

Custom OpenID Connect applications

If you'd like to add applications that aren't in our catalog, you can add a custom application and specify the details specific to your desired application.

For web applications that aren't in the Application Catalog and that use OpenID Connect authentication, use the custom OpenID Connect application template. For this type of application, you need to configure some settings in Admin Portal and also in the application itself.

If this is the first application you are configuring for SSO through Centrify, read the following topics before you get started:

- Introduction to application management
- [Configuring Single Sign-On \(SSO\)](#)

Protocol support details

The Centrify OpenID Connect custom application template supports the following OpenID Connect flows for obtaining ID Tokens (the type of flow is determined in the application):

- Authorization code flow
Used for web applications that can maintain a client secret with the authorization server. The user is authenticated with the Centrify Identity Service before the application receives the ID Token.
- Implicit flow
Used for web applications that cannot maintain the client secret with the authorization server. The application receives the ID Token without passing user authentication information (user authentication information is sent but the authorization code is not). ID Tokens are included in the web redirection.
- Hybrid flow
The Hybrid flow is a combination of the Authorization flow and Implicit flow. It is used for web applications that can maintain a client secret with the authorization server but it is not required. The application receives the ID Token and can optionally pass user authentication information.

For more information, see the OpenID specification:

http://openid.net/specs/openid-connect-basic-1_0.html#Introduction

• • • • •

Scope support

Scopes are supported and can be used to group attributes or even an entire claims category. Scopes supported include: `openid`, `profile`, `email`, `address`, and `phone`.

Note For more information on using scopes, see the OpenID specification:

http://openid.net/specs/openid-connect-basic-1_0.html#Scopes

How SSO with OpenID Connect works

The following table describes the authorization code flow, implicit flow, and the hybrid flow available for OpenID Connect applications that use the Centrify OpenID Connect custom application template. OpenID Connect is an identity layer on top of the OAuth 2.0 protocol. Application users are authenticated by the Centrify Identity Service that provides an ID Token as part of the assertion validating the identity of a particular user.

Step	OpenID Connect authentication step (Authorization code flow)	OpenID Connect authentication step (Implicit flow)	OpenID Connect authentication step (Hybrid flow)
1	User accesses an application.	User accesses an application.	User accesses an application.
2	The application/relaying party (RP) prepares an authentication request containing the desired request parameters and sends it to the Centrify Identity Service. The response_type requested is code.	The application/relaying party (RP) prepares an authentication request containing the desired request parameters and sends it to the Centrify Identity Service. The response_type requested is id_token or id_token token.	The application/relaying party (RP) prepares an authentication request containing the desired request parameters and sends it to the Centrify Identity Service. The response_type requested is code id_token, code token, or code id_token token.
3	The Centrify Identity Service verifies the user's identity in Active Directory or other user stores, and authenticates the user.	The Centrify Identity Service verifies the user's identity in Active Directory or other user stores, and authenticates the user.	The Centrify Identity Service verifies the user's identity in Active Directory or other user stores, and authenticates the user.
4	The Centrify Identity Service sends the user back to the application with an authorization code.	The Centrify Identity Service sends the user back to the application with an ID Token (id_token or id_token token) and an Access Token (token).	The Centrify Identity Service sends the user back to the application with an authorization code (code id_token, code token, or code id_token token) and an Access Token (token).
5	The application sends the code to the Token Endpoint to receive an Access Token and ID Token in the response.	The application uses the ID Token to authorize the user. At this point the application/RP can access the userInfo endpoint for claims.	The application sends the code to the Token Endpoint to receive an Access Token and ID Token in the response.
6	The application uses the ID Token to authorize the user. At this point the application/RP can access the userInfo endpoint for claims.		The application uses the ID Token to authorize the user. At this point the application/RP can access the userInfo endpoint for claims.

Note The prompt parameter with a value of login or none is supported. For example: `OIDCAuthRequestParams prompt=none` or `OIDCAuthRequestParams prompt=login`

See the http://openid.net/specs/openid-connect-core-1_0.html for details.

Preparing for configuration

OpenID Connect application configuration overview

The following overview covers the steps required in order to configure an OpenID Connect application to use the Centrify Identity Platform for authentication.

To deploy a OpenID Connect application with single sign-on (an overview):

- 1 To prepare for configuration, make sure that you have configuration settings handy from your existing OpenID Connect application deployment (see Obtaining application configuration information).
- 2 In Admin Portal, add the Custom OpenID Connect application and enter the information used in your OpenID Connect application.
- 3 Complete application configuration in Admin Portal, such as User Access, Policy, Account Mapping, and so forth (see Configuring Single Sign-On (SSO) for more information).
- 4 Edit the Custom OpenID Connect advanced script in Admin Portal to set application user attributes. The Centrify Identity Platform passes these user attributes in the ID Token.

