SAML 2.0 Single Sign On with Citrix NetScaler

This guide focuses on defining the process for deploying NetScaler as a SAML IdP for most enterprise applications that support SAML 2.0.
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

NetScaler’s SAML integration capabilities allow NetScaler to act as a SAML IDP (Identity Provider), enabling enterprise users to log on to their enterprise SalesForce application portal through NetScaler, removing the need to configure an additional authentication source.

**Introduction**

NetScaler and NetScaler Gateway allow enterprise application users to enable single window SAML-based authentication to all their applications, along with solutions requiring pre-authentication and end point analysis, making applications more secure with the ability to limit access by username or IP address and several other advanced security management capabilities.

**Configuration**

Successful integration of a NetScaler appliance with a SAML 2.0 compliant application requires an appliance running NetScaler software release 11.1 or later, with an Enterprise or Platinum license.

**NetScaler features to be enabled**

The following feature must be enabled to use single sign-on with the SAML 2.0 application:

**Authentication, authorization and auditing (AAA)**

The AAA feature 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.
Solution Description

Enabling SSO for the SAML 2.0 application with NetScaler consists of two parts — configuring the SAML 2.0 application portal and the NetScaler appliance. The SAML 2.0 application 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 SAML 2.0 application account has been created, the relevant domain has been added and domain verification for the same has been completed.

Before proceeding, you should verify that you have the signing certificate that NetScaler will use to sign the assertion. To get the certificate from the NetScaler appliance, follow these steps:

- Log on to your NetScaler appliance, and then select the Configuration tab.
- Select Traffic Management > SSL
- On the right, under Tools, select Manage Certificates / Keys / CSR’s

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.
Part 1: Configure the SAML 2.0 application

To configure the SAML 2.0 application, login to your account with administrator credentials, then perform the following steps –

Note: This configuration description is for a generic SAML SSO setup, and will describe common configuration methods for applications which should suffice in most cases. However, in case the required information cannot be found using these means, the support team for the enterprise application should be able to provide the required information.

1. The following information is required for SAML SSO Configuration on NetScaler -
   • ACS (Assertion Consumer Service) URL
   • IDP Certificate (This is the certificate used when configuring the Service Provider)
   • SP Certificate (For some applications, the certificate used to sign the request may be different. This is used to specify the certificate in such cases)
   • Signature (Sign Assertion, Response or Both) - change this setting as per the SP's requirements. You can also choose to send the password (if required)
   • Issuer Name (This value is normally also specified on the SP. This corresponds to the Entity ID for SalesForce, for example)
   • If the SP provides a Service Provider ID as part of its request, it should be specified in the Service Provider ID field. NetScaler will match the value here against the value in the request.
   • the Reject Unsigned Requests option is an added measure for securing the SAML deployment. Not all SPs sign their requests, however, so this is disabled by default.
   • Signature Algorithm and Digest Method - this information can normally be found in the metadata file for the SP. Either SHA-1 or SHA-256.
   • SAML Binding - POST or REDIRECT. This may or may not be documented by the SP, the most common method is POST. If login fails with POST, REDIRECT should be used.
   • Audience - Audience for which assertion sent by NetScaler is applicable. This is typically entity name or url that represents ServiceProvider; not all vendors require it
• For the Request Signature Method, select the hashing algorithm for encrypted requests, either RSA-SHA1 or RSA-SHA256. (we have used SHA-1 for this test, make sure the setting in the NetScaler device matches this value)
• Select Assertion Not Encrypted in the Assertion Decryption Certificate field. This field is available only if your organization supports multiple single sign-on configurations.
• For the SAML Identity Type, select Assertion contains the Federation ID from the User object.
  Note: For each user requiring login to The SAML 2.0 application, the Federation ID (which should correspond to the email address specified in the user’s Active Directory profile) should be defined by navigating to Manage Users>Edit <user name> and then specifying the Federation ID under Single Sign On Information.
• For the SAML Identity Location, select Identity is in the NameIdentifier element of the Subject statement.
• For the Service Provider Initiated Request Binding, select HTTP POST.

