K2cloud Identity Federation Services

Integration Overview

Date: 19 September 2025

Version: 1.5

Synopsys

This document explains how to integrate customer Identity Providers (IdPs) such as Microsoft Entra ID, Okta, PingFederate, and other SAML-compliant platforms with K2cloud's CyberArk Identity Federation Service to enable Single Sign-On (SSO) and role-based access control. It describes the exchange of metadata, domain, and group information required for setup, and how customer-managed security groups map to Fabric roles via K2cloud's federation service. Step-by-step instructions are provided for each supported IdP, ensuring that user authentication and authorization remain centrally managed by the customer's IdP while K2view enforces secure access to Spaces, Projects, and K2cloud Orchestrator resources.

Table of Contents

Overview

This document explains how to integrate customer Identity Providers (IdPs) with **K2cloud's CyberArk Identity Federation Service**, which supports secure access to K2cloud and Fabric environments.

The guide is intended for identity management administrators and security teams responsible for establishing Single Sign-On (SSO) and role-based access control (RBAC) between enterprise IdPs and K2view services. It outlines:

- **Supported Identity Providers (IdPs):** Microsoft Entra ID, Okta, PingFederate, and other SAML-compliant IdPs.
- **Integration Principles:** How customer-managed security groups in the IdP are mapped to Fabric roles through K2cloud's CyberArk federation layer.
- **Delegated Authentication:** How authentication and authorization are enforced by the customer's IdP while leveraging K2cloud's CyberArk service for group-to-role mapping.
- **Required Artifacts:** Metadata exchange, domain information, and group mappings necessary to establish trust and configure SSO.
- **Step-by-Step Guidance:** Detailed instructions for integrating with each supported IdP, including configuration, metadata handling, and testing.

Documentation References

Please consult the following content for background:

1. SSO Overview: link
2. SAML Fundamentals, Terminology, and Security: link
3. How Fabric Works with SAML: link
4. User IAM Configuration: link
5. Microsoft Entra ID SAML Setup Guide: link
6. Okta SAML Setup Guide: link
7. K2cloud Roles and Identity Mapping: link

K2cloud CyberArk Identity Federation Services

The K2cloud platform integrates customer identity provider (IDP) services using its K2cloud CyberArk identity federation service, a US FedRAMP-certified identity and access management provider.

K2view's Fabric services delegate identity and group mapping to its CyberArk identity federation service. Fabric manages authorization based on the roles and groups defined within a customer's IDP and mapped by the K2cloud CyberArk identity federation service. This ensures users receive appropriate access according to their roles in K2view Fabric services.

Delegated Authentication

K2cloud supports Single Sign-On (SSO) integration, making login easier while ensuring secure access across various K2view Spaces. After integrating with the K2cloud CyberArk identity federation service, all authentication depends on the customer's IDP, including managing security groups within the IDP. Without SSO and identity federation, authentication is handled by the K2cloud Directory integrated with K2cloud's CyberArk service.

Users can access K2view Spaces and Projects only according to their roles and permissions, ensuring that access is strictly controlled and aligned with their responsibilities. This is achieved by mapping IDP security groups to Fabric roles via the K2cloud CyberArk identity federation service.

Mapping Security Groups to Fabric Roles

Security groups managed by the IDP assign users to the privileges associated with the groups it manages. These groups are mapped to Fabric roles by K2cloud's CyberArk to the corresponding Fabric roles.

Figuratively, the mapping of a security group to a Fabric role is performed as follows:

> IDP Security Group > K2cloud CyberArk Service Group > K2view Fabric Role
>
> Where:

1. **IDP Security Group** - Created and managed by customers
2. **K2cloud CyberArk Service Groups** - Created by K2view and used to map IDP Security Groups to a K2view Fabric Role.
3. **Fabric Roles** – Created by the customer and mapped in CyberArk by K2view support personnel.

Please consult the K2cloud CyberArk Service Overview section for a functional overview of K2cloud's identity federation services.

To learn more how to map K2cloud roles for use with Fabric and TDM see the K2cloud Roles and Identity Mapping technical note.

Integrating a Customer IDP with the K2cloud CyberArk Service

To integrate a customer IDP with K2cloud's CyberArk identity federation service, metadata must be exchanged between the IDP administrator and K2cloud service personnel.