Obtaining application configuration information

Before you configure the connection between your existing OpenID Connect application and the Centrify Identity Platform, obtain the following application information:

- **Resource Application URL:** You will need to enter the Resource Application URL into the application settings in Admin Portal.
- **Authorized Redirect URIs:** You will need to enter the Authorized Redirect URIs into the application settings in Admin Portal.

Note OpenID Connect does not directly support SP-initiated SSO. However, if the URI provided detects that the user is not authenticated and redirects to the Centrify Identity Service, and the user is already authenticated in the Centrify Identity Service, the user is then authenticated and redirected back to the application. The result is the user is authenticated after clicking on the application icon with a redirect to the Centrify Identity Service.

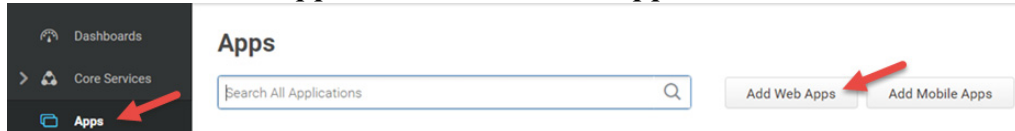
- **Client Secret:** You need to enter this information into the application settings in Admin Portal. This is the shared secret established between the Centrify Identity Service and the application.

Adding and configuring the custom OpenID Connect application

This section covers how to add the custom OpenID Connect application to Admin Portal and configure initial settings. For information about changing the Advanced script, see [Customizing the OpenID Connect Advanced script](#).

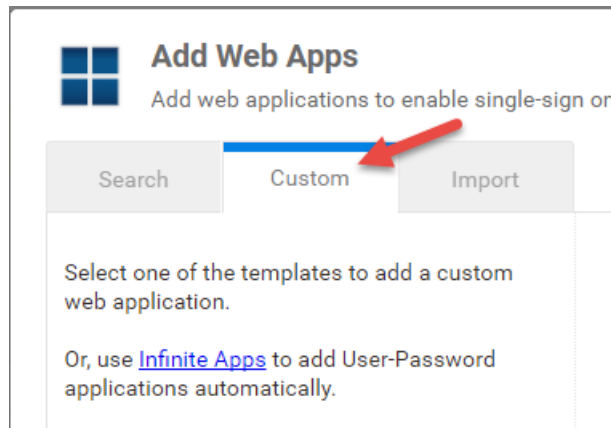
To add and configure a generic OpenID Connect application:

- 1 In Admin Portal, click **Apps**, then click **Add Web Apps**.



The Add Web Apps screen appears.

- 2 Click **Custom**.



- 3 On the Custom tab, next to the **OpenID Connect** application, click **Add**.

- 4 In the Add Web App screen, click **Yes** to add the application.

Admin Portal adds the application.

- 5 Click **Close** to exit the Application Catalog.

The application that you just added opens to the Application Settings page.

- 6 Configure fields in the Application Settings page.

For the following, copy the content from the application website to Admin Portal > Application Settings.

Option	Description
Resource application URL	Enter the URL of your OpenID Connect application.
Authorized Redirect URIs	Enter all desired redirect URIs registered with the Centrify Identity Service. At least one redirect URI is required.
Open ID Client Secret	Enter the Client Secret established between the Centrify Identity Service and application.

For the following, copy the content from the Admin Portal > Application Settings to the application website.

Option	Description
OpenID Connect Client ID	Copy the Client ID and paste it into the appropriate field on the application website.
OpenID Connect Metadata URL	Copy the metadata URL and paste it into the appropriate field on the application website.
OpenID Connect Issuer URL	A URL unique to this application profile. This value is the entity ID used in the assertion to identify the identity provider attempting to authenticate. The web application doesn't contact this URL so it doesn't need to be functional.

- 7 (Optional) On the **Application Settings** page, click **Enable Derived Credentials for this app on enrolled devices (opens in built-in browser)** to use derived credentials on enrolled mobile devices to authenticate with this application.


For more information, see [Derived Credentials](#).

- 8 On the **Description** page, change the name and description for the application.


Description [Learn more](#)

Application Name *

Application Description

Category * 

Logo (60 x 60 pixels recommended)



Because this is a generic or custom application, it's recommended to give this application a unique name. You can also provide a custom application logo.

