CITRIX

NetScaler with Unified Gateway

Configuring PagerDuty

Abstract

Configuring PagerDutyfor SSO enables administrators to manage their users using NetScaler.

Contents

ABSTRACT....0
CONTENTS....1
DISCLAIMER (DOCUMENTATION)....2
PREFACE....3
OVERVIEW....4
CONFIGURING PAGERDUTY FOR SINGLE SIGN-ON....4
CONFIGURING NETSCALER FOR SINGLE SIGN-ON....8
TESTING THE CONFIGURATION....13

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.

PagerDuty provides SaaS incident response platform for IT departments for call schedule management, alerting, and incident tracking solution that collects alerts from monitoring tools.

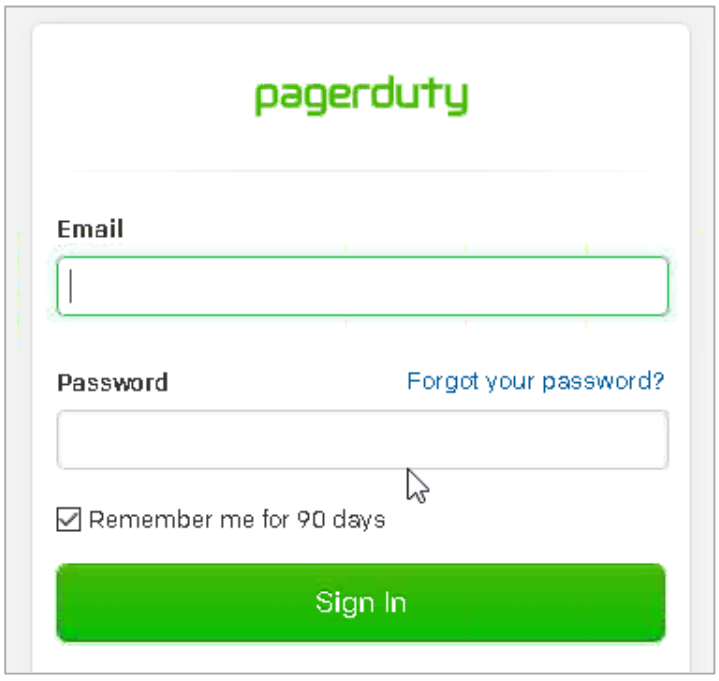
You can connect PagerDuty with NetScaler by using your company's credentials to log on to your account via Single Sign-On (SSO).

Configuring PagerDuty for Single Sign-On

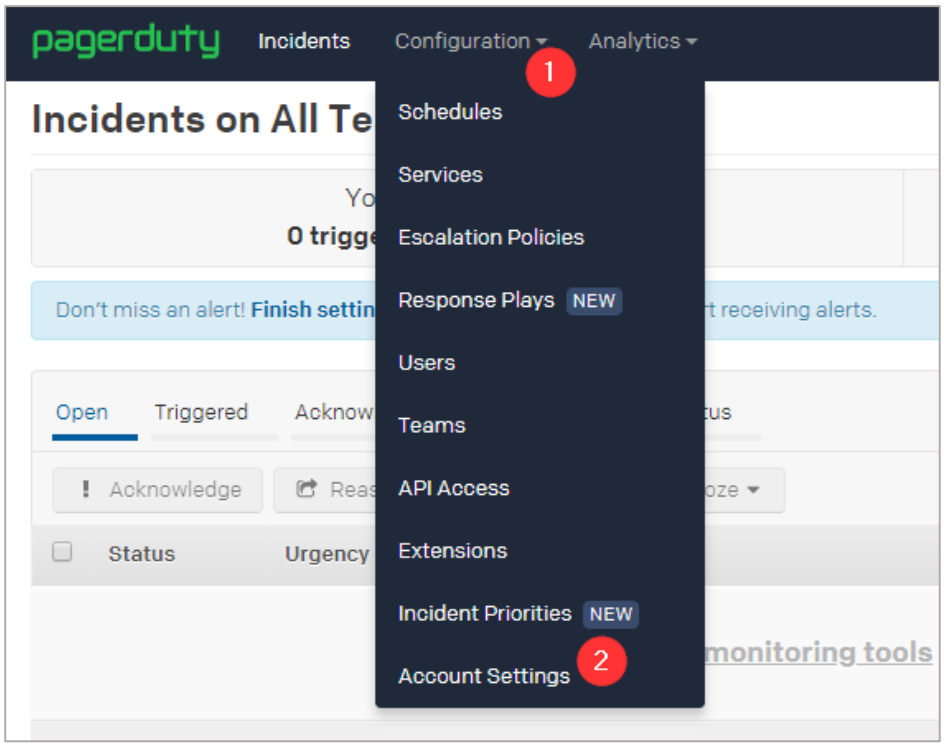
Configuring PagerDuty for SSO enables administrators to manage their users using NetScaler. Users can securely log on to PagerDuty using their enterprise credentials.

