Forcepoint CASB and Ping Federate

Integration Guide

Forcepoint

Integration Guide

Rabih Abou 14 September 2020 Public

Table of Contents

Summary	2
Step 1 – Setup Risk Exporter	3
Step 2 – Setup Ping Federate	6
Troubleshooting	18

Version	Date	Author	Notes
0.1	07 April 2020	Rabih Abou Fakher	First draft
0.2	13 April 2020	Neelima Rai	Review
0.3	15 April 2020	Mattia Maggioli	Review
0.4	19 May 2020	Jonathan Knepher	Review
0.5	14 September 2020	Mattia Maggioli	Minor updates

Summary

This guide provides step by step instructions to configure Forcepoint CASB and Ping Federate to enable dynamic authentication policies based on user risk.

The code and instructions provided enable administrators to automatically:

- → Provide the risk score calculated by Forcepoint CASB for each user to Ping Federate
- → Adjust authentication policies applied by Ping Federate to users based on their risk level

A description of the workflow between the components involved in this POC is depicted in this diagram:



Caveats

These implementation instructions are tested with the following product versions:

- → Forcepoint CASB 2020 R2
- → Ping Federate 9.2 and 10.0

The following activities are out of the scope of this document and therefore left to the system administrator, as part of ordinary maintenance procedures to be put in place within the existing infrastructure:

 \rightarrow Monitoring of the scripts, services and applications involved in the solution

Implementation options

Two implementation options are provided in this document

- → **Docker** leverages a docker image where the integration component is already installed with all necessary dependencies: the user must only edit one configuration file and run the container on an existing docker setup
- → **Traditional** requires manual deployment of the integration component inside a clean host machine (recommended) or an existing one, provided all requirements are satisfied.

The docker image for exporting risk level information has been tested working with the following requirements

- → Docker 19.03.5
- → The docker host machine should meet the minimum hardware requirements of 2GB RAM, 20GB free storage and the system needs to be 64-bit

while the traditional version of the risk exporter has been tested working with the following requirements

 \rightarrow CentOS 7 or Ubuntu 18.04 (64bit versions only) with at least 2GB RAM, 20GB free storage

The files needed to setup the integration are available at the following links:

- → fp-riskexporter-api-v1.tar.gz available at https://frcpnt.com/fp-riskexporter-api-latest
- → ping-connector.tar.gz available at https://frcpnt.com/ping-connector-latest

Step 1 – Setup Risk Exporter

Risk Exporter provides a REST API endpoint used by the Ping connector to retrieve the risk level from the mapped risk score calculated by Forcepoint CASB. It is provided as a tar file with one associated configuration file.

Risk Exporter is deployed to a Linux machine with network connectivity to Forcepoint CASB and to Ping Federate, typically within the same infrastructure hosting both components.

Implementation – Traditional

1. Unpack the **fp-riskexporter-api-v1.tar.gz** file. The examples use the location **/opt/fp-riskexporter-api-v1/** however, the administrator can change to another location if desired.

wget --content-disposition <u>https://frcpnt.com/fp-riskexporter-api-latest</u> tar -zxvf fp-riskexporter-api-v1.tar.gz -C /opt/

2. Install script below will install the system prerequisites, run with a user with administrative privileges.

/opt/fp-riskexporter-api/deploy/install.sh

3. Edit the **cfg.yml** file located in **/opt/fp-riskexporter-api-v1** and change the values to match the hostnames/IP addresses, ports, paths, filenames, and credentials in your current environment relevant to your setup with CASB.

```
casb_login_name:
casb_login_password:
```

Note: The API port must be accessible through the firewall

4. Run the setup script with the command in the example below to install the program prerequisites. Run the command with a user with administrative privileges.

