Integrating Oracle Access Manager with Citrix NetScaler as SAML IDP

Solution Guide

This guide focuses on defining the process for deploying Oracle Access Manager as an IdP, with NetScaler acting as the SAML IDP.

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 Oracle Fusion Middleware users to log on to their enterprise Oracle applications through NetScaler, removing the need to log on with Oracle Access Manager and avoiding having to configure an additional authentication source.

Introduction

This solution allows the integration of Oracle Access Manager with NetScaler. This guide focuses on enabling OAM single sign on with Citrix NetScaler acting as a SAML IDP, allowing Oracle Fusion Middleware applications to authenticate users with NetScaler AAA credentials.

Oracle Access Management provides traditional access management capabilities along with some advanced identity management capabilities such as adaptive authentication, federated single-sign on (SSO), risk analysis, and fine-grained authorization which can also be extended to mobile clients and mobile applications. OAM is an integral part of the authentication and authorization framework that facilitates access to the Oracle enterprise software suite.

Configuration

Successful integration of a NetScaler appliance with OAM requires an appliance running NetScaler software release 11.0 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 OAM:
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.

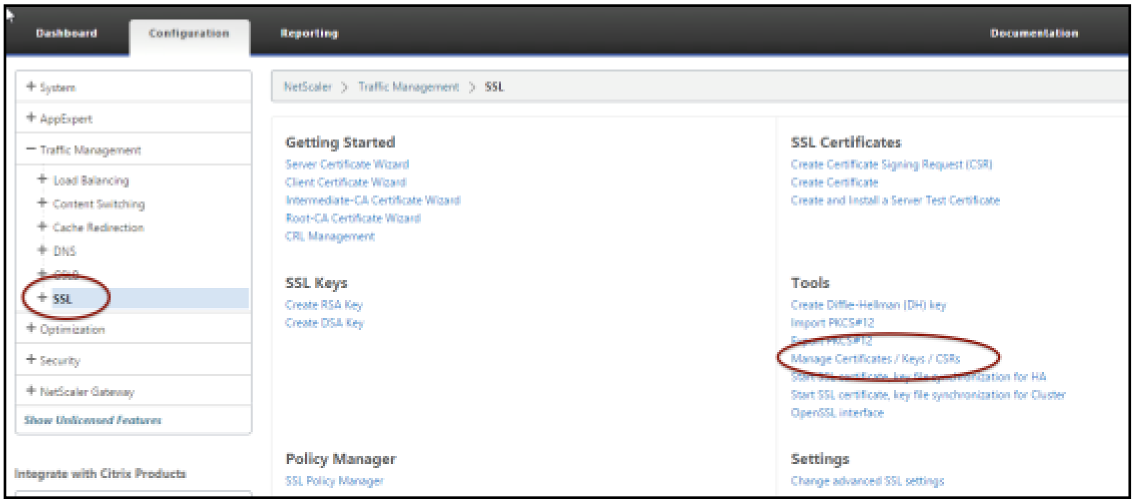
Solution Description

Enabling SSO for OAM with NetScaler has two parts: configuring the OAM portal and configuring the NetScaler appliance. OAM 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, along with the authentication (LDAP in our example) policy used to authenticate users for issuing the SAML token.

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 user accounts and the required user directories have been created and configured on OAM.

Before proceeding, you will require the certificate that OAM will use to verify the SAML assertion from NetScaler. To get the verification 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

