Adobe Creative Cloud

SURFconext cannot verify the configuration steps below as we are not a customer of this service provider. We have collected the information below from our connected institutions to the best of our knowledge. Sometimes procedures change; we depend on someone notifying us. Sorry if the below info does not work for you. If you have remarks or tips you want to share, please send them to support@surfconext.nl.

Since every institution gets their own instance of Adobe Creative Cloud with which a connection needs to be configured, institutions need to sign in with the account that comes with their Adobe license. SURF does not have that information, so institutions need to configure part of the connection. After the institution has taken some steps, SURF also needs to take some steps to finish setting up the connection.

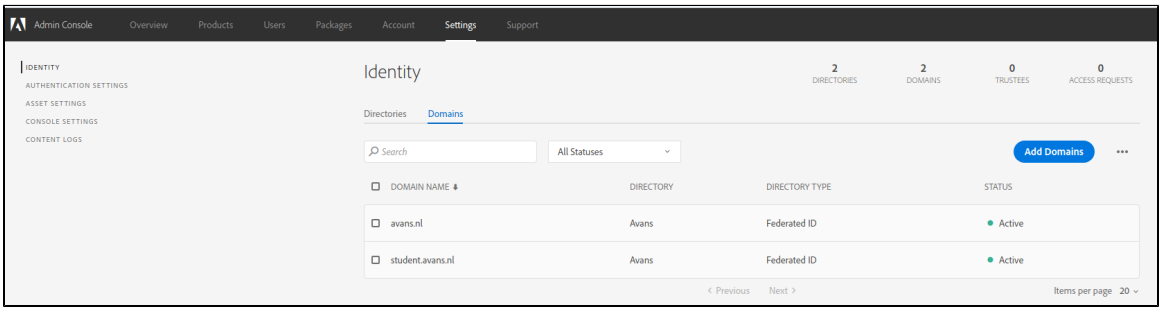
This document describes how to do this and is based on the experience of AVANS. Replace links as shown by what you have configured in your Adobe Application. After following the steps below the users of your IdP should be able to connect to Adobe Creative Cloud.

After reading this page you will know about:

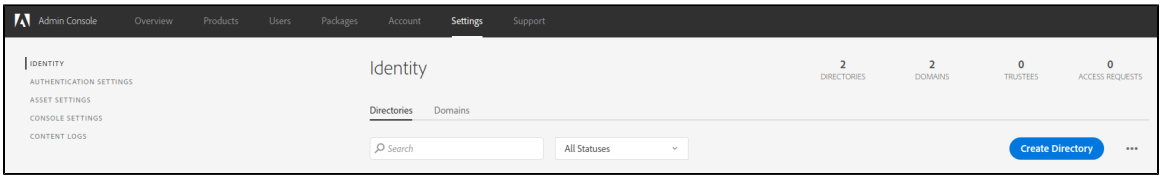
- Configuration of Adobe
- Configuration of SURFconext
- Attribute Manipulation
- How to log on to the service as an and user
- Active sessions
- Set up the User Sync tool management of users

