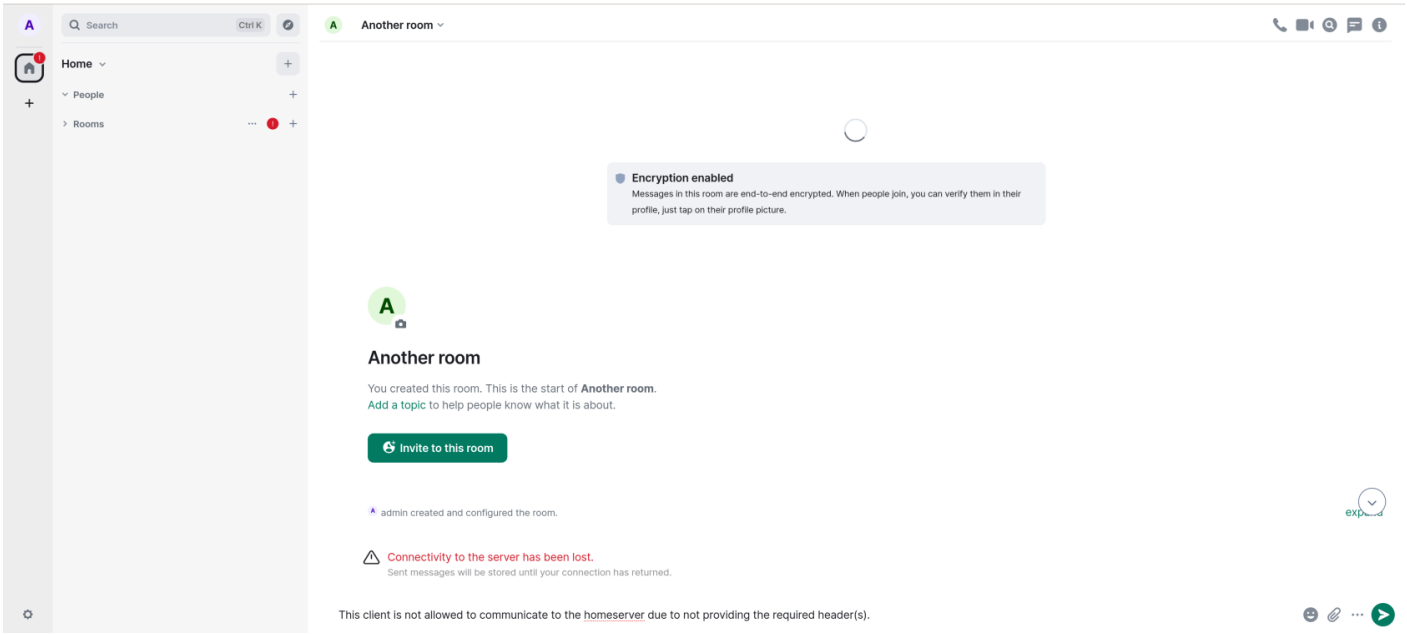
For each header, enter the name of the header (case-insensitive) and a regular expression pattern that the header's value must match.

If a client does not supply the appropriate headers in a request, that request will be rejected with HTTP status code 403, and a standard Matrix error response with `errcode` field `M_FORBIDDEN`.

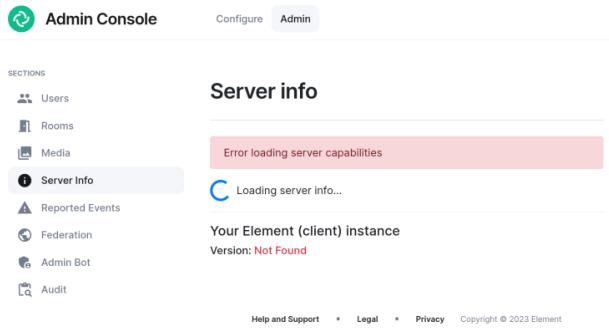
A header name that is stripped by the SBG should not be used as a required client header. Otherwise no client will be able to access the service. For example, an Element Web client that does not supply the appropriate headers will see the following when attempting to log in:



or if they are already logged in when the check was enabled:



Once any required client headers are defined, both the included Element Web instance and the "Admin" tab of the ESS Installer will not be able to connect to the homeserver, as they will not provide the appropriate client header. You may see the following under the ESS Installer Admin tab:



If no header entries are defined, this option has no effect.

