Single Sign On for ZenDesk with NetScaler

Deployment Guide

This deployment guide focuses on defining the process for enabling Single Sign On into ZenDesk with Citrix NetScaler.
Table of Contents

Introduction 3
Configuration details 4
NetScaler features to be enabled 4
Solution description 5
Step 1: Configure ZenDesk 5
Step 2: Configure NetScaler 8
  Configure LDAP domain authentication 8
  To Configure the SAML IDP Policy and Profile 11
  To Configure your AAA Virtual Server 13
Validate the configuration 14
Troubleshooting 15
Conclusion 18
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

ZenDesk is a popular cloud-based customer service platform that includes ticketing, self-service options, and customer support features on a subscription basis. It is a preferred solution for several leading enterprises.

Introduction
This guide focuses on enabling ZenDesk single sign on with Citrix NetScaler.
Configuration Details
The table below lists the minimum required software versions for this integration to work successfully. The integration process should also work with higher versions of the same.

<table>
<thead>
<tr>
<th>Product</th>
<th>Minimum Required Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler</td>
<td>11.0, Enterprise/Platinum License</td>
</tr>
</tbody>
</table>

NetScaler features to be enabled
The following feature must be enabled to use single sign-on with ZenDesk:

- AAA-TM (Authentication, authorization and auditing - Traffic Management)

AAA-TM
The AAA feature set controls NetScaler authentication, authorization, and auditing policies. These policies include definition and management of various authentication schemas. NetScaler supports a wide range of authentication protocols and a strong, policy-driven application firewall capability.
Solution description
Enabling SSO for ZenDesk with NetScaler consists of two parts – configuring the ZenDesk portal and the NetScaler appliance. ZenDesk should be configured to use NetScaler as a third party SAML IDP (Identity Provider). The NetScaler is configured as a SAML IDP by creating the AAA Virtual Server that will host the SAML IDP policy.

The following instructions assume that you have already created the appropriate external and/or internal DNS entries to route authentication requests to a NetScaler-monitored IP address, and that an SSL certificate has already been created and installed on the appliance for the SSL/HTTPS communication. This document also assumes that a ZenDesk account has been created and the relevant organizational domain (*.zendesk.com) has been created and verification for the same has been completed.

Part 1: Configure ZenDesk
• In a web browser, log in to your ZenDesk administration portal at https://<your domain>.zendesk.com using an account with administrative rights.
• Enter the administrative console by clicking on the nut shaped icon as indicated.

• Here, navigate to Settings>Security and for both Admins and Agents as well as End users, enable single sign on by clicking on the tick mark next to it. Provide settings as shown in the next screenshot.
### Single sign-on (SSO)

Admins and agents use your SSO service to sign in to your Zendesk. Requires configuration.

**SAML**

SAML is an industry standard SSO framework typically used by large enterprises for communicating with their SAML providers.

<table>
<thead>
<tr>
<th><strong>SAML SSO URL</strong></th>
<th><a href="https://nssaml.citrix.com/saml/login">https://nssaml.citrix.com/saml/login</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the URL that Zendesk will invoke to redirect users to your Identity Provider (IdP)’s Single Sign-On (SSO) service. The ACS URL is <a href="https://oidc.sendesk.com/aspnet.mvc/ACS.aspx">https://oidc.sendesk.com/aspnet.mvc/ACS.aspx</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Certificate fingerprint</strong></th>
<th>c8 91 b3 8b 72 38 39 d5 43 e7 96 f5 35 e be 5f 21 f4 bf 65</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SHA256 or SHA1 (deprecated) fingerprint of the SAML certificate. Certificate fingerprints should be 64 characters long using only hexadecimal digits (a-f, A-F, 0-9).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Remote logout URL</strong></th>
<th><a href="https://nssaml.citrix.com/cgi/tmlogout">https://nssaml.citrix.com/cgi/tmlogout</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the URL that Zendesk will use to redirect your users to your IdP’s logout page. The logout page URL is: <a href="https://www.yourcompany.com/services/sendesk_logout.aspx">https://www.yourcompany.com/services/sendesk_logout.aspx</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IP ranges</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests from these IP ranges will always be routed via remote authentication. Other IP ranges will be routed to the normal sign-in form. To route all requests to the remote logout URL, you can add the IP address of your IdP’s SAML service to this IP range. Your current IP address is: 116.202.102.156</td>
</tr>
</tbody>
</table>