Configuration of Adobe

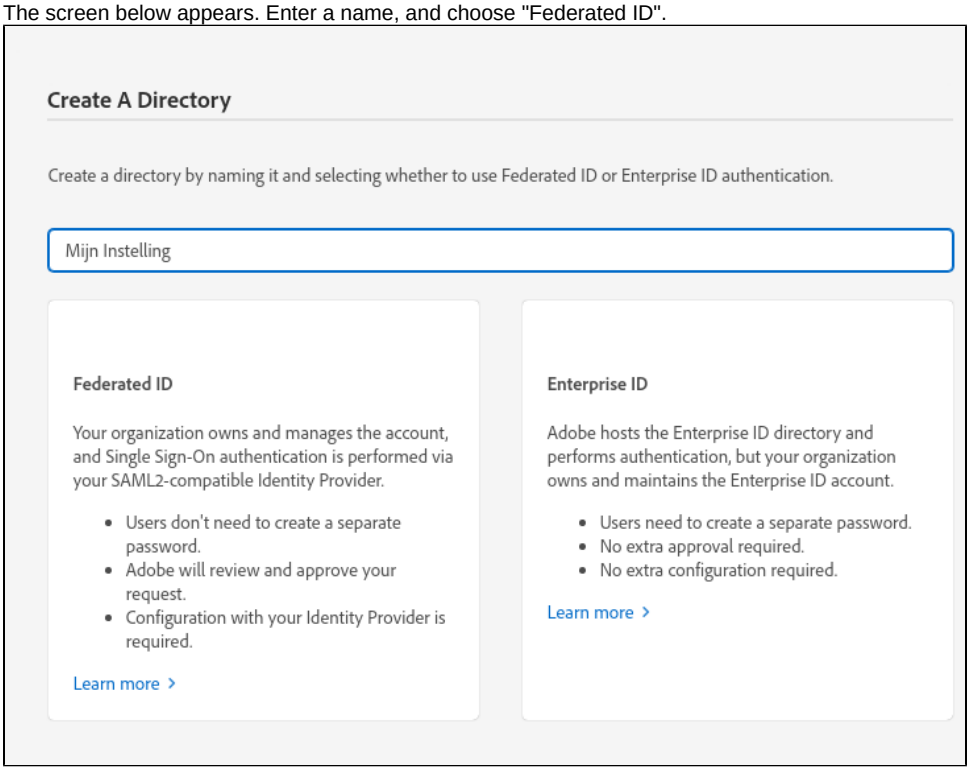
- Navigate to the Adobe Admin console and logon to the service: https://adminconsole.adobe.com/
- Under Settings - Identity - Domains add the domain names your users use in the email address, and confirm these via DNS changes as prompted during entry.



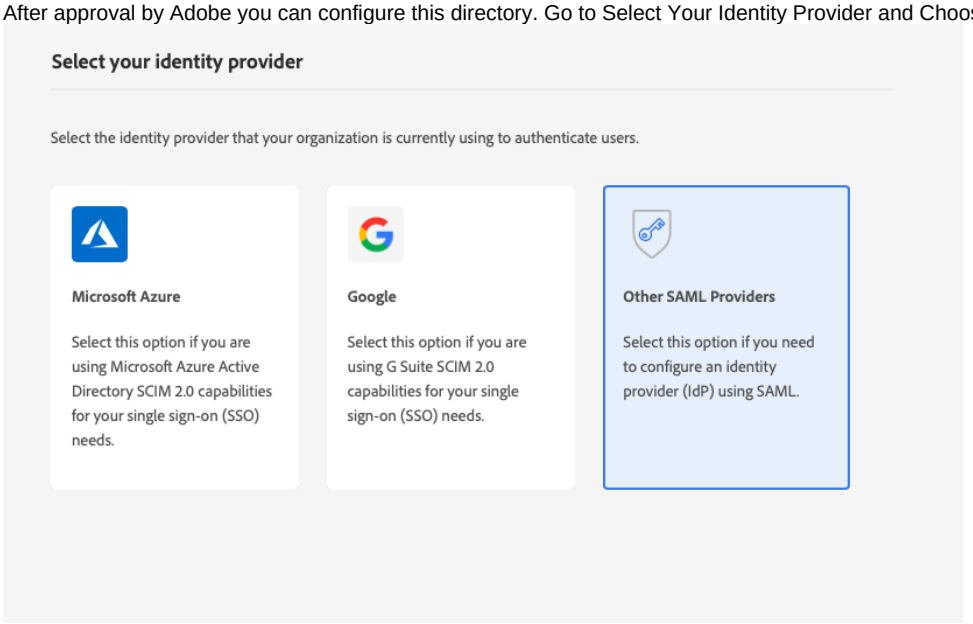
- In Settings - Identity create a new directory by clicking the button "Create Directory".



