PingFederate Installation and Configuration Document

Table of Contents

1. Cisco's Ping Identity SSO Integration Overview

The Ping Identity SSO integration process on the ASP comprises of 2 components - Ping Federate Server and Plugin-Adapter on the web server.

1.1. PingFederate Server

Installing and configuring the PingFederate server (SP) – Communicates with Cisco IdP (for SAML Assertion exchange) and the ASP Web Server (for setting up HTTP Headers and opentoken cookie) through Browser.

Ping Federate runs on the jboss application server, which is contained in the installation package. The port numbers 9999 and 9031 will be set as default once the PingFederate server is installed and started.

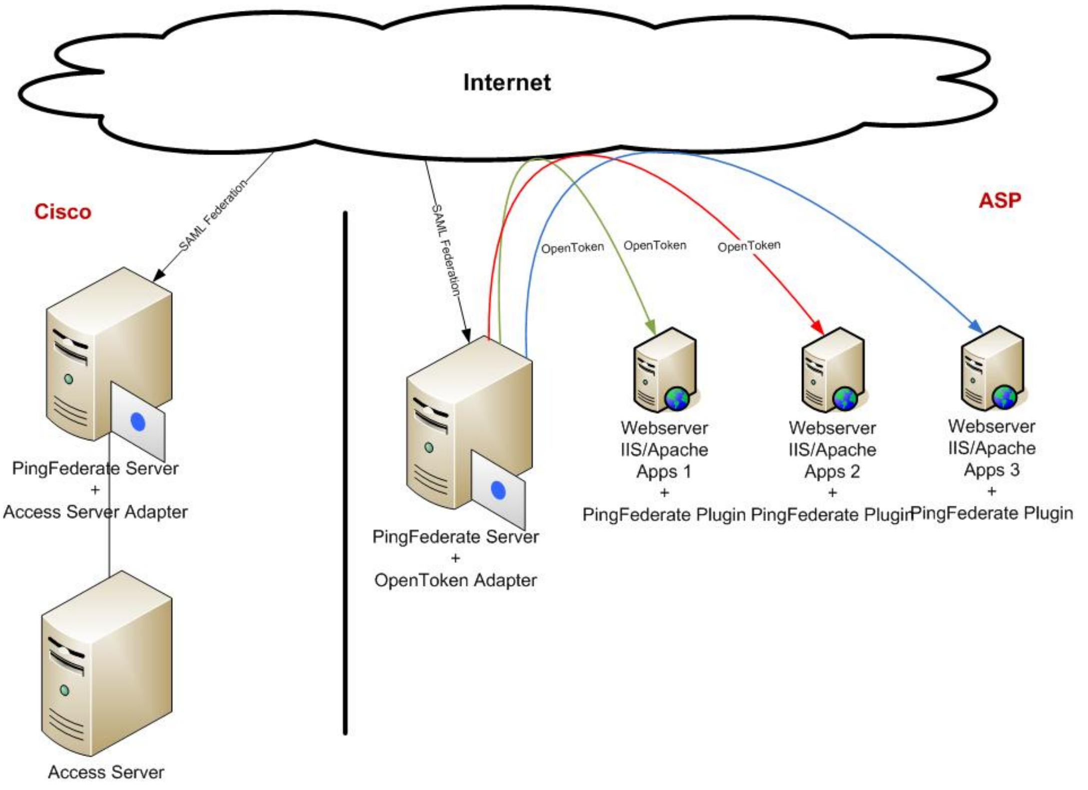
9999 - Ping Federate Admin Console port (Configuration and Administration)

9031 - Ping Federate SSL Server Port, SSL enabled. (The Cisco PingFederate Server communicates to this port for SAML federation through browser)

1.2. Plugin-Adapter

Installing and configuring the Plug-in Adapter – Works in conjunction with the PingFederate OpenToken Adapter to allow an ASP enterprise to accept SAML assertions and provide SSO to IIS/Apache Web applications.

