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

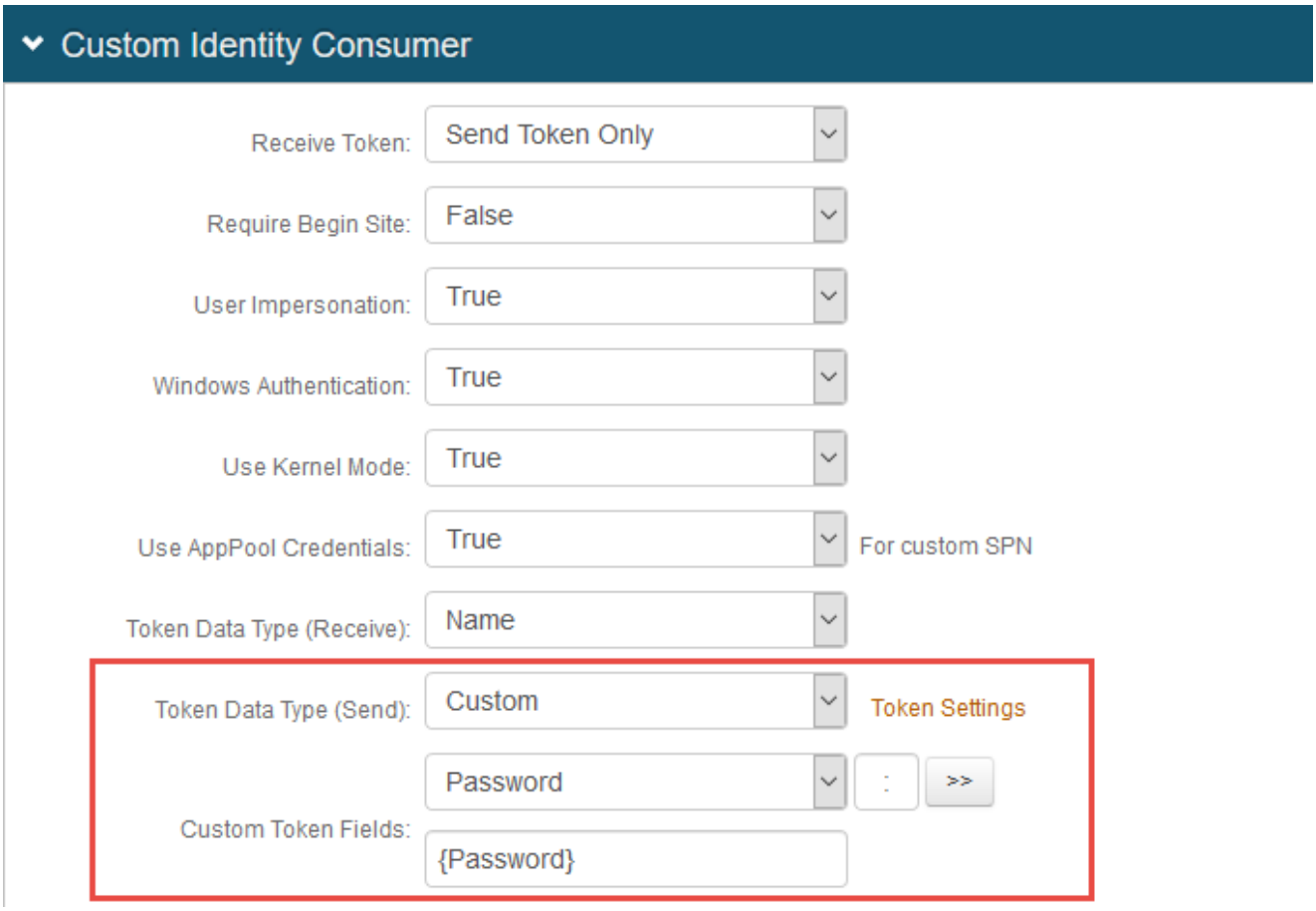
3. Select the **Workflow** tab.

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

    a. Set **Token Data Type (Send)** to **Custom**.

    b. Set the **Custom Token Fields** to **Password**.

    c. Click the **>>** button to populate the next field with **{Password}**.



