CITRIX

NetScaler with Unified Gateway

Configuring Workplace

Contents

Disclaimer (Documentation)

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.

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

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 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, your customer instance is <*customer domain*>.

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

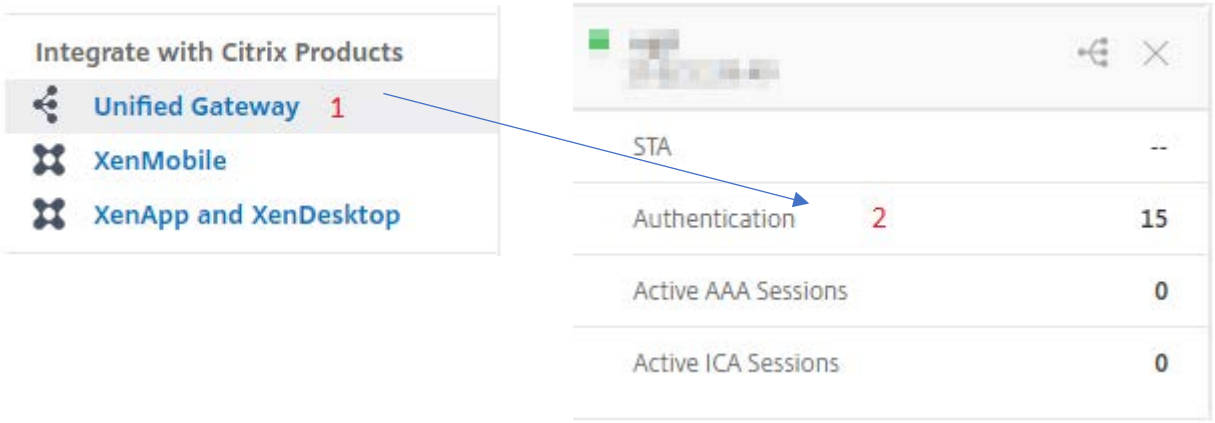
Workplace Configuration

The Workplace configuration steps are as follows:

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

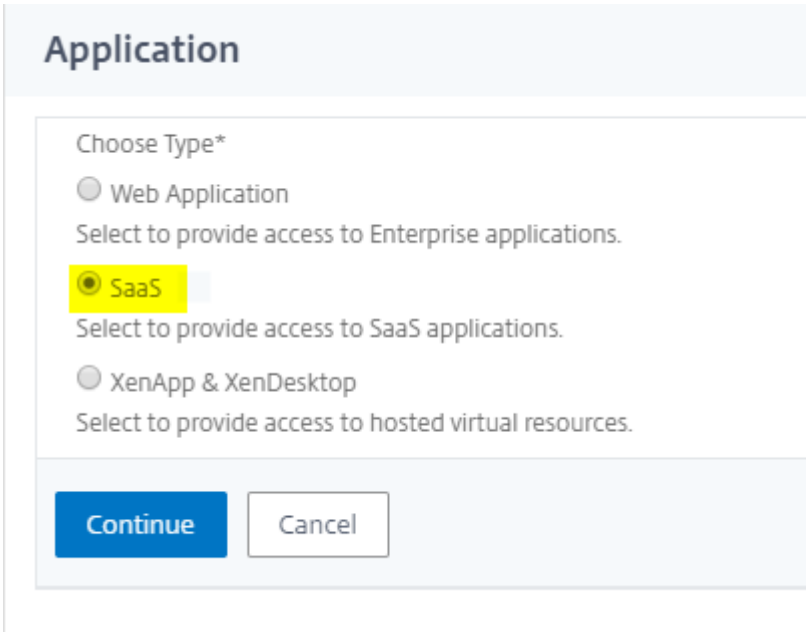
Step 1: Configure Workplace with App Catalog

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

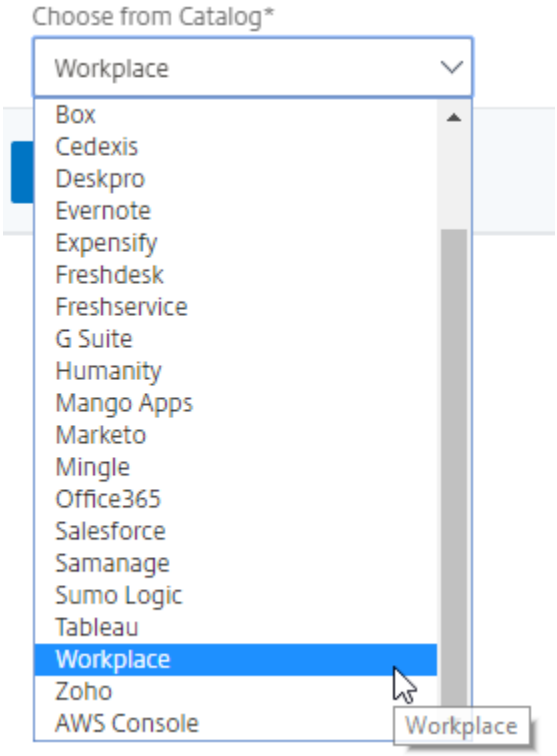


The **Unified Gateway Configuration** screen appears.