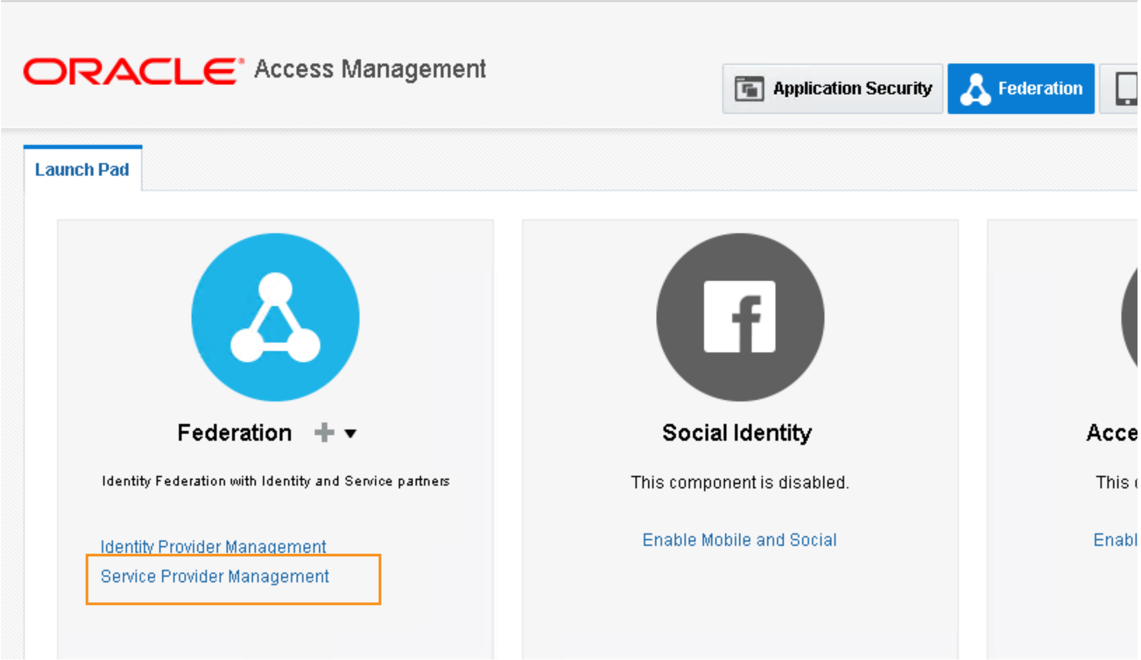

Dashboard
Configuration
Reporting
Documentation
+ System
+ AppExpert
− Traffic Management
+ Load Balancing
+ Content Switching
+ Cache Redirection
+ DNS
+ GSLB
+ SSL
+ Optimization
+ Security
+ NetScaler Gateway
Show Unlicensed Features
Integrate with Citrix Products
NetScaler > Traffic Management > SSL
Getting Started
Server Certificate Wizard
Client Certificate Wizard
Intermediate-CA Certificate Wizard
Root-CA Certificate Wizard
CRL Management
SSL Certificates
Create Certificate Signing Request (CSR)
Create Certificate
Create and Install a Server Test Certificate
SSL Keys
Create RSA Key
Create DSA Key
Tools
Create Diffie-Hellman (DH) key
Import PKCS#12
Export PKCS#12
Manage Certificates / Keys / CSRs
Start SSL certificate, key file synchronization for HA
Start SSL certificate, key file synchronization for Cluster
OpenSSL interface
Policy Manager
SSL Policy Manager
Settings
Change advanced SSL settings

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.

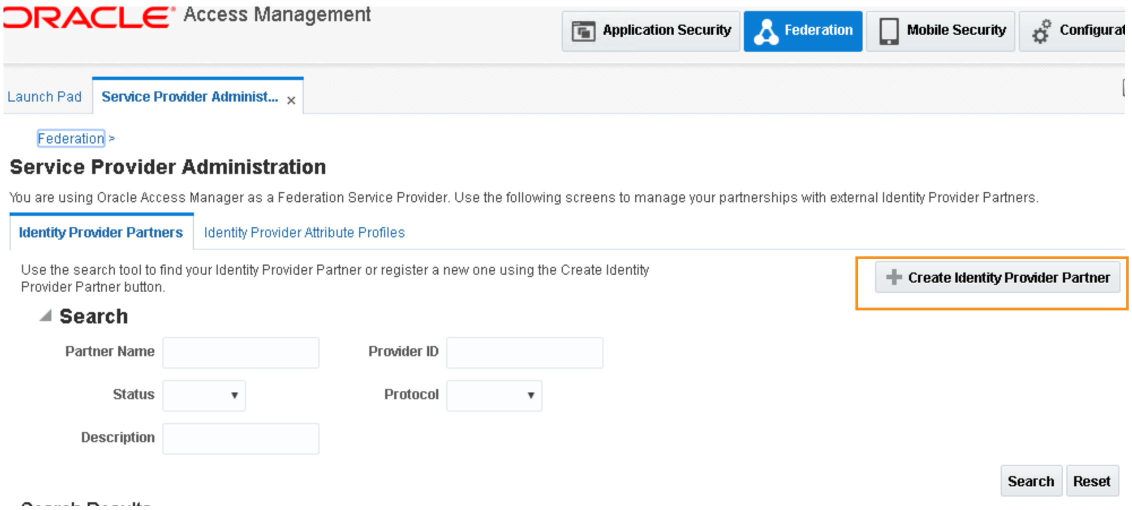
Part 1: Configure OAM

To configure OAM, log on to your OAM account with administrator credentials, and then do the following:

1. On the main configuration page, click the Federation button in the top right corner of the screen.
2. On the Federation page, in the Federation section, click the Service Provider Management link. (In the OAM console, the Identity Provider Management section manages SPs (Service providers) bound to OAM, and the Service Provider Management section manages IDPs (Identity Providers) bound to OAM).


ORACLE Access Management
Application Security
Federation
Launch Pad
Federation
Identity Federation with Identity and Service partners
Identity Provider Management
Service Provider Management
Social Identity
This component is disabled.
Enable Mobile and Social
Acce
This
Enabl

3. On the Service Provider Administration screen, click the Create Identity Provider Partner button.


ORACLE Access Management
Application Security
Federation
Mobile Security
Configurat
Launch Pad
Service Provider Administ... ×
Federation >
Identity Provider Partners
Identity Provider Attribute Profiles
Create Identity Provider Partner
Search

