GENERAL SECURITY REQUIREMENTS

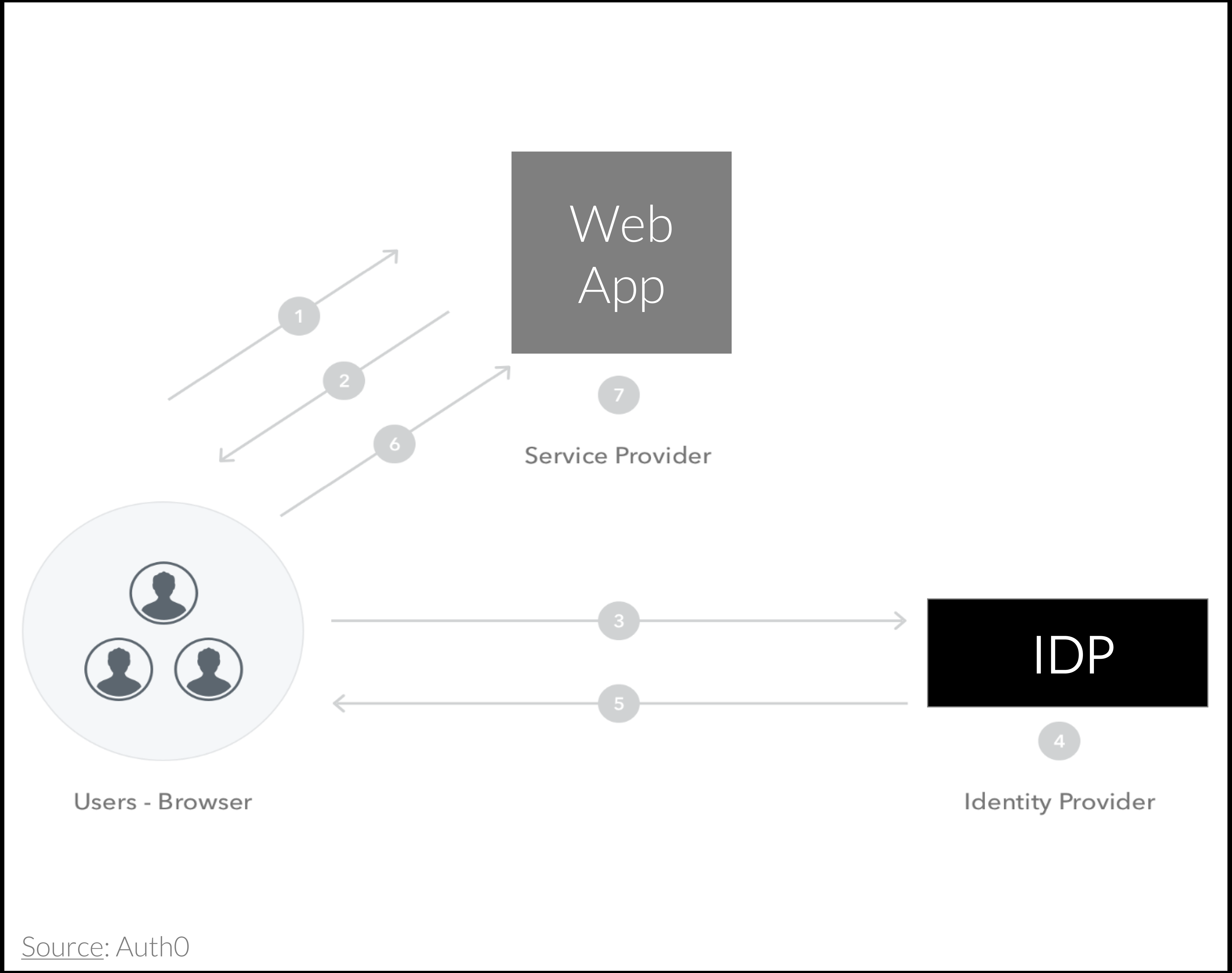
AUTHENTICATION

- All applications MUST rely on **Identity Provider (IDP)** and Active Directory (AD) to authenticate and SHOULD provide SSO to end-users wherever the application is hosted.
- Local authentication is prohibited except for setup and support.
- The authentication process depends on the application type and the protocols that are supported by the application.
  - Dynatrace relies on SAML authentication method

AUTHORIZATION

- After successful authentication, the **application** MUST check user access rights to application resources (permissions).
  - Identity Provider MAY provide AD user attributes (login, name, country, division, role, location, group membership…) to manage permissions in the application.
  - Identity Provider SHOULD control third party resources access by the application on behalf on the user