Customer Provided Information

IDP Service Provider Metadata File

The simplest way to integrate a customer IDP with the K2cloud CyberArk Service is for the customer to share its SAML metadata XML descriptor document with K2view. K2view will use this artifact to set up a federation configuration for the customer's IDP. A sample of the XML Service Provider metadata file is available in the Sample Federation Metadata Descriptor XML section of this document. The certificate and identifying details have been removed from this sample.

Email Domain

K2view needs the customer's email domain to set up the federation.

Security Group Information

K2view maps the default Fabric roles of the K2view Project and Sites owner role to the corresponding IDP security group. After the initial integration, other roles can be configured. Please refer to the K2cloud Roles and Identity Mapping technical note to learn how to create these roles and mappings.

The group information required includes:

IDP Group Name	Intended Fabric Role
	Cloud Project and Site Owner

Note: For Microsoft Entra ID the group name and its corresponding ID are required.

Attributes Claims Required

K2view does not have specific claim requirements. However, we prefer that the Organization claim be included. This helps K2view better understand the claims it processes, especially those involving organizations with multiple sub-organizations. While not mandatory, this is encouraged. For example,

```
<RequestedAttribute isRequired="false" Name="Organization" FriendlyName="Description" />
```

K2view Provided Information

Once the federation is provisioned, K2view will share its Federation Metadata XML descriptor file – similar to the sample shown in the Sample Federation Metadata Descriptor XML section.

URL Callback

Two callback URLs will be provided, each representing the same endpoint. The first identifies K2cloud's CyberArk service. The second is an alias for the first, allowing the IDP to resolve either. The replyURLs will be:

1. https://aaj4067.my.idaptive.app/my
2. https://authcloud.k2view.com/my

K2cloud CyberArk Service Overview

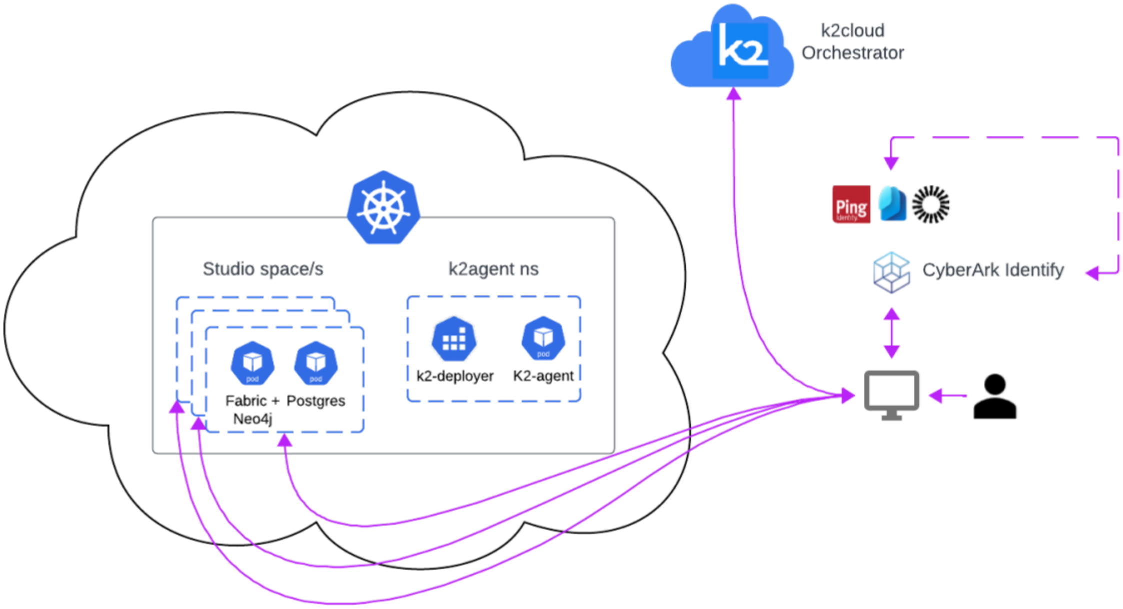
K2view supports Single Sign-On (SSO) integration, making login easier while keeping access secure across different K2view Spaces.

K2cloud Directory Identities

Before Identity Federation is set up, authentication is handled by the K2cloud Directory that co-resides with its CyberArk service.

Identity Federation

Once integrated with the K2cloud CyberArk identity federation service, all authentication is delegated to the customer's IDP, including the management of security groups within the IDP.