The Category field specifies the default grouping for the application in the user portal. Users have the option to create a tag that overrides the default grouping in the user portal.

- 9 On the **User Access** page, select the role(s) that represent the users and groups that have access to the application.

When assigning an application to a role, select either **Automatic Install** or **Optional Install**:


- Select **Automatic Install** for applications that you want to appear automatically for users.
- If you select **Optional Install**, the application doesn't automatically appear in the user portal and users have the option to add the application.

10 (Optional) On the **Policy** page, specify additional authentication controls for this application.

Policy


[Learn more](#)

Application Challenge Rules

|  Drag rule to specify order. The highest priority is on top.

Condition	Authentication Profile
Nothing configured	

Default Profile (used if no conditions matched)

- Always Allowed - 

Use script to specify login authentication rules (configured rules are ignored)

- a Click **Add Rule**.
The Authentication Rule window displays.

- b Click **Add Filter** on the Authentication Rule window.
- c Define the filter and condition using the drop-down boxes.
For example, you can create a rule that requires a specific authentication method when users access the Centrify Identity Platform from an IP address that is outside of your corporate IP range. Supported filters are:

Filter	Description
IP Address	The authentication factor is the computer's IP address when the user logs in. This option requires that you have configured the IP address range in Settings, Network, Corporate IP Range.
Identity Cookie	The authentication factor is the cookie that is embedded in the current browser by the identity platform after the user has successfully logged in.
Day of Week	The authentication factor is the specific days of the week (Sunday through Saturday) when the user logs in.
Date	The authentication factor is a date before or after which the user logs in that triggers the specified authentication requirement.
Date Range	The authentication factor is a specific date range.
Time Range	The authentication factor is a specific time range in hours and minutes.
Device OS	The authentication factor is the device operating system.
Browser	The authentication factor is the browser used for opening the Centrify user portal.

Filter	Description
Country	The authentication factor is the country based on the IP address of the user computer.
Risk Level	<p>The authentication factor is the risk level of the user logging on to user portal. For example, a user attempting to log in to Centrify from an unfamiliar location can be prompted to enter a password and text message (SMS) confirmation code because the external firewall condition correlates with a medium risk level. This Risk Level filter, requires additional licenses. If you do not see this filter, contact Centrify support. The supported risk levels are:</p> <ul style="list-style-type: none"> • Non Detected -- No abnormal activities are detected. • Low -- Some aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. • Medium -- Many aspects of the requested identity activity are abnormal. Remediation action or simple warning notification can be raised depending on the policy setup. • High -- Strong indicators that the requested identity activity is anomaly and the user's identity has been compromised. Immediate remediation action, such as MFA, should be enforced. • Unknown -- Not enough user behavior activities (frequency of system use by the user and length of time user has been in the system) have been collected.
Managed Devices	The authentication factor is the designation of the device as "managed" or not. A device is considered "managed" if it is managed by Centrify, or if it has a trusted certificate authority (CA has been uploaded to tenant).

For the Day/Date/Time related conditions, you can choose between the user's local time and Universal Time Coordinated (UTC) time.

- d Click the **Add** button associated with the filter and condition.
- e Select the profile you want applied if all filters/conditions are met in the **Authentication Profile** drop-down.
The authentication profile is where you define the authentication methods. If you have not created the necessary authentication profile, select the **Add New Profile** option. See [Creating authentication profiles](#).
- f Click **OK**.
- g (Optional) In the **Default Profile (used if no conditions matched)** drop-down, you can select a default profile to be applied if a user does not match any of the configured conditions.
If you have no authentication rules configured and you select **Not Allowed** in the **Default Profile** dropdown, users will not be able to log in to the service.
- h Click **Save**.
If you have more than one authentication rule, you can prioritize them on the **Policy** page. You can also include JavaScript code to identify specific circumstances when you want to block an application or you want to require

additional authentication methods. For details, see Application access policies with JavaScript.

Note If you left the Apps section of Admin Portal to specify additional authentication control, you will need to return to the Apps section before continuing by clicking **Apps** at the top of the page in Admin Portal.

