Single Sign On for Google Apps with NetScaler

Deployment Guide

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

- Introduction .................................................. 3
- Configuration details ......................................... 4
- NetScaler features to be enabled .......................... 4
- Solution description ........................................... 5
- Step 1: Configure Google Apps ............................. 5
- Step 2: Configure NetScaler ................................. 7
  - Configure LDAP domain authentication .................. 7
  - To Configure the SAML IDP Policy and Profile ....... 10
  - To Configure your AAA Virtual Server ................. 14
- Validate the configuration .................................... 15
- Troubleshooting .............................................. 16
- Conclusion ...................................................... 20
The Citrix NetScaler application delivery controller (ADC) is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

Google Apps for Work is a suite of cloud computing productivity and collaboration applications provided by Google on a subscription basis. It includes Google's popular web applications including Gmail, Google Drive, Google Hangouts, Google Calendar and Google Docs. Google Apps for Work adds business-specific features to these freely available apps such as custom domains for email, large amounts of storage as well as 24/7 support. The apps are widely used by SMEs and large enterprises to enable their business without needing much capital investment.

**Introduction**

This guide focuses on defining the guidelines for enabling Google Apps for Work 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 Build 64.x, Enterprise/Platinum License</td>
</tr>
</tbody>
</table>

NetScaler features to be enabled
The essential NetScaler feature that needs to be enabled is explained below.

- 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
The process for enabling SSO into Google Apps for Work with NetScaler consists of two parts – configuration of the Google Apps portal and configuration of the NetScaler appliance. To begin with we will have to first complete the configuration for Google Apps to use the NetScaler appliance as a third party SAML IDP (Identity Provider). After this, the NetScaler should be configured as a SAML IDP by creating a 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 Google Apps for Work account has been created and domain verification for the same has been completed.

Step 1: Configure Google Apps
1. In a web browser, log in to your Google Apps administration portal at https://admin.google.com/<yourdomainname>/AdminHome?fral=1 with a user account that has administrative rights. (where <yourdomainname> is the domain name that is registered with Google Apps)
2. Select the Security link in the panel presented on the admin console home page.
3. Scroll down to the Set up single sign-on settings drop down.
4. On the Single sign on Configuration page, check the Setup SSO with third party identity provider checkbox.
5. In the Sign-in page URL field, enter: https://aaavip.domain.com/saml/login (where aaavip.domain.com is the FQDN of the AAA vserver on the NetScaler appliance)
6. In the Sign-out page URL field, enter: https://aaavip.domain.com/cgi/tmlogout (where aaavip.domain.com is the FQDN of the AAA vserver on the NetScaler appliance)
7. Leave the Change password URL field empty.
8. For the Verification certificate, provide the certificate file that has been used for the SAML IDP AAA vserver. (aaavip.domain.com). The steps for obtaining this certificate are described after the screenshot shown below.
As all SAML assertions are signed using the private key configured on the SAML IDP (the AAA vserv-
er on the NetScaler device) the associated certificate (public key) is required for signature verification.

To get the verification certificate from the NetScaler appliance, follow these steps:

1. Login to your NetScaler appliance via the Configuration Utility.
2. Select Traffic Management > SSL
3. On the right, under Tools, select Manage Certificates / Keys / CSR’s

4. From the Manage Certificates window, browse to the certificate you will be using for your AAA Virtual Server. Select the certificate and choose the Download button. Save the certificate to a location of your choice.
Step 2: Configure NetScaler
The following configuration is required on the NetScaler appliance for it to be supported as a SAML identity provider for Google Apps for Work:

- 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 only 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 by using their corporate email addresses, you must configure an LDAP authentication server and policy on the appliance and bind it 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 GoogleApps_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 GoogleApps_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 Google Apps for Work, you must configure a SAML IDP policy and profile, and bind them to the AAA virtual server to which the users send their credentials.

Use the following procedure:
1. Open the NetScaler Configuration Utility and navigate to Security > AAA – Application Traffic > Policies > Authentication > Basic Policies > SAML IDP
2. On the Policies Tab, select the Add button.
3. In the Create Authentication SAML IDP Policy Window, provide a name for your policy (for example – GoogleApps_SSO_Policy).
4. To the right of the Action field, click the ‘+’ icon to add a new action or profile.
5. Provide a name (for example, GoogleApps_SSO_Profile).
6. In the Assertion Consumer Service URL field, enter https://www.google.com/a/<yourdomainname>/acs
7. Leave the SP Certificate Name blank.
8. In the IDP Certificate Name field, browse to the certificate installed on the NetScaler that is will be used to secure your AAA authentication Virtual Server.
9. In the Issuer Name field enter the identifier added earlier in the Identity Provider Entity ID field in the Citrix Organization Centre.
10. Set the Encryption Algorithm to AES256 and leave the Service Provider ID field blank.
11. Set both the Signature and Digest algorithms to SHA-256.
12. Set the SAML Binding to REDIRECT.
Configure Authentication SAML IDP Profile

Name
GoogleApps_SSO_Profile

Assertion Consumer Service Url
https://www.google.com/a/ctxns.com

IDP Certificate Name
NSSAML

SP Certificate Name

Encryption Algorithm
AES256

Send Password

Issuer Name

Service Provider ID

Reject Unsigned Requests

Signature Algorithm*
- RSA-SHA1
- RSA-SHA256

Digest Method*
- SHA1
- SHA256

SAML Binding*
REDIRECT
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 the identifier added earlier in the Identity Provider Entity ID field in the Citrix Organization Centre.
10. Set the Encryption Algorithm to AES256 and leave the Service Provider ID field blank.
11. Set both the Signature and Digest algorithms to SHA-256.
12. Set the SAML Binding to REDIRECT.
13. Click on More, then put https://www.google.com/a/<yourdomainname>/acs 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 Google Apps server for the validity of the SAML assertion.
15. Set the Name ID Format to Unspecified, and put HTTP.REQUEST.USER.ATTRIBUTE(1) in the Name ID Expression field. This directs NetScaler to provide the mail attribute that was defined earlier during LDAP configuration as the user ID for Google Apps.
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.REQUEST.URL.CONTAINS("google")
18. Click Create to complete the SAML IDP Configuration.
To Configure your AAA Virtual Server

