NetScaler with Unified Gateway

Configuring G Suite

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.

G Suite can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to G Suite using the same Single Sign On (SSO).

Terminology

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 various terms that are used alternatively for completing configurations for service providers and identity providers.

Table 2: Terminology used for SP and IdP configurations

Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring G Suite for Single Sign-On

G Suite has SP/IdP initiated flow, which is supported in NetScaler (12.1.).

Before you start, you need the following:

- Admin account for G Suite
- Customer instance

  For example, if your deployment url https://www.google.com/a/<customer_domain>.com , your customer instance is <*customer domain*>.

  This is required for App Catalog creation in NetScaler.
- Admin account for NetScaler

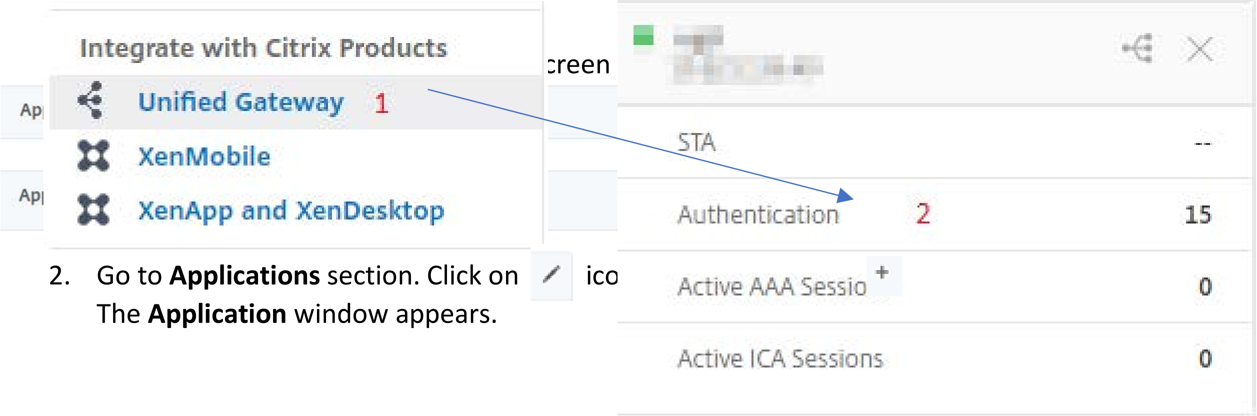
G Suite Configuration

The G Suite configuration steps are as follows:

1. Configure G Suite with the App Catalog.
2. Configure IdP into G Suite.

Step 1: Configure G Suite with App Catalog

1. Click on **Unified Gateway > Authentication.**



[redacted]

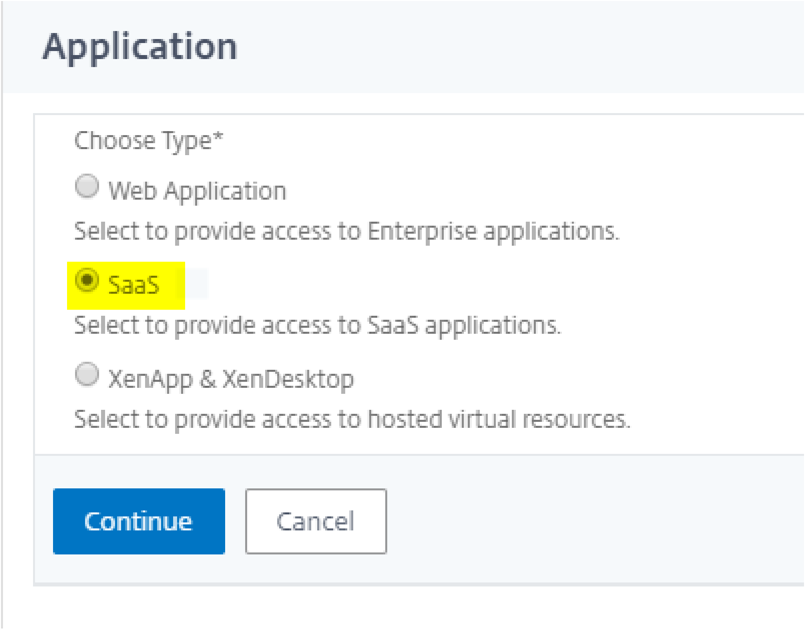
STA --

Authentication 15

Active AAA Sessio 0

Active ICA Sessions 0

2. Go to **Applications** section. Click on ✎ ico
   The **Application** window appears.



Application

Choose Type*

○ Web Application

Select to provide access to Enterprise applications.

