Configure Silverfort for PingFederate

Release 3.8

Table of Contents

1 Configure Silverfort with PingFederate

This topic describes how to configure PingFederate to use Silverfort authentication as part of an authentication policy. When this is configured, user attempts to access a resource protected by PingFederate will, optionally and according to the policies defined, be redirected to Silverfort. On Silverfort, a policy will be applied which can be configured to send an MFA request to the user. The result of this policy passed back to Ping Fed, to complete the policy chain there, and either approve or deny the original request.

This configuration involves deploying a Silverfort Adapter on PingFederate.

1.1 Benefits

This integration extends the capabilities of PingFederate to use Silverfort authentication policies and MFA.

It also extends Silverfort authentication to include cloud environments that use cloud-based authentication methods, such as Ping One.

1.2 Integration steps

The integration with PingFederate involves these steps, which are described in the following sections:

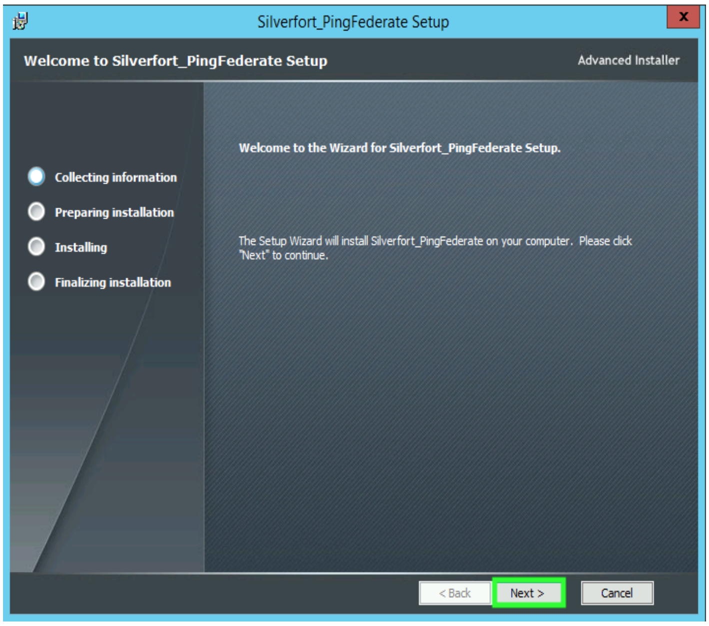
- Install Silverfort Adapters on PingFederate instance
- Configure Adapters on PingFederate
- Configure PingFederate apps on Silverfort (Settings)
- Configure Policy Contract & Policy on PingFederate, using Silverfort authentication as a step in the chain
- Configure Silverfort Policy for users authenticating with PingFederate

1.3 PingFederate configuration

These steps are performed on the PingFederate instance.

1.3.1 Install the Silverfort Adapter

1. Download the Silverfort PingFederate Installer to the host with the PingFederate instance, from here.
2. Run the installer.



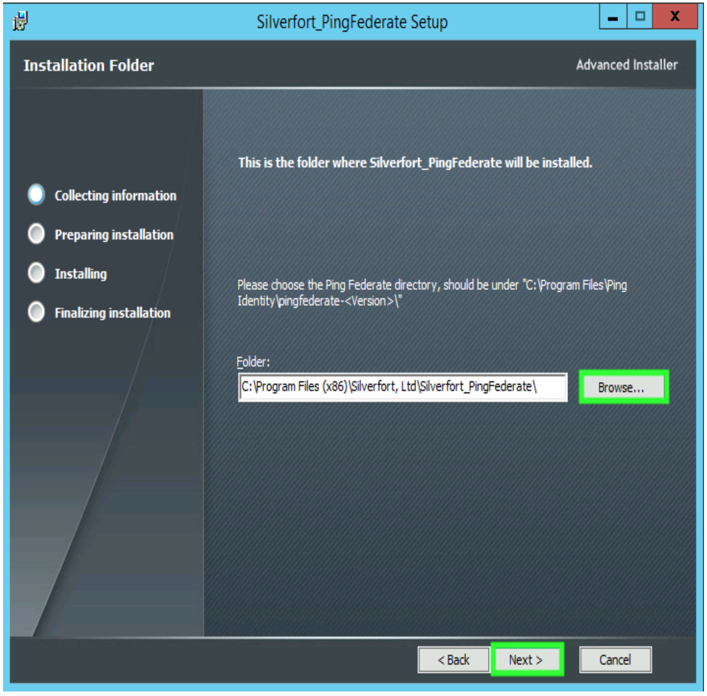
Silverfort_PingFederate Setup

Welcome to Silverfort_PingFederate Setup

Welcome to the Wizard for Silverfort_PingFederate Setup.

