CITRIX®

NetScaler with Unified Gateway

Configuring Domo

Abstract

Configuring Domo for SSO enables administrators to manage their users using NetScaler.

Contents

Disclaimer (Documentation)

This document is furnished "AS IS." Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix System, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

Citrix Systems, Inc., the Citrix logo, and Citrix Provisioning Services are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Preface

This section provides an overview about the information included in this guide.

Intended Audience

The information in this guide is intended for the System Administrators.

Document Conventions

The following table lists various conventions used in this guide.

Table 1: Document conventions used in this guide

Convention	Description
Bold	Used for names of interface elements (such as names of fields, panes, windows, menus, buttons, dialog boxes) and what the user specifically selects, clicks, presses, or types.
Note	Used to highlight information that is important.

Overview

The Citrix NetScaler application delivery controller (ADC) helps to load balance, accelerate, optimize, and secure enterprise applications.

Domo provides cloud-based business management suite that integrates with multiple data sources including spreadsheets, databases, social media, and existing software solutions. Domo offers business intelligence tools and data visualization that provides real time access to business data.

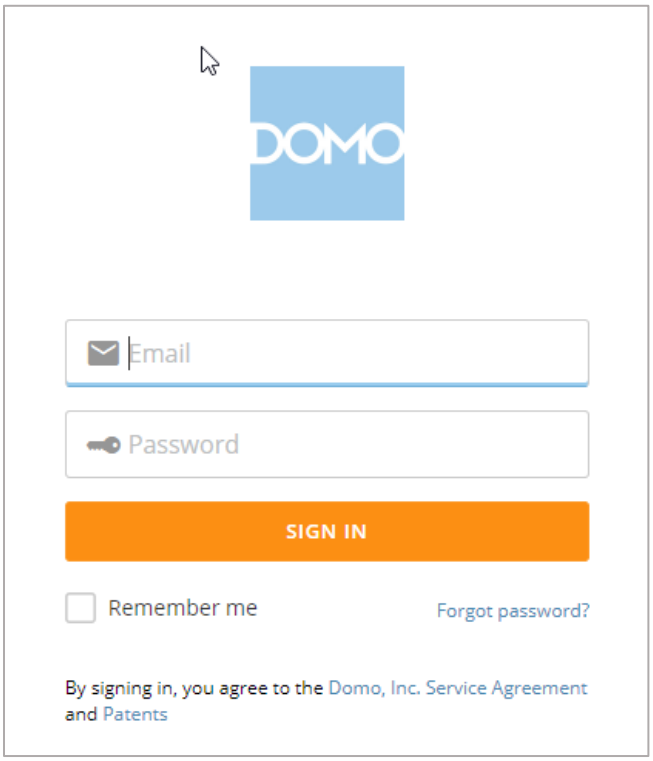
You can connect Domo with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring Domo for Single Sign-On

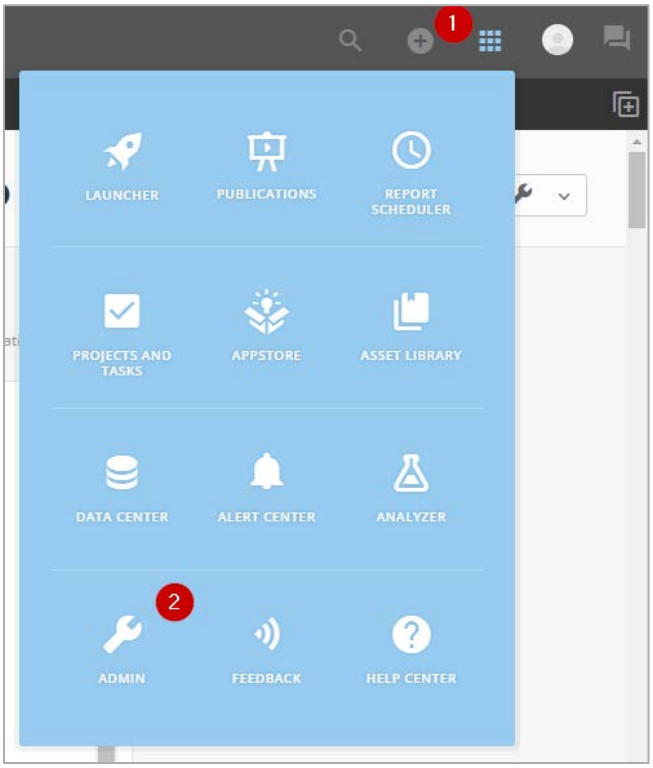
Configuring Domo for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Domo using their enterprise credentials.

