Creatio Academy

Authentication

Version 8.0

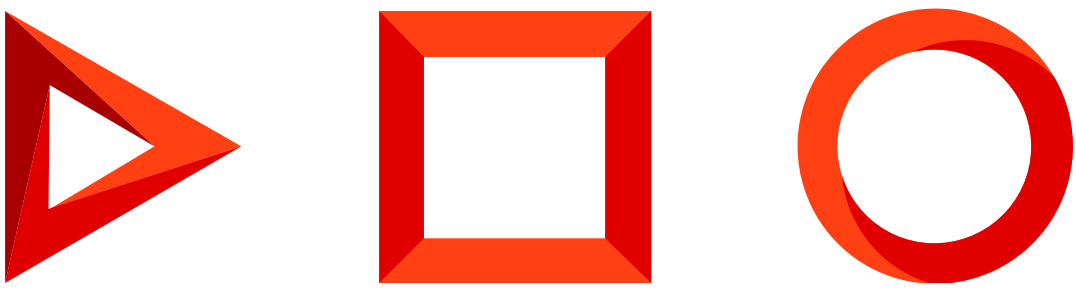


Table of Contents

Set up Single Sign-On

PRODUCTS: ALL CREATIO PRODUCTS

The Single Sign-On technology in Creatio enables users to log in to multiple services using a single account. After a user signs in once via an identity provider, they can access their applications and services without the need to enter their login credentials. When a user signs out of any of the applications, sessions of all other connected applications end as well.

Prerequisites:

1. A Creatio website available over HTTPS.
2. Administrator privileges on the website.
3. Administrator privileges in the identity provider.
4. Users in the corporate domain.

In general, the following **steps** are required to set up Single Sign-On:

1. Download the file that contains the integration metadata.
2. Set up the identity provider by adding Creatio to trusted websites.
3. Set up the trusted identity provider in Creatio.

You can expedite the setup by using one of the following pre-configured providers:

- AD FS
- Azure AD
- Okta

Also, you can integrate Creatio with any identity provider that supports the SAML 2.0 protocol.

Single Sign-On via AD FS

PRODUCTS: ALL CREATIO PRODUCTS

> This article is relevant to Creatio version 8.0.3 and later. If you need to set up integration with Creatio version 8.0.2 and earlier for testing purposes or to look for errors, follow the instructions for Creatio version 7.18.

You can integrate your Active Directory Federation Services (AD FS) instance to manage single sign-on for your members. To do this, perform the setup both in AD FS and Creatio.

> **Attention.** This example uses the, https://site01.creatio.com/Demo_161215/ Creatio website and http://ADFS01.mysite.com/ADFS/ AD FS website. Replace these URLs with the corresponding URLs of your

websites when you perform the actual setup.

In general, the following **steps** are required to set up Single Sign -On in Creatio:

1. Download the file that contains the integration metadata. Read more >>>
2. Perform the setup in AD FS. Read more >>>
3. Perform the setup in Creatio. Read more >>>

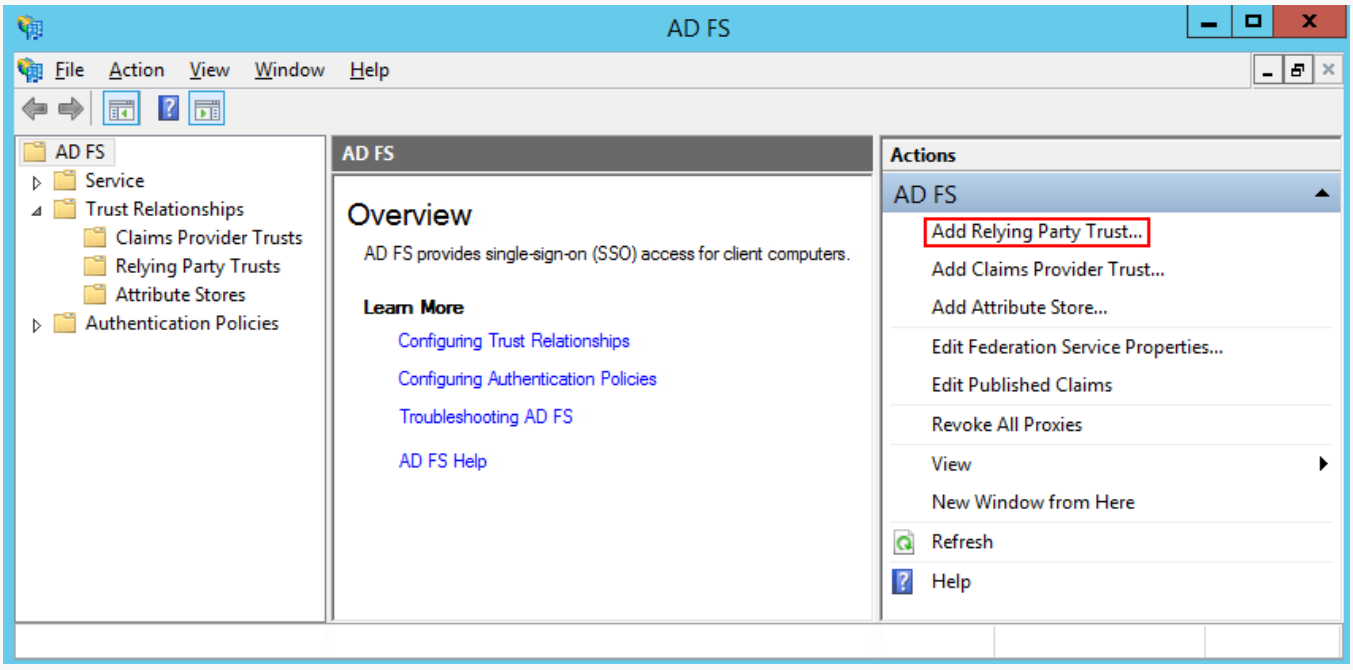
Download the metadata

1. Click the button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “AD FS.” This opens the setup page.
5. Click [*Get metadata*].
6. Save the file to your local machine.

Perform the setup in AD FS

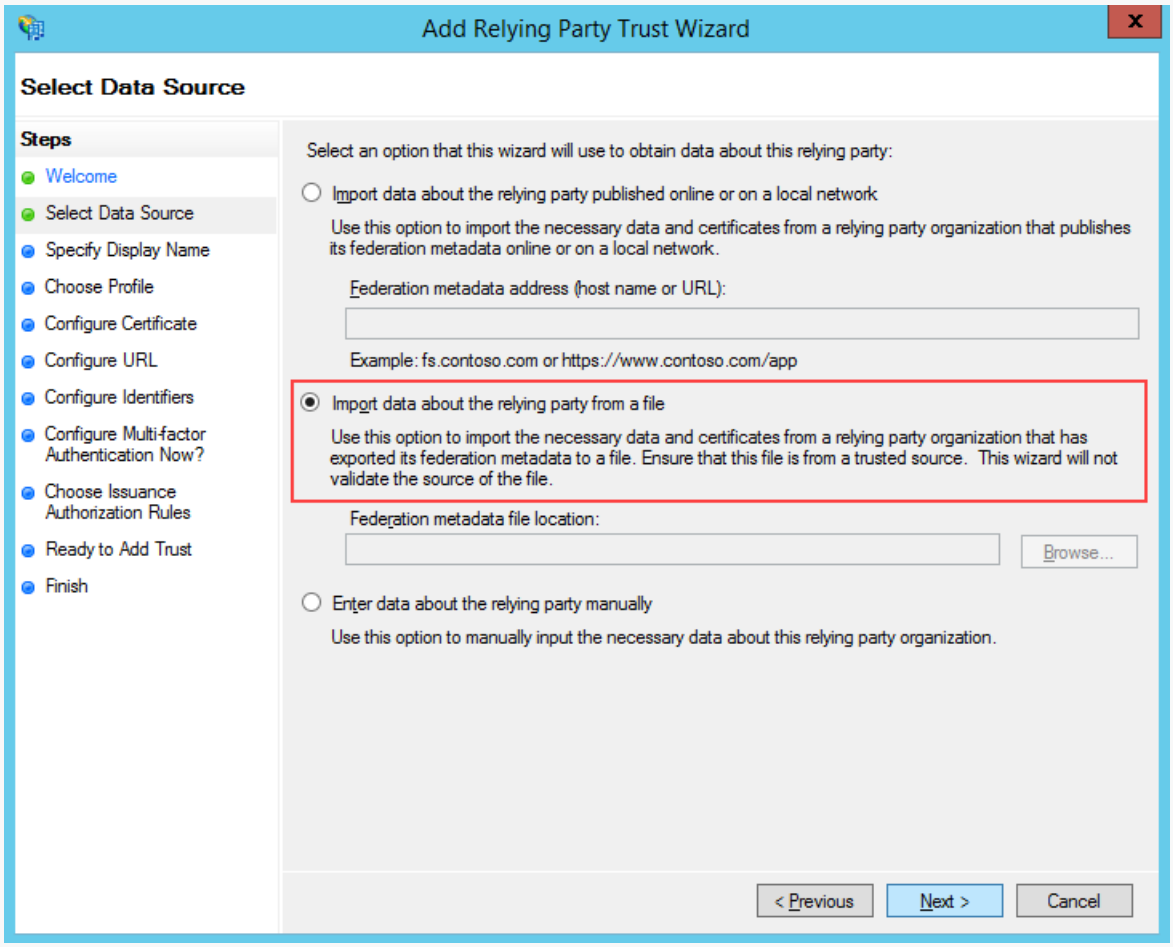
1. Add a new Relying Party Trust to ADFS (Fig. 1).

Fig. 1 Relying Party Trust menu



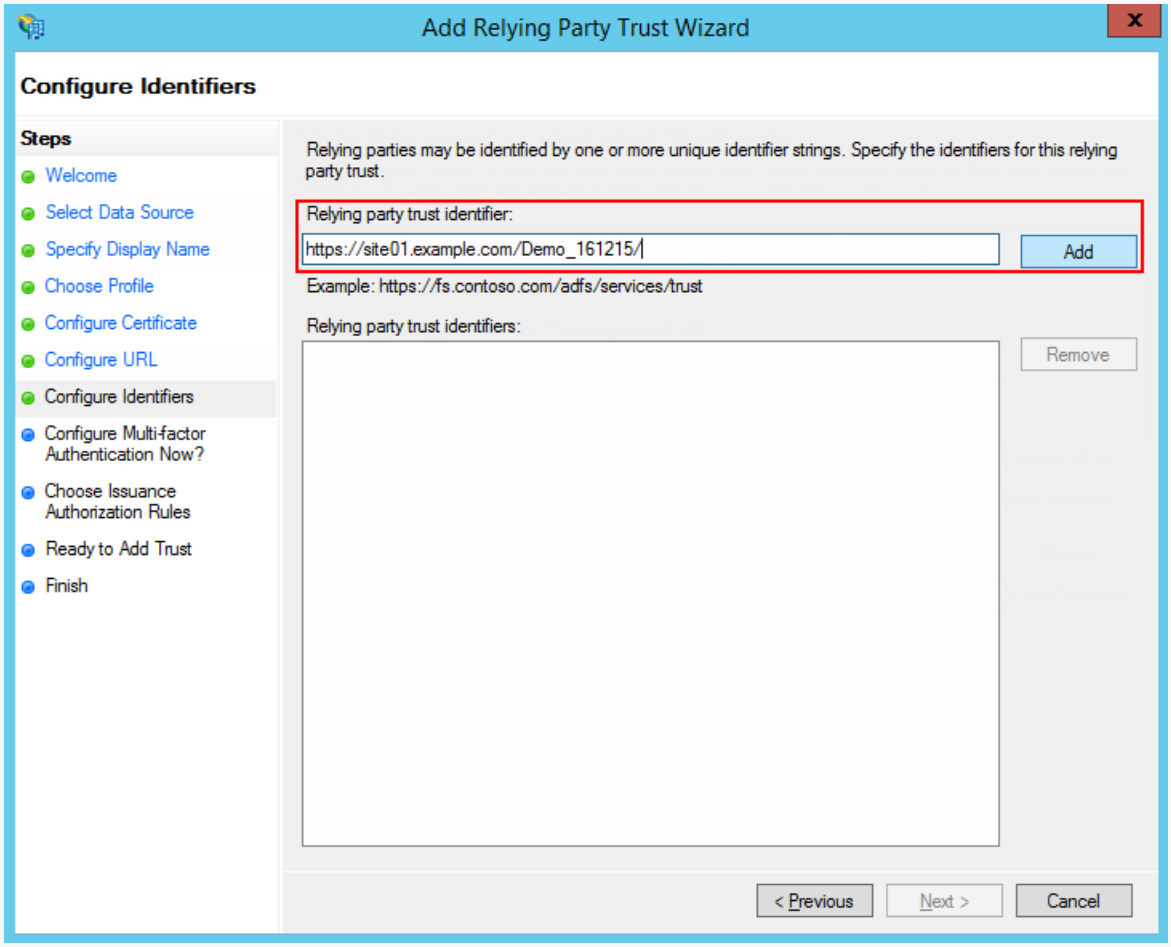
2. Select “Import data about the relying party from file,” as shown on the Fig. 2.