SAML AUTHENTICATION FLOW



Source: Auth0

1. The end-user tries to log in to the Web App from a browser
2. The Web App responds by generating a SAML request
3. The browser redirects the user to IDP
4. IDP parses the SAML request, prompts the user for login/password if necessary and generates a SAML response
5. IDP returns the encoded SAML response to the browser
6. The browser sends the SAML response to the Web App for verification
7. If the verification is successful, the end-user will be logged in to the Web App and granted access to all the various resources

0. SSO SIGNING CERTIFICATE RENEWAL

Certificate rollover is handled by Global IT’s Security Run Team.
You must follow their guidelines and requirement during the certificate renewal period to guarantee success of the operation.

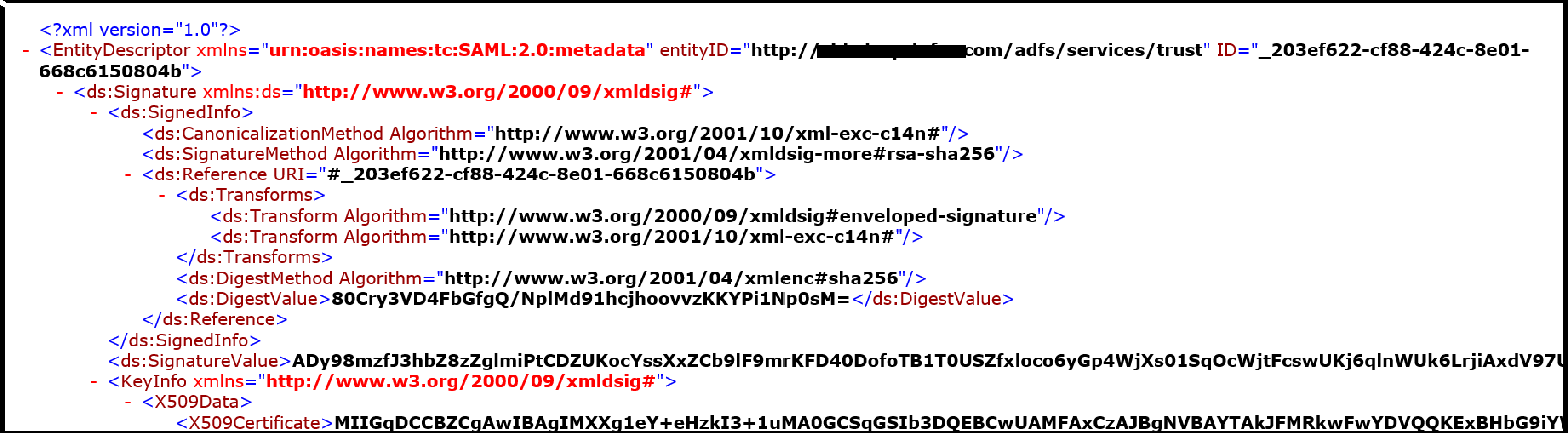
A specific Teams environment will be created especially for the certificate renewal period in which project manager will find:

- ✓ General information on the process
- ✓ New SSO signing certificate
- ✓ Discussion space with the Security Run Team that handle the rollover

1. GET METADATA.XML FILE FROM THE SECURITY TEAM

Once the certificate rollover is made, the Security Run Team will be able to provide the new metadata from Chanel IDP. These will be used to update the SSO configuration in Dynatrace interface.

federationmetadata.xml



```
  <?xml version="1.0"?>
- <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://[redacted]com/adfs/services/trust" ID="_203ef622-cf88-424c-8e01-
  668c6150804b">
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      - <ds:Reference URI="#_203ef622-cf88-424c-8e01-668c6150804b">
        - <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>80Cry3VD4FbGfgQ/NplMd91hcjhoovvzKKYPi1Np0sM=</ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>ADy98mzfJ3hbZ8zZglmiPtCDZUKocYssXxZCb9lF9mrKFD40DofoTB1T0USZfxloco6yGp4WjXs01SqOcWjtFcswUKj6qlnWUk6LrjiAxdV97U
    - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      - <X509Data>
          <X509Certificate>MIIGqDCCBZCgAwIBAgIMXXg1eY+eHzkI3+1uMA0GCSqGSIb3DQEBCwUAMFAxCzAJBgNVBAYTAkJFMRkwFwYDVQQKExBHbG9iY
```

