Single Sign On for Google Apps with NetScaler Unified Gateway

Deployment Guide

This deployment guide focuses on defining the process for enabling Single Sign On into Google Apps with Citrix NetScaler Unified Gateway

Table of Contents

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.

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 eatures 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 GoToMeeting single sign on with Citrix NetScaler Unified Gateway. For more information, go to https://www.citrix.co.in/products/netscaler-unified-gateway/resources/netscaler-unified-gateway.html

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.

Product	Minimum Required Version
NetScaler	11.1, Enterprise/Platinum License

NetScaler features to be enabled

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

- 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.

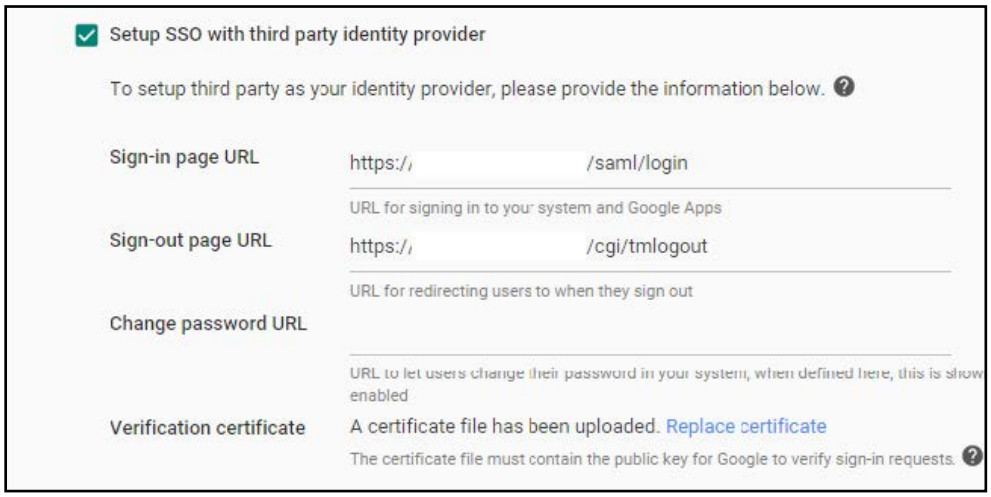
Solution description

The process for enabling SSO into Google Apps for Work with NetScaler consists of two parts – configu ation of the Google Apps portal and configu ation of the NetScaler appliance. To begin with we will have to first complete the config ation 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 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 al eady 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: Configu e Google Apps

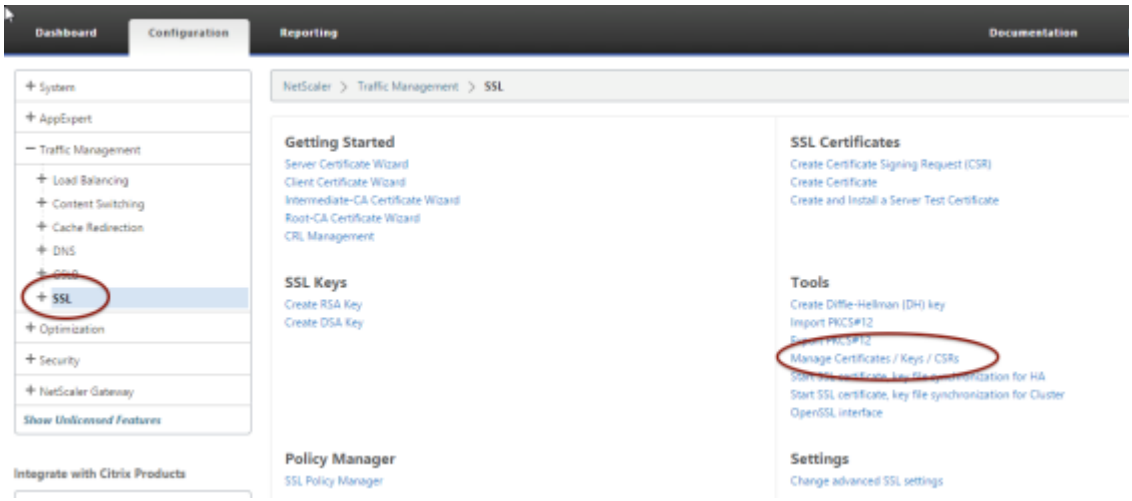
1. In a web browser, log in to your Google Apps administration portal at https://admin.google.com/<yourdomainname>/AdminHome?fral=1 with a user account that has administrative rights. (where <yourdomainname> is the domain name that is registered with Google Apps)
2. Select the Security link in the panel 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 Configu ation page, check the Setup SSO with third party identity provider checkbox.
5. In the Sign-in page URL field, enter: https://.... p.domain.com/saml/login (where ugvip.domain.com is the FQDN of the UG vserver on the NetScaler appliance)
6. In the Sign-out page URL field, enter: https://ugvip.domain.com/cgi/tmlogout (where ugvip.domain.com is the FQDN of the UG vserver on the NetScaler appliance)
7. Leave the Change password URL field empty
8. For the Verification certificate, ovide the certificate file that has been used for the SA IDP AAA vserver. (ugvip.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 UG vserver on the NetScaler device) the associated certificate (public key) is required for signature verification.