Fig. 2 “Import data about the relying party from file” option



3. Specify the full website address in the identifier settings and click [*Add*], as shown on the Fig. 3.

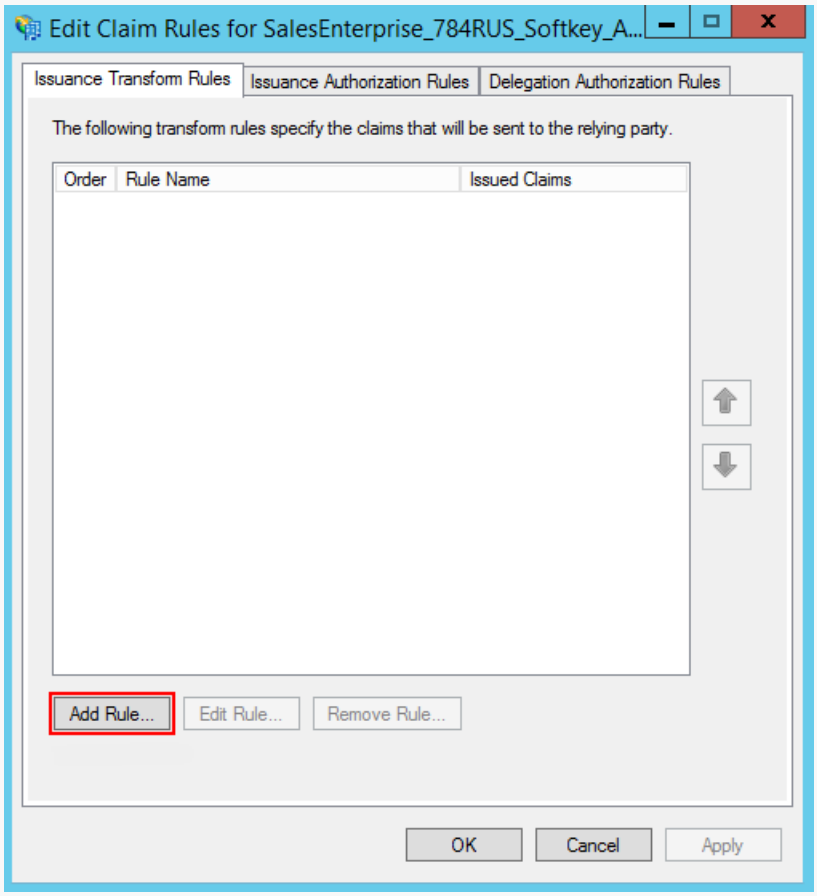
Fig. 3 Identifier



Attention. The identifier is required to verify the authenticity of a source that requests authentication. The URL must match verbatim, including the "/" at the end.

4. Set up the rest of the parameters according to your security requirements. You can leave default values for test purposes.
5. Click [*Finish*]. This opens a window.
6. Click [*Add Rule*] and add a new SAML Assertion to SAML Response rule (Fig. 4)

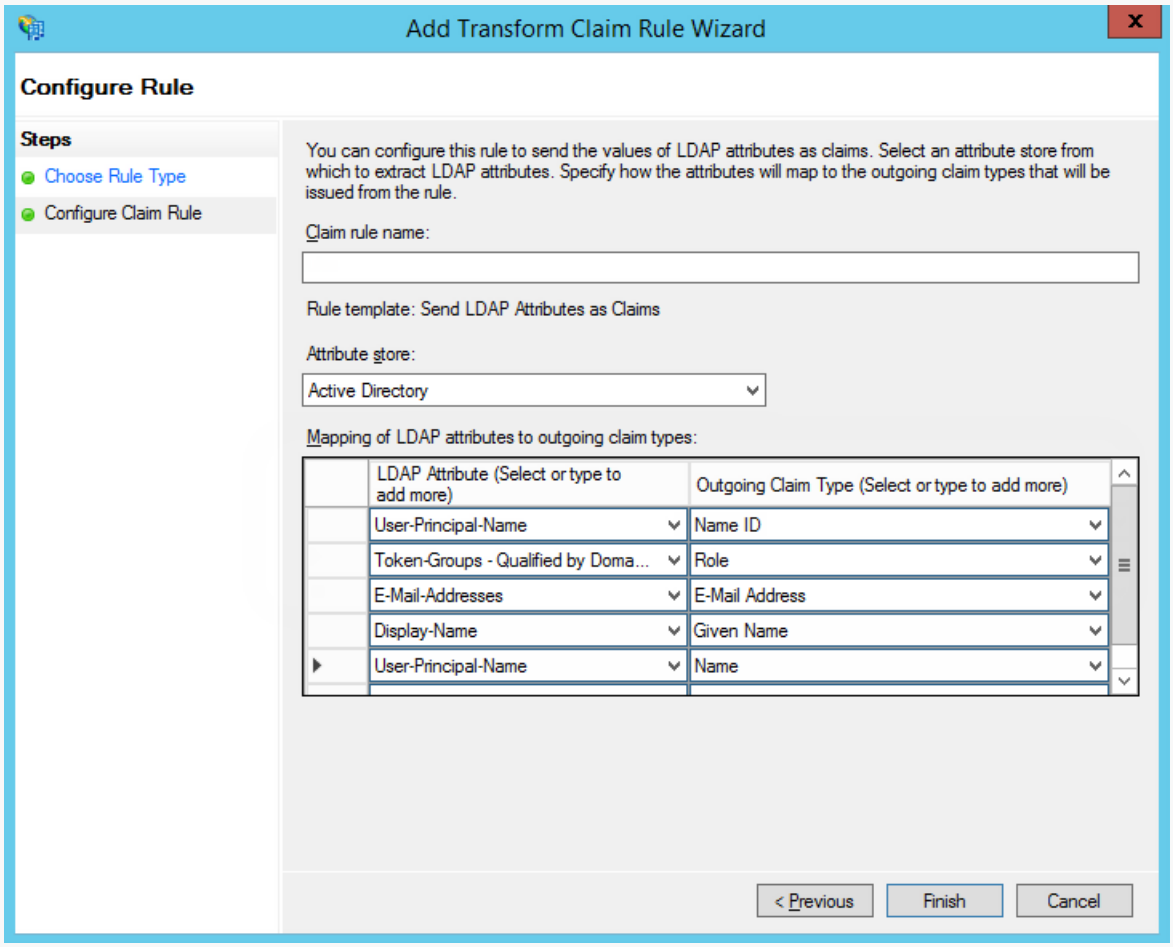
Fig. 4 "Add rule" button



Note. Creatio will use the data generated based on the new rule to search for users, as well as to update their profiles and roles.

7. Keep the default settings and click [*Next*] on the first step of the Rule Wizard. Set up a set of parameters to receive from the user's data (Fig. 5). In this example, the user's name and a list of domain groups will be passed via SAML Assertion.

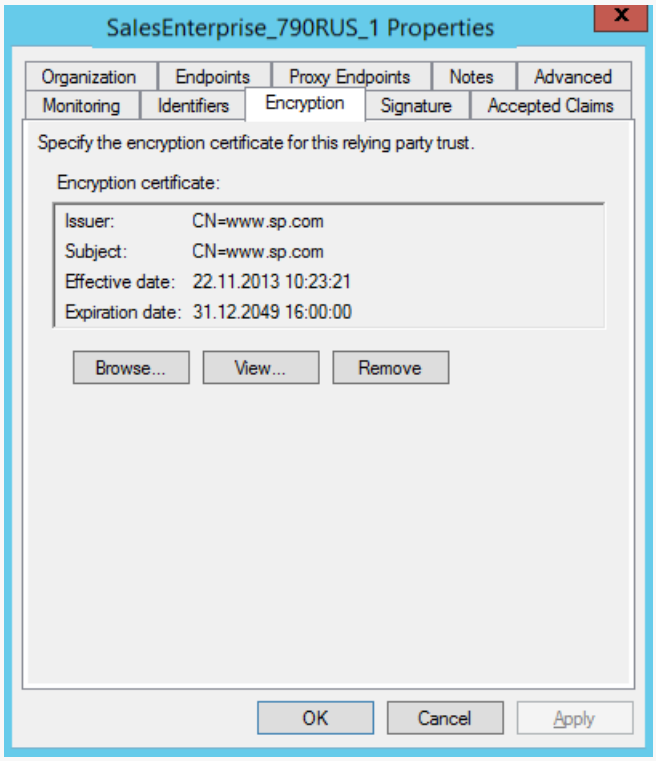
Fig. 5 Rule parameters



8. Click [*Save*].
9. Open the Trusted Relay settings, go to the [*Advanced*] tab, and specify SHA-1 encryption according to the website certificate algorithm.
10. Add the public certificate key on the [*Encryption*] tab to set up the SAML encryption (Fig. 6).

Note. If you are using Creatio in the cloud, get the public certificate key from the Creatio support service.

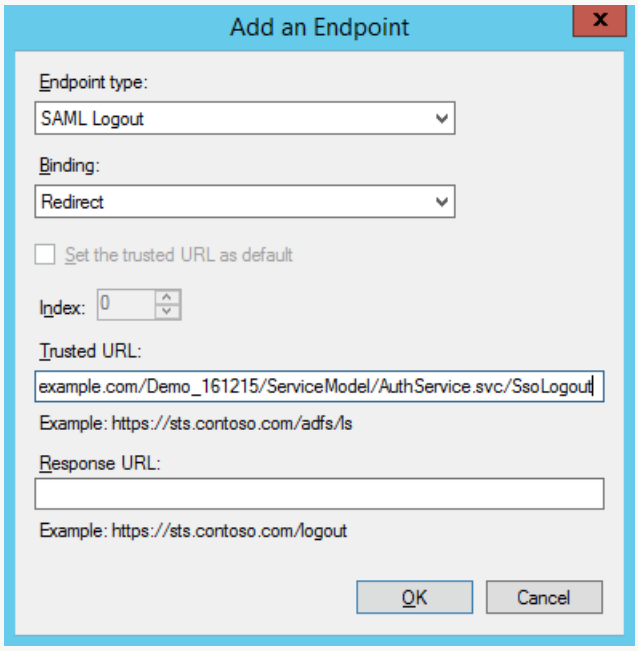
Fig. 6 [*Encryption*] tab



11. Add the logout endpoint and set the following parameters (Fig. 7) on the [*Endpoints*] tab:

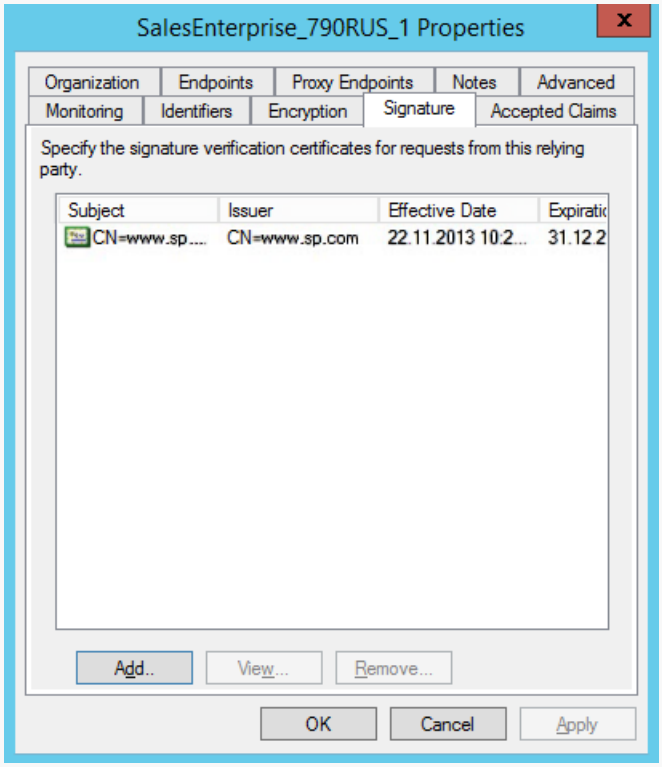
- Set [*Endpoint type*] to “SAML Logout”.
- Set [*Binding*] to “Redirect”.
- Enter https://site01.creatio.com/Demo_161215/ServiceModel/AuthService.svc/SsoLogout in the [*Trusted URL*] parameter.

Fig. 7 Endpoint parameters



12. Add the Logout Request certificate to the [*Signature*] tab, as specified on the Fig. 8.

Fig. 8 Logout Request certificate



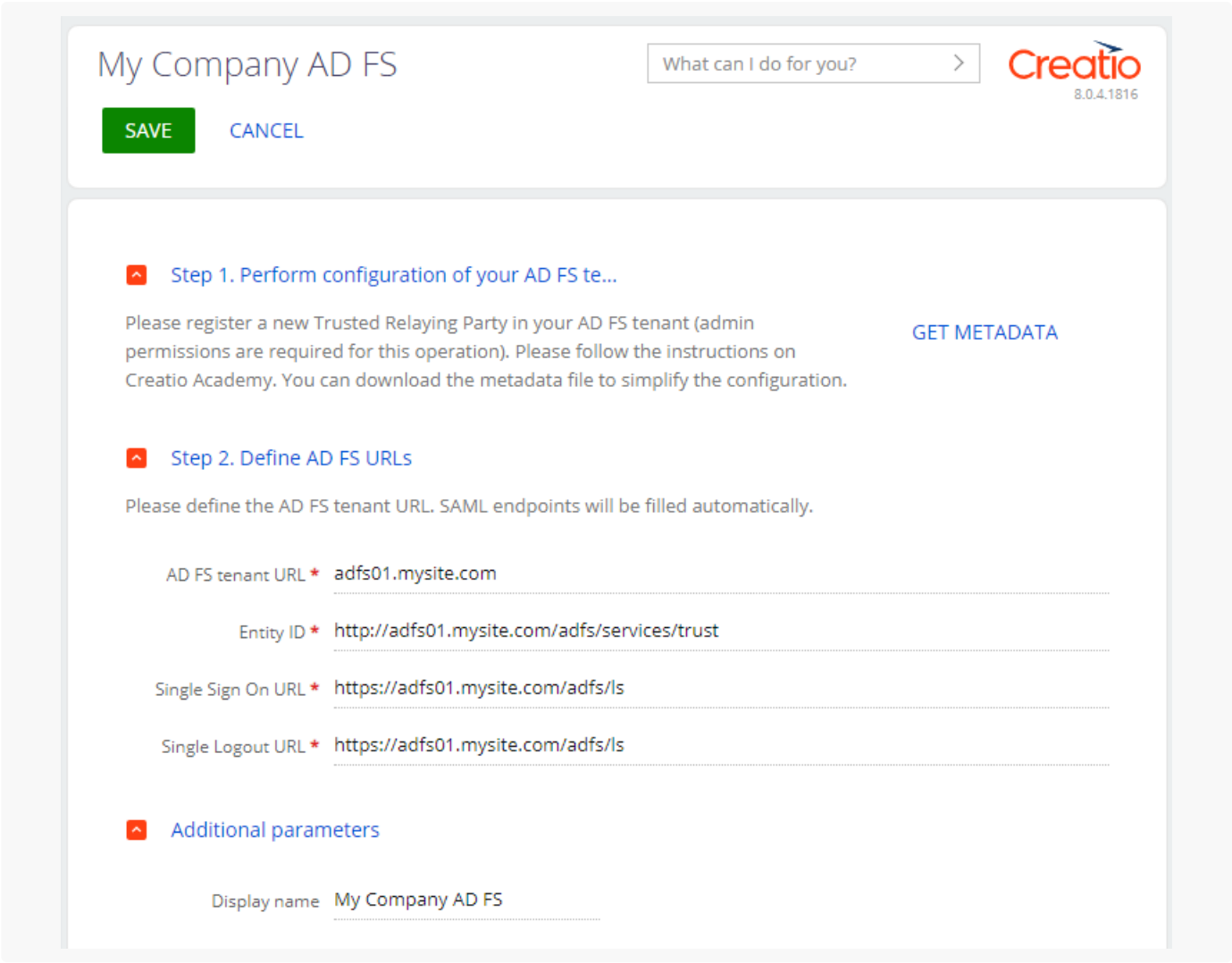
Attention. Single Sign-Out does not work without a certificate.

