CITRIX

NetScaler with Unified Gateway

Configuring Mango

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.

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

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

Before you start, you need the following:

- Admin account for Mango
- Customer instance

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

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

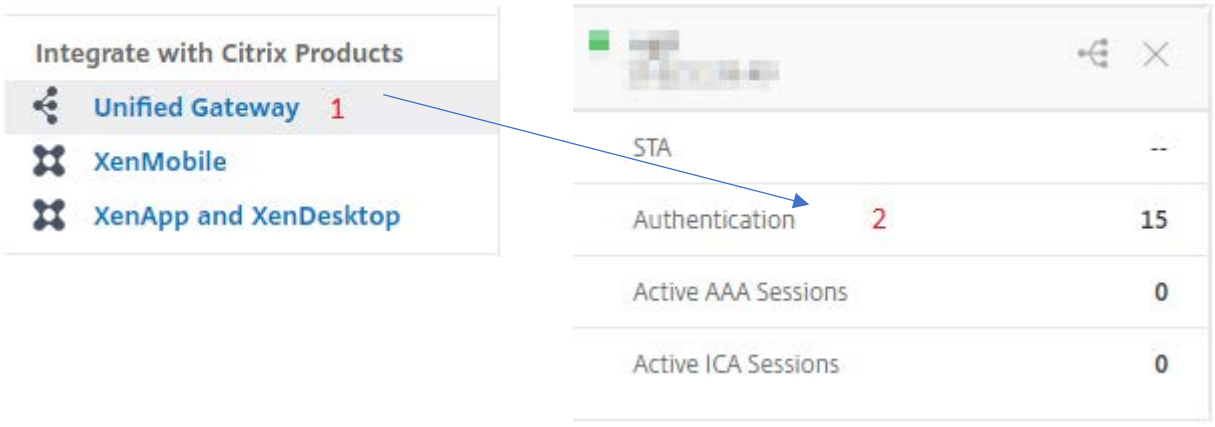
Mango Configuration

The MangoApps configuration steps are as follows:

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

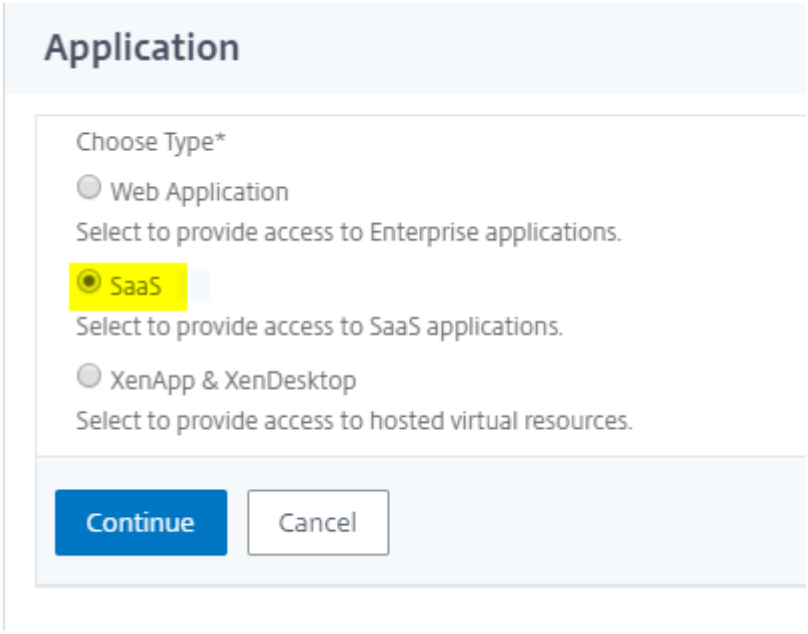
Step 1: Configure MangoApps with App Catalog