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

1. Login to your NetScaler appliance via the Configu ation Utility.
2. Select Traffic Management > SS
3. On the right, under Tools, select Manage Certificates / eys/ CSR's



4. From the Manage Certificates window, b owse to the certificate you will be using for you UG Virtual Server. Select the certificate and choose the Download button. Save the certificate to a location of your choice.

Step 2: Configu e NetScaler

The following configu ation 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 config ed for the FQDN presented by the certi - cate (Wildcard certificates a e supported.)
- SAML IDP policy and profil
- UG virtual server

This guide only covers the configu ation described above. The SSL certificate and DNS config a- tions should be in place prior to setup.

Configuring L AP 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 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 GoogleApps_ LDAP_SSO_Policy as the name. In the Server field, click the '+' icon to a d a new server. The Authentication LDAP Server window appears.
3. In the Name field, enter GoogleApps_L AP_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 configu ation) 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 configu ed has a password expiration.

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

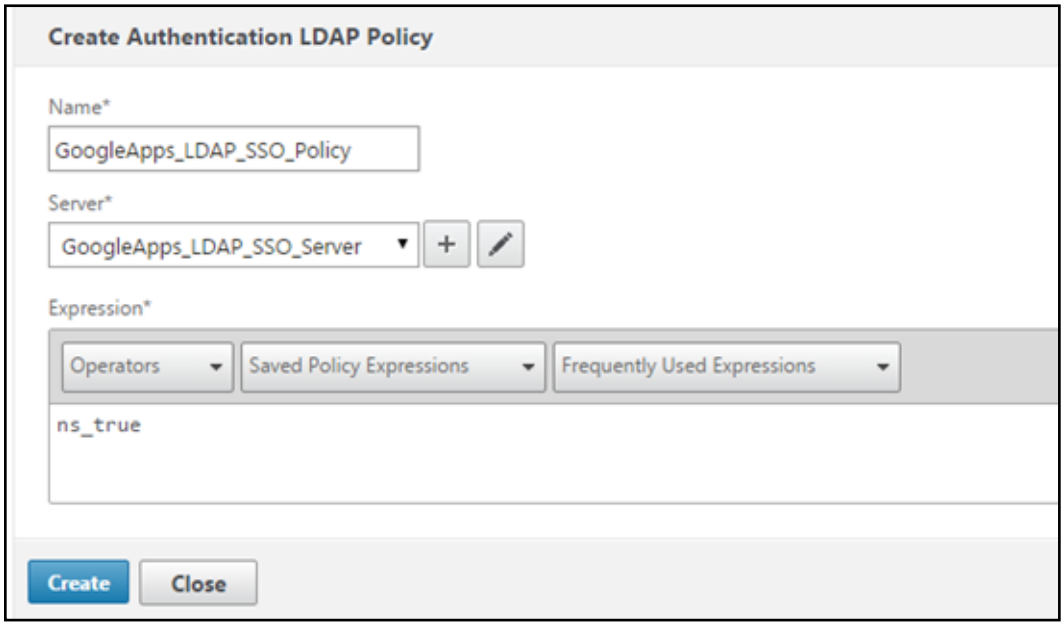
9. Under Other Settings: Enter samaccountname as the Server Logon Name Attribute.