Service Provider Administration

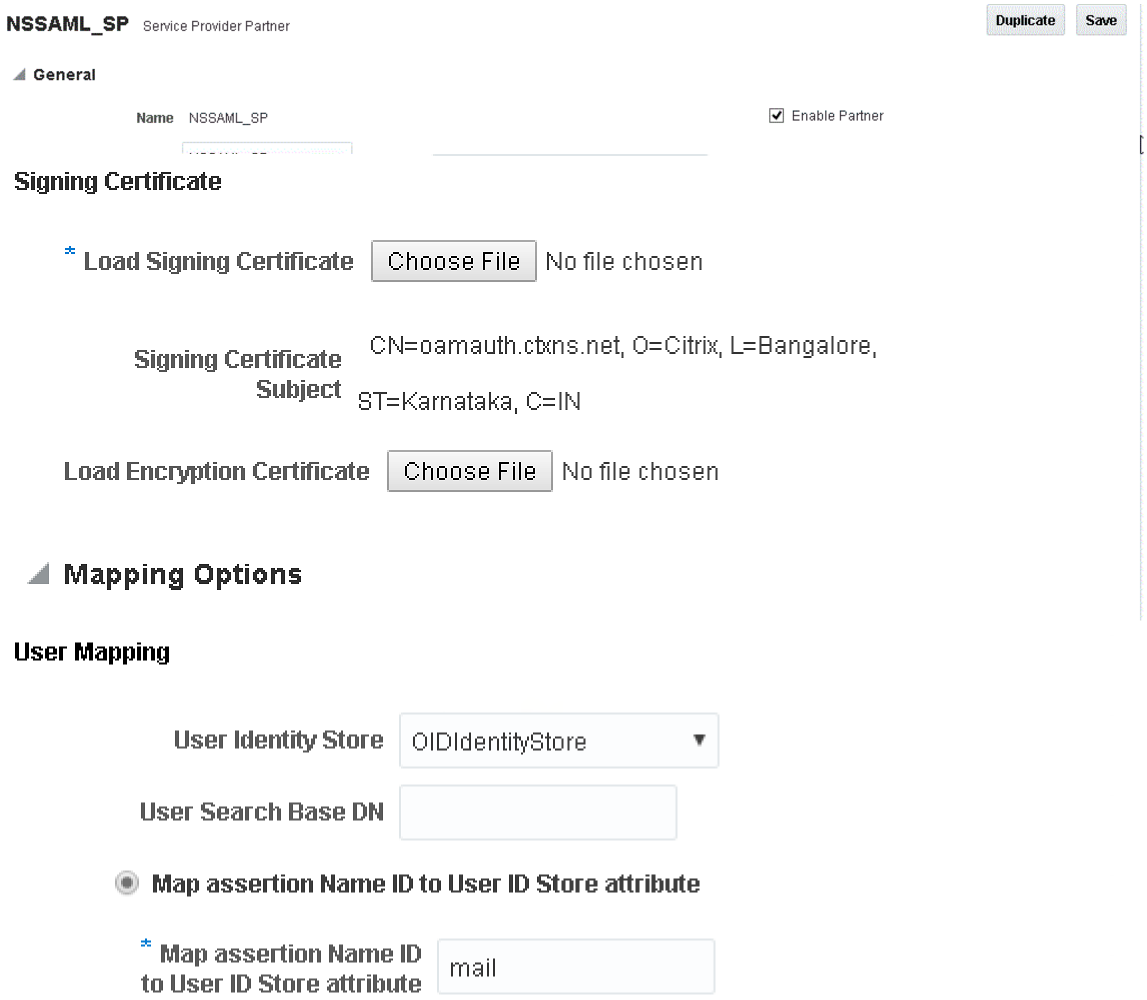
You are using Oracle Access Manager as a Federation Service Provider. Use the following screens to manage your partnerships with external Identity Provider Partners.

Use the search tool to find your Identity Provider Partner or register a new one using the Create Identity Provider Partner button.

Partner Name
Provider ID
Status ▾
Protocol ▾
Description

Search Reset

4. On the configuration screen, set the parameters listed under the following screen shot.



NSSAML_SP Service Provider Partner

Name NSSAML_SP

☑ Enable Partner

Signing Certificate

* Load Signing Certificate: Choose File No file chosen

Signing Certificate Subject: CN=oamauth.ctxns.net, O=Citrix, L=Bangalore, ST=Karnataka, C=IN

Load Encryption Certificate: Choose File No file chosen

Mapping Options

User Mapping

User Identity Store: OIDIdentityStore ▾

User Search Base DN:

● Map assertion Name ID to User ID Store attribute

* Map assertion Name ID to User ID Store attribute: mail

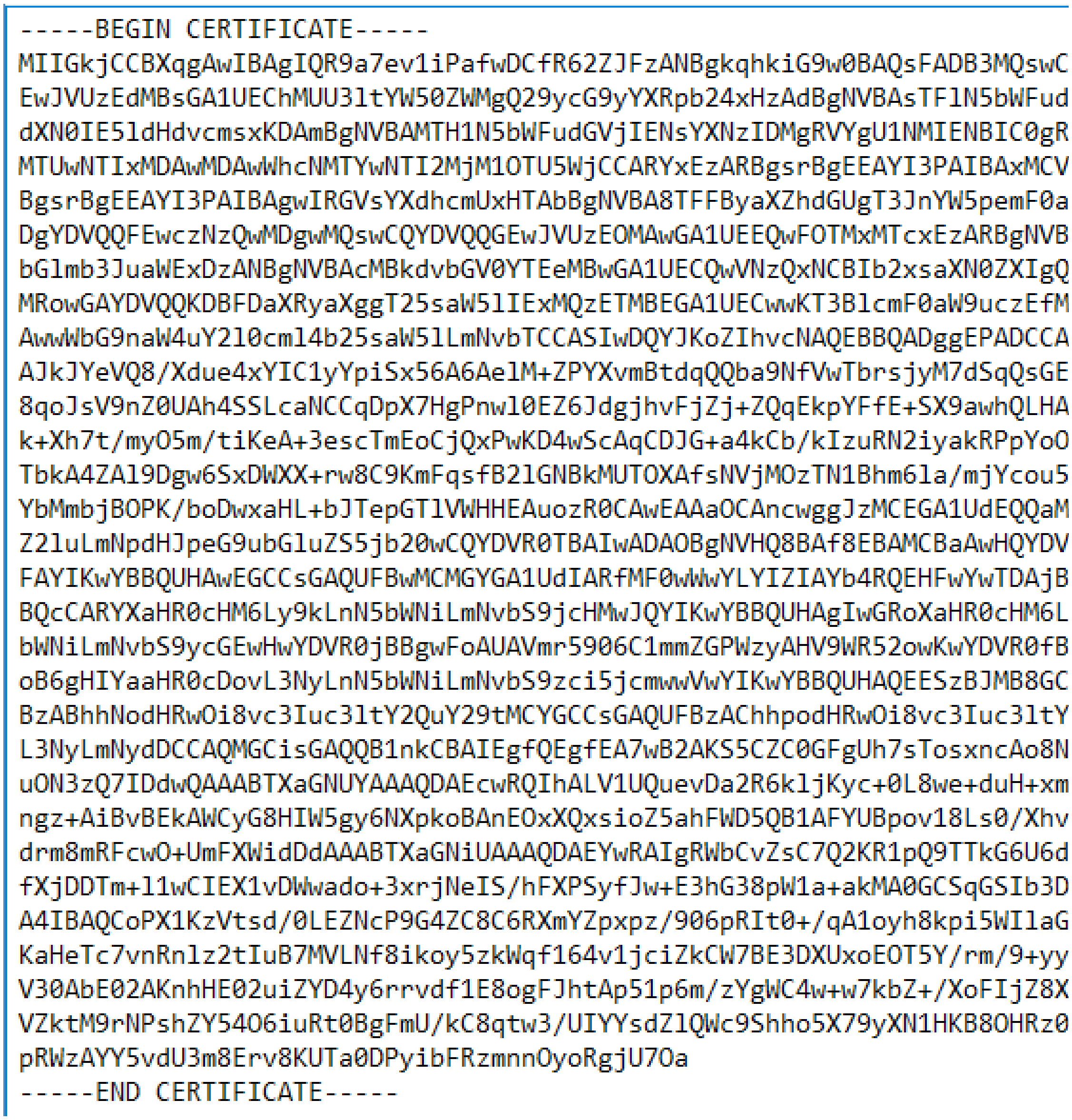
In the Signing Certificate section:
Load signing Certificate: Browse to the signing certificate that is specified as the Service Provider (SP) certificate on the NetScaler appliance.
Load Encryption Certificate: Add a certificate to be used to encrypt the assertions sent (Optional)

