

Configure Cascade Strategy for Single Sign-On

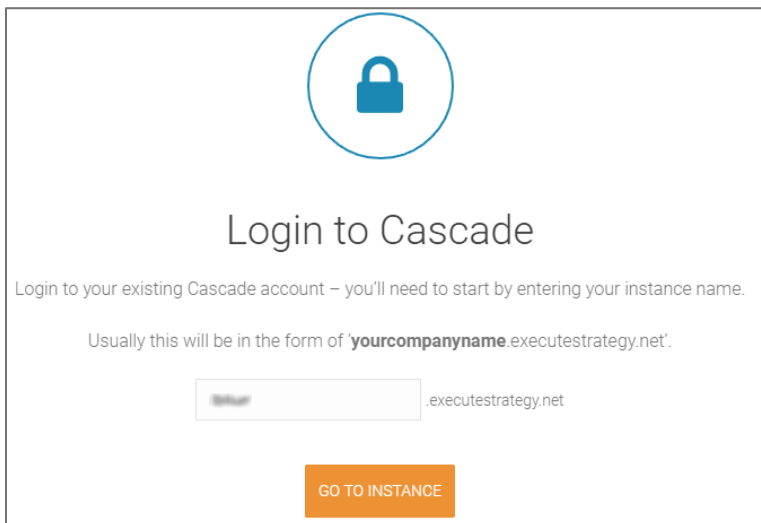
Configuring Cascade Strategy for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Cascade Strategy by using the enterprise credentials.


Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Cascade Strategy for SSO by using SAML:

1. In a browser, type <https://www.executestrategy.net/login/> and press **Enter**.
2. Enter your domain name and click **GO TO INSTANCE**.





Login to Cascade

Login to your existing Cascade account – you'll need to start by entering your instance name.

Usually this will be in the form of 'yourcompanyname.executestrategy.net'.