Header Stripping

For each incoming request, the SBG will strip all request headers other than the following:

- Any header beginning with `X-`
- `Content-Type`
- `Authorization`
- `User-Agent`
- `Accept`
- `Accept-Language`
- `Host`
- `Access-Control-Request-Headers`
- `Access-Control-Request-Method`
- `Cookie`

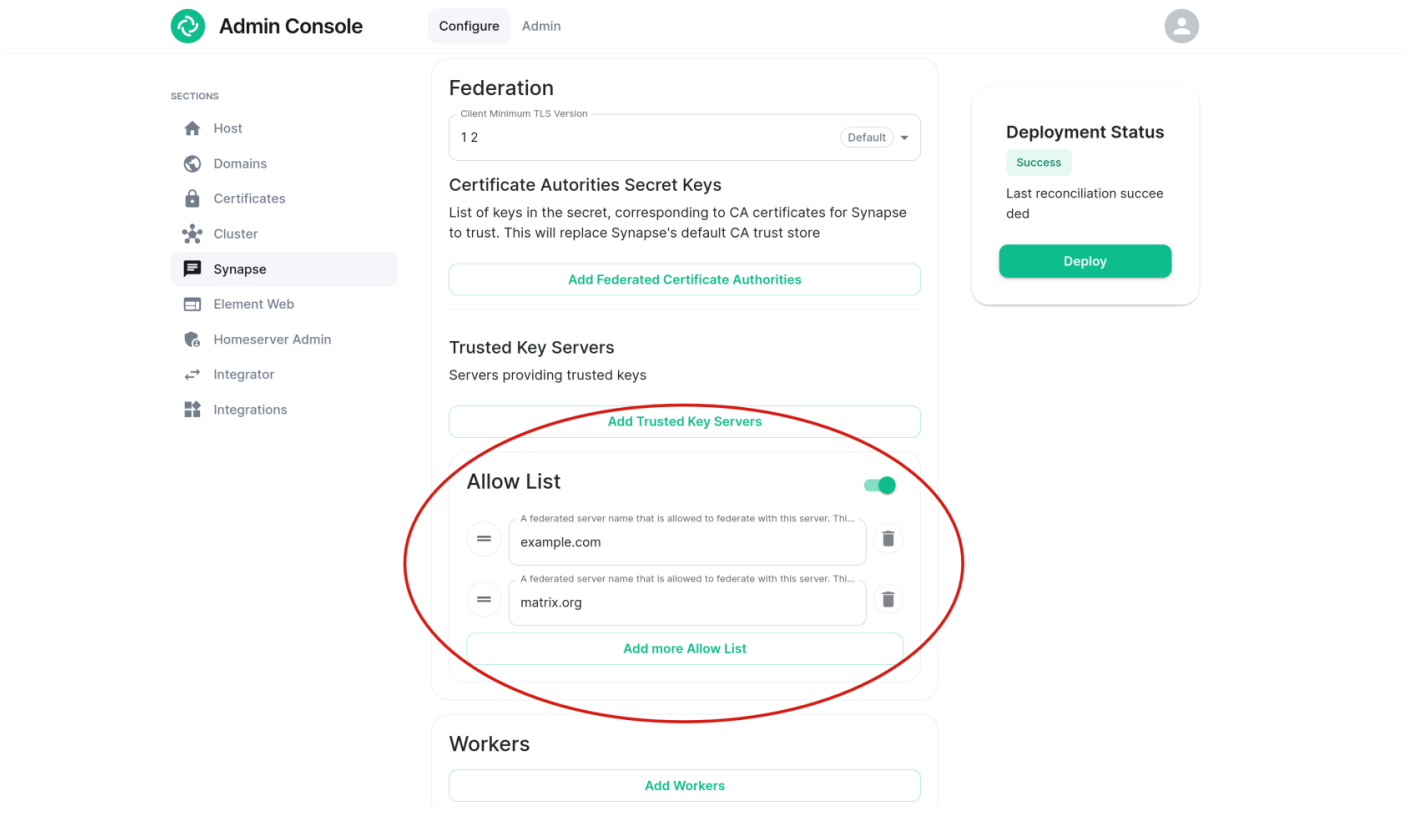
If making use of the Required Client Headers feature, be sure not to use a header name that isn't on the above list.

