

Citrix NetScaler Gateway OWA (SP-initiated) integration guide

Introduction

Use this guide to enable Single Sign-on (SSO) access via SAML to Outlook Web Access (OWA) on Citrix NetScaler Gateway and NetScaler AAA. NetScaler AAA is the authentication, authorization, and auditing feature configured in virtual servers on the NetScaler Gateway appliance.

The following is an outline briefly describing the order of configurations for SecureAuth IdP, NetScaler Gateway, and NetScaler AAA:

- **SecureAuth IdP configuration** – SecureAuth IdP configured for SAML assertion with NetScaler as a Service Provider
- **NetScaler AAA configuration** – SecureAuth IdP and OWA form-based authentication
 - **Load balancing virtual server** – create a load balancing virtual server configured with OWA on Exchange server as a service
 - **AAA authentication virtual server** – for the OWA virtual server, add AAA authentication virtual server in the Authentication Policy
 - **Traffic policy for OWA logout** – create a traffic policy for OWA logout
- **NetScaler AAA configuration** – for SecureAuth IdP and OWA Integrated Windows Authentication
 - **Active Directory configuration** – add an Active Directory service account in NetScaler
 - **Kerberos configuration** – add a Kerberos (KCD) account in NetScaler
- **NetScaler Gateway configuration** – for SecureAuth IdP and OWA forms-based authentication
 - **VPN virtual server** – add a VPN virtual server in NetScaler
 - **OWA on Exchange 2010** – add rewrite policy for OWA on Exchange 2010 authentication
 - **OWA on Exchange 2010 for iPhone and iPad** – add two rewrite policies for OWA on Exchange 2010 authentication for iPhone and iPad

Prerequisites

- SecureAuth IdP version 9.1 or later with a realm ready for the NetScaler OWA integration
- [SAML20SPInitPost.aspx-9.1.zip](#) file
- Citrix NetScaler 11.0 with a valid and appropriate license
- Citrix NetScaler platform license with AAA feature functionality enabled
- Exchange 2013 or 2016 (Note: Exchange 2010 is supported with the right Post Parameters - contact Customer Support.)

SecureAuth IdP configuration steps

1. Download the [SAML20SPInitPost.aspx-9.1.zip](#) file and extract contents into the \Customized folder for the SecureAuth IdP realm used for this integration.

For example, D:\SecureAuth\SecureAuth(Realm#)\Customized\

2. Log in to your **SecureAuth IdP Admin** console.

Workflow tab

3. Select the **Workflow** tab.

4. In the Custom Identity Consumer section, make the following entries:

- Set **Token Data Type (Send)** to **Custom**.
- Set the **Custom Token Fields** to **Password**.
- Click the >> button to populate the next field with **{Password}**.

Custom Identity Consumer

Receive Token: Send Token Only

Require Begin Site: False

User Impersonation: True

Windows Authentication: True

Use Kernel Mode: True

Use AppPool Credentials: True For custom SPN

Token Data Type (Receive): Name

Token Data Type (Send): Custom [Token Settings](#)

Custom Token Fields: Password

Custom Token Fields: {Password}

5. Click **Save**.

Post Authentication tab

6. Select the **Post Authentication** tab.

7. In the **Post Authentication** section, make the following entries:

- a. Set **Authenticated User Redirect** to **Use Custom Redirect**.
- b. Set **Redirect To** to **Customized\SAML20SPInitPost.aspx**.

Post Authentication

Authenticated User Redirect: Use Custom Redirect

Redirect To: Customized\SAML20SPInitPost.aspx

Upload a Page: **Browse...** No file selected.

[Download Customized Pages](#)

8. In the **User ID Mapping** section, make the following entries:

- a. Set **User ID Mapping** to **Authenticated User ID**.
- b. Set **Encode to Base64** to **True**.

▼ User ID Mapping

User ID Mapping: Transformation Engine

Name ID Format:

Encode to Base64:

9. In the **SAML Assertion / WS Federation** section, make the following entries:

- a. Set **WSFed/SAML Issuer** to a unique name that identifies the SecureAuth IdP to the application (as the SAML ID).

This value is shared with the application and can be any word, phrase, or URL, but must match exactly in the SecureAuth IdP and NetScaler configurations.

- b. Set the **SP Start URL** to the login URL to enable SSO and redirect users appropriately to access NetScaler virtual server (or VIP) for OWA.

For example, <https://vpn.company.com>

- c. Set **SAML Signing Algorithm** to **SHA1**.

NetScaler defaults to SHA1 for digest method, so the settings must be identical on SecureAuth IdP.

- d. Set **SAML Offset Minutes** to make up for time differences between devices.

- e. Set **SAML Valid Hours** to how long the SAML assertion is valid.

▼ SAML Assertion / WS Federation

WSFed Reply To/SAML Target URL:	<input type="text"/>
SAML Consumer URL:	<input type="text"/>
WSFed/SAML Issuer:	<input type="text" value="UniqueName"/>
SAML Recipient:	<input type="text"/>
SAML Audience:	<input type="text"/>
SP Start URL:	<input type="text" value="https://vpn.company.com"/>
WS-Fed Version:	<input type="text" value="1.2"/>
WS-Fed Signing Algorithm:	<input type="text" value="SHA1"/>
SAML Signing Algorithm:	<input type="text" value="SHA1"/>
SAML Offset Minutes:	<input type="text" value="0"/>
SAML Valid Hours:	<input type="text" value="24"/>

f. Click **Select Certificate** and choose the appropriate certificate to be used to sign the SAML assertion. This is also the same certificate that will be uploaded to the NetScaler SAML Authentication Server.

g. **Download** the metadata file and store it either in a local PC or on the NetScaler appliance.