/opt/fp-riskexporter-api/deploy/setup.sh

Implementation – Docker

1. Login into docker repository, you'll be asked to enter your username and password (provided below):

docker login docker.frcpnt.com

Username: fp-integrations

Password: t1knmAkn19s

risk_level_5: 100+

2. Run the command below to download the image

docker pull docker.frcpnt.com/fp-riskexporter-api

3. Create a new file named **cfg.yml** and insert the following contents

API port number, default 5000 api_port: 5000 # Full path including the file name of the Server SSL cert in the docker container (leave as it is) ssl_certfile: /app/fp-riskexporter-api/certs/server.crt # Full path including the file name of the Server SSL cert private key in the docker container (leave as it is) ssl_keyfile: /app/fp-riskexporter-api/certs/server.key # SSL private key password if exists ssl_password: # Set to True if this API is being setup for CASP Risk Score casb_risk_score_fetch_enable: True # How often data get collected from the data source, default value 10 minutes casb_fetch_data_period_in_min: 10 # e.g. https://my.skyfence.com casb_saas_url: casb_login_name: casb_login_password: # Risk Score mapping into Risk Level, example provided below. risk_level_1: risk_level_2: risk_level_3: risk level 4: risk_level_5: # Risk Score mapping example: # risk_level_1: 0-19 # risk_level_2: 20-49 # risk_level_3: 50-79 # risk_level_4: 80-99

- 4. Run the container with either one of the following commands, depending on your scenario
- → if cfg.yml file is located locally, then run the command below, replacing the red part with the full path of the cfg.yml file and the SSL certificates:

docker run --detach \
--name fp-riskexporter-api \
--publish 5000:5000 \
--volume <cfg.yml-full-path>:/app/fp-riskexporter-api/cfg.yml \
--volume <server.crt-full-path>:/app/fp-riskexporter-api/certs/server.crt \
--volume <server.key-full-path>:/app/fp-riskexporter-api/certs/server.key \
--volume RiskScoreDBVolume:/app/fp-riskexporter-api/db \
docker.frcpnt.com/fp-riskexporter-api

→ if cfg.yml file is hosted in a remote location, then run the command below, replacing the red part with the URL of the cfg.yml file to download and the full path of the SSL certificates:

docker run --detach \

- --name fp-riskexporter-api \
- --publish 5000:5000 \
- --env CONFIG_FILE_URL_LOCATION=<config-file-url> \
- --volume <server.crt-full-path>:/app/fp-riskexporter-api/certs/server.crt \
- --volume <server.key-full-path>:/app/fp-riskexporter-api/certs/server.key \
- --volume RiskScoreDBVolume:/app/fp-riskexporter-api/db \
- docker.frcpnt.com/fp-riskexporter-api

Step 2 – Setup Ping Federate

Ping Federate normally uses **Identity Provider** (IdP) as system entities that authenticate users and provide identity attributes to Ping. In our case, we will leverage an IdP to communicate with Forcepoint CASB Risk Exporter API.

1. Download and unpack **ping-connector.tar.gz** and place the files in the location specified in the following table (change the red parts to match your setup)

wget --content-disposition <u>https://frcpnt.com/ping-connector-latest</u> tar -zxvf_ping-connector.tar.gz

File	Target location
pf.plugins.generic-device-risk-adapter.jar	/ <pingfed-home>/pingfederate/server/default/deploy</pingfed-home>
devicerisk.html.form.login.template.html	/ <pingfed-home>/pingfederate/server/default/conf/template</pingfed-home>
devicerisk.min.capture.template.html	/ <pingfed-home>/pingfederate/server/default/conf/template</pingfed-home>
client.min.js	/ <pingfed-home>/pingfederate/server/default/conf/template/assets/scripts</pingfed-home>

 Edit the file /<pingfed-home>/pingfederate/server/default/data/configstore/org.sourceid.common.ExpressionManager.xml and change "evaluateExpressions" to true

- Restart the Ping service to load the new files, see this page on Ping website for options available: <u>https://support.pingidentity.com/s/document-item?bundleld=pingfederate-</u> <u>92&topicId=gettingStartedGuide%2Fpf_t_startAndStopPingfederate.html</u>
- 4. Login to the Ping Federate console
- 5. Select Identity Provider > Integration > Adapters



- 6. Select the existing HTMLFormSimplePCV adapter
- 7. Select **Extended Contract** and add **pf.envdata** in **Extend the Contract** field, then select **Done** to save the configuration of this IdP. Click **Save** on the next page to save these changes.