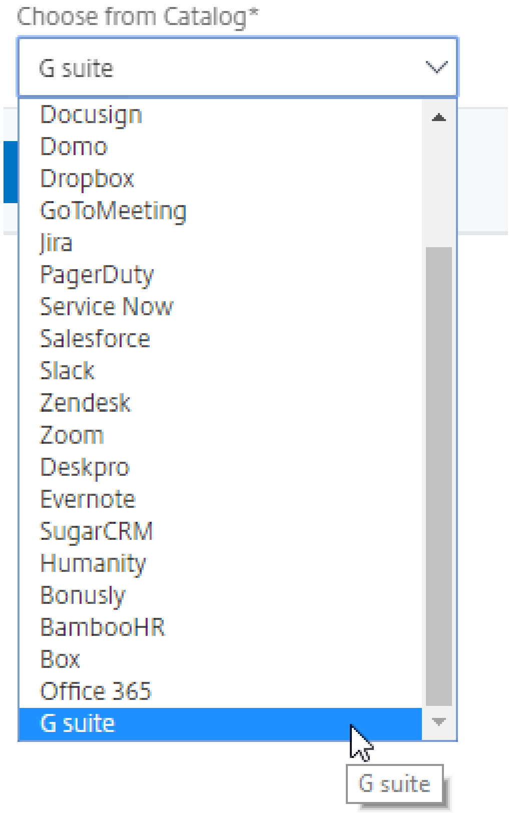
● SaaS

Select to provide access to SaaS applications.

○ XenApp & XenDesktop

Select to provide access to hosted virtual resources.

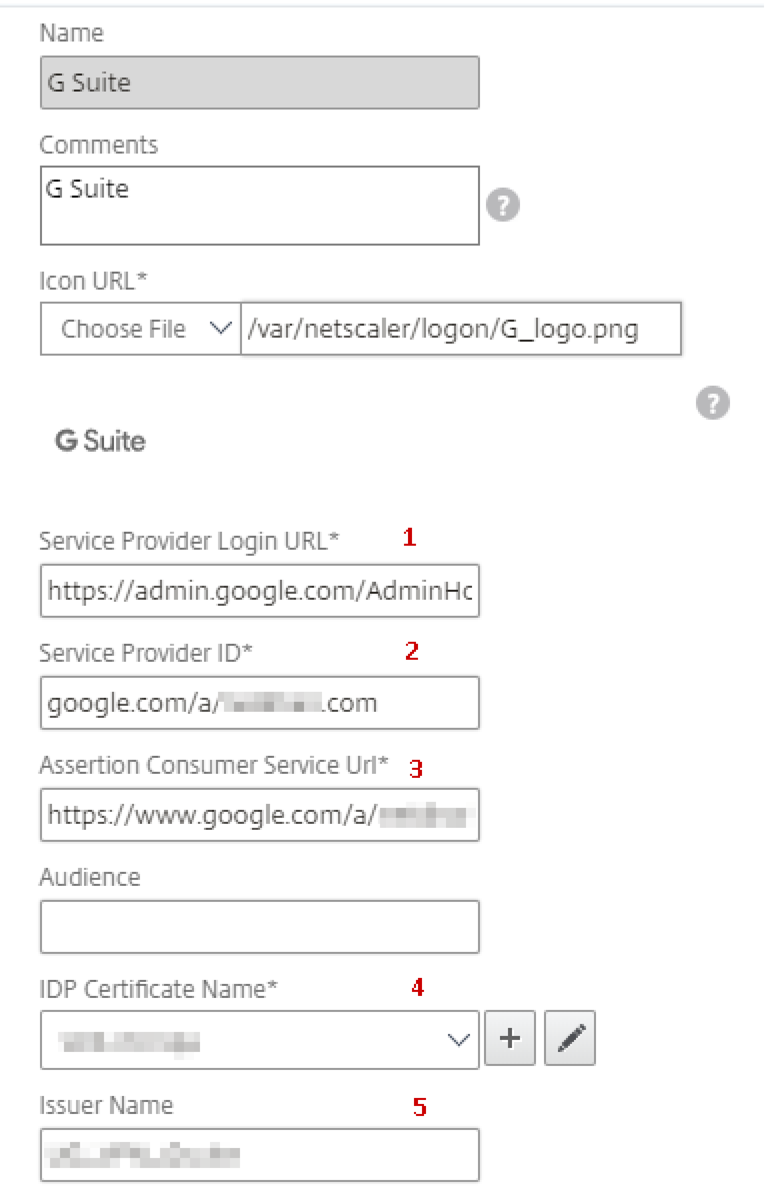
3. Select **SaaS** from the Application type.
4. Select **G Suite** from the drop-down list.