Select the appropriate User Identity Store in the User Mapping Section, and select Map assertion Name ID to User ID Store attribute.

Post this configuration, bind this profile to the Authentication Scheme and module created for the Oracle FMW application that is integrated with OAM.

Extracting the OAM SP certificate for NetScaler

To extract the OAM SP certificate, navigate to http://public-oam-host:public-oam-port/oamfed/sp/metadata (http://10.105.157.147:14100/oamfed/sp/metadata in our setup), and then download the metadata XML file. In the file, look for the X.509 certificate tag, and copy the contents of the tag into a Notepad file. Add BEGIN and END certificate tags at the beginning and end of the file as shown below.



```
-----BEGIN CERTIFICATE-----
MIIGkjCCBXqgAwIBAgIQR9a7ev1iPafwDCfR62ZJFzANBgkqhkiG9w0BAQsFADB3MQswC
EwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAdBgNVBAsTFlN5bWFud
dXN0IE5ldHdvcmsxKDAmBgNVBAMTH1N5bWFudGVjIENsYXNzIDMgRVYgU1NMIENBIC0gR
MTUwNTIxMDAwMDAwWhcNMTYwNTI2MjM1OTU5WjCCARYxEzARBgsrBgEEAYI3PAIBAxMCV
BgsrBgEEAYI3PAIBAgwIRGVsYXdhcmUxHTAbBgNVBA8TFFByaXZhdGUgT3JnYW5pemF0a
DgYDVQQFEwczNzQwMDgwMQswCQYDVQQGEwJVUzEOMAwGA1UEEQwFOTMxMTcxEzARBgNVB
bGlmb3JuaWExDzANBgNVBAcMBkdvbGV0YTEeMBwGA1UECQwVNzQxNCBIb2xsaXN0ZXIgQ
MRowGAYDVQQKDBFDaXRyaXggT25saW5lIExMQzETMBEGA1UECwwKT3BlcmF0aW9uczEfM
AwwWbG9naW4uY2l0cml4b25saW5lLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCA
AJkJYeVQ8/Xdue4xYIC1yYpiSx56A6AelM+ZPYXvmBtdqQQba9NfVwTbrsjyM7dSqQsGE
8qoJsV9nZ0UAh4SSLcaNCCqDpX7HgPnwl0EZ6JdgjhvFjZj+ZQqEkpYFfE+SX9awhQLHA
k+Xh7t/myO5m/tiKeA+3escTmEoCjQxPwKD4wScAqCDJG+a4kCb/kIzuRN2iyakRPpYoO
TbkA4ZAl9Dgw6SxDWXX+rw8C9KmFqsfB2lGNBkMUTOXAfsNVjMOzTN1Bhm6la/mjYcou5
YbMmbjBOPK/boDwxaHL+bJTepGTlVWHHEAuozR0CAwEAAaOCAncwggJzMCEGA1UdEQQaM
Z2luLmNpdHJpeG9ubGluZS5jb20wCQYDVR0TBAIwADAOBgNVHQ8BAf8EBAMCBaAwHQYDV
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMGYGA1UdIARfMF0wWwYLYIZIAYb4RQEHFwYwTDAjB
BQcCARYXaHR0cHM6Ly9kLnN5bWNiLmNvbS9jcHMwJQYIKwYBBQUHAgIwGRoXaHR0cHM6L
bWNiLmNvbS9ycGEwHwYDVR0jBBgwFoAUAVmr5906C1mmZGPWzyAHV9WR52owKwYDVR0fB
oB6gHIYaaHR0cDovL3NyLnN5bWNiLmNvbS9zci5jcmwwVwYIKwYBBQUHAQEESzBJMB8GC
BzABhhNodHRwOi8vc3Iuc3ltY2QuY29tMCYGCCsGAQUFBzAChhpodHRwOi8vc3Iuc3ltY
L3NyLmNydDCCAQMGCisGAQQB1nkCBAIEgfQEgfEA7wB2AKS5CZC0GFgUh7sTosxncAo8N
uON3zQ7IDdwQAAABTXaGNUYAAAQDAEcwRQIhALV1UQuevDa2R6kljKyc+0L8we+duH+xm
ngz+AiBvBEkAWCyG8HIW5gy6NXpkoBAnEOxXQxsioZ5ahFWD5QB1AFYUBpov18Ls0/Xhv
drm8mRFcwO+UmFXWidDdAAABTXaGNiUAAAQDAEYwRAIgRWbCvZsC7Q2KR1pQ9TTkG6U6d
fXjDDTm+l1wCIEX1vDWwado+3xrjNeIS/hFXPSyfJw+E3hG38pW1a+akMA0GCSqGSIb3D
A4IBAQCoPX1KzVtsd/0LEZNcP9G4ZC8C6RXmYZpxpz/906pRIt0+/qA1oyh8kpi5WIlaG
KaHeTc7vnRnlz2tIuB7MVLNf8ikoy5zkWqf164v1jciZkCW7BE3DXUxoEOT5Y/rm/9+yy
V30AbE02AKnhHE02uiZYD4y6rrvdf1E8ogFJhtAp51p6m/zYgWC4w+w7kbZ+/XoFIjZ8X
VZktM9rNPshZY54O6iuRt0BgFmU/kC8qtw3/UIYYsdZlQWc9Shho5X79yXN1HKB8OHRz0
pRWzAYY5vdU3m8Erv8KUTa0DPyibFRzmnnOyoRgjU7Oa
-----END CERTIFICATE-----
```