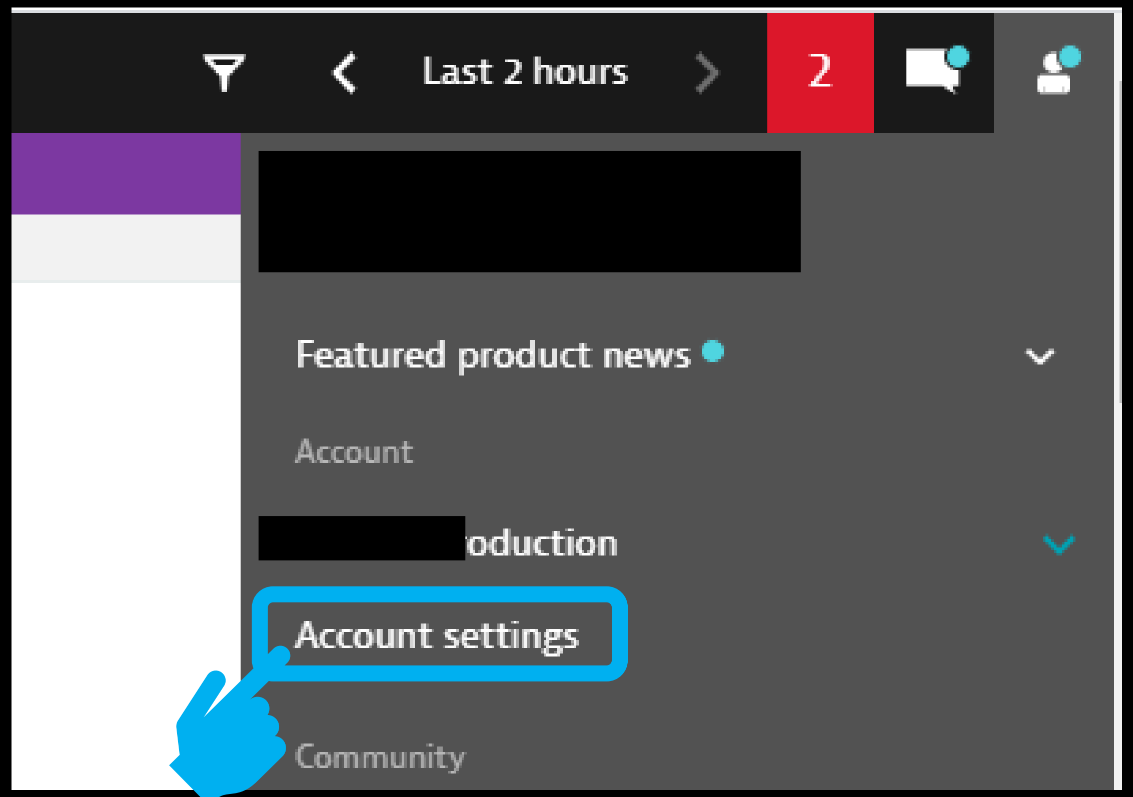
dynatrace

2. VERIFY OWNERSHIP ON THE DOMAIN

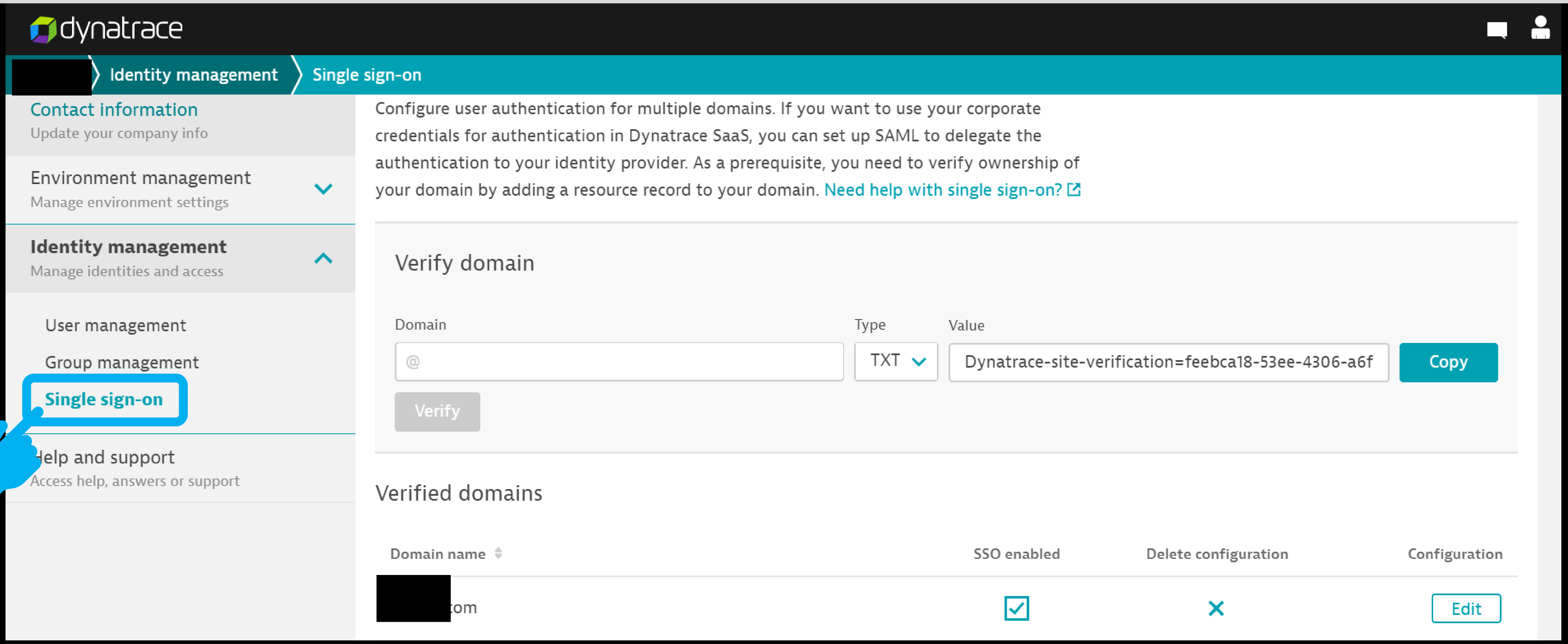
Before you can configure the domain for which you want to set up SAML, you need to prove ownership of the domain.

After following the two steps below, you should have the *xxxx.com* domain listed in the "verified domains" field.

You can click on the "Edit" button to set up or update the SSO configuration.



Select "**Account settings**" from the user menu on the right side of the menu bar



