Ping Identity™

PingFederate®

Integration Kit for Entrust IdentityGuard

Version 1.2.2

User Guide

PingFederate Integration Kit for Entrust IdentityGuard User Guide Version 1.2.2
May 2017 (Original: August 2012)
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

Trademarks

Ping Identity, the Ping Identity logo, PingFederate, and the PingFederate icon are trademarks or registered trademarks of Ping Identity Corporation.

All other trademarks or registered trademarks are the properties of their respective owners.

Disclaimer

This document is provided for informational purposes only, and the information herein is subject to change without notice. Ping Identity Corporation does not provide any warranties and specifically disclaims any liability in connection with this document.

Contents

Introduction

This PingFederate Integration Kit for Entrust IdentityGuard allows an enterprise to leverage its investment in the Entrust multi-factor authentication solution to provide secure single sign-on (SSO) for online services across Internet domains. The included Entrust IdentityGuard Adapter provides for multi-factor authentication in conjunction with a first-factor PingFederate adapter, such as one performing Integrated Windows Authentication (IWA) or the Lightweight Directory Access Protocol (LDAP).

Intended Audience

This document is intended for system administrators with experience in the configuration and maintenance of information-technology infrastructure. Knowledge of networking and user-management configuration is assumed as well as some familiarity with Entrust IdentityGuard and PingFederate.

Additional Resources

Administrators may want to review the PingFederate *Administrator's Manual*—in particular, information on integration kits and two-factor authentication.

Tip: If you encounter any difficulties with configuration or deployment, please try searching the Ping Identity Customer Portal (www.pingidentity.com/support-and-downloads/portal.cfm) under **Answers**.

ZIP Manifest

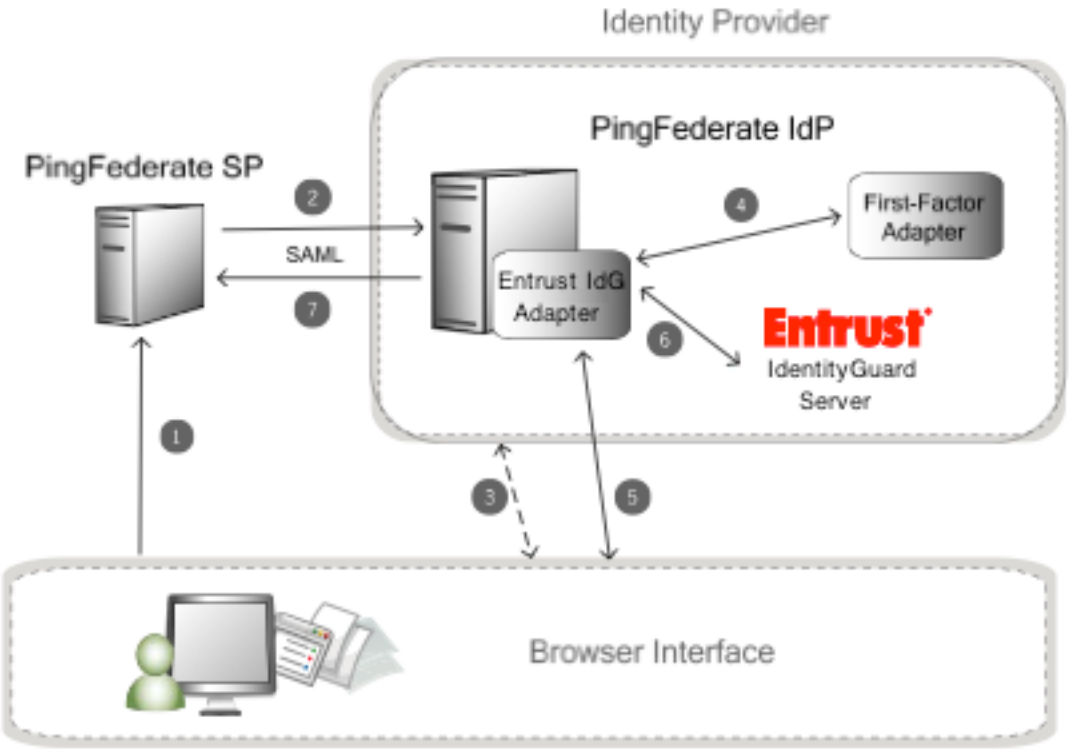
The distribution ZIP file for the Integration Kit contains the following:

- `/docs` – contains this documentation:
  - Entrust_IG_Integration_Kit_User_Guide.pdf – this document
- `/dist` – contains libraries needed for the Entrust IdentityGuard Adapter
  - `pf-entrust-identityguard-adapter-1.2.2.jar` - the Entrust IdentityGuard IdP Adapter for PingFederate
  - `/apis`
    - `IdentityGuardAuthAPIV6.jar` - the IdentityGuard authentication service client library
    - `jaxrpc.jar` - supporting 3rd party Java library required by IdentityGuard library
    - `mailapi.jar` - supporting 3rd party Java library required by IdentityGuard library

    - `saaj.jar` - supporting 3rd party Java library required by IdentityGuard library
    - `wsdl4j-1.5.1.jar` - supporting 3rd party Java library required by IdentityGuard library
- `/war`
    - `ig-adapter-security-code-challenge.war` – an application that prompts the user for a multi-factor authentication challenge

Overview

The following figure shows an SP-initiated SSO scenario integrating PingFederate into a multi-factor authentication scenario using Entrust IdentityGuard.

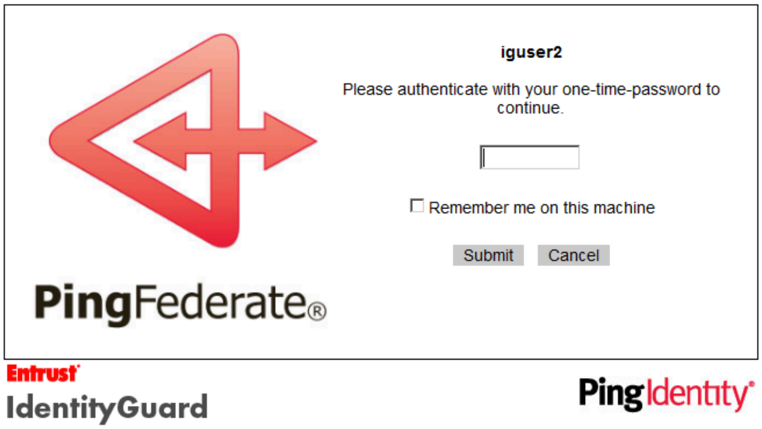


Processing Steps

1. The user initiates SSO from an SP application through a PingFederate SP server.

   Note: This SP-initiated scenario represents the optimal use case, one in which both the IdP and SP are using PingFederate. However, PingFederate accepts any valid SAML authentication request from an SP. In addition, you can enable IdP-initiated SSO; in this case, the user attempts SSO to an SP application from the IdP site, and the processing sequence would not include the next step.

2. The PingFederate SP server generates a SAML `AuthnRequest` to the PingFederate IdP server.
3. If not already logged on at the IdP, the user is challenged to authenticate.
4. The PingFederate IdP server obtains user-session information via the first-factor adapter.
5. The Entrust IdentityGuard Adapter requests an authentication challenge from the user. The actual authentication type depends on the adapter configuration as well as Entrust IdentityGuard server's policy.
   The following is an example screen for an out of band one-time-password challenge:



iguser2

Please authenticate with your one-time-password to continue.

□ Remember me on this machine

6. The Entrust IdentityGuard Adapter uses the username obtained by the first-factor adapter and the user's challenge response to verify the user and the code via the Entrust IdentityGuard Authentication API.
7. If the validation succeeds, the PingFederate IdP server generates a SAML assertion with the username as the Subject and passes it to the PingFederate SP server.
8. (Not shown) The user is logged on to the SP target application.

