PingIdentity- PingAccess Lab Guide

Base PingAccess Setup

Before we delve into specific practice scenarios, there are several initial PingAccess setup steps, along with our initial directory setup which will be used across multiple different use cases.

The PingAccess Setup Wizard

The very first time you navigate to the PingAccess URL, there are some initial configurations that must be done before you can access the Administrative Console. Follow the below steps.

First, you must enter your **Base URL**, and press **Next.**

Select the license file and press **Import**.

Import License

You do not have a valid license configured. To obtain a valid license, contact us or visit Ping Identity Licensing. If you have already obtained a license, you may upload and install it into PingAccess.

(Choose File)

📄 PingAccess-8.0-Development 2.lic
Remove

[Import]

Base setup is now complete. You should be redirected to the **Administrative Console.**
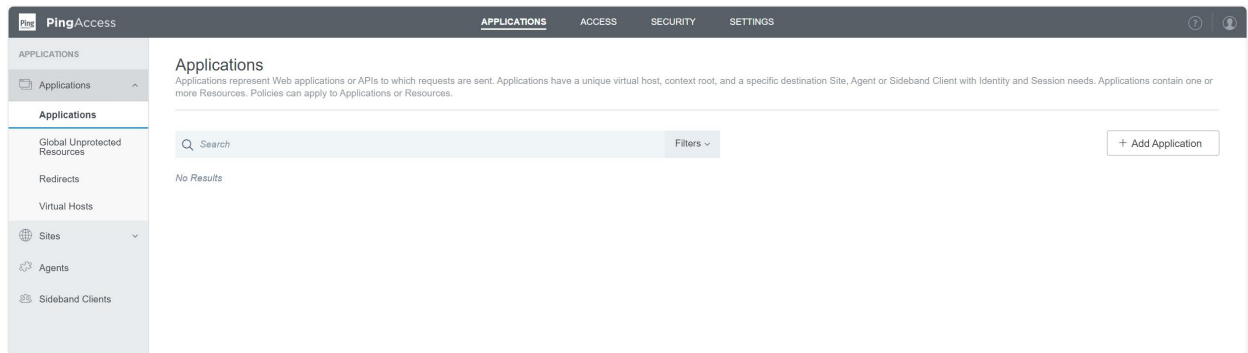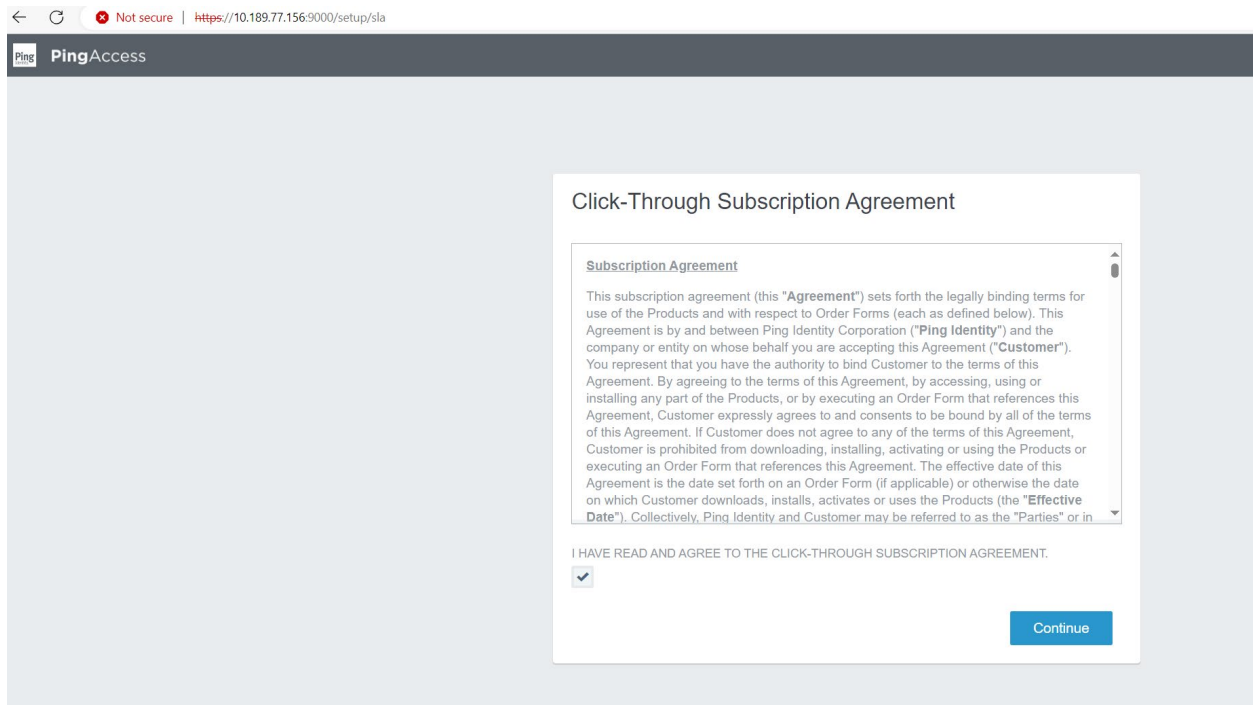
Not secure | https://10.189.77.156:9000/login