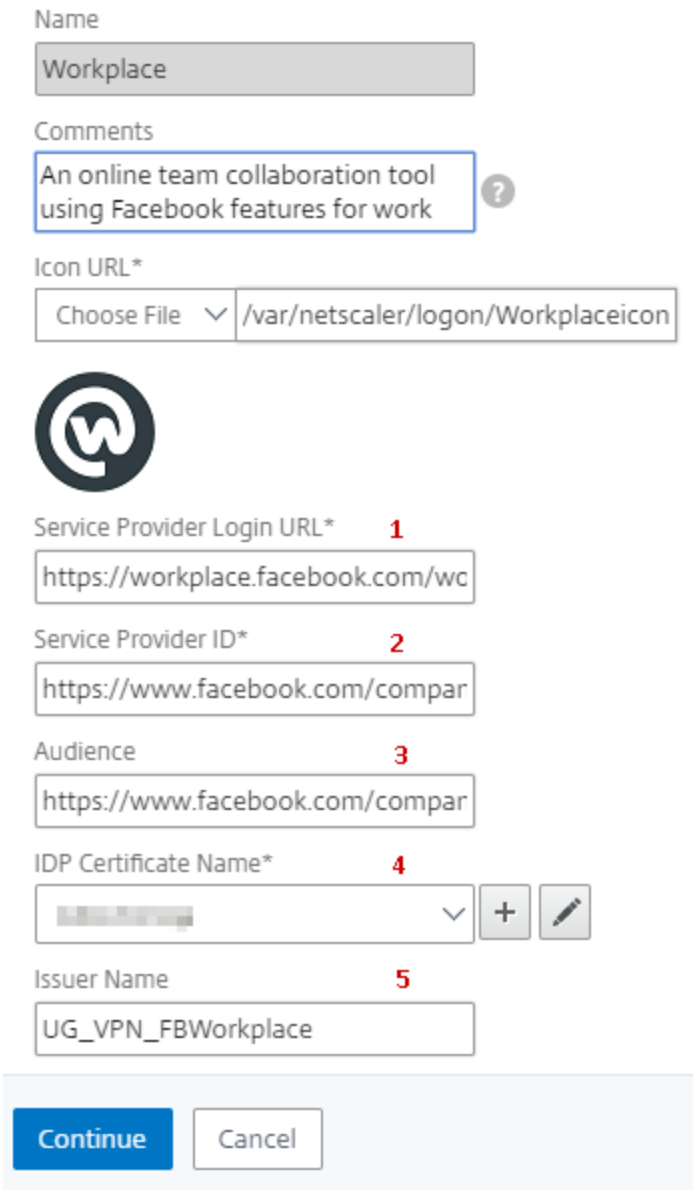
2. Go to **Applications** section. Click on icon. Now, you can see + icon**.** Click on it. The **Application** window appears.



