

# Configure StatusDashboard for Single Sign-On

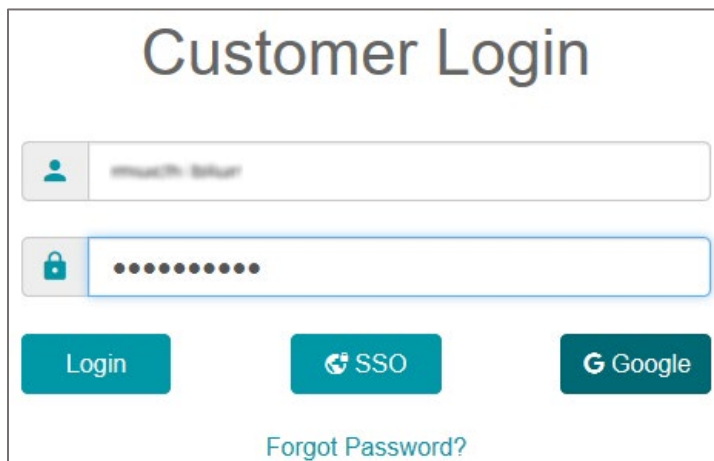
Configuring StatusDashboard for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to StatusDashboard by using the enterprise credentials.

## Prerequisite

Browser Requirements: Internet Explorer 11 and above

## To configure StatusDashboard for SSO by using SAML:

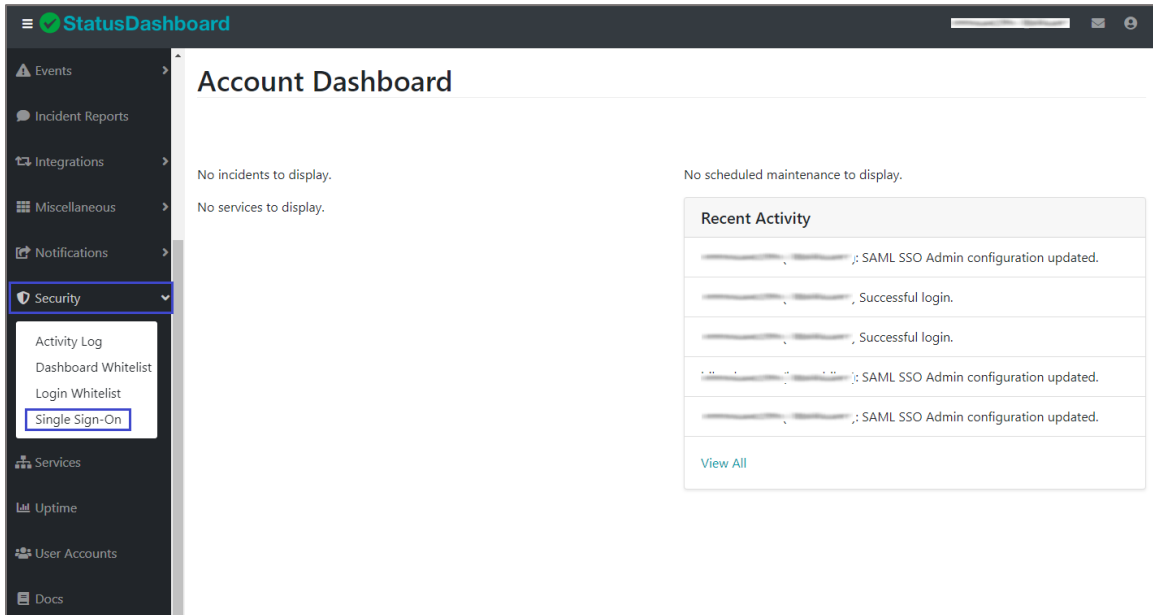
1. In a browser, type <https://www.statusdashboard.com/accounts/login/?next=/admin> and press **Enter**.
2. Type your StatusDashboard admin account credentials (**username** and **password**) and click **Login**.



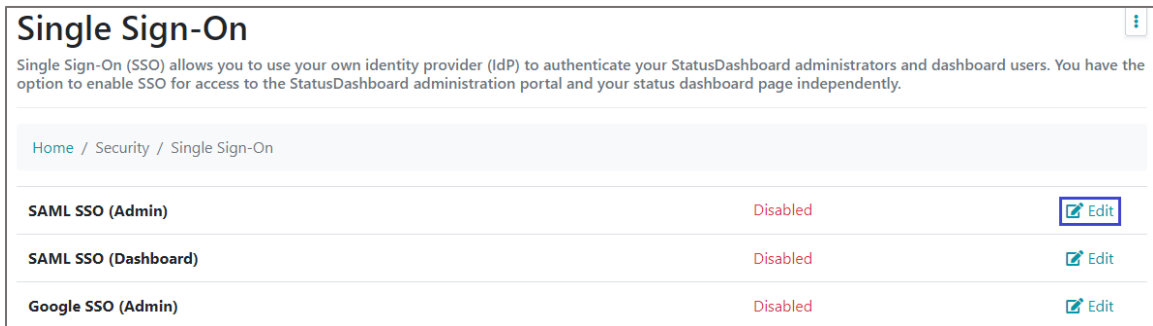
Customer Login

[Forgot Password?](#)