Supported Authenticators

The following authentication options are available as part of the Entrust IdentityGuard Integration Kit:

Authentication Type	Details
Grid Card	Users enter cell values from their uniquely generated and assigned grid card. Both printed and e-grid cards are supported. Temporary PIN authentication can be used as a backup if the user misplaces their grid card.

Token (Response Only)	Users enter their response generated by a hardware or software based one-time-password token. Temporary PIN authentication can be used as a backup if the user misplaces their token.
Token (Challenge Response)	Users enter their response generated by a hardware token after input a presented challenge into the device. Temporary PIN authentication can be used as a backup if the user misplaces their token.
One Time Password	Users enter a one-time-password that was sent to them out of band (e.g.: via SMS text message or e-mail).
Knowledge Based Authentication (Q&A)	Users respond to some registered questions randomly chosen by the Entrust IdentityGuard server.
Machine Authentication	Combined with other authenticators, this authentication type allows a user to register their machine with Entrust IdentityGuard so they can be transparently authenticated without user interaction. Registering a machine is performed by checking the box labeled "Remember me on this machine" on the challenge page. **Note:** This implementation requires browser cookies enabled. No application data (such as browser parameters) is sent to Entrust IdentityGuard server - only machine and sequence nonces are used. Please consult Entrust IdentityGuard documentation for more details.
Risk Based Authentication	Session related parameters (such as IP Address / IP Geo-location information) could be used to control how users are authenticated, challenged or rejected. An advanced adapter configuration setting dictates whether the "Normal" or "Enhanced" policy is used.
Mutual Authentication	Mutual authentication is supported by displaying a user's grid card or token serial number in the challenge page.

System Requirements

- PingFederate 6.4, 6.5, 6.9 or higher
- For IWA integration, the PingFederate IWA Integration Kit (available separately)

Note: This kit is not compatible with PingFederate 6.6 to 6.8.

Entrust IdentityGuard Requirements

- Entrust IdentityGuard 9.3 or higher (V6 Authentication API).

- If SSL is required for communications with the Authentication API, then the issuing CA or self-signed certificate must be imported into PingFederate to enable trust.
- Valid Entrust IdentityGuard accounts and authenticators for end users. If users are not yet enrolled, the Self-Service URL redirection feature can be used to let users enroll themselves via a portal.

Installation and Configuration

Setting up the Integration Kit involves:

- Installing the Entrust IdentityGuard Adapter
- Configuring PingFederate

Note: It is assumed that Entrust IdentityGuard is installed and its authentication service can be contacted from PingFederate.

Step 1—Install the Entrust IdentityGuard Adapter

1. Stop the PingFederate server if it is running.
2. From the integration kit `/dist/apis` directory, copy:
   - `IdentityGuardAuthAPIV6.jar`
   - `jaxrcp.jar`
   - `mailapi.jar`
   - `saaj.jar`
   - `wsdl4j-1.5.1.jar`

   into the directory `<PF-install>/server/default/lib`
3. From the integration kit `/dist` directory, copy:
   - `pf-entrust-identityguard-adapter-1.2.2.jar`
   - `/war/ig-adapter-security-code-challenge.war`

   into the directory `<PF-install>/server/default/deploy`
4. If you are using PingFederate 6.4 or 6.5 then modify the following configuration file with a text editor:
   - `pingfederate/server/default/data/config-store/org.sourceid.websso.authn.AdapterChainingManager.xml`

   Edit the file to include the Java class `com.pingidentity.adapters.entrust.IdentityGuardAdapter` as both a Non-Primary Adapter and Secondary Adapter.

   The resulting file contents should look similar to the following. Newly added lines are **bolded**.

```
<?xml version="1.0" encoding="UTF-8"?>
  <con:config xmlns:con="http://www.sourceid.org/2004/05/config">
```

```
    <con:map name="NonPrimaryAdapters">
      <con:item
name="com.pingidentity.adapters.vip.IdpVIPAdapter">true</con:item>
       <con:item
name="com.pingidentity.clientservices.product.integrationkit.entrust.IdentityGu
ardAdapter">true</con:item>
    </con:map>
    <con:map name="SecondaryAdapters">
      <con:item
name="com.pingidentity.adapters.vip.IdpVIPAdapter">true</con:item>
       <con:item
name="com.pingidentity.clientservices.product.integrationkit.entrust.IdentityGu
ardAdapter">true</con:item>
    </con:map>
</con:config>
```

Save the changes and close the file when done.