For the certificate fingerprint, you will need to download the signing certificate that NetScaler will use to sign the assertion. To get the verification certificate from the NetScaler appliance, follow these steps:

1. Select Traffic Management > SSL
2. Select Manage Certificates / Keys/ CSR’s under the Tools section on the right as shown below.
4. After the download is complete, open the certificate file in Windows, then copy the thumbprint listed under details as shown below.
Step 2: Configure NetScaler
The following configuration is required on the NetScaler appliance for it to be supported as a SAML identity provider for ZenDesk:

• LDAP authentication policy and server for domain authentication
• SSL certificate with external and internal DNS configured for the FQDN presented by the certificate (Wildcard certificates are supported.)
• SAML IDP policy and profile
• AAA virtual server

This guide covers the configuration described above. The SSL certificate and DNS configurations should be in place prior to setup.

Configuring LDAP domain authentication
For domain users to be able to log on to the NetScaler appliance with their corporate email addresses, you must configure an LDAP authentication server and policy on the appliance that is bound to your AAA VIP address. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler configuration utility, in the navigation pane, select Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > LDAP.
2. To create a new LDAP policy: On the Policies tab click Add, and then enter ZenDesk_LDAP_SSO_Policy as the name. In the Server field, click the ‘+’ icon to add a new server. The Authentication LDAP Server window appears.
3. In the Name field, enter ZenDesk_LDAP_SSO_Server.
4. Select the bullet for Server IP. Enter the IP address of one of your Active Directory domain controllers. (You can also point to a virtual server IP for the purpose of redundancy if you are load balancing domain controllers)
5. Specify the port that the NetScaler will use to communicate with the domain controller. Use 389 for LDAP or 636 for Secure LDAP (LDAPS). Leave the other settings as they are.
6. Under Connection Settings, enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) for which you want to allow authentication. The example below uses cn=Users,dc=ctxns,dc=net.

7. In the Administrator Bind DN field, add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. A service account is advisable, so that there will be no issues with logins if the account that is configured has a password expiration.

8. Check the box for Bind DN Password and enter the password twice.

9. Under Other Settings: Enter samaccountname as the Server Logon Name Attribute.

10. In the SSO Name Attribute field, enter UserPrincipalName. Enable the User Required and Referrals options. Leave the other settings as they are.
11. Click on More at the bottom of the screen, then add mail as Attribute 1 in the Attribute Fields section. Leave Nested Group Extraction in the Disabled state (we are not going to be using this option for this deployment).

12. Click the Create button to complete the LDAP server settings.

13. For the LDAP Policy Configuration, select the newly created LDAP server from the Server drop-down list, and in the Expression field type ns_true.

14. Click the Create button to complete the LDAP Policy and Server configuration.
Configure the SAML IDP Policy and Profile

For your users to receive the SAML token for logging on to ZenDesk, you must configure a SAML IDP policy and profile, and bind them to the AAA virtual server where users’ credentials are sent.

Use the following procedure:
1. Select the NetScaler Configuration tab and navigate to Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > SAML IDP.
2. In the Policies tab, select the Add button.
3. In the Create Authentication SAML IDP Policy window, create a name for your policy (for example – ZenDesk_SSO_Policy).
4. Click the ‘+’ icon next to the Action field to add a new action or profile.
5. Create an action name (for example, ZenDesk_SSO_Profile).
6. In the Assertion Consumer Service URL field, enter https://<your domain>.zendesk.com/access/saml/
7. Leave the SP Certificate Name blank.
8. In the IDP Certificate Name field, browse to the certificate installed on the NetScaler that will be used to secure your AAA authentication Virtual Server.
9. In the Issuer Name field enter https://nssaml.citrix.com/saml/login (where nssaml.citrix.com refers to your AAA vserver domain name).
10. Set the Encryption Algorithm to AES256 and the Service Provider ID field to <your domain>.zendesk.com.
11. Set both the Signature and Digest algorithms to SHA-1.
12. Set the SAML Binding to REDIRECT.
13. Click on More, then put zendesk.com in the Audience field.

