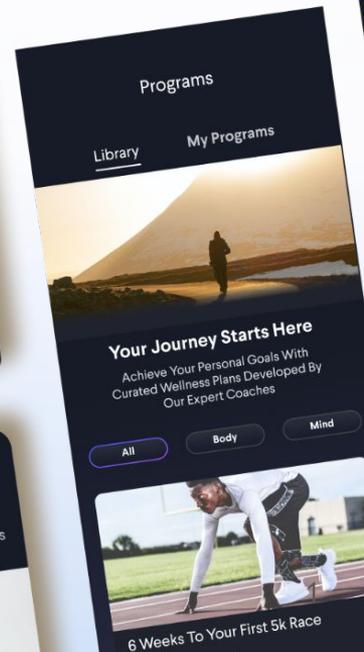
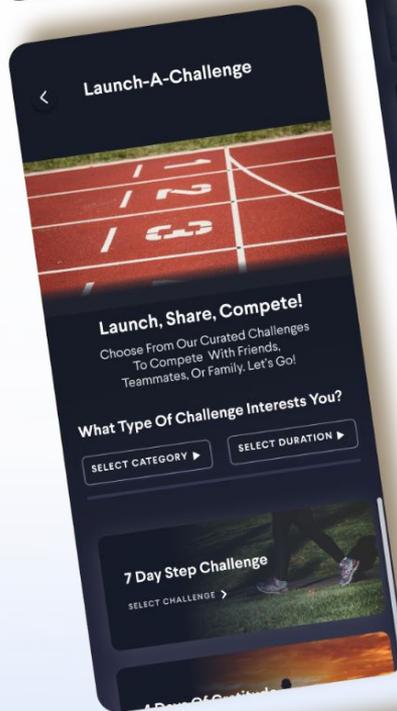




DUO

SSO Setup Guide



Wellness Coach supports Single Sign On (SSO) (DUO) to access the app with one set of login credentials

- **Single Sign On**

DUO Single Sign On (SSO) Solution provides easy and seamless access to Wellness Coach with one set of credentials, from any type of device or application whether they are in the cloud or on premise

- **Fraud Prevention**

DUO helps to prevent fraud with its dynamic risk engine in conjunction with enterprise specific security policy. It supports a combination of the Device ID, Location, and Time of access as multi-factor authentication that can help to detect and block fraud in real-time, without any interaction with the employee

- **Employee Access Management**

With SSO through DUO, employee access to Wellness Coach will be managed automatically. Any new hires will automatically get access to Wellness Coach on their date of hire and any terminated employees access will be revoked on their termination date



