

Configure a proxy service with Proxy Connect

ON THIS PAGE

Configure a proxy service with Proxy Connect

Allow network access only through a proxy service

Block network access from the public internet

Exceptions to Proxy Connect rules

Add-on

Advanced Identity Cloud add-on capability

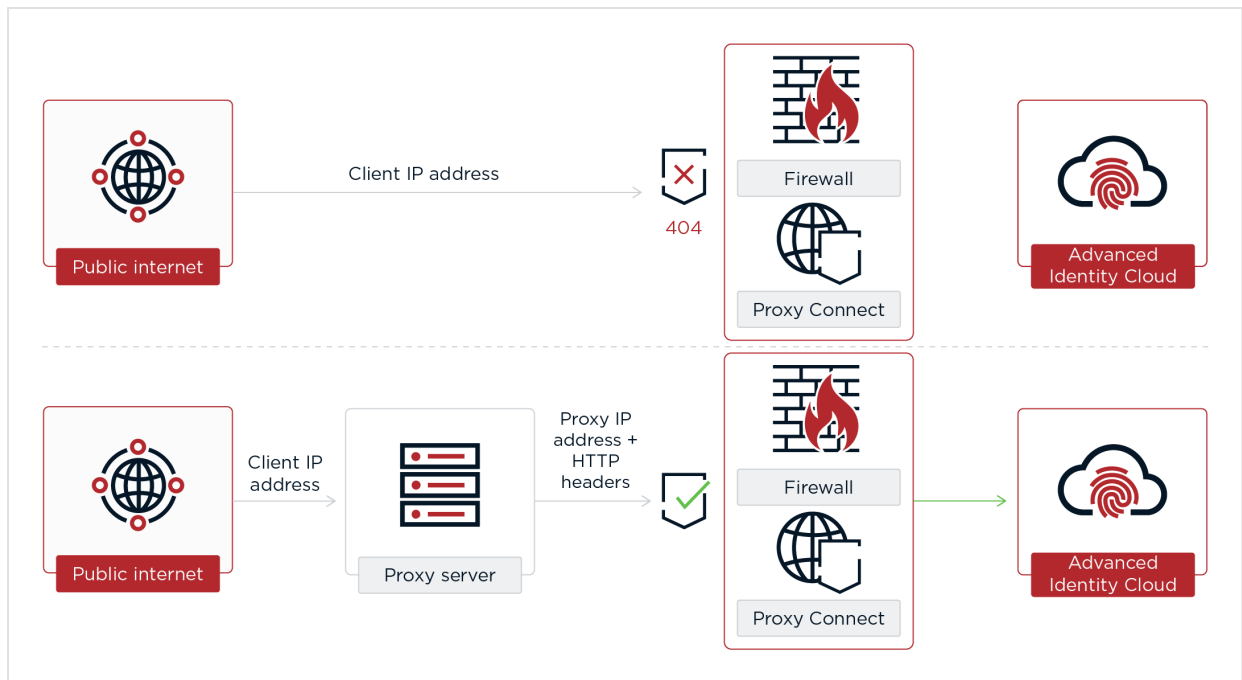
Contact your Ping Identity representative if you want to add Proxy Connect to your PingOne Advanced Identity Cloud subscription. Learn more in [Add-on capabilities](#).

You can use Proxy Connect to configure a proxy service, such as a web application firewall (WAF) or a content delivery network (CDN), in front of your Advanced Identity Cloud tenant environments. This lets you secure traffic to your tenant environments in seamless compliance with the security controls you apply to your company's other network resources.

Proxy Connect lets you restrict access to your tenant environments in two ways:

- Use *IP address rules* to restrict client IP addresses to specified ranges.
- Use *HTTP header rules* to define one or more security headers that client applications must add to each request.

When a client request fails to meet the rules you defined, Advanced Identity Cloud returns HTTP 404 Not Found.



You can set the HTTP header and IP rules independently of each other, so you can set one or both rulesets to suit the requirements of the proxy service. When both rulesets are set, they work as an OR logic gate: only one ruleset needs to be satisfied to allow a successful connection.

Each tenant environment can be configured separately, meaning that you can set different rulesets and combinations of rulesets per environment. Up to 5 security header rules and 60 IP rules can be set per environment.

If you use [Secure Connect](#) to access your tenant environments from a private network, Proxy Connect can also provide an additional layer of security by letting you block network access from the public internet.

Allow network access only through a proxy service

If you use a proxy service to control access to your company's network resources, you can use Proxy Connect to block direct network access to your tenant environments and only allow network access through the proxy.

To only allow network access to a tenant environment through a proxy service:

- For cloud-based proxy services (such as Akamai) where your forwarded requests may share IP addresses with the forwarded requests from other customers of the proxy service:

1. Prepare the proxy service:
 - a. Configure it to forward requests to the tenant environment.
 - b. Configure it to include a security header in forwarded requests.
 2. Activate the proxy service by configuring your DNS records to route traffic to the tenant environment through the proxy.
 3. Secure the tenant environment by configuring Proxy Connect with **only** the proxy service's security header. Learn more in [Create or update rulesets](#).
- For other proxy services:
 1. Prepare the proxy service:
 - a. Configure it to forward requests to the tenant environment.
 - b. (Optional) Configure it to include a security header in forwarded requests.
 2. Activate the proxy service by configuring your DNS records to route traffic to the tenant environment through the proxy.
 3. Secure the tenant environment by configuring Proxy Connect with the proxy service's security header, the proxy service's IP address, or both. Learn more in [Create or update rulesets](#).

Block network access from the public internet

If you use [Secure Connect](#) to access your tenant environments from a private network, you can use Proxy Connect to block access to the environments from the public internet.

To block public internet access to a tenant environment:

1. Set up [Secure Connect](#) so that you can access the tenant environment from your private network.
2. Access your tenant environment from your private network and activate a header ruleset with no rules. Refer to the steps in [Create or update rulesets](#), with the following changes:
 - In step 4b, use the payload `--data '{"enabled": true, "headers": []}'`.
 - Skip step 5.

Exceptions to Proxy Connect rules

The following processes retain access to your tenant environments when Proxy Connect rules are configured:

Process	Reason
Ping Identity SRE and support teams	Lets Ping Identity investigate and resolve support issues.
Monitoring scripts	Lets Ping Identity monitor the behavior and performance of your environments.
Promotions	Lets a lower environment access an upper environment to promote static configuration changes.
Scripting API calls	Lets an environment call its own APIs from scripts.