



PingAccess Agent Configuration

Avi Technical Reference (v18.2)

Copyright © 2020

PingAccess Agent Configuration

[view online](#)

Overview

Starting with release 18.2.3, Avi Vantage administrators can use Ping Identity's PingAccess Agent to control client access to a virtual service.

How It Works

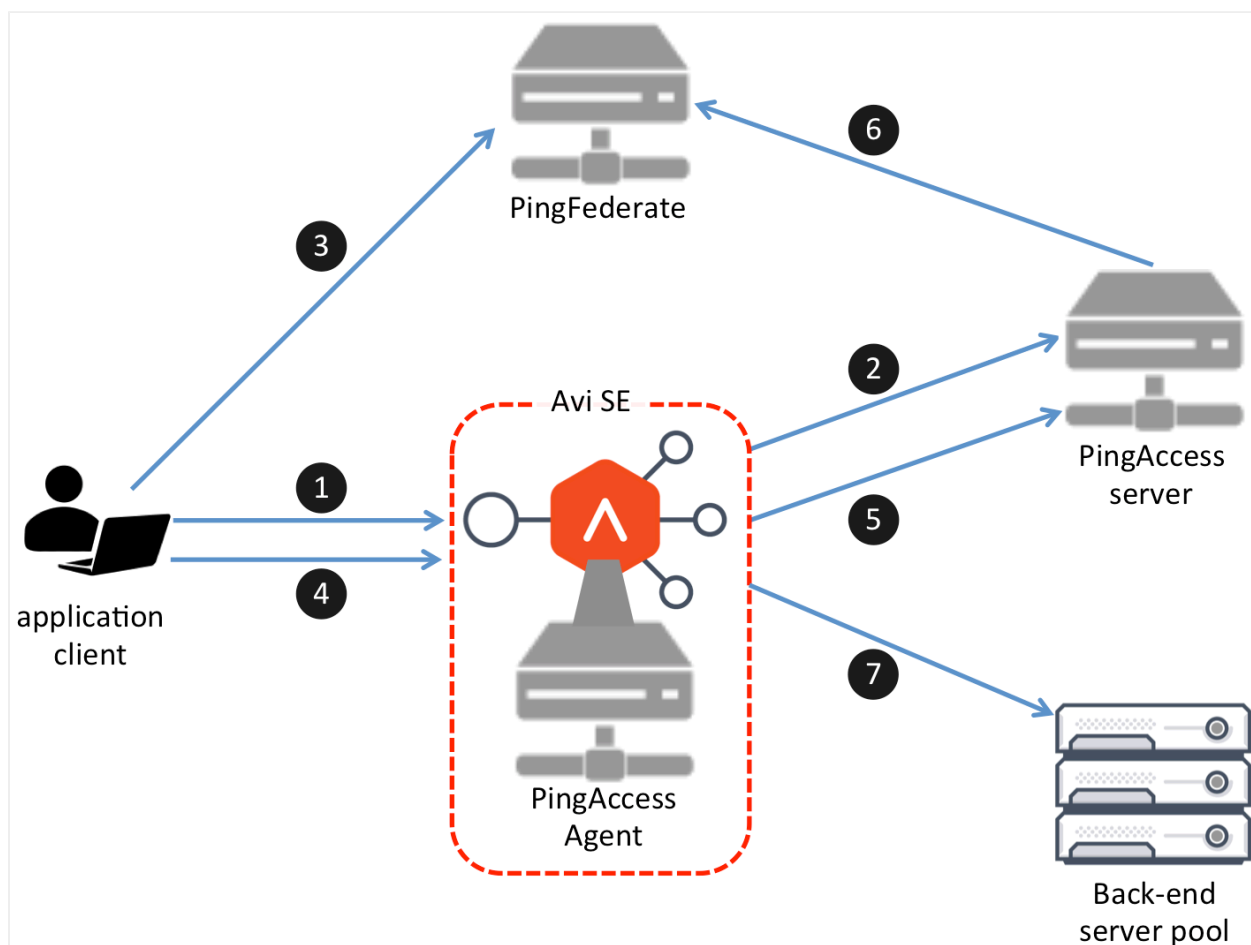


Figure 1. How Avi Vantage and the PingAccess Agent work together

Refer to Figure 1. The numbered arrows correspond with the below numbered steps. This scenario assumes the client has not yet authenticated itself, i.e., has no cookie that would indicate it had previously logged into PingFederate.

1. The client accesses the virtual service running on the SE. For this particular VS, the SE has been configured to check with the PingFederate Agent for both authentication and authorization purposes. If the Agent determines the client has already been authenticated, it continues with step 5.
2. Assume the PingAccess Agent has no record in its cache of authenticating this client. It will direct Avi Vantage to temporarily park the request. The following then happens.

