



NetScaler with Unified Gateway

Configuring DocuSign

Abstract

Configuring DocuSign for SSO enables administrators to manage their users using NetScaler.

Contents

- ABSTRACT0
- CONTENTS1
- DISCLAIMER (DOCUMENTATION)2
- PREFACE.....3
- OVERVIEW4
- CONFIGURING DOCUSIGN FOR SINGLE SIGN-ON4
- CONFIGURING NETSCALER FOR SINGLE SIGN-ON9
- TESTING THE CONFIGURATION.....16

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.

DocuSign provides electronic signature technology and digital transaction management services. DocuSign enables you to electronically sign documents, request signatures, check document status, send reminders, and view audit trails.

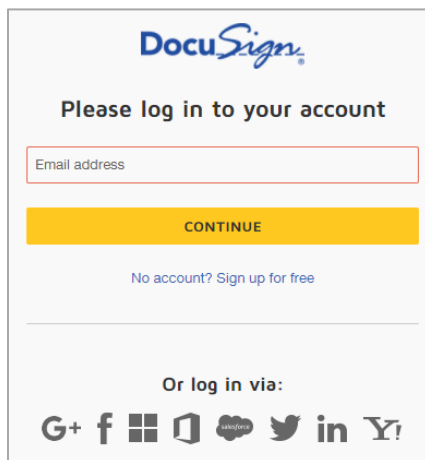
You can connect DocuSign with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring DocuSign for Single Sign-On

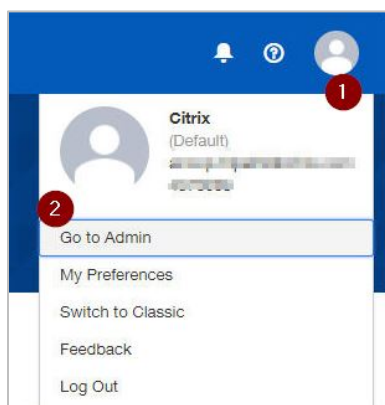
Configuring DocuSign for SSO enables administrators to manage their users using NetScaler. Users can securely log on to DocuSign using their enterprise credentials.

To configure DocuSign for SSO through SAML, follow the steps below:

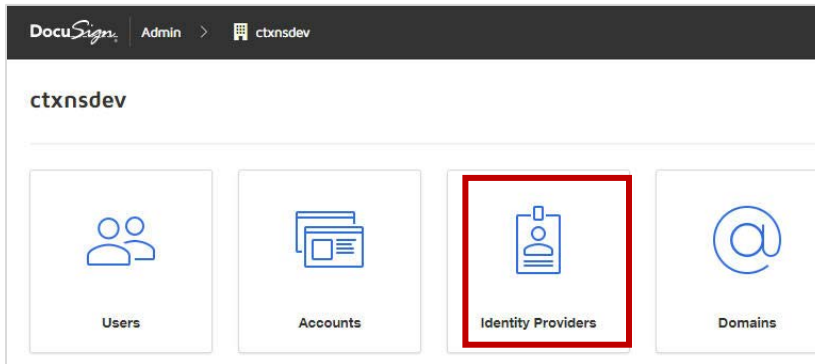
1. In a browser, type <https://account-d.docusign.com/#/username> and press enter.
2. Log on to your DocuSign account.



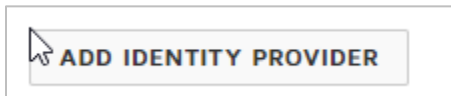
3. On the **Home** page, at the upper right corner, click your profile photo and then click **Go to Admin**.



