

Configure CloudPassage for Single Sign-On

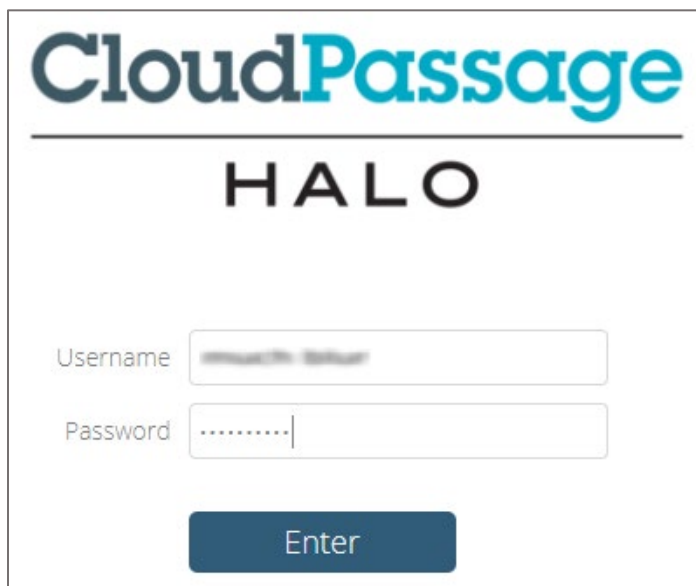
Configuring CloudPassage for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to CloudPassage by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

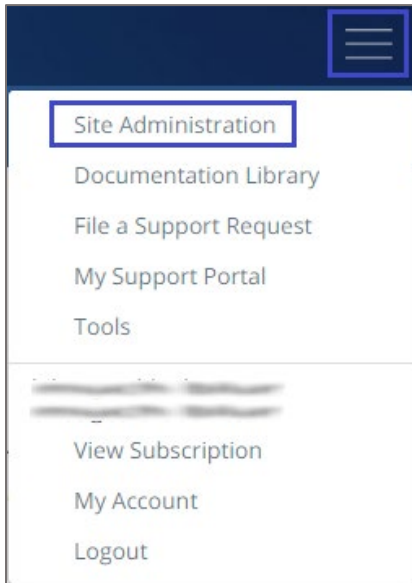
To configure CloudPassage for SSO by using SAML:

1. In a browser, type <https://portal.cloudpassage.com/login> and press **Enter**.
2. Type your CloudPassage admin account credentials (**Username** and **Password**) and click **Enter**.

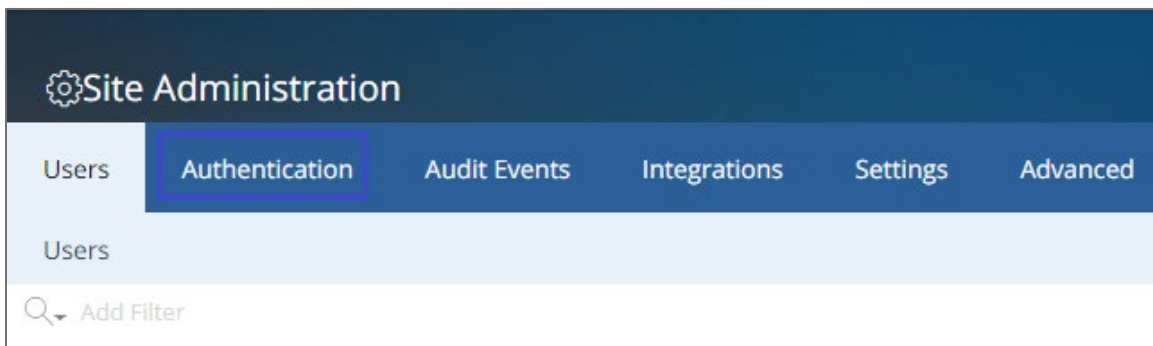


The image shows a screenshot of the CloudPassage login interface. At the top, the 'CloudPassage' logo is displayed in blue. Below the logo, a horizontal line separates it from the word 'HALO' in large, bold, black capital letters. Underneath 'HALO', there are two input fields: 'Username' with a light blue placeholder text and 'Password' with a light blue placeholder text consisting of a series of dots. Below these fields is a dark blue button with the word 'Enter' in white text.

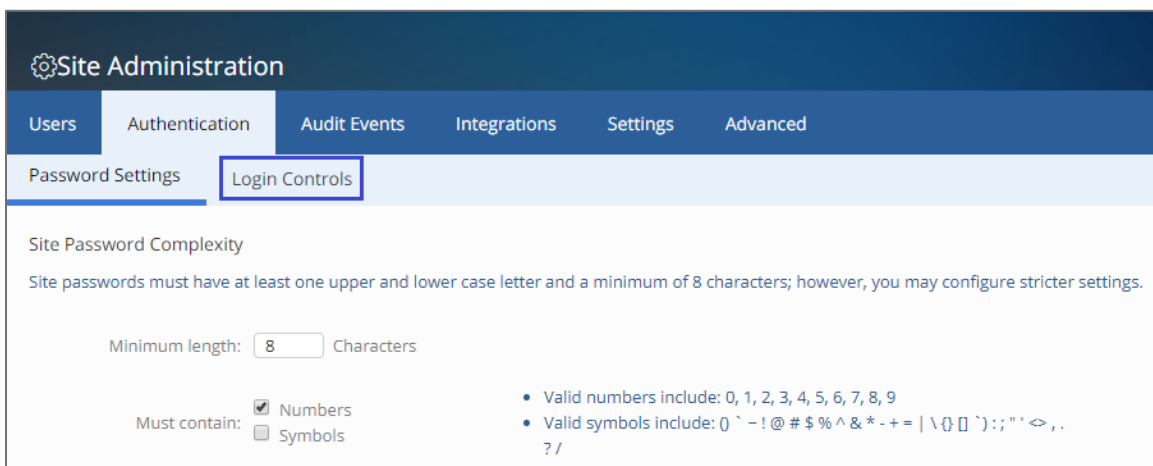
3. In the top-right corner, click the menu icon and select **Site Administration** from the list.



4. In the **Site Administration** page, click the **Authentication** tab.



5. Under the **Authentication** tab, click **Login Controls**.



6. Scroll down and select the **Enable Single Sign-On (SSO) to the Halo portal for Halo portal logins** check box.
7. Enter the values for the following fields:

| Field Name | Description |
|-------------------|--|
| SAML Issuer URL | IdP issuer URL |
| SAML Endpoint URL | IdP logon URL |
| x.509 certificate | Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: 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/<citrixcloudcust_id>/<app_id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml |

The screenshot shows the 'Login Controls' configuration page. The 'Single Sign-On' section is expanded, showing the 'Enable Single Sign-On (SSO) to the Halo portal for Halo portal logins' checkbox checked. Below this, there are instructions and input fields for SAML configuration: 'SAML Issue URL', 'SAML Endpoint URL', and 'Logout Landing page'. A large text area for the 'x.509 certificate' is present, with a blurred certificate pasted into it. At the bottom, there is a checkbox for 'Make SSO required'.

8. Finally, click **Save**.