Configure user authentication for multiple domains. If you want to use your corporate credentials for authentication in Dynatrace SaaS, you can set up SAML to delegate the authentication to your identity provider. As a prerequisite, you need to verify ownership of your domain by adding a resource record to your domain. Need help with single sign-on?

Verify domain

Domain: @
Type: TXT
Value: Dynatrace-site-verification=feebca18-53ee-4306-a6f

Copy

Verify

Verified domains

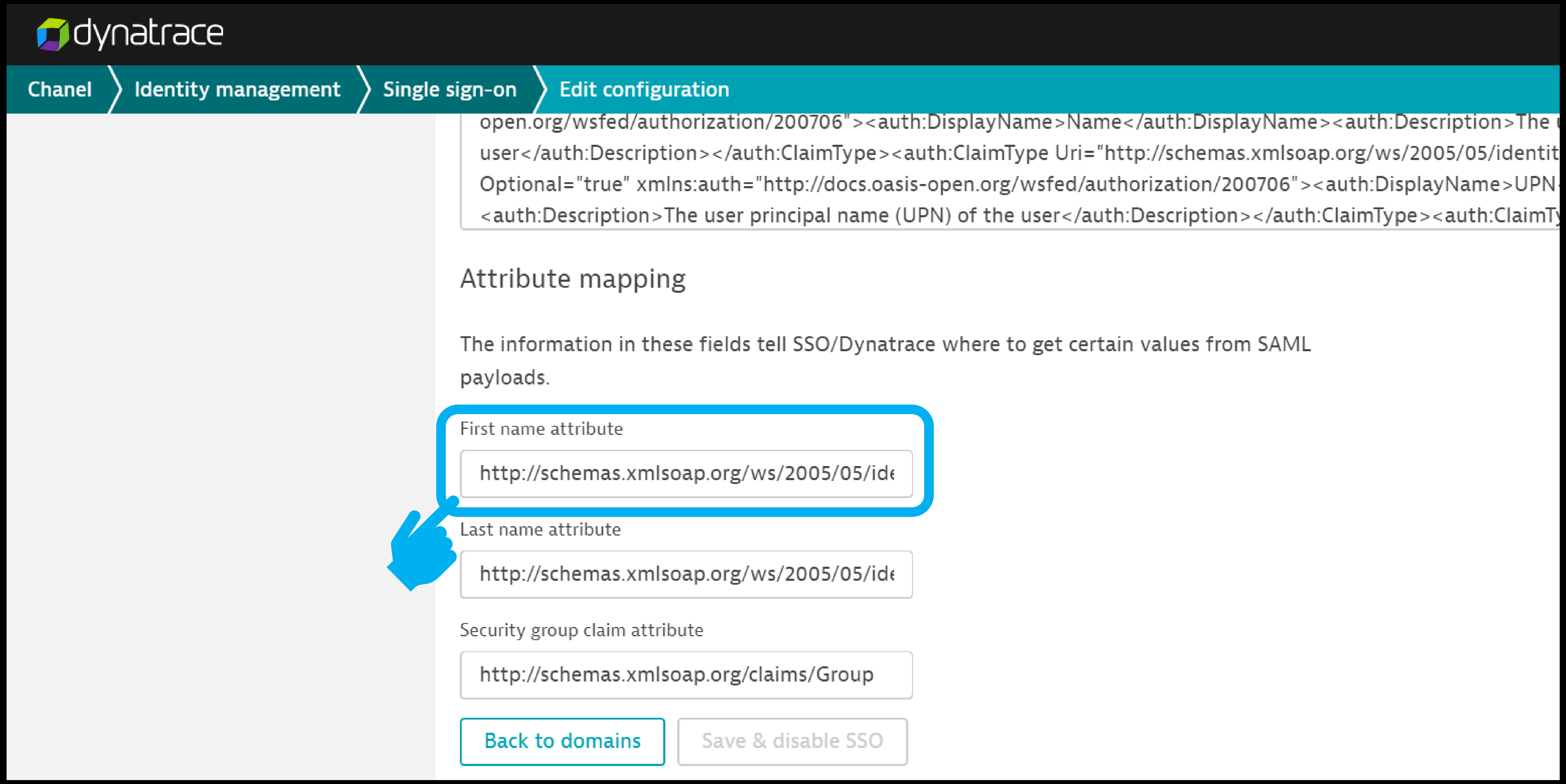
Domain name	SSO enabled	Delete configuration	Configuration
[redacted]om	☑	×	Edit