Signing Cert Serial Number:	<input type="text" value="Certificate"/>	Select Certificate
Assertion Signing Certificate:	certificate.wse3.cer	
Domain:	<input type="text"/>	
Metadata File:	Download	

10. In the **SAML Attributes / WS Federation** section, make the following entries:

- Set **Name** to **username**.
- Set **Value** to **Authenticated User ID**.

▼ SAML Attributes / WS Federation

Attribute 1

Name:	<input type="text" value="username"/>
Namespace (1.1):	<input type="text"/>
Format:	<input type="text" value="Basic"/> ▼
Value:	<input type="text" value="Authenticated User ID"/> ▼
Group Filter Expression:	<input type="text" value="*"/>

NetScaler AAA configuration for SecureAuth IdP and OWA form-based authentication

This section describes how to configure NetScaler AAA for SecureAuth IdP and OWA form-based authentication. The following steps include these three main components:

- Add load balancing virtual server
- Add AAA authentication virtual server
- Add traffic policy for OWA logout

Prerequisites

- SecureAuth IdP configured realm (See [SecureAuth IdP configuration steps](#))

Load balancing virtual server

1. In NetScaler, create a load balancing virtual server configured with OWA on Exchange server as a service.

← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings

Name	mail. .com	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● UP	Range	1
IP Address		Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

Services and Service Groups

- 1 Load Balancing Virtual Server Service Binding >
- No Load Balancing Virtual Server ServiceGroup Binding >

Certificate

- 1 Server Certificate >
- No CA Certificate >

SSL Ciphers

AAA authentication virtual server

2. In NetScaler, create an AAA authentication virtual server which serves as the credential collector and authentication provider for the OWA virtual server.

← Authentication Virtual Server

Basic Settings

Name	aaa-ns-sa. .com	IP Address	
Authentication Domain	.com	Port	443

Certificate

1 Server Certificate	>
No CA Certificate	>

Advanced Authentication Policies

1 Authentication Policy	>
No SAML IDP Policy	>

Basic Authentication Policies

To add, please click on the + icon

401 Based Virtual Servers

No Load Balancing Virtual Server	>
No Content Switching Virtual Server	>

Form Based Virtual Servers

1 Load Balancing Virtual Server	>
No Content Switching Virtual Server	>

3. In the Advanced Authentication Policy for the AAA virtual server, add the SecureAuth IdP SAML identity provider.

Authentication Policy

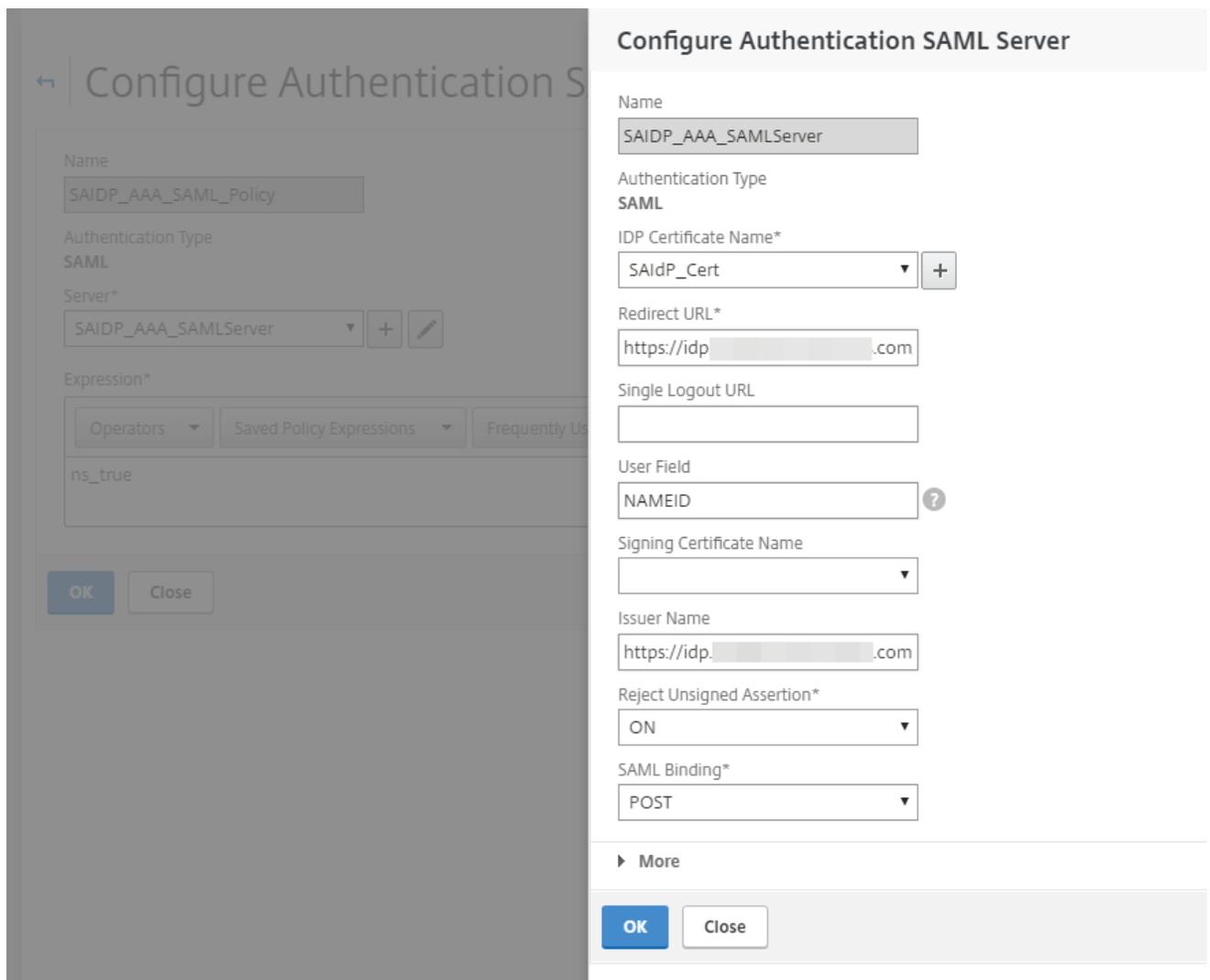
Add Binding Unbind Regenerate Priorities Edit