Perform the setup in Creatio

Follow these steps to set up single sign-on in Creatio:

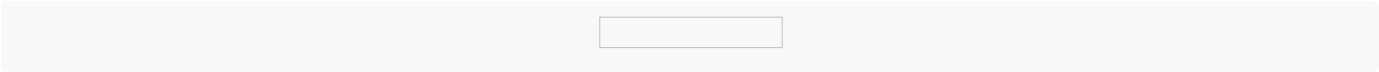
1. Click the button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “AD FS.” This opens the setup page.
5. Fill out the [*AD FS tenant URL*] parameter. Creatio will populate other parameters automatically.
6. Fill out the provider's name to display on the Creatio login page in the [*Display name*] field.

Fig. 9 AD FS settings



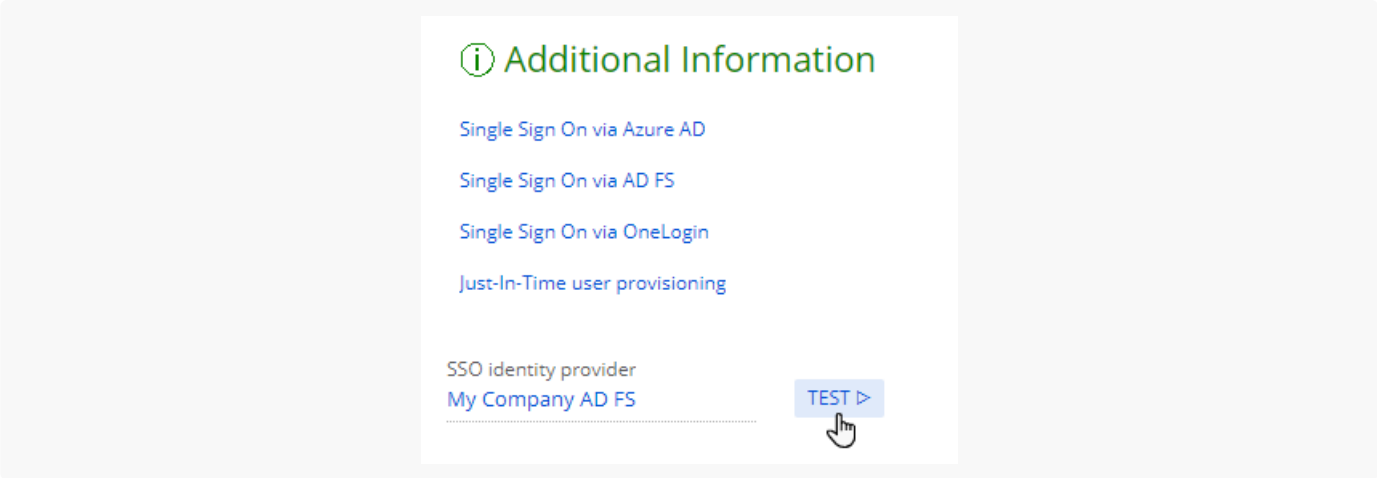
7. Save the changes.
8. Turn on Just-In-Time Provisioning (optional). This mechanism automatically creates the corresponding Creatio user account with proper data from the identity provider, such as user group, employee name, contact information, etc. To do this, select the [*Create and update users data when log in (Just-In-Time Provisioning)*] checkbox and map the fields (Fig. 10).

Fig. 10 Set up Just-In-Time Provisioning



9. Select your provider in the [*SSO identity provider*] field and save the changes.
10. Click [*Test*] to test whether the provider is working correctly (optional).

Fig. 11 Test the provider



Single Sign-On via Azure AD

PRODUCTS: ALL CREATIO PRODUCTS

This article is relevant to Creatio version 8.0.3 and later. If you need to set up integration with Creatio version 8.0.2 and earlier for testing purposes or to look for errors, follow the instructions for Creatio version 7.18.

You can integrate Creatio with Azure Active Directory (Azure AD) to manage single sign-on for all Creatio users that work in the corporate network.

Attention. The example uses the https://site01.creatio.com/Demo_161215/ Creatio URL. Replace these URLs with the corresponding URLs of your sites when you perform the actual setup.

In general, the following **steps** are required to set up Single Sign -On in Creatio:

1. Download the file that contains the integration metadata. Read more >>>
2. Perform the setup in Azure AD. Read more >>>
3. Perform the setup in Creatio. Read more >>>

Download the metadata

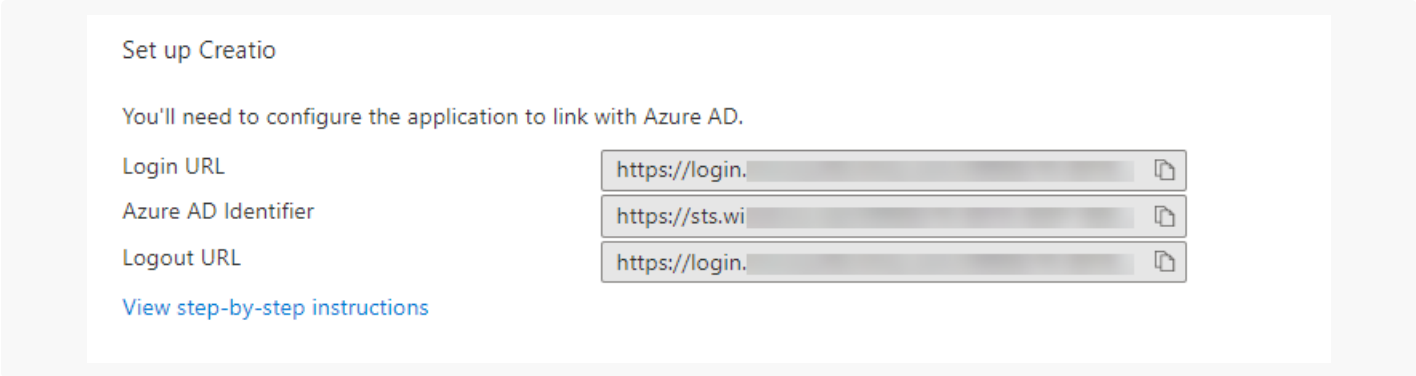
1. Click the button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “Azure AD.” This opens the setup page.
5. Click [*Get metadata*].
6. Save the file to your local machine.

Perform the setup in Azure AD

To configure the settings below, register Creatio in the administrator account of the enterprise identity service of Azure Active Directory (Azure AD). Learn more in the Microsoft documentation.

1. Add a new SSO application (Trusted Relaying Party) to Azure AD:
   a. Open the [*Enterprise applications*] section → [*All Applications*].
   b. Click [*New application*].
   c. Select “Creatio” in the [*Add from the gallery*] section and add the application. Learn more in the Microsoft documentation: Add Creatio from the gallery.
2. Open the [*Single sign-on*] section and specify the following parameters:
   a. Select “SAML” in the [*Single Sign-on Mode*] parameter.
   b. Enter the full website name, for example, “https://site01.creatio.com/Demo_161215/,” in the [*Identifier*] parameter.
   c. Enter the full website name and “svc/SsoLogin” address, for example, “https://site01.creatio.com/Demo_161215/ServiceModel/AuthServiceModel/AuthService.service.svc/SsoLogin,” in the [*Reply URL*] parameter.
3. Save the following data to perform the setup in Creatio (Fig. 1):
   - Azure AD Identifier
   - Login URL
   - Logout URL

Fig. 1 Data required to perform the setup in Creatio



Note. By default, Azure AD passes the following fields to Creatio: [*Given name*], [*Surname*], [*Email address*], [*Name*]. The email address serves as the username.

Perform the setup in Creatio

Follow these steps to set up single sign-on in Creatio:

1. Click the ⚙ button to open the **System Designer**.

2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “Azure AD.” This opens the setup page.
5. Fill out the following parameters:

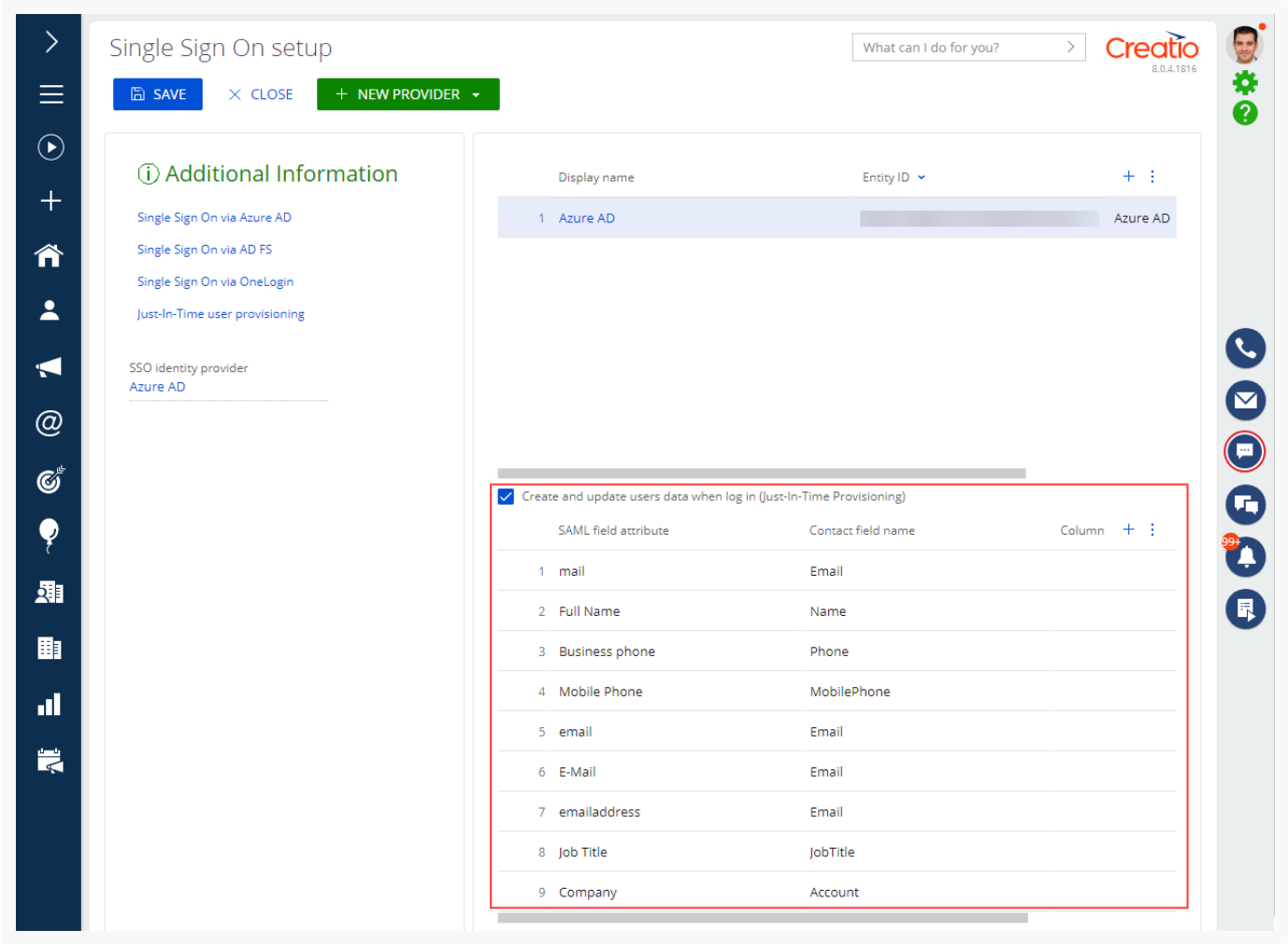
   a. Enter the unique identifier you got while setting up Azure AD in the [*Azure AD identifier*] parameter.

   b. Enter the URL of the identity provider’s single sign-on in the [*SingleSignOnServiceUrl*] parameter. For Azure AD, this is usually https://login.microsoftonline.com//saml2. Find out the settings of the added connector in the Azure account.

   c. Enter the URL of the identity provider’s single sign-off in the [*SingleLogoutServiceUrl*] parameter. For Azure AD, this is usually https://logout.microsoftonline.com//saml2. Find out the settings of the added connector in the Azure account.

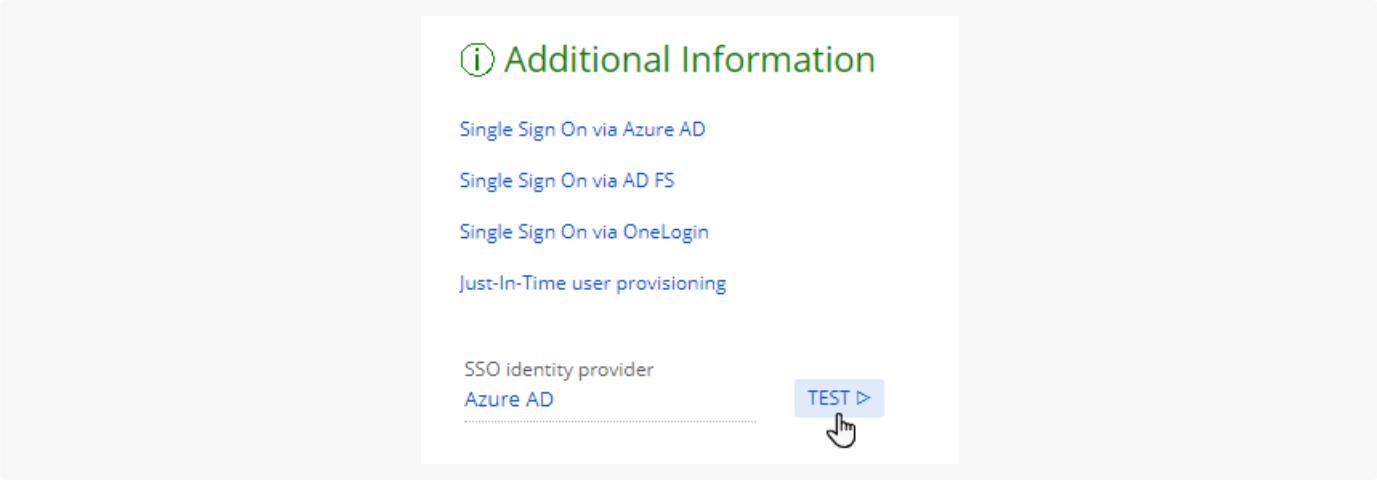
6. Fill out the provider's name to display on the Creatio login page in the [*Display name*] field.
7. Turn on Just-In-Time Provisioning (optional). This mechanism automatically creates the corresponding Creatio user account with proper data from the identity provider, such as user group, employee name, contact information, etc. To do this, select the [*Create and update users data when log in (Just-In-Time Provisioning)*] checkbox and map the fields.