To configure Domo for single sign on through SAML, follow the steps below:

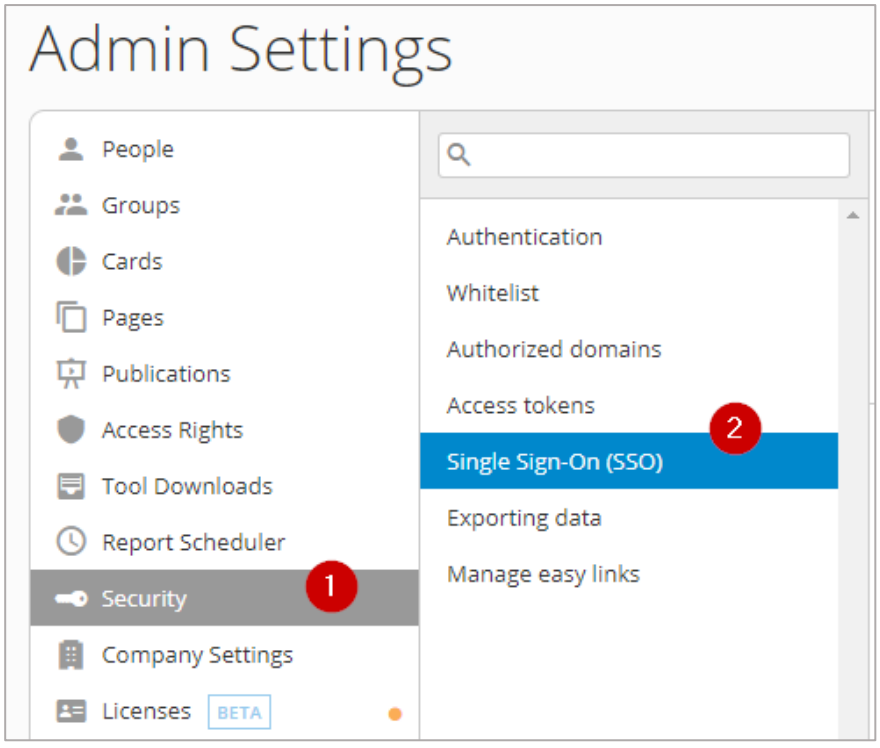
1. In a browser, type the URL in https://<your-organization>.domo.com format and press Enter.
2. Log on to your Domo account.



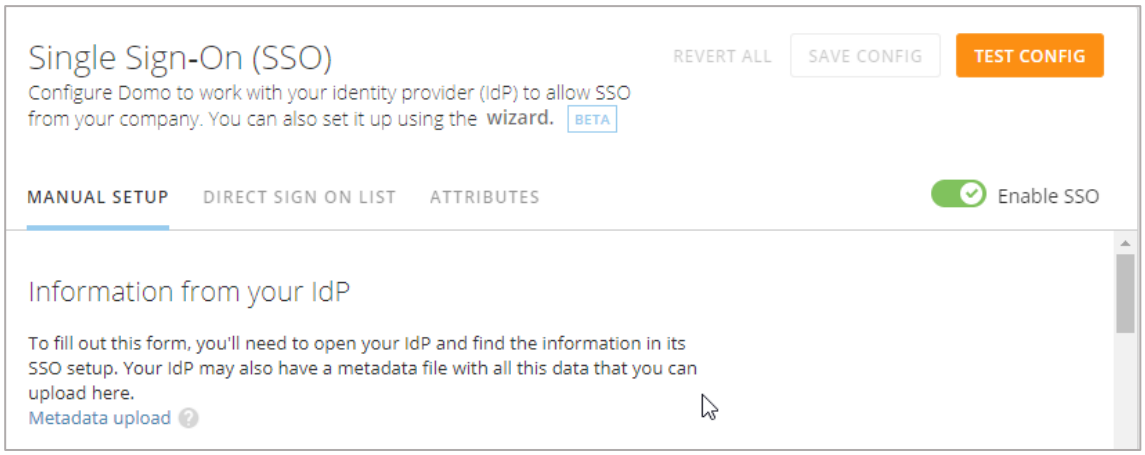
3. On the home page, in the upper right corner, click  > **Admin**.