The Setup Wizard will install Silverfort_PingFederate on your computer. Please click "Next" to continue.

3. Select the root folder for the PingFederate instance, then click **Next**



Silverfort_PingFederate Setup

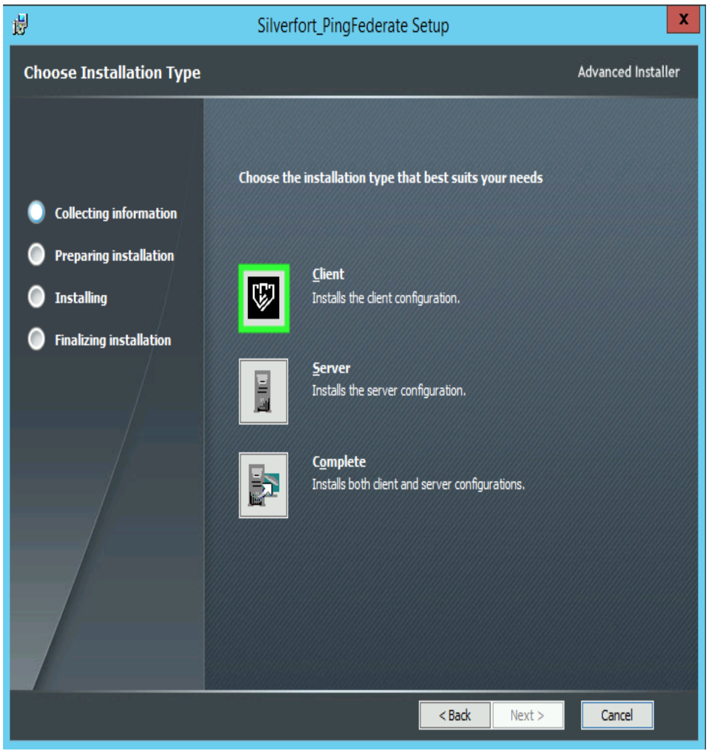
Installation Folder

This is the folder where Silverfort_PingFederate will be installed.

Please choose the Ping Federate directory, should be under "C:\Program Files\Ping Identity\pingfederate-<Version>\"

Folder: C:\Program Files (x86)\Silverfort, Ltd\Silverfort_PingFederate\

4. Select **Client**, and then click **Next**, to complete the installation. The Silverfort Adapters will then be included in the list of available adapters in PingFederate.



Choose the installation type that best suits your needs

Client
Installs the client configuration.

Server
Installs the server configuration.

Complete
Installs both client and server configurations.

1.3.2 Configure PingFederate adapters

These adapters are configured on PingFed:

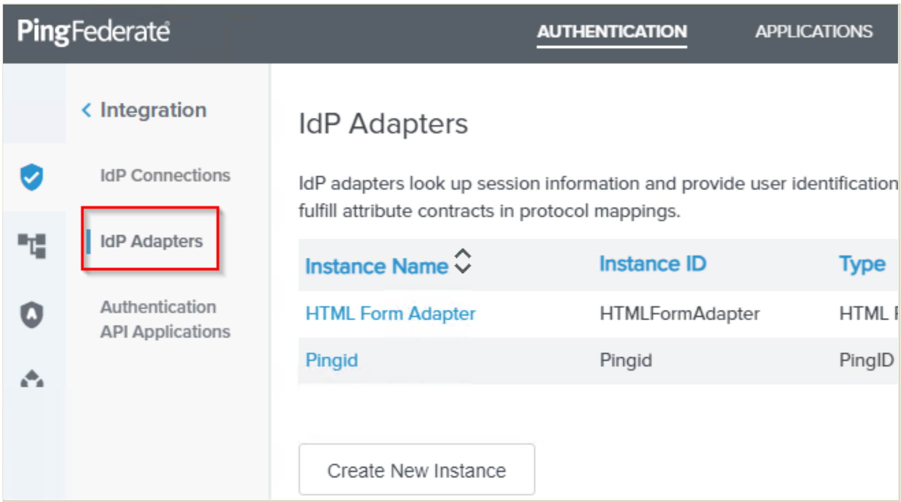
Silverfort Adapter - this is a mandatory adapter in order to use Silverfort