Fig. 2 Set up Just-In-Time Provisioning



8. Select your provider in the [*SSO identity provider*] field and save the changes.
9. Click [*Test*] to test whether the provider is working correctly (optional).

Fig. 3 Test the provider



Single Sign-On via Okta

PRODUCTS: ALL CREATIO PRODUCTS

This article is relevant to Creatio version 8.0.3 and later.

You can integrate Creatio with Okta to manage single sign-on for all Creatio users that work in the corporate network.

Attention. The example uses the https://site01.creatio.com/Demo_161215/ Creatio URL. Replace this URL with the corresponding URL of your website when you perform the actual setup.

In general, the following **steps** are required to set up Single Sign-On in Creatio:

1. Download the file that contains the integration metadata. Read more >>>
2. Perform the setup in Okta. Read more >>>
3. Perform the setup in Creatio. Read more >>>

Download the metadata

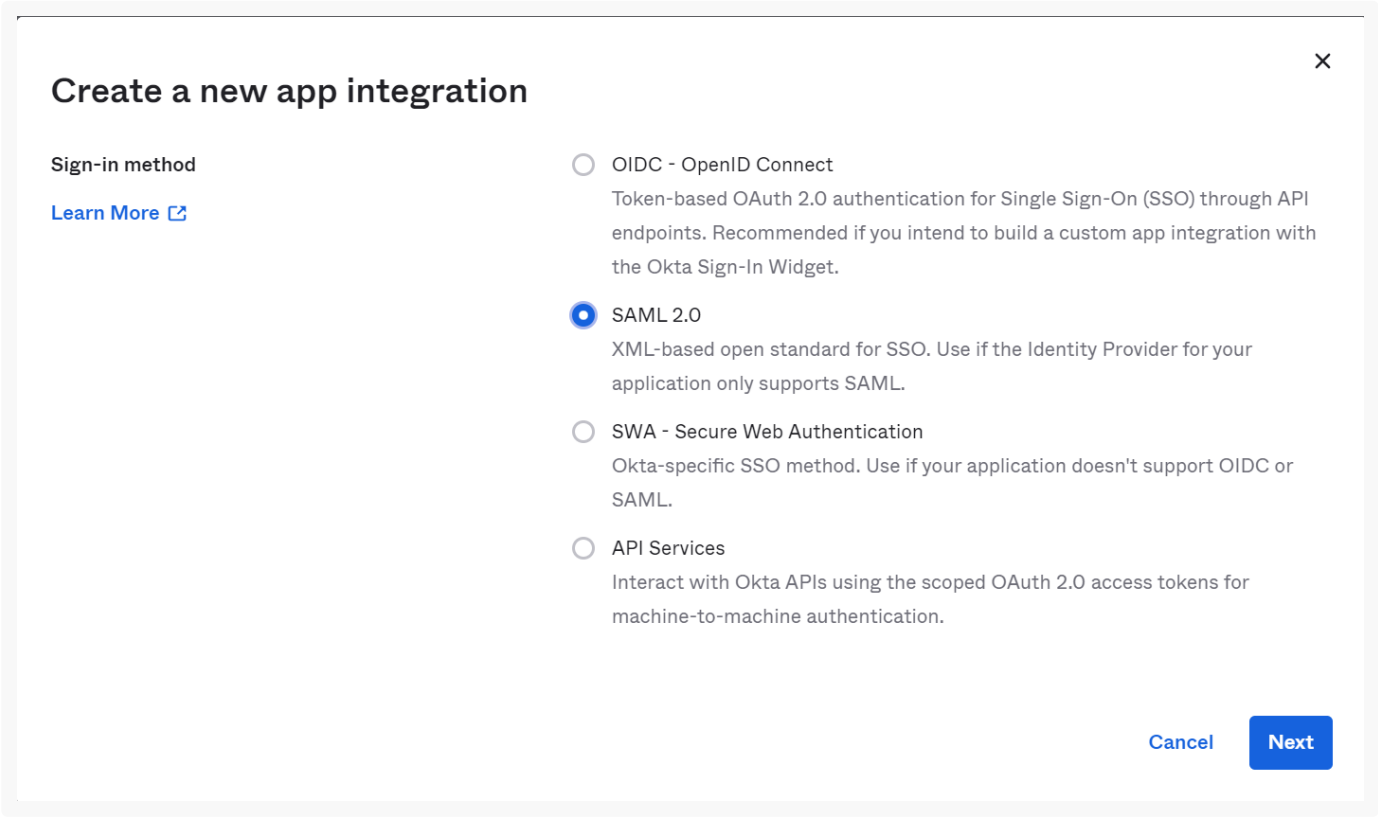
1. Click the ⚙ button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “Okta.” This opens the setup page.

5. Click [*Get metadata*].
6. Save the file to your local machine.

Perform the setup in Okta

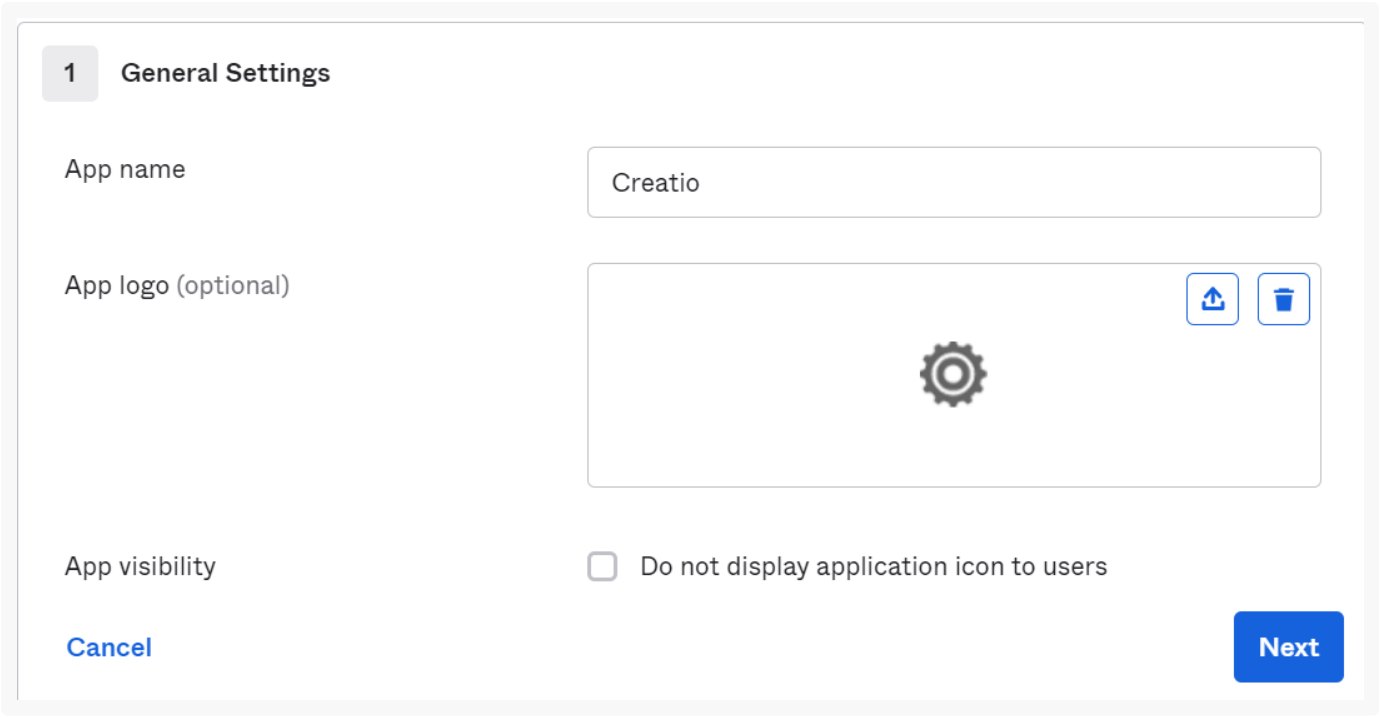
1. Add a new SAML 2.0 app.

Fig. 1 New SAML 2.0 app



2. Fill out the general parameters: app name, logo, and description. These parameters will be displayed to all users. Click [*Next*].

Fig. 2 The general parameters



3. Fill out the SSO parameters:

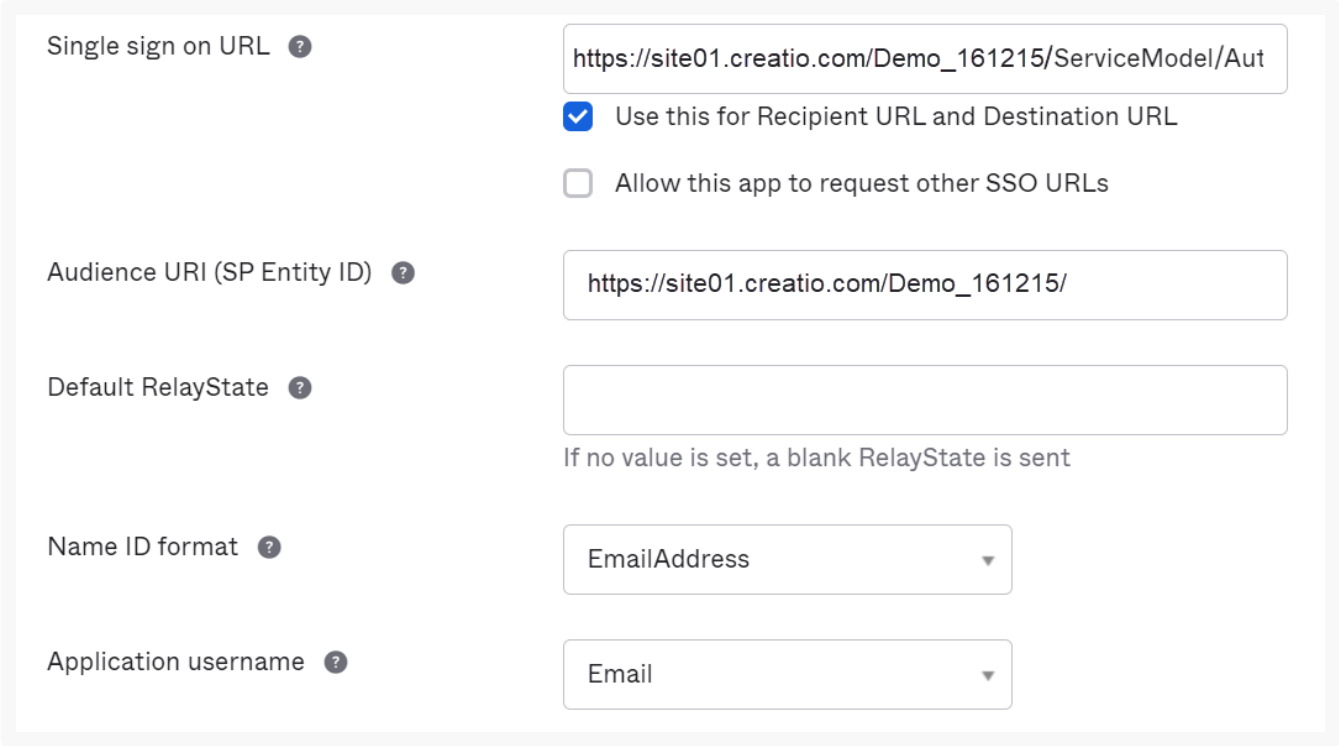
   a. Enter the URL of your Creatio website SSO in the [*Single sign on URL*] parameter. Use the following pattern: https:///ServiceModel/AuthService.svc/SsoLogin.

   b. Enter the URL of your Creatio website in the [*Audience URI (SP Entity ID)*] parameter. For example, https://site01.creatio.com/Demo_161215/.

   c. Select “EmailAddress” in the [*Name ID Format*] parameter. This specifies the data type required to log in to your website.

   d. Select “Email” in the [*Application username*] parameter. This specifies the parameter required for Just-In-Time Provisioning to work correctly.