Select "**Identity management**" then "**Single sign-on**" from the navigation menu on the left

IMPORTANT: You must have a fallback user account so you don't get locked out if you have configuration troubles. Or make sure that somebody with a non-federated access can be able to troubleshoot if you have configuration issues.

3. VERIFY SAML ATTRIBUTES

At the very bottom of the configuration panel, you can find the “Attribute mapping” section which lists the 3 attributes required for authentication to Dynatrace. These are :
Givenname, Surname & Groups



```
open.org/wsfed/authorization/200706"><auth:DisplayName>Name</auth:DisplayName><auth:Description>The 
user</auth:Description></auth:ClaimType><auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identit
Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706"><auth:DisplayName>UPN
<auth:Description>The user principal name (UPN) of the user</auth:Description></auth:ClaimType><auth:ClaimTy
```

Attribute mapping

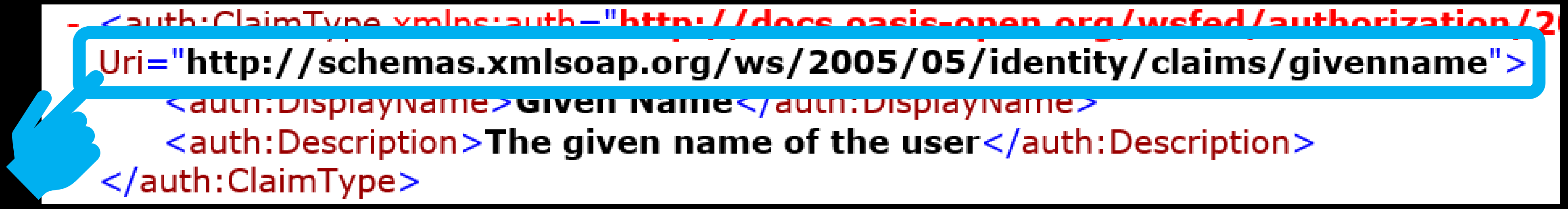
The information in these fields tell SSO/Dynatrace where to get certain values from SAML payloads.