Ping PingFederate	
MAIN	Manage IdP Adapter Instances Create Adapter Instance
ି _ Identity Provider	Type IdP Adapter Extended Contract Adapter Attributes Adapter Contract Mapping Summary
D Service Provider	This adapter type supports the creation of an extended adapter contract after initial deployment of the adapter instance. This adapter contract may be used to fulfill the attribute contract, look up additional attributes from a local data store, or create a persistent name identifier which uniquely identifies the user passed to your SP partners.
OAuth Server	Core Contract
	policy.action
SETTINGS	username
	Extend the Contract Action
Security	pf.envdata Edit I Delete
[⊸] ⁺→ System	Add
Copyright © 2003-2018 Ping Identity Corporation All rights reserved	Cancel Previous Next Done

8. Go to Identity Provider > Integration > Adapters > HTMLFormSimplePCV > Adapter Contract Mapping, then click Configure Adapter Contract

7

9. Click on Adapter Contract Fulfillment, change the Source for pf.envdata to Expression (as shown in the

screenshot below) and add the following expression into the Value area as one line.

#result = #this.get("context.HttpRequest").getObjectValue().getParameter("pf.envdata") != null ?
#this.get("context.HttpRequest").getObjectValue().getParameter("pf.envdata").toString() : null

Ping Federate					
MAIN 인권 Identity Provider	Manage IdP A Attribute Sources Fulfill your Adapter C	Adapter Instances & User Lookup Adapt	Create Adapt	er Instance Adapter Contract Mapping Issuance Criteria Summary or with dynamic text values.	
Service Provider	Contract	Source	Value		Actions
OAuth Server SETTINGS	pf.envdata	Expression	<pre>#result #this.g .getPar #this.f .getPar</pre>	<pre>e et("context.HttpRequest").getObjectValue() ameter("pf.envdata") != null ? et("context.HttpRequest").getObjectValue() ameter("pf.envdata").toString() : null //</pre>	Edit
Security	policy.action	Adapter	~		None available
t⊷ System	username	Adapter	~		None available

10. Click **Done** to save the new value. On the next page that appears, click **Done** again. Click **Save** on the next screen to finally save these changes.

Next, we create a new IdP that will be used by Ping Federate to action authentication policies.

11. Click **Identity Provider > Adapters > Create New Instance** and fill the relevant fields using the following values so they match the instructions in the rest of this document:

Instance Name: DeviceRiskAdapter Instance ID: DeviceRiskAdapter Type: Device Risk Adapter

Once done click Next.

Ping PingFederate		
MAIN	Manage IdP Adapter Instances Create Adapter Instance	
ି - Identity Provider	Type IdP Adapter Extended Contract Adapter Attributes Adapter Contract Mapping	Summary
Service Provider	Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applicable. The Adapter Type adapters currently installed on your server.	is limited to the
OAuth Server	INSTANCE NAME DeviceRiskAdapter	
	INSTANCE ID DeviceRiskAdapter	
SETTINGS	TYPE Device Risk Adapter V	
⁻⁺ ⁺ → System	PARENT INSTANCE V	

12. In the page that follows fill the relevant fields with the following values, making sure to change the path and ports to match the ones used in your current setup:

Event ingest endpoint: https://<Risk Exporter hostname or IP>:5000/riskexporter/dummy/event Risk score endpoint: https://<Risk Exporter hostname or IP>:5000/casb/risk/level

Note: The cert for the Risk Exporter API above need to be trusted by ping host machine.

SCIM ENDPOINT		The SCIM resource endpoint where users are managed.
SCIM USERNAME		The username used to authenticate to the SCIM resource.
SCIM PASSWORD		The password used to authenticate to the SCIM resource.
DEVICE CONTAINER DN		The container where the device entries will be stored.
EVENT INGEST ENDPOINT	https://	The REST Ingest endpoint.
RISK SCORE ENDPOINT	https://	The Risk Score endpoint.
HTML FORM TEMPLATE NAME	devicerisk.min.capture.template.html	The html form template that will capture the environment variable.)
ENABLE DEBUG LOGGING	✓	Log debug logging for troubleshooting.

Once done click Next.

13. Click **Next** again and once on **Adapter Attributes** tab and tick the checkboxes **Pseudonym** for both "**risk_level**" and "**username**". Once done click **Next** in the next two pages that appear and once Summary page is reached, click **Done** and in the next page click **Save** to save the changes.

