



NetScaler with Unified Gateway

Configuring Expensify

Contents

- CONTENTS 1
- DISCLAIMER (DOCUMENTATION) 2
- PREFACE 3
- OVERVIEW 4
- CONFIGURING EXPENSIFY FOR SINGLE SIGN-ON 5

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.

Expensify can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to Expensify 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 Expensify for Single Sign-On

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

Before you start, you need the following:

- Admin account for Expensify
- Customer instance

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

This is required for App Catalog creation in NetScaler.

- Admin account for NetScaler

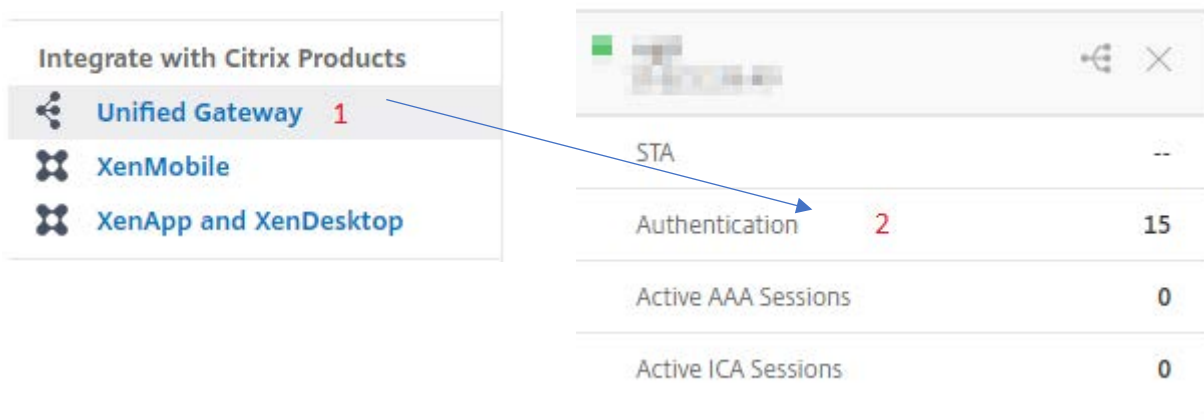
Expensify Configuration

The Expensify configuration steps are as follows:

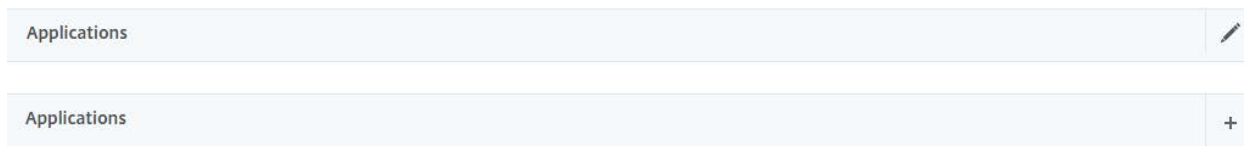
1. Configure Expensify with the App Catalog.
2. Export Expensify IdP metadata from NetScaler and edit
3. Configure IdP into Expensify.



Step 1: Configure Expensify with App Catalog

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



The **Unified Gateway Configuration** screen appears.



2. Go to **Applications** section. Click on  icon. Now, you can see  icon. Click on it. The **Application** window appears.

The image shows a dialog box titled 'Application'. It contains a section 'Choose Type*' with three radio button options: 'Web Application', 'SaaS', and 'XenApp & XenDesktop'. The 'SaaS' option is selected and highlighted in yellow. Below the options are 'Continue' and 'Cancel' buttons.

Application

Choose Type*

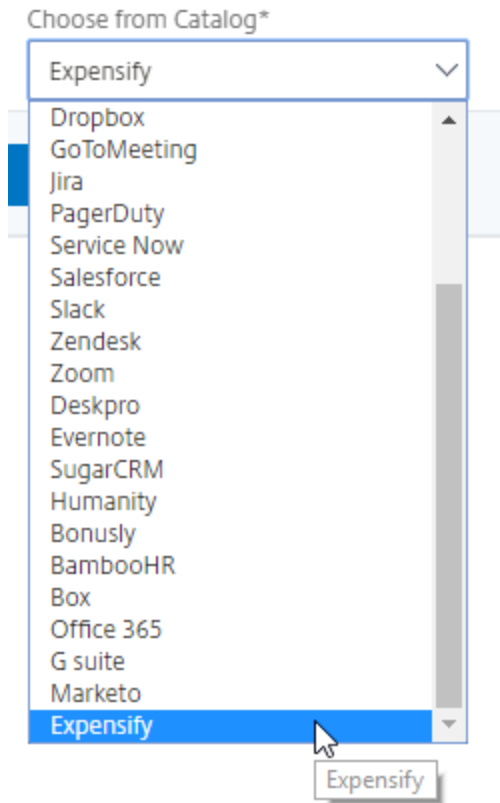
Web Application
Select to provide access to Enterprise applications.

