

# Configuring Duo

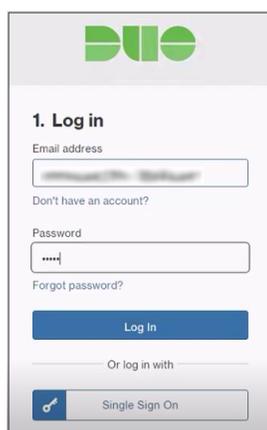
Configuring Duo for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Duo by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

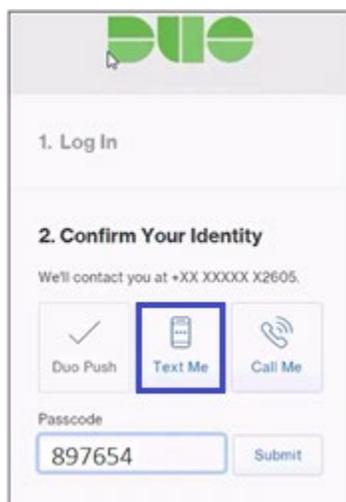
## To configure Duo for SSO by using SAML:

1. In a browser, type <https://admin.duosecurity.com> and press **Enter**.
2. Type your DUO admin credentials (**Email address** and **Password**) and click **Log in**.



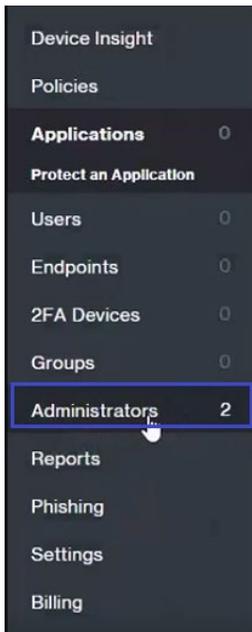
The screenshot shows the Duo login interface. At the top is the Duo logo. Below it, the heading "1. Log in" is followed by an "Email address" input field. A link "Don't have an account?" is positioned below the email field. The "Password" input field is next, with a "Forgot password?" link underneath. A blue "Log In" button is centered below the password field. At the bottom, there is a section "Or log in with" containing a "Single Sign On" button with a key icon.

3. To log on, click **Text Me**. A numerical code will be sent to your registered mobile number.
4. Type the code in the **Passcode** textbox and click **Submit**.

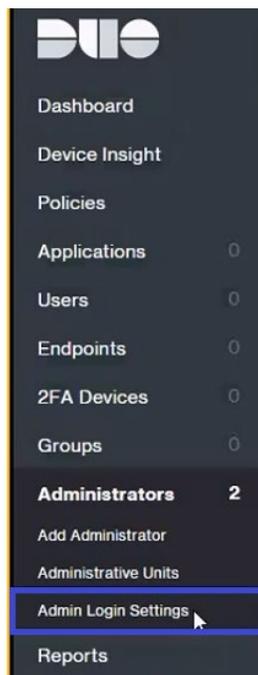


The screenshot shows the "2. Confirm Your Identity" step. It displays a message: "We'll contact you at +XX XXXXX X2605." Below this are three buttons: "Duo Push" (with a checkmark icon), "Text Me" (with a mobile phone icon and highlighted by a blue box), and "Call Me" (with a telephone handset icon). Below the buttons is a "Passcode" input field containing the number "897654" and a "Submit" button.

5. Under **Applications**, click **Administrators**.



6. Under **Administrators**, click **Admin Login Settings**.



7. To create SSO, enter the values for the following fields:

Field	Description
Identity provider	Select <b>Customer Identity Provider</b> from the drop-down list.
Configuration method	Select <b>From file</b> from the drop-down list.
Metadata File	The SAML metadata is provided by Citrix and can be accessed from the link below: <a href="https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml">https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml</a>
Encrypt assertions	Select <b>Require unencrypted assertions</b> from the drop-down list.
Sha-1 signatures	Sha-256 is recommended for signatures. All the responses and assertions with Sha-1 are rejected.
Signed elements	Select <b>Only assertions must be signed</b> from the drop-down list.

**SAML Identity Provider Settings**

**Identity provider**

**Configuration method**

**Metadata File**   
Upload the SAML federation metadata file.

**Encrypt assertions**   
Encryption prevents third parties from reading private data from assertions. Encryption is not supported by Azure, Duo Access Gateway, Google, or PingOne.

**Advanced SAML options**

Duo recommends only customizing these options where absolutely necessary as they are less secure.

**SHA-1 signatures**  Reject all responses and assertions with SHA-1 signatures

**Signed elements**   
Identity providers sign different parts of a SAML request. Select how Duo should check for a valid signature.

Field	Description
Metadata URL	Make a note of the customer ID and the account ID. These IDs are used for IdP configuration.

**Metadata for Configuring with Custom Identity Provider**

**XML File**      [Download duo\\_saml\\_motadata.xml](#)

**Metadata URL**     

**Entity ID or Issuer ID**     

**Assertion consumer service URL or single sign-on URL**     

**Audience restriction**     

**Encryption certificate**      Assertions are currently not encrypted.

8. Finally, click **Save**.