- Silverfort Collector Adapter - this is optional; use it if you plan to use PingID as an authentication token
- PingID Adapter - optional; use this if you plan to use PingID

1.3.2.1 Silverfort Adapter

Create an adapter for Silverfort:

1. In PingFederate, select **IdP Adapters** from the home page, and then **IdP Adapters** from menu on the left.



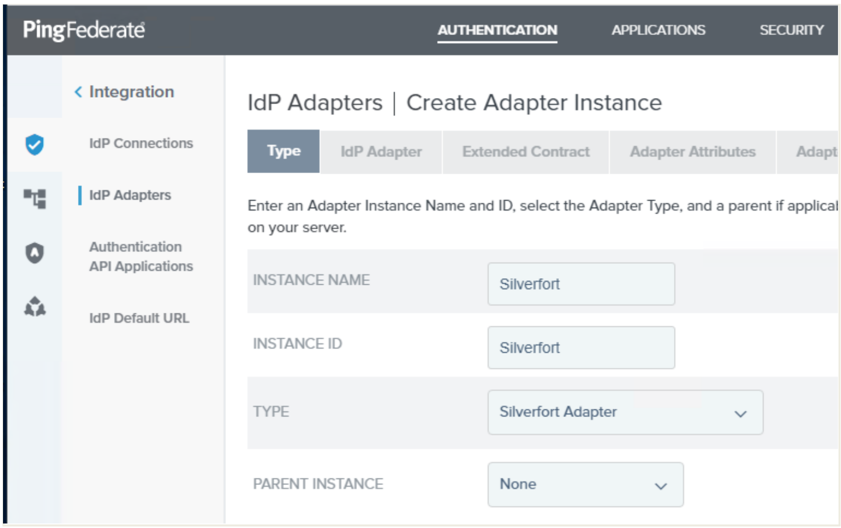
IdP Adapters

IdP adapters look up session information and provide user identification
fulfill attribute contracts in protocol mappings.

Instance Name	Instance ID	Type
HTML Form Adapter	HTMLFormAdapter	HTML F
Pingid	Pingid	PingID

2. Click **Create New Instance.**
3. Enter a **Name** & **Instance Id** (freetext).
4. For the TYPE, select type **Silverfort Adapter**, from the list.

5. Leave the Parent Instance as **None**, then click Next.

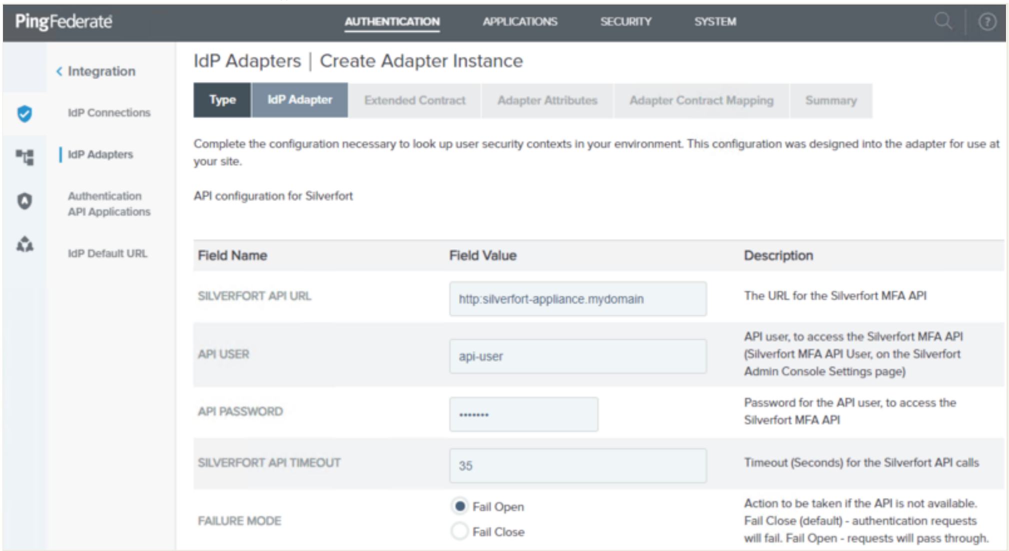


IdP Adapters | Create Adapter Instance

Enter an Adapter Instance Name and ID, select the Adapter Type, and a parent if applical on your server.