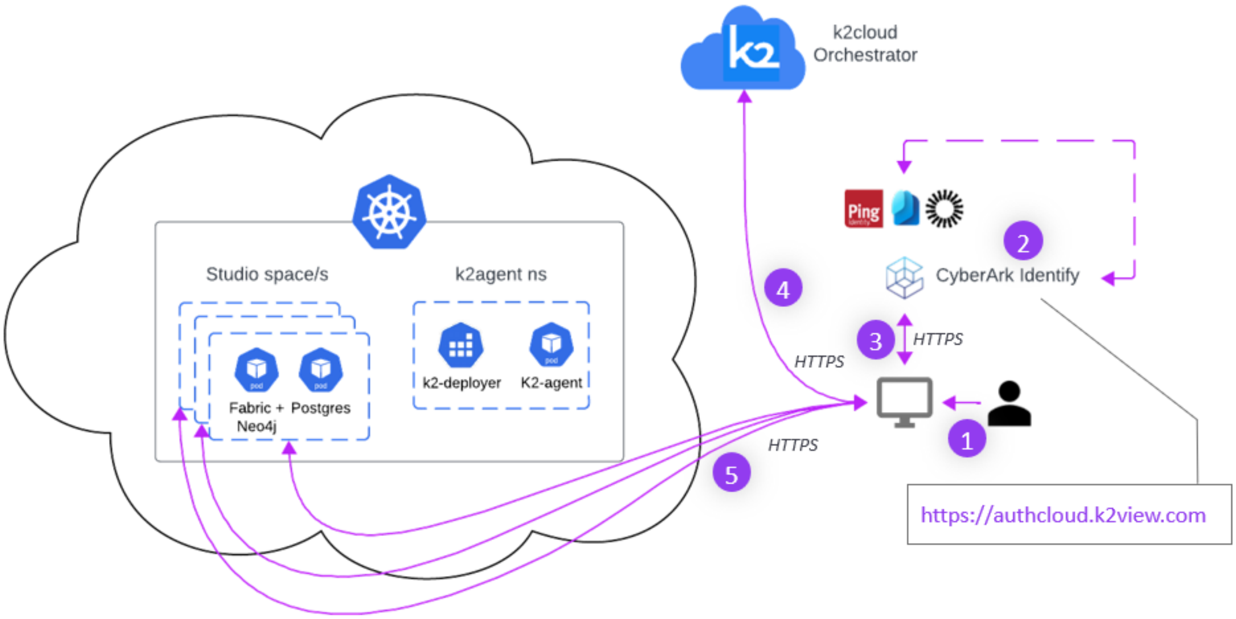


K2cloud's CyberArk identity federation service:

- Enables multi-factor authentication using various authenticators while applying different policies based on profiles.
- Enables SSO Integration (federation using SAML)
- Maps IDP security groups to grant role-based access to K2cloud Orchestrator or Spaces.

Role-based Access Control

The authentication and authorization flow is depicted here.



1. User browses to K2cloud Orchestrator or a space URL
2. The user is redirected to the K2cloud CyberArk Identity Federation service to check their authentication and authorization (https://authcloud.k2view.com)
3. If the user is not logged in, the user is redirected to the login process
4. When a user is authenticated, the user's authorization is checked against the specific URL (the K2cloud Orchestrator or a Space) that the user tries to access.
5. Once verified, the user is redirected back to the app (the Space or K2cloud Orchestrator), where they perform functions based on their roles. Roles and permissions for Spaces are managed through the Space's Web Admin UI.