First name attribute: http://schemas.xmlsoap.org/ws/2005/05/ide

Last name attribute: http://schemas.xmlsoap.org/ws/2005/05/ide

Security group claim attribute: http://schemas.xmlsoap.org/claims/Group

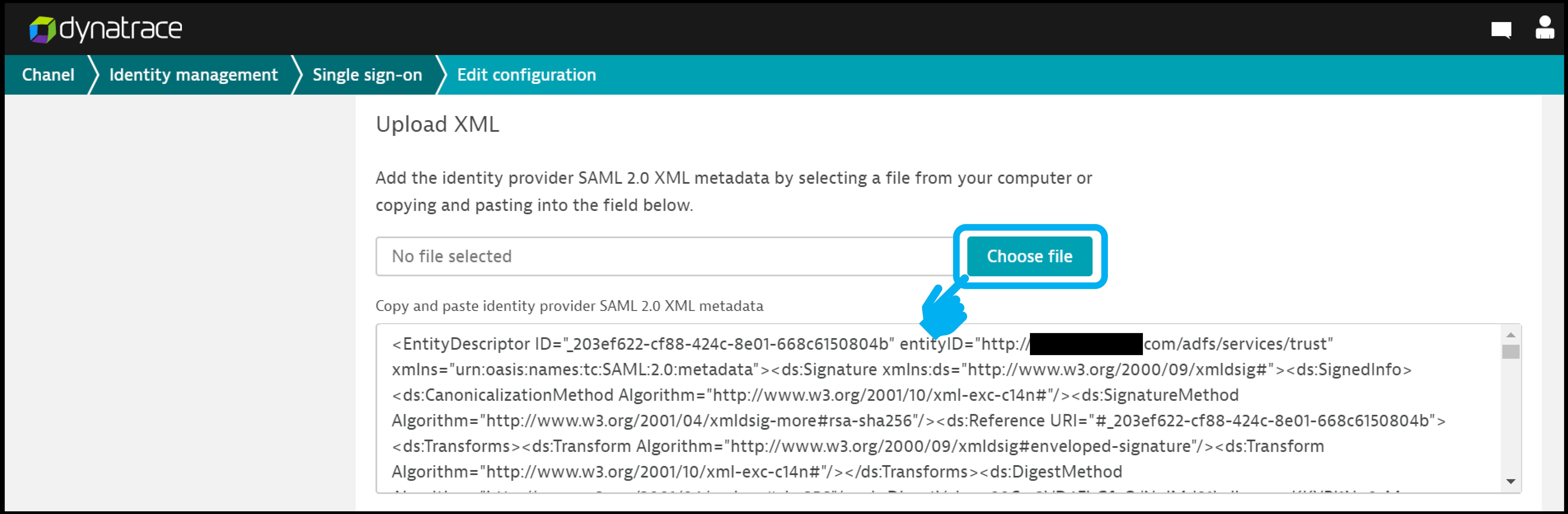
Verify that the attributes mapping is still accorded to the new federationmetadata.xml file



```
- <auth:ClaimType xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/2
  Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
    <auth:DisplayName>Given Name</auth:DisplayName>
    <auth:Description>The given name of the user</auth:Description>
  </auth:ClaimType>
```

4. UPDATE METADATA CONFIGURATION

Once you have verified that the attribute mapping is correct and accorded to the new metadata of the IDP, you can upload the new configuration file.



Upload XML

Add the identity provider SAML 2.0 XML metadata by selecting a file from your computer or copying and pasting into the field below.

No file selected

Copy and paste identity provider SAML 2.0 XML metadata

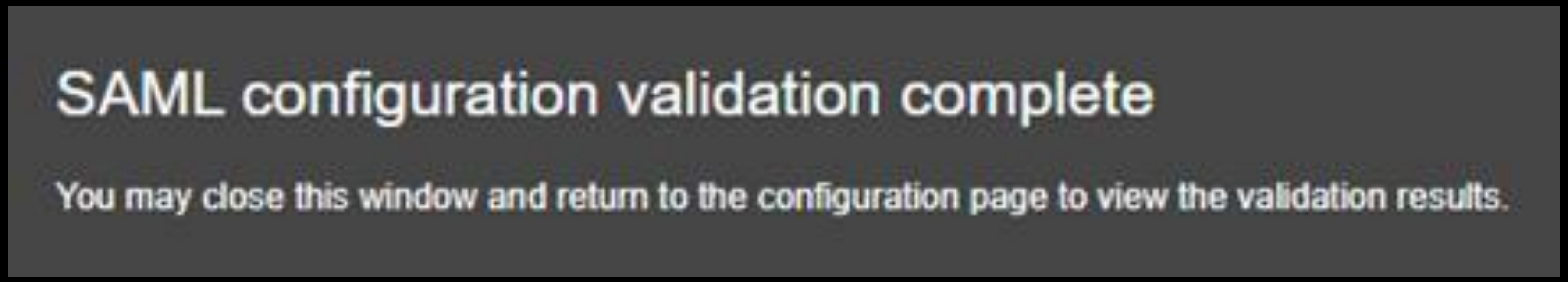
```
<EntityDescriptor ID="_203ef622-cf88-424c-8e01-668c6150804b" entityID="http://[redacted]com/adfs/services/trust"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><ds:Reference URI="#_203ef622-cf88-424c-8e01-668c6150804b">
<ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod
```

Select **"Choose file" to upload the new federationmetada.xml file that the Security Team has provided.**

NOTE: Since it is a renewal of certificate, an SSO configuration is already in place. In the field below, you can see the current SAML IDP metadata configuration.