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

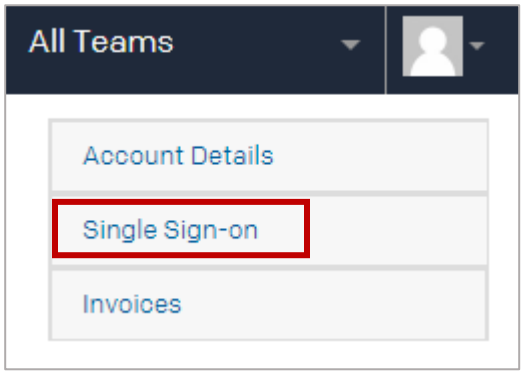
1. In a browser, type https://<your-organization>.pagerduty.com/ and press enter.
   Note: For example, ff the URL you use to access pager duty is https://myserver.pagerduty.com, then you must replace <your-organization> with myserver.
2. Log on to your PagerDuty account as an administrator.



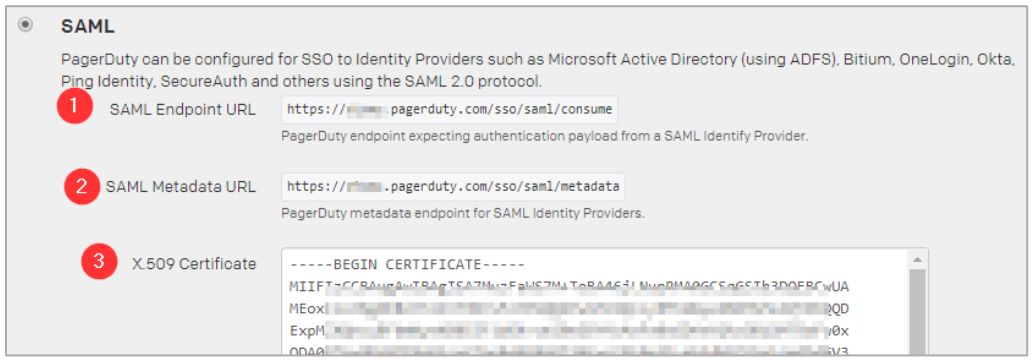
3. On the home page, click **Configuration** > **Account Settings**.



4. In the upper right corner, click **Single Sign-on**.



5. On the **Enable Single Sign-on (SSO)** page, in the **SAML** area, review and specify required details.



Note: By default, SAML option is selected. If not, ensure that you click **SAML**.

i. **SAML Endpoint URL** – displays assertion consumer service URL.
Note: Copy this value to use it while configuring NetScaler for SSO for the Assertion Consumer Service URL field.

ii. **SAML Metadata URL** – displays metadata URL. This is an XML file that contains data such as endpoints, supported bindings, identifier, and public keys required for interaction with SAML-enabled identity or service provider.
Note: Copy this value to use it while configuring NetScaler for SSO.

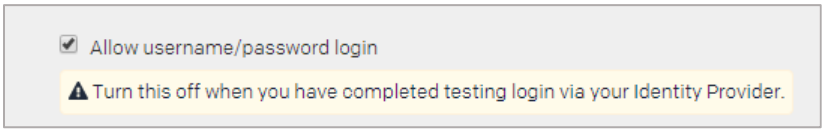
iii. **X.509 Certificate** – paste the Identity provider certificate.
Browse to the folder where you saved the IdP provided certificate and upload it.
To obtain your IdP certificate, follow the steps below:

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

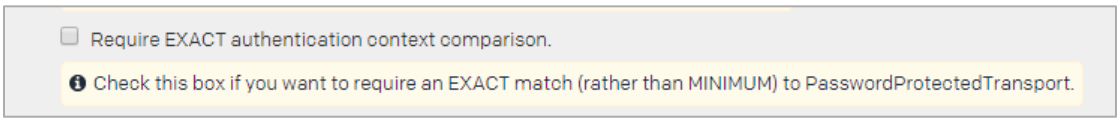
iv. **Login URL** - type the IdP URL followed by /saml/login. For example: https://<customerFQDN>/saml/login

v. **Logout URL (optional)** - type a redirect URL for logging out.