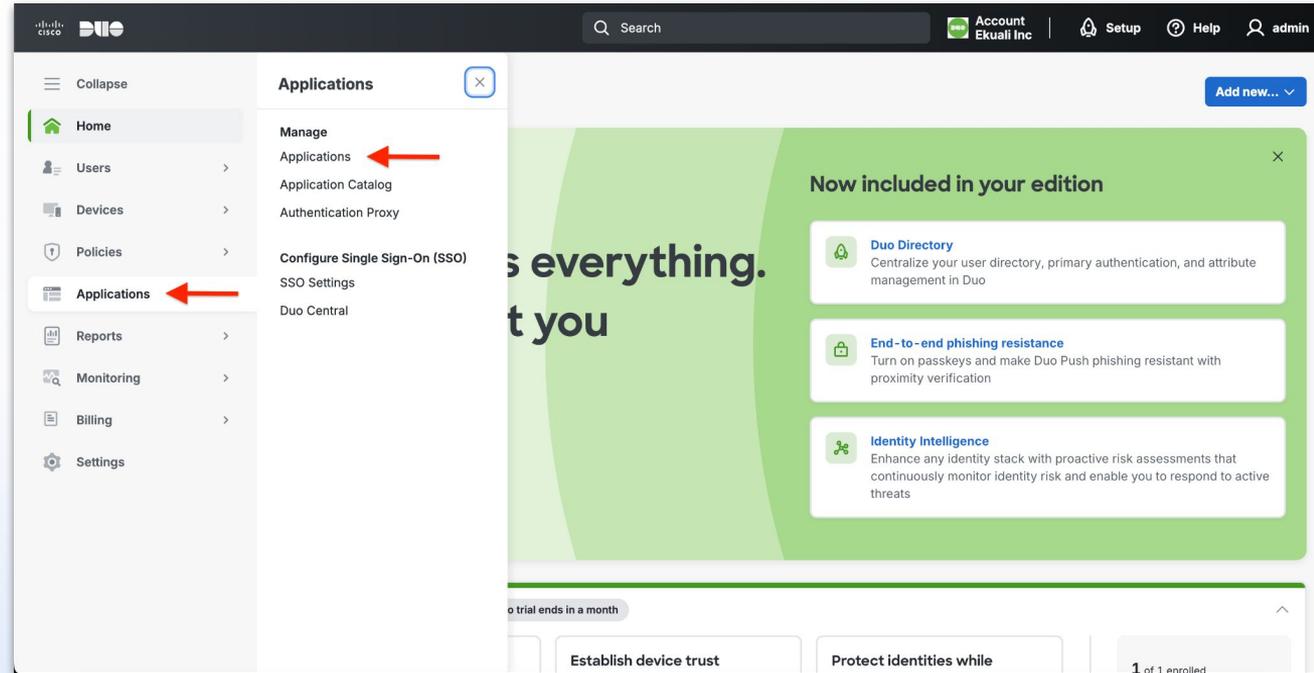
Wellness Coach supports Active Directory sync through SCIM

- **SCIM: System for Cross-domain Identity Management**
- **Benefits of SCIM**
 - **Employee Access Management** - the automation of enabling and disabling employees' access to Wellness Coach
 - Once an employee is added to DUO, their access to Wellness Coach is established, no additional steps are required by IT or the HR department



Technical Steps Needed to Launch SSO for with Wellness Coach





1. Go to DUO Admin Console
2. Click on "Applications" on left hand side menu



Click "Add application"

Account Ekuall Inc | Setup Help admin

Applications

Applications integrate Duo into one or more of your services or platforms. You can protect as many applications with Duo as you need.

Migrate to the Universal Prompt
Duo Technical Support Team no longer supports the Traditional Prompt. Temporary [exclusions](#) apply.
[View migration progress](#) [Learn about Duo's Universal Prompt](#)

Configured applications

Search by name or key Protection Type Provisioning Filters 1 result [Export CSV](#) [+ Add application](#)

Name	Protection Type	Provisioning	Application Type	Application Policy	Application-Group Policies
------	-----------------	--------------	------------------	--------------------	----------------------------

Rows per page 10 1-1 of 1 < 1 >

© 2025 Duo Security. All rights reserved. [Terms of service](#)

Selected: Ekuall Inc / ID: 2077-1419-22
Deployment ID: [DUO69](#)



Search "generic saml"
Click on "+Add"

The screenshot displays the Duo SSO Application Catalog interface. The top navigation bar includes the Cisco Duo logo, a search bar, and user information for 'Account Ekuall Inc' with 'Setup', 'Help', and 'admin' links. The left sidebar contains a navigation menu with options: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Billing, and Settings. The main content area is titled 'Applications' and 'Application Catalog', with a sub-header: 'Browse all of our available applications and filter by supported features. View documentation links for more information about each application.' A search bar contains the text 'generic saml' and a 'Supported Features' dropdown menu. Below the search results, a card for 'Generic SAML Service Provider' is shown, featuring a green icon with a plus sign, the text 'Generic SAML Service Provider', and tags for 'SSO' and 'Provisioning'. The description reads: 'Secure access using Duo SSO and SAML, with MFA and flexible security policies.' At the bottom of the card, there is a blue '+ Add' button and a 'Documentation' link with an external icon. Two red arrows are overlaid on the image: one pointing to the search bar and another pointing to the '+ Add' button.