INSTANCE NAME	Silverfort
INSTANCE ID	Silverfort
TYPE	Silverfort Adapter
PARENT INSTANCE	None

6. Enter the URL of the Silverfort API (of the form https://silverfort-appliance.FQDN), where *FQDN* is the fully qualified domain name.
7. Enter the Silverfort **API user** and **password**, (for steps to obtain this, see /document/preview/19030#UUIDbf9fd4d713e760532c0f6872056ec572).Silverfort Authentication API Reference
8. Optionally, adjust the timeout period.
9. Select the **Fail Mode**. This is the action to be taken if there is no response from the Silverfort API. Default is Fail Close (request is failed).



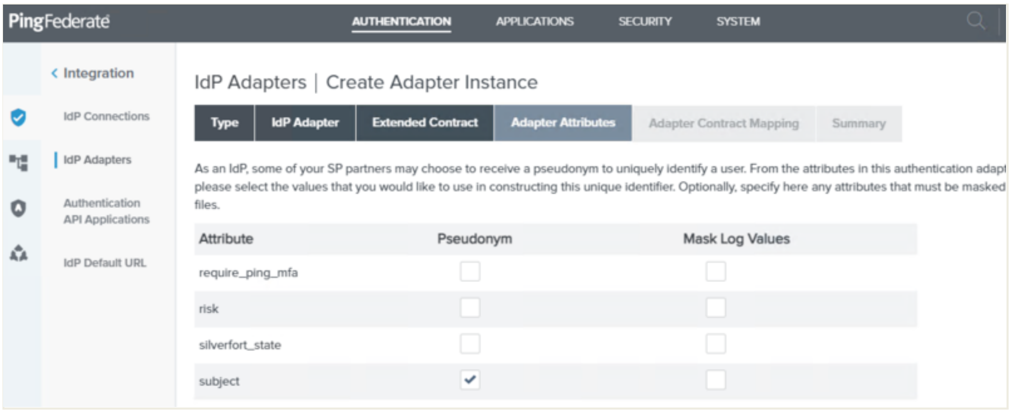
IdP Adapters | Create Adapter Instance

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

API configuration for Silverfort

Field Name	Field Value	Description
SILVERFORT API URL	http:silverfort-appliance.mydomain	The URL for the Silverfort MFA API
API USER	api-user	API user, to access the Silverfort MFA API (Silverfort MFA API User, on the Silverfort Admin Console Settings page)
API PASSWORD	•••••••	Password for the API user, to access the Silverfort MFA API
SILVERFORT API TIMEOUT	35	Timeout (Seconds) for the Silverfort API calls
FAILURE MODE	● Fail Open ○ Fail Close	Action to be taken if the API is not available. Fail Close (default) - authentication requests will fail. Fail Open - requests will pass through.

10. Click **Next**.
11. Select the '*subject*' attribute.



IdP Adapters | Create Adapter Instance

As an IdP, some of your SP partners may choose to receive a pseudonym to uniquely identify a user. From the attributes in this authentication adapt please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked files.

Attribute	Pseudonym	Mask Log Values
require_ping_mfa	□	□
risk	□	□
silverfort_state	□	□
subject	☑	□

12. Click **Save**. The new adapter will appear in the list.

1.3.2.2 PingID

If you are using PingID as an authentication token, add another adapter, the *Silverfort Collector Adapter*.

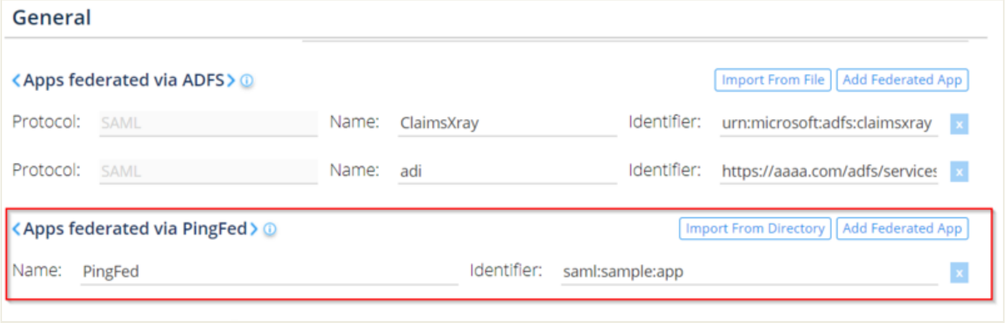
Repeat the steps above, but in step 4, select **Silverfort Collector Adapter**. This option does not have a Fail Mode (step 9).