5. Click **Save**.

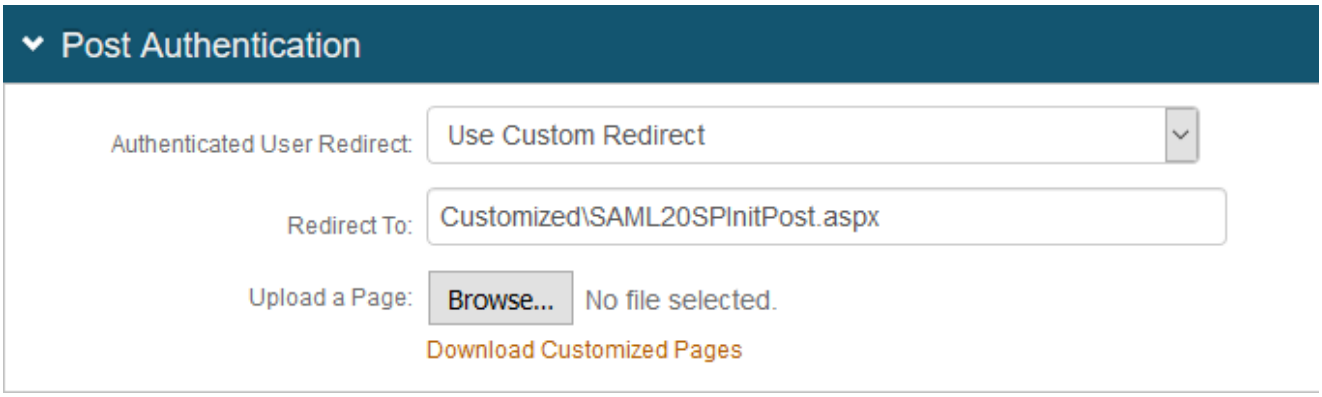
Post Authentication tab

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**.

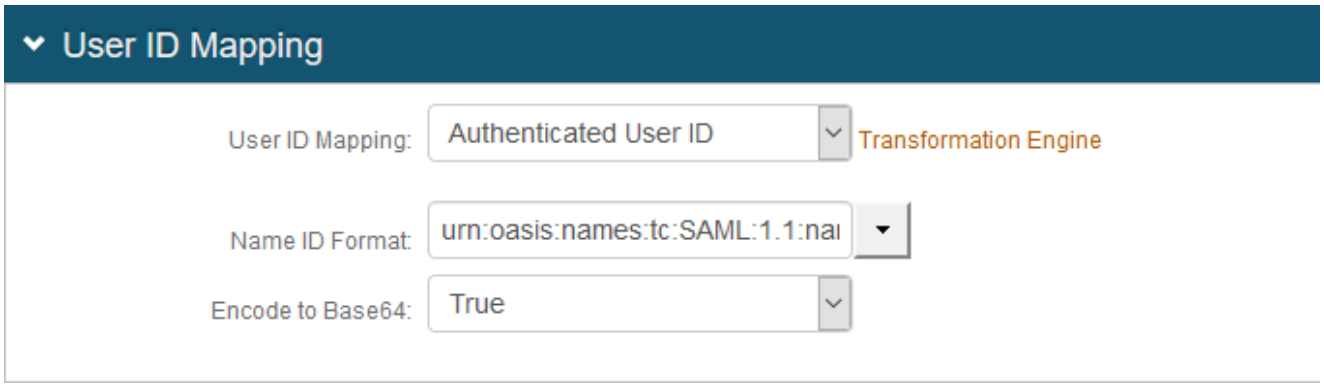
    b. Set **Redirect To** to **Customized\SAML20SPInitPost.aspx**.



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**.



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.

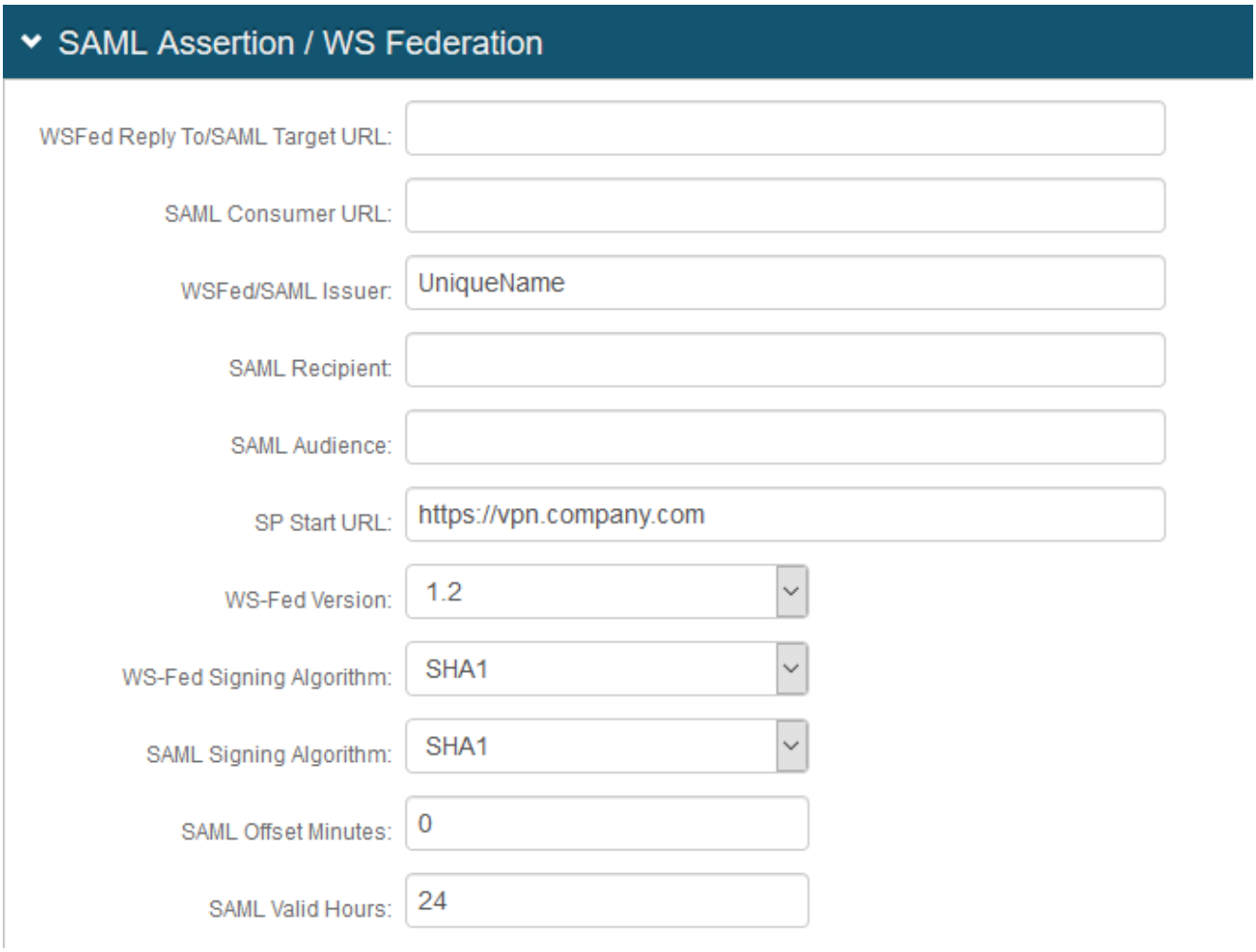
    For example, https://vpn.company.com