To make sure the certificate can be added in NetScaler, place an **Enter** character after every 64th character.

Add the certificate to the NetScaler appliance in the **Traffic Management > SSL > Manage Certificates** section.

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 OAM:

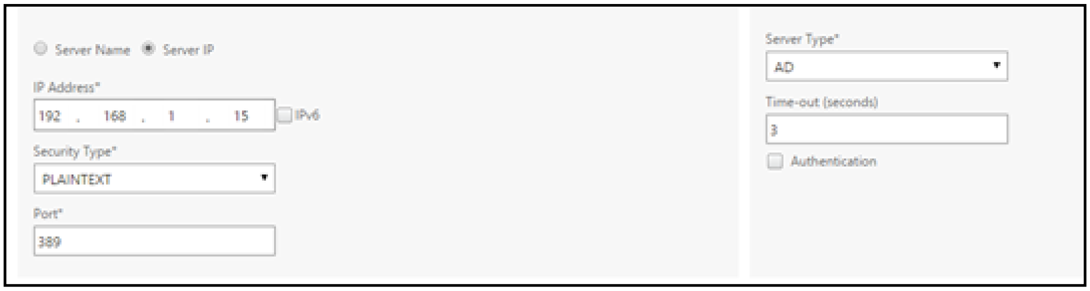
- LDAP authentication policy and server for domain authentication
- SSL certificate with external and internal DNS configured for the FQDN presented by the certificate (Wildcard certificates are supported.)
- SAML IDP policy and profile
- AAA virtual server

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 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.
   - In the Name field, enter OAM_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).



○ Server Name ● Server IP

IP Address*: 192 . 168 . 1 . 15 □ IPv6

Security Type*: PLAINTEXT

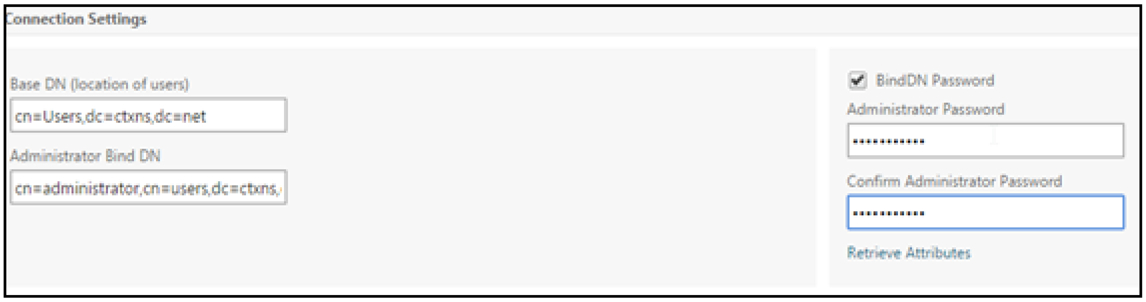
Port*: 389

Server Type*: AD

Time-out (seconds): 3

□ Authentication

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.



Connection Settings

Base DN (location of users)
cn=Users,dc=ctxns,dc=net

Administrator Bind DN
cn=administrator,cn=users,dc=ctxns,

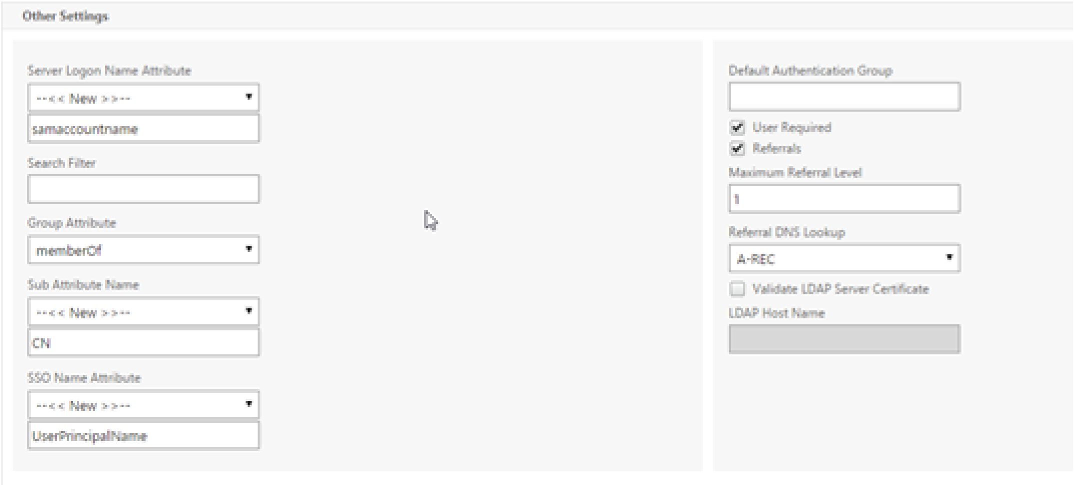
☑ BindDN Password

Administrator Password
••••••••••••

Confirm Administrator Password
••••••••••••

Retrieve Attributes

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.