	Priority	Policy Name	Expression	Action	Goto Expression
<input type="checkbox"/>	110	SAIDP_AAA_AuthenticationPolicy	true	SAIDP_AAA_SAMLServer	NEXT

Close

4. To use SecureAuth IdP, make the following entries:

- Set **IDP Certificate Name** to use the SecureAuth IdP certificate.
- Set the **Redirect URL** to point to the SecureAuth IdP SAML realm.
- Set **User Field** to **NAMEID**.



5. Expand **More** and continue to make the following entries:

- a. Set the **Signature Algorithm** to **RSA-SHA1**.
- b. Set the **Digest Method** to **SHA1**.

The above two configurations are important because the NetScaler digest method defaults to SHA1. Otherwise, the NetScaler SP would not process the SAML assertion generated by the SecureAuth custom IdP.

- c. In the **Attributes** section, be sure to set the case-sensitive attributes that are also defined in the assertion.

Two Factor

ON OFF

Assertion Consumer Service Index

255

Attribute Consuming Service Index

255

Requested Authentication Context*

Exact ▼

Authentication Class Types

InternetProtocol
InternetProtocolPassword
Kerberos

Signature Algorithm*

RSA-SHA1 RSA-SHA256

Digest Method*

SHA1 SHA256

Send Thumbprint

Enforce Username

Attribute 1

username

Attribute 2

Password

Attribute 3

Attribute 4

6. In the **Configure Session Policy** section, create a **Session Profile** and make the following entries and ensure the applicable **Override Global** check box is selected:

- a. Set **Single Sign-on to Web Applications** to **ON**.
- b. Set the domain name in the **Single Sign-on Domain** field.
- c. If you are using a Content Switching VIP, ensure the following configurations are set:
 - i. Set **Enable Persistent Cookie** to **ON**.
 - ii. Set the **Persistent Cookie Validity** to **30**.

Configure Session Policy

Name
OWA_SSOsession_Policy

Request Profile*
OWA_SSOsession_Profile

Expression*
true

Switch to Classic Syntax

OK Close

Configure Session Profile

Name
OWA_SSOsession_Profile

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

	Override Global
Session Time-out (mins) 30	<input type="checkbox"/>
Default Authorization Action* ALLOW	<input checked="" type="checkbox"/>
Single Sign-on to Web Applications* ON	<input checked="" type="checkbox"/>
Credential Index* PRIMARY	<input checked="" type="checkbox"/>
Single Sign-on Domain [redacted].com	<input checked="" type="checkbox"/>
HTTPOnly Cookie* YES	<input type="checkbox"/>
Enable Persistent Cookie* OFF	<input type="checkbox"/>
Persistent Cookie Validity [redacted]	<input type="checkbox"/>
KCD Account [redacted]	<input type="checkbox"/>
Home Page [redacted]	<input type="checkbox"/>

OK Close

7. Attach the OWA session policy to the AAA virtual server.

SSL Parameters ✎ ✕

Enable DH Param DISABLED	Clear Text Port 0	SSLv2 Redirect DISABLED
Enable DH Key Expire Size Limit DISABLED	Enable Cipher Redirect DISABLED	SSLv2 DISABLED
Enable Ephemeral RSA ENABLED	Client Authentication DISABLED	SSLv3 ENABLED
Refresh Count 0	Send Close-Notify YES	TLSv1 ENABLED
Enable Session Reuse ENABLED	PUSH Encryption Trigger Always	TLSv11 ENABLED
Time-out 120	SNI Enable DISABLED	TLSv12 ENABLED
SSL Redirect DISABLED		