4. On the **Admin Settings** page, click **Security** > **Single Sign-On (SSO)**> **Enable SSO**.



5. In the **Single Sign-On (SSO)** section, provide the following information.

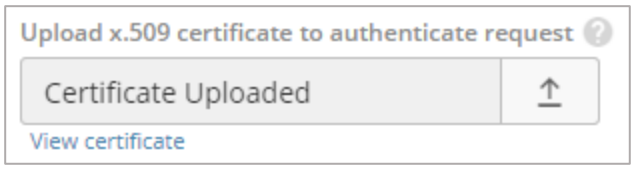


   i. In the **MANUAL SETUP** section, under **Information from your IdP**, specify the IdP information.
   Note: If you want to upload a metadata file, click **Metadata upload** or, to continue adding information manually click **Manual Entry**.

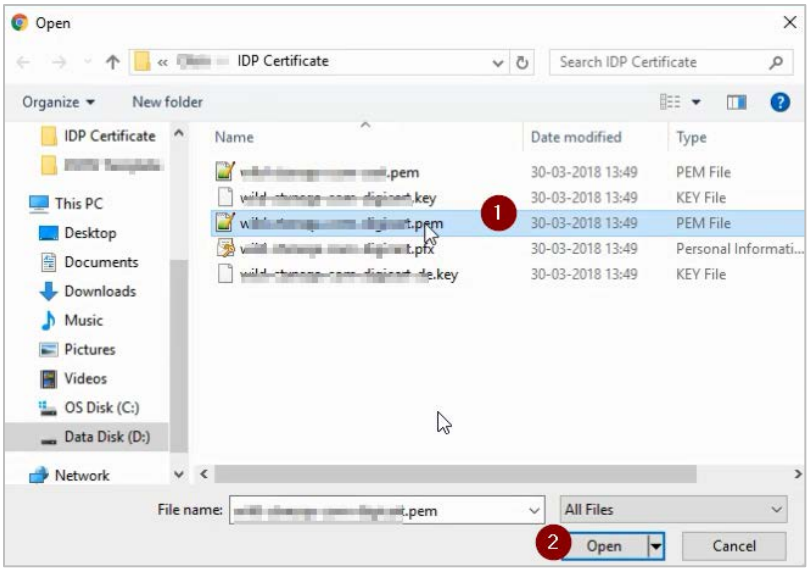
   ii. In the **Identity provider endpoint URL** box, type the URL in https://<your-organization>/saml/login format.

   iii. In the **Entity ID** box, type a unique(org url) entity ID.

   iv. In the **Upload x.509 certificate to authenticate request** box, upload the IdP certificate.



   Click the arrow to browse to the folder where you saved the IdP provided certificate and upload it.