Fig. 3 The SSO parameters



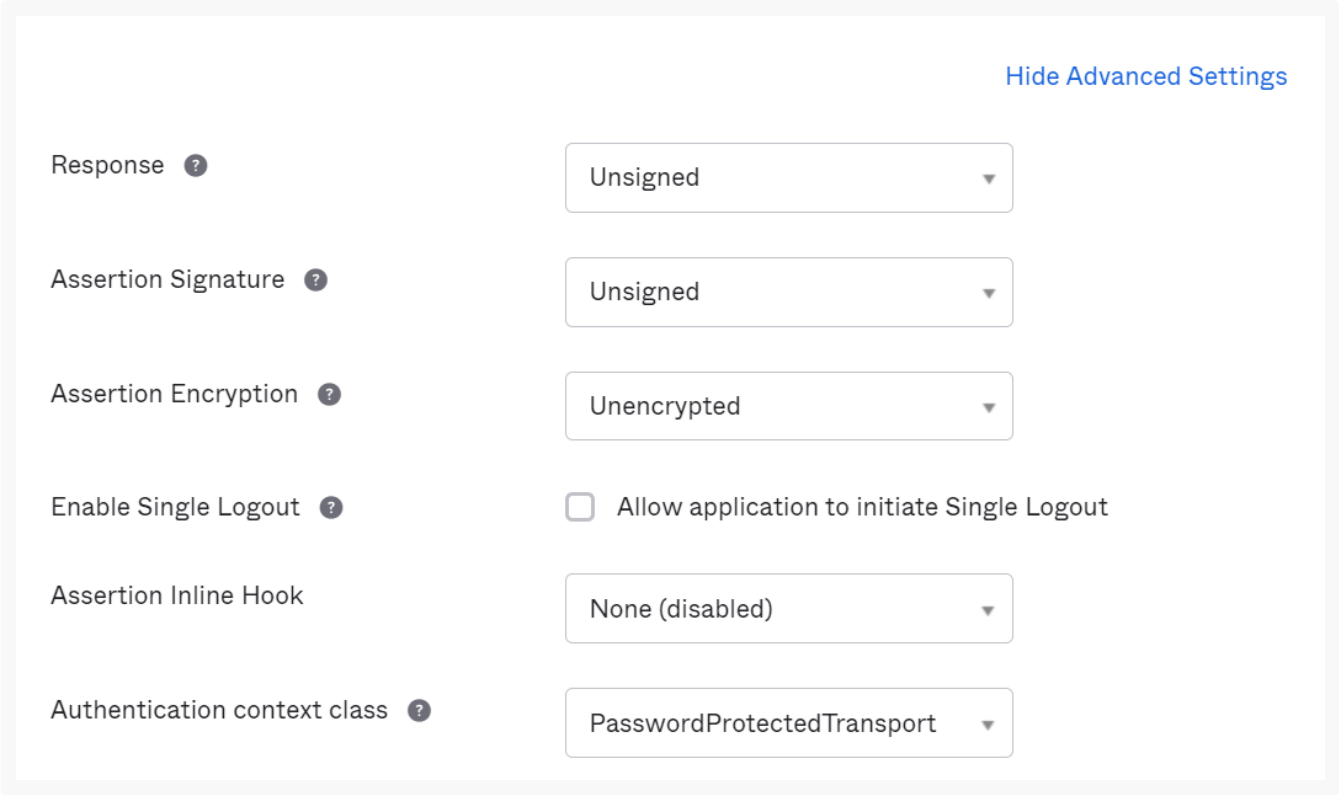
4. Fill out the advanced settings:

   a. Specify whether to sign queries for safe data transfer in the [*Response*] parameter. Select “Signed” for the production environment or “Unsigned” for the testing environment.

   b. Specify the security configuration type in the [*Assertion Signature*] parameter. Select “Signed” for the production environment or “Unsigned” for the testing environment.

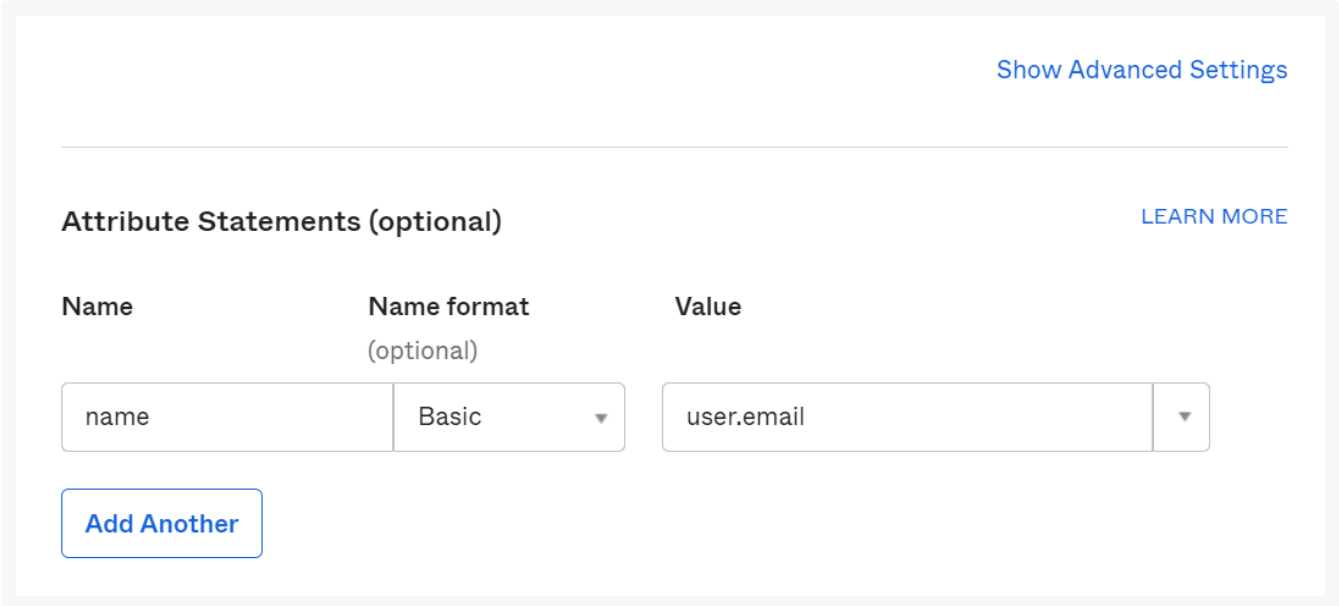
   c. Set [*Enable Single Logout*] to turn on single sign-out for your Creatio website.

Fig. 4 The advanced settings



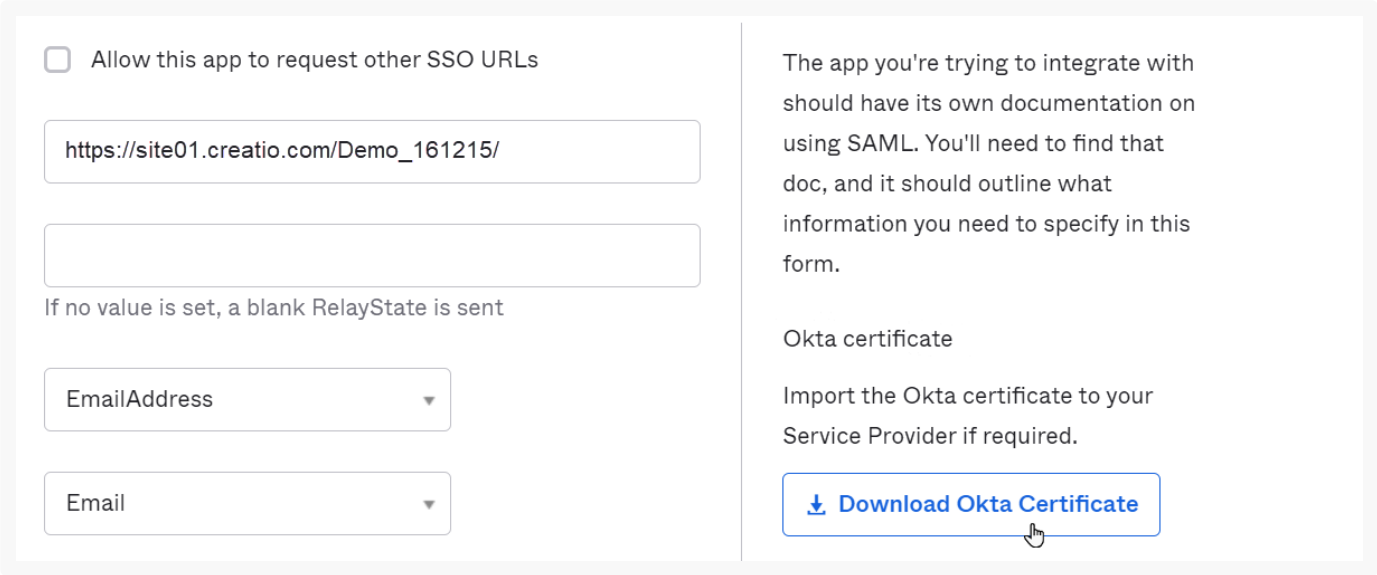
5. Map the following fields for JIT Provisioning:
   a. Map [*Name*] to “name.”
   b. Map [*Name format*] to “Basic.”
   c. Map [*Value*] to “user.email.”

Fig. 5 Mapping fields



6. Download the Okta Certificate if you are going to use Signed Response, Assertion Signature, and Single Logout.

Fig. 6 The Okta certificate download

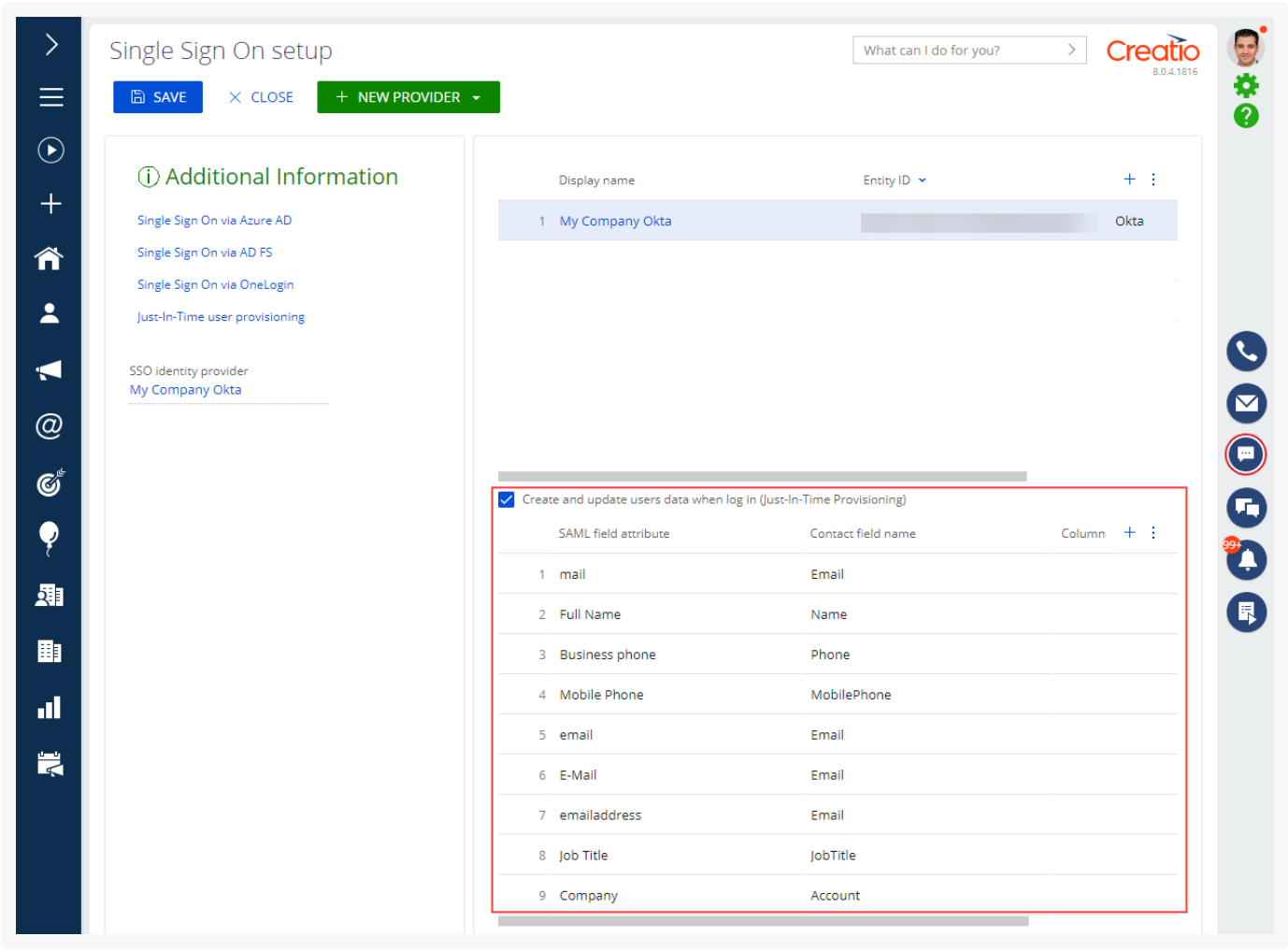


Perform the setup in Creatio

Follow these steps to set up single sign-on in Creatio:

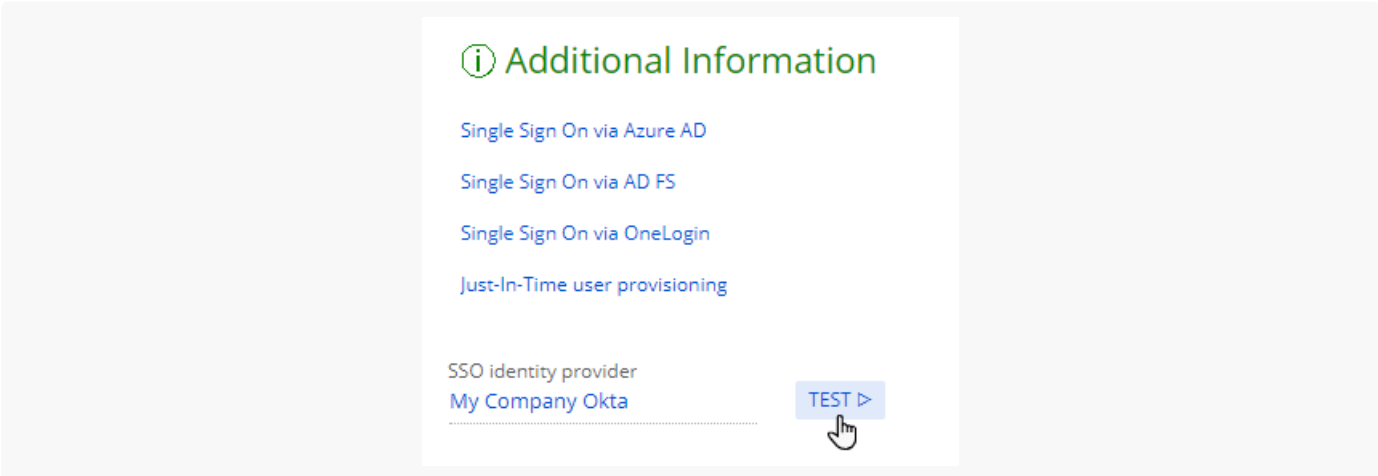
1. Click the button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “Azure AD.” This opens the setup page.
5. Fill out the following parameters:
   a. Enter the unique identifier you got while setting up Okta in the [*IdP Issuer*] parameter.
   b. Enter the URL of the identity provider’s single sign-on in the [*SingleSignOnServiceUrl*] parameter. For Okta, this is usually https://okta.com/qmBNBnkAkopZXwJpjpu5/sso/saml.
   c. Enter the URL of the identity provider’s single sign-off in the [*SingleLogoutServiceUrl*] parameter. For Okta, this is usually https://test-site.okta.com/app/test-site_creatio_1/qmBNBnkAkopZXwJpjpu5/sso/saml.
6. Fill out the provider's name to display on the Creatio login page in the [*Display name*] field.
7. Save the changes.
8. Turn on Just-In-Time Provisioning (optional). This mechanism automatically creates the corresponding Creatio user account with proper data from the identity provider, such as user group, employee name, contact information, etc. To do this, select the [*Create and update users data when log in (Just-In-Time Provisioning)*] checkbox and map the fields.