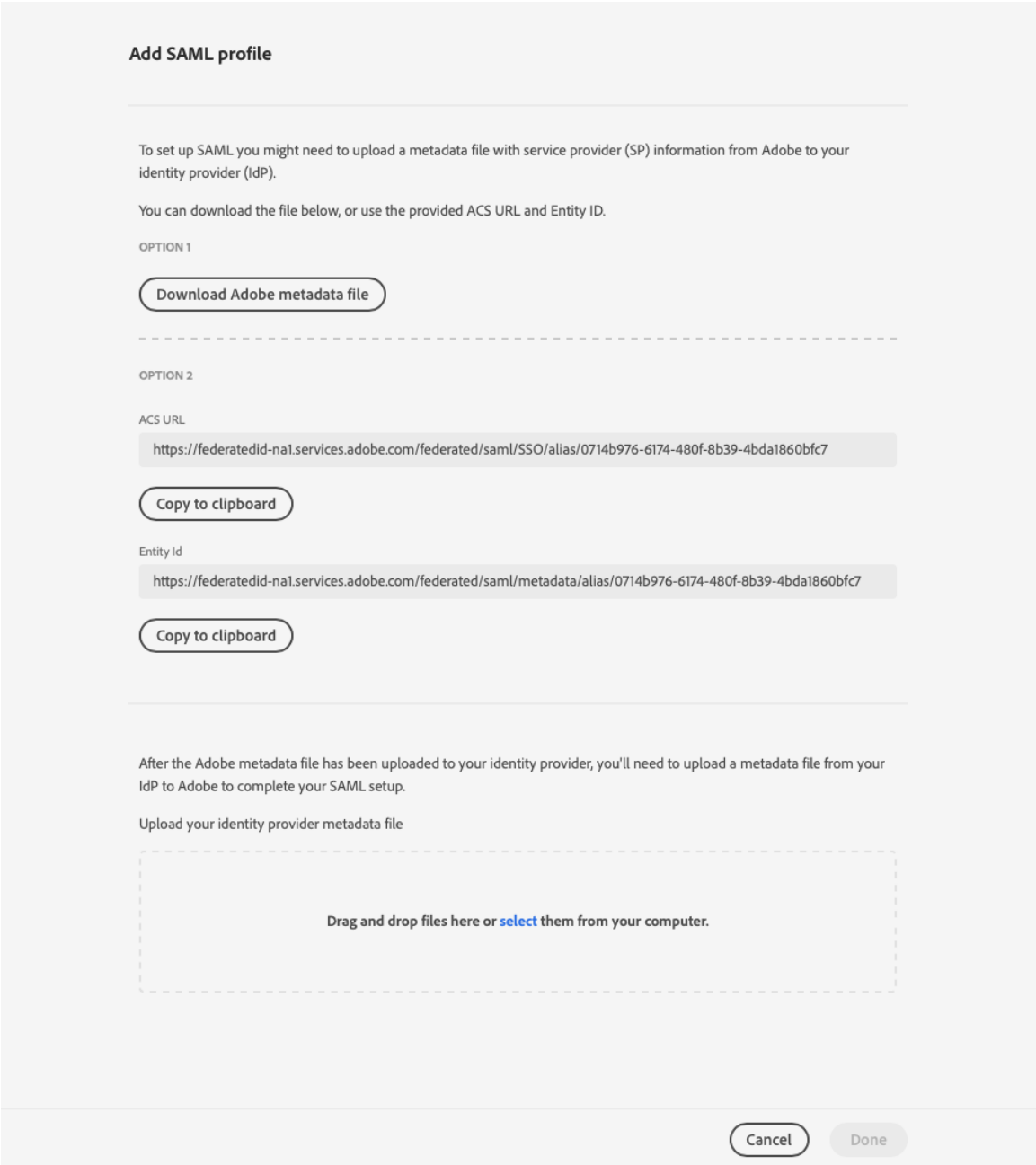
- The screen below appears. Enter a name, and choose "Federated ID".



- After approval by Adobe you can configure this directory. Go to Select Your Identity Provider and Choose 'Other SAML Providers':



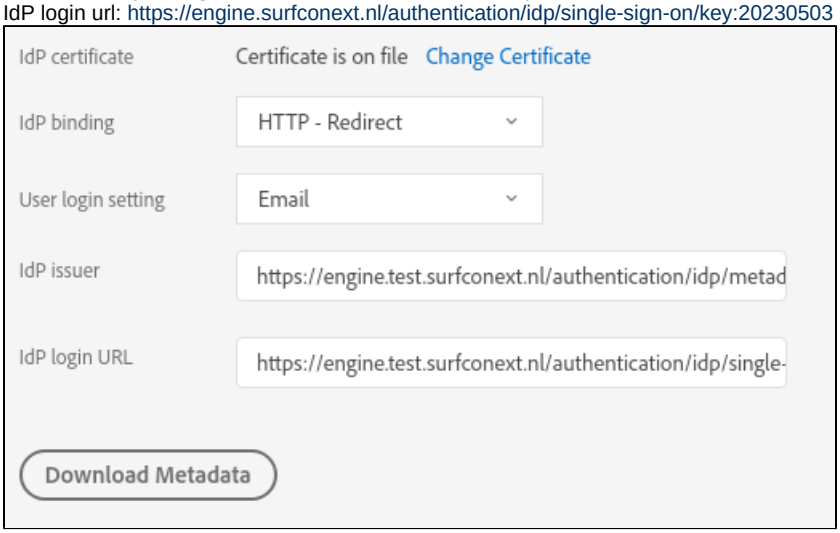
- The following screen will appear.