Sample Federation Metadata Descriptor XML

```
<EntityDescriptor ID="_cc2cdc47-d8c9-427e-9741-c3cfec150c6d" entityID="CN=Idaptive:Customer:AAJ4067"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
    <SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <Organization>
            <OrganizationName xml:lang="en-US">Idaptive</OrganizationName>
            <OrganizationDisplayName xml:lang="en-US">Idaptive</OrganizationDisplayName>
            <OrganizationURL xml:lang="en-US">urn:idaptive</OrganizationURL>
        </Organization>
        <KeyDescriptor use="signing">
            <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
                <X509Data> … </X509Data>
            </KeyInfo>
        </KeyDescriptor>
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://aaj4067.my.idaptive.app/Security/Logout"
ResponseLocation="https://aaj4067.my.idaptive.app/my" />
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:WindowsDomainQualifiedName</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:entity</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
        <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://aaj4067.my.idaptive.app/my" index="0"
ResponseLocation="https://aaj4067.my.idaptive.app/my" isDefault="true" />
        <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://aaj4067.my.idaptive.app/my" index="1"
ResponseLocation="https://aaj4067.my.idaptive.app/my" />
        <AttributeConsumingService index="0">
            <ServiceName xml:lang="en-US">CyberArk CyberArk Identity Service</ServiceName>
            <RequestedAttribute isRequired="false" Name="Description" FriendlyName="Description" />
            <RequestedAttribute isRequired="false" Name="DisplayName" FriendlyName="DisplayName" />
            <RequestedAttribute isRequired="false" Name="EmailAddress" FriendlyName="EmailAddress" />
            <RequestedAttribute isRequired="false" Name="Group" FriendlyName="Group" />
            <RequestedAttribute isRequired="false" Name="HomeNumber" FriendlyName="HomeNumber" />
            <RequestedAttribute isRequired="false" Name="LoginName" FriendlyName="LoginName" />
            <RequestedAttribute isRequired="false" Name="MobileNumber" FriendlyName="MobileNumber" />
            <RequestedAttribute isRequired="false" Name="Name" FriendlyName="Name" />
            <RequestedAttribute isRequired="false" Name="OfficeNumber" FriendlyName="OfficeNumber" />
            <RequestedAttribute isRequired="false" Name="Photo" FriendlyName="Photo">
                <!--Warning: Photos should only be sent when using the
urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST binding because of URL length restrictions.-->
            </RequestedAttribute>
            <RequestedAttribute isRequired="true" Name="UserPrincipalName"
FriendlyName="UserPrincipalName" />
        </AttributeConsumingService>
    </SPSSODescriptor>
    <Organization>
        <OrganizationName xml:lang="en-US">Idaptive</OrganizationName>
        <OrganizationDisplayName xml:lang="en-US">Idaptive</OrganizationDisplayName>
        <OrganizationURL xml:lang="en-US">urn:idaptive</OrganizationURL>
    </Organization>
</EntityDescriptor>
```

Integration Steps

Integrating with Microsoft Entra ID

The integration with Microsoft Entra ID is achieved through a configuration that maps Microsoft Entra ID security groups to K2view Fabric Roles via the K2cloud CyberArk service, enabling role-based access control. Microsoft Entra ID acts as the Identity Provider (IdP), with metadata exchanged to establish trust with the CyberArk service. K2cloud's CyberArk service maps Entra ID groups to the corresponding K2view Fabric Roles. The group-to-role mapping flow can be summarized as follows:

Microsoft Entra ID Group → CyberArk Service Group → Fabric Role

Components:

- **Microsoft Entra ID Groups**: Created and managed by the customer to organize users and assign access privileges via Entra ID groups
- **CyberArk Service Groups**: Maps Microsoft Entra ID security groups with the appropriate Fabric Roles.
- **Fabric Roles**: Used for authorization within the K2view platform.

Review the Microsoft Entra ID Setup Guide

To learn how to navigate Microsoft Entra ID's configuration, please review the Microsoft Entra ID SAML Setup Guide.

The Steps

Step 1: Obtain the K2cloud metadata file

In Step 4 below, you must upload the K2cloud metadata file to support the integration of Entra ID with K2cloud. If you have not yet received this file, please request it.

Step 2: Share your Domain with K2view

The domain name you share must match the Microsoft Entra ID domain that you are integrating K2cloud with. For example, if you sign in to Microsoft Entra ID as user@example.com, provide "example.com" to K2view. When users sign in (a Service Provider-initiated flow), the K2cloud CyberArk service will detect the user's domain suffix and direct the user to the Microsoft Entra ID (the IdP) for authentication.

Step 3: Share the list of Entra ID security groups to be mapped to K2cloud roles.