10. In the SSO Name Attribute field, enter UserPrincipalName. Enabl 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 Configu ation, select the newly created LDAP server from the Server drop-down list, and in the Expression field type ns_true



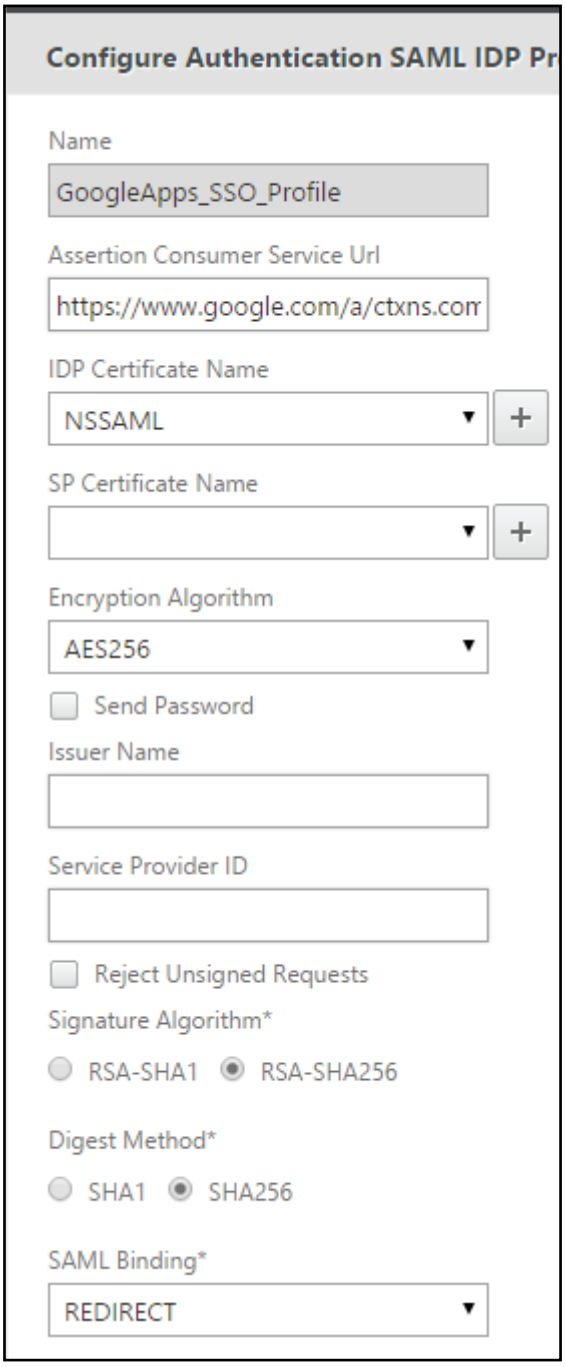
14. Click the Create button to complete the LDAP Policy and Server configu ation.

Configu e the SAML IDP Policy and Profil

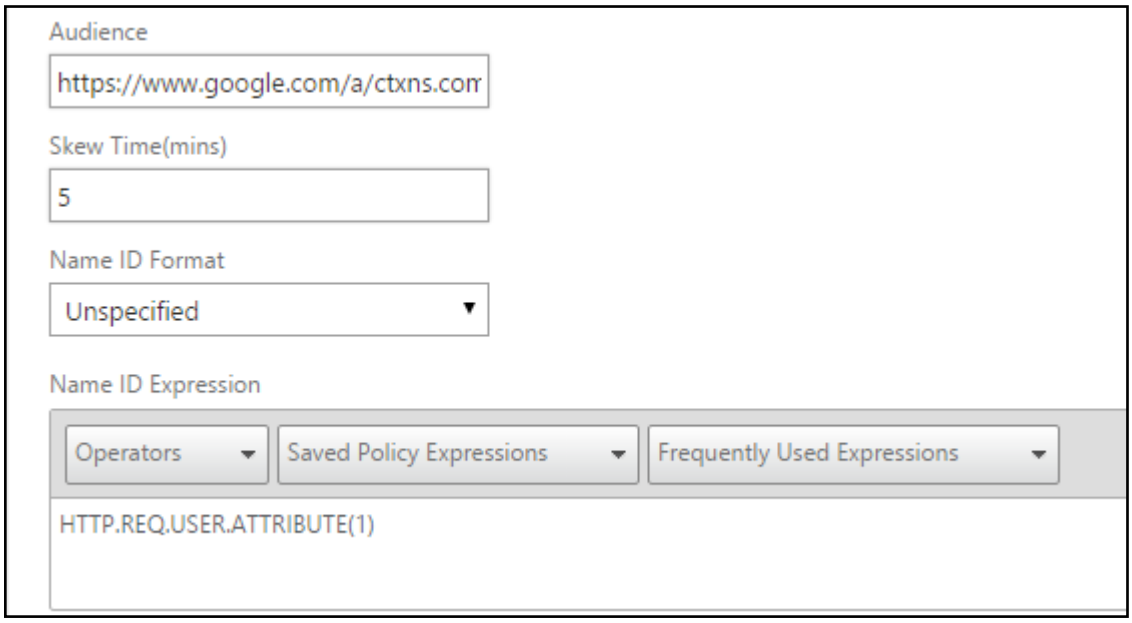
For your users to receive the SAML token for logging on to Google Apps for Work, you must con-figure a SAML IDP policy and profile, and bind them to the UG virtual server to which the users send their credentials.