Choose from Catalog*

G suite

5. Fill the application template with the appropriate values.



Name
G Suite

Comments
G Suite

Icon URL*
/var/netscaler/logon/G_logo.png

Service Provider Login URL*
https://admin.google.com/AdminHc

Service Provider ID*
google.com/a/[redacted].com

Assertion Consumer Service Url*
https://www.google.com/a/[redacted]

Audience

IDP Certificate Name*
[redacted]

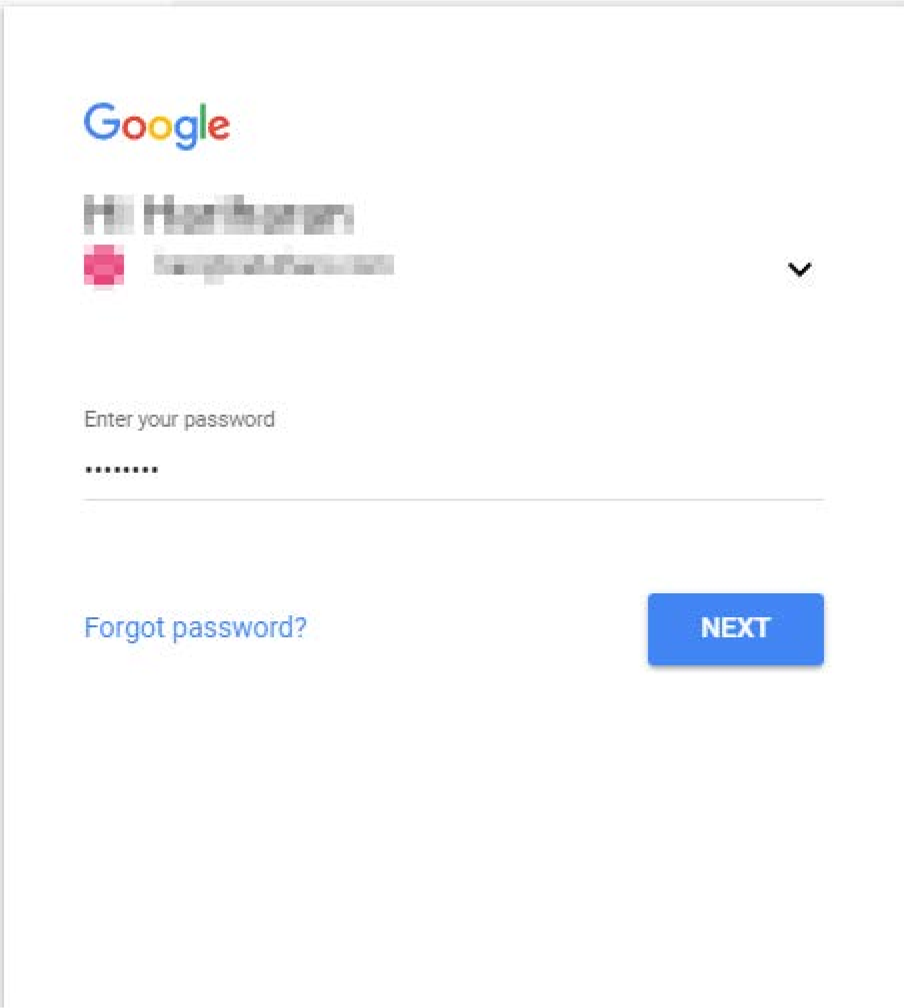
Issuer Name
[redacted]

6. You must update the fields in NetScaler with the following values:

Field Name	Values
URL	https://admin.google.com/AdminHome?hl=en&fral=1
Service Provider ID	google.com/a/<customer_domain>.com
ACS URL	https://www.google.com/a/<customer_domain>.com/acs
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