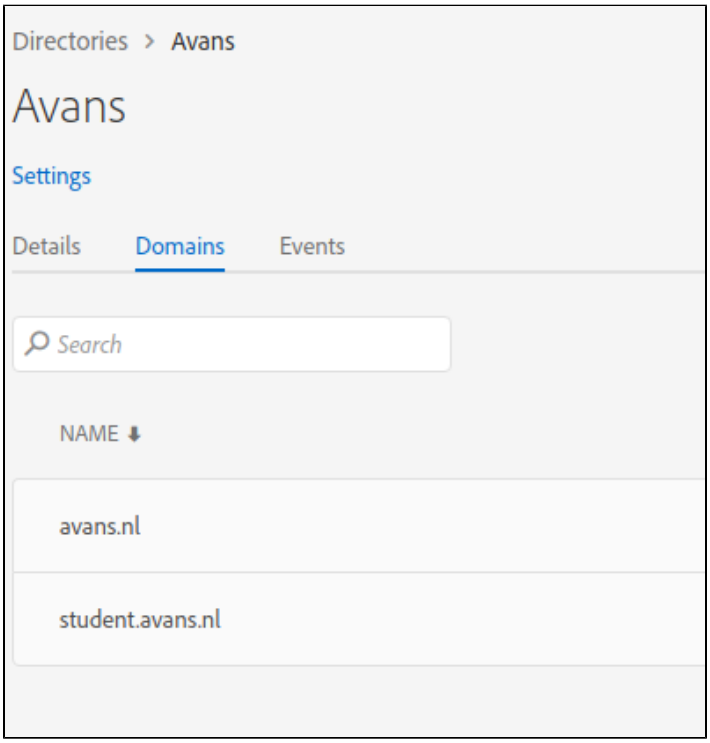
- On this page you can download the metadata of the Adobe Creative Cloud for use with our SURFconext SP Dashboard and you can upload the SURFconext metadata in the Adobe Admin Console.Click the button 'Download Adobe metadata file' and save this for future use, see the steps below.
- Decide if you want to connect to our test or our production environment. You must upload the SURFconext IdP metadata file to Adobe to complete the SAML setup as shown in the screenshot above. To connect to the SURFconext **Test Environment** use the following metadata and save this as an XML:
    a. https://metadata.test.surfconext.nl/idp-metadata.xml. If asked, the following applies:
        i. IdP certificate is the Assertion signing certificate as found on https://metadata.test.surfconext.nl/ (engine.test.surfconext.nl 20230403 certificate)
        ii. IdP binding: choose "HTTP - Redirect"
        iii. User login setting: choose "Email"
        iv. IdP issuer: https://engine.test.surfconext.nl/authentication/idp/metadata
        v. IdP login url: https://engine.test.surfconext.nl/authentication/idp/single-sign-on/key:20230403

2. If you want to configure the connection for your **production** IdP, connect to the SURFconext **Production Environment** using the following data:
    a. https://metadata.surfconext.nl/idp-metadata.xml
        i. IdP certificate is the Assertion signing certificate as found on https://metadata.surfconext.nl/ (engine.surfconext.nl 20230503 certificate)
        ii. IdP binding: choose "HTTP - Redirect"

iii. User login setting: choose "Email"
iv. IdP issuer: https://engine.surfconext.nl/authentication/idp/metadata
v. IdP login url: https://engine.surfconext.nl/authentication/idp/single-sign-on/key:20230503



- Some work on SURFconext needs to be done as well. You will see a 'Download Metadata' button. You will need this downloaded metadata later on, when you define the service in SURFconext. See the paragraph below for more on that.
- Now that you have configured the Directory as mentioned above you can link this directory to the previously created domains. Navigate to the 'Domains' screen as shown below:



- In the tab "Events" you will find logging when the link is active.