Ping PingAccess
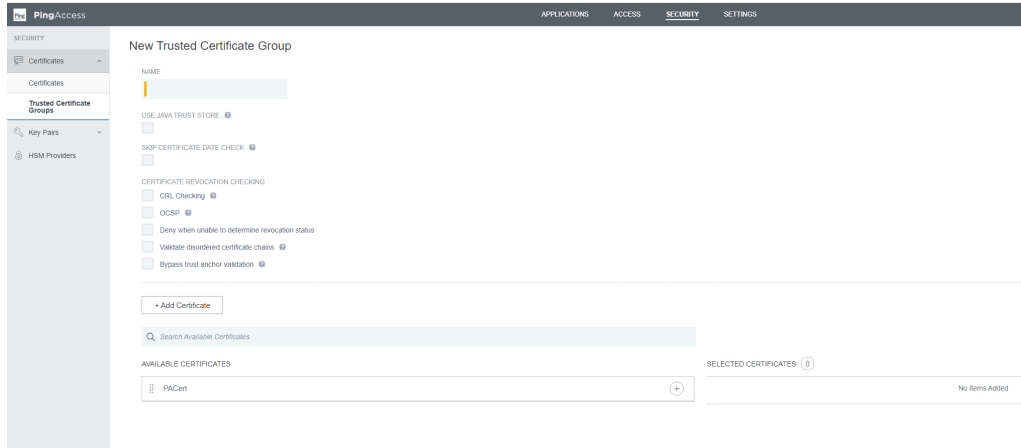
Sign On

administrator

••••••••

[Sign On]

Configuring the Token Provider

1. Create a Trusted Certificate Group
2. Configure PingFederate runtime
3. Configure PingDFederate administration
4. Configure an OAuth resource server

1. Create Trusted Certificate Group

  a) Goto Security > Trusted Certificate Groups > +Add Trusted Certificate Group

1. Import PingFederate server certificate or a CA certificate that anchor's trust to PingFederate server's certificate
   a) Click +Add Certificate
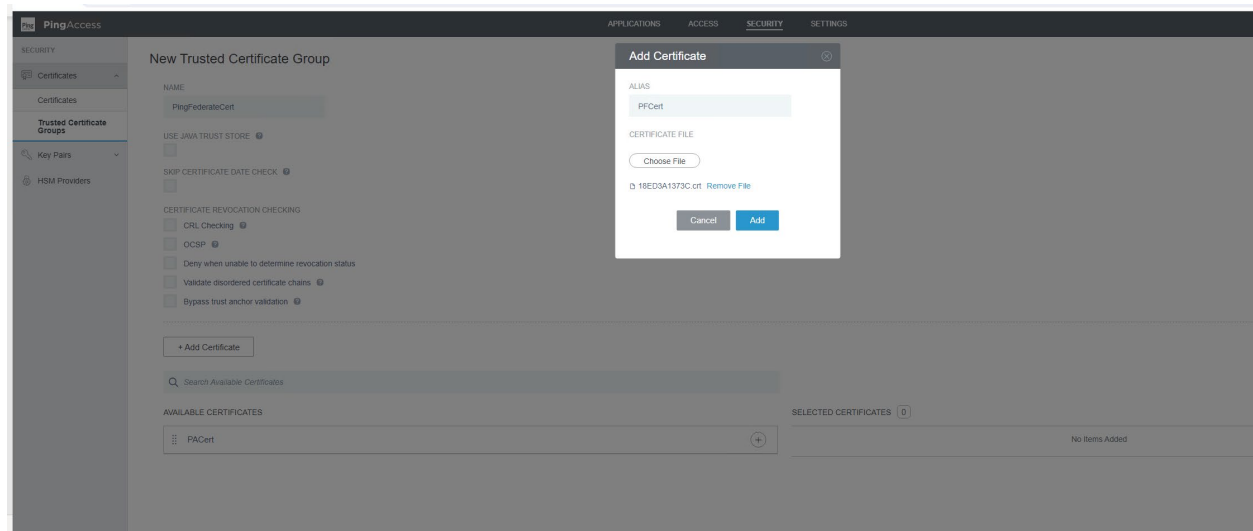
2. Add certificates to the Trusted certificate group
   Double click the certificate or click the + sign next to Available certificates to add them to Selected Certificates