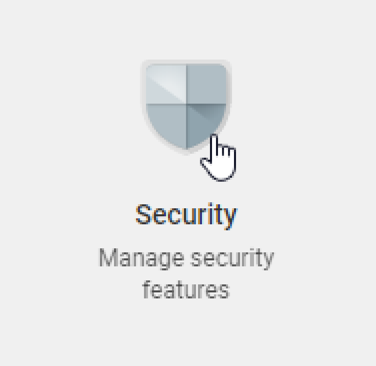
7. In place of <customer domain>, enter your company name (See **Introduction** to know more about the <customer domain> value.)
8. After providing the required values, click **Continue.** Click **Done.**

Step 2: Configure IdP into G Suite

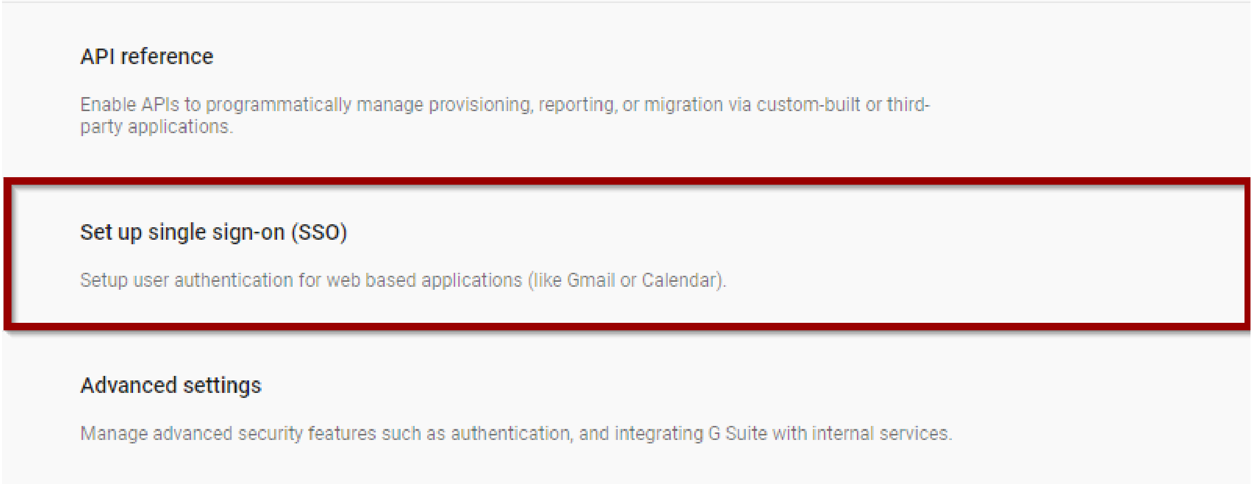


Enter your password
••••••••

1. Login to G Suite as an Admin user.



2. Click on **Security.**



API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

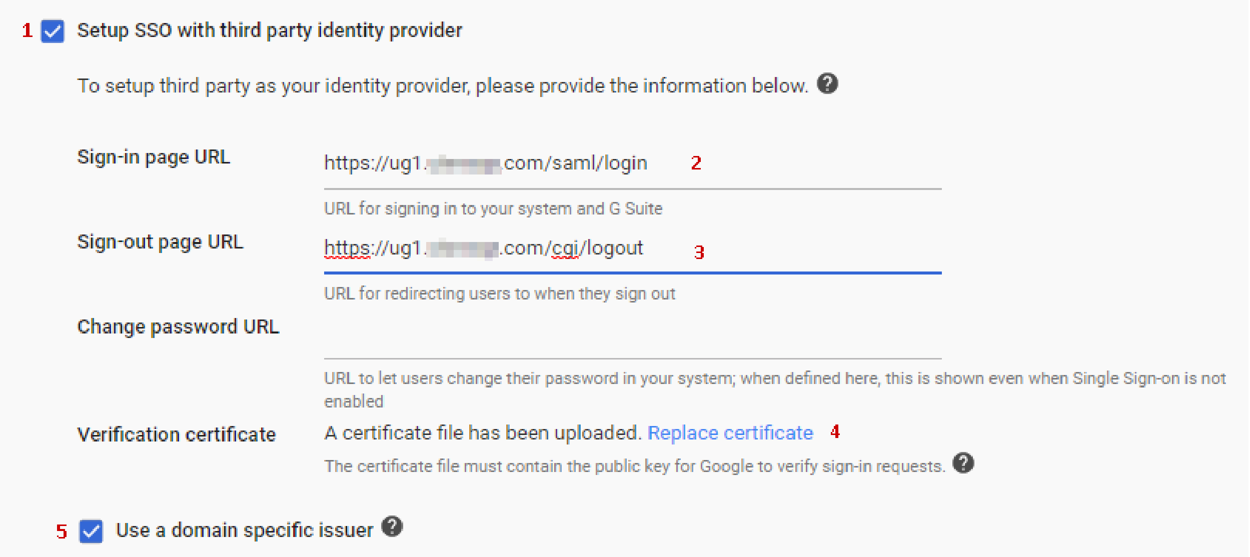
Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.