You must also create a PingID adapter. Contact your Ping support team for details for this. Silverfort requires version 2.7 or later for this adapter.

1.4 Configure Silverfort

On Silverfort, you specify the PingFederate applications that will use Silverfort authentication policies as part of the PingFederate authentication chain.

1. Navigate to the **Settings** page on the Silverfort Admin Console.
2. Scroll down to **<Apps federated via PingFed>**, in the General section.



General

<Apps federated via ADFS>

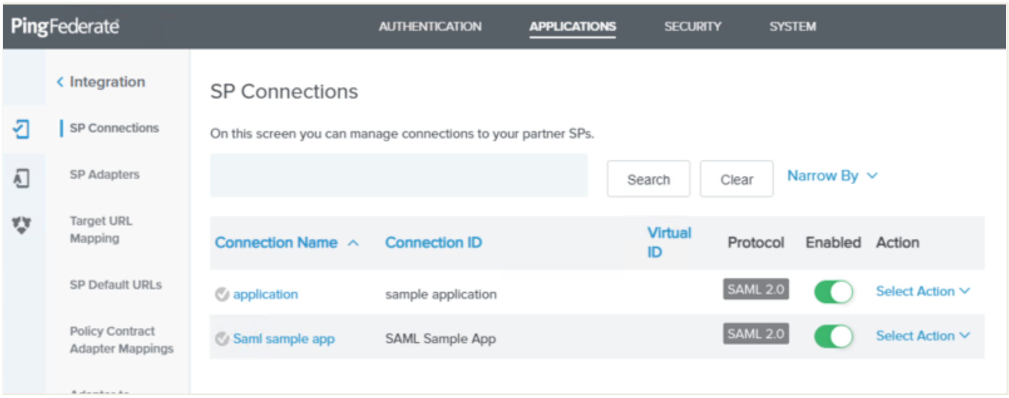
Protocol: SAML Name: ClaimsXray Identifier: urn:microsoft:adfs:claimsxray

Protocol: SAML Name: adi Identifier: https://aaaa.com/adfs/services

<Apps federated via PingFed>

Name: PingFed Identifier: saml:sample:app

3. Click **Add Federated App.**
4. Enter a name for the app. This is the name that will appear when creating Silverfort authentication policies, and in log records.
5. Enter the **Identifier** for the App. To obtain this, follow these steps:
   a. On Ping Federate, select **SP Connections** from the home page. This will show a list of Service Providers (Applications).



SP Connections

On this screen you can manage connections to your partner SPs.

Connection Name	Connection ID	Virtual ID	Protocol	Enabled	Action
application	sample application		SAML 2.0	●	Select Action
Saml sample app	SAML Sample App		SAML 2.0	●	Select Action

   b. For the SP you wish to add in Silverfort, take **Connection ID**, convert to lower case and replace spaces with colons (":"). For example, *SAML Sample App* becomes *saml:sample:app.* Use this as the Identifier.
6. Click **Save Changes** (bottom of page).

1.5 Use the Silverfort Adapters

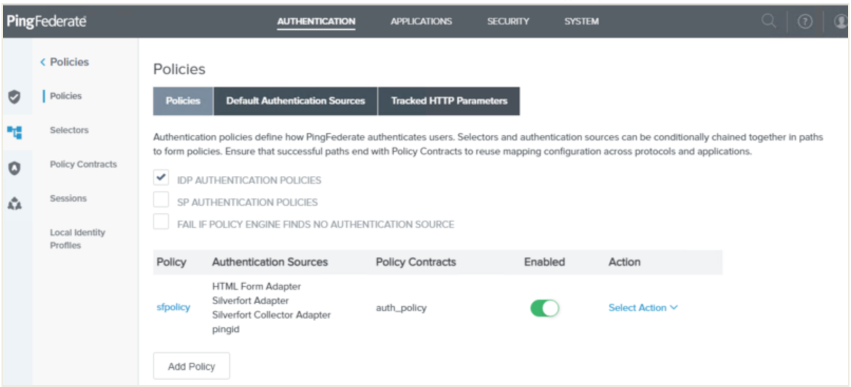
Once the integration between your Silverfort and Ping Federation instances is established, you create authentication policies on Ping Federation that use Silverfort as part of the authentication chain.