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



5. Fill the application template with the appropriate values.

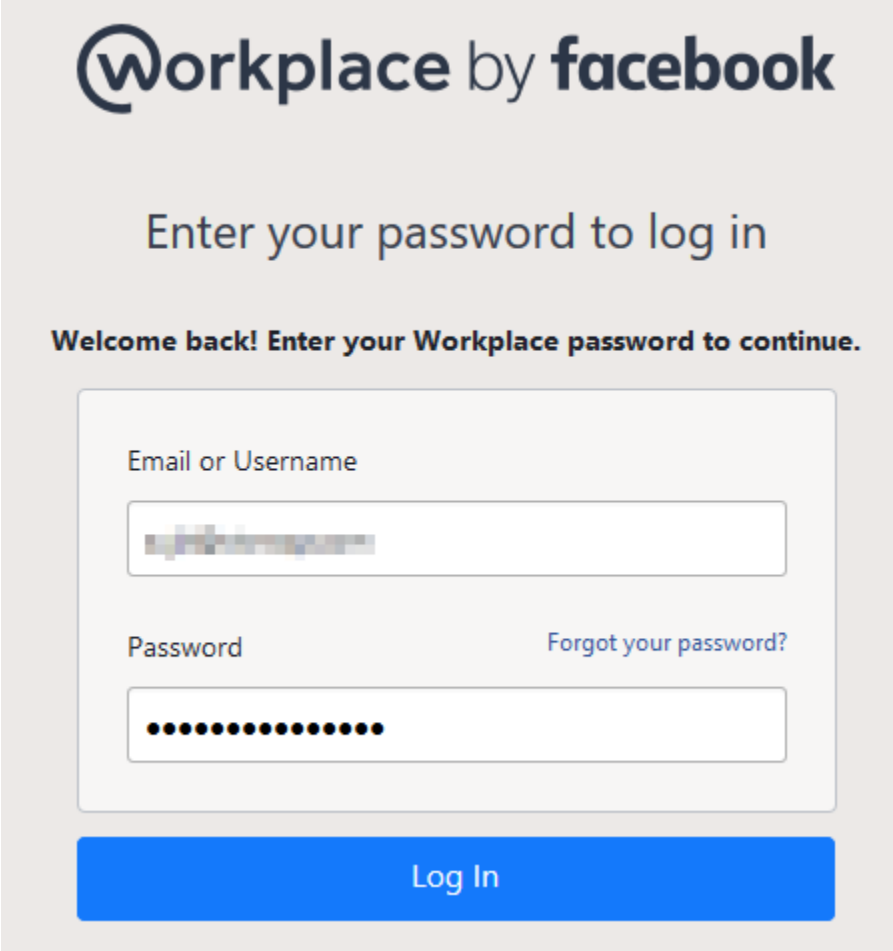


6. You must update the fields in NetScaler with the following values:

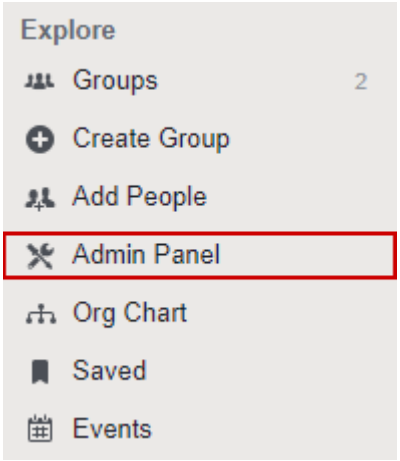
Field Name	Values
URL	https://workplace.facebook.com/work/saml.php
Service Provider ID	https://www.facebook.com/company/<customer_id>
Audience	https://www.facebook.com/company/<customer_id>
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your 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.**