SSL Ciphers ✎ ✕

Configured (1)
Remove All

DEFAULT

Policies + ✕

1 Session Policy >

8. In the **Configure Form SSO Profile** section, create the required settings for back-end authentication by NetScaler to OWA with the following entries:

- a. Set Action URL to **/owa/auth.owa**.
- b. Set **User Name Field** to **username**.
- c. Set **Password Field** to **password**.
- d. Set **Success Criteria Expression** to the following:

```
http.RES.SET_COOKIE.COOKIE("cadata").VALUE("cadata").LENGTH.GT(70)
```

- e. Set the **Name Value Pair** to the following:

```
flags=4&trusted=4
```

Note-- For the **Name Value Pair** to work correctly, you might have to use the following:

```
flags=4&trusted=4&destination=https://mail.company.com/owa
```

- f. Set the **Response Size**.

Configure Form SSO Profile

Name

Action URL*

User Name Field*

Password Field*

Success Criteria Expression*

Operators ▼

Saved Policy Expressions ▼

Frequently Used Expressions ▼

Name Value Pair

Response Size

Extraction*

DYNAMIC ▼

Submit Method*

POST ▼

OK

Close

9. In the **Configure Traffic Profile** section, make the following entries.

The traffic profile extracts the user name and password from the SAML response and is used for SSO to back-end servers for OWA. This traffic profile will be assigned to the policy in step 10 and the configured NetScaler virtual server for OWA.

- a. Set **Single Sign-on** to **ON**.
- b. Set **Form SSO Profile** to **OWA_Form_SSO**.
- c. Set **KCD Account** to **NONE**.
- d. Use the command-line to create the SSO user and password expressions required for the traffic profile. (Creating them through the GUI is not available, so, use the command-line.) Run the following command-line parameters:

```
add tm trafficAction ns-saidp-creds_profile -sso on -userExpression http.REQ.user.name
-passwdExpression http.req.user.passwd.b64DECODE
```

For issues with executing the commands, seek help from either a Citrix Admin or contact Citrix Technical Support.

Configure Traffic Profile

Name

ns-saidp-creds_profile

AppTimeout (minutes)

Single Sign-on

ON

Form SSO Profile

OWA_Form_SSO



SAML SSO Profile



Enable Persistent Cookie ?

Initiate Logout

KCD Account*

NONE



Forced Timeout

SSO User Expression

Operators



Saved Policy Expressions



Frequently Used Expressions



http.REQ.user.name

SSO Password Expression

Operators



Saved Policy Expressions



Frequently Used Expressions



http.req.user.passwd.b64DECODE

10. Go back to the **Configure Form SSO Profile** section and add the Form SSO profile you just created.

11. Create a traffic policy and attach the profile you created in step 9.

Name

Profile*

Expression*

`http.req.url.contains("logon.aspx")`

12. Open the NetScaler OWA virtual server and add the AAA Authentication Virtual Server in the Authentication Policy.

ECC Curve <input type="button" value="✕"/>		
4 ECC Curves <input type="button" value=">"/>		
SSL Parameters <input type="button" value="✎"/> <input type="button" value="✕"/>		
Enable DH Param DISABLED Enable DH Key Expire Size Limit DISABLED Enable Ephemeral RSA ENABLED Refresh Count 0 Enable Session Reuse ENABLED Time-out 120 SSL Redirect DISABLED	Clear Text Port 0 Enable Cipher Redirect DISABLED Client Authentication DISABLED Send Close-Notify YES PUSH Encryption Trigger Always SNI Enable DISABLED	SSLv2 Redirect DISABLED SSLv2 DISABLED SSLv3 ENABLED TLSv1 ENABLED TLSv11 ENABLED TLSv12 ENABLED
Authentication <input type="button" value="✎"/> <input type="button" value="✕"/>		
Form Based Authentication ON Authentication Virtual Server aaa-ns-sa.com	Authentication FQDN aaa-ns-sa.com Authentication Profile -	
Policies <input type="button" value="+"/> <input type="button" value="✕"/>		
Request Policies		
1 Traffic Policy <input type="button" value=">"/>		

13. Bind the traffic policy to the NetScaler OWA virtual server and save the settings.

Load Balancing Virtual Server Traffic Policy Binding

<input type="checkbox"/>	Priority	Policy Name	Expression	Profile
<input type="checkbox"/>	100	ns-saidp-creds_policy	http.req.url.contains("logon.aspx")	ns-saidp-creds_profile

Traffic policy for OWA logout

14. Create a new traffic policy for OWA logout.

A. Configuring the traffic policy

Configure Traffic Policy

Name

Profile*

Expression*

`HTTP.REQ.URL.CONTAINS("logoff.owa")`

15. Add the traffic profile and select the **Initiate Logout** check box.

B. Configuring the traffic profile

Configure Traffic Profile

Name
Exchange_2013_owa_logout_profile

AppTimeout (minutes)

Single Sign-on

Form SSO Profile
 +

SAML SSO Profile
 +

Enable Persistent Cookie
 Initiate Logout

KCD Account*
NONE +

Forced Timeout

16. Bind the policy to the OWA virtual server.

NetScaler AAA configuration for SecureAuth IdP and OWA Integrated Windows Authentication