This involves creating a policy on PingFederate and an associated policy on Silverfort.

1.5.1 Create a PingFederate Policy using Silverfort in the authentication chain

1.5.1.1 Create a PingFederate Policy Contract

1. On PingFederate, select **Policies** from the home page.



Authentication policies define how PingFederate authenticates users. Selectors and authentication sources can be conditionally chained together in paths to form policies. Ensure that successful paths end with Policy Contracts to reuse mapping configuration across protocols and applications.

☑ IDP AUTHENTICATION POLICIES

□ SP AUTHENTICATION POLICIES

□ FAIL IF POLICY ENGINE FINDS NO AUTHENTICATION SOURCE

Policy	Authentication Sources	Policy Contracts	Enabled	Action
sfpolicy	HTML Form Adapter Silverfort Adapter Silverfort Collector Adapter pingid	auth_policy	●	Select Action ⌄

2. Select **Policy Contracts** from the menu on the left.
3. Click **Create New Contract.**
4. Enter a name for the contract, and then click **Next**, **Next** again, and then **Save**.

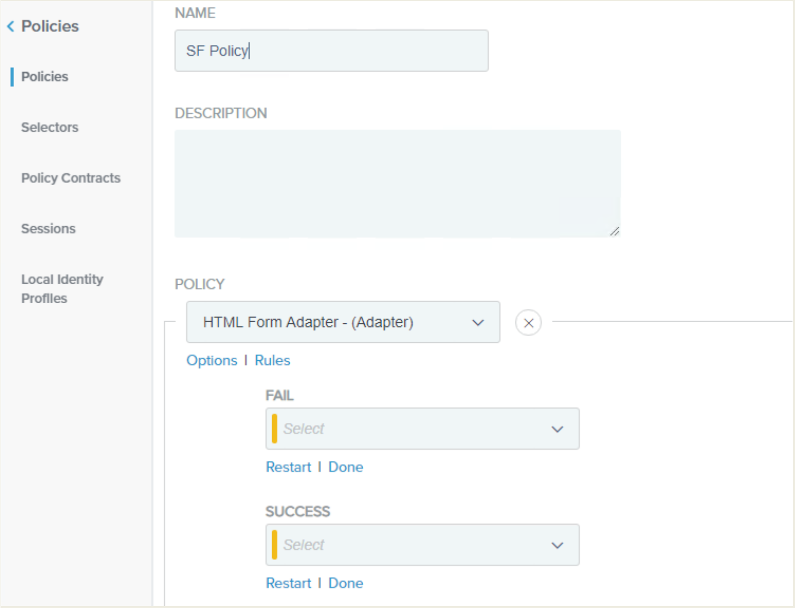
1.5.1.2 Create a PingFederate Policy

The PingFederate policy will determine how the authentication request is handled. In this configuration, the Silverfort adapter will be selected in one of the steps of the policy.

See here for more details about defining PingFederate policies.

The PingFederate policy described here uses the HTMLFormAdapter

1. On PingFederate, select **Policies** from the menu (or home page).
2. Click **Add Policy**.
3. Enter a **name** and **description** for the policy.
4. For the POLICY, select **IdP Adapters**, and then, from the list, **HTMLFormAdapter**. This is the first step of the policy. This step has two possible outcomes, SUCCESS and FAIL, which will be configured in the following steps.



NAME

SF Policy

DESCRIPTION

POLICY

HTML Form Adapter - (Adapter)