- The PingAccess Agent asks the PingAccess Server for instructions.
 - The PingAccess Server checks its URL policy and determines that access has been requested to one of its protected resources. It responds to the PingAccess Agent with a code the SE passes back to the client without interpreting it. The client will interpret the code as a redirect for the purpose of establishing a session with PingFederate.
3. Upon receipt of that code, the client sends a request to PingFederate. If PingFederate determines the client should be validated, it creates the session.
 4. The client is then redirected back to the resource, i.e., back to the Avi SE. This time the request includes a cookie identifying it as a legitimate user. The PingAccess Agent caches the client's authentication information.
 5. The PingAccess Agent recognizes the client has been authenticated.
- Once again, while Avi Vantage has parked the request, the PingAccess Agent asks the PingAccess Server for authorization instructions.
 - PingAccess Server checks its URL policy and determines that it is a protected resource. It checks the session token, determines that it is valid, and replies back to the Agent that the client is authorized to access the resource.
6. Not applicable to Avi Vantage, but if session revocation is enabled, the PingAccess Server checks and updates the central session revocation list maintained by PingFederate. If the session is valid, the Agent is instructed to re-establish identity HTTP headers.
 7. The SE passes the authenticated and authorized request through to a selected back-end server.

Note: All request logs for a virtual service configured with PingAccessAgent will contain evidence of the PingAccess subrequests via which the PingAccess Agent obtains the information it needs. Such log entries include a "PaaLog" string for easy identification.

Configuring a Virtual Service to Use the PingAccess Agent

1. Navigate to Templates > Security > PingAccess Agent Profile and click on Create.

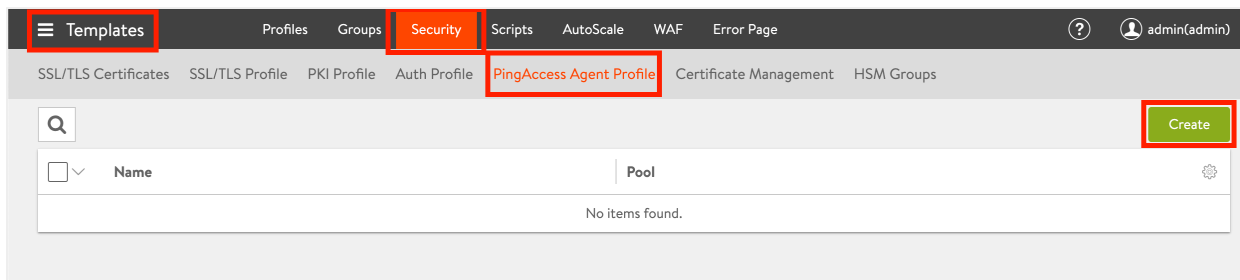


Figure 2. Templates > Security > PingAccess Agent Profile

2. In the PingAccess Agent editor, enter a Name for the agent, and click the radio button to upload its properties one of two ways. In Figure 3 the Upload File option has been chosen, and the file (*AviAgent_agent.properties* in this particular example) has been identified. Click on Save.

About the `.properties` file: The PingAccess administrator will have used the PingAccess UI to download to his workstation's file system from the PingAccess Server a properties file containing the shared secrets needed by the SE's PingAccess Agent. Its file name has the form `<agent_name>_agent.properties`. By placing that file in the administrator's current directory, s/he is able to refer to it via a simple pathname comprised solely of the file name, `AviAgent_agent.properties`.

Note: It is not possible to modify the properties of the PingAccess Agent once it is installed. Instead, one needs to

delete the previous Agent and upload a new one.

The screenshot shows a web form titled "New PingAccess Agent". At the top right is a close button (X). The form has two main sections. The first section is labeled "Name" with a red asterisk and a help icon. It contains a text input field with the value "ExampleAgent". The second section is labeled "PingAccess Agent Properties" with a red asterisk and a help icon. It has two radio buttons: "Enter Text" (which is selected) and "Upload File". Below the radio buttons is a text input field containing "AviAgent_agent.properties" and a grey "Upload File" button. At the bottom center of the form is a large green "Save" button.

Figure 3. PingAccess Agent editor

3. Navigate to Templates > Security > Auth Profile and click on Create.

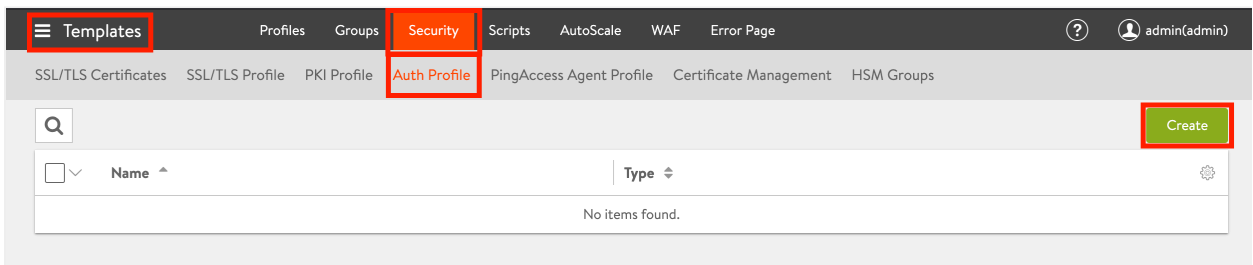


Figure 4. Templates > Security > Auth Profile

4. In the Auth Profile editor, give the new profile a name. Select a Type of PING. Enter the name of the agent specified in Step 2 into the PingAccess Agent field. Click on Save.

