

# PingFederate<sup>®</sup>

## Duo Security Integration Kit

Version 2.1

## User Guide



© 2016 Ping Identity® Corporation. All rights reserved.

PingFederate Duo Security Integration Kit User Guide  
Version 2.1  
April, 2016

Ping Identity Corporation  
1001 17th Street, Suite 100  
Denver, CO 80202  
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)

Fax: 303.468.2909

Web Site: [www.pingidentity.com](http://www.pingidentity.com)

## Trademarks

Ping Identity, the Ping Identity logo, PingFederate, PingOne, PingConnect, and PingEnable are registered trademarks of Ping Identity Corporation ("Ping Identity"). All other trademarks or registered trademarks are the property of their respective owners.

## Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. Ping Identity disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Ping Identity or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Ping Identity or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

## Document Lifetime

Ping Identity may occasionally update online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to [documentation.pingidentity.com](http://documentation.pingidentity.com) for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **April 28, 2016**.

# Contents

## Table of Contents

<b>INTRODUCTION.....</b>	<b>4</b>
SUPPORTED FEATURES.....	4
PREREQUISITES.....	4
ZIP MANIFEST .....	4
<b>INSTALLATION AND SETUP.....</b>	<b>4</b>
GETTING STARTED .....	5
<i>Obtain Your Integration Key, Secret Key and API Host .....</i>	<i>5</i>
INSTALLATION.....	5
CONFIGURATION .....	6
<i>Configuring the Duo Security Adapter.....</i>	<i>6</i>
<i>Configuring a Composite Adapter.....</i>	<i>8</i>
USE CASES.....	12
<i>Primary Use Case .....</i>	<i>12</i>
LOGGING.....	13

# Introduction

This user guide is intended for use by PingFederate clients, who would like to leverage Duo Security authentication for two-factor authentication.

The Duo Security Integration Kit includes a PingFederate custom adapter that is integrated with the Duo web security SDK in order to provide additional authentication for the client application.

## Supported Features

Browser-based SP-initiated and IdP-initiated SSO as second factor of a composite adapter

## Prerequisites

This document assumes that you already have the following installed and configured:

- A functional PingFederate environment, version 7.1+
- JDK version 7+
- At least one IdP adapter for use as the primary form of authentication (e.g., HTML Form Adapter leveraging an LDAP Password Credential Validator (PCV))
- A Duo Security integration, which should include the following for configuration in the Duo Security adapter in PingFederate:
  - Integration key
  - Secret key
  - API hostname

## ZIP Manifest

The distribution ZIP file for the Connector contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation.
- `/dist` – contains libraries needed for the Connector:
  - `pf-duo-security-integration-kit-2.1.jar` – PingFederate Duo Security Integration Kit
  - `duo.form.login.template.html` - Template for Duo Security login page
  - `duo-web/` - Folder containing Duo login page content

## Installation and Setup

The following sections explain how to obtain the necessary information required for installing and configuring this Integration Kit. Please follow these sections completely and in order.

## Getting Started

Before you can configure this Connector, you will need to complete the following steps.

---

**Tip:** Some of the following steps result in information to be used at a later time in this User Guide. It is recommended that you copy this information to a secure location to reference in later steps.

---

### Obtain Your Integration Key, Secret Key and API Host

The Duo Security Integration Kit's requires you to protect an application using the Web SDK.

#### To Your Integration Key, Secret Key and API Host from Duo Security:

1. Log into Duo Security
2. Go to the **Applications**
3. Click **Protect and Application** and type Web SDK in the search bar, the select **Protect this application** under Web SDK
4. Make note of the **Integration Key, Secret Key, and API Hostname**

Web SDK Authentication Log Remove Application

**Setup Instructions**  
See the [Duo Web SDK Documentation](#) to integrate Duo into your custom web application.  
Not the sysadmin? [Add him/her as a Duo administrator](#)

**Details** Reset Secret Key

Treat your secret key like a password. Don't write it down or share it with anyone.

