Continuous Dynamic Single Sign-On with PingFederate

Black Duck Software, Inc.

2025-02-11

Table of Contents

Chapter 1. Single Sign-On for Black Duck Continuous Dynamic

Black Duck uses PingFederate, an enterprise federation server, to provide secure single sign-on (SSO) access for Continuous Dynamic.

1.1. How does Single Sign-On Work?

PingFederate sets up a federation—a trust or public key service—that allows Black Duck to confirm that a login request originated from a legitimate user that is authorized by the customer. When the user logs in to their SSO tool and accesses the Continuous Dynamic Portal, the SSO tool sends a SAML message to Continuous Dynamic requesting to have the user logged in. Continuous Dynamic is able to validate that the message is legitimate by using the trust/public key that SAML has established and, once confirmed, look for the user. If the user exists in Continuous Dynamic, and the public key certification is correct, the user is logged into Continuous Dynamic automatically.

IMPORTANT

Removing users

Whenever you remove a user from your SSO tool, you must also remove that user from Continuous Dynamic and ensure that the associated API key has been deleted. Contact Black Duck Support if you need any assistance with these tasks.

1.2. Setting up SSO using file import

Black Duck Support will send you an export of our SSO configuration details as a `metadata.xml` file. Use the `metadata.xml` file to set up your system via a file import. If there is an issue with this approach, we suggest that you contact PingIdentity to see if they can resolve any importing issues.

We strongly recommend using the `metadata.xml` import method. However, if you cannot resolve any importing issues, you can use the following data to set up the connection manually; Black Duck will send you our certificate and key in PKCS12 format to import into your PingFederate instance to complete the setup.

1.3. Manual Setup

Customer Information

You will need to set up SSO according to the following configuration:

Connection Type	
Connection Role	SP
Browser SSO Profiles	True

Connection Type	
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	False
Outbound Provisioning	False
Connection Options	
Browser SSO	True
Attribute Query	False
General Information	
Partner’s Entity ID	`WH-SP-PROD`
Base URL (US region)	https://sentinel-sso.whitehatsec.com:443
Base URL (EU region)	https://sentinel-sso.whitehatsec.eu:443
Browser SSO	
IdP-initiated SSO	True
IdP-initiated SLO	False
SP-initiated SSO	True
SP-initiated SLO	False
Assertion Lifetime	
Assertion Minutes Before	5
Assertion Minutes After	5
Identity Mapping	
Enable Standard Identifier	True (should have `SAML_SUBJECT` in attributes) or False (need not have `SAML_SUBJECT` in attributes)
Attribute Contract	
Attribute E-mail	Required
Attribute SAML_SUBJECT	(Acceptable but not critical unless **Enable Standard Identifier** has been set to **True**)
IDP Adapter Mapping	All fields are unique to the customer’s setup, not defined by Black Duck
Assertion Consumer Service	
Endpoint URL (US region)	https://sentinel-sso.whitehatsec.com/sp/ACS.saml2 (POST)

Connection Type	
Endpoint URL (EU region)	https://sentinel-sso.whitehatsec.eu/sp/ACS.saml2 (POST)
Allowable SAML Bindings	POST and Redirect (True) — all others false
Signature Policy	
Require digitally signed AuthN requests	True
Always sign the SAML assertion	True
Encryption Policy	
Status	Inactive (if encrypting the assertion is preferred—it already travels over a secure channel—this can be set to **Active**, but Black Duck must be informed.)

Black Duck Information

Black Duck will provide:

- Our SAML Entity ID.
- The Login URL that should receive the assertion.
- The binding type we use (Browser Post).
- For manual setup, our certificate and key in PKCS12 format.

This will enable us to establish the federation and begin accepting SSO requests.

1.4. FAQs: Single Sign-On with PingFederate

1. **Can Continuous Dynamic be configured for SSO authentication?**
   Yes, Continuous Dynamic can support IdP-initiated SAML SSO via Browser POST. In this scenario, a user logs in to their company's access portal (IdP) for authentication and is then redirected to the Black Duck Continuous Dynamic Portal website with an authorization token.
2. **Can Continuous Dynamic be configured to allow for both SSO and Continuous Dynamic native authorization, and then at a future date be changed to restrict it to SSO only?**
   Yes, both native authorization and SAML can co-exist, and you can switch to SAML-only at a future date.
3. **What version of SAML is supported?**
   SAML 2.0 is supported only.
4. **Does the digital signature handle SHA-256?**
   Yes. We currently support a digital signature of SHA-256.
5. **Does Black Duck have a test environment that we can validate against before enabling SSO in**

production?
No, unfortunately Continuous Dynamic does not have a dedicated test environment. We will add your SAML setup information and you will be able to test your SAML setup; your users can still log in using their Continuous Dynamic user name and password. Once everything is working we will switch them over to SAML login only.

6. **We would prefer to have users be required to authenticate against us and then be redirected to Continuous Dynamic. Are users going to be able to bypass our authentication server and go directly to Continuous Dynamic once federation is in place?**
Once SAML is active and the only login method, we do not support users going directly to Continuous Dynamic. We require your users to authenticate against your identity provider and then we redirect the user to Continuous Dynamic with the SAML response.

7. **Does the SAML signing certificate need to be issued to a Public Certificate Authority (CA), or is a certificate signed by our CA acceptable?**
A public certificate authority would be the quickest to deploy, but a self-signed certificate will also work. A self-signed certificate will require coordination with our IT team.

8. **What is the EntityID? That is, what is the unique and meaningful connection identifier for each partnership?**

```
Entity ID: WH-SP-PROD
Audience: WH-SP-PROD
```

9. **What is the Base URL of the application?**
US region: https://source.whitehatsec.com
EU region: https://source.whitehatsec.eu

10. **What should the ACS URL be? That is, the Assertion Consumer URL, the URL where the assertion will be posted once the user has been successfully authenticated?**
Login URL: https://sentinel-sso.whitehatsec.com/sp/ACS.saml2
Binding: POST

11. **Do you support static or dynamic federation?**
Continuous Dynamic supports static federation only.

12. **What is the format of the User ID at the service provider (what attributed)? What is the friendly name (e.g. User ID)?**
Continuous Dynamic users an email address for the user ID.

13. **What nameid format is supported (persistent, unspecified, email, etc.)?**
Continuous Dynamic uses a URI for the `nameid` format.

14. **Does Continuous Dynamic require any additional attributes to identify a user?**
No.

15. **Does Continuous Dynamic forward identity assertions to other entities?**
No.

16. **Does Continuous Dynamic require tiered log-in (e.g. SSO to tier 1 and password required for**

tier 2 or 3)?
No.

17. **What session timeouts does Continuous Dynamic enforce for users?**
Continuous Dynamic enforces a four (4) hour session and a 20-minute inactivity timeout for users.

18. **Does Continuous Dynamic support user provisioning and role updates via SAML?**
Continuous Dynamic does not currently support user provisioning and role updates. Continuous Dynamic does have three role types (admin, SecOps, and viewer) that can be mapped to manually when users are added to the system.

19. **Can Continuous Dynamic restrict user location by ensuring they are coming only from my network?**
No.

20. **What should I do when I remove a user from our SSO?**
Whenever you remove a user from your SSO, you should also:

    - Remove the user from Continuous Dynamic.
    - Notify Black Duck if you need assistance removing a user or a user's API Key.
    - Review your Continuous Dynamic user list quarterly to ensure that anyone who has been removed from the SSO has also been removed from Continuous Dynamic and had their API key deleted.