4. Click **Identify Providers**.



5. Click **ADD IDENTITY PROVIDER**.



6. In the **Identity Provider Settings** area, specify the following information:

- **Name** - provide a unique name for the IdP provider. The name must help identify the identity provider
- **Identity Provider Issuer** - type a unique issuer ID. For example: `https://<company domain name>.com`
- **Identity Provider Login URL** - enter the IdP URL of your NetScaler app: `https://<NetScaler Gateway FQDN>/saml/login`
- **Identity Provider Logout URL** - enter `https://<NetScaler Gateway FQDN>/cgi/tmlogout`

A screenshot of the 'Identity Provider Settings' form. At the top, there are 'SAVE' and 'CANCEL' buttons. Below them, the 'SSO Protocol' is set to 'SAML 2.0'. There are five input fields: 'Name *', 'Identity Provider Issuer *', 'Identity Provider Login URL *', 'Identity Provider Logout URL', and 'Identity Provider Metadata URL'. The first four fields have red circles with numbers 1, 2, 3, and 4 respectively, indicating they are required. At the bottom, there are two checkboxes: 'Sign AuthN request' and 'Sign logout request', both of which are unchecked.

7. In the **Send AuthN request by** and **Send logout request by** area, click **POST**.

Send AuthN request by:

GET

POST **1**

Send logout request by:

GET

POST **2**

8. Click **ADD NEW MAPPING** for adding each attribute.

Custom Attribute Mapping

Please refer to the Identity Provider documentation for details on attribute mapping and default attribute name values.

Field	Attribute Name
+ ADD NEW MAPPING	

SAVE **CANCEL**

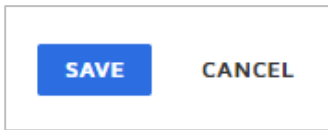
9. In the **Field** list, click the appropriate field and type the attribute name for the field in the **Attribute Name** box.

Custom Attribute Mapping

Please refer to the Identity Provider documentation for details on attribute mapping and default attribute name values.

Field	Attribute Name
1 emailaddress	emailaddress
2 givenname	givenname
3 surname	surname

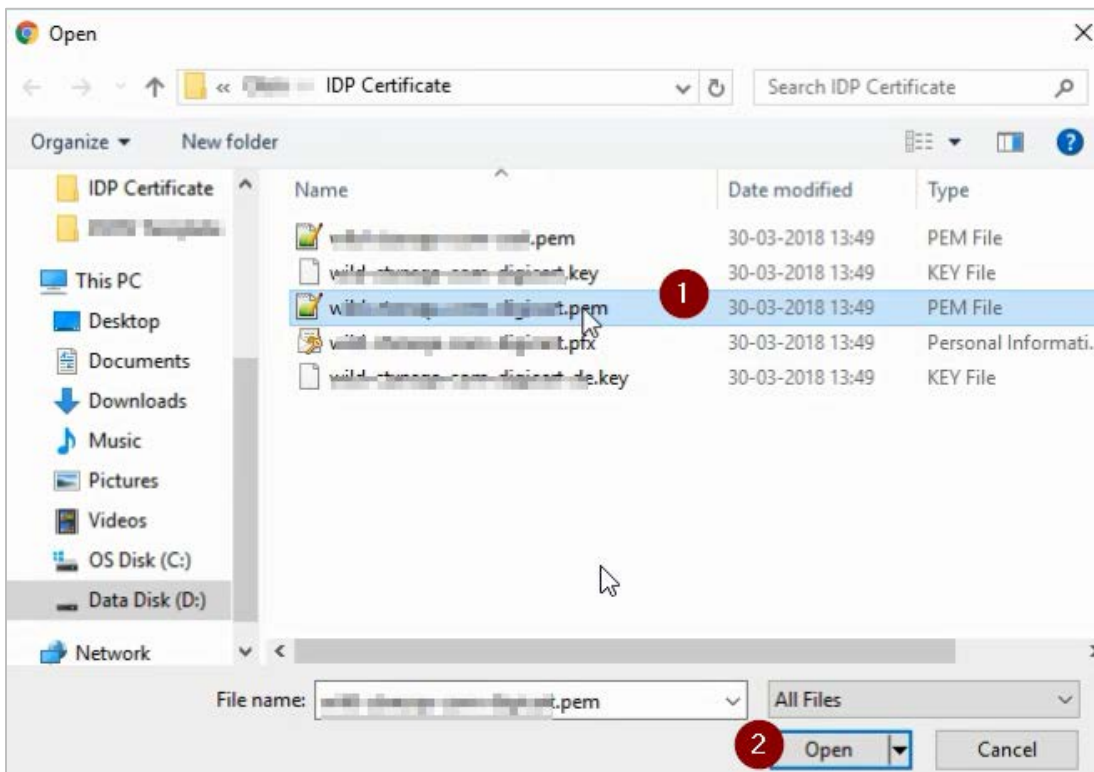
10. Click **SAVE**.