Integration key	DIEIWPWBNS180DNU1KSL
Secret key	<a href="#">Click to view</a>
API hostname	api-a5f635d0.duosecurity.com

## Installation

1. From the /dist folder in *pf-duo-security-integration-kit-2.1.zip*, copy the following files to the directory <PingFederateInstall>/pingfederate/server/default/deploy/ in your PingFederate:
  - pf-duo-security-integration-kit-2.1.jar
  - /duo-web/\* (the folder and contents in its entirety)

- From the /dist folder in *pf-duo-security-integration-kit-2.1.zip*, copy the following files to the directory <PingFederateInstall>/pingfederate/server/default/conf/template/ in your PingFederate:
  - duo.form.login.template.html
- Start or restart PingFederate.

## Configuration

To Configure a Duo Security adapter, please follow the following instructions

### Configuring the Duo Security Adapter

- Log into the PingFederate admin console and click **Adapters** under **IdP Configuration >> Application Integration Settings**.
- Click **Create New Instance**.
- Enter the Instance Name and ID, choose **Duo Adapter 2.1**, and click **Next**.

#### Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
Enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.					
INSTANCE NAME	<input type="text" value="DuoldpAdapter"/>				
INSTANCE ID	<input type="text" value="DuoldpAdapter"/>				
TYPE	<input type="text" value="Duo Adapter 2.1"/>				<a href="#">Visit PingIdentity.com for additional types</a>
PARENT INSTANCE	<input type="text" value="None"/>				
					<input type="button" value="Cancel"/> <input type="button" value="Next"/>

- On the IdP Adapter page, enter the applicable information requested, and click **Next**.

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.

Duo Adapter

Field Name	Field Value	Description
INTEGRATION KEY	DI1BOQLVFXVPWIQD140G	The application integration key provided by Duo (must of the type 'WebSDK').
SECRET KEY	.....	The secret key provided by Duo (must of the type 'WebSDK').
API HOST	api-725630fe.duosecurity.com	The API hostname provided by Duo (i.e. api-XXXXXXXX.duosecurity.com)
SESSION STATE	<input checked="" type="radio"/> Globally <input type="radio"/> None	Determines how state is maintained within one adapter or between different adapter instances.
SESSION TIMEOUT	60	Session Timeout (in minutes). Leave blank for indefinite sessions. Ignored if 'None' is selected for Session State.
LOGIN TEMPLATE	duo.form.login.template.html	HTML template (in <pf_home>/server/default /conf/template) to render for login. The default value is duo.form.login.template.html.

Cancel Previous **Next**

5. Check the **Pseudonym**, and click **Next**.

Manage IdP Adapter Instances | 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 adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
subject	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES		

Cancel Previous **Next**

6. Review the adapter summary, and click **Done**.

Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Adapter Contract Mapping	Summary
IdP adapter instance summary information.					
<b>Create Adapter Instance</b>					
<b>Type</b>					
Instance Name	DuoIdPAdapter				
Instance Id	DuoIdPAdapter				
Type	Duo Adapter 2.1				
Class Name	com.pingidentity.clientservices.product.IntegrationKit.Duo.DuoIdPAdapter				
Parent Instance Name	None				
<b>IdP Adapter</b>					
Integration Key	D11B00LVPXVPW1QD140G				
API Host	api-725630fe.duosecurity.com				
Session State	Globally				
Session Timeout	60				
Login Template	duo.form.login.template.html				
<b>Extended Contract</b>					
Attribute	subject				
<b>Adapter Attributes</b>					
Mask all OAuth expression log values	false				
Pseudonym	subject				
<b>Adapter Contract Mapping</b>					
<b>Attribute Sources &amp; User Lookup</b>					
Data Sources	(None)				
<b>Adapter Contract Fulfillment</b>					
subject	subject (Adapter)				
<b>Issuance Criteria</b>					
Criterion	(None)				
					<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input type="button" value="Done"/>

7. Click **Save** to save the adapter that was just configured.

## Configuring a Composite Adapter

1. Click **Adapters** under **IdPConfiguration >> Application Integration Settings**.
2. Click **Create New Instance**.
3. Enter the Instance Name and ID, choose **Composite Adapter**, and click **Next**.

Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Summary
Enter an Adapter Instance Name and Id, select the Adapter Type, and a parent if applicable. The Adapter Type is limited to the adapters currently installed on your server.				
INSTANCE NAME	CompositelPAdapter			
INSTANCE ID	CompositelPAdapter			
TYPE	Composite Adapter			<a href="#">Visit PingIdentity.com for additional types</a>
PARENT INSTANCE	None			
				<input type="button" value="Cancel"/> <input type="button" value="Next"/>



- Click **Add a new row to 'Adapters'**, select an adapter that will be used as the primary form of authentication, and click **Update**. In this example, the HTML Form Adapter leveraging an LDAP PCV is used.
- Click **Add a new row to 'Adapters'** again, and add the Duo Security adapter that was just created. The Duo Security adapter will be used as the secondary form of authentication.

ADAPTER INSTANCE	POLICY	AUTHN CONTEXT WEIGHT	AUTHN CONTEXT OVERRIDE	Action
HTMLFormIdPAdapte	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move down Edit Delete
DuoldPAdapter	<input checked="" type="radio"/> Required <input type="radio"/> Sufficient	3		Move up Edit Delete

[Add a new row to 'Adapters'](#)

- Click **Add a new row to 'Input User ID Mapping'**, select the Duo Security adapter as the **Target Adapter**, the designated user ID for **User ID Selection**, and click **Update**.

TARGET ADAPTER	USER ID SELECTION	Action
DuoldPAdapter	username	Edit Delete

[Add a new row to 'Input User Id Mapping'](#)

- Add **Attribute Name Synonyms** if needed as in this example:

NAME	SYNONYM	Action
subject	username	Move down Edit Delete
username	subject	Move up Edit Delete

[Add a new row to 'Attribute Name Synonyms'](#)

- Click **Next**.
- Extend the contract by adding an attribute, and click **Next**.

## Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Summary
------	-------------	-------------------	--------------------	---------

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.

Extend the Contract	Action
subject	<a href="#">Edit</a>   <a href="#">Delete</a>
<input type="text"/>	<input type="button" value="Add"/>

[Cancel](#)

10. Select **subject** as the **Pseudonym**.

## Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Summary
------	-------------	-------------------	--------------------	---------

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 adapter, please select the values that you would like to use in constructing this unique identifier. Optionally, specify here any attributes that must be masked in log files.

Attribute	Pseudonym	Mask Log Values
subject	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> MASK ALL OGNL-EXPRESSION GENERATED LOG VALUES		

[Cancel](#)

11. Review the adapter summary, and click **Done** then **Save**.

## Manage IdP Adapter Instances | Create Adapter Instance

Type	IdP Adapter	Extended Contract	Adapter Attributes	Summary
------	-------------	-------------------	--------------------	---------

IdP adapter instance summary information.

### Create Adapter Instance

**Type**

Instance Name	CompositeldPAdapterForDuo
Instance Id	CompositeldPAdapterForDuo
Type	Composite Adapter
Class Name	com.pingidentity.pf.adapters.composite.CompositeAdapter
Parent Instance Name	None

**IdP Adapter**

Adapters	HTMLFormIdPAdapter, Required, 3, {no value}
Adapters	DuoldPAdapter, Required, 3, {no value}
Input User Id Mapping	DuoldPAdapter, username
Attribute Name Synonyms	subject, username
Attribute Name Synonyms	username, subject
Attribute Insertion	Add To Back

**Extended Contract**

Attribute	subject
-----------	---------

**Adapter Attributes**

Mask all OGNL expression log values	false
Pseudonym	subject

[Cancel](#) [Previous](#) [Done](#)