Options | Rules

FAIL

Select

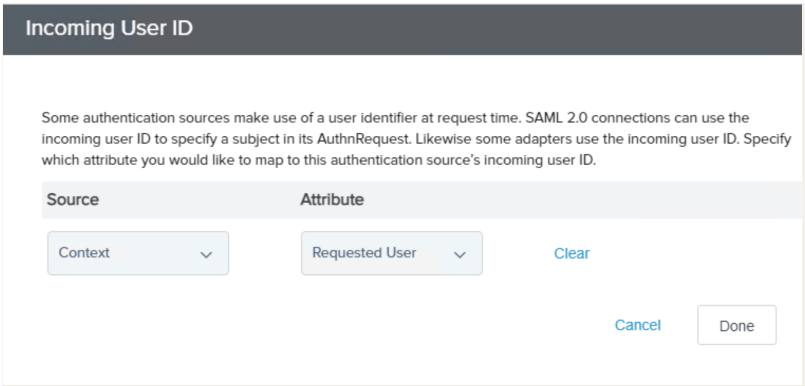
Restart | Done

SUCCESS

Select

Restart | Done

5. Click **Options**.
6. For the **Source**, select *Context*, and for the **Attribute**, select *Requested User*.

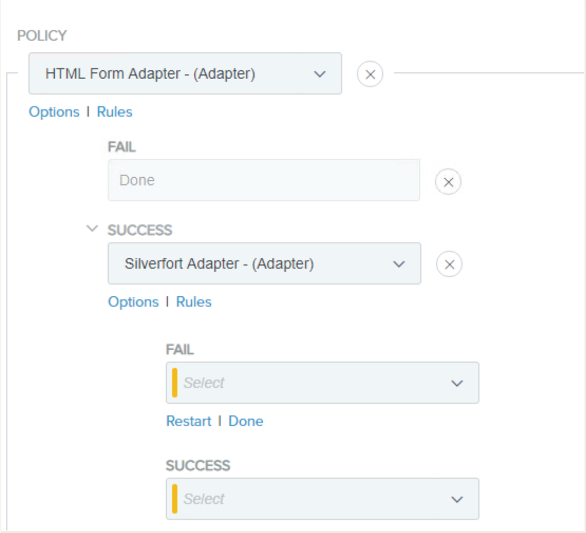


Incoming User ID

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.

Source	Attribute
Context	Requested User

7. For the FAIL case for this step, select **Done** (if the user fails this first step of the authentication with PingFederate, no further actions are done).
8. For the SUCCESS case, select the **Silverfort Adapter.** This adds a second step in the policy chain, which refers the request to Silverfort, using the Silverfort Adapter. This step also has two outcomes, SUCCESS and FAIL, which will be configured.



POLICY

HTML Form Adapter - (Adapter)

Options | Rules

FAIL

Done

SUCCESS

Silverfort Adapter - (Adapter)

Options | Rules

FAIL

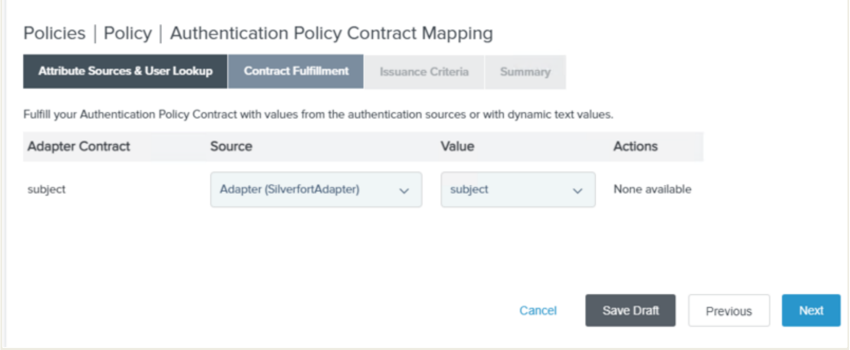
Select

Restart | Done

SUCCESS

Select

9. Click **Options** (under the Silverfort Adapter), and select **Source**, *Context*, and **Attribute**, *Requested User*. This passes the user requesting authentication (with PingFed) to Silverfort, where it will be evaluated by a Silverfort policy and Risk Engine.
   The Silverfort policy (see below, next section), can have the usual actions, including MFA, to trigger an MFA request to the user. It will return a result, success or fail, which is returned through the adapter to the PingFederate policy.
10. For the FAIL case, select **DONE**. If the Silverfort policy returns a fail result to PingFederate, the original authentication request has failed, and there are no further steps.
11. For the SUCCESS case, select **Policy Contracts**, and then, from the list, the Silverfort Policy contract created above.
12. Click **Contract Mapping** (below the SUCCESS option).
13. Click **Next**.
14. For the attribute *subject*, select for the **Source**, select *Silverfort (Adapter)*, and, then, for **Value**, select *subject* , to map this attribute to equivalent attribute in the Silverfort adapter.