11. Click **ADD CERTIFICATE**.



12. Browse to the folder where you saved the IdP provided certificate.



13. Click the IdP digital certificate.

To obtain your IdP certificate, follow the steps below:

- i. Remotely access your NetScaler instance using PuTTY.
- ii. Navigate to /nsconfig/ssl folder (using shell command `cd /nsconfig/ssl`) and press Enter.
- iii. Type `cat <certificate-name>` and press Enter.

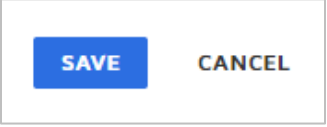

```
root@persistent# cd /nsconfig/ssl
root@persistent# cat adobe-sp.pem
-----BEGIN CERTIFICATE-----
MIIClzCCAkCgAwIBAgIGAWHYpNi8MAOGCSqGSIb3DQEEBQUAMIGuMQswCQYDVQQGEwJVUzETMBEG
A1I1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
4B1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
N1I1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
FA1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
cj1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
1k1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
oC1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
oa1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
N+1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
7x1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1Y2E1
0PrC4ydcwMxqGdFFSQ/LHWUPGvGlpHzj47MzcNOEbdrVmKF6le4/fTkVz3ST3U=
-----END CERTIFICATE-----

root@persistent# █
```

- iv. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
- v. Paste the text in a text editor and save the file in an appropriate format such as <your company name>.pem

14. After selecting a certificate, click **Open**.

15. Click **Save**.



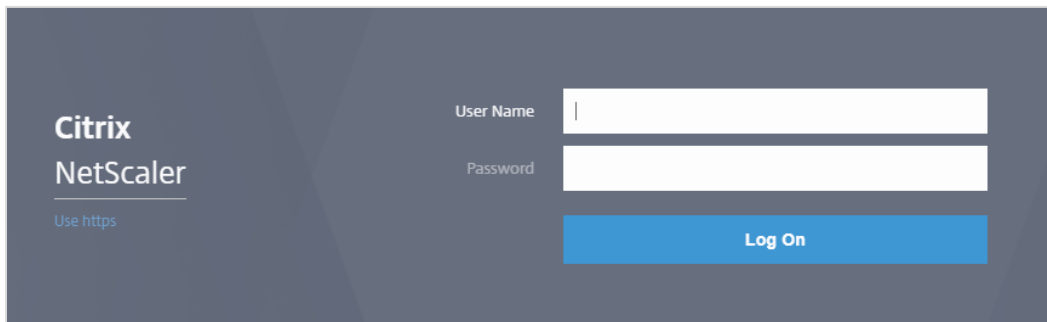
You have completed the required configuration on the service provider which is in this case – DocuSign.