2. The ASP architecture Diagram



3. Set up PingFederate Server

Please follow the following guidelines to install and configure the PingFederate server.

3.1. Pre-requisites

- PingFederate server can run on any of the following OS.
    - Microsoft Windows Server 2003 with Service Pack 2 on x86 (32- and 64-bit)
    - Microsoft Windows Server 2008 on x86 (64-bit)
    - Windows XP Professional with Service Pack 2 (32-bit)
    - Red Hat Enterprise Linux 4 and 5 (32-bit)
    - Red Hat Enterprise Linux ES 4.2 with 2.6.9-22.0 Kernel on x86 (32- and 64-bit)
    - SUSE Linux Enterprise 9 (64-bit)
    - Solaris 10 (64-bit)

- JDK 1.7 should be installed. (There should not be any spaces in the installation path)
  For example, C:\j2sdk1.7

- SSL enabled domain for PingFederate server is required.
  The default SSL port for PingFederate Server is 9031. This port should be opened from outside.
  For example, https://aspdomain.com:9031

- The time on the PingFederate server should be synchronized with any public NTP server.
  Cisco Time is synchronized with NIST time "http://nist.time.gov/timezone.cgi?Pacific/d/-8/java "

- Cisco Security Services team recommends using trusted certificate for Pingfederate server. End user would get warning message in browser if certificate is not from trusted CA.

3.2. Installation

- Ensure you are logged into your system with appropriate privileges to install and run an application.

- Download the JDK at: http://www.oracle.com/technetwork/java/javase/downloads/jdk7-downloads-1880260.html

- Install the JDK to a location with NO SPACES in the path (for example, C:\j2sdk1.7).

- Set the JAVA_HOME environment variable to the JDK installation directory path and add the /bin directory to the PATH variable for your platform.

    - **Note**: If you are running PingFederate as a service, you must set JAVA_HOME at the system level.

- Create an installation directory.

    - **Note**: The installation path and the directory name should NOT contain any spaces.

- Extract the Cisco's Ping Federate distribution ZIP file into the installation directory.

- Get the License key file and save it in the directory:
  <pf_install>/pingfederate/server/default/conf
  - **Note**: Ensure the file name is renamed to pingfederate.lic
- If you have SSL configured in the Load balancer and want to disable the SSL in PingFederate Server, modify the following fields in the file <pf_install>/pingfederate/bin/run.properties

```
pf.http.port=9031
pf.https.port=-1
```

4. Configure PingFederate Server

4.1. Start the PingFederate Server

Start the PingFederate server by running the following script:

```
(Windows) <pf_install>/pingfederate/bin/run.bat
(Linux) <pf_install>/pingfederate/bin/run.sh
```

Wait for the script to finish the startup—the last message displayed in the sequence is:

```
Started in XXs:XXms
Loading config file
EvaluateExpressions silent
```

Note: To install the PingFederate as a Service, refer PingFederate's Getting-Started.pdf document (page 19) which is under <pf_install>/pingfederate/docs/ directory.

4.2. Login to AdministrativeConsole

Launch your browser and go to

- URL: https://<asphostname.aspdomain.com>:9999/pingfederate/app
- Username: Administrator
- Password: Cisco2asp

The PingFederate is configured and packaged with the following default values. But, please make sure to change the values that are in red as per your environment.

Note: After changing the values in each screen, make sure to click "Done" and "Save" the settings.