This list will be used by K2cloud's CyberArk service to perform its group-to-role mapping flow:

Microsoft Entra ID Group → CyberArk Service Group → Fabric Role

Obtaining the Entra ID Group

To find the Microsoft Entra ID group object ID, log in to the Microsoft Entra ID portal, navigate to **Groups**, and select the group you want to map. Copy the **Object ID** string of characters and provide it to K2view. You can share a table like this with K2view:

Entra ID Group Name	Entra ID Group ID specified in the generated Claim	Intended Fabric Role
		Cloud Project and Site Owner

Step 4: Configure a new enterprise application in the Microsoft Entra ID portal

1. Open a new browser window and access the Microsoft Entra ID portal. You will need permission to create an enterprise application. See Create Custom Roles to manage enterprise apps in Microsoft Entra ID for more information.
2. Go to **Enterprise Applications** > **New application** > **Create your application**.
3. Enter the application name, select **Integrate any other application you don't find in the gallery (Non-gallery)**, click **Create**, then assign users and/or groups to this application.
4. Go to **Users > Add users and groups** and select the groups that will log in to K2cloud.
5. Go to **Single sign-on** > **SAML** > **Upload metadata file**, select the K2cloud metadata file provided by K2view, and click **Add**.
6. In the **Basic SAML Configuration** window, select a default option to ensure the IdP-initiated logins work in the **Reply URL (Assertion Consumer Service URL)** section and click **Save**.
   If you are prompted to test the SSO, click **No, I'll test later**.
7. Go to **Attributes & Claims** > **Add new claim**, then enter **UserPrincipalName** in the **Name** text field.
8. Select **user.userprincipalname** in the **Source attribute**, then click **Save**.
9. (Optional) Add the following:

   We ask that you optionally add email and organization claims. These are used to help K2view more easily identify users and their organization.

Name	Source attribute
emailAddress	user.mail
MobileNumber	user.mobilephone
organization	organization

10. Click **Add a group claim**, then select the group type for the group you want to map with K2cloud. For example, Security groups.
11. Expand **Advanced options**, then select **Customize the name of the group claim**, type **group** in the name text field, and click **Save**.
12. Go to **SAML Certificates** and copy the **App Federation Metadata URL**.

Step 5: Export Microsoft Entra ID Metadata XML File

This step gives K2view the information needed to complete the SAML trust configuration from its side.

After configuring the Enterprise Application and setting up the SAML single sign-on, you'll need to **export the SAML metadata XML file** from Microsoft Entra ID and share it with K2view.

Here's how to do that:

1. **Open the Microsoft Entra ID portal**
    - Go to https://entra.microsoft.com (or https://portal.azure.com > Entra ID).
    - Log in with an account with admin privileges to manage Enterprise Applications.
2. **Navigate to your configured Enterprise Application**
    - From the left-hand menu, select **Enterprise Applications**.
    - Click on the name of the application you created for K2cloud.
3. **Go to the SAML-based Single Sign-On configuration**
    - In the application blade, select **Single sign-on** from the left pane.
    - Under **Single sign-on mode**, confirm that **SAML** is selected.

4. **Locate the App Federation Metadata URL**
    - Scroll down to the **SAML Certificates** section.
    - Find the **App Federation Metadata URL**.
5. **Download the XML metadata**
    - Click the **App Federation Metadata URL** link. This will open an XML file in the browser.
    - Right-click anywhere in the browser window and choose **Save As**.
    - Save the file as entra-id-metadata.xml (or any other appropriate filename).

Note: This file contains essential information, such as the X.509 certificate and the SSO endpoint URL required for SAML configuration.

Step 6: Finalize Integration with K2view

1. **Share the file with K2view**
    - Send the downloaded XML file to the K2view team securely.
    - K2view uses this file to establish trust with your Entra ID as the Identity Provider (IdP).
2. **K2view Configuration**:
    - K2view will use the Entra ID metadata to configure the K2cloud CyberArk Identity Federation Service.
    - They will map Entra ID groups to K2view roles based on the information provided.

Step 7: Test the Integration

When K2view confirms that the configuration has been completed, you are ready to test.

- Navigate to the K2cloud login page: https://cloud.k2view.com
- Enter your email

Integrating with Okta

This section outlines the steps to integrate your Okta Identity Provider (IdP) with K2cloud's CyberArk Identity Federation Services using SAML. This integration enables Single Sign-On (SSO) and centralized identity management for K2cloud Orchestrator and Spaces.

Prerequisites

- **Okta Administrator Access**: Ensure you have administrative privileges in your Okta organization.
- **K2view Metadata File**: Obtain the SAML metadata file from K2view to configure the integration.

Review the Okta SAML Setup Guide

To learn how to navigate Okta's configuration, please review the Okta SAML Setup Guide.