Configuring NetScaler for Single Sign-On

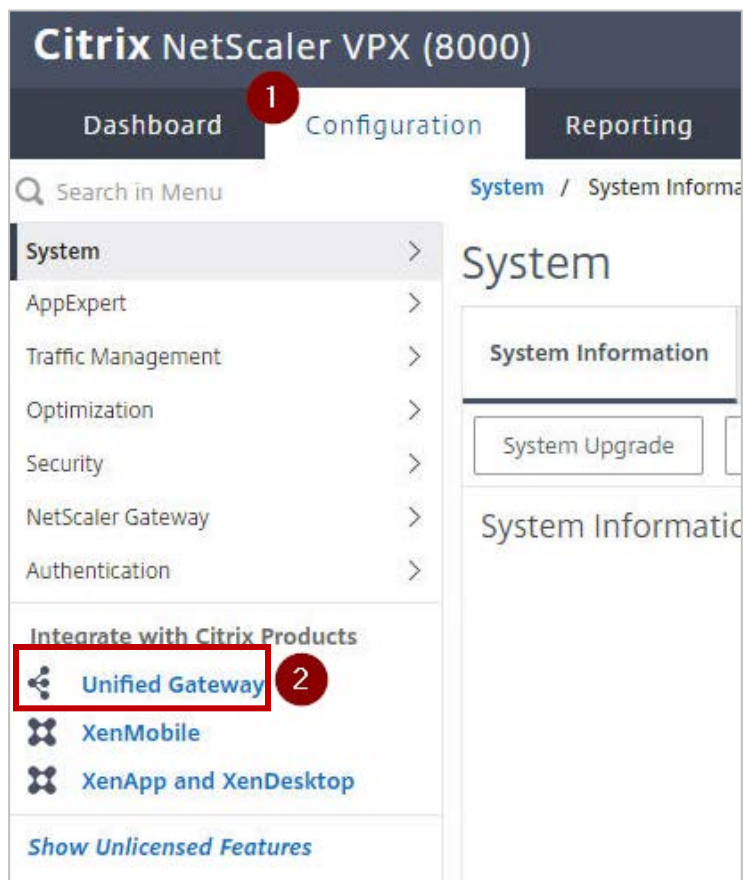
For configuring NetScaler for DocuSign, you must retrieve and set specific values such as assertion consumer URL, and entity ID.

To configure NetScaler for single sign on through SAML, complete the following steps:

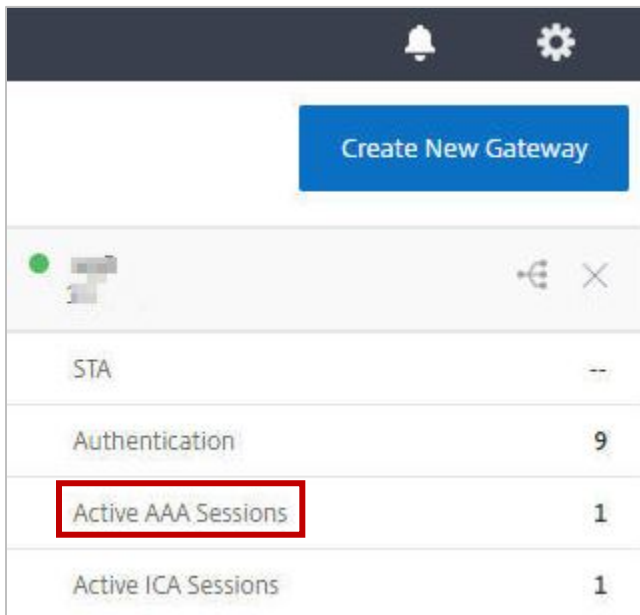
1. Connect to VPN using NetScaler with Unified Gateway.
2. Log on to NetScaler using your user name and password.



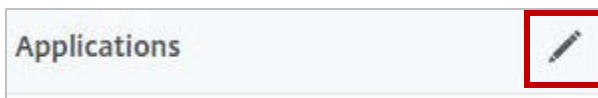
3. Click **Configuration > Unified Gateway**.