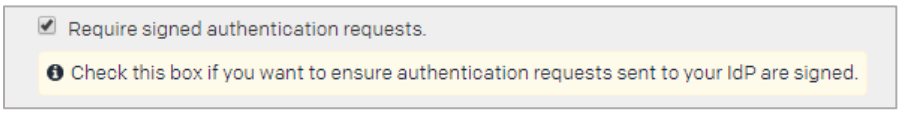
vi. **Allow username/password login**-. select the check box. Clear the check box after completing testing of logging on via Identity Provider if you do not want users to log on using user name and password.



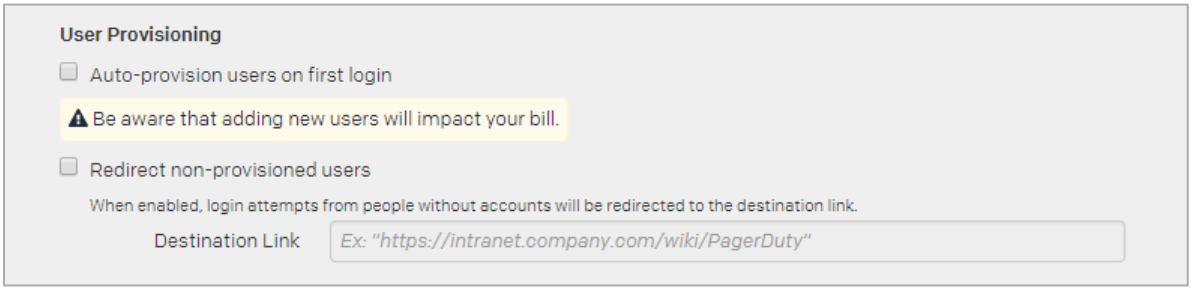
vii. **Require EXACT authentication context comparison** – select the check box if you want to mandate exact authentication. For this configuration, leave the check box unchecked.



viii. **Require signed authentication requests** - select the check box if you want to ensure authentication requests are signed. For this configuration, leave the check box unchecked.



ix. **Auto-provision users on first login** – select the checkbox in the **User provisioning** section to auto-provision users. After you enable auto-provisioning, if a user for whom a user account is not created uses SSO to log on to PagerDuty, the associated user account is created automatically.



x. **Redirect non-provisioned users** – select the check box to redirect people without an account to a specific link and type the link in the **Destination Link** box.

6. Click **Save Changes**.

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

Configuring NetScaler for Single Sign-On

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

Prerequisites

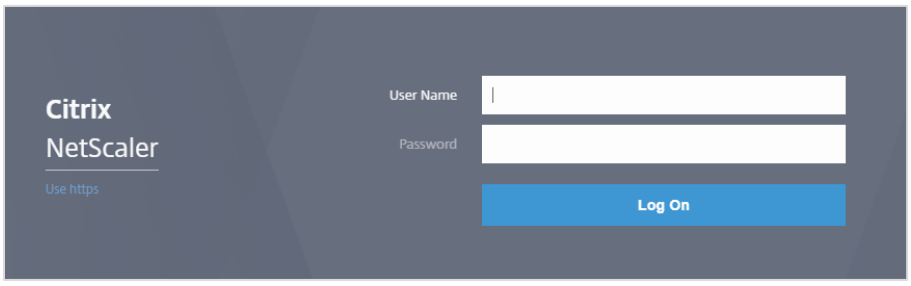
Ensure that you obtain the SP certificate before you start with the configuration.
To obtain the SP certificate follow the steps below:

a. Connect to VPN using NetScaler with Unified Gateway.
b. Download the XML file using the URL displayed by the SAML Metadata URL field while configuring PagerDuty.
c. Refer to the XML that you have downloaded while configuring PagerDuty.
d. Open the file in notepad and copy the text inside the X509Certificate tag.
e. Create a new notepad file, add the text that you have copied between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----.
f. Ensure that you add 65 characters per line to follow the PEM format.
g. Do not add a new line at the end or beginning of the text.
h. Save the file using an appropriate name for example: pagerduty.pem.
i. Copy the file to the NetScaler I.P. at /nsconfig/ssl using WinSCP or other similar tool.
j. Remotely access your NetScaler instance using PuTTY.
k. Run the following command: add ssl certkey pagerduty-sp -cert pagerduty.pem