The Steps

Step 1: Obtain the K2cloud metadata file

In Step 5, you will need information found in K2cloud's metadata file to support the integration of Okta with K2cloud. If you have not yet received this file, please request it.

Step 2: Share your Domain with K2view

The domain name you share must match the domain that you are integrating K2cloud with. For example, if you sign in to Okta as user@example.com, provide "example.com" to K2view. When users sign in (a Service Provider-initiated flow), the K2cloud CyberArk service will detect the user's domain suffix and direct the user to Okta (the IdP) for authentication.

Step 3: Share the list of Okta security groups to be mapped to K2cloud roles.

This list will be used by K2cloud's CyberArk service to perform its group-to-role mapping flow:

Okta Group → CyberArk Service Group → Fabric Role

You can share a table like this with K2view:

Okta Group Name	Intended Fabric Role
	Cloud Project and Site Owner

Step 4: Create a New SAML Application in Okta

1. **Log in to Okta**: Access your Okta Admin Console.
2. **Navigate to Applications**:
   - Go to **Applications** > **Applications**.
   - Click **Create App Integration**.
3. **Select SAML 2.0**:
   - Choose **SAML 2.0** as the Sign-in method.
   - Click **Next**.

Step 5: Configure SAML Settings

1. **General Settings**:
   - **App Name**: Enter K2cloud (or a preferred name).
   - (Optional) Upload a logo and set app visibility preferences.
   - Click **Next**.
2. **SAML Settings**:
   - **Single Sign-On URL**: Copy the Service Provider Authentication Response URL (from the XML metadata file) and paste it in the **Single sign on URL** text field
   - **Audience URI (SP Entity ID)**: Copy the Service Provider Certificate Authority (from the XML metadata file) and paste it in the **Audience URI** text field.
3. **Attribute Statements**:
   We ask that you add email and organization claims. These are used to help K2view more easily identify users and their organization. Here is a proposed list of attribute statements to configure.

Name	Value
UserPrincipalName	user.login
DisplayName	user.displayName
LoginName	user.login
mobileNumber	user.mobilePhone
emailAddress	user.email
organization	organization’s name

4. **Group Attribute Statements**:
   - **Name**: groups
   - **Filter**: Matches regex with .* (to include all groups).
   - This setup ensures Okta group memberships are sent to K2view for role mapping. The Attribute Group value should match the Okta group name to allow access to apps on K2cloud. For example, Okta group 1 is allowed access to a K2cloud Space but not Orchestrator.

Step 6: Configure Okta Group Assignments

Assign Groups:
- In the **Assignments** tab of your Okta application, click **Assign**.
- Choose **Assign to Groups**.
- Select the Okta groups that correspond to K2view roles.
- Click **Assign** and then **Done**.

Step 7: Obtain Okta Metadata

Identity Provider Metadata:

- In the **Sign On** tab of your Okta application, click **View SAML setup instructions**.
- Download the **Identity Provider metadata** file.
- Provide this metadata file to K2view to complete the SAML federation setup.

Step 8: Finalize Integration with K2view

1. **Provide Okta Metadata to K2view**:
   - Send the downloaded Okta metadata file to your K2view support contact.
2. **K2view Configuration**:
   - K2view will use the Okta metadata to configure the K2cloud CyberArk Identity Federation Service.
   - They will map Okta groups to K2view roles based on the information provided.

Step 9: Test the Integration

When K2view confirms that the configuration has been completed, you are ready to test.

1. **Access K2view Applications**:
   - Navigate to the K2cloud login page: https://cloud.k2view.com
   - You should be redirected to Okta for authentication.
2. **Verify Access**:
   - Upon successful authentication, confirm that you have the appropriate access and permissions within K2cloud, as determined by your Okta group memberships.

Integrating with PingFederate

This guide outlines the steps to integrate your PingFederate Identity Provider (IdP) with K2cloud's CyberArk Identity Federation Services using SAML. This integration enables Single Sign-On (SSO) and centralized identity management for K2cloud Orchestrator and Spaces.

Prerequisites

- **PingFederate Administrator Access**: Ensure you have administrative privileges in your PingFederate environment.
- **K2view Metadata URL**: Obtain the Service Provider (SP) Metadata URL from K2view to configure the integration.

Step 1: Obtain the K2cloud metadata file

In Step 2, you will need information found in K2cloud's metadata file to support the integration of PingFederate with K2cloud. If you have not yet received this file, please request it.