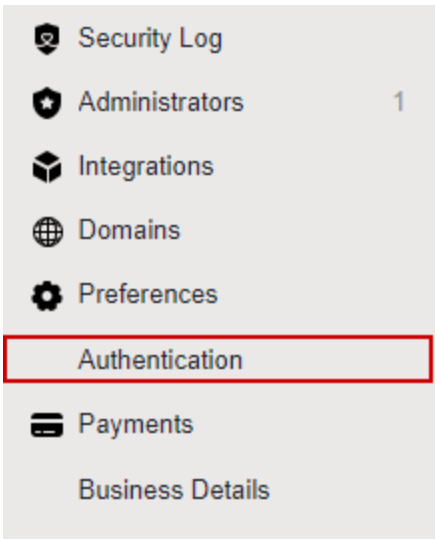
Step 2: Configure IdP into Workplace



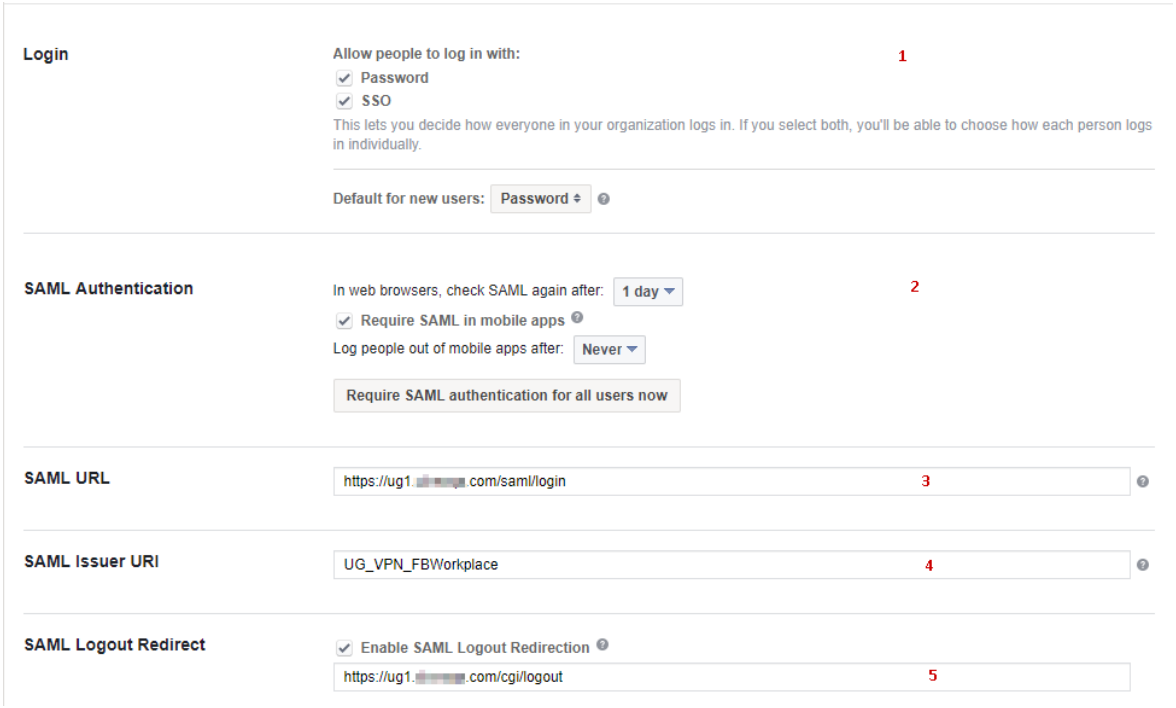
1. Login to Workplace as an Admin user.

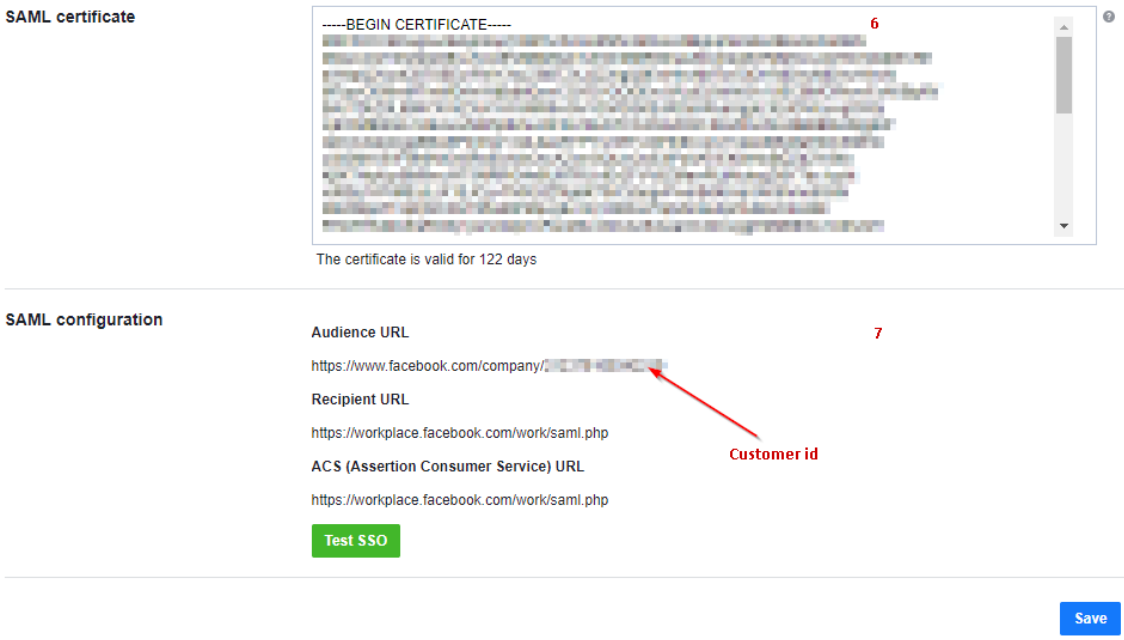


2. Select **Admin Panel** from the left panel under the tab **Explore.**



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





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	https://ug1.<customer_domain>.com/saml/login
SAML Issuer URI	As you mentioned in IdP
SAML Logout Redirect	Enable SAML Logout Redirection should be checked https://ug1.<customer_domain>.com/cgi/logout
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.**