14. Set the Skew Time to an appropriate value. This is the time difference that will be tolerated between the NetScaler appliance and the ZenDesk server for the validity of the SAML assertion.

15. Set the Name ID Format to EmailAddress, and put HTTP.REQ.USER.ATTRIBUTE(1) in the Name ID Expression field. This directs NetScaler to provide the mail attribute added earlier as the user ID for ZenDesk. If this user does not already exist, Zendesk will automatically create one.

16. Click Create to complete the SAML IDP profile configuration and return to the SAML IDP Policy creation window.

17. In the Expression field, add the following expression: HTTP.REQ.URL.CONTAINS("zendesk")

18. Click Create to complete the SAML IDP Configuration.
To Configure your AAA Virtual Server

An employee trying to log in to ZenDesk is redirected to a NetScaler AAA virtual server which validates the employee’s corporate credentials. This virtual server listens on port 443, which requires an SSL certificate, in addition to external and/or internal DNS resolution of the virtual server’s IP address on the NetScaler appliance. The following steps require a pre-existing virtual server to be in place and assume that the DNS name resolution is already in place, and that the SSL certificate is already installed on your NetScaler appliance.

1. In the NetScaler Configuration tab navigate to Security > AAA – Application Traffic > Virtual Servers and click the Add button.
2. In the Authentication Virtual Server window, enter the virtual server’s name and IP address. (av1 and 10.105.157.62 in this example)
3. Scroll down and make sure that the Authentication and State check boxes are selected.
4. Click Continue.
5. In the Certificates section, select No Server Certificate.
6. In the Server Cert Key window, click Bind.
7. Under SSL Certificates, choose your AAA SSL Certificate and select Insert. (Note – This is NOT the ZenDesk SP certificate.)
8. Click Save, then click Continue.
9. Click Continue again to bypass the Advanced Policy creation option, instead opting to add a Basic Authentication Policy by selecting the ‘+’ icon on the right side of the window.
10. From the Choose Type window, select Choose Policy from the drop-down list, select LDAP, leaving Primary as the type, and select Continue.
11. Select Bind and from within the Policies window select the ZenDesk_LDAP_SSO_Policy created earlier.
12. Click OK to return to the Authentication Virtual Server screen.
13. Under Basic Authentication Policies click the ‘+’ icon on the right to add a second Basic Policy.
14. From the Choose Policy drop-down list, select SAMLIDP, leave Primary as the type, and click Continue.
15. Under Policies select Bind, select your ZenDesk_SSO_Policy, and click Insert and OK.
16. Click Continue and Done.
After completing the AAA configuration above, this is how the Basic Settings screen of the AAA vserver will look:

![Authentication Virtual Server](image)

**Validate the configuration**
Point your browser to https://<your domain>.zendesk.com. You should be redirected to the NetScaler AAA logon form.

Log in with user credentials that are valid for the NetScaler environment you just configured. Your ZenDesk account details should appear. Note that you cannot now login to Zendesk directly. To do so, use https://<your domain>.zendesk.com/access/normal.
Troubleshooting

In order to help while troubleshooting, here is the list of entries that will be observed in the ns.log file (located at /var/log on the NetScaler appliance) for a successful SAML login (note that some of the entries such as encrypted hash values etc. will vary)

Section 1: The NetScaler receives the authentication request from ZenDesk and parses the same.