Other Settings

Server Logon Name Attribute
--<< New >>--
samaccountname

Search Filter

Group Attribute
memberOf

Sub Attribute Name
--<< New >>--
CN

SSO Name Attribute
--<< New >>--
UserPrincipalName

Default Authentication Group

☑ User Required
☑ Referrals

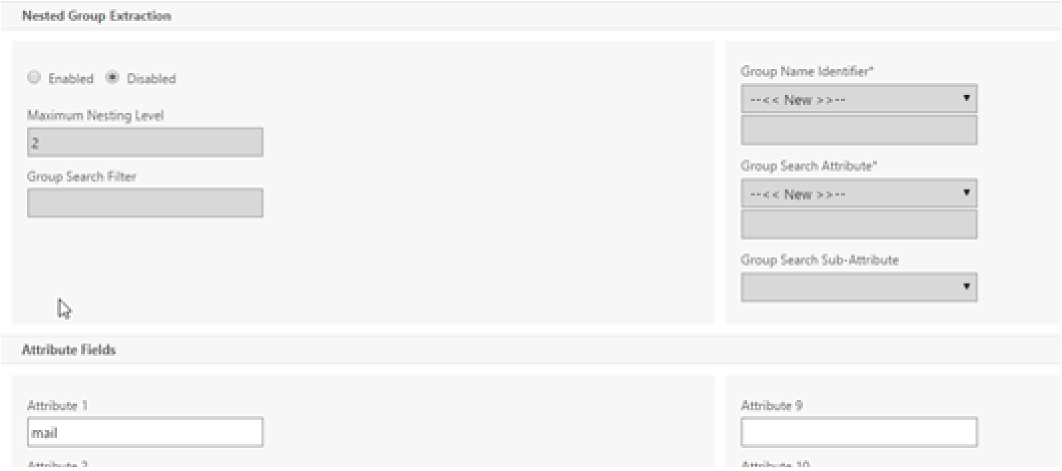
Maximum Referral Level
1

Referral DNS Lookup
A-REC

☐ Validate LDAP Server Certificate

LDAP Host Name

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)



Nested Group Extraction

○ Enabled ● Disabled

Maximum Nesting Level
2

Group Search Filter

Group Name Identifier*
--<< New >>--

Group Search Attribute*
--<< New >>--

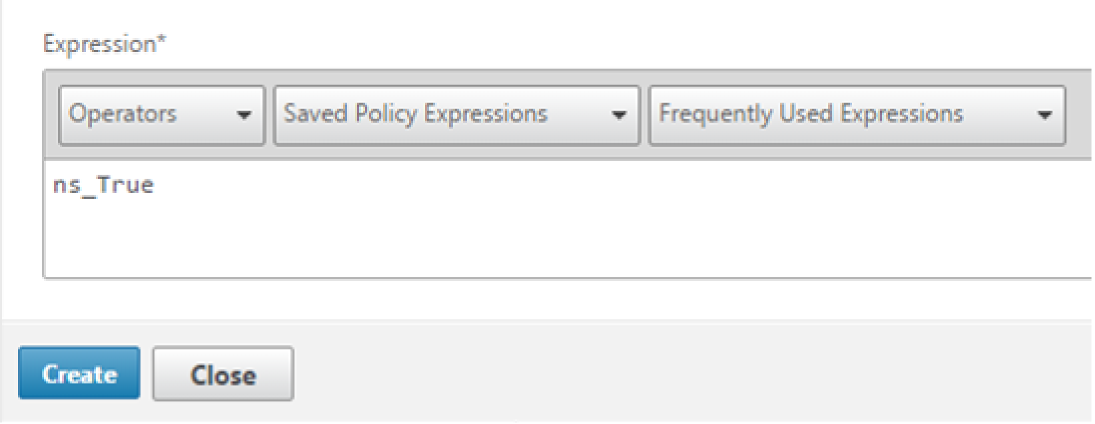
Group Search Sub-Attribute

Attribute Fields

Attribute 1
mail

Attribute 9

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.



```
ns_True
```

Configure the SAML IDP Policy and Profile

For your users to receive the SAML token for logging on to OAM, 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 – OAM_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, OAM_SSO_Profile).
6. In the Assertion Consumer Service URL field, enter the URL obtained earlier during OAM configuration (http://<FQDN of the OAM server> :<port hosting IDM/OAM server>/oam/fed>) (The example URL in the test environment is http://idmlb.ctxns.net:14100/oam/fed)
7. In the SP Certificate Name, provide the name for the certificate that was downloaded from OAM 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
11. Set the Service Provider ID field to the value set for the Provider ID field in OAM IDP configuration.
12. Set both the Signature and Digest algorithms to SHA-1.
13. Set the SAML Binding to POST.

