Single Sign-On with OAUTH2/ODIC

https://campus.barracuda.com/doc/96023985/

Notes

- These configurations can only be performed by Security Awareness Training administrators who have been granted the **Single Sign On - Can Manage All** or **Client User Manager – Can Manage All** privilege. For information on granting this privilege to one or more administrators, refer to User Management.
- These configurations affect users of Security Awareness Training, not end users who receive training and other content through Security Awareness Training campaigns.
- If you are configuring this with the intent to use it for RestAPI authentication, the identity provider must be configured to allow the **Resource Owner Password Grant (ROPG)**. Do this by allowing the **password** scope.

Important It is your responsibility to make sure that your identity provider will only authenticate and authorize users that should have accounts in the Security Awareness Training system.

As described in Single Sign-On, Single Sign-On (SSO) enables users to log into Security Awareness Training using your organization's common authentication service.

This optional SSO solution is implemented with the OAUTH2 specification.

Just In Time Provisioning

Some Security Awareness Training administrators prefer not to create all users manually. Just In Time (JIT) provisioning enables new users to log in without an account, then the system creates an account automatically.

Just In Time provisioning, described in the steps below, is not required for Single Sign-On functionality. However, if you want to use Just In Time provisioning, you must enable SSO.

Notes for Just In Time Provisioning

- If you change the default permissions, it will affect new users going forward, but will not retroactively change permissions of accounts already created through SSO. If you want to change permissions for a user account, you must go to System > User Manager, regardless of how the account was created.
- If you change the default permissions, it will affect new users going forward, but will not retroactively change permissions of accounts already created through SSO. If you want to change permissions for a user account, you must go to System > User Manager, regardless of how the account was created.

Important Information for Just In Time Provisioning

It is your responsibility to change the configuration for new users if you do not want new users to have administrative privileges.

By default, new administrative users are added as members of the following groups

- Campaign Administrative
- Everyone - All Users Must Be In This Group

If you want all new users to be able to manage administrative users, select the following, additional group:

- Client User Administrator - Can Manage All Client Users

Enabling Single Sign-On

To enable Single Sign-On:

1. Navigate to **System > Single Sign On (OAUTH2)**.
2. Click **New**.
3. Complete the information in this section. If you need help with any of the information, ask the system administrators in your organization.
    - **Identity Provider Name** – Enter a name to use as the label for the new SSO button on Barracuda Networks' Security Awareness Training login screen after you enable SSO. This name is not part of the SSO configuration itself.
    - **Discovery URI** – (Optional, but recommended) If the identity provider has a discovery endpoint enter it here. After you enter the URI, most of the other configuration options for SSO will be entered automatically. If you do not have a Discovery URI, you must enter information manually.
4. Click **Save**.
5. Enter the **Client ID** and **Client Secret** you received from the identity provider when you set up the Security Awareness application.
6. Enter the following values with information obtained from your identity provider. If you entered a valid **Discovery URI** in Step 3 above, these values are automatically entered for you.
    - **Authorization Endpoint**
    - **Token Endpoint**
    - **User Informational Endpoint** – Optional
    - **JWKS URI**
    - **Endpoint Authorization Method** – Not always provided as part of the discovery process, but must be set to a value supported by the identity provider.
    - **Endpoint Response Method** – Not always provided as part of the discovery process, but must be set to a value supported by the identity provider.
    - **Client Scopes** – Must include the **openid** and **email** scopes.

- **PKCE Enabled** – Enable OAUTH2 Proof Key for Code Exchange (PKCE). PKCE allows the embedded application to authenticate without the need for the OAUTH2 Client Secret.
- **Hidden** – If checked, the login button for this SSO configuration will be hidden from the login form. This is used primarily for SSO configurations that are intended for the RestAPI OAUTH2/ODIC authentication.

7. Click **Save**.
8. After you have enabled the Single Sign On (OAUTH2) configuration, the SSO button appears on the top of the Security Awareness Training login form.
9. Navigate to **System > User Manager** to change the **Authorization Type** for affected users to **Single Sign On (OAUTH2)**. For details, refer to User Management.

> **Important** To confirm this new configuration is functional, use a test user account. If your configuration has any errors and you test with your own account, you might become locked out of the system.