Similarly, the SBG will strip all response headers other than the following:

- Any header beginning with `X-`
- `Content-Type`
- `Content-Disposition`
- `Access-Control-Allow-Credentials`
- `Access-Control-Allow-Headers`
- `Access-Control-Methods`
- `Access-Control-Allow-Origin`
- `Access-Control-Expose-Headers`

- `Access-Control-Max-Age`
- `Date`
- `Cache-Control`
- `Strict-Transport-Security`
- `Set-Cookie`

Private Federation Enforcement



If you have configured a Federation Allow List in Synapse settings, the SBG will similarly enforce this private federation.

Homeservers that are not on the configured allow list will receive a HTTP status code `403` and a standard Matrix error response with `errcode` field `M_FORBIDDEN`. This adds an extra layer of protection, preventing outside traffic from even reaching the Synapse process.

The SBG determines whether a request from a remote homeserver is allowed based on the `Authorization` header that is included in the request. For incoming requests, it checks that the `origin` field matches one of the allowed remote server names. It also checks that the `destination` field matches the local server name.

Note that `destination` is an optional field in the Matrix Federation spec, and was only added in Matrix v1.3. Thus, your deployment will not be able to federate with older homeserver versions (Synapse <1.58) if a Synapse federation allow list is configured.

If an `Authorization` header is not present at all in the request, then that request will be blocked. There are some exceptions that are necessary for federation to function:

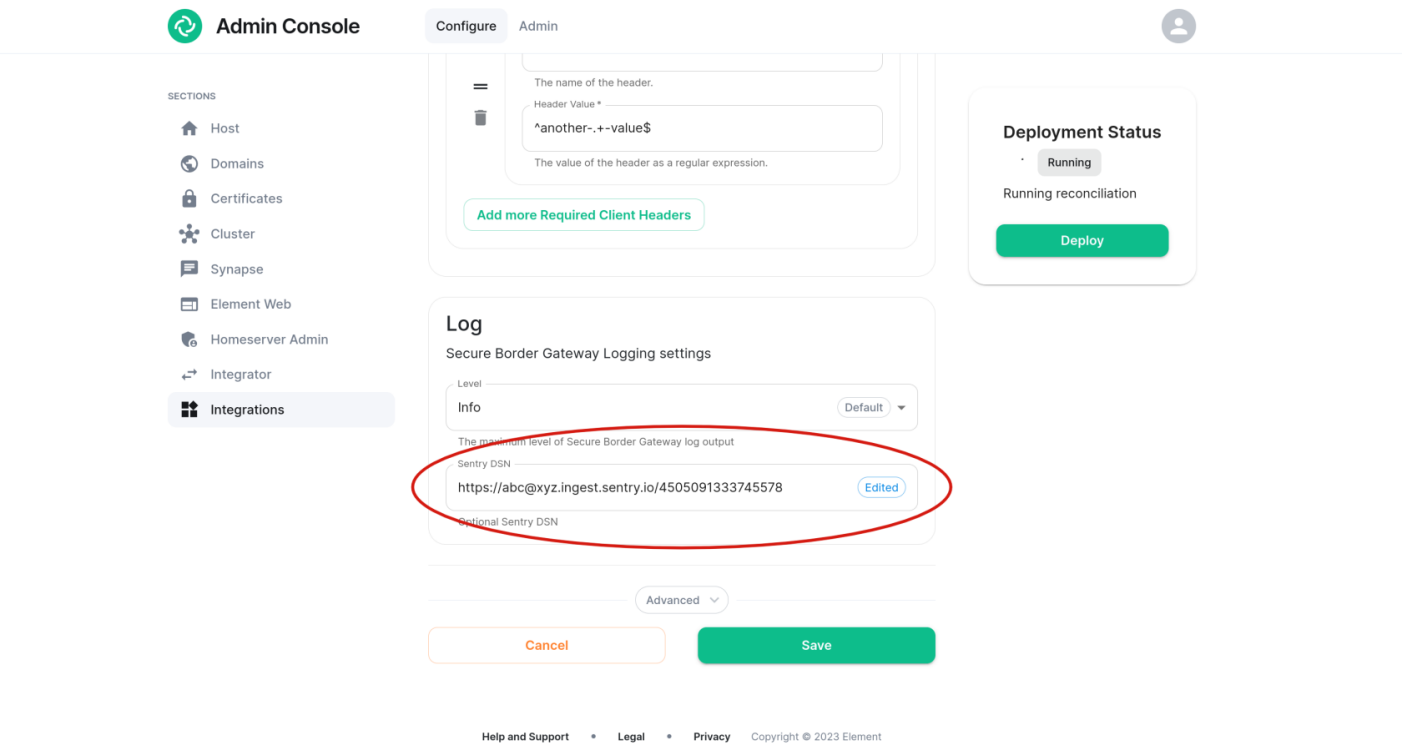
- `/_matrix/key/v2/server`
- `/_matrix/key/v2/query`