This section describes how to configure NetScaler AAA for SecureAuth IdP SAML and OWA Integrated Windows Authentication and includes two main components:

- Active Directory configuration
- Kerberos configuration

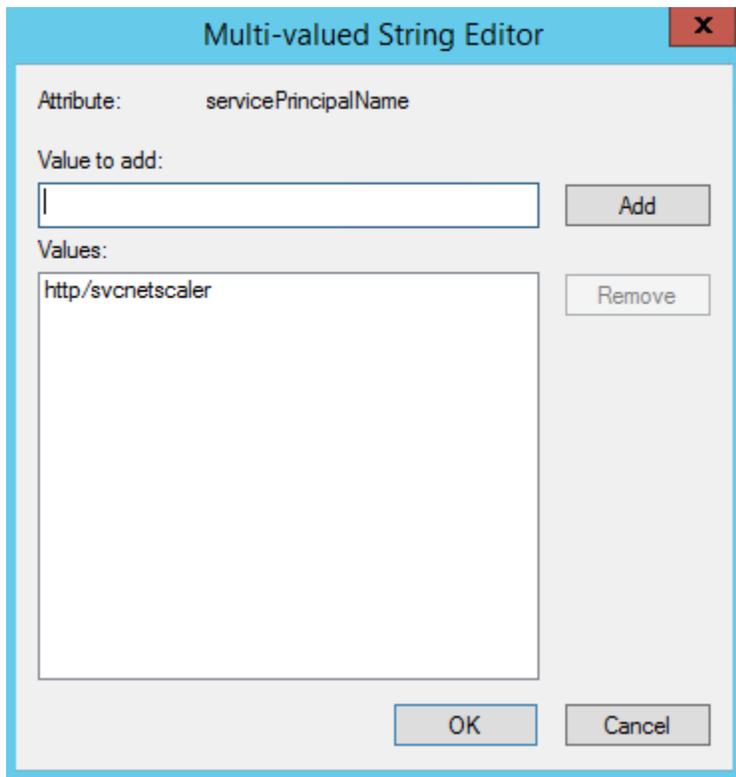
Prerequisites

- SecureAuth IdP configured realm (See [SecureAuth IdP configuration steps](#))
- NetScaler Traffic virtual server created in the previous section
- NetScaler AAA server created in the previous section

Active Directory configuration

1. Create a service account with the following entries:

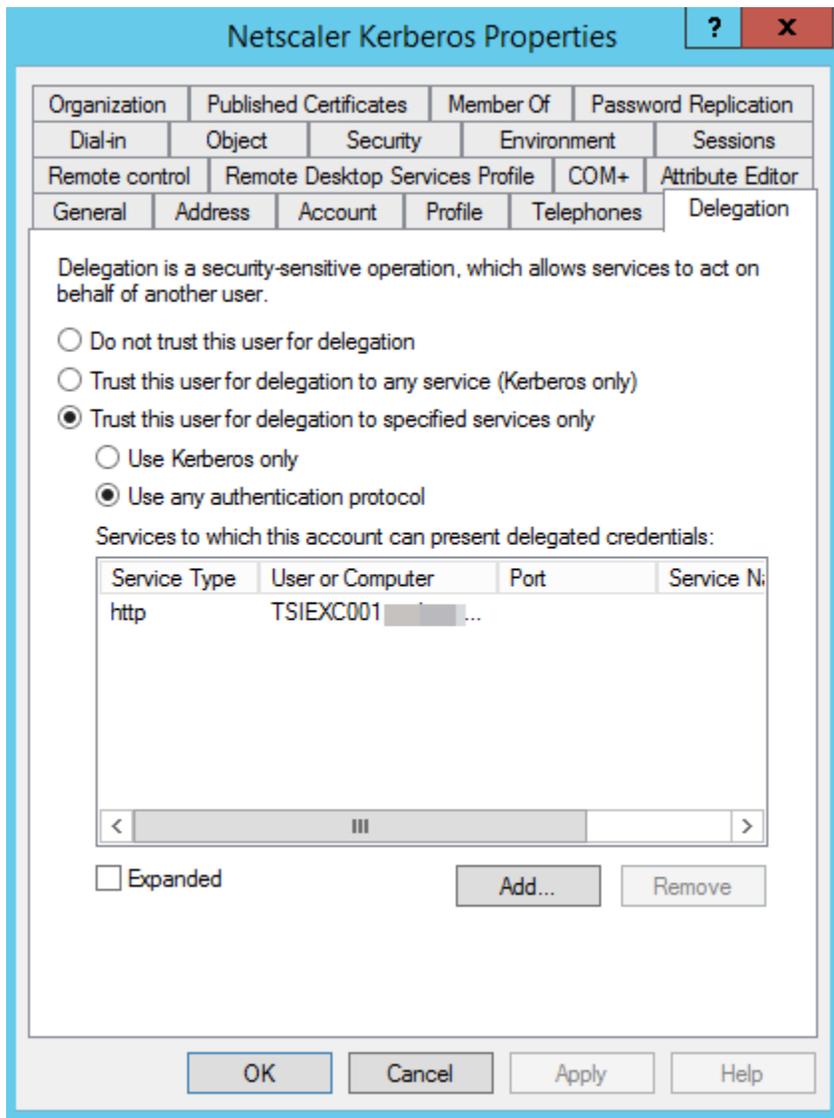
- a. Use the **servicePrincipalName** attribute.
- b. Set the **Values** as http/account_name.