1. Enter Application name
"Wellness Coach"
2. Choose User access
("Enable for all users" is recommended)

The screenshot shows the Duo SSO console interface. At the top, there's a navigation bar with the Duo logo, a search bar, and user information for 'Account Ekuall Inc' with 'Setup', 'Help', and 'admin' links. A left sidebar contains navigation options: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Billing, and Settings. The main content area displays a success message: 'Successfully added Generic SAML Service Provider - Single Sign-On to protected applications. Add another.' Below this, the page title is 'Generic SAML Service Provider - Single Sign-On' with links for 'Authentication Log' and 'Remove Application'. The 'Single Sign-On' tab is active. A link to 'Generic SSO documentation' is provided. The 'Basic Configuration' section includes: 'Application name *' set to 'Wellness Coach' (with a red arrow pointing to the text box), 'Application Type' set to 'Generic SAML Service Provider - Single Sign-On', and 'User access' with three radio button options: 'Disable for all users', 'Enable only for permitted groups', and 'Enable for all users' (selected, with a red arrow pointing to the radio button).



1. Type Entity ID -> "WellnessCoach"
2. Type "Assertion Consumer Service (ACS) URL" -> "https://api.meditation.live/auth/sso/callback"
3. Default Relay State (Mandatory)

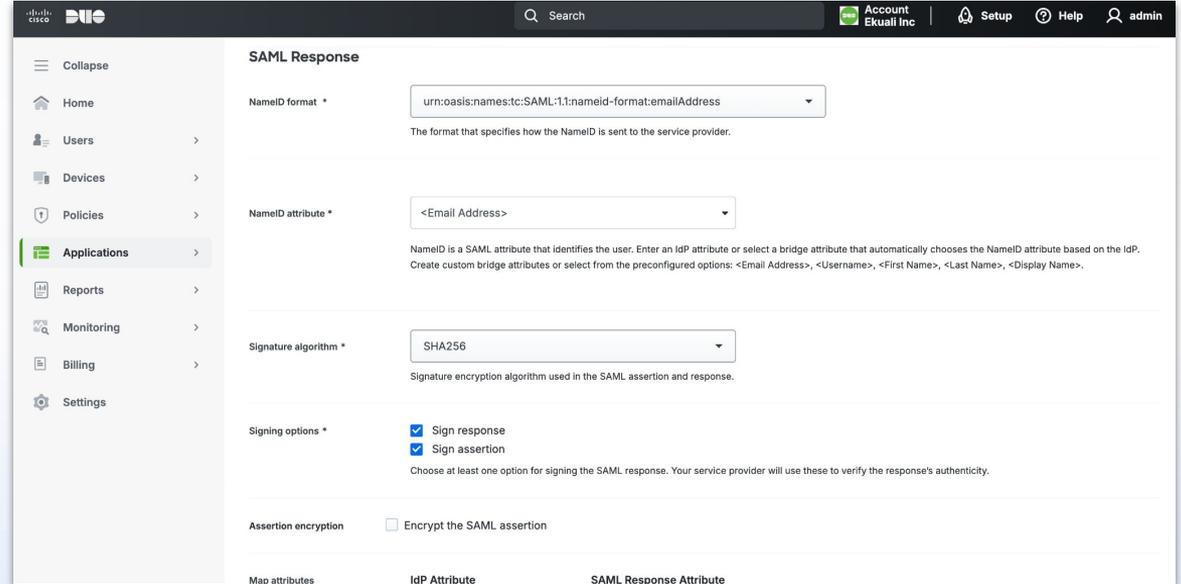
*Key will be supplied by Wellness Coach:
Please contact your CS rep or
CustomerSuccess@wellnesscoach.live for the
key*

The screenshot displays the Duo SSO configuration page for Wellness Coach. The left sidebar contains navigation options: Collapse, Home, Users, Devices, Policies, Applications, Reports, Monitoring, Billing, and Settings. The main content area is titled 'Metadata Discovery' and includes the following fields:

- Metadata Discovery:** A dropdown menu set to 'None (manual input)'.
- Entity ID:** A text input field containing 'WellnessCoach'. A red arrow points to this field. Below it is the text: 'The unique identifier of the service provider.'
- Assertion Consumer Service (ACS) URL:** A text input field containing 'https://api.meditation.live/auth/sso/callback'. A red arrow points to this field. Below it is the text: 'The service provider endpoint that receives and processes SAML assertions.' There is a '+ Add an ACS URL' link below the field.
- Single Logout URL:** A text input field containing 'Single Logout URL'. Below it is the text: 'Optional: The service provider endpoint that receives and processes SAML logout requests.'
- Service Provider Login URL:** A text input field containing 'Service Provider Login URL'. Below it is the text: 'Optional: A URL provided by your service provider that will start a SAML authentication. Leave blank if unsure.'
- Default Relay State:** A text input field containing '68cabd7657f21cbd13210097'. A red arrow points to this field. Below it is the text: 'Optional: When set, all IdP-initiated requests include this relaystate. Configure if instructed by your service provider.'



1. Scroll page to “SAML Response” section
2. Set the “NameID format” shown in the screen
3. “NameID attribute” should be “Email Address”



The screenshot shows the Duo SSO configuration interface for the SAML Response section. The left sidebar contains navigation options: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Billing, and Settings. The main content area is titled "SAML Response" and includes the following configuration fields:

- NameID format ***: A dropdown menu set to "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress". Below it, a note states: "The format that specifies how the NameID is sent to the service provider."
- NameID attribute ***: A dropdown menu set to "<Email Address>". Below it, a note states: "NameID is a SAML attribute that identifies the user. Enter an IdP attribute or select a bridge attribute that automatically chooses the NameID attribute based on the IdP. Create custom bridge attributes or select from the preconfigured options: <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name>."
- Signature algorithm ***: A dropdown menu set to "SHA256". Below it, a note states: "Signature encryption algorithm used in the SAML assertion and response."
- Signing options ***: Two checkboxes are checked: "Sign response" and "Sign assertion". Below them, a note states: "Choose at least one option for signing the SAML response. Your service provider will use these to verify the response's authenticity."
- Assertion encryption**: A checkbox labeled "Encrypt the SAML assertion" is unchecked.

At the bottom of the configuration area, there are three columns: "Map attributes", "IdP Attribute", and "SAML Response Attribute".



1. Scroll page to “Map Attributes” section
2. Create the attributes shown in the screen
3. “email”
4. “firstName”
5. “lastName”

Use the green + icon to add more

Choose at least one option for signing the SAML response. Your service provider will use these to verify the response's authenticity.

Assertion encryption Encrypt the SAML assertion

Map attributes	IdP Attribute	SAML Response Attribute
	<Email Address>	email
	<First Name>	firstName
	<Last Name>	lastName

Map the values of an IdP attribute to another attribute name to be included in the SAML response (e.g. Username to User.Username). Enter in an IdP attribute or select one of Duo's preconfigured bridge attributes that automatically chooses the SAML response attribute based on the IdP. There are five preconfigured bridge attributes: <Email Address>, <Username>, <First Name>, <Last Name>, <Display Name> and any additional bridge attributes that you have configured. <AMR> refers to Authentication Method Reference, which will send authentication information to the service provider. While most service providers use "amr" in the response, you may need to contact them for more information on their attribute names.

Create attributes	Name	Value

Specify attributes with hard-coded values to optionally send in the SAML response (e.g. accountNumber with value of 48152547). Consult your service provider for more information.