5. Start PingFederate.

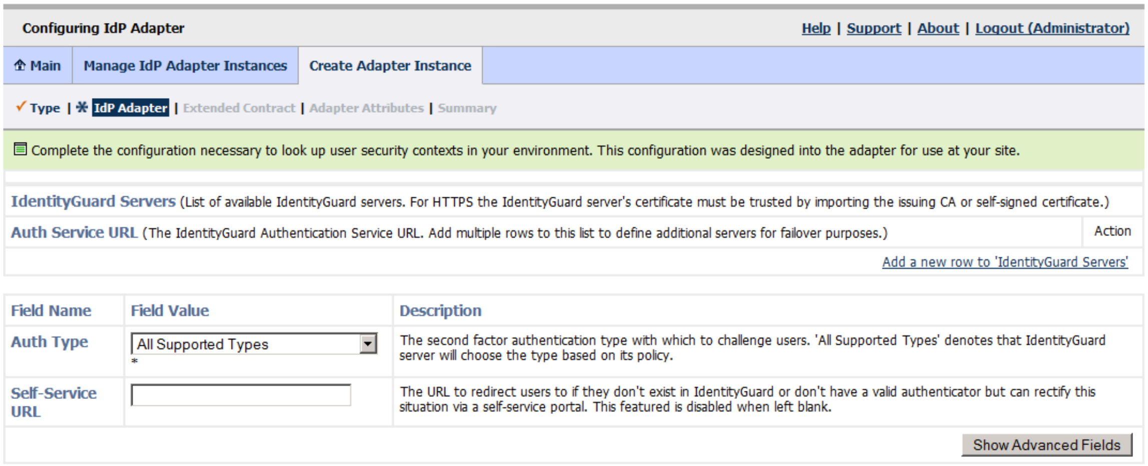
Step 2—Configure PingFederate

Configuring PingFederate to use the Entrust IdentityGuard Integration Kit involves:

- Creating an Entrust IdentityGuard Adapter Instance.
- If one does not already exist, create an instance of an adapter that will perform first factor authentication (e.g.: IWA Adapter).
- Chaining the first factor authentication adapter and Entrust IdentityGuard Adapter instances for two-factor adapter mapping in an SP connection.

To configure the Entrust IdentityGuard Adapter:

1. Log on to the PingFederate administrative console and click **Adapters** under My IdP Configuration on the Main Menu.
   (For more information about IdP Adapters, see the PingFederate *Administrator's Manual*.)
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. On the Type screen, enter an Instance Name and Instance ID.
   The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.
4. Select Entrust IdentityGuard Adapter 1.2.2 from the Type drop-down list and click **Next**.



Configuring IdP Adapter

Help | Support | About | Logout (Administrator)
Main
Manage IdP Adapter Instances
Create Adapter Instance
✓ Type | ✱ IdP Adapter | Extended Contract | Adapter Attributes | Summary

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.

IdentityGuard Servers (List of available IdentityGuard servers. For HTTPS the IdentityGuard server's certificate must be trusted by importing the issuing CA or self-signed certificate.)

Auth Service URL (The IdentityGuard Authentication Service URL. Add multiple rows to this list to define additional servers for failover purposes.)	Action

Field Name	Field Value	Description
Auth Type	All Supported Types *	The second factor authentication type with which to challenge users. 'All Supported Types' denotes that IdentityGuard server will choose the type based on its policy.
Self-Service URL		The URL to redirect users to if they don't exist in IdentityGuard or don't have a valid authenticator but can rectify this situation via a self-service portal. This featured is disabled when left blank.