5. VALIDATE CONFIGURATION

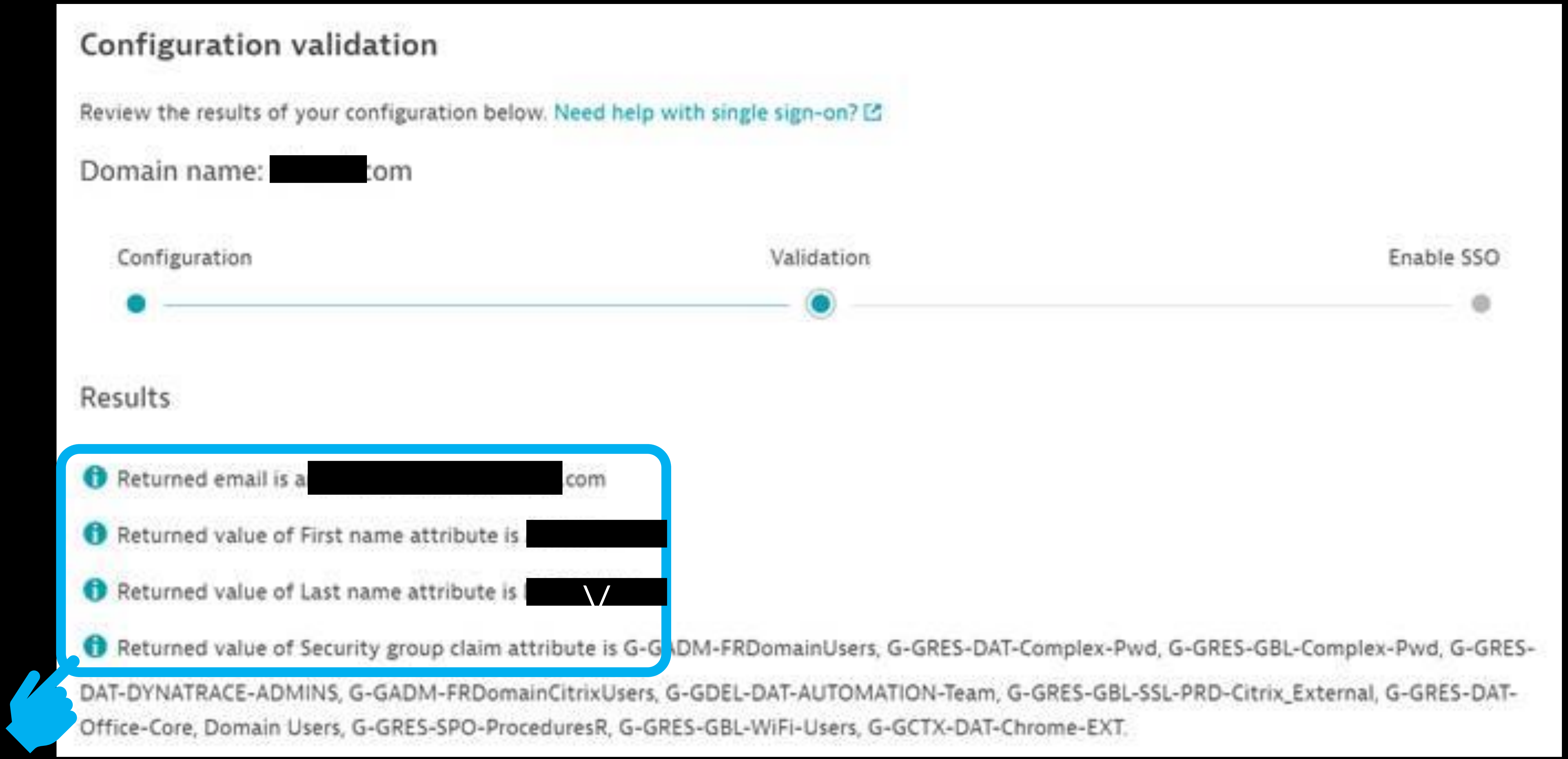
Once you have uploaded the new configuration file, you can click on the "Validate configuration" at the very bottom of the panel.