Typically, these values should be available in the SAML Metadata for the Service Provider. A sample of the metadata file's contents is given below -

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <md:SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICoDCCAgkCCQCP3M3sQ6/NDANBgkqhkiG9w0BAQUFADCBboEMLAAkGA1UEBhMCVVMxGzA
RBgNVBAsTCKhNhbgG1m3bJuaWEwFjAUsNvBAGcMDyYoY29ycG9ydEVyMDEwMDAwMB4GCSqG
MA0GCSqGSIb3DQEBAQUAA4GAEBlZPzcxMwoGCCsGCSqGSIb3DQEBCwUAA4IBAQuhIb1L2
9f2+upmEaZDzv82cX5i4jQ9dkFLoJYtd4TPW6bLZ7aefxTt5Rg1J7vRnN0b+e1X4I71zW
Vxk6O30HybMnui3i0x+CN860hF3s5l50Hn31mY+VxWQF6wvhhKmGcPvMz6vzJiJk9O
hYQj2831C7sh8Aw2sTc0qZtqB5TtB1q6g9F9f36P7UyX2Ko1Gn2X6t91ZK
</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
m/BjJ6gxNnMi5wBh1tWueqkgT.8RCAFkZUMyp" index="0" isDefault="true"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```
Part 2: Configure the NetScaler Appliance

The following configuration is required on the NetScaler appliance for it to be supported as a SAML identity provider for the application:

- 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 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 LDAP_SSO_Policy as the name. In the Server field, click the ‘+’ icon to add a new server. The Authentication LDAP Server window appears.
   - In the Name field, enter The SAML 2.0 application_LDAP_SSO_Server.
   - 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)
   - Specify the port that the NetScaler will use to communicate with the domain controller. Use 389 for LDAP or 636 for Secure LDAP (LDAPS).
3. 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.
4. 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.
5. Check the box for Bind DN Password and enter the password twice.
6. Under Other Settings: Enter samaccountname as the Server Logon Name Attribute.

7. In the SSO Name Attribute field, enter UserPrincipalName. Enable the User Required and Referrals options. Leave the other settings as they are.

8. 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).

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

10. 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.
Configure the SAML IDP Policy and Profile

For your users to receive the SAML token for logging on to a SAML 2.0 application, 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 (this is an example configuration for SalesForce. Other application configurations will be similar):

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 – application_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, application_SSO_Profile).
6. In the Assertion Consumer Service URL field, enter the URL obtained earlier during SAML application configuration (https://<yourdomain>.my.salesforce.com?so=<encoded value>)
7. In the SP Certificate Name, provide the name for the certificate that was downloaded from the SAML 2.0 application and added to the NetScaler. In case you haven’t, you may do so here by clicking on the + button and providing the certificate file and requisite information.
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://<AAA vserver FQDN>/saml/login
10. Set the Encryption Algorithm to AES256
12. Set both the Signature and Digest algorithms to SHA-1.
13. Set the SAML Binding to POST.
### Solution Guide: SAML 2.0 Single Sign On with Citrix NetScaler

**Assertion Consumer Service URL**
- `https://ctxnstest-dev-ed.my.salesforce`

**IDP Certificate Name**
- `NSSAML`

**SP Certificate Name**
- `SFDC-S5O-Cert`

**Encryption Algorithm**
- `AES256`

**Name ID Format**
- `Unspecified`

**Name ID Expression**
- `HTTP.REQ.USER.ATTRIBUTE(1)`

15. Set the Skew Time to an appropriate value. This is the time difference that will be tolerated between the NetScaler appliance and the The SAML 2.0 application server for the validity of the SAML assertion.

16. Set the Name ID Format to Unspecified, and put HTTP.REQ.USER.ATTRIBUTE(1) in the Name ID Expression field. This directs NetScaler to provide the mail attribute attribute that was defined earlier during LDAP configuration as the user ID for The SAML 2.0 application.

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

18. In the Expression field, add the following expression: HTTP.REQ.HEADER("Referer").CONTAINS("<enterprise application name>")

19. Click Create to complete the SAML IDP Configuration.

Note that this is an example configuration for SalesForce. In general, the following values are sufficient for most applications - ACS (Assertion Consumer Service) URL, Issuer Name, Certificates. some SPs use SHA-1 while others use SHA-256; SPs also vary in terms of binding, with some using POST while others use REDIRECT. It is best to try out different values for these two settings to see which ones will work.

The ACS url, Issuer Name and certificates can generally be obtained from the SP.

To Configure your AAA Virtual Server

Login requests to SAML applications are redirected to a NetScaler AAA or Gateway virtual server that validates the employee’s corporate credentials. This virtual server listens on port 443, which requires an SSL certificate. External and/or internal DNS resolution of the virtual server’s IP address (which is on the NetScaler appliance) is also required. The following steps require a preexisting virtual server to be in place. In addition, they assume that DNS name resolution is already in place, and that the SSL certificate is already installed on your NetScaler appliance.

