



# **NetScaler with Unified Gateway**

## **Configuring Workplace**

# Contents

CONTENTS .....	1
DISCLAIMER (DOCUMENTATION) .....	2
PREFACE .....	3
OVERVIEW .....	4
CONFIGURING WORKPLACE 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
<b>Bold</b>	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.
<b>Note</b>	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.

Workplace can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to Workplace 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**

<b>Service Provider (SP)</b>	<b>Identity Provider (IdP)</b>
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

# Configuring Workplace for Single Sign-On

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

Before you start, you need the following:

- Admin account for Workplace
- Customer instance

For example, if your deployment url [https://ug1.<customer\\_domain>.com/saml/login](https://ug1.<customer_domain>.com/saml/login), your customer instance is *<customer domain>*.

This is required for App Catalog creation in NetScaler.

- Admin account for NetScaler

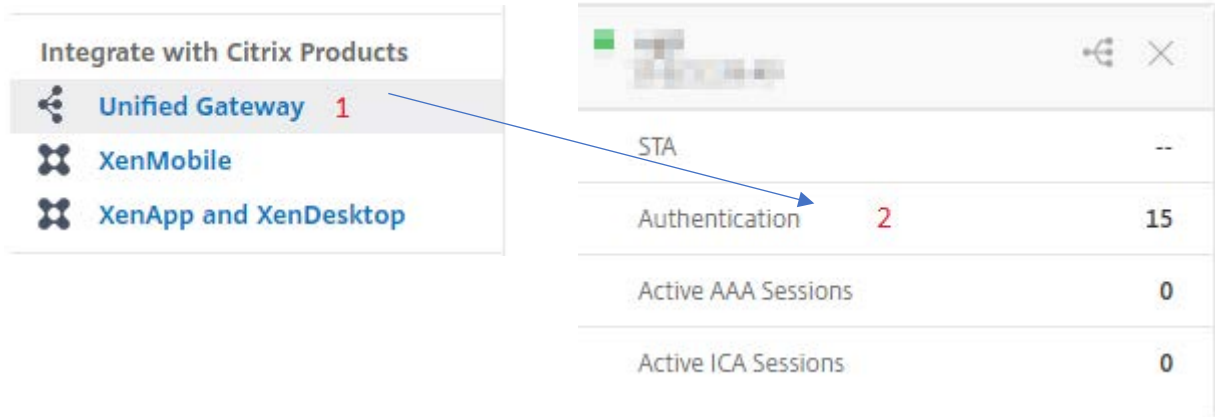
## Workplace Configuration

The Workplace configuration steps are as follows:

1. Configure Workplace with the App Catalog.
2. Configure IdP into Workplace.



## Step 1: Configure Workplace 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.

### 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 **Workplace** from the drop-down list.

Choose from Catalog\*

Workplace

- Box
- Cedexis
- Deskpro
- Evernote
- Expensify
- Freshdesk
- Freshservice
- G Suite
- Humanity
- Mango Apps
- Marketo
- Mingle
- Office365
- Salesforce
- Samanage
- Sumo Logic
- Tableau
- Workplace**
- Zoho
- AWS Console

Workplace

5. Fill the application template with the appropriate values.



Name  
Workplace

Comments  
An online team collaboration tool using Facebook features for work ?