An employee trying to log in to Google Apps is redirected to a NetScaler AAA virtual server for evaluation of 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 preexistence of the virtual server 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 Utility 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.
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, from the Choose Policy drop-down list, select LDAP, leaving Primary as the type, and select Continue.
11. Select Bind and from within the Policies window select the Google Apps_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 Google Apps_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://mail.google.com/a/<your domain>/acs. 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 Google Apps folders should appear.
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 Google Apps

Jan 8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT 0-PPE-0 : default AAATM Message 2850 0 : “SAMLIDP: GET AuthnRequest seen”
Jan 8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT 0-PPE-0 : default AAATM Message 2851 0 : “SAMLIDP: Redirect Binding: SAMLRequest is gleaned successfully; SAMLRequest=fVlJtsMwEL0j8%2Bw79iAILCaoAIC5GKJ2acBm%2BNMUrfxOHicFv6eNnUBb%7Z89VGc%2Fk4s20DAOotMwUJ2HMGaCylcYm5u%2FPTXDGL7LDgwJ0cZl2vslzG1B%2FJse1kkxuuU9w6FlaRJoDRAiwuuxmN%2FaMwpP2z2sirbcja7Ntmn9MqprKrlcqWa9UmaAtVuDuJa7Lz2hgpua5KXY1Z89fsY52aWZEPcYQVEG%2FQHfYGrJSJt8V8bk4PbJyQrh%2F89i1Xs4u1yIP8cVMAhqtdgXesy2ClvrglaciJU10%2FtcEunNAneyeBszSgTOdwGvLFJvrC3AbSp%2Fljphyfedyslalndht8ykyyUf0PanxXxbBysGLu5Hx5p9P7n8ubbZt%2FYk%2BiVFX7YrsfsOretVu9s2zZ2e%2BVAt2BqGEd%2F3Q4cY6l%2F3fbkmYj1lunqkih6Ap6VrDRVnUb23%2Fb02w758AA%3D%3D”
Jan 8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT 0-PPE-0 : default AAATM Message 2852 0 : “SAMLIDP: Redirect Binding: RelayState is gleaned successfully”
Jan 8 09:32:03 <local0.info> 10.105.157.60 01/08/2016:09:32:03 GMT 0-PPE-0 : default AAATM Message 2853 0 : “SAMLIDP: Redirect Binding: response or relaystate or sigalg missing; response 1, relaystate 1 sigalg 0 ”
Jan 8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT 0-PPE-0 : default AAATM Message 2854 0 : “SAMLIDP: Redirect Binding: no sigalg 0 or sign_len 0, trying to inflate data ”
</nsampl:AuthnRequest>"M"
Section 2: Messages indicating successful authentication and extraction of parameters from the backend LDAP server.

Section 3: Messages verifying SAML transaction and sending of SAML assertion with signature
Jan 8 08:35:35 <local0.info> 10.105.157.60 01/08/2016:08:35:35 GMT 0-PPE-0:
default AAATM LOGIN 2804 0: Context administrator@10.105.1.6 - SessionId: 14 - User
administrator - Client_ip 10.105.1.6 - Nat_ip "Mapped Ip" - Vserver 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 8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT 0-PPE-0:
default AAATM Message 2805 0: “SAMLIDP: Checking whether current flow is SAML IdP
flow,inputR1RN1NTT19Qcm9maWxlLAR1PWE0MGlmZ2pqODZmZmRmaWc0aDZqaGdmODNiZTJnZ2YmYmluZDlw
b3N0Jmh0dHBzOi8vZ2xvYmFsLmdvdG9tZ2V0aW5nLnNvbS9qX3NwcmluZ19jYXNfc2VjdXJpdHlIY2hIY2s=

Jan 8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT 0-PPE-0:
default SSLVPN Message 2806 0: “UnifiedGateway: SSOID update skipped due to StepUp
or LoginOnce OFF, user: administrator”

Jan 8 09:32:13 <local0.debug> 10.105.157.60 01/08/2016:09:32:13 GMT 0-PPE-0:
default AAATM Message 2871 0: “SAML: SendAssertion: Response tag is <samlp:Response
ID="_5d9a40ab9ad31b1adfb7c57577357d3" InResponseTo="fjmcpgdbjcgkjacneokmbnkbmfcaonaajibgf"
IssueInstant="2016-01-08T09:32:13Z
Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:Status>

Jan 8 09:32:13 <local0.debug> 10.105.157.60 01/08/2016:09:32:13 GMT 0-PPE-0:
default AAATM Message 2872 0: “SAML: SendAssertion: Assertion tag is
<saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">Administrator@ctxns.com</saml:NameID><saml: SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <saml:SubjectConfirmationData InResponseTo="fjmcpgdbjcgkjacneokmbnkbmfcaonaajibgf"
NotOnOrAfter="2016-01-08T09:37:13Z" Recipient="https://www.google.com/a/ctxns.com/acs"></saml:SubjectConfirmationData>
https://www.google.com/a/ctxns.com/acs</saml:Audience>
</saml:Audience>"

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