(This configuration uses the AAA configuration workflow, but the same policies can be used with VPN virtual servers as well)

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 application 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 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 the SSO policy created earlier, 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://<application FQDN>. 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 application profile should appear.
**Troubleshooting**

To help with troubleshooting, here is the list of entries that should be in the ns.log file (located at /var/log on the NetScaler appliance) generated by a successful SAML login. Note that some of the entries such as encrypted hash values will vary.

Jan 24 21:59:49 <local0.debug> 10.105.157.60 01/24/2016:21:59:49 GMT 0-PPE-0 : default AAATM Message 4097 0 : "SAMLIDP: ParseAuthnReq: signature method seen is 4"

Jan 24 21:59:49 <local0.debug> 10.105.157.60 01/24/2016:21:59:49 GMT 0-PPE-0 : default AAATM Message 4098 0 : "SAMLIDP: ParseAuthnReq: digest method seen is SHA1"

Jan 24 21:59:49 <local0.debug> 10.105.157.60 01/24/2016:21:59:49 GMT 0-PPE-0 : default AAATM Message 4099 0 : "SAML verify digest: digest algorithm SHA1, input for digest: <samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" AssertionConsumerServiceURL="https://ctxnstest-dev-ed.my.TheSAML 2.0 applicationtest.com?so=00D280000017RJa" Destination="https://nssaml.abc.com/saml/login" ID="_2CAAAAVMF2dNRME8wMjgwMDAwMDA0Qzk3AAAXxmsWAke7ouLLn-jaXRvQESM03_sXxdORaoCarGgbpLrqza7jb_eoaAsZKfpXgnulPpb8uRkVWVhVa2niiXvxF7AQ1kij2ICAgJNaLgtvPIAV6jhuWMU11-rje3Pq__dW0nFqRz196yv766q7a5bvd02rdqvTpQz38jWz-oOsnQ9s7a1L9EhHhDpUr11VxbyPnmzF1UakABTLWC1T_qXZyN3J3xhSaYnLc7-YbRD8VrsehWUyP0dp7Qoeu5RVkwQ" IssueInstant="2016-01-24T22:01:15.269Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">\nsaml:AuthnRequest xmlns:samlc:SAML:2.0:assertions: https://ctxnstest-dev-ed.my.TheSAML 2.0 applicationtest.com</samlp:AuthnRequest>"


Jan 24 22:00:05 <local0.info> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default AAA Message 4106 0 : "In update aaa _ cntr: Succeeded policy for user u3test = ldap2"
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default AAATM Message 4107 0 : "extracted SSOnusername: U3Test@CTXNS.net for user u3test"
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default SSLVPN Message 4108 0 : "sslvpn_extract_attributes_from_resp: attributes copied so far are U3Test@ctxns.com"
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default SSLVPN Message 4109 0 : "sslvpn_extract_attributes_from_resp: total len copied 21, mask 0x1"
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default AAATM Message 4110 0 : "SAMLIDP: Checking whether current flow is SAML IdP flow, input U0ZEQ19TU09fUHJvZmlsZQBDQk1fMkNBQUFBVkJGmROUk1F0-HdNamd3TURBd0IEQTBRemszQUFbQXhcldBa2U3b3VMbg4tamFYUnZRWWNNDFnc1h4ZE9SY-W9DYVWJhWJxclpqY119i9fZkwmcnFhmbVMUHBLOHSVai1XZTnZoQWYebmkyeFZGNOFRMwtpa-jlxQ0EZf0PUxndH2QSFUNmpoV01VSWtcmpM11jX19kVzBuRnFSenNsOTZ5djc2NhE3YWE1Yn-ZkMrJy2Hf2HvBRm41d61W9pBuNnUw1c2E3TDFeWhAeRwqVVybDFWGJ5GfWkZaWVFrQU-JUTFdpfDFReVhAe4uzSjN4aFNhW5MYzcTW1CRDWhCnN1aFVeVAwZHA3UW9lTV5Vmt3USZiaW5k-PXBvc3QmLw="
Jan 24 22:00:05 <local0.info> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default AAA EXTRACTED_GROUPS 4111 0 : Extracted_groups "LyncDL,TestDL-Lync"
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default AAAATM LOGIN 4112 0 : Context u3test@116.202.102.156 - SessionId: 28- User u3test - Client_ip 116.202.102.156 - 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 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT 0-PPE-0 : default SSLVPN Message 4114 0 : "UnifiedGateway: SSOID update skipped due to SteeUp or LoginOnce OFF, user: u3test"


Conclusion

NetScaler provides a secure and seamless experience with The SAML 2.0 application by enabling single sign-on into The SAML 2.0 application accounts, avoiding the need for users to remember multiple passwords and user IDs, while reducing the administrative overhead involved in maintaining these deployments.