4.3. Configure Server Settings

(Main Menu > My Server > System Settings > Server Settings)

- **System Info:** (Cisco will use these contact information for any communication)

Company	Cisco ASP Company <ASP Company Name>
Contact Name	Cisco ASP Contact Name <ASP Contact Name>
Contact Number	<Please provide ASP contact number>
Contact Email	aspcontact@aspdomain.com <ASP Email address>

- **Account Management:** (Admin console login password)

Change the password	Cisco2asp <PingFederate Admin console Password>

- **Federation Info:**

Base URL	https://aspdomain.com:9031 <ASP PingFederate Base Url. 9031 is the default SSL port for PingFederate server and this base URL should be accessible from internet>
SAML v2.0 Entity ID	aspdomain.com

4.4. Configure Adapters Setting

(Main Menu > My SP Configuration > Application Integration Settings > Adapters)

Click **CiscoOpenTokenAdapter** adapter instance

- **SP Adapter Instance:**
  < Click "Show Advanced Fields" >

Password <Don't share this password to Cisco. This password is used to encrypt the asp opentoken cookie>	Cisco2asp
Cookie Domain	.aspdomain.com
Token Lifetime <Idle Timeout for asp's opentoken cookie>	3600 (1hr)
Session Lifetime (Max Timeout) <Max Timeout for asp's opentoken cookie>	43200 (12hrs)

- **Extended Adapter Contract:**

Extend the Contract <By default, Cisco would pass only uid (user id) attribute. But if you require more attributes, add the list of attributes that Cisco agreed to send (e.g., email, company, etc)>	uid

- **Adapter Actions**

Click the “download” link and then click “Export” to download the **agent-config.txt** properties file. You will require this file later when you setup the PingFederate Apache / IIS plug-in.

4.5. Configure Default URLs

(Main Menu > My SP Configuration > Application Integration Settings > Default URLs)

Add the ASP's default URL you would like to send the user to when Single Sign On (SSO) has succeeded.

4.6. Configure IDP Connections Setting

(Main Menu > My SP Configuration > IdP Connections)
Click "**Cisco**" Connection

- **General Info**

(Main > IdP connection -> general Info)

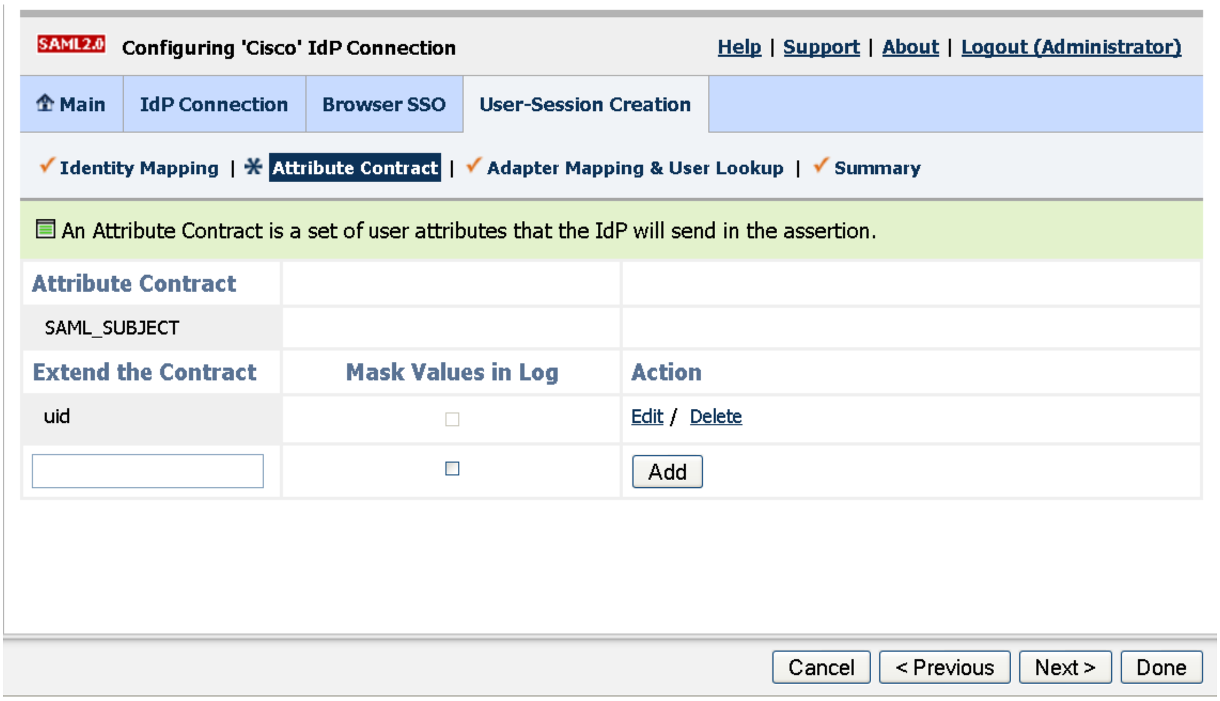
Partner's Entity ID (Connection ID)	cloudsso-test.cisco.com (for Non-Production) < **https://fedtst.cisco.com** should be used for any Non-prod environment like POC, Test, Dev or Stage> cloudsso.cisco.com (for Production) <**https://fed.cisco.com** should be used only for production environment >
Connection Name <Don't Change this field>	Cisco
Virtual Server ID	aspdomain.com (Optional) <The VirtualServer ID is used to uniquely identify the ASP. It's not necessarily to be a valid url or domain. We used domain name here just to identify the ASP easily. However you can give any valid name here.>
Base URL	https://cloudsso-test.cisco.com (for Non-Production) < **https://fedtst.cisco.com** should be used for any Non-prod environment like POC, Test, Dev or Stage> https://cloudsso.cisco.com (for Production) <**https://fed.cisco.com** should be used only for production environment >