New Trusted Certificate Group

NAME

PingFederateCert

USE JAVA TRUST STORE ❓

☐

SKIP CERTIFICATE DATE CHECK ❓

☐

CERTIFICATE REVOCATION CHECKING

☐ CRL Checking ❓

☐ OCSP ❓

☐ Deny when unable to determine revocation status

☐ Validate disordered certificate chains ❓

☐ Bypass trust anchor validation ❓

+ Add Certificate

🔍 Search Available Certificates

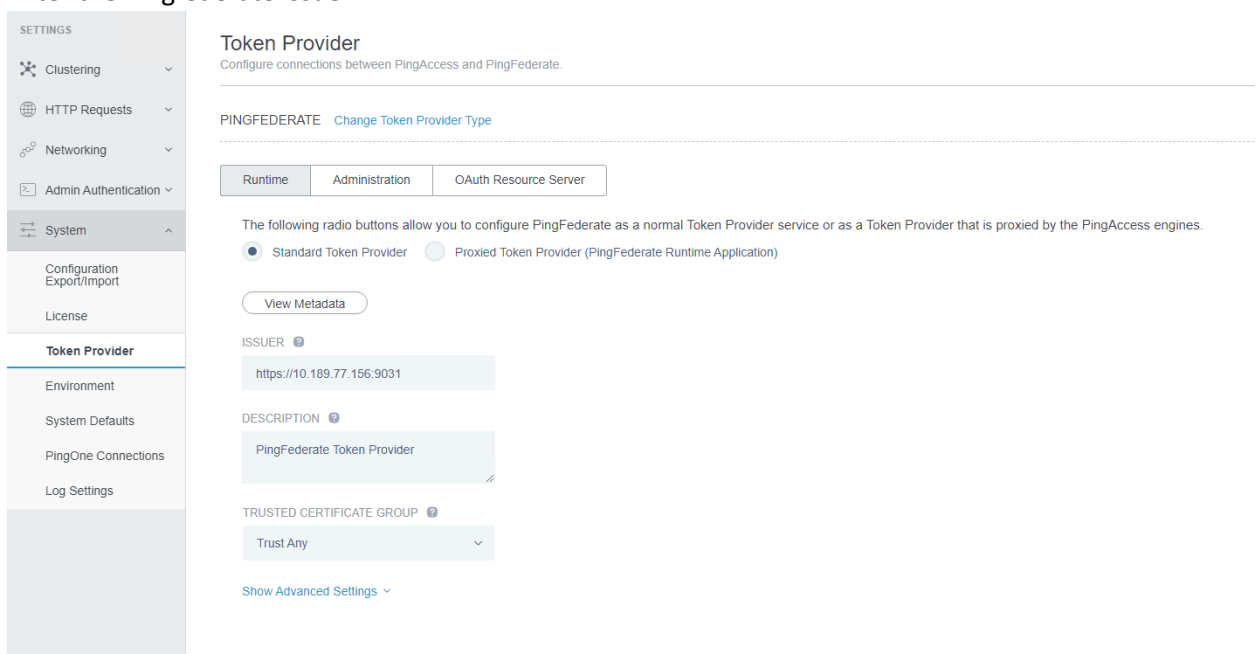AVAILABLE CERTIFICATES   SELECTED CERTIFICATES [1]