Use the following procedure:

1. Open the NetScaler Configuration Utility and navigate to NetScaler Gateway > Policies > Authentication > 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 ne action or profile
5. Provide a name (for example, GoogleApps_SSO_Profile)
6. In the Assertion Consumer Service URL field, enter https://www. oogle.com/a/<yourdomainname>/acs
7. Leave the SP Certificate Name blank
8. In the IDP Certificate Name field, owse to the certificate installed on the NetScaler tha is will be used to secure your UG authentication Virtual Server.
9. In the Issuer Name field enter the identifier added earlier in e Identity Provider Entity ID field in the Citrix Organization Cent e.
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 Pr
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, owse to the certificate installed on the NetScaler tha will be used to secure your UG authentication Virtual Server.
9. In the Issuer Name field enter the identifier added earlier in e Identity Provider Entity ID field in the Citrix Organization Cent e.
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 HTT .REQ.USER.ATTRIBUTE(1) in the Name ID Expression field. This di ects NetScaler to provide the mail attribute that was defined ea - lier during LDAP configu ation as the user ID for Google Apps.
16. Click Create to complete the SAML IDP profile config ation and return to the SAML IDP Policy creation window.
17. In the Expression field, add the following exp ession: *HTTP.REQ.URL.CONTAINS("google")*
18. Click Create to complete the SAML IDP Configu ation.

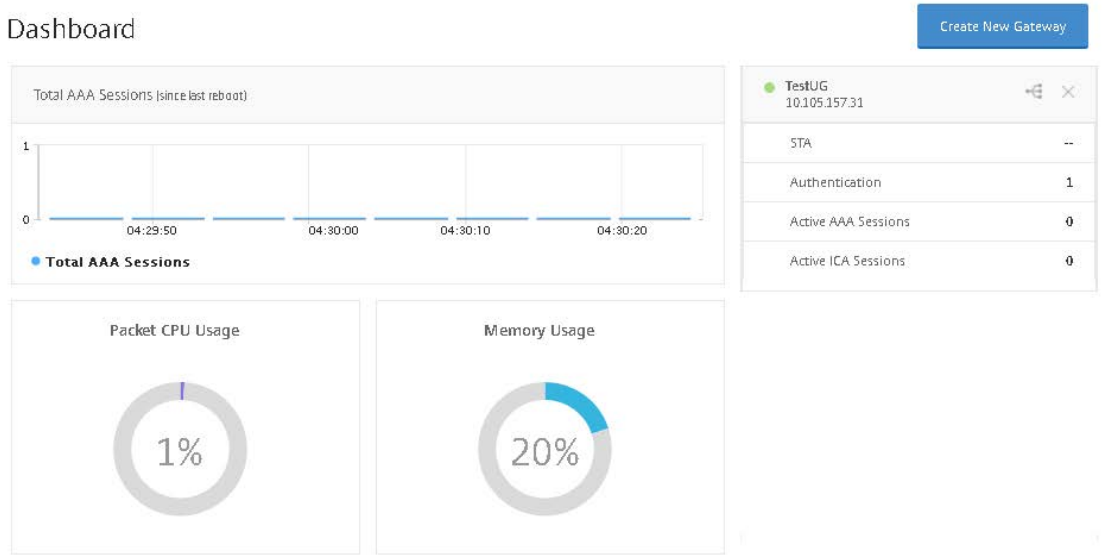
To Configure your Unified Gateway (UG) Virtual Server

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:



Validate the configu ation

Point your browser to https://mail.google.com/a/<your domain>/acs . You should be redirected to the NetScaler UG logon form.