SAML configuration validation complete

You may close this window and return to the configuration page to view the validation results.

This will open a new windows on your browser to test the connection to the IDP and validate the SSO configuration



Configuration validation

Review the results of your configuration below. Need help with single sign-on?

Domain name: [redacted]com

Results

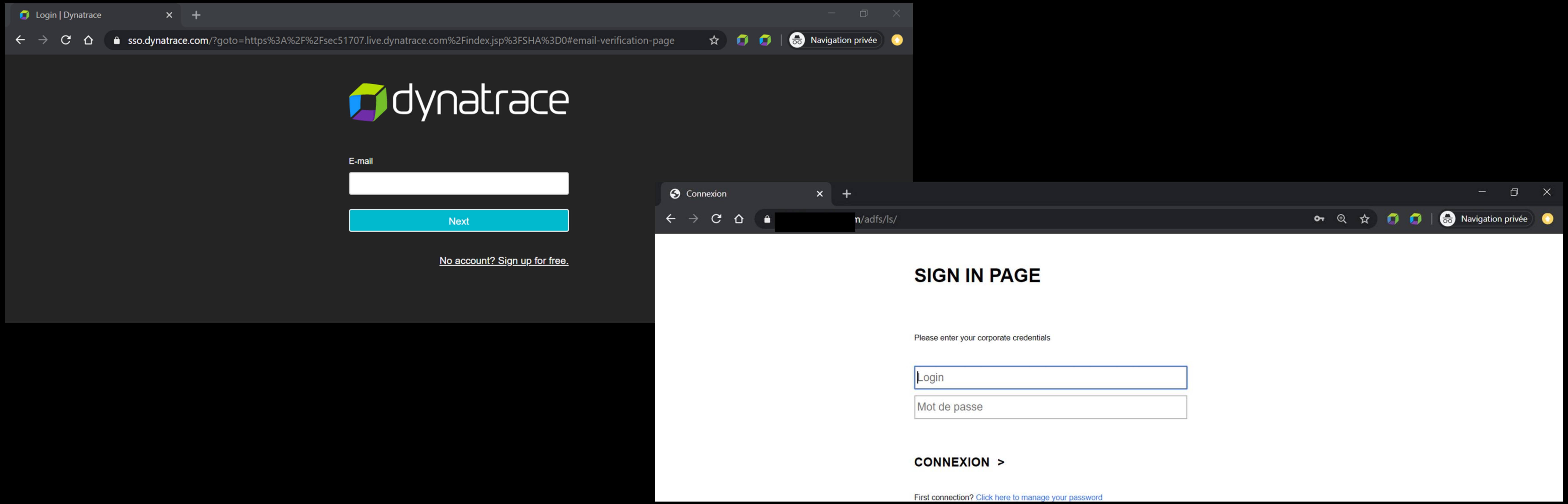
- Returned email is a[redacted]com
- Returned value of First name attribute is [redacted]
- Returned value of Last name attribute is [redacted]
- Returned value of Security group claim attribute is G-GADM-FRDomainUsers, G-GRES-DAT-Complex-Pwd, G-GRES-GBL-Complex-Pwd, G-GRES-DAT-DYNATRACE-ADMINS, G-GADM-FRDomainCitrixUsers, G-GDEL-DAT-AUTOMATION-Team, G-GRES-GBL-SSL-PRD-Citrix_External, G-GRES-DAT-Office-Core, Domain Users, G-GRES-SPO-ProceduresR, G-GRES-GBL-WiFi-Users, G-GCTX-DAT-Chrome-EXT.

On the other window, Dynatrace should display this validation screen, proving that Dynatrace can retrieve your connection information (email, name, and groups belongings)

NOTE: If the validation step of the configuration is correct, you can now terminate the configuration by re-enabling SSO on the domain.

6. FURTHER CHECK OF CONFIGURATION

To be sure that the SSO configuration has been made and that there is no service interruption, you can check from an incognito browser window to access Dynatrace application and make sure that SAML authentication via AD is up and running.



Login | Dynatrace

sso.dynatrace.com/?goto=https%3A%2F%2Fsec51707.live.dynatrace.com%2Findex.jsp%3FSHA%3D0#email-verification-page

Navigation privée

dynatrace

E-mail

Next

No account? Sign up for free.

Connexion

[redacted]n/adfs/ls/

Navigation privée

SIGN IN PAGE

Please enter your corporate credentials

Login

Mot de passe

CONNEXION >

First connection? Click here to manage your password