- **User-Session Creation**

(Main > IdP connection -> User-Session Creation)
Click "**Configure User-Session Creation**"

➢ Attribute Contract

<By default, Cisco would pass only uid (user id) attribute. But if you require more attributes, add the list of attributes that Cisco agreed to send (e.g., email, company, etc)>


SAML2.0
Configuring 'Cisco' IdP Connection
Help | Support | About | Logout (Administrator)
Main
IdP Connection
Browser SSO
User-Session Creation
✓ Identity Mapping | ✱ Attribute Contract | ✓ Adapter Mapping & User Lookup | ✓ Summary
Cancel
< Previous
Next >
Done

An Attribute Contract is a set of user attributes that the IdP will send in the assertion.

Attribute Contract		
SAML_SUBJECT		
Extend the Contract	**Mask Values in Log**	**Action**
uid	□	Edit / Delete
	□	Add

➢ Adapter Mapping & User Lookup
Click "**CiscoOpenTokenAdapter**"

▪ Adapter Contract Fulfillment
<Map the adapter contract with Assertion Value>

Subject	Assertion	SAML_SUBJECT
Uid	Assertion	uid

- **Credentials**

(Main > IdP connection -> Credentials)
Click “**Configure Credentials**” -> **Basic SOAP Authentication (Outbound)** -> Click “**Configure**”

➢ **Back-Channel Authentication -> Basic SOAP Authentication (Outbound)**

Note: When setting up the password, make sure it fulfills the following password restrictions and then send this credential to Cisco IT Team to have a successful SSO backchannel authentication)

- It has 9 to 12 characters long
- It contains only alphanumeric characters
- It shouldn’t contain any special characters

Username	aspdomain

Password	Cisco2asp

- **Activation & Summary**

(Main > IdP connection -> Activation & Summary)
Make sure the Connection Status is set to Active and then Saved.

Connection Status	Active

Make note of the SSO Application Endpoint URL. You will need it later when configuring the IIS/Apache plug-in.

4.7. Configure SSL Server Certificates

(Main > My Server > Security > SSL Server Certificates)

Note: If you have SSL configured in the Load balancer, please skip this step.

If you already have a VeriSign (or any Certificate Authority) signed Certificate for this server and want to use it for Ping, then you need to convert the certificate key first to PKCS12 format and then import it in the SSL Server Certificates screen and activate it.

Otherwise you can create a new Certificate by clicking “Create New” button.