AIN	Manage IdP	Adapter Instances	Create Adapter Instance		
Identity Provider	Type IdP A	dapter Extended Contract	Adapter Attributes Adapter Contract	t Mapping Summary	
Service Provider	As an IdP, some of y would like to use in	your SP partners may choose to constructing this unique identified	receive a pseudonym to uniquely identify a user er. Optionally, specify here any attributes that mu	. From the attributes in this authentication adapter, ust be masked in log files.	please select the values that yo
	Attribute		Pseudonym	Mask Log Values	
OAuth Server	risk_calc_timestam	ıp			
	risk_level		~		
THNGS	username		<		
-	asenance				
] Identity Provider	Manage IdP Adapter	r Instances formation and provide user identificatio	on to PingFederate. Here you can manage instances of a	idapters that may be used to fulfill attribute contracts in proto	ocol mappings.
] Identity Provider	Manage IdP Adapter IdP adapters look up session int Instance Name 🗘	r Instances formation and provide user identification Instance ID	on to PingFederate. Here you can manage instances of a Type	idapters that may be used to fulfill attribute contracts in proto Parent Name	ocol mappings.
] Identity Provider	Manage IdP Adapte IdP adapters look up session int Instance Name DeviceRiskAdapter	r Instances formation and provide user identificati Instance ID DeviceRiskAdapter	on to PingFederate. Here you can manage instances of a Type Device Risk Adapter	idapters that may be used to fulfill attribute contracts in proto Parent Name	ocol mappings. Action Delete
] Identity Provider) Service Provider OAuth Server	Manage IdP Adapter IdP adapters look up session ini Instance Name DeviceRiskAdapter HTMLFormSimplePCV	r Instances formation and provide user identification Instance ID DeviceRiskAdapter HTMLFormSimplePCV	on to PingFederate. Here you can manage instances of a Type Device Risk Adapter HTML Form IdP Adapter	idapters that may be used to fulfill attribute contracts in proto Parent Name	Action Delete Delete
Identity Provider Service Provider OAuth Server TINGS	Manage IdP Adapter IdP adapters look up session ini Instance Name DeviceRiskAdapter HTMLFormSimplePCV Create New Instance	r Instances formation and provide user identificativ Instance ID DeviceRiskAdapter HTMLFormSimplePCV	on to PingFederate. Here you can manage instances of a Type Device Risk Adapter HTML Form IdP Adapter	idapters that may be used to fulfill attribute contracts in proto Parent Name	Action Delete Delete
Identity Provider Service Provider OAuth Server TINGS Security	Manage IdP Adapte: IdP adapters look up session ini Instance Name DeviceRiskAdapter HTMLFormSimplePCV Create New Instance	r Instances formation and provide user identification Instance ID DeviceRiskAdapter HTMLFormSimplePCV	on to PingFederate. Here you can manage instances of a Type Device Risk Adapter HTML Form IdP Adapter	idapters that may be used to fulfill attribute contracts in proto Parent Name	Action Delete Delete
Identity Provider Service Provider OAuth Server TINGS Security System	Manage IdP Adapte: IdP adapters look up session in Instance Name DeviceRiskAdapter HTMLFormSimplePCV Create New Instance	r Instances formation and provide user identificativ Instance ID DeviceRiskAdapter HTMLFormSimplePCV	on to PingFederate. Here you can manage instances of a Type Device Risk Adapter HTML Form IdP Adapter	idapters that may be used to fulfill attribute contracts in proto Parent Name	Action Delete Delete

- 14. In the Identity Provider page go to Integration > Adapters, click HTMLFromSimplePCV then IdP Adapter
- 15. Scroll to the bottom of the page and click Show Advanced Fields
- 16. Find the Login Template field and replace the existing value with

devicerisk.html.form.login.template.html

Ping PingFederate			٢
MAIN	ACCOUNT UNLOCK		Allows users with a locked account to unlock it using the self-service password reset type.
리 Identity Provider	LOCAL IDENTITY PROFILE	Select One V	Optionally associate this instance with a Local Identity Profile.
Service Provider	ENABLE USERNAME RECOVERY		Allow users to get their username from an email.
(a) OAuth Server	LOGIN TEMPLATE	devicerisk.html.form.login.template.html	HTML template (in <pf_home>/server/default/conf/template) to render for login. The default value is html.form.login.template.html.</pf_home>
SETTINGS	LOGOUT PATH		Path on the PingFederate server to invoke the HTML Form Adapter logout functionality. This setting is intended for use when SLO is not desired or available, and only this adapter's session needs to be cleared. Paths specified must include the initial slash (e.g.: /mylogoutpath) and be unique across all adapter instances (including child instances). The resulting full
			URL will be http[s]:// <pt_host>:<port>/ext/<logout Path>.</logout </port></pt_host>