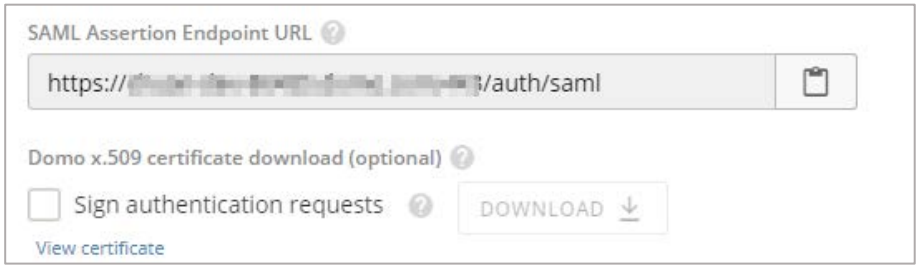


To obtain your IdP certificate, follow the steps below:

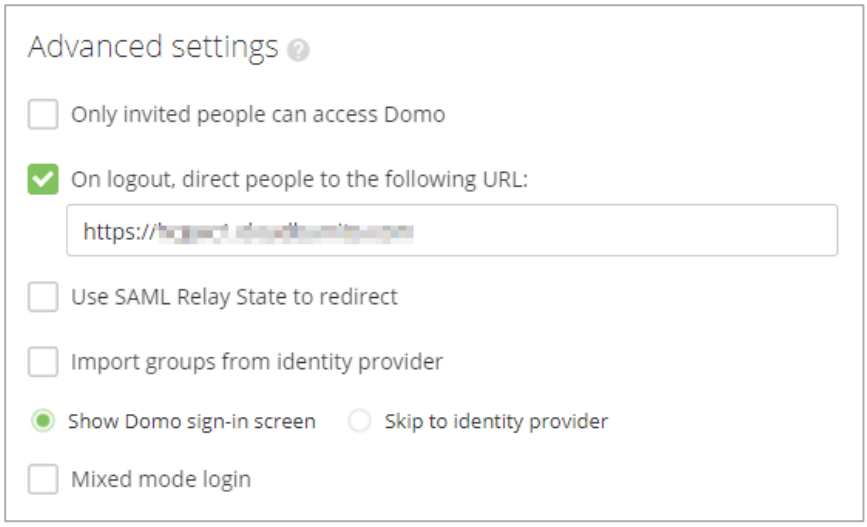
a. Remotely access your NetScaler instance using PuTTY.
b. Navigate to /nsconfig/ssl folder (using shell command cd /nsconfig/ssl) and press Enter.
c. Type cat <certificate-name> and press Enter.

d. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
e. Paste the text in a text editor and save the file in an appropriate format such as <your organization name>.pem.

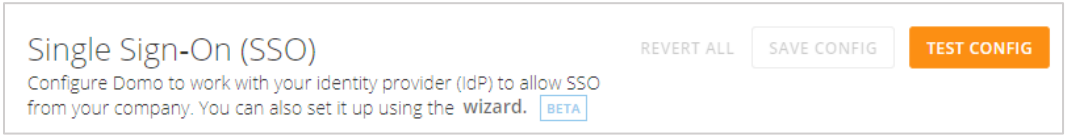
v. The **SAML Assertion Endpoint URL** box displays assertion consumer service URL.
Note: Copy this value to use it while configuring NetScaler for SSO for the Assertion Consumer Service URL field.



vi. In the **Advanced settings** area, select the **On logout, direct people to the following URL** check box and type a redirect URL for logging out.



6. In the upper-right corner, click **SAVE CONFIG**.
7. To the test the configuration, click **TEST CONFIG**.



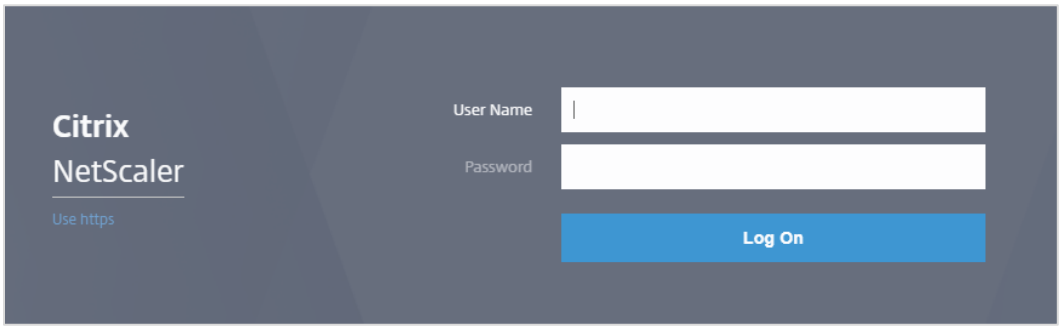
You have completed the required configuration on the service provider which is in this case – Domo.