5. On the IdP Adapter screen, provide entries for each of the fields shown.

Field Name	Instruction
IdentityGuard Servers Auth Service URL	Enter the URL to the V6 Authentication Service of your Entrust IdentityGuard server. Add multiple entries for failover purposes. It is strongly recommended to test the URL first by accessing it via a Web browser. If successful, Entrust IdentityGuard should respond with a page stating **Entrust IdentityGuard Authentication Service**.
Auth Type	Select the authentication type you would like to enforce. If "All Supported Types" is selected then the challenge that users receive depends on what they have available and what is defined by Entrust IdentityGuard policy.
Self-Service URL	Enter the URL to your self-service portal (such as Entrust IdentityGuard Self-Service Module). Users will be redirected to this URL should self-recovery of the error condition be possible. Leaving this field blank disables this feature.

6. (Optional) Click **Show Advanced Fields**.
   Change the advanced settings for additional miscellaneous options including phased user deployment, machine authentication and fail over settings.
7. On the Adapter Attributes screen, select subject as the Pseudonym. Pseudonyms are opaque subject identifiers used for SAML account linking, which may not be applicable for many SP connections. To ensure correct PingFederate performance under all circumstances, however, a selection is required. (For information about account linking, refer to the "Key Concepts" chapter in the PingFederate *Administrator's Manual*, or click **Help** on this screen.)

Tip: The adapter defines additional attributes in its contract that can be used during Assertion creation:

- authtype – The second-factor authentication type used by the end user. Possible values are: GRID, OTP, TOKENRO, TOKENCR and QA.
- group – The user's assigned group as defined in Entrust IdentityGuard.

8. On the Summary screen, verify that the information is correct and click **Done**.
9. On the Manage IdP Adapter Instances screen, click **Save**.

To configure a first factor authenticating Adapter Instance:

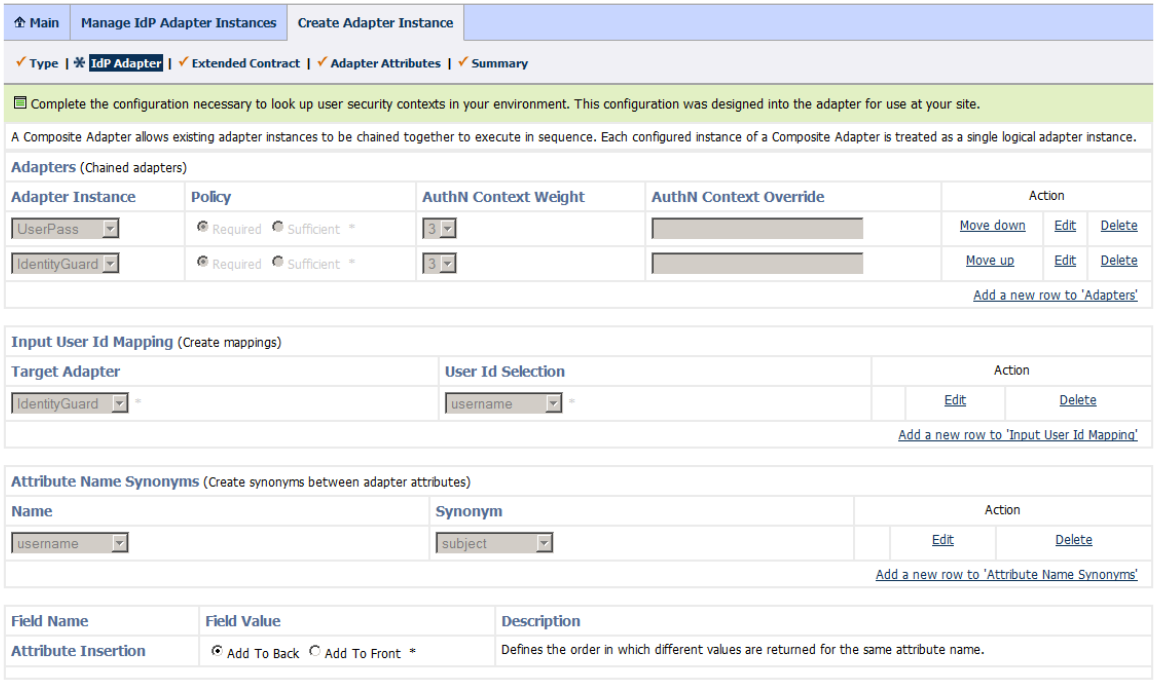
- For the IWA Adapter, follow the instructions in the *User Guide* for the IWA Integration Kit, available separately from Ping Identity.
- For others, consult the relevant documentation, such as the PingFederate *Administrator's Manual*.