Role attributes

Map Duo groups to different roles in this service provider. A Duo group can be mapped to multiple roles and each role can have multiple groups mapped to it. Optional. [Learn more about Duo groups.](#)



DUO SSO with Wellness Coach

Scroll below and
Click "Save"

The screenshot displays the Duo SSO configuration interface. The left sidebar contains navigation options: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Billing, and Settings. The main content area is titled "Configuration" and includes the following sections:

- Configuration:** Controls if a username should be altered before trying to match them with a Duo user account.
- Voice greeting:** A text input field containing "Welcome to Duo."
- Notes:** A text input field for internal use, with a maximum of 512 characters.
- Administrative unit:** A dropdown menu set to "Assign administrative unit".
- Allowed Hostnames:** A message stating that configuring allowed hostnames is no longer supported for Frameless Duo Universal Prompt, with a link to "Get more information".

A red arrow points to the "Save" button at the bottom of the configuration area. The footer contains copyright information for Duo Security, account details for Ekuall Inc (ID: 2077-1419-22, Deployment ID: DU069), and a link to the Terms of service.



Scroll up to
“Metadata” section
and download SAML
Metadata from
“Download XML”
button and share to
Wellness Coach
Team

The screenshot shows the Duo SSO Admin console interface. On the left is a navigation sidebar with options: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Billing, and Settings. The main content area is titled "Metadata" and contains several sections:

- Metadata:** A list of four URLs, each with a "Copy" button. The URLs are: `https://sso-7bceaba2.sso.duosecurity.com/saml2/sp/DIYPIUA48PLGHFF6FZMT/meta`, `https://sso-7bceaba2.sso.duosecurity.com/saml2/sp/DIYPIUA48PLGHFF6FZMT/sso`, `https://sso-7bceaba2.sso.duosecurity.com/saml2/sp/DIYPIUA48PLGHFF6FZMT/slo`, and `https://sso-7bceaba2.sso.duosecurity.com/saml2/sp/DIYPIUA48PLGHFF6FZMT/meta`.
- Certificate Fingerprints:** Two rows, each with a fingerprint value and a "Copy" button. The first is SHA-1 Fingerprint: `33:C2:91:8F:72:C1:2B:C1:5B:72:A7:3F:15:AE:8D:AA:9B:A5:D0:7A`. The second is SHA-256 Fingerprint: `8A:DC:3A:EE:20:71:DC:A5:B5:AF:00:05:C8:FC:A0:C0:CD:BE:5D:31:83:C1:B5:B0:0E:BF`.
- Downloads:** Two rows of buttons. The first row has "Download certificate" and "Copy certificate" buttons, with "Expires: 01-19-2038" to the right. The second row has "Download XML" and "Copy XML" buttons. A red arrow points to the "Download XML" button.
- Service Provider:** A "Metadata Discovery" dropdown menu currently set to "None (manual input)".

The top of the console features the Duo logo, a search bar, and user information for "Account Ekuall Inc" with "Setup", "Help", and "admin" links.



Technical Steps Needed to Launch SCIM Provisioning (DUO) with Wellness Coach



1. Go to “Provisioning” tab
2. Scroll to “Authentication”

The screenshot shows the Duo SCIM provisioning interface for a "Generic SAML Service Provider - Single Sign-On". The interface is divided into two main sections: "Provisioning" and "Authentication".

Provisioning Section:

- The "Provisioning" tab is selected, indicated by a red arrow pointing to the "Provisioning" label in the top navigation bar.
- The "Provisioning" status is "Disabled", with a "Disable provisioning" button in the top right corner.
- A blue information box contains the text: "This is a generic SCIM integration that has not been verified against this application. Please consult your application vendor's documentation to confirm their level of support and requirements for SCIM provisioning."
- Below the information box, there is a paragraph: "Set up user provisioning with this application using the System for Cross-domain Identity Management (SCIM) protocol."
- Another paragraph follows: "Before you start, check your application to get SCIM integration details and the supported authentication mechanism."
- A link "Learn more about provisioning." is provided.

Authentication Section:

- The "Authentication" section is visible below the provisioning section, indicated by a red arrow pointing to the "Authentication" header.
- It contains the text: "Set up an authentication mechanism with your application to secure the connection."
- The "Authentication mode" is set to "Bearer Token" in a dropdown menu.
- The "Base URL" field is partially visible below the authentication mode dropdown.