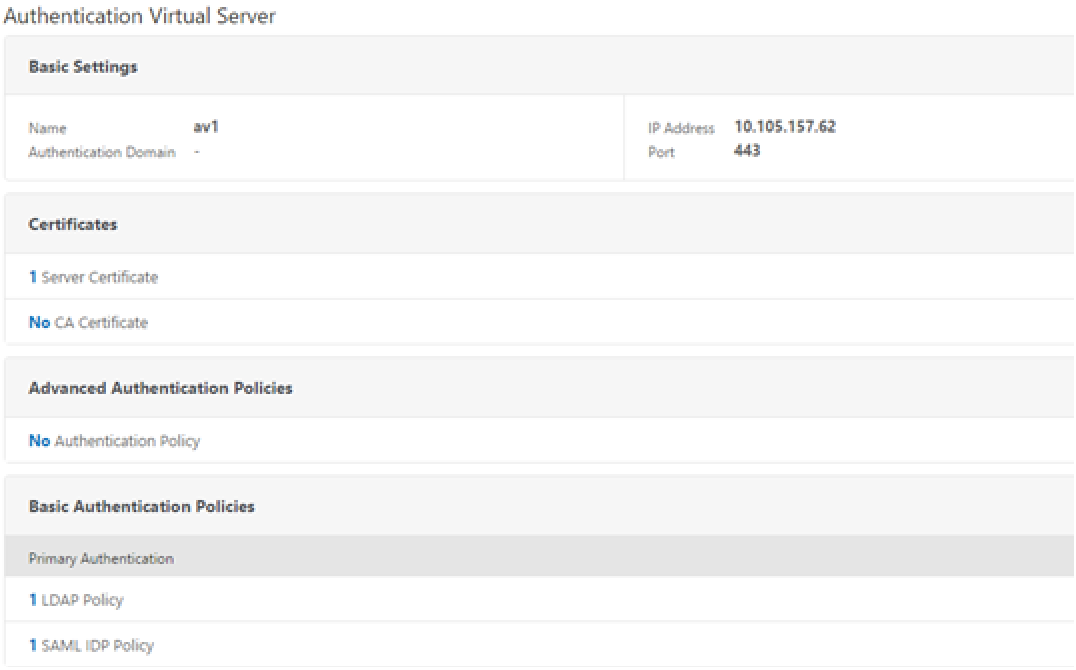
14. Click on More, then put http://idmlb.ctxns.net:14100/oam/fed. in the Audience field. (change as appropriate for your environment)
15. Set the Skew Time to an appropriate value. This is the time difference that will be tolerated between the NetScaler appliance and the OAM server for the validity of 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 OAM.
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("oam")
19. Click Create to complete the SAML IDP Configuration.

To Configure your AAA Virtual Server

An employee trying to log in to OAM is redirected to a NetScaler AAA 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.

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 OAM 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 OAM_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 OAM_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

Basic Settings

Name av1
Authentication Domain -

IP Address 10.105.157.62
Port 443

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

Validate the configuration

Point your browser to http://idmlb.ctxns.net:14100/oam/fed. 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 OAM 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 : de-
fault 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 : de-
fault 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.oamtest.
com?so=00D280000017RJa" Destination="https://nssaml.abc.com/saml/login" ID=" _ 2
CAAAAVMF2dNRME8wMjgwMDAwMDA0Qzk3AAAAxmsWAke7ouLln-jaXRvQESM03 _ sXxdORaoCaR-
GabpLrqsZjb _ eoAsZKfpXgnuLPpb8uRkVWNvhAa2ni2xVF7AQ1kij21CA6 _ JNaLgtvPIAV6jh-
WMUIl-rje3Pq _ _ dW0nFqRzsl96yv766q7aa5bvd02rdqvTpQz38jWz-oOnsnQh5sa7L9EyhH-
hDpAUrl1VXbyPnmZFlUakABTLWClT _ qXZyN3J3xhSaYnLc7-YiBD8VrsehWUyP0dp7Qoeu5RVkwQ"
IssueInstant="2016-01-24T22:01:15.269Z" ProtocolBinding="urn:oasis:names:tc:SAML
:2.0:bindings:HTTP-POST" Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names
:tc:SAML:2.0:assertion">https://ctxnstest-dev-ed.my.oamtest.com</saml:Issuer></
samlp:AuthnRequest>"
Jan 24 21:59:49 <local0.debug> 10.105.157.60 01/24/2016:21:59:49 GMT  0-PPE-0 :
default AAATM Message 4100 0 :  "SAML signature validation: algorithm is RSA-
SHA1 input buffer is: <ds:SignedInfo xmlns:ds="http://www.w3.org/2000/09/xmld-
sig#"> <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"></ds:CanonicalizationMethod> <ds:SignatureMethod Algorithm="http://www.
w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod> <ds:Reference URI="# _ 2
CAAAAVMF2dNRME8wMjgwMDAwMDA0Qzk3AAAAxmsWAke7ouLln-jaXRvQESM03 _ sXxdORaoCaR-
GabpLrqsZjb _ eoAsZKfpXgnuLPpb8uRkVWNvhAa2ni2xVF7AQ1kij21CA6 _ JNaLgtvPIAV6jh-
WMUIl-rje3Pq _ _ dW0nFqRzsl96yv766q7aa5bvd02rdqvTpQz38jWz-oOnsnQh5sa7L9EyhH-
hDpAUrl1VXbyPnmZFlUakABTLWClT _ qXZyN3J3xhSaYnLc7-YiBD8VrsehWUyP0dp7Qoeu5RVkwQ">
<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#"><ec:InclusiveNamespaces xmlns:ec="http://www.
w3.org/2001/10/xml-exc-c14n#" PrefixList="ds saml samlp"></ec:InclusiveNa
Jan 24 21:59:50 <local0.debug> 10.105.157.60 01/24/2016:21:59:50 GMT  0-PPE-
0 : default SSLLOG SSL _ HANDSHAKE _ SUCCESS 4101 0 :  SPCBId 936 - ClientIP
116.202.102.156 - ClientPort 60823 - VserverServiceIP 10.105.157.62 - VserverSer-
vicePort 443 - ClientVersion TLSv1.0 - CipherSuite "AES-256-CBC-SHA TLSv1 Non-
Export 256-bit" - Session Reuse