Jan 24 23:40:11 <local0.debug> 10.105.157.60 01/24/2016:23:40:11 GMT 0-PPE-0 : default AAATM Message 4693 0 : "SAMLIDP: GET AuthnRequest seen"

Jan 24 23:40:11 <local0.debug> 10.105.157.60 01/24/2016:23:40:11 GMT 0-PPE-0 : default AAATM Message 4694 0 : "SAMLIDP: Redirect Binding: SAMLRequest is gleaned successfully: SAMLRequest=fVHLTsJAFN3zFc3sp%2B0M5TWhJQ3ehASNAXhbheQuM8cQ4U0a%2B3VEkwRrf3%0An3Pz uNP2yejoCB5rZ3PC4pTMit4UpdEHUTzb9fw2gCCqVZF2B2qk8Zb4STW%0AARKw0gCi0sSlvV4LhqTv4F5ymlxJ %F1d1RFC7DUCi5Sn24GnKR%2Fz8xAyUSV%3AAGWUMBnQy4WMKapdt9VoMFcg5SM2sLQypA054kbb0prRn3w vsiy6I%2FBeSrR0%Aadd6kai8mM2dxcaA34A%2Figoel16uc7EM4iCRR4WQx%2FgbBaB7Eyp1EKgIYyTka%0AKbp 5RGfti%2FcaXIMf09515ZeLw6drtV7VGrt3uYeE1CcBN8A1w6cNzL8FROL%0AWXepK7rrqARKwHVZVb7NKZLiY %2Fxnz4reJw%3D%3D"

Jan 24 23:40:11 <local0.debug> 10.105.157.60 01/24/2016:23:40:11 GMT 0-PPE-0 : default AAATM Message 4695 0 : "SAMLIDP: Redirect Binding: RelayState is gleaned successfully"

Jan 24 23:40:11 <local0.info> 10.105.157.60 01/24/2016:23:40:11 GMT 0-PPE-0 : default AAATM Message 4696 0 : "SAMLIDP: Redirect Binding: response or relaystate or sigalg missing; response 1, relaystate 1 sigalg 0"

Jan 24 23:40:11 <local0.debug> 10.105.157.60 01/24/2016:23:40:11 GMT 0-PPE-0 : default AAATM Message 4697 0 : "SAMLIDP: Redirect Binding: no sigalg 0 or sign_len 0, trying to inflate data"


<?xml version="1.0"?>
Section 2: Messages indicating successful authentication and extraction of parameters from the backend LDAP server.

Jan 24 23:40:24 <local0.info> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default AAA Message 4706 0 : "In update_aaa_cntr: Succeeded policy for user u3test = ldap2"

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default AAATM Message 4707 0 : "extracted SSOUusername: U3Test@CTXNS.net for user u3test"

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default SSLVPN Message 4708 0 : "sslvpn_extract_attributes_from_resp: attributes copied so far are U3Test@ctxns.com"

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default SSLVPN Message 4709 0 : "sslvpn_extract_attributes_from_resp: total len copied 21, mask 0x1"

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default AAATM Message 4710 0 : "SAMLIDP: Checking whether current flow is SAML IdP flow, input WmVvRGVza19TQU1MAElEPXNhbWxyLTAyOTI4YjYwLWMyZjQtMTFlNS05OTI4LWVjZjRiYmQ3NTVjYyZiaW5kPXBvc3QmaHR0cCUzQSUyRiUyRmN0eG5zLnplbmRlc2suY29t"

Jan 24 23:40:24 <local0.info> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default AAA EXTRACTED_GROUPS 4711 0 : Extracted groups "LyncDL,TestDL-Lync"

Jan 24 23:40:24 <local0.info> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default AAAATM LOGIN 4712 0 : Context u3test@116.202.102.156 - SessionId: 30 - User u3test - Client_ip 116.202.102.156 - Nat_ip "Mapped Ip" - Vaer ver 10.105.157.62:443 - Browser_type "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko" - Group(s) "N/A"

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default SSLVPN Message 4714 0 : "UnifiedGateway: SSOID update skipped due to StepUp or LoginOnce OFF, user: u3test"

Section 3: Messages verifying SAML transaction and sending of SAML assertion with signature

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT O-PPE-0 : default
Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT O-PPE-0 : default
AAATM Message 4717 0 : "SAML: SendAssertion, Digest Method SHA1, SignedInfo used for
Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT O-PPE-0 : default
AAATM Message 4718 0 : "SAML: SendAssertion, Signature element is <ds:Signature

Conclusion
NetScaler provides a secure and seamless experience with ZenDesk by enabling single sign-on into ZenDesk accounts, avoiding the need for users to remember multiple passwords and user IDs, while reducing the administrative overhead involved in maintaining these deployments.