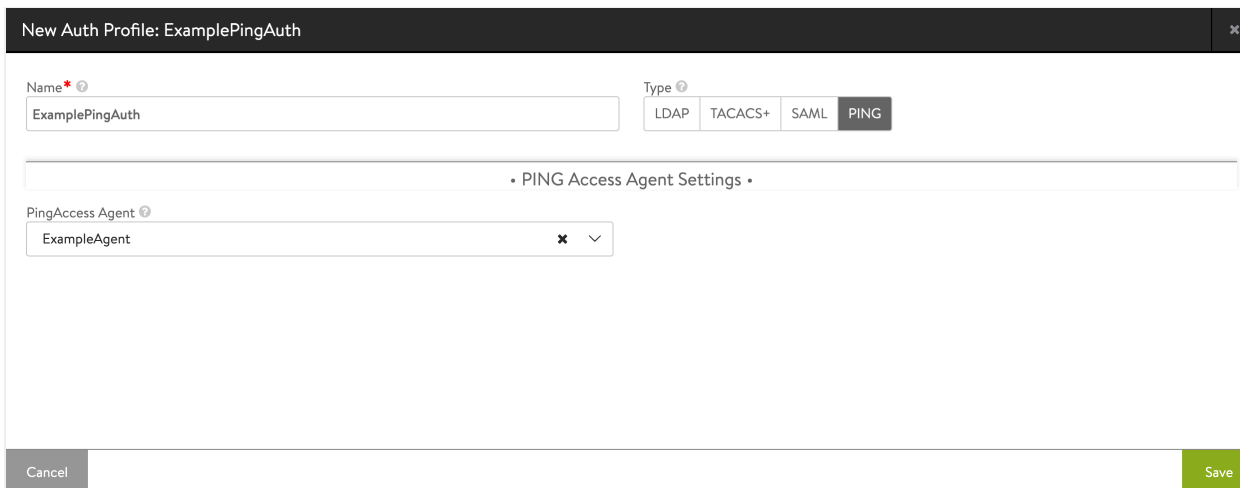


Figure 5. Auth profile editor

- 5. At the time of this writing, there is no Avi UI support for this step. Therefore, use the Avi CLI as shown below to define the SSO policy that will be needed in Step 6.

```
[admin:ctrlr-1]: > configure ssopolicy ExampleSSO
[admin:ctrlr-1]: ssopolicy> authentication_policy default_auth_profile ExampleAuthProfile
[admin:ctrlr-1]: ssopolicy:authentication_policy> save
[admin:ctrlr-1]: ssopolicy> save
```

- 6. Associate the SSO policy just defined with the virtual service access to which PingFederate will oversee.

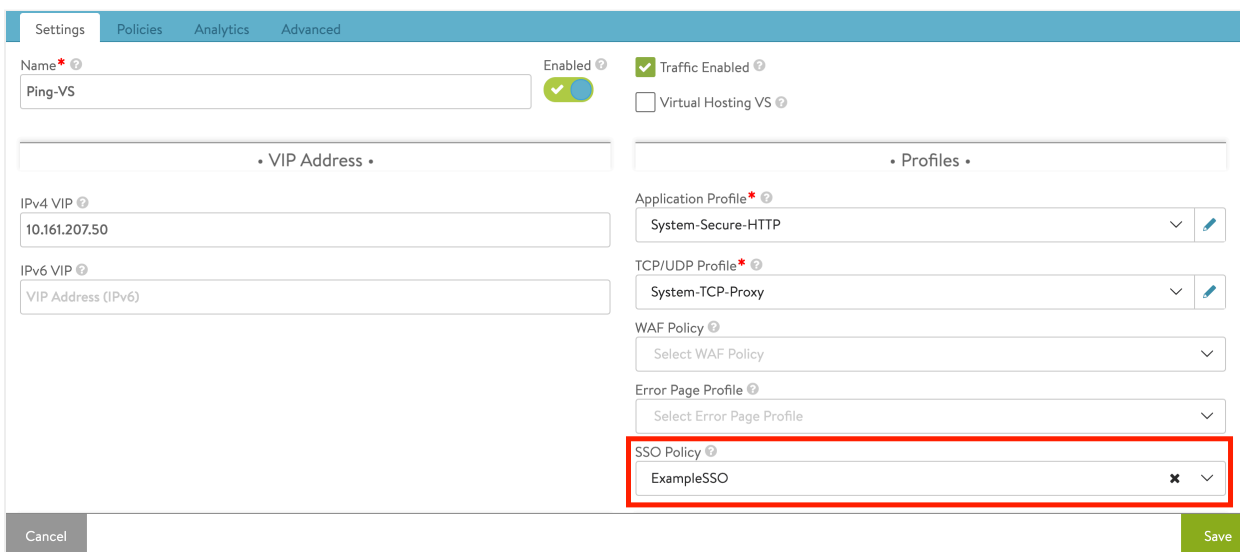


Figure 6. Virtual service wizard