To configure an SP connection in PingFederate for two-factor authentication (for PingFederate 6.4 – 6.5):

1. For any new or existing connection, on the IdP Adapter Mapping screen in the Assertion Creation task flow, click **Map New Adapter Instance**. Assertion Creation is located under the Browser SSO tab in the top-level connection task flow.
2. On the Authentication Type screen, select Two-Factor Authentication.
3. On the Adapter Instance screen, select either the Adapter Instance previously configured.
4. On the First Factor ID screen, select the attribute that corresponds to a unique identifier for the user.
5. On the Secondary Adapter Instance screen, select the previously configured Entrust IdentityGuard Adapter Instance.
6. (Optional) On the Adapter Mapping screen, if you are using a data store to retrieve additional user attributes, then select that option.
7. On the Attribute Contract Fulfillment screen, map all attributes for the Attribute Contract. For more information about adapter mapping, refer to the context-sensitive **Help**.
8. On the Summary screen, click **Done**.
9. For a new connection, continue the Browser SSO configuration; for an existing connection, click **Save** when you reach the Browser SSO screen.

To configure an SP connection in PingFederate for two-factor authentication (for PingFederate 6.9 and up):

1. Follow the instructions in the *PingFederate Administrator's Manual* to create an instance of the Composite Adapter.
2. Chain the Entrust IdentityGuard Adapter instance with the first factor adapter instance. A sample working configuration screen follows:


Main
Manage IdP Adapter Instances
Create Adapter Instance
✓ Type | ✱ IdP Adapter | ✓ Extended Contract | ✓ Adapter Attributes | ✓ Summary

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.

A Composite Adapter allows existing adapter instances to be chained together to execute in sequence. Each configured instance of a Composite Adapter is treated as a single logical adapter instance.

Adapters (Chained adapters)

Adapter Instance	Policy	AuthN Context Weight	AuthN Context Override	Action		
UserPass	● Required ○ Sufficient *	3		Move down	Edit	Delete
IdentityGuard	● Required ○ Sufficient *	3		Move up	Edit	Delete

Add a new row to 'Adapters'

Input User Id Mapping (Create mappings)

Target Adapter	User Id Selection	Action		
IdentityGuard *	username *		Edit	Delete

Add a new row to 'Input User Id Mapping'

Attribute Name Synonyms (Create synonyms between adapter attributes)

Name	Synonym	Action		
username	subject		Edit	Delete

Add a new row to 'Attribute Name Synonyms'

Field Name	Field Value	Description
Attribute Insertion	● Add To Back ○ Add To Front *	Defines the order in which different values are returned for the same attribute name.

Note: Since the Entrust IdentityGuard Adapter is a V2 adapter type the Input User Id Mapping must be completed to map the first factor authenticating adapter instance's username into it.

3. Assign this Composite Adapter instance to your SP Connection in the IdP Adapter Mapping screen of the Assertion Creation task flow. Map resulting attributes from the adapter instance into the Adapter Contract.

Customizing the Entrust IdentityGuard Logon Page

End users enter challenge responses for multi-factor authentication on a Web page presented by the PingFederate Entrust IdentityGuard Adapter. You can revise this page for branding or other purposes. The files that make up the page are located in the installed WAR directory:

```
    <PF-install>/pingfederate/server/default/deploy/ig-
adapter-security-code-challenge.war
```