Single Sign-On with SAML2

https://campus.barracuda.com/doc/17065/

Notes

- These configurations can only be performed by Security Awareness Training administrators who have been granted the **Single Sign On - 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.

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 SAML2 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 (SAML2)**.
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.
   - **Configuration Name** – This name will be the label for the new button on the Security Awareness Training login screen when SSO is enabled, as shown above. It is not part of the SAML2 configuration itself.
   - **Configuration Description** – Optional description of the configuration record. It is not part of the SAML2 configuration itself.
   - **Enable JIT Provisioning** – Used only if you are also configuring Just In Time Provisioning.
4. Click **Save**.
5. The following steps describe the option of setting up Just In Time Provisioning. To bypass these steps, continue below with **Step 9**.
6. As mentioned in the note above, **by default, new users added through JIT provisioning are added as Administrators.** You can change their roles by changing their Security Group assignments.
   When the page refreshes, click **Security Group Configuration**.
7. On the **SAML Provisioning Group Manager** page, the **Campaign Administrator** and **Everyone - All Users Must Be In This Group** checkboxes are selected by default, giving all new users Administrative privileges. If you also want new users to be able to administer users, select the **Client User Administrator - Can Manage All** checkbox.
8. Click the **Return to the Single Sign On (SSO) SAML2** link in the top right of the page.
9. Select the **Active** checkbox to activate this configuration.
10. Select the **Force Identity Provider Login** checkbox to ensure the user always enters their user and password when they are redirected to the identity provider.
11. Select the **Debug** checkbox if instructed to do so by a Barracuda Networks representative.
12. The following three fields are populated automatically. You need these fields to configure authentication forwarding in your identity provider. Take note of the settings for the following

fields and enter them in your identity provider system. Contact your system administrator if you need assistance with this part of the configuration.

- **SP Entity ID**
  - This default can be modified to meet the requirements of your Identity Provider (IdP).
- **SP Assertion Consumer Service**
- **SP Single Logout Service**
- **Name ID Format**

13. In the **Identity Provider** section, enter information you obtain from your identity provider. Again, contact your system administrator if you need assistance with this part of the configuration.
    You need the following information:
    - **IdP Entity Id**
    - **IdP Single Sign On Service**
    - **IdP Single Logout Service**
    - **IdP X.509 Certificate**
14. Click **Save**.

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.