SaaS
Select to provide access to SaaS applications.

XenApp & XenDesktop
Select to provide access to hosted virtual resources.

Continue Cancel

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




5. Fill the application template with the appropriate values.

Name
Expensify

Comments
Expensify ?

Icon URL*
Choose File ▾ /var/netScaler/logon/expensify_logc ?



Service Provider Login URL*
https://www.expensify.com/inbox

Service Provider ID* 1
https://www.expensify.com

Assertion Consumer Service Url* 2
https://www.expensify.com/authent

IDP Certificate Name* 3
[blurred] ▾ + ✎

Issuer Name 4
UG_VPN_Expensify

Continue Cancel

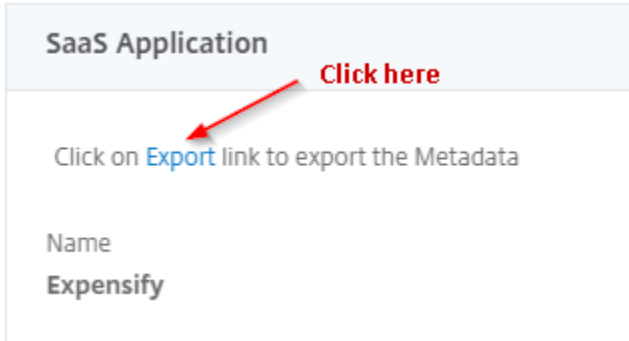
6. You must update the fields in NetScaler with the following values:

Field Name	Values
Service Provider ID	https://www.expensify.com
ACS URL	<a href="https://www.expensify.com/authentication/saml/loginCallback?domain=<customer_domain>.com">https://www.expensify.com/authentication/saml/loginCallback?domain=<customer_domain>.com
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

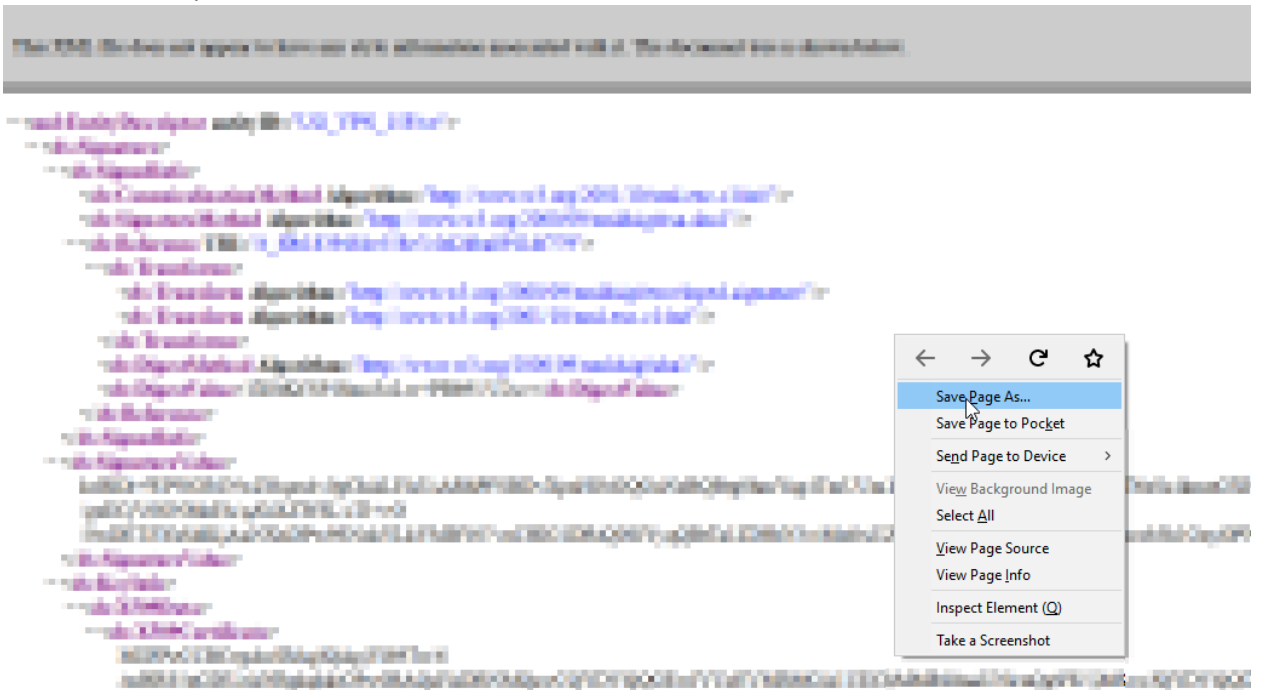
- In place of <customer domain>, enter your company name (See **Introduction** to know more about the <customer domain> value.)
- After providing the required values, click **Continue**. Click **Done**.