Step 2: Share your Domain with K2view

The domain name you share must match the domain that you are integrating K2cloud with. For example, if you sign in to PingFederate as user@example.com, provide "example.com" to K2view. When users sign in (a Service Provider-initiated flow), the K2cloud CyberArk service will detect the user's domain suffix and direct the user to PingFederate (the IdP) for authentication.

Step 3: Share the list of PingFederate security groups to be mapped to K2cloud roles.

This list will be used by K2cloud's CyberArk service to perform its group-to-role mapping flow:

PingFederate Group → CyberArk Service Group → Fabric Role

You can share a table like this with K2view:

PingFederate Group Name	Intended Fabric Role
	Cloud Project and Site Owner

Step 4: Configure a New SP Connection in PingFederate

1. **Access PingFederate Admin Console**:
   - Open the PingFederate Admin Console in a web browser.
2. **Create SP Connection**:
   - Navigate to **Applications** > **SP Connections**, then click **Create Connection**.
   - Choose **Do not use a template for this connection** and click **Next**.
3. **Select SSO Profile**:
   - Select **Browser SSO Profiles**, choose **SAML 2.0**, and click **Next**.
4. **Load Metadata**:

    - Choose **URL** and click **Manage Partner Metadata URLs**.
    - Click **Add New URL**, provide a name, and paste the **Service Provider Metadata URL** from K2view.
    - Uncheck **Validate Metadata Signature**, then click **Load Metadata**.
    - Click **Next**, **Save**, and **Done**.
5. **Configure Connection**:
    - Select the newly added metadata URL, click **Load Metadata**, and proceed with **Next**.
    - Name the connection as desired, then click **Next**.
6. **Configure Browser SSO**:
    - Enable both **IDP-Initiated SSO** and **SP-Initiated SSO**, then click **Next**.
    - Keep the default **Assertion Lifetime** and click **Next**.
7. **Set Attribute Contract**:
    - Choose **Standard** and click **Next**.
    - Ensure the following attributes are included:
        - displayName
        - EmailAddress
        - LoginName
        - UserPrincipalName
        - Organization – this helps K2view better identify users/groups

    - then click **Next**.
8. **Map Authentication Source**:
    - Authentication source mapping can be configured to use an adapter or an authentication policy, see PingIdentity's Managing authentication source mapping for more information
    - Click **Map New Adapter Instance**.
    - Create or select an **Adapter Instance** that aligns with your attribute contract, then click **Next**.
    - Choose the appropriate mapping method and proceed with **Next**.
    - In **Attribute Contract Fulfillment**, assign the source for each attribute, then click **Next**.
    - Click **Next** and **Done** to finalize.
9. **Configure Protocol Settings**:
    - Deselect **Artifact** and **SOAP**, then click **Next**.
    - Set **Encryption Policy** to **None**, then click **Next** and **Done**.
10. **Configure Credentials**:
    - Select the appropriate **Signing Certificate**.
    - Ensure **Include the Certificate in the Signature <Keyinfo> Element** is checked, then click **Next** and **Done**.
11. **Finalize Connection**:
    - Click **Next**, verify the **SSO Application Endpoint** is enabled, and click **Save**.

Step 5: Export Inbound Metadata from PingFederate

Export Metadata:

- In the SP Connections list, locate your newly created connection.
- Click **Select Action** next to it, choose **Export Metadata**, and select the previously chosen **Signing Certificate**.

- Ensure **Include the Certificate in the Signature <Keyinfo> Element** is checked, then click **Next**.
- Click **Export**, save the metadata.xml file, and click **Done**.

Step 6: Finalize Integration with K2view

3. **Provide PingFederate Metadata to K2view**:
    - Send the downloaded PingFederate metadata file to your K2view support contact.
4. **K2view Configuration**:
    - K2view will use the PingFederate metadata to configure the K2cloud CyberArk Identity Federation Service.
    - They will map PingFederate groups to K2view roles based on the information provided.

Step 7: Test the Integration

When K2view confirms that the configuration has been completed, you are ready to test.

2. **IDP-Initiated SSO:**
    - Access the PingFederate-provided URL for K2cloud.
    - Sign in with your PingFederate credentials.
    - Verify successful authentication and access to K2cloud applications.
3. **SP-Initiated SSO:**
    - Navigate to the K2cloud login page: https://cloud.k2view.com
    - Enter your email