Configuration of SURFconext

By now, you should be finished with configuring the instance of Adobe Creative Cloud and it is ready to be used with SURFconext. Before you can use it to authenticate to the service using SURFconext, Adobe Creative Cloud needs to be configured in SURFconext. At this point there are three options for you to proceed:

- If you are familiar with SURFconext you can make use of the Service Provider Dashboard and define the service using the created and downloaded metadata as shown above. If you want us to create a new instance to your dashboard for this, send us an email at support@surfconext.nl and mention who needs access at your institution. **This is the preferred way** of managing entities in SURFconext.
- If you are new to the SP Dashboard or SURFconext and can't wait to get started with the SP dashboard, send us a mail at support@surfconext.nl and we will help you get started.

- If you are not familiar with SURFconext and do not intend to create instances in the SP Dashboard in the future, you can send us a mail at support@surfconext.nl. We will use the generated metadata to configure the entity in SURFconext for you.

> **Certificate**
>
> The certificate as generated by Adobe Creative Cloud is currently incompatible with the SP Dashboard. Remove the generated certificate and paste this random but compatible certificate to continue publishing the service through the SP Dashboard. It is not used in SURFconext, but for now needed to publish you service. We will not use this during the logon process. This is only used when you decide to do a signed authentication with SURFconext, wich is not the case with Adobe.

Attribute Manipulation

Adobe does not use standard attribute names. As a result, SURFconext will have to make adjustments to make this work. Send a mail to support@surfconext.nl and ask to enable **attribute manipulation** for the entity of the following attributes :

- The NameIDFormat of the entity needs to be set to "**urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified**"
- The e-mail address of the user needs to be mapped to the Subject, the **NameID**
- urn:mace:dir:attribute-def:givenName (urn:oid:2.5.4.42) to be sent as **FirstName**
- urn:mace:dir:attribute-def:sn (urn:oid:2.5.4.4) to be sent as **LastName**
- urn:mace:dir:attribute-def:mail (urn:oid:0.9.2342.19200300.100.1.3) to be sent as **Email**

The code of the attribute manipulation will be similar to what you see below.

Attribute Manipulation

```
# Required attributes
$attr_gn       = 'urn:mace:dir:attribute-def:givenName';
$attr_sn       = 'urn:mace:dir:attribute-def:sn';
$attr_mail     = 'urn:mace:dir:attribute-def:mail';

# attributes to let through (ARP)
$requiredAttributes = array(
  'FirstName',
  'LastName',
  'Email'
);

if (isset($attributes) and ($attributes !== FALSE)) {
    if (!empty($attributes[$attr_mail][0])) {
        $subjectId = $attributes[$attr_mail][0];
        $attributes['Email'] = $attributes[$attr_mail];
    }
    if (!empty($attributes[$attr_gn])) {
        $attributes['FirstName'] = $attributes[$attr_gn];
    }
    if (!empty($attributes[$attr_sn])) {
        $attributes['LastName'] = $attributes[$attr_sn];
    }
}

# Remove all other attributes
foreach ($attributes as $k => $v) {
  if (!in_array($k, $requiredAttributes)) {
    unset($attributes[$k]);
  }
}
```

How to log on to the service as an and user

When you have configured the service you can logon to the service through SURFconext as follows.

- Navigate to 'https://www.adobe.com/nl/'
- You will probably be redirected to the Dutch part of the Adobe site, so click 'Aanmelden' (Dutch for Logon) in the upper right of the screen.
- Because you are using SURFconext to log on, continue by clicking 'Aanmelden met een Enterprise ID'.

- Enter your email-adres or simply the domain of your institution (the part after '@' of your email adres). There is no need to fill in your password. You will be redirected as soon as you click on the password field.
- Enter your credentials at your institution and you will be logged on to Adobe Connect through SURFconext

Active sessions

Adobe Creative Cloud allows two active sessions. If you have activated your individual Creative Cloud membership on two computers already, you must first deactivate it on one of the two systems to get going on a third device.

Set up the User Sync tool management of users

The User Sync tool from Adobe is a command-line utility that moves user and group information from your organization's enterprise directory system (such as an Active Directory or other LDAP systems) to your organization's directory in the Adobe Admin Console. Each time you run the User Sync tool, it looks for differences between the user and group information in the two systems and updates the Adobe directory to match the information in your directory. This is also referred to as 'Just In Time' management of users. This document provides step-by-step instructions to interface an Active Directory system with the Adobe Admin Console. If you're using a directory system other than Active Directory, the instructions in this documentation do not apply and need to be modified as required. See the supplied links on that page for more information.