The following endpoints are always blocked, even if an `Authorization` header is passed. This is necessary to ensure that a homeserver that isn't in the private federation cannot access them:

- `/_matrix/federation/v1/version`
- `/_matrix/federation/v1/3pid/onbind`
- `/_matrix/federation/v1/openid/userinfo`

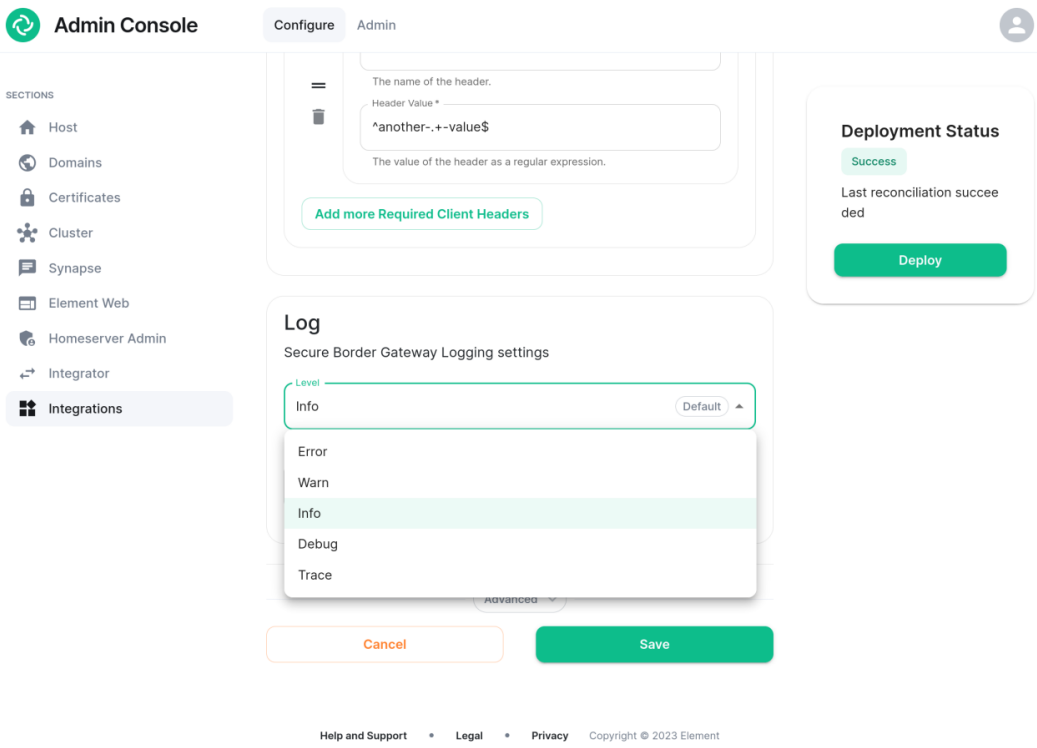
If no federation allow list is configured in the Synapse settings, the SBG will not perform this check.

Sentry



An optional Sentry DSN can be configured in order to log traffic to your external sentry.io instance.

Set the log level



The level at which the SBG logs at can be selected via drop-down. "Info" is the least verbose, whereas "Trace" will provide the maximum amount of logging. Consider using "Debug" to debug issues as it will still log requests and responses, whereas "Trace" will additionally output information only relevant to developers.

URL Previews

URL previews are currently not proxied through the SecureBorderGateway. To protect against the homeserver reaching out to external services without proxying those requests through the Secure Border Gateway, URL Previews on the homeserver are automatically disabled if the Secure Border Gateway is enabled. This can be overridden by adding `url_preview_enabled: true` to your extra Synapse config.

Maximum Request Size

The SBG will enforce a maximum request size of 64 MiB (mebibytes) for client-server traffic as well as both incoming and outgoing federation traffic. This cannot currently be configured.

Revision #5
Created 2023-10-17 09:46:52 UTC by Andrew Morgan
Updated 2024-11-06 12:49:47 UTC by Kieran Mitchell Lane