Click “Certificate Signing” to generate the CSR or to import CSR response.

4.8. Log Level

Pingfederate server has **DEBUG as default log level**. Log level of Pingfederate server can be set as INFO or DEBUG. For each log level separate configuration file is present under <Pingfederate Installation Directory>/server/default/conf folder.

INFO – log4j-INFO.xml
DEBUG – log4j-DEBUG.xml

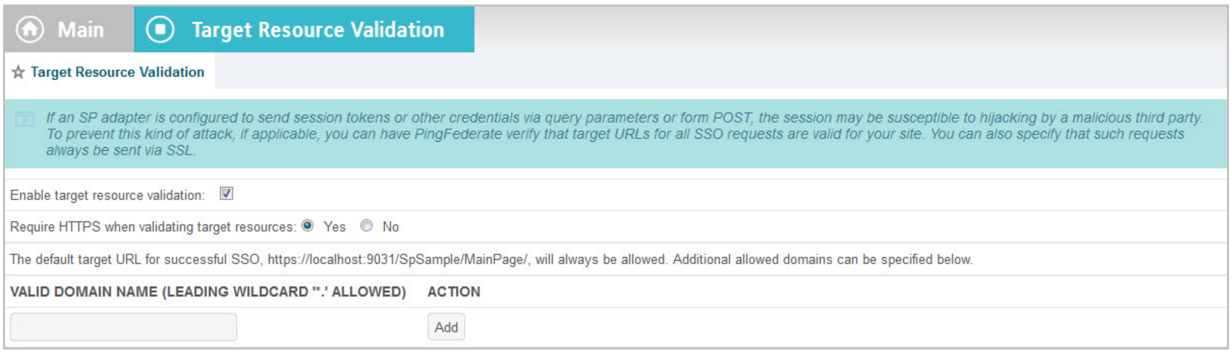
To set appropriate log level, rename corresponding file to **log4j.xml**
Restart Pingfederate Server

4.9. Target Resource Validation

Several SP adapters can be configured to pass security tokens or other user credentials from PingFederate to the target resource via HTTP query parameters or POST transmittal. In both cases, these transport methods open the possibility that a third party (with specific knowledge of aspects of the IdP and/or SP network, as well as PingFederate endpoints and configuration) might be able to obtain and use valid security tokens to gain improper access to the target resource.

This potential security vulnerability would involve using well-formed SSO links to start an SSO request for a resource at the SP site. However, the target resource designated in the link would be intended to intercept the security token by redirection to a malicious Web site.

To prevent such an attack, PingFederate provides a means of validating SSO transactions to ensure that the designated target resource exists in a domain controlled by the SP.



If an SP adapter is configured to send session tokens or other credentials via query parameters or form POST, the session may be susceptible to hijacking by a malicious third party. To prevent this kind of attack, if applicable, you can have PingFederate verify that target URLs for all SSO requests are valid for your site. You can also specify that such requests always be sent via SSL.

Enable target resource validation: ☑

Require HTTPS when validating target resources: ● Yes ○ No

The default target URL for successful SSO, https://localhost:9031/SpSample/MainPage/, will always be allowed. Additional allowed domains can be specified below.

VALID DOMAIN NAME (LEADING WILDCARD '*.' ALLOWED)	ACTION
	Add

1. To reach this screen:

   Click Target Resource Validation on the Main Menu.

2. To enable target resource validation:

   Select the first checkbox.

   Indicate whether to require HTTPS for query and POST transmittals.

3. Enter the domain or IP address containing a target resource and click Add.

   Use the domain only, without qualifiers. For example:

   mycompany.com

   Using an initial wildcard and period for a domain name will cover multiple subdomains. For example:

   *.mycompany.com

   covers hr.mycompany.com or email.mycompany.com.