Once done click **Done.** In the next page, click **Save**

2 Identity Provider	Manage IdP Adapter	Instances			
	IdP adapters look up session inf	ormation and provide user identification to PingFederate.	Here you can manage instances of adapters that may be used	to fulfill attribute contracts in protocol map	Action
E Service Provider	DeviceRiskAdapter	DeviceRiskAdapter	Device Risk Adapter	T dicit Hume	Delete
OAuth Server	HTMLFormSimplePCV	HTMLFormSimplePCV	HTML Form IdP Adapter		Delete
SETTINGS	Create New Instance				
💩 Security					
⇒ System					
					Cancel Save

The next step is to define **Policy Contracts**: this will be used by Ping Federate to oppose different authentication steps to each user based on his risk level.

- 17. Click Identity Provider > Authentication Policies > Policy Contracts > Create New Contract
- Enter a name in the Contact Name field (e.g. "Simple" in the rest of this document), then Next > Next > Done > Save

PingFederate*					
MAIN	Authentication Policy Co	ntracts Authentication Policy Contract			
ି Identity Provider	Contract Info Contract Attribut	tes Summary			
Service Provider	Authentication policy contract summary	y information.			
(A) OAuth Server	Authentication Policy Contract				
© OAdarociter	Contract Info	Simple			
SETTINGS	Contract Attributes				
le Security	Attribute	subject			
$\xrightarrow{*}{\stackrel{*}{\to}}$ System					
			Cancel	Previous	Done

- Click OAuth Server > Grant Mapping > Authentication Policy Contract Mapping and select from the dropdown menu the contract created in the previous step, then click Add Mapping > Next which takes you to the Contract Fulfillment tab
- 20. For both USER_KEY and USER_NAME contracts select Authentication Policy Contract from the drop-down menus; select subject as value

Once done click Next, do nothing in Issuance Criteria in the next screen but click Next then Save

Ping PingFederate		
MAIN <- 2 Identity Provider	Authentication Policy Contract Mappings Policy Contract Mapping Attribute Sources & User Lookup Contract Fulfillment Issuance Criteria Summary	
Service Provider	Policy Contract Mapping	
OAuth Server	Attribute Sources & User Lookup	
CETTINICO	Data Sources (None)	
SETTINGS	Contract Fulfillment	
Security	USER_NAME subject (Authentication Policy Contract)	
	USER_KEY subject (Authentication Policy Contract)	
🕂 System	Issuance Criteria	
	Criterion (None)	

Click **Identity Provider > Authentication Policies > Policies**, and make sure that IDP AUTHENTICATION POLICIES checkbox is selected.

Jula milita Dava dalar	Authentication Policies						
 Identity Provider 	Policies	Default Authentication Sources	Tracked HTTP Parameters				
Service Provider	Authenticatio	n policies define how PingFederate au	thenticates users. Selectors and a	authenticatior			
D OAuth Samer	V IDP AUT	HENTICATION POLICIES					
9 OAuth Server	SP AUTHENTICATION POLICIES						
	FAIL IF F	POLICY ENGINE FINDS NO AUTHENTI	CATION SOURCE				
TTINGS							

21. Click Identity Provider > Authentication Policies > Policies > Add Policy, use the following values

Name: Device Risk Policy Policy: Pick HTMLFormSimplePCV from IdP Adapters in the drop-down menu

For the **Fail** case click **Done**, while for the **Success** case click on the drop-down menu and select **DeviceRiskAdapter** from the **IdP Adapters** menu

Ping PingFederate		
MAIN		
ି Identity Provider	Options I Rules	xpand All I Collapse All
Service Provider	FAIL Done	
OAuth Server	V SUCCESS DeviceRiskAdapter - (Adapter) V ×	
SETTINGS	Options I Rules	
💩 Security	FAIL Select	
🕂 System	Restart I Done	
	Select V Restart I Done	

