Manage Proxy Connect using the API

ON THIS PAGE

You can find background information on Proxy Connect in PingOne Advanced Identity Cloud in Configure a proxy service with Proxy Connect.

Proxy Connect API endpoints

Proxy Connect provides these Advanced Identity Cloud API endpoints:

- Header rules API endpoint (`/environment/proxy-connect/header-rules`)
  - Use `GET` to view the header ruleset and determine if the ruleset is active.
  - Use `PUT` to update the header ruleset and activate or deactivate the ruleset.
- IP Address rules API endpoint (`/environment/proxy-connect/ip-rules`)
  - Use `GET` to view the IP ruleset and determine if the ruleset is active.
  - Use `PUT` to update the IP ruleset and activate or deactivate the ruleset.

Authenticate to Proxy Connect API endpoints

To authenticate to Proxy Connect API endpoints, use an access token created with one of the following scopes:

Scope	Description
`fr:idc:proxy-connect:*`	Full access to Proxy Connect API endpoints. Use this scope to view, create, activate, deactivate, or delete rules.
`fr:idc:proxy-connect:read`	Read-only access to Proxy Connect API endpoints. Use this scope if you only need to View default rulesets or View configured rulesets.
`fr:idc:proxy-connect:write`	Write access to Proxy Connect API endpoints. Use this scope to create, activate, deactivate, or delete rules.

Prerequisite actions for accessing a tenant when rulesets are configured

> **Note**
>
> The prerequisite actions are not required if you configured a proxy service to access your tenant or if you configured Secure Connect and can access your tenant from a private network.

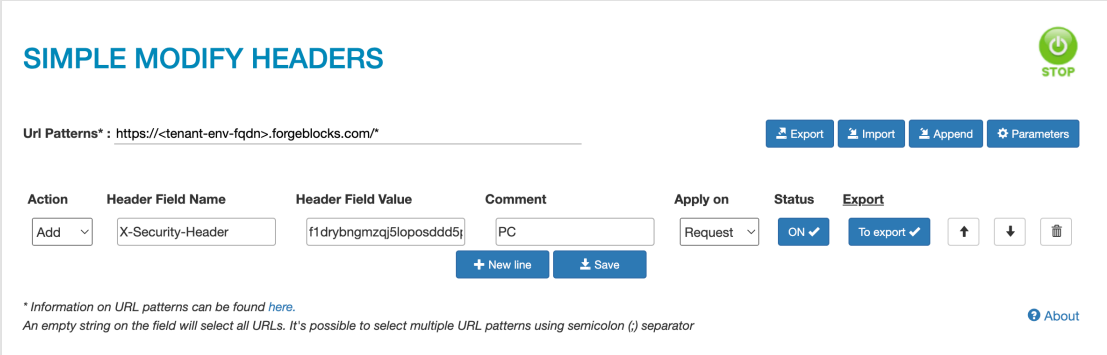
1. Consult with your team to find out what header rules are configured for the environment:
    a. If header rules are configured, you need the name and value of a configured security header.
    b. Add the security header to all cURL requests using the format:

    ```
    --header '<security-header-name>: <security-header-value>'
    ```

    For example:

    ```
    --header 'X-Security-Header: f1drybngmzqj5loposddd5p98z886jp9'
    ```

c. Add the security header to all browser requests using a browser extension; for example, the SimpleModifyHeaders extension lets you modify headers for Chrome and Firefox:



2. Consult with your team to find out what IP rules are configured for the environment:

   a. If IP rules are configured, your IP address needs to be in one of the configured CIDR ranges. You may need to join your company's VPN to change your IP address, or you may need your team to add your IP address to the IP rules configuration.

   b. Run all cURL and browser requests from a configured IP address.

View default rulesets

By default, the header and IP rulesets in each of your tenant environments are inactive. You can view the default ruleset configurations using the API without adding a security header or using a particular IP address.

In any tenant environment (where the header and IP rulesets are inactive):

1. Get an access token created with the `fr:idc:proxy-connect:read` scope.
2. Get the header ruleset configuration from the `/environment/proxy-connect/header-rules` endpoint:

```
$ curl \
--request GET 'https://<tenant-env-fqdn>/environment/proxy-connect/header-
--header 'Authorization: Bearer <access-token>' \②
--header 'Content-Type: application/json'
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

The response shows the default header ruleset configuration:

▼ *Show response*

```
[
    {
        "enabled": false, ①
        "headers": null, ②
        "requestStatus": "SUCCESS" ③
    }
]
```

① The header ruleset is not active.

② The header ruleset contains no rules.

③ The header ruleset is synchronized with the environment's load balancer.

3. Get the IP ruleset configuration from the `/environment/proxy-connect/ip-rules` endpoint:

```
$ curl \
--request GET 'https://<tenant-env-fqdn>/environment/proxy-connect/ip-rule
--header 'Authorization: Bearer <access-token>' \②
--header 'Content-Type: application/json'
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

The response shows the default IP ruleset configuration:

▼ *Show response*

```
[
    {
        "enabled": false, ①
        "ipRanges": null, ②
        "requestStatus": "SUCCESS" ③
    }
]
```

① The IP ruleset is not active.