Step 2: Export Expensify IdP metadata from NetScaler and edit.

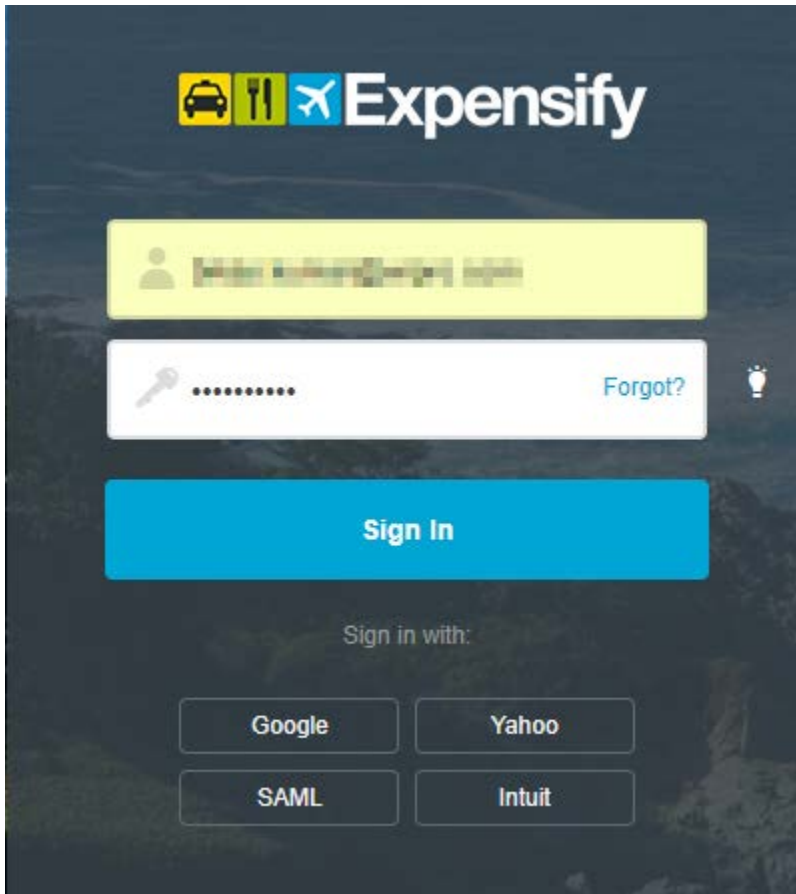
1. Click on **Unified Gateway > Authentication**.
2. Scroll down and click on **Expensify** template. The **SaaS Application** window appears. Click on **Export** link.



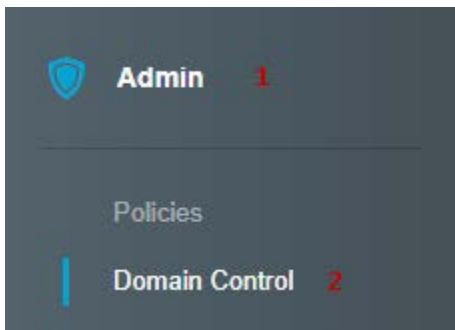
3. **Metadata** will open in a different window. Save the **IdP Metadata** file.



