Single Sign On for GoToMeeting with NetScaler

Deployment Guide

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

Introduction 3
Configuration details 4
NetScaler features to be enabled 4
Solution description 5
Step 1: Configure GoToMeeting 5
Step 2: Configure NetScaler 8
  To configure LDAP domain authentication 8
  To Configure the SAML IDP Policy and Profile 11
  To Configure your AAA Virtual Server 15
Troubleshooting 17
Conclusion 21
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.

Citrix GoToMeeting is an online meeting, desktop sharing, and video conferencing software that enables the user to meet with other computer users, customers, clients or colleagues via the Internet in real time. It is designed to broadcast the desktop view of a host computer to a group of computers connected to the host through the Internet. Transmissions are protected with high-security encryption and optional passwords. By combining a web-hosted subscription service with software installed on the host computer, transmissions can be passed through highly restrictive firewalls.

Introduction

This guide focuses on defining the guidelines for enabling Citrix GoToMeeting 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 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 GoToMeeting with NetScaler consists of two parts – configuration of the Citrix Online portal, which handles organization logins for GoToMeeting and configuration of the NetScaler appliance. To begin with we will have to first complete the configuration for GoToMeeting to use the NetScaler appliance as a third party SAML IDP (Identity Provider). This can only be done with an organization account and after domain verification has been completed. 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 GoToMeeting organization account has been created and domain verification for the same has been completed.

Step 1: Configure GoToMeeting/Citrix Online

- In a web browser, navigate to the Citrix Online administrative page at https://account.citrixonline.com/organization/administration/
- You will be redirected to the Citrix Online login page as shown below:

![Citrix Online login page]

- Enter your organization administrator account login credentials and Click Sign In.

• Enter your organization administrator account login credentials and Click Sign In.
After successful sign in, you will see the Citrix Organization Center screen. Click on the Identity provider link at the top of the page.

- 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). Set the sign-in binding as POST.
- 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). Set the sign-out binding as POST. This setting is optional.
- In the Identity Provider Entity ID field, enter a unique identifier for the SAML identity provider (here, we use nssaml). The same should be configured on the NetScaler appliance as well.
- 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 vserver 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 GoToMeeting:

- 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 GTM_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 GTM_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 is.
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 GoToMeeting, 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 – GTM_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, GTM_SSO_Profile).

6. In the Assertion Consumer Service URL field, enter https://login.citrixonline.com/saml/global.gotomeeting.com/acs

7. For the SP Certificate Name field, you will require the certificate that is used by the login.citrixonline.com portal. To get this certificate, open the login.citrixonline.com page in a web browser, then click on the green bar icon (shown below as visible in Google Chrome). In the window that is then shown, select the Connection tab, then click on Certificate Information.

[Image of certificate information]
In the window shown, select the Details tab, then click on Copy to File to export the certificate. Add this certificate in the NetScaler appliance by navigating to Traffic Management>SSL>Certificates and selecting the Install button. Provide the filename that you have saved the certificate to in the Certificate File Name field, then select Install.

Alternatively, if you are unable to access the login.citrixonline.com website during the deployment, save the text shown on the next page in a separate file, giving it an indicative name such as citrix.cer.
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 https://login.citrixonline.com/saml/sp as the Service Provider ID.

11. Set both the Signature and Digest algorithms to SHA-1.

12. Set the SAML Binding to POST.
13. Click on More, then put https://login.citrixonline.com/saml/sp 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 GoToMeeting server for the validity of the SAML assertion.

15. Set the Name ID Format to EmailAddress, and put HTTPREQ.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 GoToMeeting.
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: \texttt{HTTPREQ.HEADER("Referer").CONTAINS("citrixonline")}

18. Click Create to complete the SAML IDP Configuration.

**To Configure your AAA Virtual Server**

An employee trying to log in to GoToMeeting 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. (Note – This is NOT the GoToMeeting SP certificate.)
After completing the AAA configuration above, this is how the Basic Settings screen of the AAA vserver will look:

**Authentication Virtual Server**

<table>
<thead>
<tr>
<th>Basic Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Authentication Domain</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Port</td>
</tr>
</tbody>
</table>

**Certificates**

- 1 Server Certificate
- No CA Certificate

**Advanced Authentication Policies**

- No Authentication Policy

**Basic Authentication Policies**

- Primary Authentication
  - 1 LDAP Policy
  - 1 SAML IDP Policy
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 Citrix Online

Jan  8 08:35:27 <local0.debug> 10.105.157.60 01/08/2016:08:35:27 GMT 0-PPE-0 :
default AAATM Message 2789 0 : “SAMLIDP: ParseAuthnReq: signature method seen is 4”