4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



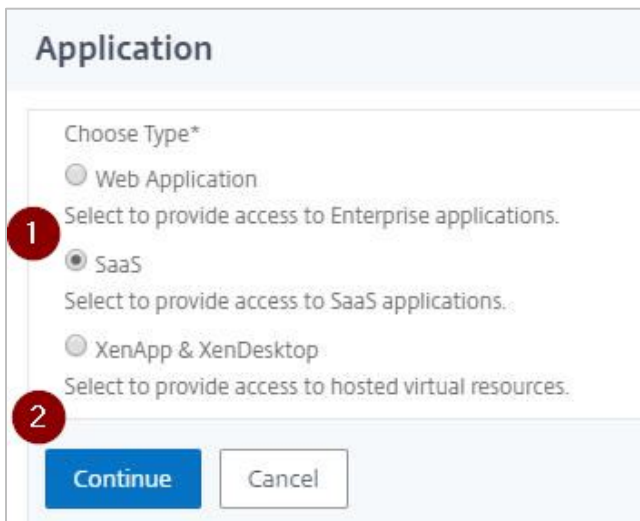
5. Click the edit icon for **Applications** section.



6. For adding a SaaS application, click the plus icon **+** that appears in the edit mode.



7. Click **SaaS > Continue**.



8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **DocuSign**.

Application

Choose Type
SaaS

SaaS Application: Catalog vs. Customized

1
 Choose from Catalog Customized Application

Choose from Catalog*

Office 365

- Office 365
- Salesforce
- Sharefile
- AWS Console
- G Suite
- Workday
- Concur
- Dropbox
- 15Five
- Zoom
- Zendesk
- Slack
- DocuSign** **2**
- Service Now
- Creative Cloud
- GoToMeeting
- GitHub

10. Click **Continue**.
11. In the **Create Application from Template** section, type the name of your SaaS application, in this case DocuSign, and relevant comments.

Create Application from Template

Name* **1**

Comments **2**

Icon URL (Imported from chosen application template)

DocuSign

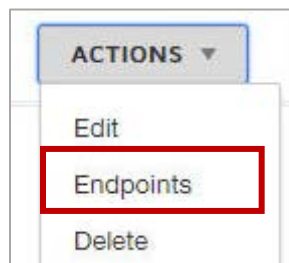
12. The Application section displays the values that are populated based on the JSON template.



The screenshot shows the 'Application' configuration page for DocuSign. At the top is the DocuSign logo. Below it are several input fields: 'Enter URL*' with a value starting with 'https://', 'Service Provider ID*', 'Assertion Consumer Service Url*' with a value starting with 'https://', 'SP Certificate Name' (a dropdown menu), 'Signing Certificate Name*' (a dropdown menu with a '+' icon and a pencil icon), and 'Issuer Name' with a value starting with 'https://'. At the bottom are 'Continue' and 'Cancel' buttons.

13. In the **Enter URL** box, enter your custom URL that you have copied from the Service Provider Issuer URL field obtained from the end point details.

- i. To access end point details, after logging on to DocuSign, on the Identity Providers page, after adding identity provider details, click **ACTIONS** in the bottom right corner. Then click **Endpoints**.



Assertion Consumer Service Url*

https://[redacted]

SP Certificate Name

[redacted] + [edit]

Signing Certificate Name*

[redacted] + [edit] ?

Issuer Name 2

[redacted]

Continue Cancel

Note: To update the certificate, click the plus icon for **Signing Certificate Name** list > Edit the information. > Click **OK**.

Application / Update Certificate

Update Certificate

Certificate-Key Pair Name

[redacted]

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Update the certificate and key

Certificate File Name

[redacted]

Key Filename

[redacted]

Certificate Format

PEM

Notify When Expires

Notification Period

30

OK Close

17. In the **Issuer Name** box, type the issuer ID that you entered while configuring DocuSign.

18. Click **Continue**.

19. Click **Done**.

Testing the Configuration

Testing the IdP Initiated Flow

To test the IdP initiated configuration, follow the steps below:

1. Access the IdP URL.
2. Log on to NetScaler appliance using your enterprise credentials.
3. Click **Clientless Access**.
4. On the home page, click **Apps** tab.
5. Click **DocuSign**.
Your DocuSign profile appears.
You have completed testing the IdP initiated flow.



Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2018 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).