2. Select the **Delegation** tab and make this entry:

a. Select the Exchange server with http service.

If there is more than one server, select each applicable server.



Kerberos configuration

3. In NetScaler, configure a KCD account and enter the realm name in upper case.

Configure KCD Account

Name

Use Keytab File

Realm*

User Realm

Enterprise Realm

Service SPN

User Certificate

Choose File ▾

CA Certificate

Choose File ▾

Delegated User

Password for Delegated User

OK

Close

4. Configure a session profile with the following entries and ensure the applicable **Override Global** check box is selected:

- a. Set **Default Authorization Action** to **ALLOW**.
- b. Set **Single Sign-on to Web Applications** to **ON**.
- c. Type the **Single Sign-on Domain** name.
- d. Select the applicable **KCD Account**.

Configure Session Profile

Name

OWA_SSOsession_KCD_Profile

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

	Override Global
Session Time-out (mins)	<input type="checkbox"/>
30	
Default Authorization Action*	<input checked="" type="checkbox"/>
ALLOW	
Single Sign-on to Web Applications*	<input checked="" type="checkbox"/>
ON	
Credential Index*	<input type="checkbox"/>
PRIMARY	
Single Sign-on Domain	<input checked="" type="checkbox"/>
.com	
HTTPOnly Cookie*	<input type="checkbox"/>
YES	
Enable Persistent Cookie*	<input type="checkbox"/>
OFF	
Persistent Cookie Validity	<input type="checkbox"/>
KCD Account	<input checked="" type="checkbox"/>
KCD_	
Home Page	<input type="checkbox"/>

OK

Close

5. Configure a **Session Policy** with the profile you just created.
 - a. Set the **Request Profile** to the profile that you just created in step 4.

← Configure Session Policy

Name
OWA_SSOSession_KCD_Policy

Request Profile*
OWA_SSOSession_KCD_Profile + 

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
true

[Switch to Classic Syntax](#)

OK Close

6. In the **Configure Traffic Profile** section, make the following entries:

The traffic profile extracts the user name and password from the SAML response and is used for SSO to back-end servers for OWA. This traffic profile will be assigned to the policy in step 7 and the configured NetScaler virtual server for OWA.

- a. Set **Single Sign-on** to **ON**.
- b. Select the applicable **KCD Account**.
- c. Use the command-line to create the SSO user and password expressions required for the traffic profile. (Creating them through the GUI is not available, so use the command-line.) Run the following command-line parameters:

```
set tm trafficAction OWA_Traffic_KCD_Profile -sso on -userExpression http.REQ.user.name  
-passwdExpression http.req.user.passwd.b64DECODE
```

For issues with executing the commands, seek help from either a Citrix Admin or contact Citrix Technical Support.

Name

OWA_Traffic_KCD_Profile

AppTimeout (minutes)

Single Sign-on

ON

Form SSO Profile

 + 

SAML SSO Profile

 + 

Enable Persistent Cookie

Initiate Logout 

KCD Account*

 KCD_ 

Forced Timeout

SSO User Expression

Operators

Saved Policy Expressions

Frequently Used Expressions

http.REQ.user.name

SSO Password Expression

Operators

Saved Policy Expressions

Frequently Used Expressions

http.req.user.passwd.b64DECODE

7. In the **Configure Traffic Policy** section, make the following entry:

- a. Set **Profile** to the one you just created in step 6.

← Configure Traffic Policy

Name
OWA_Traffic_KCD_Policy

Profile*
OWA_Traffic_KCD_Profile ▼ + ✎

Expression*
Operators ▼ Saved Policy Expressions ▼ Frequently Used Expressions ▼
true

OK Close

8. In the **Session Policy** section, add the session policy you created in steps 4-5 to the AAA server that will be used for OWA authentication.

Session Policy

Add Binding Unbind Regenerate Priorities Edit ▼

<input type="checkbox"/>	Priority	Policy Name	Expression	Request Profile
<input type="checkbox"/>	100	OWA_SSOsession_KCD_Policy	true	OWA_SSOsession_KCD_Profile

Close

9. Modify the **Authentication** policy of the NetScaler OWA virtual server.

Authentication ✎ ✕

Form Based Authentication	ON	Authentication FQDN	aaa-ns-sa. .com
Authentication Virtual Server	aaa-ns-sa. .com	Authentication Profile	-

10. Bind the traffic policy to the NetScaler virtual server.

Load Balancing Virtual Server Traffic Policy Binding

Add Binding

Unbind

Regenerate Priorities

Edit

<input type="checkbox"/>	Priority	Policy Name	Expression	Profile
<input type="checkbox"/>	100	OWA_Traffic_KCD_Policy	true	OWA_Traffic_KCD_Profile

Close

NetScaler Gateway configuration for SecureAuth IdP and OWA forms-based authentication

This section describes how to configure NetScaler Gateway for SecureAuth IdP SAML and OWA on Exchange Server 2013 or 2016 form-based authentication and includes

Prerequisites

- SecureAuth IdP realm SAML settings (See [SecureAuth IdP configuration steps](#))

VPN virtual server configuration

- Create a NetScaler Gateway VPN virtual server with a new IP address.