.executestrategy.net

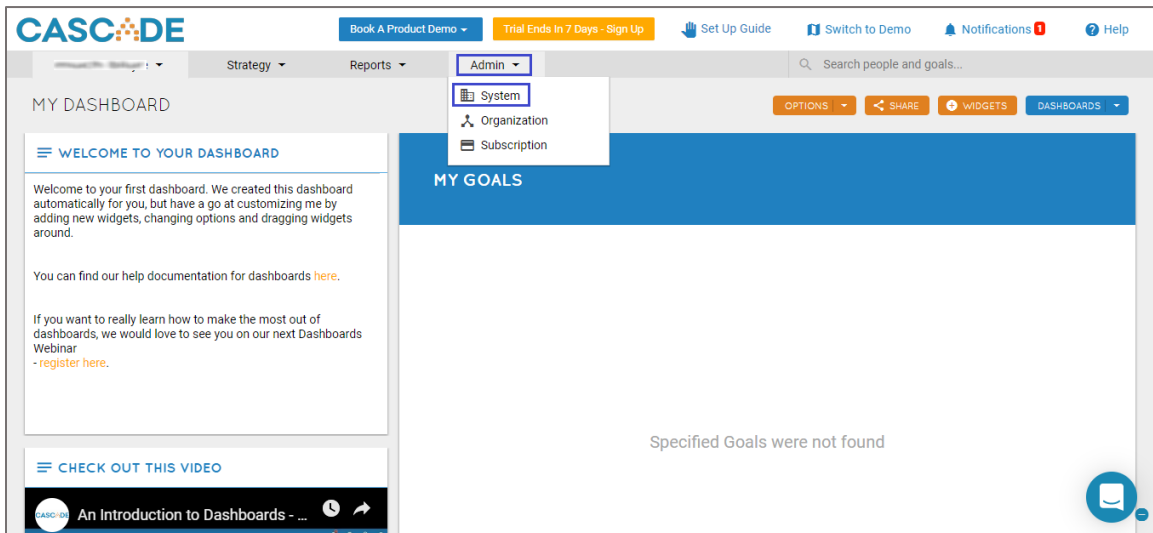
GO TO INSTANCE

3. Type your Cascade Strategy admin account credentials (**Username** and **Password**) and click **SIGN IN**.



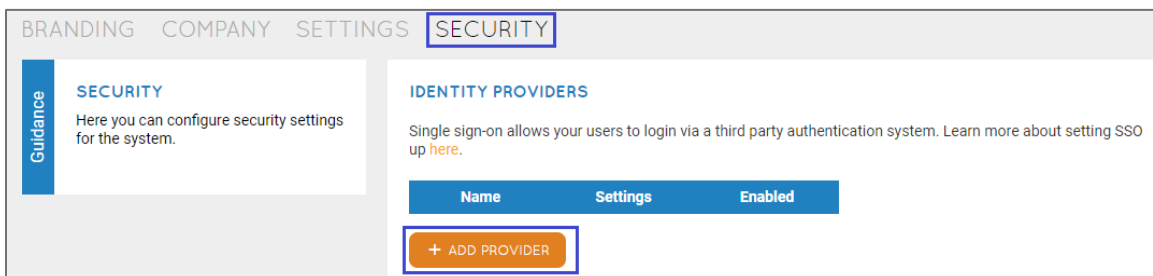
The image shows the Cascade Strategy login page. At the top is the Cascade logo. Below it is an orange button labeled "LOGIN WITH CITRIX NETSCALER". Underneath are two input fields: the first for a username (containing "admin@cascadestrategy.com") and the second for a password (containing "admin123456"). At the bottom is a blue button labeled "SIGN IN".

4. In the dashboard page, click **Admin > System**.



The image shows the Cascade Strategy dashboard. The top navigation bar includes the Cascade logo, a "Book A Product Demo" button, a "Trial Ends In 7 Days - Sign Up" button, a "Set Up Guide" link, a "Switch to Demo" link, a "Notifications" bell icon with a red badge, and a "Help" link. Below the navigation bar is a search bar labeled "Search people and goals...". The main content area is divided into two columns. The left column is titled "MY DASHBOARD" and contains a "WELCOME TO YOUR DASHBOARD" section with a welcome message and a "CHECK OUT THIS VIDEO" section with a video player. The right column is titled "MY GOALS" and contains a "Specified Goals were not found" message. A "Admin" dropdown menu is open, showing options for "System", "Organization", and "Subscription".

5. Click the **SECURITY** tab and click **ADD PROVIDER** under **IDENTITY PROVIDERS**.



The image shows the Cascade Strategy Security settings page. The top navigation bar includes the Cascade logo, a "Book A Product Demo" button, a "Trial Ends In 7 Days - Sign Up" button, a "Set Up Guide" link, a "Switch to Demo" link, a "Notifications" bell icon with a red badge, and a "Help" link. Below the navigation bar is a search bar labeled "Search people and goals...". The main content area is divided into two columns. The left column is titled "SECURITY" and contains a "Guidance" section with a "Here you can configure security settings for the system." message. The right column is titled "IDENTITY PROVIDERS" and contains a "Single sign-on allows your users to login via a third party authentication system. Learn more about setting SSO up here." message. Below the text is a table with columns for "Name", "Settings", and "Enabled". At the bottom of the table is a blue button labeled "+ ADD PROVIDER".

6. In the **Single Sign-On** page, enter the values for the following fields:

Required Information	Description
Name	Citrix NetScaler
Type	Select Azure from the drop-down list.
Name ID Format	Select urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted from the drop-down list.
Entity ID	Entity ID
Single Sign-On Service URL	IdP logon URL
Single Sign-Out Service URL	IdP logout 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>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.</p> <p><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</p>

SINGLE SIGN-ON

Need some Guidance? Read our [step by step guide](#) to setting up single sign on.

GENERAL

Name:

Citrix NetScaler

Type:

Azure

SP CONFIGURATION

Name ID Format:

urn:oasis:names:tc:SAML:2.0:nameid-format:encrypted

IDP CONFIGURATION

Entity ID:

Single Sign-On Service URL:

Single Sign-Out Service URL:

X509 Certificate:

DELETE

SAVE

7. Finally, click **Save**.