Fig. 7 Set up Just-In-Time Provisioning



9. Select your provider in the [*SSO identity provider*] field and save the changes.
10. Click [*Test*] to test whether the provider is working correctly (optional).

Fig. 8 Test the provider



Single Sign-On via a custom provider

PRODUCTS: ALL CREATIO PRODUCTS

Creatio can be integrated with any identity provider that supports the SAML 2.0 protocol. You can use OneLogin SSO portal as a single sign-on point for all your services, including Creatio. To do this, perform he setup both in OneLogin and Creatio.

Attention. The example uses https://site01.creatio.com/ Creatio URL and “appid” application id in OneLogin. Replace these values with your website URL and the id of the corresponding application in OneLogin when you perform the actual setup.

In general, the following **steps** are required to set up Single Sign-On in Creatio:

1. Download the file that contains the integration metadata. Read more >>>
2. Perform the setup in your provider. Read more >>>
3. Perform the setup in Creatio. Read more >>>

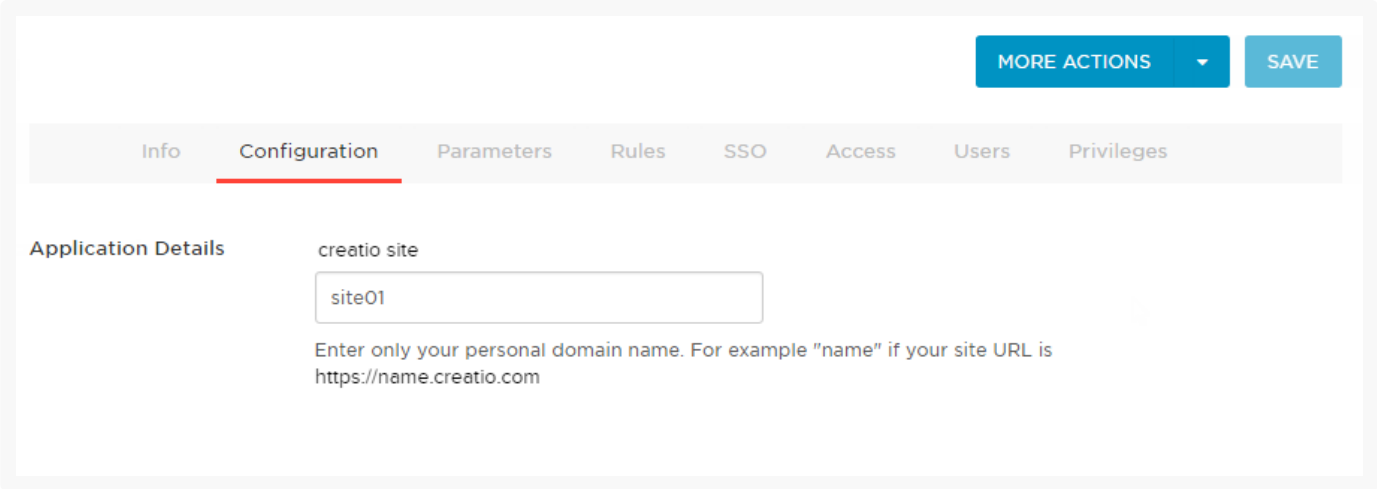
Download the metadata

1. Click the button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “Custom.” This opens the setup page.
5. Click [*Get metadata*].
6. Save the file to your local machine.

Perform the setup in OneLogin

1. Log in to OneLogin using an administrator account.
2. Click [*Apps*] and select [*Add Apps*]. Enter “Creatio” in the search bar and select the Creatio application.
3. If needed, change the value in the [*Display name*] field, modify the application icons, or clear the [*Visible in portal*] checkbox. These settings affect the way the website is displayed on the OneLogin website.
4. Click [*Save*].
5. Go to the [*Configuration*] tab and enter your website domain name in the [*Creatio site*] field (Fig. 1). For example, “site01.”

Fig. 1 Website configuration page

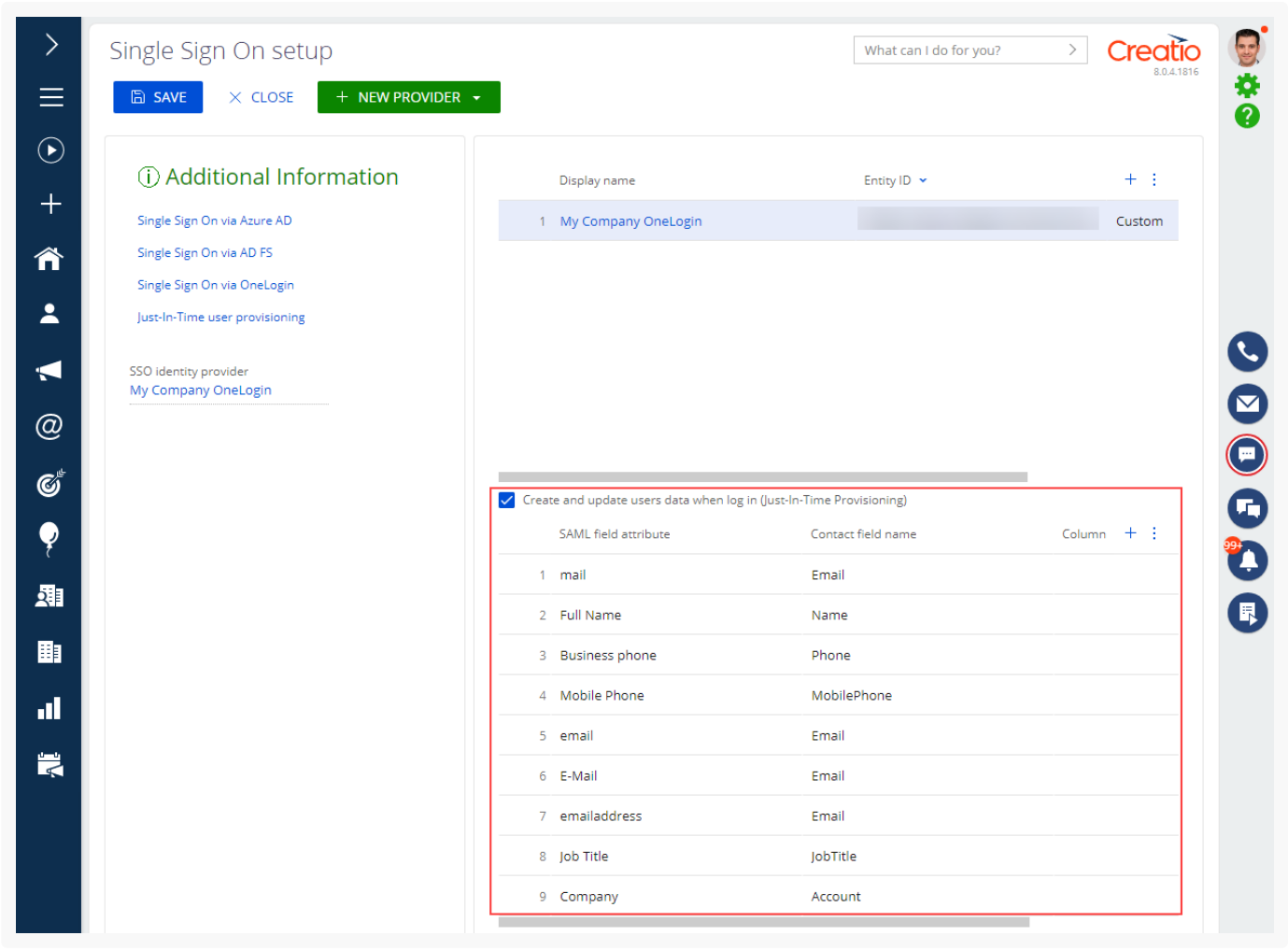


Perform the setup in Creatio

Follow these steps to set up single sign-on in Creatio:

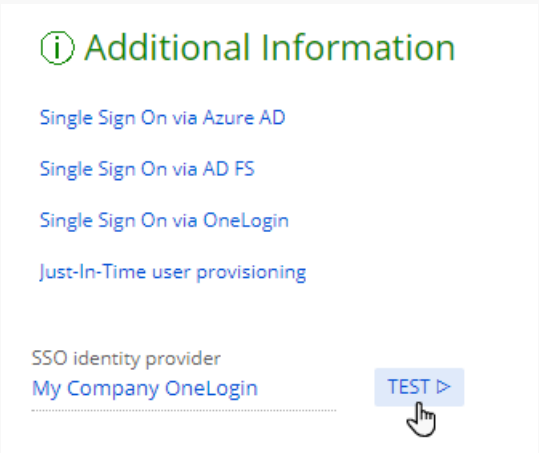
1. Click the button to open the **System Designer**.
2. Click [*Single Sign On configuration*].
3. Click [*New provider*]. This opens a drop-down menu.
4. Select “Azure AD.” This opens the setup page.
5. Fill out the following parameters:
   a. Enter your provider’s website in the [*Entity ID*] parameter. For example, httpsw://app.onelogin.com/saml/metadata/appid for OneLogin.
   b. Enter the URL of the identity provider’s single sign-on in the [*Single Sign On URL*] parameter. You can retrieve the URL from the SAML 2.0 Endpoint (HTTP) on the trusted application page.
   c. Enter the URL of the identity provider’s single sign-off in the [*Single Logout URL*] parameter. You can retrieve the URL from the SLO Endpoint (HTTP) on the trusted application page.
6. Fill out the provider's name to display on the Creatio login page in the [*Display name*] field.
7. Save the changes.
8. Turn on Just-In-Time Provisioning (optional). This mechanism automatically creates the corresponding Creatio user account with proper data from the identity provider, such as user group, employee name, contact information, etc. To do this, select the [*Create and update users data when log in (Just-In-Time Provisioning)*] checkbox and map the fields.

Fig. 2 Set up Just-In-Time Provisioning



9. Select your provider in the [*SSO identity provider*] field and save the changes.
10. Click [*Test*] to test whether the provider is working correctly (optional).

Fig. 3 Test the provider



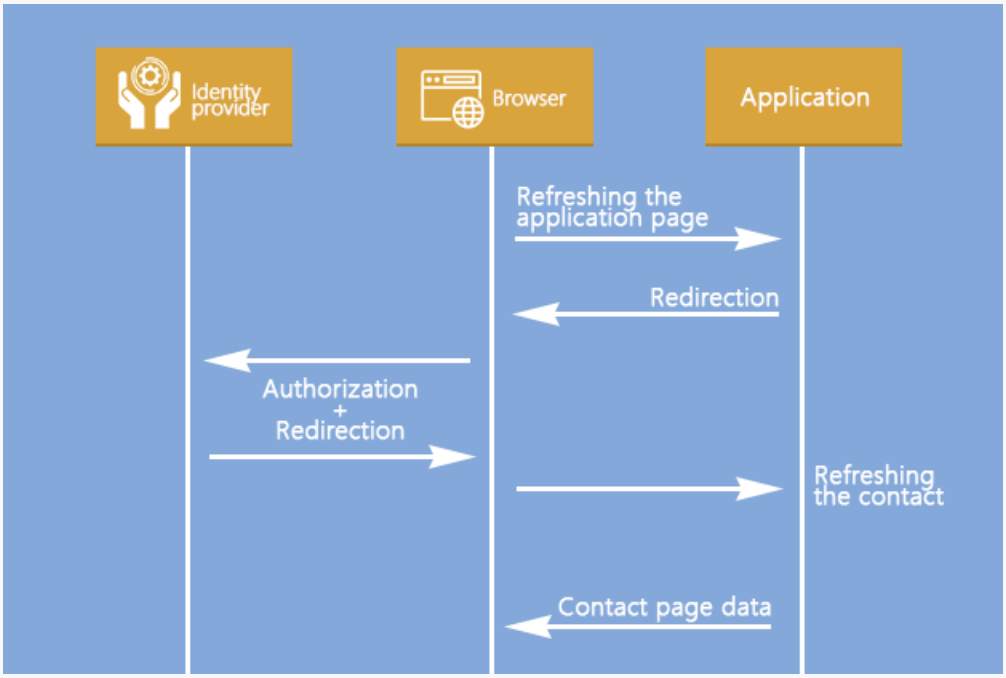
Just-In-Time User Provisioning

PRODUCTS: ALL CREATIO PRODUCTS

This article is relevant to Creatio version 8.0.2 and earlier. If you set up integration with Creatio version 8.0.3 and later follow the instructions on single sign-on setup.

Use Just-In-Time User Provisioning (JIT UP) function to avoid creating accounts for each separate service and to keep user database up-to-date. JIT UP extends the Single Sign-On (SSO) technology and helps to reduce the number of operations for administrating accounts and personal data in contact records. Each time a user logs on using SSO, the data on the contact page are updated with the data obtained from the identity provider (Fig. 1). If a user has no account in the Creatio, it can be created when the user logs in for the first time.