22. Under the top Success drop-down menu click Options and pick the following entries for each drop-down menu
 Source: Adapter (HTMLFormSimplePCV)
 Attribute: username

Ping PingFederate		
MAIN		
ି Identity Provider		Expand All I Collapse All
Service Provider		
(A) OAuth Server	Some authentication sources make use of a user identifier at request time. SAML 2.0 connections can use the incoming user ID to specify a subject in its AuthnRequest. Likewise some adapters use the incoming user ID. Specify which attribute you would like to map to this authentication source's incoming user ID.	
SETTINGS	Source Attribute	
💩 Security	Adapter (HTMLFormSimp v Clear	
	Cancel Done	

Click Done once finished

23. Under the top Success drop-down now click Rules and add one line for each possible risk level value returned by Forcepoint CASB as in the picture below, each of these lines will be assigned with a different action so that Ping will oppose different challenges based on the risk_level value. User can add a new entry (rule) by clicking Add button.

Ping PingFe	derate											
MAIN	_	DESCRIPTION		_	_				_		_	
ේ Identity P	Rules										*	
Service F	Define au If all the r	uthentication policy r rules fail, you may ch	rules using noose to d	g attributes from the pre lefault to the general Su	evious Authentica Iccess action or F	tion Source. Eacl ail.	h rule is evaluat	ed to determine	the next acti	on in the policy.	•	
OAuth Se		Attribute Name		Condition		Value		Result		Action	ollapse	All
SETTINGS	~	risk_level	~	equal to	~	1		Risk Level 1		Delete		
💩 Security	^ v	risk_level	~	equal to	~	2		Risk Level 2		Delete		
[→] → System	^ v	risk_level	~	equal to	~	3		Risk Level 3		Delete		
	~ ~	risk_level	~	equal to	~	4		Risk Level 4		Delete		
	^	risk_level	~	equal to	~	5		Risk Level 5		Delete		
Copyright © 2003-2018	✓ DEF	FAULT TO SUCCESS	;					Cancel	Add	Done		

The **Risk Exporter** returns risk level -1 for entities that do not exist. This can be configured as a policy rule to utilize a specific risk level, or by ticking the **Default to success** box will let users authenticate normally if they have no risk level.

Please note that Ping Federate does not provide inequality operators for the **risk_level** value, therefore the system administrator must create a policy rule for each possible case (e.g. it is not possible to configure a rule for the case "risk_level > 2")

Once finished, click Done

Typically, a system administrator may configure:

- \rightarrow Standard authentication steps for low risk users (e.g. risk_level = 1 or 2)
- \rightarrow Multi-factor authentication for medium risk users (e.g. risk_level = 3 or 4)
- \rightarrow More complex, or deny authentication for the most risky users (e.g. risk_level = 5)
- \rightarrow A custom action or one of the above options for users whose risk level has not been calculated yet (risk_level = -1)

The choice of how to map **risk_level** values to authentication steps is left to the system administrator, since there might already be in place custom authentication policies, and more importantly because the mapping decision differs from customer to customer based on their security policies.

Example – Authentication policy rules

For system administrators with no previous authentication policies in place, here is an example of how to configure Ping Federate based on the risk level provided by Forcepoint CASB.

The configuration described in the next pages

- → allows standard access with username/password for users whose **risk_level** is 1 to 4, and for users whose risk level has not been calculated yet
- → denies access to users whose risk_level equals 5

The process to configure this is as follows:

- 1. Click **Expand All** to see all rules as a tree.
- 2. For the Fail case under DeviceRiskAdapter click Done.
- 3. Under **Risk Level 1**, click on the drop-down menu and on the next drop-down menu select **Policy Contracts**, select **Simple** (created earlier in step 18 of Step 2 Setup Ping Federate)

Simple - (Policy Contract)	∧ (×)
Policy Contracts	✓ Q Search
ID	NAME

- 4. Click Contract Mapping
- 5. Click **Next** in the **Attribute Source & User Lookup** page and in the **Contract Fulfillment** page use the following choices in the drop-down menus then click **Next**

Source: Adapter (HTMLFormSimplePCV)
Value: username

6. In **Issuance Criteria** page, pick the following values in each drop-down menu:

Source: Adapter (DeviceRiskLevel) Attribute Name: risk_level Condition: equal to Value: 1 Error Result: Low – Risk Level 1

Once done click Add then Next. Click Done.