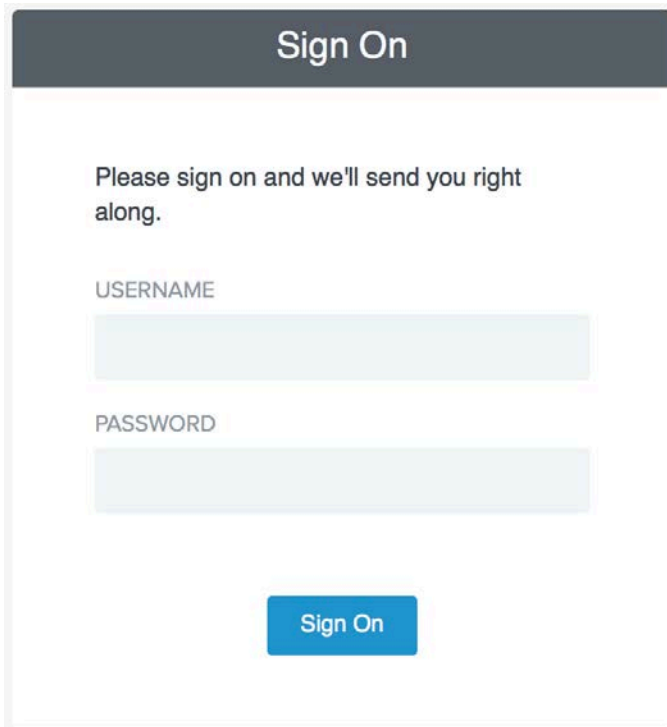
12. Configure or modify the connection(s) to your SP partner(s) using the Composite Adapter Instance.

For more information, see [Identity Provider SSO Configuration](#) in the *PingFederate Administrator's Manual*.

## Use Cases

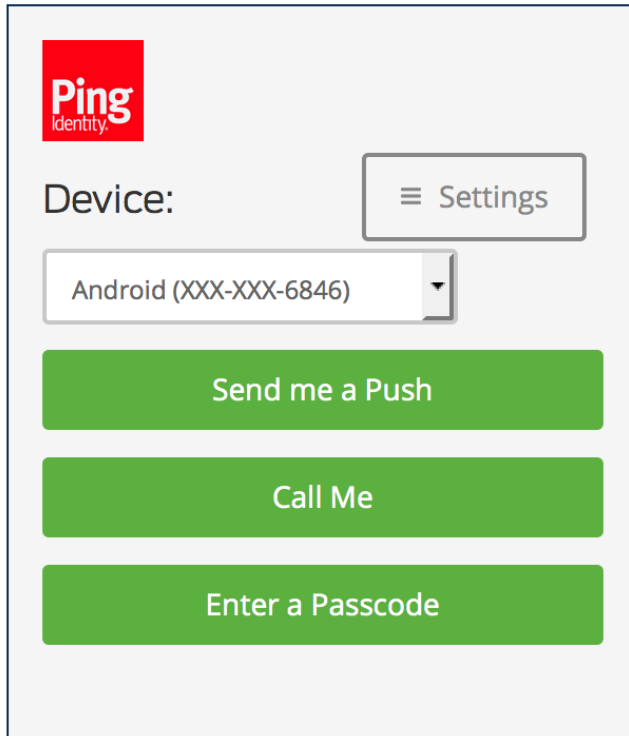
### Primary Use Case

1. Open a browser and go to the IdP login form chosen as the primary form of authentication. In this example, the HTML Form Adapter was chosen.

A screenshot of a web-based login form titled "Sign On". The form has a dark grey header with the text "Sign On" in white. Below the header, there is a message: "Please sign on and we'll send you right along." followed by two input fields. The first field is labeled "USERNAME" and the second is labeled "PASSWORD". Both fields are empty and have a light blue border. Below the input fields is a blue button with the text "Sign On" in white.

2. Login using your credentials.
3. On the next screen, the Duo Security login form is presented for two-factor authentication.

## Two-Factor Authentication



The screenshot displays a mobile application interface for Two-Factor Authentication. At the top left is the Ping Identity logo. Below it, the text 'Device:' is followed by a 'Settings' button. A dropdown menu is open, showing 'Android (XXX-XXX-6846)'. Below the dropdown are three large green buttons: 'Send me a Push', 'Call Me', and 'Enter a Passcode'.

4. Login as appropriate.
5. If reached the target destination, two-factor authentication was a success.

### Logging

To enable various logging modes for the Duo Security adapter, add the following to `<PingFederateInstall>/pingfederate/server/default/conf/log4j.xml`:

```
<logger name="com.pingidentity.clientservices.product.integrationkit.duo">  
  <level value="[ DEBUG | INFO | WARN | ERROR ]"/>  
</logger>
```

Detailed training on using Log4j in PingFederate can be found at:

<https://ping.force.com/Support/PingIdentityKnBSearchHome?searchText=log4j>