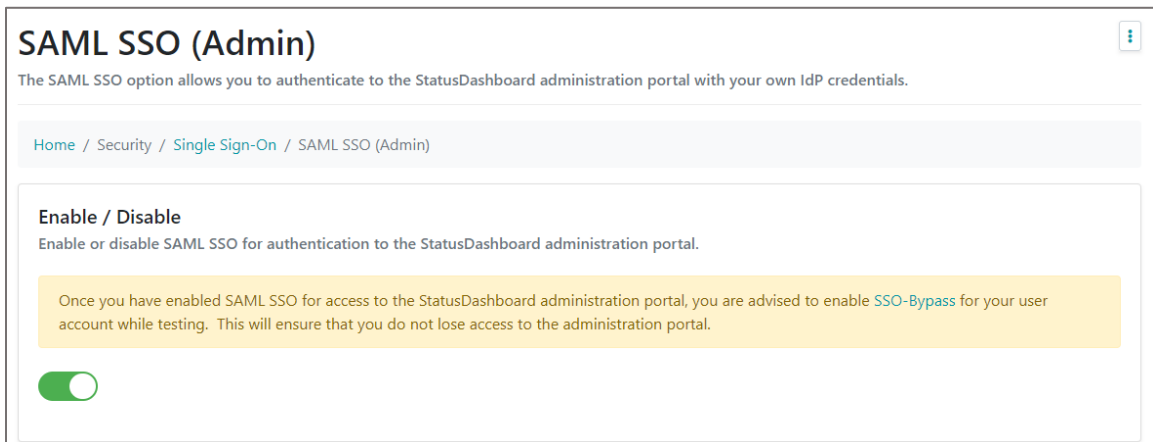
3. In the dashboard page, click **Security > Single Sign-On** from the left pane.



4. In the **Single Sign-On** page, click **Edit** in the **SAML SSO (Admin)** tile.



5. In the **SAML SSO (Admin)** page, turn on the **Enable / Disable** toggle button.



6. Scroll down and enter the values for the following fields under **Identity Provider (IdP)**:

Required Information	Description
Entity ID / Issuer*	Issuer URL
Single Sign-On (SSO) Service URL*	IdP logon URL
x509 Certificate	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with            -----Begin Certificate----- and -----End Certificate-----</p> <p><b>Note:</b> The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app.  <a href="https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust_id&gt;/&lt;app_id&gt;/idp_metadata.xml">https://gateway.cloud.com/idp/saml/&lt;citrixcloudcust_id&gt;/&lt;app_id&gt;/idp_metadata.xml</a></p>

**Identity Provider (IdP)**  
 Enter the configuration settings for your IdP. Configuration guides for most major IdPs are available in the StatusDashboard documentation.

<b>Entity ID / Issuer*</b>	<input type="text"/>
<b>Single Sign-On (SSO) Service URL*</b>	<input type="text"/>
<b>SSO Binding</b>	urn:oasis:names:tc:SAML2.0:bindings:HTTP-Redirect
<b>Single Logout Service (SLO) URL</b>	<input type="checkbox"/> <input type="text" value="Enter Single Logout Service URL"/>
<b>SLO Binding</b>	urn:oasis:names:tc:SAML2.0:bindings:HTTP-Redirect
<b>IdP Logout URL ⓘ</b>	<input type="text" value="Enter IdP Logout URL"/>
<b>Logout Redirect URL ⓘ</b>	<input type="text" value="Enter Logout Redirect URL"/>
<b>x509 Certificate ⓘ</b>	<div style="border: 1px solid gray; padding: 5px; min-height: 150px;"> <pre>-----Begin Certificate----- -----End Certificate-----</pre> </div> <p><b>ISSUED BY (O):</b> <input type="text"/>  <b>ISSUED TO (CN):</b> DEVIdP Assertion Signing Certificate.1  <b>SERIAL NUMBER:</b> <input type="text"/>  <b>EXPIRATION:</b> 2045-09-09 23:21:15 UTC</p>
<b>Require Message Signature ⓘ</b>	<input type="checkbox"/>
<b>Require Assertion Signature ⓘ</b>	<input type="checkbox"/>
<b>Require NameID Encryption ⓘ</b>	<input type="checkbox"/>

7. Finally, click **Save Changes**.