Ping Federate*						
MAIN	Authentication Polic	ies Policy Auther	ntication Policy C	contract Mapping		
E Identity Provider	Attribute Sources & User Loo	okup Contract Fulfillment	Issuance Criteria	Summary		
E Service Provider	PingFederate can evaluate vario this conditional authorization.	ous criteria to determine wheth	er users are authorized to	access SP resources. Use	this optional screen to configure the crit	eria for use with
	Source	Attribute Name	Condition	Value	Error Result	Action
OAuth Server	Adapter (DeviceRiskAdapter)	risk_level	equal to	1	Low - Risk Level 1	Edit I Delete
SETTINGS	- SELECT - 🗸 🗸	- SELECT - 🗸 🗸	- SELECT -	~		Add

Repeat steps 2 to 4 for each Risk Level 1 to 4.

7. For **Risk Level 5** click **Contract Mapping** then **Next** in the **Attribute Source & User Lookup** page since no changes are to be made in this page. In the **Contract Fulfillment** page use the following choices in the drop-down menus then click **Next**

Source: Adapter (HTMLFormSimplePCV)
Value: username

8. In the Issuance Criteria page, select the values in the drop-down menus as follows

Source: Adapter (DeviceRiskLevel) Attribute Name: risk_level Condition: not equal to Value: 5 Error Result: High – Risk Level 5

Once done click Add then Next. Click Done.

Ping Federate						
MAIN	Authentication Po	olicies Policy Aut	hentication Policy C	Contract Mapping		
2 Identity Provider	Attribute Sources & Use	er Lookup Contract Fulfill	ment Issuance Criteria	Summary		
E Service Provider	PingFederate can evaluate with this conditional author	various criteria to determine w ization.	hether users are authorized to	access SP resources. Use this	optional screen to configure the	e criteria for use
	Source	Attribute Name	Condition	Value	Error Result	Action
OAuth Server	Adapter (DeviceRiskAdapter)	risk_level	not equal to	5	High Risk - Level 5	Edit I Delete
SETTINGS	- SELECT - V	- SELECT - V	- SELECT -			Add

By doing this, when Ping Federate processes the policy for a user with **risk_level** = 5, will route the user to the "**RISK LEVEL** 5" rule. This rule would authorize the login only if the **Issuance Criteria** is met, but since we configured **not equal to** as **Condition**, this will never be met thus no authentication for the user whose risk level is 5.

For **Success** under **DeviceRiskAdapter**, click on the drop-down menu and on the next drop-down menu select **Policy Contracts**, select **Simple** (created earlier in step 18 of Step 2 – Setup Ping Federate).

 Click Contract Mapping then Next in the Attribute Source & User Lookup page since no changes are to be made in this page. In the Contract Fulfillment page use the following choices in the drop-down menus then click Next

Source: Adapter (HTMLFormSimplePCV)

Value: username

- 2. Once done click Next then Next. Click Done.
- 3. Once all the risk levels are mapped correctly, click **Done** at the bottom of the page.

Ping PingFederate				? (
MAIN		Done	(\otimes)		
		SUCCESS			
ldentity Provider		Simple - (Policy Contract) 🗸 🗸	\otimes		
E Comios Devidor		Contract Mapping			
Service Provider	RISK LE	VEL 5			
(A) OAuth Server	Simp	e - (Policy Contract) \checkmark \times			
	Contra	t Mapping			
SETTINGS	SUCCE	23			
& Socurity	Simp	e - (Policy Contract) × ×			
© Security	Contra	t Mapping			
≒ System					
Copyright © 2003-2019 Ping identity Corporation All rights reserved Version 10.0.0.15			Cano	el Done	

4. In the next screen, Click Save to save the configuration for the Device Risk Policy

PingFederate [®]					? (
MAIN	Authentication policies d to form policies. Ensure t	efine how PingFederate authenticates hat successful paths end with authenti	users. Selectors and authentication cation policy contracts to reuse map	sources can be conditionapping configuration across	ally chained together in paths protocols and applications.
名 Identity Provider	IDP AUTHENTICAT	ION POLICIES			
E Service Provider	FAIL IF POLICY ENG	GINE FINDS NO AUTHENTICATION SC	DURCE		
OAuth Server	Policy	Authentication Sources	Policy Contracts	Enabled	Action
SETTINGS	Device Risk Policy	HTMLFormSimplePCV DeviceRiskAdapter PingID	Simple		Select Action 🗸
Security	Add Policy				
Copyright © 2003-2019 Ping Identity Corporation All rights reserved Version 10.0.015				Cancel	Next Save

Troubleshooting

Follow these steps to identify issues impacting the normal operation of the integration described in this document.