The interface also features a left-hand navigation menu with options like "Collapse", "Home", "Users", "Devices", "Policies", "Applications", "Reports", "Monitoring", "Billing", and "Settings". The top right corner includes a search bar, user information for "Account Ekual Inc", and links for "Setup", "Help", and "admin".



1. Select Authentication mode as “Bearer Token”
2. Add Base URL as <https://ed.wellnesscoach.live/scim>
3. Add Token. *Please send an email to Wellness Coach for the token*
4. Test by clicking “Connect to application”

The screenshot shows the Duo Provisioning interface. The left sidebar contains navigation options: Collapse, Home, Users, Devices, Policies, Applications (highlighted), Reports, Monitoring, Billing, and Settings. The main content area is titled "Single Sign-On Provisioning" and includes a "Provisioning" section with a "Disabled" status and a "Disable provisioning" button. A blue information box states: "This is a generic SCIM integration that has not been verified against this application. Please consult your application vendor's documentation to confirm their level of support and requirements for SCIM provisioning." Below this, instructions for setting up user provisioning and a link to "Learn more about provisioning" are provided. The "Authentication" section is set up with the following fields: "Authentication mode" set to "Bearer Token", "Base URL" set to "https://ed.wellnesscoach.live/scim", and "Token" field with a "Show" button. A "Connect to application" button is at the bottom. A green success message at the bottom states: "Successfully connected to the application. Finish setting up this connection to ensure that Duo can send user information to the application." Four red arrows point to the "Bearer Token", "Base URL", "Token", and "Connect to application" elements.



1. Scroll to Attribute Mapping
2. Select Email Address for userName
3. Click on Edit Mappings and select name.familyName and name.givenName
4. Click "Save Mapping"

The screenshot displays the Duo SCIM configuration interface. On the left is a navigation sidebar with options: Collapse, Home, Users, Devices, Policies, Applications, Reports, Monitoring, Billing, and Settings. A red arrow points to the 'Applications' menu item. The main content area is titled 'Attribute mapping' and includes a sub-header 'Attribute mapping' and a descriptive paragraph: 'Configure how Duo user attributes are mapped to the attributes in your application so that user information is received in the correct format. To view or create Duo user attributes, go to [User Attributes](#).' Below this is a table with two columns: 'Duo user attribute' and 'Application attribute'. The first row shows 'Email Address' mapped to 'userName'. A 'Groups' section follows, with a blue information box stating: 'Users or groups will be automatically created, updated, and deactivated in this application.' Below the box are radio buttons for 'Select groups' (selected), 'Use groups with SSO access', and 'Exclude group information'. A 'Save and enable' button is at the bottom of the main panel. On the right, an 'Edit mappings' modal is open, showing a list of attributes under 'Required attributes' (userName is checked) and 'Optional attributes' (name.familyName and name.givenName are checked). At the bottom of the modal, it shows 'Selected (4 items)' and buttons for 'Cancel' and 'Save mapping'.



1. Select "First Name" for givenName
2. Select "Last Name" for familyName
3. Click "Save and enable"

The screenshot displays the Duo SCIM configuration interface. The left sidebar contains navigation options: Collapse, Home, Users, Devices, Policies, Applications, Reports, Monitoring, Billing, and Settings. The main content area is titled "Attribute mapping" and includes a table for mapping Duo user attributes to application attributes. Below this is a "Groups" section with a "Save and enable" button at the bottom.

Attribute mapping

Configure how Duo user attributes are mapped to the attributes in your application so that user information is received in the correct format. To view or create Duo user attributes, go to [User Attributes](#).

Duo user attribute	Application attribute	Action
Email Address	userName	—
Last Name	name.familyName	□
First Name	name.givenName	□

Groups

Select existing groups that will receive updates from Duo in this application.

Users or groups will be automatically created, updated, and deactivated in this application.

Select groups

Groups

Select...

Use groups with SSO access

Exclude group information

If checked, Duo will send only user details without group information.

Save and enable