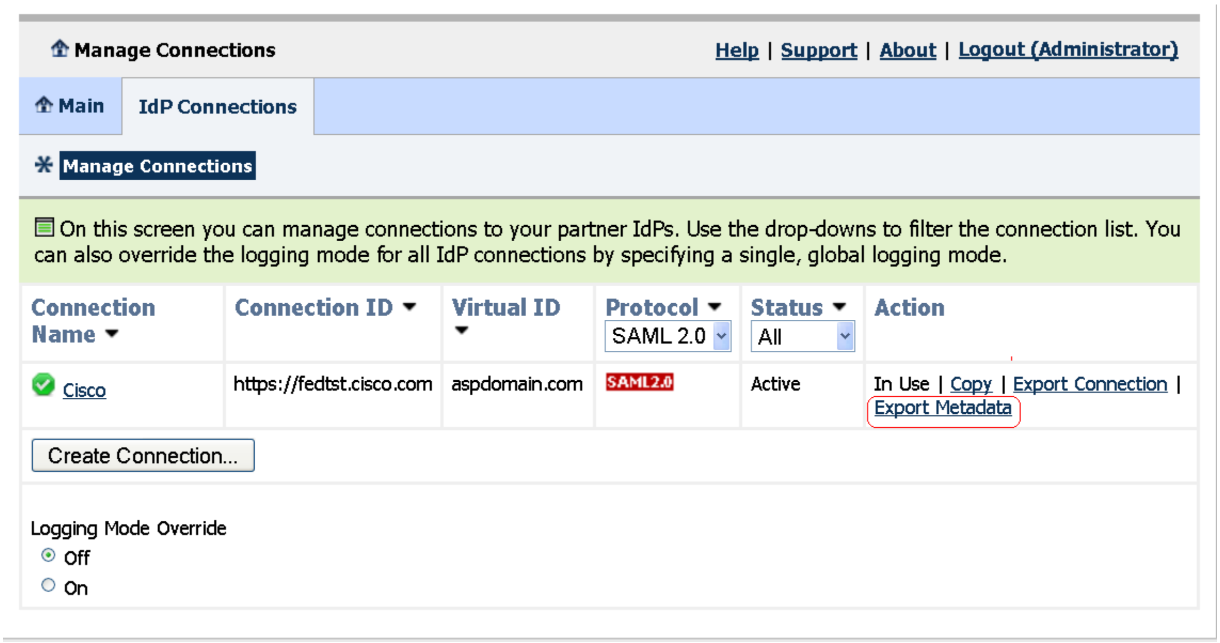
4. Repeat the previous step as needed.

5. Finish Integration Setup with Cisco IT Team

Once you have completed the PingFederate Server setup, please export and send the following items back to Cisco IT team.

5.1. Export metadata.xml File

(Main Menu > My SP Configuration > IdP Connections > Manage all IdP)



On this screen you can manage connections to your partner IdPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all IdP connections by specifying a single, global logging mode.

Connection Name	Connection ID	Virtual ID	Protocol SAML 2.0	Status All	Action
Cisco	https://fedtst.cisco.com	aspdomain.com	SAML2.0	Active	In Use | Copy | Export Connection | Export Metadata