← VPN Virtual Server

Basic Settings

Name	ns-owa. .com	Maximum Users	0
IPAddress	10.145.240.47	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	● UP	ICA Only	true
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	false	Mac EPA Plugin Upgrade	-
DTLS	false	ICA Proxy Session Migration	false
AppFlow Logging	false	Enable Device Certificate	false

Certificate

- 1 Server Certificate >
- No CA Certificate >

Basic Authentication

Primary Authentication

- 1 SAML Policy >

Advanced Authentication

- No SAML IDP Policy >

- Add the server certificate for SSL.

3. In the Basic Authentication section, specify the SAML server that was configured with SecureAuth IdP.

Configure Authentication SAML Server

Name
SAIDP_AAA_SAMLServer

Authentication Type
SAML

IDP Certificate Name*
SAIDP_Cert

Redirect URL*
https://idp. .com

Single Logout URL
[Empty]

User Field
NAMEID

Signing Certificate Name
[Empty]

Issuer Name
https://idp. .com

Reject Unsigned Assertion*
ON

SAML Binding*
POST

► More

OK Close

3. **Save** the configuration settings.

4. In the NetScaler Gateway, from the Policies section, create a new Session Profile and on the **Network Configuration** tab, make the following entries and ensure the applicable **Override Global** check box is selected.

This session profile will be added to the NetScaler Gateway VPN virtual server created in step 1.

Name

ns_owa_gw_SessionProfile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration	Client Experience	Security	Published Applications	Remote Desktop
------------------------------	-------------------	----------	------------------------	----------------

Override Global

DNS Virtual Server

WINS Server IP

Kill Connections*

- a. Set **Clientless Access** to **Off**.
- b. Set **Clientless Access URL Encoding** to **Clear**.
- c. Set **Plug-in Type** to **Windows/MAC OS X**.
- d. Set **AlwaysON Profile Name** to **SAAlwaysOn**.

Accounting Policy

Override Global

Display Home Page

Home Page

URL for Web-Based Email

Split Tunnel*

Session Time-out (mins)

Client Idle Time-out (mins)

Clientless Access*

Clientless Access URL Encoding*

Clientless Access Persistent Cookie*

Plug-in Type*

Windows Plugin Upgrade

Linux Plugin Upgrade

MAC Plugin Upgrade

AlwaysON Profile Name

5. Scroll down and continue to make these entries and ensure the applicable **Override Global** check box is selected:

- a. Select the **Single Sign-on to Web Applications** check box.
- b. Set **Credential Index** to **PRIMARY**.

c. Set **Single Sign-on with Windows** to **ON**.

Single Sign-on to Web Applications

Credential Index*

PRIMARY

KCD Account

+

Single Sign-on with Windows*

ON

Client Cleanup Prompt*

ON

6. On the **Security** tab, make the following entry:

a. Set **Default Authorization Action** to **ALLOW** and ensure the **Override Global** check box is selected.

Network Configuration Client Experience **Security**

Override Global

Default Authorization Action*

ALLOW

Secure Browse*

ENABLED

Smartgroup

Advanced Settings

7. On the **Published Applications** tab, make the following entry:

a. Set the **Web Interface Address** URL to your OWA which is a load balanced traffic VIP on the NetScaler.

For example, <https://mail.company.com/owa>

Network Configuration	Client Experience	Security	Published Applications
Override Global			
ICA Proxy*			
ON			<input checked="" type="checkbox"/>
Web Interface Address			
https://mail. .com			<input checked="" type="checkbox"/>
Web Interface Address Type*			
IPV4			
Web Interface Portal Mode*			
NORMAL			<input type="checkbox"/>
Single Sign-on Domain			
.com			<input checked="" type="checkbox"/>
Citrix Receiver Home Page			
			<input type="checkbox"/>
Account Services Address			
			<input type="checkbox"/>

8. Create a **Session Policy** and add the profile created in step 4.

Name

ns-owa-gw_SessionPolicy

Profile*

ns_owa_gw_SessionProfile

Expression*

Operators Saved Policy Expressions Frequently Used Expressions

ns_true

9. Go to **Policies > Configure Traffic Profile** and make the following entries to create a **Form SSO Profile**--

- Set the **Action URL** to `/owa/auth.owa`.
- Set **User Name Field** to `username`.
- Set **Password field** to `password`.
- Set **Success Criteria Expression** to the following:

```
http.RES.SET_COOKIE.COOKIE("cadata").VALUE("cadata").LENGTH.GT(70)
```

e. Set the **Name Value Pair** to the following:

```
flags=4&trusted=4
```

f. Set the **Response Size**.

Note-- The response size may vary, and typically for OWA, a value of 15000 should work.

g. Set **Extraction** to **DYNAMIC**.

h. Set **Submit Method** to **POST**.