Icon URL\*  
Choose File ▾ /var/netscaler/logon/Workplaceicon



Service Provider Login URL\* **1**  
https://workplace.facebook.com/wc

Service Provider ID\* **2**  
https://www.facebook.com/compar

Audience **3**  
https://www.facebook.com/compar

IDP Certificate Name\* **4**  
[Redacted] ▾ + ✎

Issuer Name **5**  
UG\_VPN\_FBWorkplace

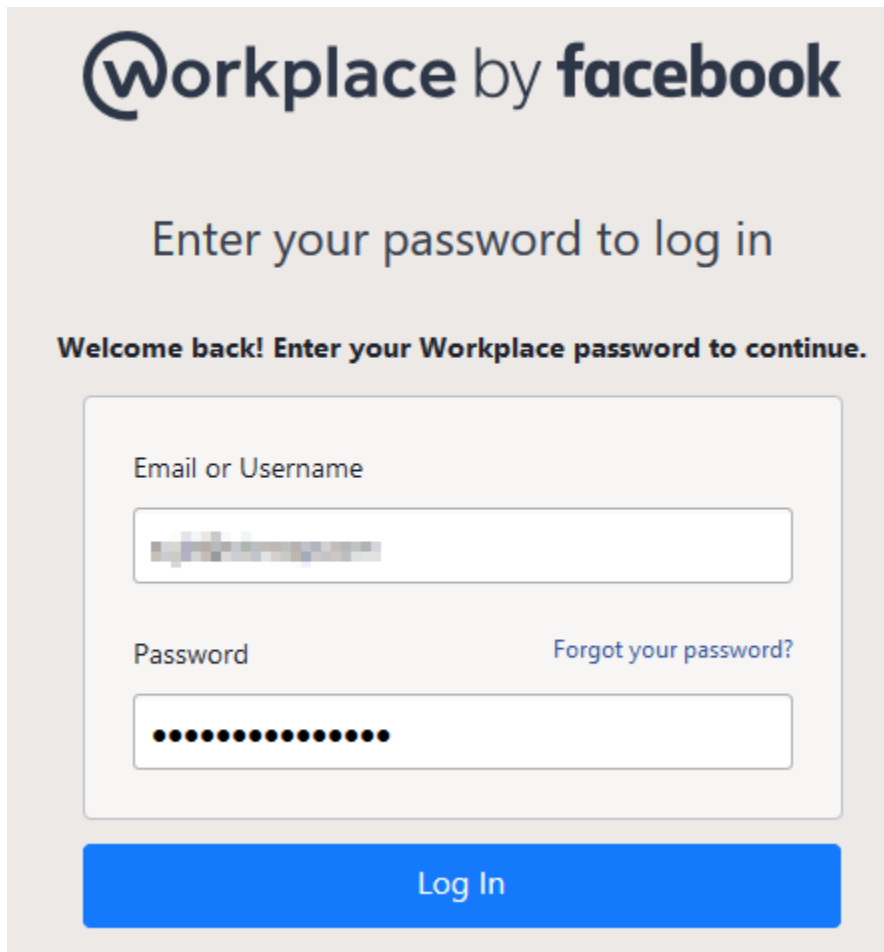
**Continue** Cancel

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

Field Name	Values
URL	<a href="https://workplace.facebook.com/work/saml.php">https://workplace.facebook.com/work/saml.php</a>
Service Provider ID	<a href="https://www.facebook.com/company/&lt;customer_id&gt;">https://www.facebook.com/company/&lt;customer_id&gt;</a>
Audience	<a href="https://www.facebook.com/company/&lt;customer_id&gt;">https://www.facebook.com/company/&lt;customer_id&gt;</a>
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

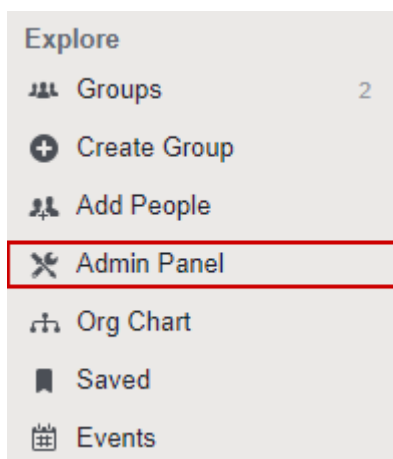
7. In place of <customer id>, enter your customer id (See **Step 2** to know more about the <customer id> value.)
8. After providing the required values, click **Continue**. Click **Done**.

## Step 2: Configure IdP into Workplace

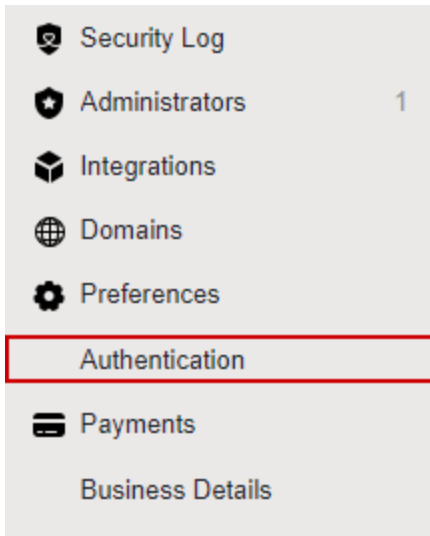


The image shows the Workplace by Facebook login interface. At the top is the logo "Workplace by facebook". Below it, the text "Enter your password to log in" is displayed. A message reads "Welcome back! Enter your Workplace password to continue." There are two input fields: "Email or Username" and "Password". The "Password" field is masked with dots. A link "Forgot your password?" is located to the right of the password field. A blue "Log In" button is at the bottom.

1. Login to Workplace as an Admin user.



2. Select **Admin Panel** from the left panel under the tab **Explore**.



3. **Admin Panel** window will open > Select **Authentication** from the left panel under the tab **Preferences**.

<b>Login</b>	Allow people to log in with: <input checked="" type="checkbox"/> Password <input checked="" type="checkbox"/> SSO <small>This lets you decide how everyone in your organization logs in. If you select both, you'll be able to choose how each person logs in individually.</small> Default for new users: Password + ⓘ	1
<b>SAML Authentication</b>	In web browsers, check SAML again after: 1 day ▾ <input checked="" type="checkbox"/> Require SAML in mobile apps ⓘ Log people out of mobile apps after: Never ▾  Require SAML authentication for all users now	2
<b>SAML URL</b>	https://ug1.████████.com/saml/login ⓘ	3
<b>SAML Issuer URI</b>	UG_VPN_FBWorkplace ⓘ	4
<b>SAML Logout Redirect</b>	<input checked="" type="checkbox"/> Enable SAML Logout Redirection ⓘ https://ug1.████████.com/cgi/logout ⓘ	5

**SAML certificate**

```
-----BEGIN CERTIFICATE-----  
[Blurred Certificate Content]  
-----END CERTIFICATE-----
```

The certificate is valid for 122 days

**SAML configuration**

Audience URL

https://www.facebook.com/company/[Blurred]

Recipient URL

https://workplace.facebook.com/work/saml.php

ACS (Assertion Consumer Service) URL

https://workplace.facebook.com/work/saml.php

**Test SSO**

Customer id

**Save**

4. **Authentication Settings** window will open > Fill the template with appropriate values.

Field Name	Values
Login	Password & SSO should be checked
SAML Authentication	Required SAML in mobile apps should be checked
SAML URL	<a href="https://ug1.&lt;customer domain&gt;.com/saml/login">https://ug1.&lt;customer domain&gt;.com/saml/login</a>
SAML Issuer URI	As you mentioned in IdP
SAML Logout Redirect	Enable SAML Logout Redirection should be checked <a href="https://ug1.&lt;customer domain&gt;.com/cgi/logout">https://ug1.&lt;customer domain&gt;.com/cgi/logout</a>
SAML certificate	Paste IdP certificate

- 5. In place of <customer domain>, enter your company instance (See **Introduction** to know more about the <customer domain> value.)
- 6. Test the configuration using the button **Test SSO**.
- 7. Click **Save**.