Logging Mode Override

◉ Off

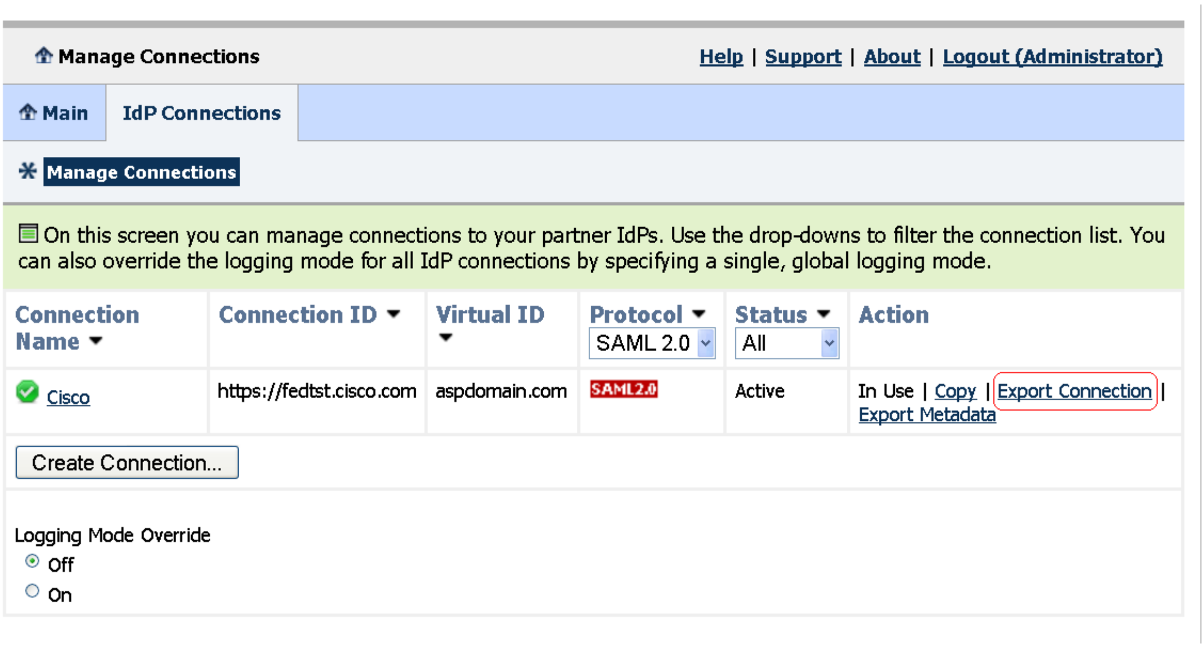
○ On

1. Click on “Export Metadata” button
2. In “Metadata Signing” section do not select anything. Click “Next” button
3. Click “Export” button and save the file “metadata.xml”

5.2. Export idp-pingfederate-connection.xml File

(Main Menu > My SP Configuration > IdP Connections > Manage all IdP)

Click “Export” and save the file, **idp-pingfederate-connection.xml**



Manage Connections

On this screen you can manage connections to your partner IdPs. Use the drop-downs to filter the connection list. You can also override the logging mode for all IdP connections by specifying a single, global logging mode.

Connection Name	Connection ID	Virtual ID	Protocol SAML 2.0	Status All	Action
✓ Cisco	https://fedtst.cisco.com	aspdomain.com	SAML2.0	Active	In Use | Copy | Export Connection | Export Metadata

Logging Mode Override
● Off
○ On

5.3. Export run.properties File

Locate in the directory of <pf_install>/pingfederate/bin/

5.4. Export agent-config.txt File

Please refer to Section 4.4

5.5. Send Required Files Back to Cisco

Please send the following files you just exported back to Cisco IT Team for setup.

metadata.xml
idp-pingfederate-connection.xml
run.properties
agent-config.txt

Cisco would let you know as soon as they finished the setup based on the files you send to them.

6. REVISION HISTORY

Date	Revision Number	Revision Author	Revision Description
01/22/2008	1.0	Solai Jayaraman	Initial document
02/26/2008	1.1	Solai Jayaraman	Added more comments
04/22/2008	1.2	Solai Jayaraman	Added Base URL and modified adapter conf.
11/20/2009	1.3	Aakash Wasnik	Updated JDK version from 1.5 to 1.6
03/30/2010	1.4	Aakash Wasnik	Added note for use of trusted certificate
08/19/2010	2.0	Aakash Wasnik / Sean Zhang	Added screenshot as per Pingfederate 6.3 UI. Updated supported operating system section.
03/09/2012	2.1	Sean Zhang	Updated to cloudsso (RCDN/MVDC)
12/05/2014	3.0	Sean Zhang	Including Information needed for 7.2 Package. Also mandate the Target Validation as part of the setup.