11 On the **Account Mapping** page, configure how the login information is mapped to the application's user accounts.

Account Mapping

[Learn more](#)

Map to User Accounts:

Use the following Directory Service field to supply the user name

Directory Service field name *

mail

Everybody shares a single user name

Use Account Mapping Script

The options are as follows:

- **Use the following Directory Service field to supply the user name:** Use this option if the user accounts are based on user attributes. For example, specify an Active Directory field such as *mail* or *userPrincipalName* or a similar field from the Centrify Directory.
- **Everybody shares a single user name:** Use this option if you want to share access to an account but not share the user name and password. For example, some people share an application developer account.
- **Use Account Mapping Script:** You can customize the user account mapping here by supplying a custom JavaScript script. For example, you could use the following line as a script:

```
LoginUser.Username = LoginUser.Get('mail')+'.ad';
```

The above script instructs the Centrify Identity Platform to set the login user name to the user's mail attribute value in Active Directory and add '.ad' to the end. So, if the

user's mail attribute value is Adele.Darwin@acme.com then the Centrify Identity Platform uses Adele.Darwin@acme.ad. For more information about writing a script to map user accounts, see the SAML application scripting.

- 12 (Optional) Click **App Gateway** to allow users to securely access this application outside of your corporate network. For detailed configuration instructions, see *Configuring an application to use the App Gateway*.

Note The App Gateway feature is a premium feature and is available only in the Centrify Identity Service App+ Edition. Please contact your Centrify representative to have the feature enabled for your account.

- 13 (Optional) On the **Changelog** page, you can see recent changes that have been made to the application settings, by date, user, and the type of change that was made.

- 14 (Optional) Click **Workflow** to set up a request and approval work flow for this application.

The Workflow feature is a premium feature and is available only in the Centrify Identity Service App+ Edition. See *Configuring Workflow* for more information.

- 15 Click **Save**.

Next, you're ready to edit the Advanced Script (see *Customizing the OpenID Connect Advanced script*).

Customizing the OpenID Connect Advanced script

For OpenID Connect applications, you must edit the Advanced script to specify which assertion user attribute and other settings go inside the ID Token.

Before you edit the script, be sure that you've already located the claims information that you need to specify in the script.

You must modify the script for it to work; it does not have the specific details required to work with your application until you edit the script.

Parameters that you can use when specifying values

You can use the following object attributes and parameters to generate the desired claims when specifying values in the script.

Parameter or Object attribute	Description
Application	This is the application object from the cloud storage. Use the GET method to get an application property. Example: <code>var url = Application.Get('URL');</code>
Issuer	Use this to refer to the same Issuer value that's specified in the Application Settings page. String value of the Issuer. This value is the same as <code>Application.Get('Issuer')</code> .
LoginUser	This is the login user object - the user that the Centrify Identity Platform and OpenID Connect application are authenticating for the user session.
LoginUser.Username	Use this to refer to the same user name that's specified in the Account Mapping page.
LoginUser.Get	Use this to get the user's attribute from the directory service. Example: <code>LoginUser.Get('mail');</code>
LoginUser.GroupNames	Use this to refer to the array of group names that the user is a direct member of.
LoginUser.EffectiveGroupNames	Use this to refer to the array of ALL group names that the user is a member of. This includes cases where the user is a member of a group that is a member of another group.
LoginUser.GroupDNs	Use this to refer to the array of group DN's that the user is a direct member of.
LoginUser.EffectiveGroupDNs	Use this to refer to the array of ALL group DN's that the user is a member of. This includes cases where the user is a member of a group that is a member of another group.

Required functions

There are functions that must be in the assertion. Some of these functions are automatically set from the values that you enter in the Application Settings page.

Function	Description
SetClaim()	Create a claim with name 'Name' and value 'Value' in the UserInfo response. Example: <code>SetClaim('Name', 'Value')</code>
setIssuer()	Sets the Issuer. By default, this is set to the Issuer parameter, which is the value specified in Application Settings page. Example: <code>setIssuer(Issuer);</code>

Optional functions

The Advanced script contains examples and explanations of functions that you can specify if necessary. Refer to the Advanced script for more information.

Editing the OpenID Connect Advanced Script

To edit the OpenID Connect Advanced script:

- 1 In Admin Portal, open your custom OpenID Connect application.
- 2 Click **Advanced**.
- 3 Edit the script as desired.

Note The editor provides color coding and error checking. For substantial edits, you may want to use a specialized JavaScript editor and paste your script in this page after you're done.

- 4 (Optional) Click **Test** and then specify a user in the Select User field.

The Advanced Script Results window opens showing ID Token details and the results of a trace of the script. The ID token is generated by the Admin Portal for the user to log in to the web application.

- 5 (Optional) Click **Reset Script** to set the script back to its default configuration. Any edits made to the script are lost.
- 6 Click **Save** to save your changes.