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

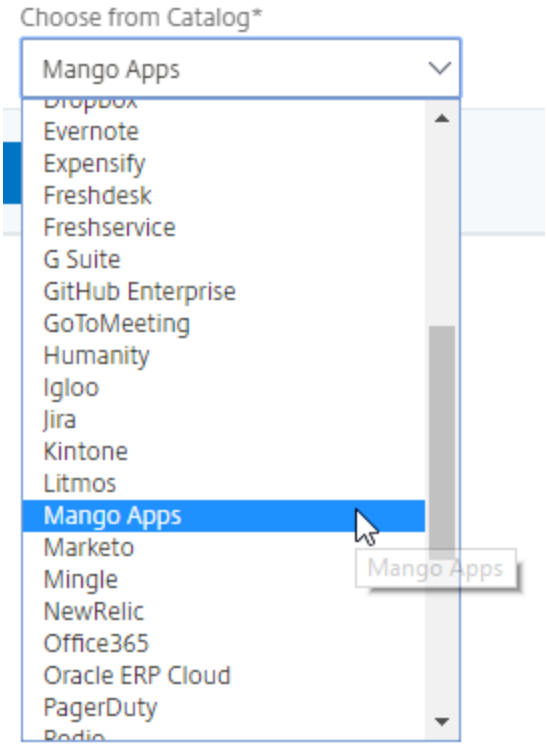


The **Unified Gateway Configuration** screen appears.

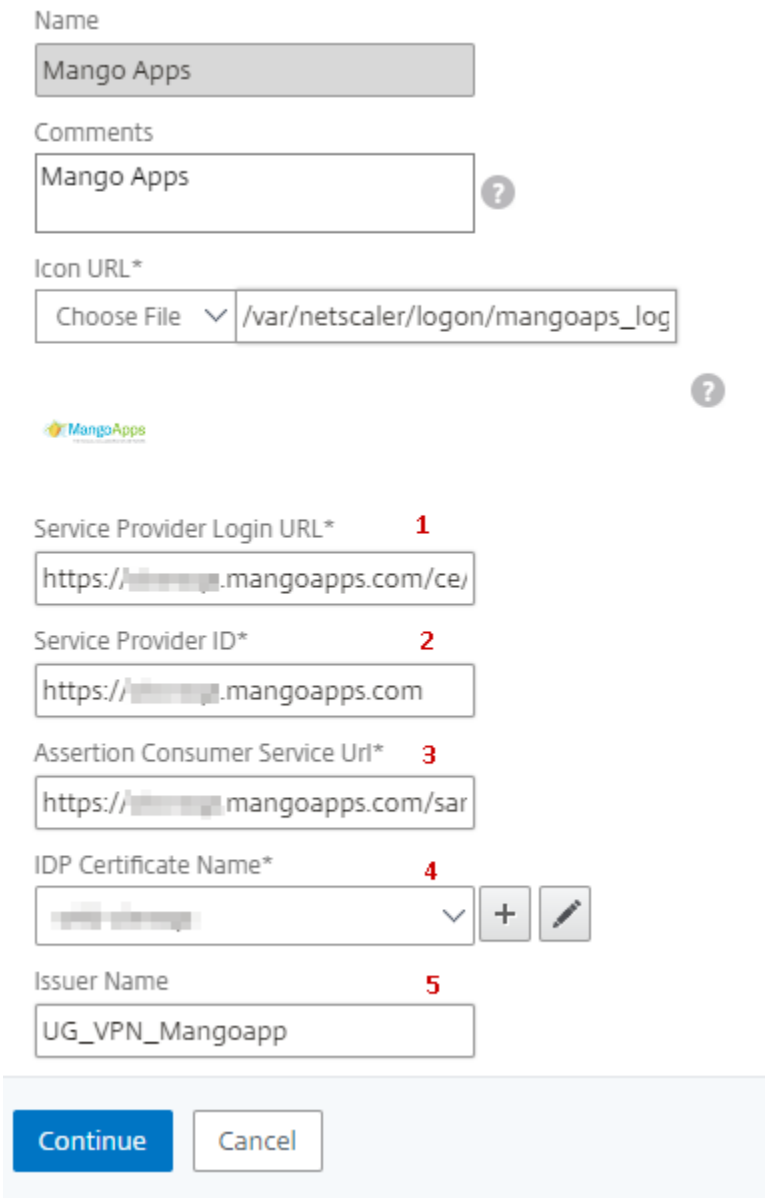
2. Go to **Applications** section. Click on icon. Now, you can see icon**.** Click on it. The **Application** window appears.