3. Security window will open. Click on **Set up single sign-on (SSO)**.



1 ☑ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below.

Sign-in page URL: https://ug1.[redacted]com/saml/login 2

URL for signing in to your system and G Suite

Sign-out page URL: https://ug1.[redacted].com/cgi/logout 3

URL for redirecting users to when they sign out

Change password URL:

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

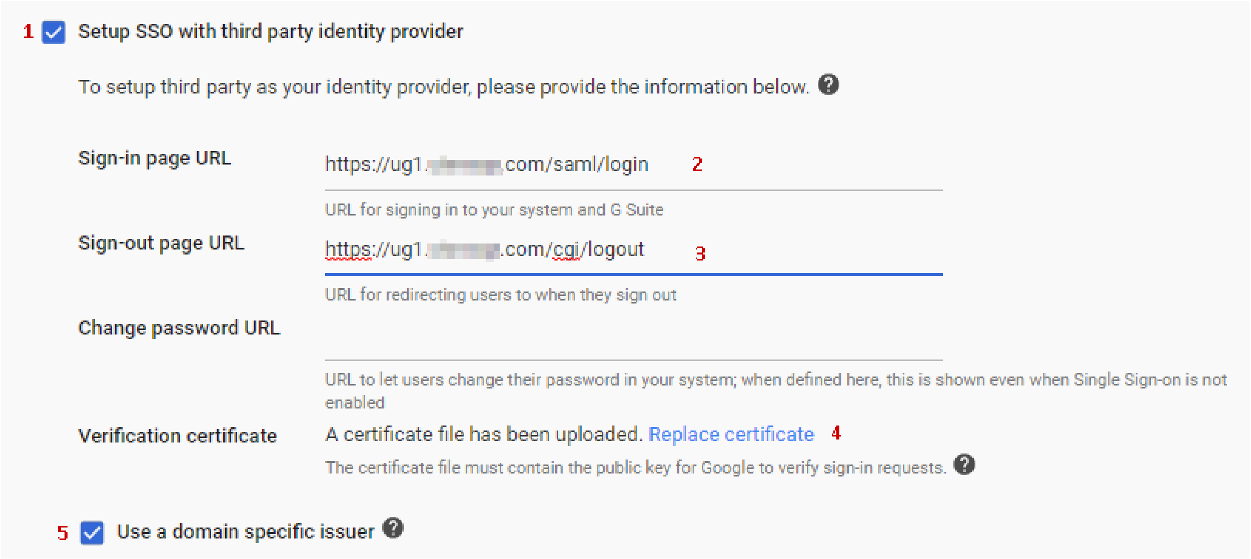
Verification certificate: A certificate file has been uploaded. Replace certificate 4

The certificate file must contain the public key for Google to verify sign-in requests.

5 ☑ Use a domain specific issuer

4. Fill the fields with the following values:-

Field Name	Values
Setup SSO with third party IdP	Should be checked
Sign-in page URL	https://ug1.<customer_domain>.com/saml/login
Sign-out page URL	https://ug1.<customer_domain>.com/cgi/logout
Verification Certificate	IdP certificate needs to be uploaded
Use a domain specific issuer	Should be checked



1 ☑ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below.

Sign-in page URL: https://ug1.[redacted].com/saml/login 2

URL for signing in to your system and G Suite

Sign-out page URL: https://ug1.[redacted].com/cgi/logout 3

URL for redirecting users to when they sign out

Change password URL:

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate: A certificate file has been uploaded. Replace certificate 4

The certificate file must contain the public key for Google to verify sign-in requests.

5 ☑ Use a domain specific issuer

5. Fill the fields with the following values:

Field Name	Values
Setup SSO with third party IdP	Should be checked
Sign-in page URL	https://ug1.<customer_domain>.com/saml/login
Sign-out page URL	https://ug1.<customer_domain>.com/cgi/logout
Verification Certificate	IdP certificate needs to be uploaded
Use a domain specific issuer	Should be checked