Single Sign On for ZenDesk with NetScaler Unified Gateway

Deployment Guide
This deployment guide focuses on defining the process for enabling Single Sign On into ZenDesk with Citrix NetScaler Unified Gateway.
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 UG Virtual Server 13
Validate the configuration 14
Troubleshooting 15
Conclusion 18
Citrix NetScaler Unified Gateway provides users with secure remote access to business applications deployed in the data center or a cloud across a range of devices including laptops, desktops, thin clients, tablets and smart phones. It provides a consolidated infrastructure, simplifies IT and reduces TCO of the data center infrastructure.

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>11.1, 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:

• SSLVPN

SSLVPN
The SSLVPN feature is required for the use of Unified Gateway. It adds support for the creation of SSL-based VPN virtual servers for secure enterprise application access.
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 UG 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.
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: Login to your NetScaler appliance, then select the Configuration tab.

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
- UG 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 UG VIP address. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler configuration utility, in the navigation pane, select NetScaler Gateway > – Policies > Authentication > 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 UG virtual server where users’ credentials are sent.

Use the following procedure:

1. Select the NetScaler Configuration tab and navigate to NetScaler Gateway > Policies > Authentication > 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 UG authentication Virtual Server.
9. In the Issuer Name field enter https://nssaml.citrix.com/saml/login (where nssaml.citrix.com refers to your UG 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 Unified Gateway (UG) Virtual Server

1. Select the Unified Gateway option in the Integrate with Citrix Products section on the navigation panel to initiate the Unified Gateway Configuration Wizard.
2. First, provide an appropriate name, IP address and port for the UG virtual server.
3. In the next step, provide a server certificate (if it is already present on the NetScaler) or install a new certificate that will be used as the server certificate for the UG virtual server.
4. Next, define the authentication mechanism to be used for the UG Virtual Server.
   
   **Note:** In the Wizard, only the most common authentication mechanisms are configured. Select Active Directory/LDAP and add the LDAP server configured earlier.
5. Set the Portal Theme to Default (or a theme of your choice) and click on Continue.
6. In the Applications section, select the pencil shaped icon on the top right, then the plus-shaped icon to add a new application. Select Web Application, then provide the ACS (Assertion Consumer Service) URL provided in the NetScaler SAML IDP policy earlier with an appropriate name.
7. Click on **Done** once the application has been added.
8. To add the SAML IDP policy to the Unified Gateway, navigate to the VPN Virtual Server listing (NetScaler Gateway>Virtual Servers) to fine the virtual server created using the wizard (named UG_VPN_<UG vserver name>). Choose the option for editing the virtual server, then add the SAML IDP policy created earlier in the Advanced Authentication section.
After completing the UG configuration above, this is how the Dashboard screen of the UG vserver will look:

**Dashboard**

![Dashboard Image]

**Validate the configuration**

Point your browser to https://<your domain>.zendesk.com. You should be redirected to the NetScaler UG 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) Please note that these logs are generic and the logs for SSLVPN will be similar.–

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 4694 0 : “SAMLIDP: Redirect Binding: SAMLRequest is gleaned successfully: SAMLRequest= fVHLTsJAFN3zFc3sp%2B0M5TWhJQ3ehA5NAXxhpheQuM8c0U40a%2B3VekwRf3%0AnJPs uN2pYeJoC65r23PC4pTMit4UpdEHUTzhb9fw2gCGqVZFB2Qk8Zb4STW%AARKw0gCiosS1v4LhqTh4F5ymxlXJ %2F1dRIPCdUC5ISInZ4GnKR%2Fz8xAYUsV%0AGWJMBnQy4WMKapd7t9VoMFCq5SMZsLQypA054kb0PRn3j3w vsiY6I%2BeSr0%0Aadd6kai8M2dxcaA34A%2Filoel6uc7EM4iCRR4WQx%2FgBbAb7Eyp1EKgWiyTka%0AKbp 5RGfii1%2FeXrNf095152eLu6drtV7VOrt3uYe%1CcBN8AiW6cNz8PROL%0AXwepK7rrqARKrHVZVb7NRXLIy %2FXzn24reJw%3D%3D%0A”


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 “


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_cnr: 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 SSUsername: 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 WmVuRGVza19TQU1MAElEPXNhbWxylTAyODI4YjYwLWMyZjQtMTFlNS05OTI4LWVjZjRiYmQ3NTVjYyZiaW5kPXBvc3QmaHR0cCUzQSUyRiUyRmN0eG5zLnplbmRlc2suY29t"
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 AAATM LOGIN 4712 0 : Context u3test@116.202.102.156 - SessionId: 30- User u3test - Client_ip 116.202.102.156 - Nat_ip “Mapped Ip” - Vaerver 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 0-PPE-0 : default

Jan 24 23:40:24 <local0.debug> 10.105.157.60 01/24/2016:23:40:24 GMT 0-PPE-0 : default
XluQb8gICyc2NkUvycd2C1DtGuqIam6
Conclusion

NetScaler Unified Gateway 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.