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



5. Fill the application template with the appropriate values.

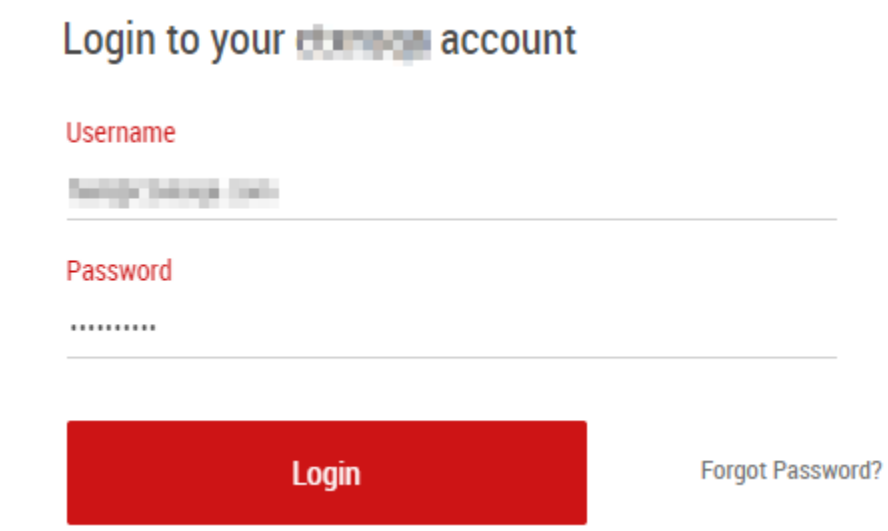


6. You must update the fields in NetScaler with the following values:

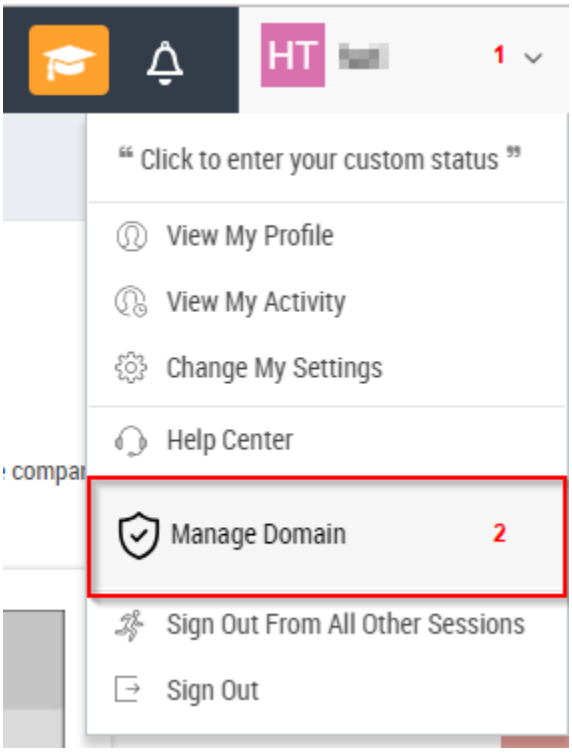
Field Name	Values
URL	https://<customer_domain>.mangoapps.com/ce/pulse/user/overview/index
Service Provider ID	https://<customer_domain>.mangoapps.com
ACS URL	https://<customer_domain>.mangoapps.com/saml/consume
Signing Certificate Name	IdP certificate needs to be selected
Issuer Name	Issuer name can 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 MangoApps