Log in with user credentials that are valid for the NetScaler environment you just configu ed. 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 fi e (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 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=fVLJTsMwEL0j8Q%2BW79lAILCaoAJCVGKJ2sCBm%2BNMUrfxOHicFv6eN
AUBB7hZz89vGc%2Fk4s20bAOOtMWUJ2HMGaCylcYm5U%2FFTXDGL7LDgwlJ03Zi2vslzuG1B%2FJseIkkxo
uU9w6FlaRJoDRAwiuxmN7fiaMwFp2z3irbcja7Tnm9MqprKrlcqWa9UmsAtGuDJa7L2ihpUa5KXTY1Z89fsY5
2sWZEPcyQvEQ%2FQHFyGsRJEJ8V8bk4PhbJyQtn%2BafTpcZ9g%2F9ilXsSiduiyIP8cVGMAhtdgXsY2Cl
vrG1aCJU1O%2FtcEunNANeyJeBsSgTODwGvLFJvwC3AbbSCp%2FldypfedySiaLvdht8ykYyUf0PanxXxb
BysGLu5HxP9P7n8cubZt%2FYk%2BiGVfX7YrsfsOretVu9s2rZ2e%2BVA%2BqGEd%2F3Q4cY6I%2F3fbkm
YjIiugnqkih6pA6VrDRVnUbZ3%2Fb0Zw758AA%3D%3D"
Jan  8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT  0-PPE-0 : de
fault 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 "
Jan  8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT  0-PPE-0 :
default AAATM Message 2855 0 :  "SAMLIDP: Redirect Binding: inflate succeeded,
outlen 600, data <?xml version="1.0" encoding="UTF-8"?>^M <samlp:AuthnRequest
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="fjmcpgdahjcgkjckeenokmnb
nkbfmcaonajbibgf" Version="2.0" IssueInstant="2016-01-08T09:33:15Z" ProtocolBinding=
"urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" ProviderName="google.com" IsPassive=
"false" AssertionConsumerServiceURL="https://www.google.com/a/ctxns.com/acs">
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">google.com
</saml:Issuer><samlp:NameIDPolicy AllowCreate="true"
Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" />
</samlp:AuthnRequest>^M  "
Jan  8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT  0-PPE-0 :
 default AAATM Message 2856 0 :  "SAMLIDP: Redirect Response: relaystate is
```

```
https%3A%2F%2Fwww.google.com%2Fa%2Fctxns.com%2FServiceLogin%3Fservice%3Dmail
%26passive%3Dtrue%26rm%3Dfalse%26continue%3Dhttps%253A%252F%252Fmail.google.com
%252Fmail%252Facs%252F%26ss%3D1%26ltmpl%3Ddefault%26ltmplcache%3D2%26
emr%3D1%26osid%3D1"

Jan  8 09:32:03 <local0.debug> 10.105.157.60 01/08/2016:09:32:03 GMT  0-PPE-0 :
default SSLLOG SSL_HANDSHAKE_SUCCESS 2857 0 :  SPCBId 639 - ClientIP 10.105.1.6 -
ClientPort 59806 - VserverServiceIP 10.105.157.62 - VserverServicePort 443 -
ClientVersion TLSv1.0 - CipherSuite "AES-256-CBC-SHA TLSv1 Non-Export 256-bit"
- Session New
```

Section 2: Messages indicating successful authentication and extraction of parameters from the backend LDAP server.

```
Jan  8 08:35:35 <local0.info> 10.105.157.60 01/08/2016:08:35:35 GMT  0-PPE-0 : default
AAA Message 2798 0 :  "In update_aaa_cntr: Succeeded policy for user
administrator = ldap2"
Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT  0-PPE-0 : default
 AAATM Message 2799 0 :  "extracted SSOusername: Administrator@CTXNS.net for user
administrator"
Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT  0-PPE-0 : default
 SSLVPN Message 2800 0 :  "sslvpn_extract_attributes_from_resp: attributes copied
so far are Administrator@ctxns.com "
Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT  0-PPE-0 : default
 SSLVPN Message 2801 0 :  "sslvpn_extract_attributes_from_resp: total len copied 28,
 mask 0x1 "
```

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