Policies | Policy | Authentication Policy Contract Mapping
Attribute Sources & User Lookup
Contract Fulfillment
Issuance Criteria
Summary
Cancel
Save Draft
Previous
Next

Fulfill your Authentication Policy Contract with values from the authentication sources or with dynamic text values.

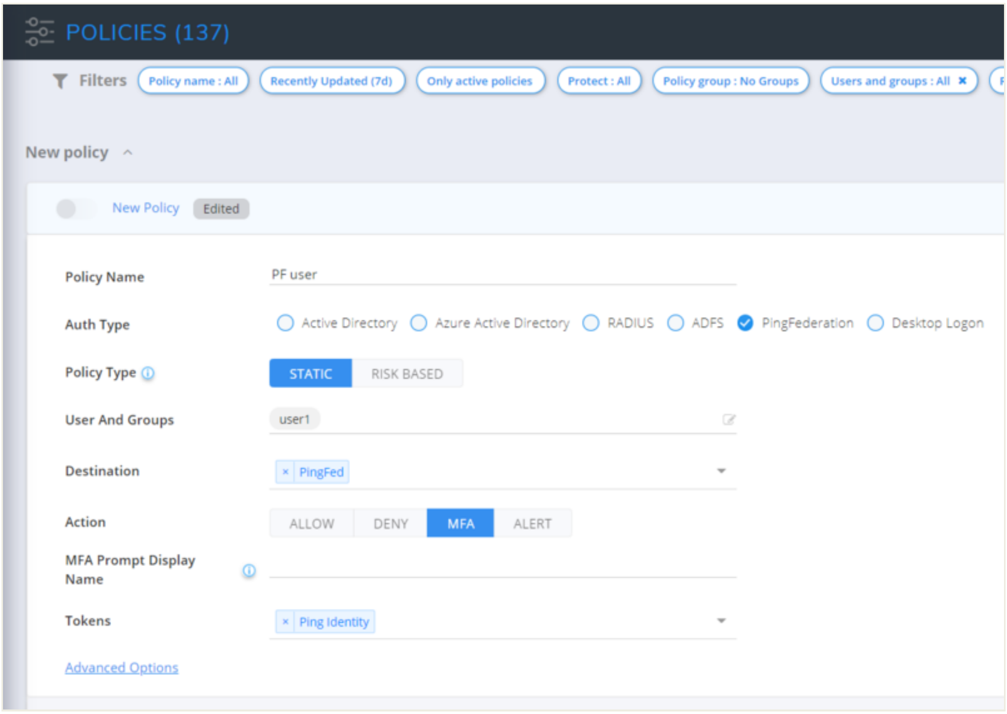
Adapter Contract	Source	Value	Actions
subject	Adapter (SilverfortAdapter)	subject	None available

15. Click **Next**, and then **Done**, to complete the mapping.
    This completes a basic policy, with two steps, one on PingFederate (using the HTML Form Adapter), and a second step (if the first succeeds) using a Silverfort policy, through the Silverfort Adapter.

1.5.2 Create a Silverfort authentication policy for requests referred from a PingFederate policy

This policy will be applied on a request from PingFederate (for example, in the PingFederate policy created above), if the policy applies to the user in the request.

1. On the Admin Console, navigate to the POLICIES page.
2. Click **CREATE POLICY.**
3. Enter a name for the policy.



POLICIES (137)

Filters: Policy name : All | Recently Updated (7d) | Only active policies | Protect : All | Policy group : No Groups | Users and groups : All ✖

New policy

New Policy Edited

Policy Name: PF user

Auth Type: ○ Active Directory ○ Azure Active Directory ○ RADIUS ○ ADFS ● PingFederation ○ Desktop Logon

Policy Type: [✓ STATIC] RISK BASED

User And Groups: user1

Destination: × PingFed

Action: ALLOW DENY [✓ MFA] ALERT

MFA Prompt Display Name:

Tokens: × Ping Identity

Advanced Options

4. Select for Auth Type, **PIng Federation.** This indicates that the source of the request is a PingFederate policy.
5. Select the users and groups covered by the policy.
6. Select destination, **PingFederate** .
7. Select the **Action**. Typically this will be MFA, to trigger an MFA from Silverfort on authentication requests.
8. Select the MFA tokens. You can select any tokens that are paired for the user, including the PingID token and the Silverfort Desktop App and Mobile App tokens.
9. Complete the policy.
10. Click **Save Changes.**