⋮   PACert   ⊕   ⋮   PFCert   ⊖

Discard Changes   Cancel   Save

2. Configuring PingFederate Runtime

1. Goto Settings > System > Token Provider > Runtime
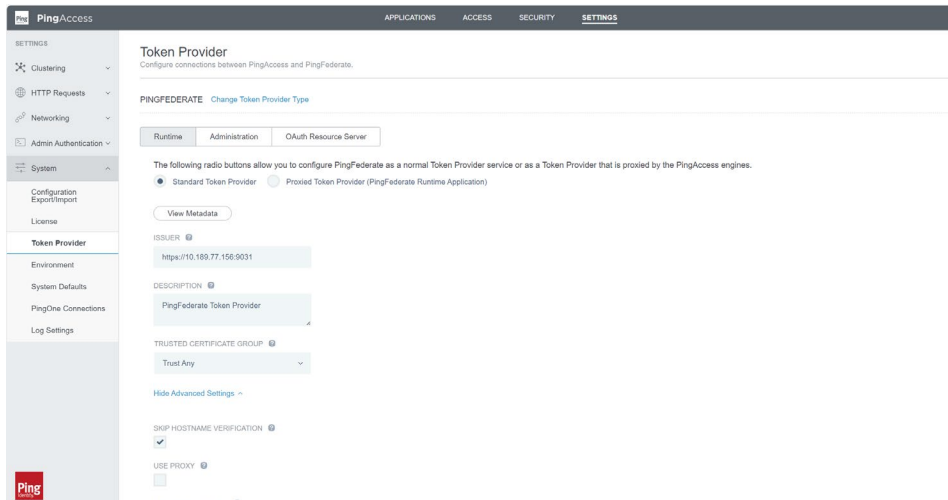
2. Enter the Pingfederate issuer

3. Select a certificate group that includes PingFederate in the **Trusted Certificate Group** list.

Clustering

HTTP Requests

Networking

Admin Authentication

System

　　Configuration
　　Export/Import

　　License

　　Token Provider

　　Environment

　　System Defaults

　　PingOne Connections

　　Log Settings

Token Provider

Configure connections between PingAccess and PingFederate.

PINGFEDERATE   Change Token Provider Type

| Runtime | Administration | OAuth Resource Server |

The following radio buttons allow you to configure PingFederate as a normal Token Provider service or as a Token Provider that is proxied by the PingAccess engines.

○ Standard Token Provider   ○ Proxied Token Provider (PingFederate Runtime Application)

Note: You cannot change types while editing the current configuration. Please save or discard your changes if you would like to change the type.

[View Metadata]

ISSUER ⓘ

https://10.189.77.156:9031

DESCRIPTION ⓘ

PingFederate Token Provider

TRUSTED CERTIFICATE GROUP ⓘ

PingFederateCert

Show Advanced Settings ⌄

3. Configuring PingFederate Administration

1. Goto Settings > System > Token Provider > Administration
2. Edit the details as below:
    A. **Host:** Provide the IPaddress or hostname of the PingFederate server
    B. **Port:** Enter the port number for access to PingFederate Administrative API
    C. **Admin User:** Pingfederate Admin user
    D. **Admin Password :** PingFederate admin password
    E. **Secure:** If Pingfederate is expecting HTTPS connections, select yes
    F. **Trusted Certificate Group:** Select the group of certificates to use when authenticating to PingFederate

4. Configure an OAuth resource server

1. Goto Settings > System > token Provider > OAuth Resource Server
2. Enter the **OAuth Client ID** and **Client Secret** when creating the PingAccess OAuth client in PingFederate
3. In the subject Attribute Name field, enter the attributes you want to use from OAuth access token as the subject for auditing purposes

Token Provider

Configure connections between PingAccess and PingFederate.

PINGFEDERATE   Change Token Provider Type

Runtime	Administration	OAuth Resource Server

CLIENT ID ❓

pa_rs ⌄

CLIENT CREDENTIALS TYPE ❓

● Secret   ○ Mutual TLS   ○ Private Key JWT

CLIENT SECRET ❓

••••••

CACHE TOKENS ❓

● No   ○ Yes

SUBJECT ATTRIBUTE NAME ❓

uid ⌄

SEND AUDIENCE ❓

☐

USE TOKEN INTROSPECTION ENDPOINT ❓

☑

DPOP TYPE ❓

Off ⌄

REQUIRE NONCE ❓

☐

DPOP PROOF LIFETIME (SEC.) ❓

120 ⌃⌄

Protect APIs using PingAccess

In this section, we protect a public api. We have used https://cat-fact.herokuapp.com/facts/ as an example.