```
Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT  0-PPE-0 : default
AAATM Message 2802 0 :  "SAMLIDP: Checking whether current flow is SAML IdP flow,
inputR1RNX1NTT19Qcm9maWxlAElEPWE0MGlmZ2pqODZmZmRmaWc0aDZqaGdmODNiZTJjN2YmYmluZD1w
b3N0Jmh0dHBzOi8vZ2xvYmFsLmdvdG9tZWV0aW5nLmNvbS9qX3NwcmluZ19jYXNfc2VjdXJpdHlfY2hlY2s="
NTT19Qcm9maWxlAElEPWE0MGlmZ2pqODZmZmRmaWc0aDZqaGdmODNiZTJjN2YmYmluZD1wb3N0Jmh0dHBzOi8
vZ2xvYmFsLmdvdG9tZWV0aW5nLmNvbS9qX3NwcmluZ19jYXNfc2VjdXJpdHlfY2hlY2s="
Jan  8 08:35:35 <local0.info> 10.105.157.60 01/08/2016:08:35:35 GMT  0-PPE-0 : default
AAA EXTRACTED_GROUPS 2803 0 :  Extracted_groups "ADSyncAdmins,ReportingGroup
{133115cb-a0b1-4a96-83db-2f4828ba1ecf},SQLAccessGroup {133115cb-a0b1-4a96-83db-2f48
28ba1ecf},PrivUserGroup {133115cb-a0b1-4a96-83db-2f4828ba1ecf},VPN-USER,RadiusUser,
LyncDL,ContentSubmitters,Organization Management,CSAdministrator,
RTCUniversalUserAdmins,RTCUniversalServerAdmins,Group Policy Creator Owners,
Domain Admins,Enterprise Admins,Schema Admins,Administrators"
```

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,inputR1RNX1NTT19Qcm9maWxlAElEPWE0MGlmZ2pqODZmZmRmaWc0aDZqaGdmODNiZTJjN2YmYmluZD1wb3N0Jmh0dHBzOi8vZ2xvYmFsLmdvdG9tZWV0aW5nLmNvbS9qX3NwcmluZ19jYXNfc2VjdXJpdHlfY2hlY2s="

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 xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://www.google.com/a/ctxns.com/acs" ID="_5d9a40ab9ad31b1a1dfb7c57577357d3" InResponseTo="fjmcpgdahjcgkjckeenokmnbnkbfmcaonajbibgf" IssueInstant="2016-01-08T09:32:13Z" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">netscaler.com</saml:Issuer><samlp:Status><samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode></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:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_5d9a40ab9ad31b1a1dfb7c57577357d" IssueInstant="2016-01-08T09:32:13Z" Version="2.0"><saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">netscaler.com</saml:Issuer><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="fjmcpgdahjcgkjckeenokmnbnkbfmcaonajbibgf" NotOnOrAfter="2016-01-08T09:37:13Z" Recipient="https://www.google.com/a/ctxns.com/acs"></saml:SubjectConfirmationData></saml:SubjectConfirmation></saml:Subject><saml:Conditions NotBefore="2016-01-08T09:27:13Z" NotOnOrAfter="2016-01-08T09:37:13Z"><saml:AudienceRestriction><saml:Audience>https://www.google.com/a/ctxns.com/acs</saml:Audience></saml:AudienceRestriction></s

Jan 8 09:32:13 <local0.debug> 10.105.157.60 01/08/2016:09:32:13 GMT 0-PPE-0 : default AAATM Message 2873 0 : "SAML: SendAssertion, Digest Method SHA256, SignedInfo used for digest is <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:CanonicalizationMethod><ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></ds:SignatureMethod><ds:Reference URI="#_5d9a40ab9ad31b1a1dfb7c57577357d"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod><ds:DigestValue>yJ1g9elD3NNJSl+23vbmSR+a1fL9ANEtvUAbSwJ3g3A=</ds:DigestValue></ds:Reference></ds:SignedInfo>"

Jan 8 09:32:13 <local0.debug> 10.105.157.60 01/08/2016:09:32:13 GMT 0-PPE-0 : default AAATM Message 2874 0 : "SAML: SendAssertion, Signature element is <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:CanonicalizationMethod><ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></ds:SignatureMethod><ds:Reference URI="#_5d9a40ab9ad31b1a1dfb7c57577357d"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"></ds:Transform><ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:Transform></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"></ds:DigestMethod><ds:DigestValue>yJ1g9elD3NNJSl+23vbmSR+a1fL9ANEtvUAbSwJ3g3A=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>VI4vOnwvSaVoYNHpcUP/2AdXBTYrhVxNQFaZ+oX6OJAUgdUIHcL8wOSTdWC7u0wGTt4kPhbMPKMq7lsJ2qyZjBBFMsBk0N4FYZxW
Jan 8 09:32:13 <local0.debug> 10.105.157.60 01/08/2016:09:32:13 GMT 0-PPE-0 : default SSLVPN Message 2875 0 : "core 0: initClientForReuse: making aaa_service_fqdn_len 0 "

Conclusion

NetScaler Unified Gateway 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.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-de ning the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.