Fig. 1 Update data via Just-in-Time User Provisioning



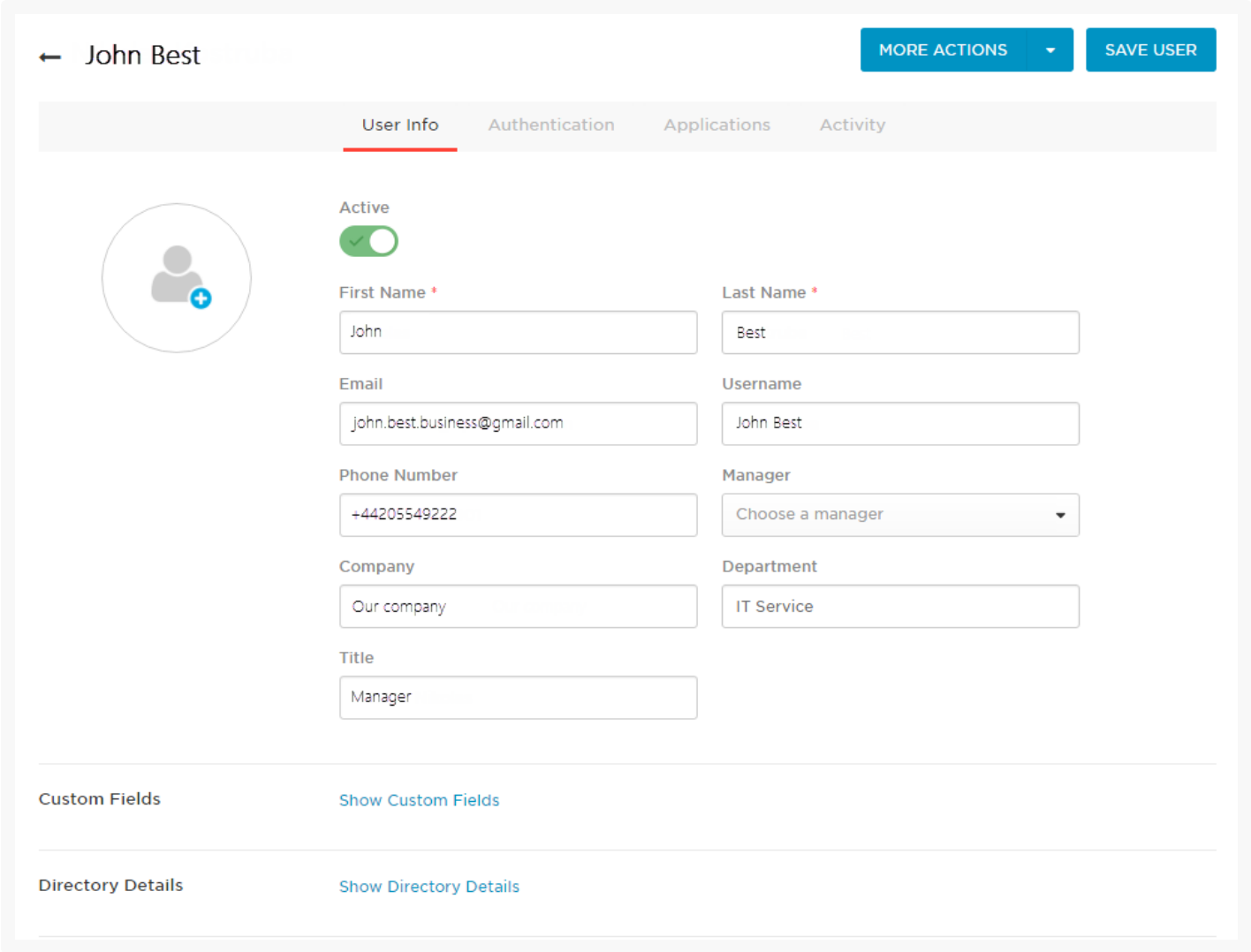
Note. Updating a contact with data from an identity provider includes updating the data on the record page and contact's connections to user groups.

You can enable JIT UP when setting up the identity provider integration. Read more: Single Sign-On via ADFS, Single Sign-On via OneLogin.

To specify contact fields that should be populated with data from the identity provider, configure the mapping of the SAML Assertion fields with Creatio columns. This is done in the SAML Assertion of the identity provider and in the [*SAML field name converters to contact field name*] lookup.

To set up mapping, you will need a configured account in the identity provider (Fig. 2) with the data required for Creatio.

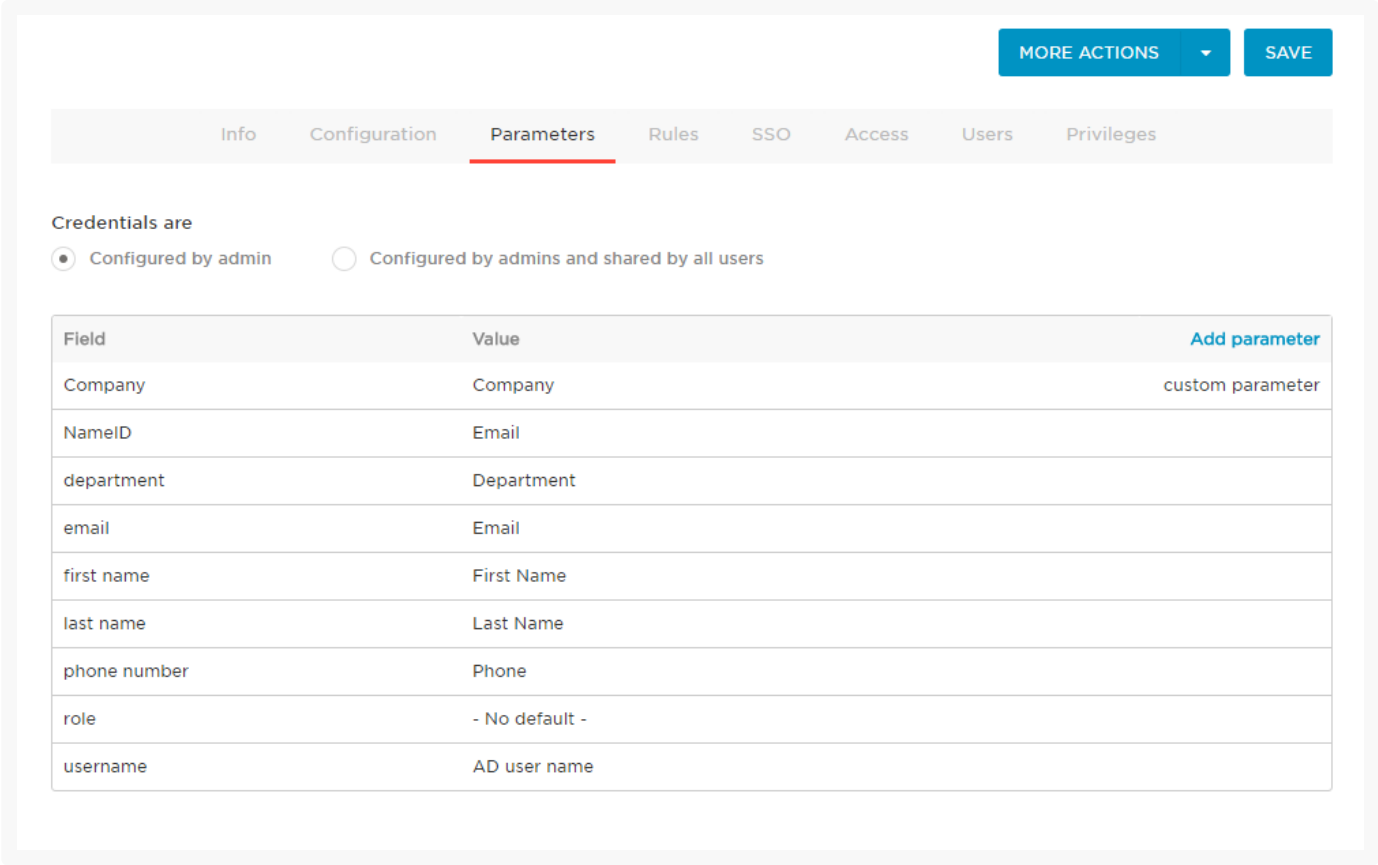
Fig. 2 Account fields in the OneLogin identity provider



To set up field population parameters:

1. Ensure that all required field values are transferred to Creatio. For example, to fill the profile of John Best with data from the [*Company*], [*Department*], [*Email*], [*First Name*], [*Last Name*], and [*Phone*] fields (Fig. 3).

Fig. 3 Application parameters in the OneLogin identity provider

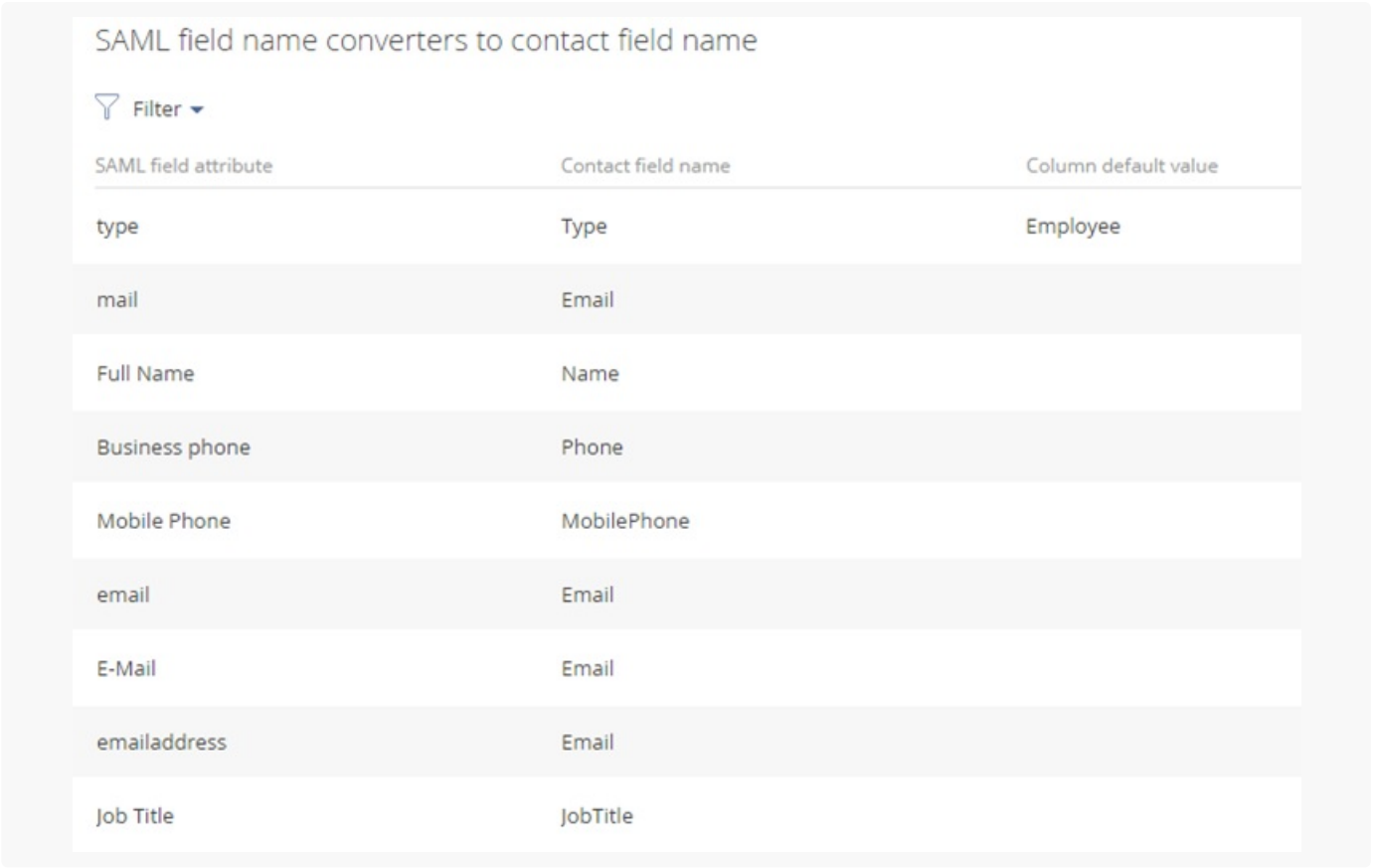


Note. Use the SAML Decoder Google Chrome extension to verify the parameters.

2. Verify that correct rules to receive values and update the columns for each required field are specified on the Creatio side. Rules are configured in the [*SAML field name converters to contact field name*] lookup. Specify a column in the Creatio for each field received from the identity provider. For example, to fill the [*Department*], [*Account*], [*Phone*], [*Email*], [*Given name*], and [*Surname*] columns in Creatio, specify them next to the corresponding SAML attributes (Fig. 4).

Note. Specify column names in the Creatio database as contact columns.

Fig. 4 The [*SAML field name converters to contact field name*] lookup configuration



3. A field that is missing in the identity provider data can be populated with the value specified in the [*Column default value*] field of the [*SAML field name converters to contact field name*] lookup. For example, the OneLogin identity provider does not contain the [*Type*] field and does not pass it when the user logs on. To populate this field in Creatio, create a rule in the lookup and specify the “Employee” value as default (Fig. 4). In this case, all created contacts will have the “Employee” value in the [*Type*] field.
4. You can add custom parameters to the OneLogin identity provider and specify macros for them. Learn more about how to work with macros in OneLogin documentation.

Windows authentication

PRODUCTS: ALL CREATIO PRODUCTS

Windows (NTLM) authentication can be used concurrently with LDAP authentication. Windows authentication requires entering login credentials in the browser. During LDAP authentication, user’s password is checked on the Active Directory server. Both Windows (NTLM) and LDAP authentications trigger when the user clicks the “Log in as domain user” link (provided that the user account is synchronized with LDAP).

Note. Windows authentication is only available for Creatio on-site due to cloud architecture specifics.

If the user attempts to log in to the system using the domain credentials, the following authentication algorithm is performed:

1. A user authentication check within the domain is performed.

2. If the domain username and the password are stored in a cookie, they will be retrieved from this cookie. Otherwise, a browser window will be displayed to enter the user credential.

   Further steps depend on the user synchronization with the LDAP directory.

1. If the user is not synchronized with LDAP:

   - User authentication check is performed through the comparison of the username and the password from the cookie and the corresponding credentials of the Creatio account. Thus, it is required to specify the same username and password that are used in the domain to enable Windows authentication for the users who are not synchronized with LDAP.
   - Based on the check results, if the data matches and the user account is licensed, the user authorization will be performed.
   - If the user is synchronized with LDAP:
   - The browser sends a request to the Active Directory service to authenticate the user.
   - The query returns the credentials of the current domain user that are compared with the username and the password details stored in the cookie.
   - If the data matches and the user account is licensed, the user authorization will be performed.