Traditional Implementation

Validate the prerequisites

Make sure the prerequisites described in the Summary chapter are all satisfied:

→ Check the versions of Forcepoint CASB and Ping Federate in use are listed as compatible

Forcepoint CASB 2020 R2 Ping Federate 9.2 or 10.0

- → Verify the integration component correctly operates on a clean CentOS 7.x or Ubuntu 18.04 machine with at least 2GB RAM and 20GB free storage and the system needs to be 64-bit
- → The API port must be accessible through the firewall
- → The Risk Exporter API SSL certificate must be trusted by the Ping host machine
- \rightarrow User must have sudo permissions to run install.sh and setup.sh scripts
- \rightarrow Check that the user can download the necessary files with the below commands:

wget --content-disposition <u>https://frcpnt.com/fp-riskexporter-api-latest</u> wget --content-disposition <u>https://frcpnt.com/ping-connector-latest</u>

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

→ Check the **host machine** (which has ping Federate appliance) has network connectivity to the Risk Exporter API, execute the following command on the **host machine**:

curl -I https://<Risk Exporter hostname or IP>:5000

replacing the Risk Exporter hostname with the ones in use. Please check the first line of the result of the command above is:

HTTP/1.0 200 OK

Check all components are configured and running properly

Make sure the products and services involved into this integration are configured as expected and they are running:

→ Check the risk exporter API is configured and running properly. Check there are no errors on the following page:

https://<ping federate host machine ip>:5000/casb/healthcheck

replacing the <ping federate host machine ip> with the one in use. Check that the following messages appear on the healthcheck URL:

casb-url available - OK!

casb-url connection is successful - OK!

→ Check the risk exporter logs file: From the home directory of **fp-riskexporter-api/logs/** check the log file **risk-score-api.log**

Check there are no error messages in this log file.

Docker Implementation

Validate the prerequisites

Make sure the prerequisites described in the Summary chapter are all satisfied:

 \rightarrow Check the versions of Forcepoint CASB and Ping Federate in use are listed as compatible

Forcepoint CASB 2020 R2 Ping Federate 9.2 or 10.0

- → Verify the integration component correctly operates on a linux based machine with an existing docker engine and a minimum of 2GB RAM and 20GB free storage and the system needs to be 64-bit
- → The Risk Exporter API SSL certificate need to be trusted by the ping host machine

Check network connectivity

Make sure firewalls or other security appliances are not impacting the network connectivity necessary for the operation of all components involved into this integration:

→ Check the host machine (which has ping Federate appliance) has network connectivity to the Risk Exporter API. Execute the following command on the host machine:

curl -I https://<Risk Exporter hostname or IP>:5000

replacing the Risk Exporter hostname with the ones in use. Please check the first line of the result of the command above is:

HTTP/1.0 200 OK

Check all components are configured and running properly

Make sure the products and services involved into this integration are configured as expected and they are running:

→ Check the risk exporter API is configured and running properly: Check there are no errors on the following page:

https://<ping federate host machine ip>:5000/casb/healthcheck

replacing the <ping federate host machine ip> with the one in use. Check that the following messages appear on

the healthcheck URL:

casb-url available - OK!

casb-url connection is successful - OK!

 \rightarrow Check the logs for **fp-riskexporter-api** container:

docker logs fp-riskexporter-api | tail

Check the output is similar to the one below and has no errors:

Configs Initialized

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the global human-centric cybersecurity company transforming the digital enterprise by continuously adapting security response to the dynamic risk posed by individual users and machines. The Forcepoint human point system delivers risk-adaptive protection to continuously ensure trusted use of data and systems. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries.

© 2020 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint. All other trademarks used in this document are the property of their respective owners.