Configuring NetScaler for Single Sign-On

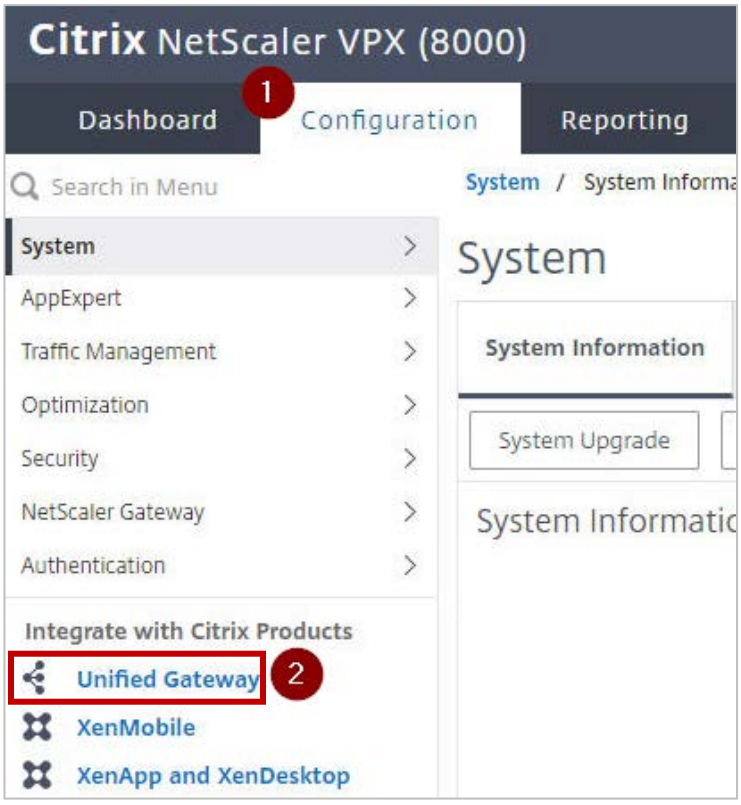
For configuring NetScaler for Domo, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

To configure NetScaler for single sign on through SAML, follow the steps below:

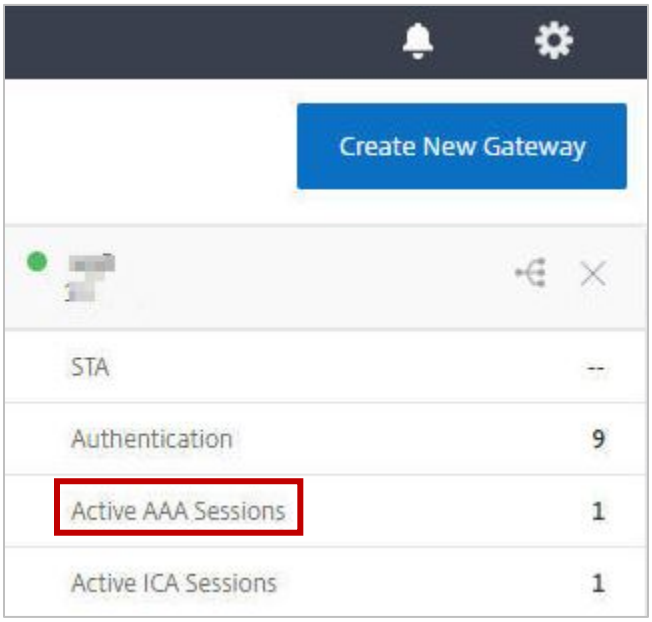
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



3. Click the **Configuration** > **Unified Gateway**.

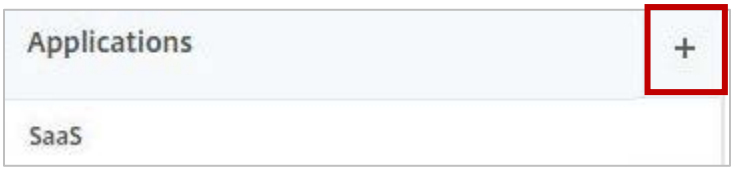


4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.