1. Pre-requisites

- PingFederate is setup as Token Provider
- Client Credentials client is created in PingFederate
- Postman is setup

Note: Follow PingFederate Lab Guide to create OAuth Client to test the protected api.

2. Configuration

1. Virtual Host

1. Goto Applications > Virtual Hosts
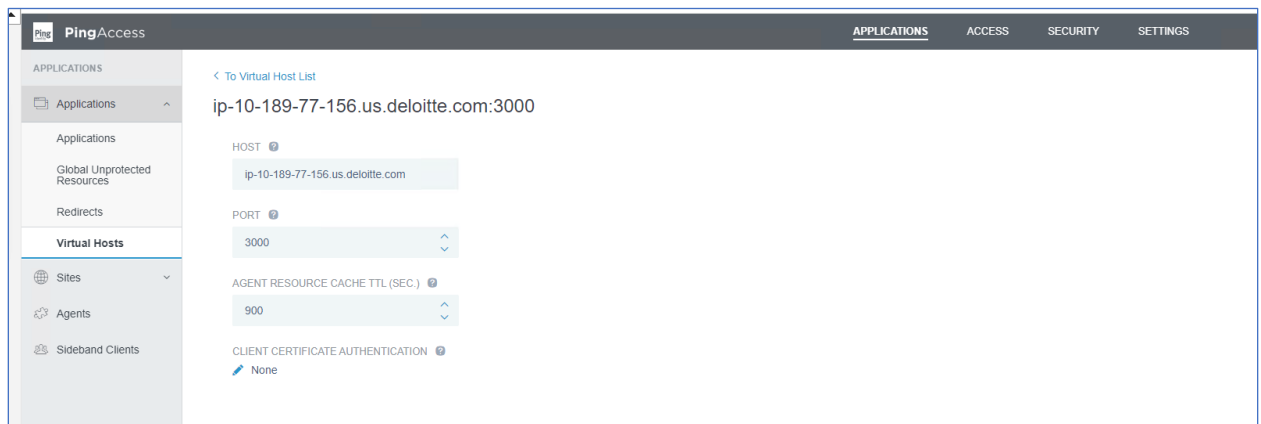
2. Site

Add the host and port of the protected API. In this case, it is https://cat-fact.herokuapp.com/

3. Applications

4. Resources

3. Testing

1. Create a new HTTP request

   Launch Postman and create a new GET request as below. Note here that PingAccess is being used as gateway, so the url has the PingAccess hostname: 10.189.77.156 (please use your own hostname) and PingAccess runtime port: 3000

2. Configure New Token in Postman

Before we access the protected API, we need the access token. In this case, we are using the access token generated from the client credentials grant type.

Click on the **Authorization tab** of the POSTMAN request and configure New Token.

Provide the values as below:

A. **Grant type :** Client Credentials
B. **Access Token URL :** https://10.189.77.156:9031/as/token.oauth2
C. **Client ID:** cc_client
D. **Client Secret :** 2Federate

3. Access protected api using token
   a) In postman, once the New Token configuration is done, scroll to the bottom and click **Get New Access Token**
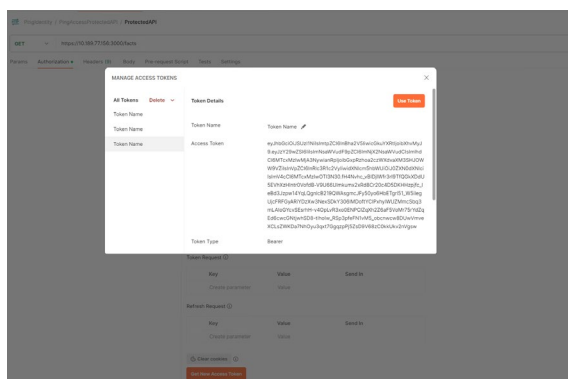
b) Click on **Use Token** and then hit Send to access the api. A successful response with Status 200 OK is received.