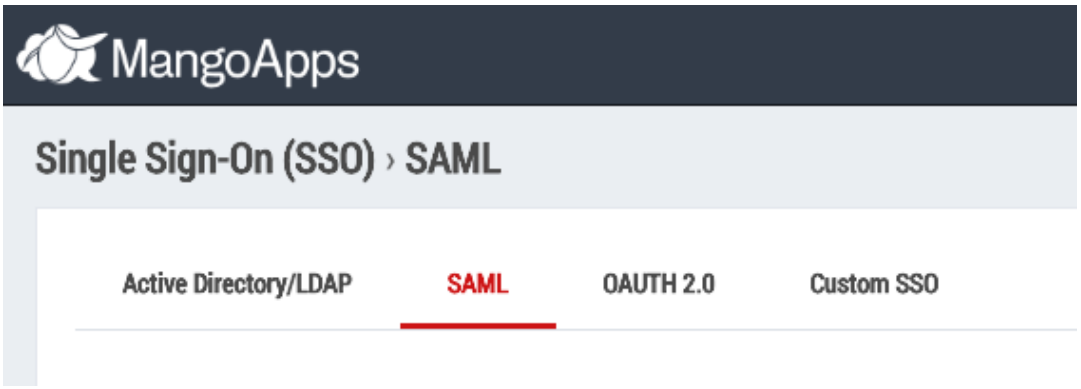


1. Login to MangoApps as an Admin user.

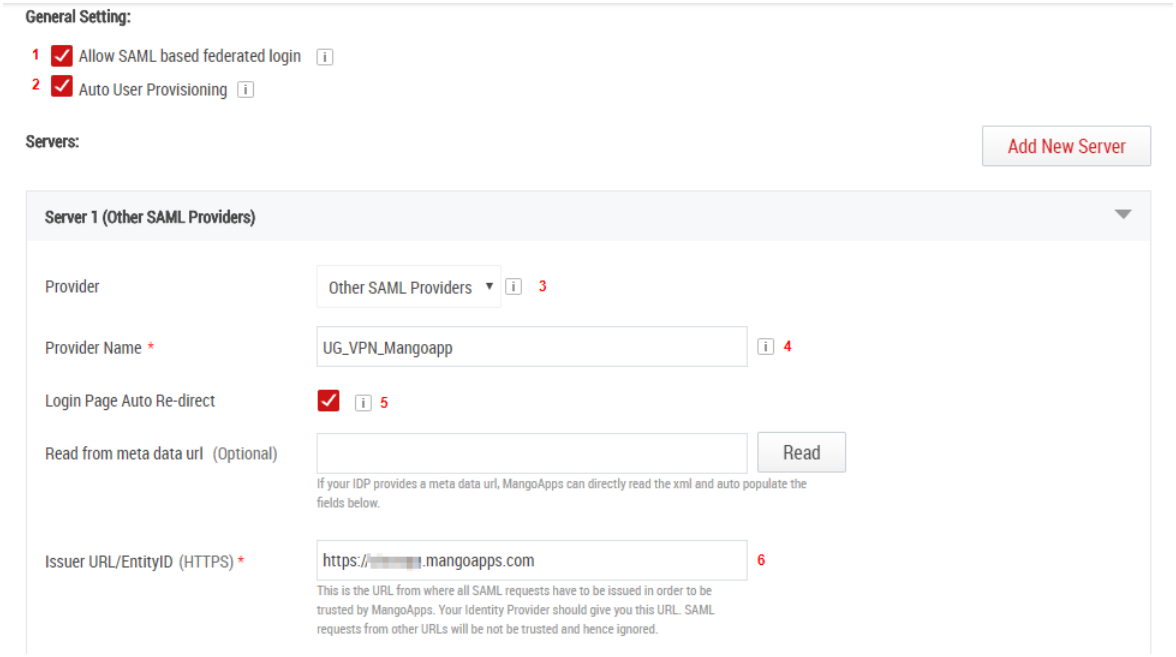


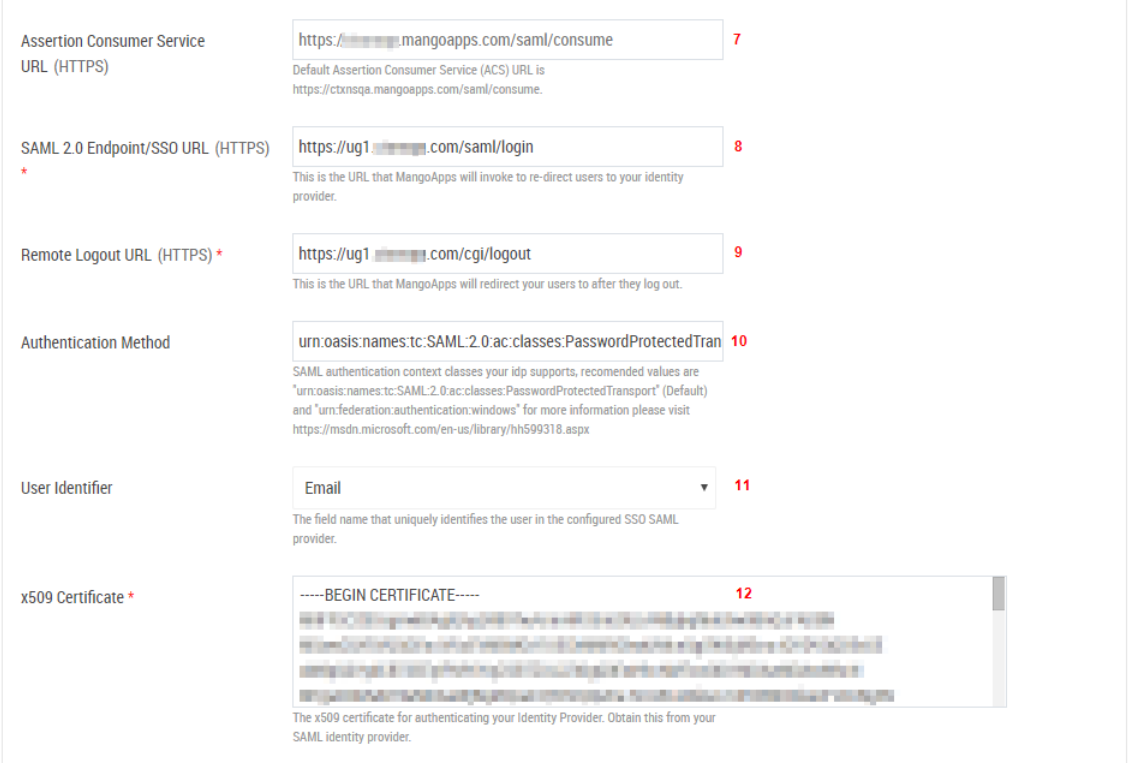
2. From the top right corner move cursor on your account name **>** List will appear, Click on **Manage Domain**.

3. **Admin** window will open **>** From the left panel select **SSO**.



4. **Single Sign-On** window will open **>** Click on **SAML**.





5. **F**ill the template with appropriate values

Field Name	Values
Allow SAML based federated login	Should be **checked**
Auto User Provisioning	Should be **checked**
Provider	Other SAML Provider
Provider Name	As mentioned in IdP
Login Page Auto Re-direct	Should be **checked**
Issuer URL/EntityID(HTTPS)	https://<customer_domain>.mangoapps.com
Assertion Consumer Service URL(HTTPS)	https://<customer_domain>.mangoapps.com/saml/consume
SAML 2.0 Endpoint/SSO URL(HTTPS)	https://ug1.<customer_domain>.com/saml/login
Remote Logout URL(HTTPS)	https://ug1.<customer_domain>.com/cgi/logout
Authentication Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (Default)
User Identifier	Email
x509 Certificate	Paste IdP certificate

6. Click on **Save Settings**.