Jan  8 08:35:27 <local0.debug> 10.105.157.60 01/08/2016:08:35:27 GMT 0-PPE-0 :
default AAATM Message 2790 0 : “SAMLIDP: ParseAuthnReq: digest method seen is SHA1”

Jan  8 08:35:27 <local0.debug> 10.105.157.60 01/08/2016:08:35:27 GMT 0-PPE-0 :
default AAATM Message 2791 0 : “SAML verify digest: digest algorithm SHA1, input for
id-format:emailAddress"></saml2p:NameIDPolicy></saml2p:AuthnRequest>”

Jan  8 08:35:27 <local0.debug> 10.105.157.60 01/08/2016:08:35:27 GMT 0-PPE-0 :
default AAATM Message 2792 0 : “SAML signature validation: algorithm is RSA-SHA1

Jan  8 08:35:27 <local0.debug> 10.105.157.60 01/08/2016:08:35:27 GMT 0-PPE-0 :
default SSLVPN Message 2793 0 : “core 0: initClientForReuse: making aaa_service_fqdn_len 0”
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, inputR1RNXINTT19Qcm9maWxlAEIPWEOMGlz2pqODZmZmRmaWc0aDZqaGdmODN1ZTJjN2ymYmluZDlw b3NOJnh0dBzoi8vZ2xvYmFsLmdvdG9tZWV0aW5nNmY2bS9qX3NwcmluZ19jYXNfcsVjdXJpdHlFy2hlY2s=“ NTT19Qcm9maWxlAEIPWEOMGlz2pqODZmZmRmaWc0aDZqaGdmODN1ZTJjN2ymYmluZDlw3NOJnh0dBzoi8 vZ2xvYmFsLmdvdG9tZWV0aW5nNmY2bS9qX3NwcmluZ19jYXNfcsVjdXJpdHlFy2hlY2s=“

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 {13315cb-a0b1-4a96-83db-2f482ba1ecf},SQLAccessGroup {13315cb-a0b1-4a96-83db-2f48 28ba1ecf},PrivUserGroup {13315cb-a0b1-4a96-83db-2f482ba1ecf},VPN-USER,RadiusUser, LyncDL,ContentSubmitters,Organization,Management,CASAdministrator, 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,inputR1RNX1NTT19Qcm9maWxlLElPEWE0MGlmZ2pqODZmZmRmaWc0aDZqaGdmODNiZTJjN2YmYmluZ2lwZnNzcmluZ2lvbTV0b3N0Jmh0dHBzOi8vZ2xvYmFsLmdvdXVjYWt3YXNvbXxhZ2UvZ2luZGV4dHl0YXNydmluZ3JrcmlnaWdaJmF1dGhvcmVzaXplLmNvbS93aXRoL29yaWdpdCB3b3JsZVZhbWlseS9wYWdlX2lkLmNub29yZ2dlbi5jbi81"
Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT 0-PPE-0 : 
default AAATM Message 2809 0 : “SAML: SendAssertion, Digest Method SHA1, SignedInfo 
used for digest is <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:Canoni 
icalizationMethod xmlns:ds="http://www.w3.org/2001/10/xml-exc-c14n#"><ds:Canonicaliz 
tureMethod><ds:Reference URI="#_03eb9d569676285fd093f69f05ee30"><ds:Transforms><ds:Transfo 
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:Transform><ds:DigestMethod 
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod><ds:DigestValue 
3jdU1JRMaYpTrz3HSbR4VQ2z2Y=""></ds:DigestValue></Reference></SignedInfo>"

Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT 0-PPE-0 : 
default AAATM Message 2810 0 : “SAML: SendAssertion, Signature element is 
://www.w3.org/2000/09/xmldsig#"><ds:CanonicalizationMethod Algorithm="http://www.w3 
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:Transform><ds:DigestMethod 
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod><ds:DigestValue 
3jdU1JRMaYpTrz3HSbR4VQ2z2Y=""></ds:DigestValue></Reference></SignedInfo><ds:SignatureValue>bLGCZXpcHjhkAI1gwZ0rH17go6NHKXyF8PjseUjM7a7MPwxQfHDLXzyVQAuyBP/u6+tgrS2adrRThRNUVtFX07gEQV9m7zfZYY/As5c1IXMY1+qYAPBHBLShX

Jan  8 08:35:35 <local0.debug> 10.105.157.60 01/08/2016:08:35:35 GMT 0-PPE-0 : 
default SSLVPN Message 2811 0 : “core 0: initClientForReuse: making aaa_service_ 
fdnm_len 0 “
Conclusion
NetScaler provides a secure and seamless experience with GoToMeeting by enabling single sign-on into GoToMeeting accounts, avoiding the need for users to remember multiple passwords and user IDs, while reducing the administrative overhead involved in maintaining these deployments.