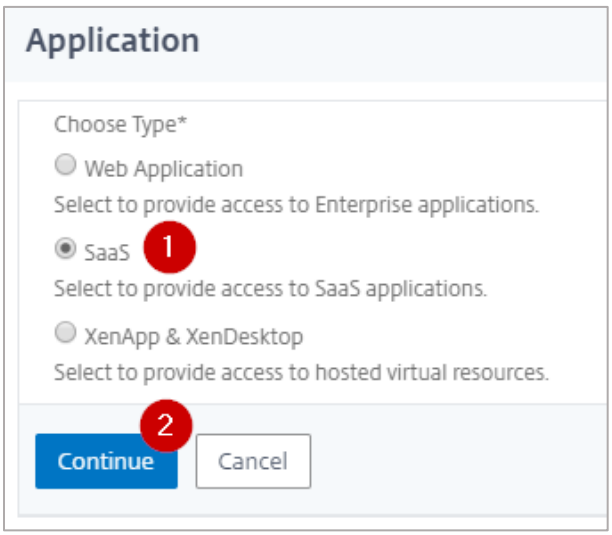


5. Click the edit icon for **Applications** section.

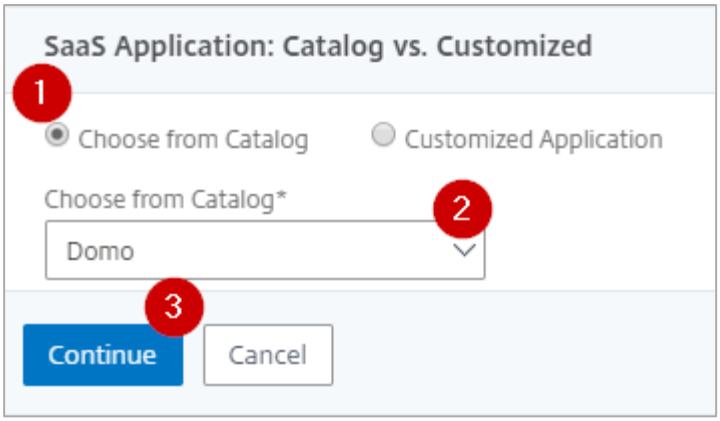
6. For adding a SaaS application, click the plus icon ⊞ that appears in the edit mode.



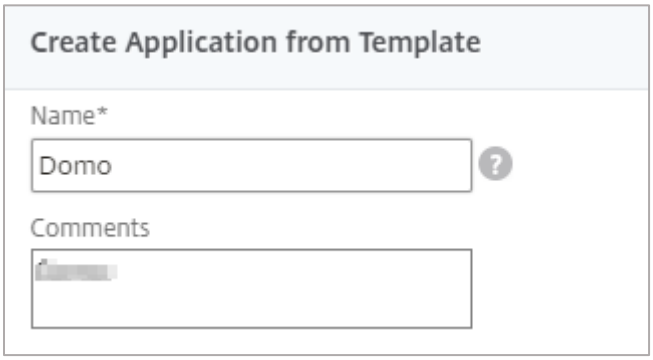
7. Click **SaaS** > **Continue**.



8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **Domo**.



10. Click **Continue**.
11. In the **Create Application from Template** section, type the name of your SaaS application, in this case Domo, and relevant comments.