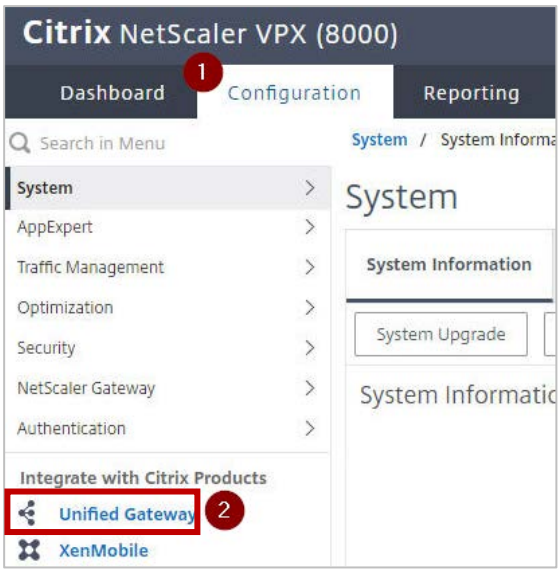
To configure NetScaler for single sign on through SAML, complete the following steps:

1. Connect to VPN using NetScaler with Unified Gateway.
   Note: Ensure that you obtain SP certificate before you start with the configuration. For more information refer Prerequisites.

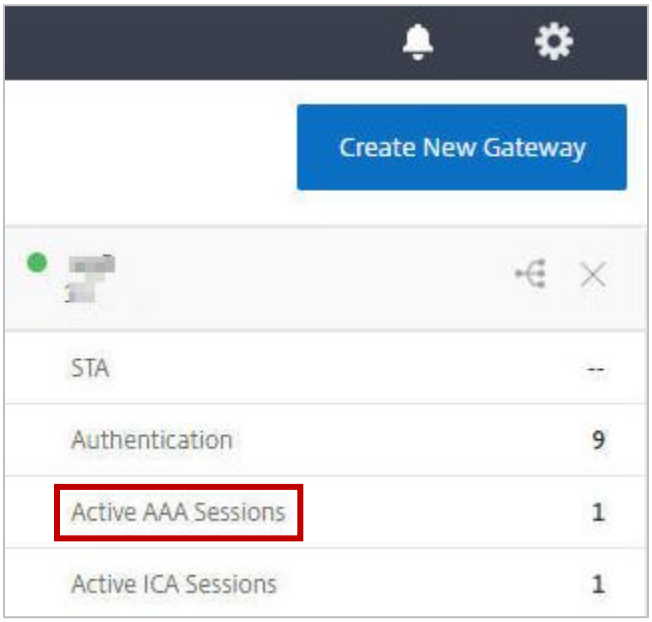
2. Log on to NetScaler using your user name and password.



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



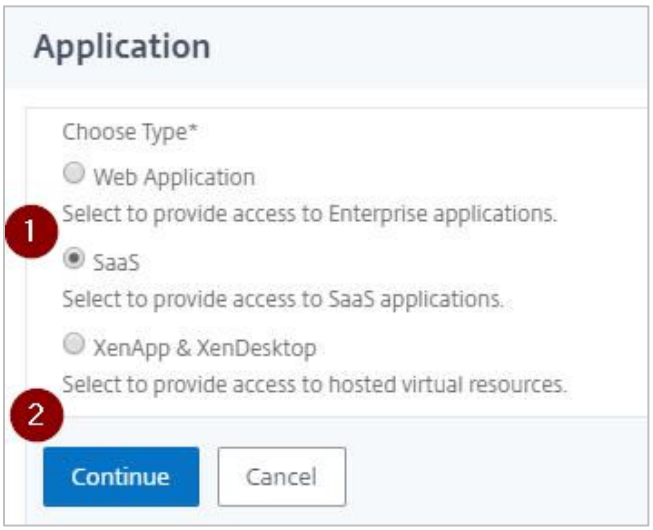
4. In the **Dashboard** area, click the configured NetScaler Gateway appliance.



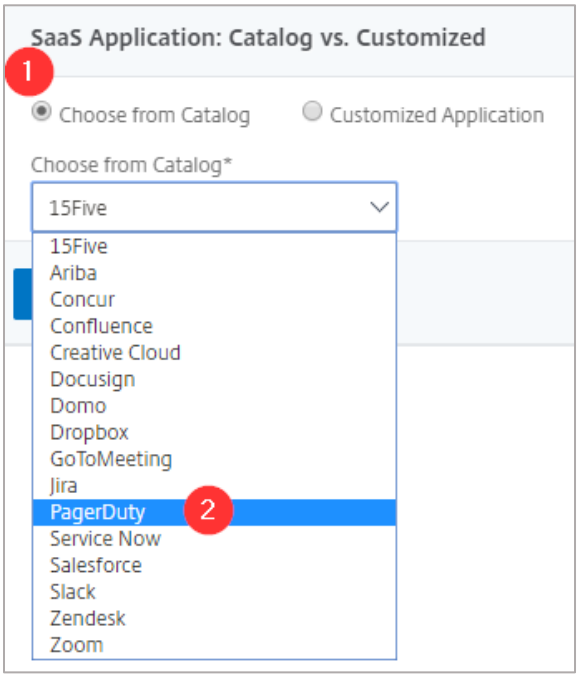
5. Click the edit icon for **Applications** section.