② The IP ruleset contains no rules.

③ The IP ruleset is synchronized with the environment's load balancer.

View configured rulesets

If the header or IP rulesets in a tenant environment have been activated, API requests return a 404 response unless you use a particular IP address and/or add a security header to your API requests.

In any tenant environment (where the header or IP rulesets are active):

1. Complete the Prerequisite actions for accessing a tenant when rulesets are configured.
2. Get an access token created with the `fr:idc:proxy-connect:read` scope.
3. Get the header ruleset configuration from the `/environment/proxy-connect/header-rules` endpoint:

```
$ curl \
--request GET 'https://<tenant-env-fqdn>/environment/proxy-connect/header-
--header 'Authorization: Bearer <access-token>' \②
--header 'Content-Type: application/json' \
--header '<security-header-name>: <security-header-value>' ③
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

③ (Optional) Review the prerequisite actions. If necessary, add an existing security header to your request; for example:

```
--header 'X-Security-Header: f1drybngmzqj5loposddd5p98z886jp9'
```

The response shows your custom configuration, which will be similar to this:

▼ ***Show response***

```
[
    {
        "enabled": true, ①
        "headers": [
            {"header": "X-Security-Header", "value": "f1drybngmzqj5lopo
        ],
        "requestId": "ag-6WQQCYKH", ③
        "requestStatus": "SUCCESS" ④
    }
]
```

① The header ruleset is active.

② The header ruleset contains one rule. Requests from a third-party service must include a `X-Security-Header` HTTP security header (set with the specified value) to be classed as a valid request.

③ The last update to the header ruleset was assigned a `requestId` of "ag-6WQQCYKH".

④ The header ruleset is synchronized with the environment's load balancer.

4. Get the IP ruleset configuration from the `/environment/proxy-connect/ip-rules` endpoint:

```
$ curl \
--request GET 'https://<tenant-env-fqdn>/environment/proxy-connect/ip-rule
--header 'Authorization: Bearer <access-token>' \②
--header 'Content-Type: application/json'
--header '<security-header-name>: <security-header-value>' ③
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

③ (Optional) Review the **prerequisite actions**. If necessary, add an existing security header to your request; for example:

```
--header 'X-Security-Header: f1drybngmzqj5loposddd5p98z886jp9'
```

▼ ***Show response***

```
[
    {
        "enabled": true, ①
        "ipRanges": [
            "1.2.3.4/32" ②
        ],
        "requestId": "ag-eZKnKPqS", ③
        "requestStatus": "SUCCESS" ④
    }
]
```

① The IP ruleset is active.

② The IP ruleset contains one rule. Requests from a third-party service must originate from an IP address in the specified CIDR range to be classed as a valid request.

③ The last update to the IP ruleset was assigned a `requestId` of "ag-eZKnKPqS".

④ The IP ruleset is synchronized with the environment's load balancer.

Create or update rulesets

Create or update the header and/or IP rulesets in a tenant environment to configure Proxy Connect.

Test ruleset configuration updates on a lower environment before you update your production environment and ensure that any automated scripts are not affected by your changes.

In any tenant environment:

1. Ensure the tenant environment is configured to use outbound static IP addresses.
2. Complete the **Prerequisite actions for accessing a tenant when rulesets are configured**.
3. Get an access token created with the `fr:idc:proxy-connect:write` scope.
4. (Optional) Update the header ruleset:
   a. Review the existing header ruleset configuration. Learn more in:
      - Step 2 in **View default rulesets**.
      - Step 3 in **View configured rulesets**.
   b. Replace the existing header ruleset configuration with your own header ruleset configuration:

```
$ curl \
--request PUT 'https://<tenant-env-fqdn>/environment/proxy-connect/hea
--header 'Authorization: Bearer <access-token>' \②
--header 'Content-Type: application/json'
--header '<security-header-name>: <security-header-value>' \ ③
--data '{"enabled": true, "headers": <headers>}' ④
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

③ (Optional) Review the **prerequisite actions**. If necessary, add an existing security header to your request; for example:

`--header 'X-Security-Header: f1drybngmzqj5loposddd5p98z886jp9'`

④ Replace *<headers>* with a JSON array of security header objects; for example:

```
[
    {"header": "X-Security-Header", "value":
"f1drybngmzqj5loposddd5p98z886jp9"},
    {"header": "X-Security-Header2", "value":
"2ey9ant69h3021b49vvdl8qnww6rmj3y"}
]
```

▼ ***Show response***

```
[
    {
        "enabled": true, ①
        "headers": [
            {"header": "X-Security-Header", "value": "f1drybngmzqj5
            {"header": "X-Security-Header2", "value": "2ey9ant69h30
        ],
        "requestId": "ag-vnYPhgaC", ③
        "requestStatus": "PENDING" ④
    }
]
```

① The header ruleset is active.

② The header ruleset contains two rules. Requests from a third-party service must include a `X-Security-Header` or `X-Security-Header2` HTTP security header (set with the specified value) to be classed as a valid request.

③ The update to the header ruleset was assigned a `requestId` of "ag-vnYPhgaC".

④ The update to the header ruleset is not yet synchronized with the environment's load balancer.

c. An asynchronous process updates the header ruleset in the environment's load balancer. This process can take up to 10 minutes to complete.

To check when the asynchronous process has completed, poll the `/environment/proxy-connect/header-rules` endpoint until the `requestStatus` key in the response changes from `PENDING` to `SUCCESS`.

```
$ curl \
--request GET 'https://<tenant-env-fqdn>/environment/proxy-connect/hea
--header 'Authorization: Bearer <access-token>' \②
```

```
--header 'Content-Type: application/json' \
--header '<security-header-name>: <security-header-value>' ③
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

③ (Optional) Review the **prerequisite actions**. If necessary, add an existing security header to your request. Otherwise, if you are setting header rules for the first time, add one of the new security headers to your request; for example:

`--header 'X-Security-Header: f1drybngmzqj5loposddd5p98z886jp9'`

When the asynchronous process has completed and updated the header ruleset in the environment's load balancer, the response should look like this:

▼ ***Show response***


```
[
    {
        "enabled": true,
        "headers": [
            {"header": "X-Security-Header", "value": "f1drybngmzqj5
            {"header": "X-Security-Header2", "value": "2ey9ant69h30
        ],
        "requestId": "ag-vnYPhgaC",
        "requestStatus": "SUCCESS"
    }
]
```


5. (Optional) Update the IP ruleset:

   a. Review the existing IP ruleset configuration. Learn more in:

   - Step 3 in **View default rulesets**.
   - Step 4 in **View configured rulesets**.

   b. Replace the existing IP ruleset configuration with your own IP ruleset configuration:

```
$ curl \
--request PUT 'https://<tenant-env-fqdn>/environment/proxy-connect/ip-
--header 'Authorization: Bearer <access-token>' \②
--header 'Content-Type: application/json'
--header '<security-header-name>: <security-header-value>' ③
--data '{"enabled": true, "ipRanges": <ip-ranges>}' ④
```

① Replace *<tenant-env-fqdn>* with the FQDN of your tenant environment.

② Replace *<access-token>* with the access token.

③ (Optional) Review the **prerequisite actions**. If necessary, add an existing security header to your request; for example:

```
--header 'X-Security-Header:
f1drybngmzqj5loposddd5p98z886jp9'
```

④ Replace *<ip-ranges>* with a JSON array of CIDR ranges; for example:

```
["1.2.3.4/32", "2.3.2.1/32"]
```

▼ ***Show response***

```
[
    {
        "enabled": true, ①
        "ipRanges": [
            "1.2.3.4/32", ②
            "2.3.2.1/32" ②
        ],
        "requestId": "ag-gdyuPUKD", ③
        "requestStatus": "PENDING" ④
    }
]
```

① The IP ruleset is active.

② The IP ruleset contains two rules. Requests from a third-party service must originate from an IP address in one of the specified CIDR ranges to be classed as a valid request.

③ The update to the IP ruleset was assigned a `requestId` of "ag-gdyuPUKD".

④ The update to the IP ruleset is not yet synchronized with the environment's load balancer.

c. An asynchronous process automatically updates the IP ruleset in the environment's load balancer.

To check when the asynchronous process has completed, follow the instructions in step 3c using the `/environment/proxy-connect/ip-rules` endpoint instead of the `/environment/proxy-connect/header-rules` endpoint.

Deactivate rulesets

To deactivate rulesets, follow the instructions in Create or update rulesets with the following changes:

- In step 4b, use the payload `--data '{"enabled": false, "headers": []}'` to deactivate the header ruleset.
- In step 5b, use the payload `--data '{"enabled": false, "ipRanges": []}'` to deactivate the IP ruleset.