Name

```
ns-owa-gw-OWA_Form_SSO
```

Action URL *

```
/owa/auth.owa
```

User Name Field*

```
username
```

Password Field*

```
password
```

Success Criteria Expression*

Operators

Saved Policy Expressions

Frequently Used Expressions

```
http.RES.SET_COOKIE.COOKIE("cadata").VALUE("cadata").LENGTH.GT(70)
```

Name Value Pair

```
flags=4&trusted=4
```

Response Size

```
200000
```

Extraction*

DYNAMIC

Submit Method*

POST

10. In the **Configure Traffic Profile** section, make the following entries.

The traffic profile extracts the user name and password from the SAML response and is used for SSO to back-end servers for OWA. This traffic profile will be assigned to the policy in step 12 and the configured NetScaler OWA virtual server.

a. Set **Protocol** to **HTTP**.

b. Set **Single Sign-on** to **ON**.

c. Set **Form SSO Profile** to **ns-owa-gw-OWA_Form_SSO**.

d. Set **KCD Account** to **NONE**.

e. Use the command-line to create the SSO user and password expressions required for the traffic profile. (Creating them through the GUI is not available, so use the command-line.) Run the following command-line parameters:

```
add vpn trafficAction ns-saidp-vpn-creds_profile HTTP -SSO ON -formsSOAction ns-owa-gw-OWA_Form_SSO  
-userExpression http.REQ.user.name -passwdExpression http.req.user.passwd.b64DECODE
```

For issues with executing the commands, seek help from either a Citrix Admin or contact Citrix Technical Support.

ns-saidp-vpn-creds_profile

Protocol

HTTP TCP

AppTimeout (minutes)

 ?

Single Sign-on

ON ▼

Form SSO Profile

ns-owa-gw-OWA_Form_SSO ▼ + ✎

SAML SSO Action

▼ + ✎

File Type Association

▼

HDX Proxy

▼

Proxy

CloudBridge

▼

KCD Account

▼ + ✎

SSO User Expression

Operators ▼ Saved Policy Expressions ▼ Frequently Used Expres

http.REQ.user.name

SSO Password Expression

Operators ▼ Saved Policy Expressions ▼ Frequently Used Expres

http.req.user.passwd.b64DECODE

11. Go back to the **Configure Form SSO Profile** section and add the Form SSO profile you just created.

12. Create a traffic policy and attach the profile you created in step 10.

Name
ns-saidp-vpn-creds_policy

Request Profile*
ns-saidp-vpn-creds_profile + 

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
URL CONTAINS logon.aspx

13. Add the session and traffic policies created in the previous steps to the NetScaler Gateway VIP or virtual server.

Policies

Request Policies

1 Session Policy

1 Traffic Policy

OWA on Exchange 2010 authentication

The previous steps work for authentication to OWA on Exchange Server 2013 or 2016. For OWA on Exchange Server 2010, you will need a rewrite policy in addition to Session and Traffic policies to address the authentication cookie (PBACK) mechanism.

14. Go to **AppExpert > Rewrite > Actions** and make the following entries:

a. Create the rewrite action.

b. For the **Expression to choose target location**, enter the following:

```
http.REQ.COOKIE.VALUE("OutlookSession")
```

c. For the **Expression**, enter the following:

```
";PBack=0"
```

Name

set_pback_cookie

Type

INSERT_AFTER

Use this action type to insert a custom text in request/response after a text reference.

Expression to choose target location*

Operators

Saved Policy Expressions

Frequently Used Expressions

http.REQ.COOKIE.VALUE("OutlookSession")

Expression

Operators

Saved Policy Expressions

Frequently Used Expressions

";PBack=0"

15. Create a rewrite policy and ensure the **Action** points to the one created in step 14.

Name

set_pback_cookie

Action*

set_pback_cookie

+



Log Action

+



Undefined-Result Action*

-Global-undefined-result-action-

Expression*

Operators

Saved Policy Expressions

Frequently Used Expressions

http.REQ.URL.CONTAINS("logon.aspx")

16. Bind the rewrite policy to the NetScaler Gateway virtual server along with the traffic and session policies.

OWA on Exchange 2010 for iPhone and iPad device authentication

For OWA on Exchange Server 2010, you will need two rewrite policies and replace the policy and profile used in steps 15 and 16.

17. To add two new rewrite policies, replace the policies and profiles, do the following:

a. Create a rewrite policy for the session cookie with the following entry:

```
add rewrite policy EXCH2010_OWA_TEST "http.REQ.URL.CONTAINS(\"logon.aspx\") &&
http.REQ.COOKIE.CONTAINS(\"OutlookSession\")" TEST_REWRITE_idevice
```

b. Create the rewrite action for the session cookie with the following entry:

```
add rewrite action TEST_REWRITE_idevice insert_before "http.REQ.HEADER
(\"Cookie\").VALUE(0)" "\"PBack=0;\""
```

c. Create a rewrite policy to detect device and browser with the following entry:

```
add rewrite policy set_pback_cookie_idevice "http.req.url.contains(\"logon.aspx\").AND
(http.REQ.HEADER(\"User-Agent\").CONTAINS(\"iPad\") || http.REQ.HEADER(\"User-Agent\").
CONTAINS(\"Safari\"))" set_pback_idevice
```

d. Create the rewrite action for device and browser detection with the following entry:

```
add rewrite action set_pback_idevice insert_http_header Cookie "\"OutlookSession=;PBack=0\""
```

18. Bind the policies to the NetScaler Gateway virtual server.