Note:

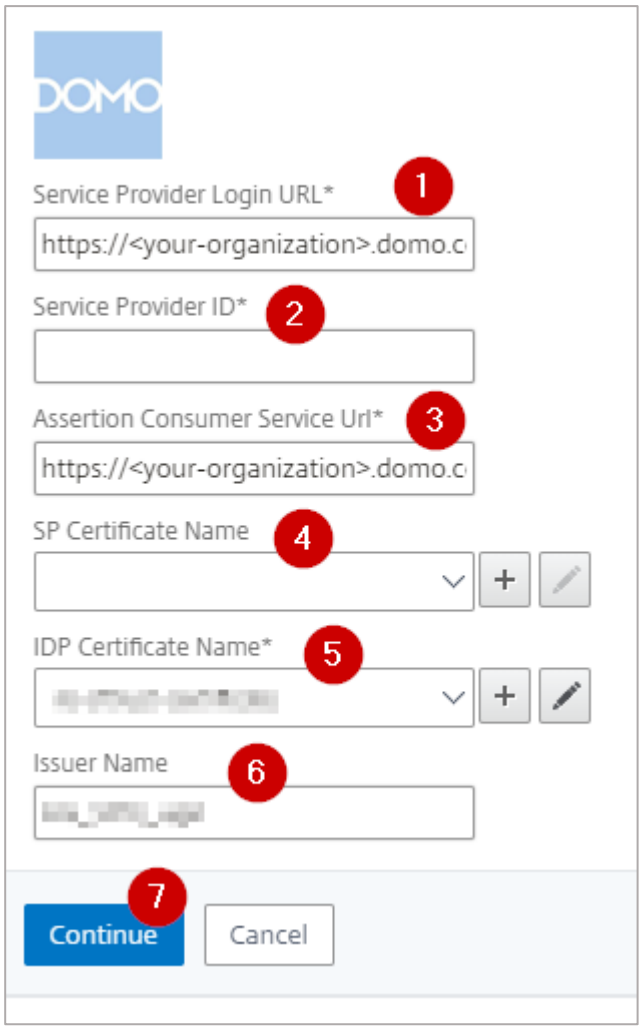
An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

The following table lists the SAML values that you need to copy while configuring SSO for SP and paste the values to appropriate fields while configuring SSO for IdP NetScaler.

Table 2: SSO field values used for SP and IdP configurations

Service Provider (SP) Domo	Identity Provider (IdP) NetScaler
Entity Id	Issuer Name
X.509 certificate	IdP Certificate
SAML Assertion Endpoint URL	Assertion Consumer Service URL

12. In the subsequent section, specify the following information:



i. **Service Provider Login URL** - enter the URL that you use to access Domo: https://<your-organization>.domo.com/auth/saml
ii. **Service Provider ID** – type a unique identifier for the service provider.
iii. **Assertion Consumer Service Url*** – enter the URL that you use to access Domo: https://<your-organization>.domo.com/auth/saml
iv. **SP Certificate Name** – click the appropriate certificate name.
To obtain this value, access the metadata file:
ttps://rpm.newrelic.com:443/accounts/<cuastomer_AccNo>/sso/saml/metadata
v. **IDP Certificate Name** – click the appropriate certificate name.
Refer to the appropriate public key certificate provided by NetScaler which you referred while configuring Domo.
vi. **Issuer Name** – type a unique name.
vii. Click **Continue**.

13. Click **Done**.
The Domo logo appears.

14. Click **Done**.

    You have completed the NetScaler configuration for Domo.

Testing the Configuration

Testing the IdP Initiated Flow

To test the IdP initiated configuration, follow the steps below:

1. Access the IdP URL.
2. Log on to NetScaler appliance using your enterprise credentials.
3. Click **Clientless Access**.
4. On the home page, click **Apps** tab.
5. Click **Domo**.
   Your Domo profile is displayed.
   You have completed testing the IdP initiated flow.

Testing the SP Initiated Flow

To test the SP initiated configuration, follow the steps below:

1. Access the login URL that is in https://[subdomain].domo.com/auth/index format.
2. You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.

   Your Domo profile is displayed which indicates that you have successfully logged on to Domo.

CITRIX®

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States