Jan 24 22:00:05 <local0.info> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-0 : de-
fault 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 : de-
fault AAATM Message 4107 0 :  "extracted SSOusername: 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 : de-
fault SSLVPN Message 4108 0 :  "sslvpn_extract_attributes_from_resp: at-
tributes 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 : de-
fault 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 U0ZEQ19TU09fUHJvZmlsZQBJRD1fMkNBQUFBVk1GMmROUk1FO-
HdNamd3TURBd01EQTBRemszQUFBQXhtc1dBa2U3b3VMbG4tamFYUnZRRVNNMDNfc1h4ZE9SY-
W9DYVJHYWJwTHJxc1pqYl9lb0FzWktmcFhnbnVMUHBiOHVSa1ZXTnZoQWEybmkyeFZGN0FRMWtpa-
jIxQ0E2X0pOYUxndHZQSUFWNmpoV01VSWwtcmplM1BxX19kVzBuRnFSenNsOTZ5djc2NnE3YWE1Yn-
ZkMDJyZHF2VHBRejM4ald6LW9PbnNuUWg1c2E3TDlFeWhIaERwQVVybDFWWGJ5UG5tWkZsVWFrQU-
JUTFdDbFRfcVhaeU4zSjN4aFNhWW5MYzctWWlCRDhWcnNlaFdVeVAwZHA3UW9ldTVSVmt3USZiaW5k-
PXBvc3QmLw=="
Jan 24 22:00:05 <local0.info> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-0 : de-
fault AAA EXTRACTED_GROUPS 4111 0 :  Extracted_groups "LyncDL,TestDL-LYnc"
Jan 24 22:00:05 <local0.info> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-
0 : default AAATM 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; Tri-
dent/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 AAATM Message 4113 0 :  "SAMLIDP: Checking whether current flow
is SAML IdP flow, input U0ZEQ19TU09fUHJvZmlsZQBJRD1fMkNBQUFBVk1GMmROUk1FO-
HdNamd3TURBd01EQTBRemszQUFBQXhtc1dBa2U3b3VMbG4tamFYUnZRRVNNMDNfc1h4ZE9SY-
W9DYVJHYWJwTHJxc1pqYl9lb0FzWktmcFhnbnVMUHBiOHVSa1ZXTnZoQWEybmkyeFZGN0FRMWtpa-
jIxQ0E2X0pOYUxndHZQSUFWNmpoV01VSWwtcmplM1BxX19kVzBuRnFSenNsOTZ5djc2NnE3YWE1Yn-
ZkMDJyZHF2VHBRejM4ald6LW9PbnNuUWg1c2E3TDlFeWhIaERwQVVybDFWWGJ5UG5tWkZsVWFrQU-
JUTFdDbFRfcVhaeU4zSjN4aFNhWW5MYzctWWlCRDhWcnNlaFdVeVAwZHA3UW9ldTVSVmt3USZiaW5k-
PXBvc3QmLw=="
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
StepUp or LoginOnce OFF, user: u3test"

Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-
0 : default AAATM Message 4115 0 :  "SAML: SendAssertion: Response tag
is <samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://ctxnstest-dev-ed.my.oamtest.com?so=00D280000017RJa"
ID="_c270d0f96123132442d36933c567946d" IssueInstant="2016-01-24T22:00:05Z"
Version="2.0"><saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Fo
rmat="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://nssaml.abc.com/
saml/login</saml:Issuer><samlp:Status><samlp:StatusCode Value="urn:oasis:names:t
c:SAML:2.0:status:Success"></samlp:StatusCode></samlp:Status>"
```

```
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-
0 : default AAATM Message 4116 0 :  "SAML: SendAssertion: Asser-
tion tag is <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:a
ssertion" ID=" _ c270d0f96123132442d36933c567946" IssueInstant="2016-01-
24T22:00:05Z" Version="2.0"><saml:Issuer Format="urn:oasis:names:tc:SAML:
2.0:nameid-format:entity">https://nssaml.abc.com/saml/login</saml:Issuer
><saml:Subject><saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">U3Test@ctxns.com</saml:NameID><saml:SubjectConfirmati
on Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmat
ionData NotOnOrAfter="2016-01-24T22:15:05Z" Recipient="https://ctxnstest-
dev-ed.my.oamtest.com?so=00D280000017RJa"></saml:SubjectConfirmationData></
saml:SubjectConfirmation></saml:Subject><saml:Conditions NotBefore="2016-
01-24T21:45:05Z" NotOnOrAfter="2016-01-24T22:15:05Z"><saml:AudienceRestrictio
n><saml:Audience>https://ctxnstest-dev-ed.my.oamtest.com</saml:Audience></
saml:AudienceRestriction></saml:Condition
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-
0 : default AAATM Message 4117 0 :  "SAML: SendAssertion, Digest Meth-
od SHA1, 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:SignatureMeth
od Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMetho
d><ds:Reference URI="# _ c270d0f96123132442d36933c567946"><ds:Transforms><ds:T
ransform 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/2000/09/xmldsig#sha1"></ds:DigestMethod><ds:DigestValue>LrFDglgJA/29P9jWEl
MXnbynS48=</ds:DigestValue></ds:Reference></ds:SignedInfo>"
Jan 24 22:00:05 <local0.debug> 10.105.157.60 01/24/2016:22:00:05 GMT  0-PPE-
0 : default AAATM Message 4118 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/2000/09/xmldsig#rsa-sha1"></ds:S
ignatureMethod><ds:Reference URI="# _ c270d0f96123132442d36933c567946"><ds:Transf
orms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signa-
ture"></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/2000/09/xmldsig#sha1"></ds:DigestMethod><ds:DigestValue>LrFDglgJA/29P9jWEl
MXnbynS48=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>HU1
oBZCHXn7L2/qKT2LzwD13QvlONjsapEBkXlQNbwG83VC61UdTnDFWmn+9RP5QmZt60TvbfCaVx2vVuM
zDFi82oO9Rvw3N4TQjnSlFatg3JKDHuOEUfi4pBxJr
```

Conclusion

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

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States