   > **Note.** User authentication is performed either for the users of the main application or for the self-service portal users. You can set the check order in the Web.config file of the loader application. Learn more: Set up the Web.config file of the loader application.

   To use Windows authentication via the NTLM protocol, first add system users (manually or by importing from LDAP) and license them. Users will need to allow writing local data to cookie files in their browsers to be able to store the data locally.

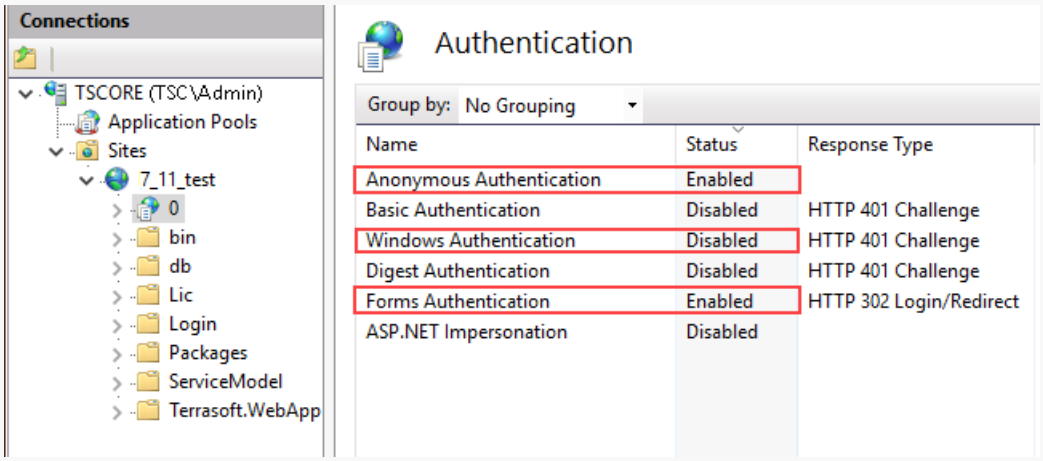
The authentication setup is performed on the application server and consists of two steps:

- IIS server setup that activates authentication using the NTLM protocol. Learn more: Set up the Windows authentication on IIS.
- Web.config file setup of the loader application that defines authentication providers and users availability check order among those registered in Creatio. Learn more: Set up the Web.config file of the loader application.

Set up the Windows authentication on IIS

1. Enable anonymous authentication and form authentication for both the web application and loader application (Fig. 1).

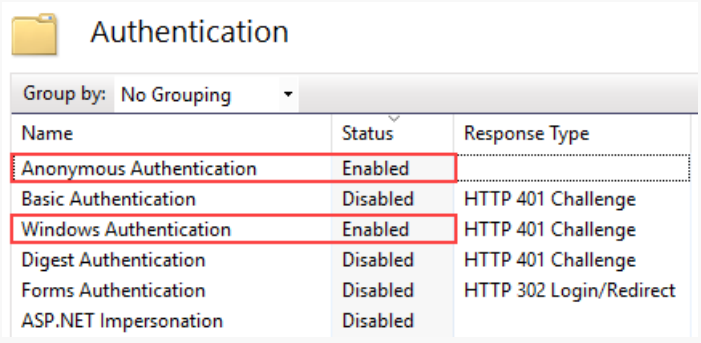
Fig. 1 Authentication settings for the loader application in IIS



Note. Make sure you disable the “Windows Authentication” setting that is enabled in IIS by default.

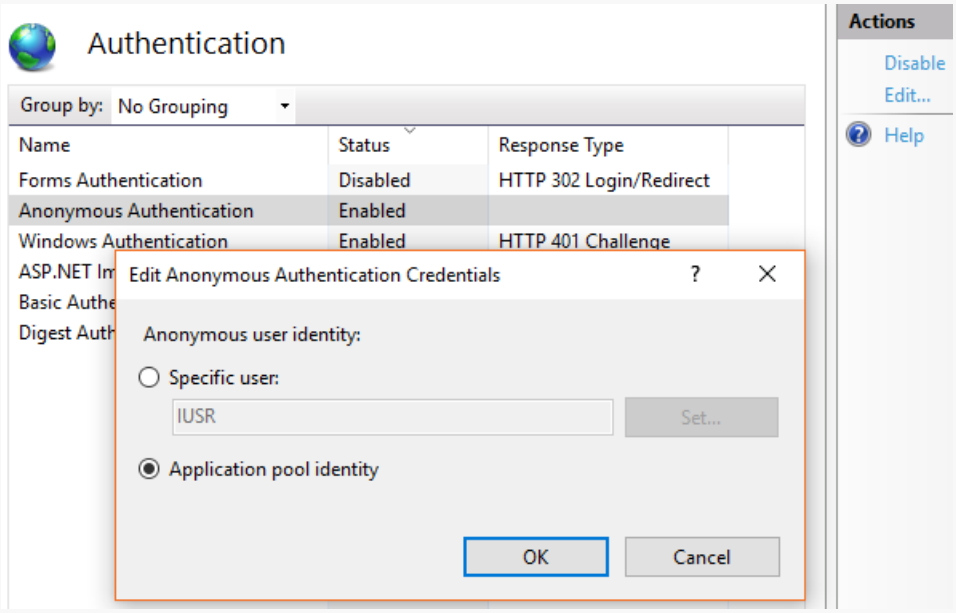
2. Disable the form authentication; enable anonymous authentication and Windows authentication for the “Login” directory within the loader application (Fig. 2).

Fig. 2 The login directory settings



Please note that anonymous authentication of the loader application and working applications must be conducted under application pool identity. To enable this, edit anonymous authentication credentials by clicking the [*Edit*] button in the [*Actions*] area of the IIS manager and select [*Application pool identity*] (Fig. 3).

Fig. 3 Enter the credentials for anonymous authentication in IIS



Note. Learn more about Windows Authentication in Microsoft documentation.

Set up the Web.config file of the loader application

1. Open the Web.config file of the loader application to be edited.
2. In this file, specify the Windows Authentication providers:

```
auth providerNames="InternalUserPassword,SSPLdapProvider,Ldap"
autoLoginProviderNames="NtlmUser,SSPNtlmUser"
```

[*InternalUserPassword*] – provider that is specified in the Web.config file by default. If you want to provide NTLM authentication only for the users who are not synchronized with LDAP, do not specify an additional value for the providerNames parameter.

[*Ldap*] – add this provider to the [*providerNames*] parameter values. As a result, the users who are synchronized with LDAP will be able to perform NTLM authentication.

[*SSPLdapProvider*] – add this parameter to the [*providerNames*] parameter value for the users of the self-service portal who are synchronized with LDAP to be able to perform NTLM authentication.

[*NtlmUser*] – add this provider to the [*autoLoginProviderNames*] parameter value. As a result, the users will able to perform NTLM authentication regardless of their synchronization with LDAP and the authentication type configured for these Creatio users.

[*SSPNtlmUser*] – add this parameter to the [*autoLoginProviderNames*] parameter value for the users of the self-service portal to be able to perform NTLM authentication regardless of their synchronization with LDAP and the authentication type configured for these Creatio users.

The record order of the [*autoLoginProviderNames*] parameter defines the order, in which Creatio checks if the system users are available in the list of application users (NtlmUser) or in the list of the self-service portal

users (SSPNtlmUser). For example, if you want the check to be performed among the main application users primarily, place the [*NtlmUser*] provider at the top of the list of the values of the [*autoLoginProviderNames*] parameter.

Attention. You can specify the [*SSPNtlmUser*] provider as an [*autoLoginProviderNames*] parameter value only if the [*NtlmUser*] provider is specified additionally. You can use the [*NtlmUser*] provider separately.

3. If you want to authenticate in Creatio at once, specify the “true” value for the [*UsePathThroughAuthentication*] parameter of the <appSettings> element:

```
<appSettings>
<add key="UsePathThroughAuthentication" value="true" />
...
</appSettings>
```

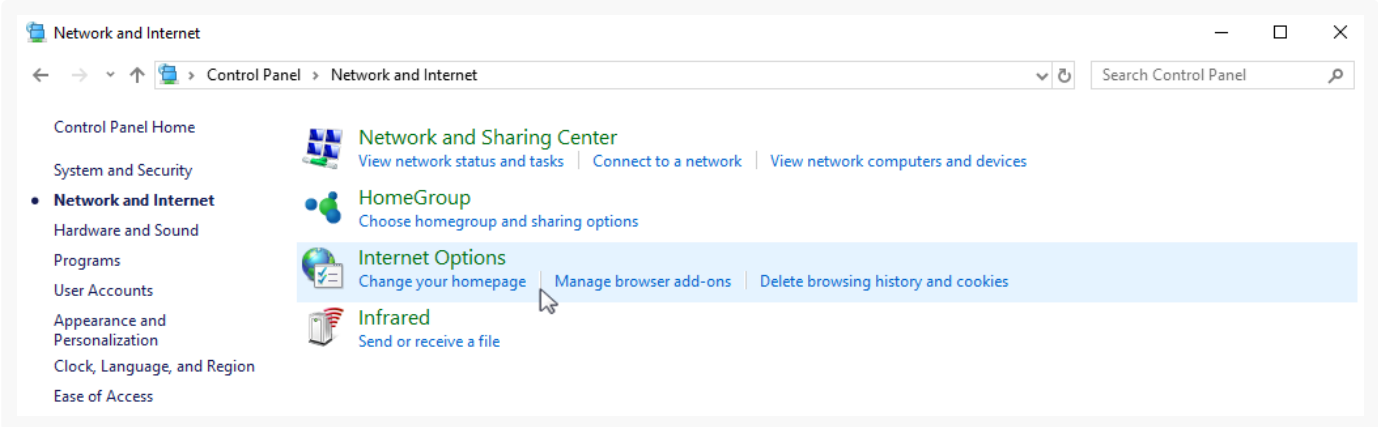
If you want the login page to be displayed with the available [*Log in as domain user*] link, specify the “false” value for the [*UsePathThroughAuthentication*] parameter. The end-to-end authentication will be performed only when accessing application main page. Add “/Login/NuiLogin.aspx” to Creatio website address.

As a result, users will be able to log in to Creatio as domain users. They may still be required to enter their credentials in a domain authentication window, which will pop up on login attempt.

To prevent displaying of the domain authentication window:

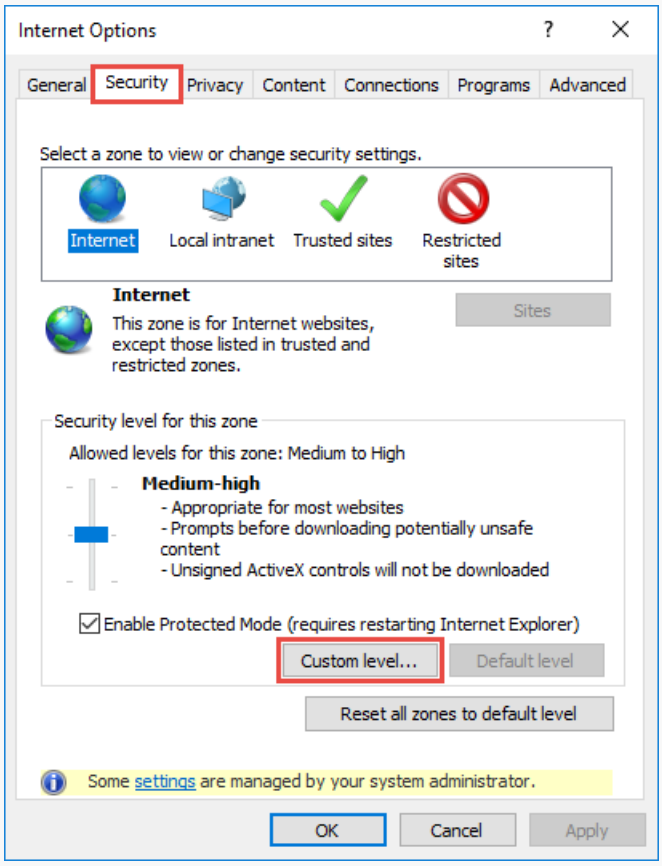
1. Click “Start” → “Settings” → “Control Panel” → “Network and Internet” menu and select “Internet options” (Fig. 4).

Fig. 4 Access the Internet options of the Windows Explorer



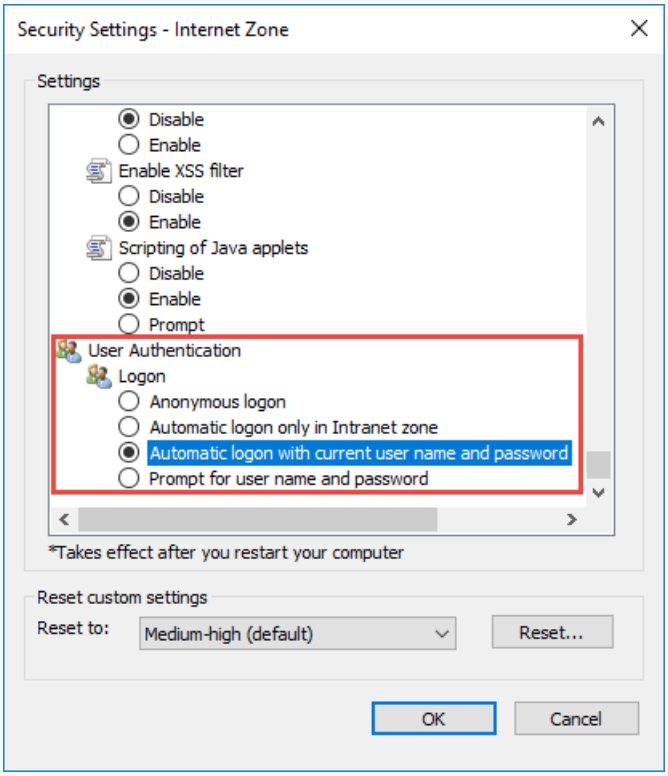
1. In the opened window, select the “Security” tab and click the “Custom level” button to go to security settings (Fig. 5).

Fig. 5 The security settings



1. In the “User authentication” group of settings, select the “Automatic logon with current user name and password” authentication method (Fig. 6).

Fig. 6 Select the user authentication method



1. Click “OK.”

   As a result, the users who are already authenticated in the domain will be able to log in to Creatio by clicking the “Log in as domain user” link, and will not have to re-enter their domain credentials each time they access Creatio.