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

7. Click **SaaS** > **Continue**.

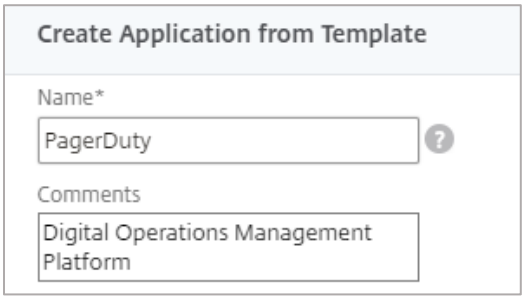


8. Click **Choose from Catalog**.
9. In the **Choose from Catalog** list, click **PagerDuty**.



10. Click **Continue**.

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



Note:

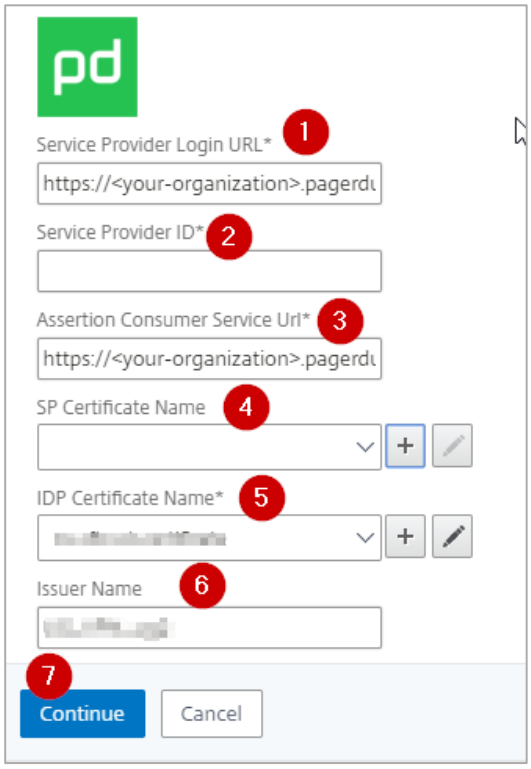
An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

The following table lists the SAML values that you need to copy while configuring SSO for SP and paste the values to appropriate fields while configuring SSO for IdP NetScaler.

Table 2: SSO field values used for SP and IdP configurations

Service Provider (SP) PagerDuty	Identity Provider (IdP) NetScaler
Service Provider Issuer	Service Provider ID
Identity Provider Issuer	Issuer Name
SAML Endpoint URL	Assertion Consumer Service Url

12. In the area below the logo, specify the following information:



i. **Service Provider Login URL** - type the URL in https://<your-organization>.pagerduty.com format. **Note**: For example, if the organization's URL is https://myserver.pagerduty.com, you must replace <your-organization> with myserver.
ii. **Service Provider ID** - enter the URL that you used for logging on to PagerDuty. To obtain this URL, refer to the metadata xml file that you downloaded while configuring Pager Duty for SAML. Copy the value for entityId attribute of the EntityDescriptor tag and paste it to this box.
iii. **Assertion Consumer Service Url*** - type the URL displayed by the **SAML Endpoint URL** field while configuring PageDuty.
iv. **SP Certificate Name** – click the appropriate certificate name. To obtain this value, refer to the metadata xml file that you downloaded while configuring PagerDuty for SAML. Copy and paste the URL that appears next to the value displayed between <ds:X509Certificate> and </ds:X509Certificate>.
For more information about how to obtain SP certificate, refer Prerequisites.
v. **IdP Certificate Name** - click the appropriate certificate name.
The IdP certificate appears last in the hierarchy in the **Server Certificate** section on **Unified Gateway Configuration** page.
vi. **Issuer Name** –type the issuer ID that you entered while configuring PagerDuty. For example: MyServer_NS_PagerDuty

13. Click **Continue.**
14. Click **Done**.

    The PagerDuty logo appears.

15. Click **Done**.

    You have completed the NetScaler configuration for PagerDuty.

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 **PagerDuty**.
   Your PagerDuty profile appears.
   You have completed testing the IdP initiated flow.

Testing the SP Initiated Flow

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

1. Access the organization's URL for PagerDuty.
2. Type your organizational user name.
   You are redirected to NetScaler appliance's log in page.
3. Log on to NetScaler appliance using your enterprise credentials.

   Your PagerDuty profile appears which indicates that you have successfully logged on to PagerDuty.

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).