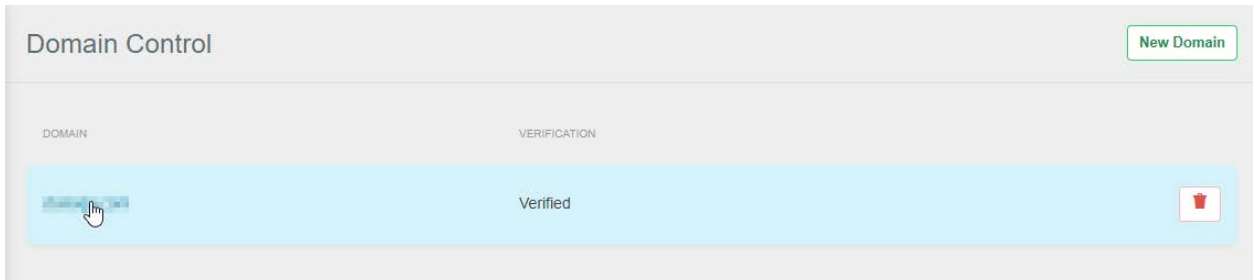
Step 3: Configure IdP into Expensify



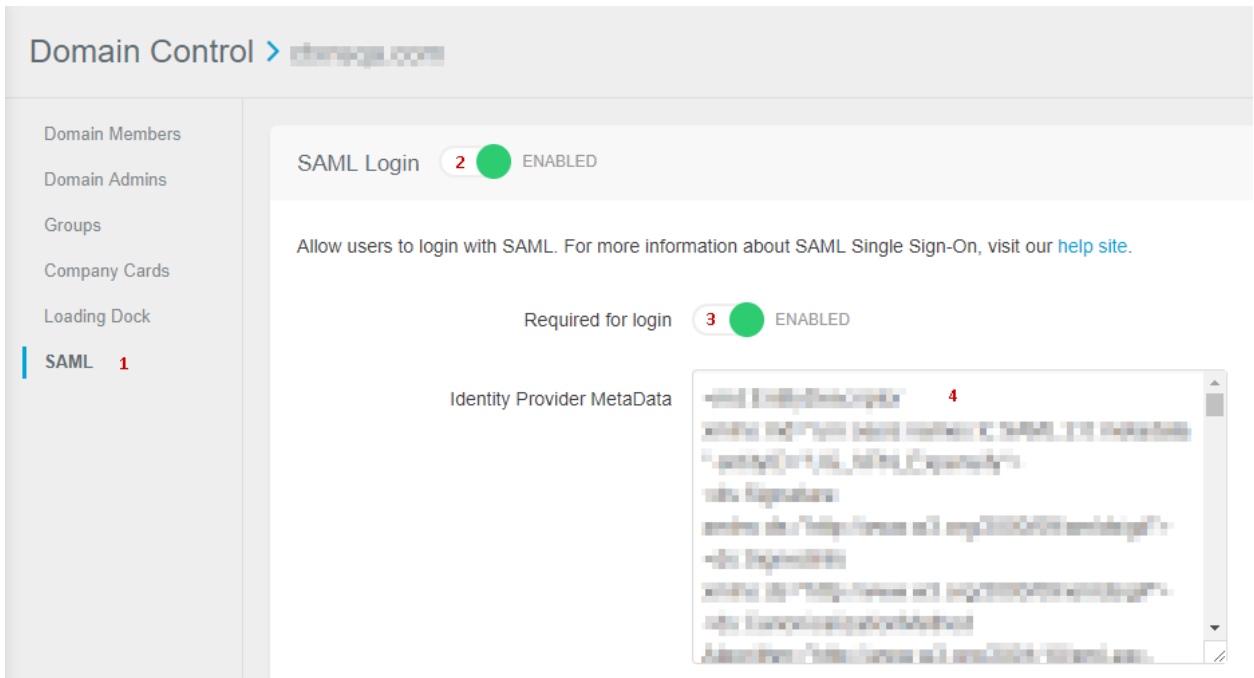
1. Login to Expensify as an Admin user.



2. From the left panel select **Admin** > Click on **Domain Control**.



3. **Domain Control** window will open > Click on your domain.



4. Your domain will open > Click on **SAML** from the left panel > Enable **SAML Login** > Enable **Required for login** > Paste IdP metadata (as shown in **Step 2**) in the **Identity Provider Metadata** field.