    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.



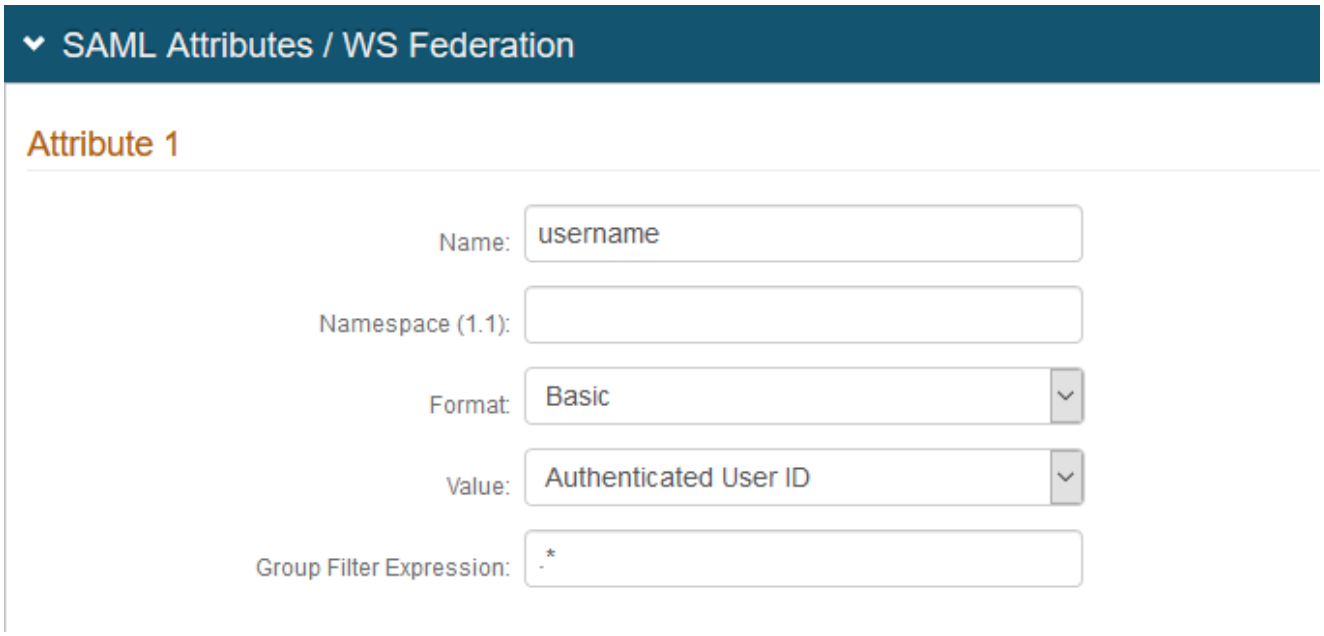
f. Click **Select Certificate** and choose the appropriate certificate to be used to sign the SAML assertion. This is also the same certificate that will be uploaded to the NetScaler SAML Authentication Server.

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

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

    a. Set **Name** to **username**.

    b. Set **Value** to **Authenticated User ID**.



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:

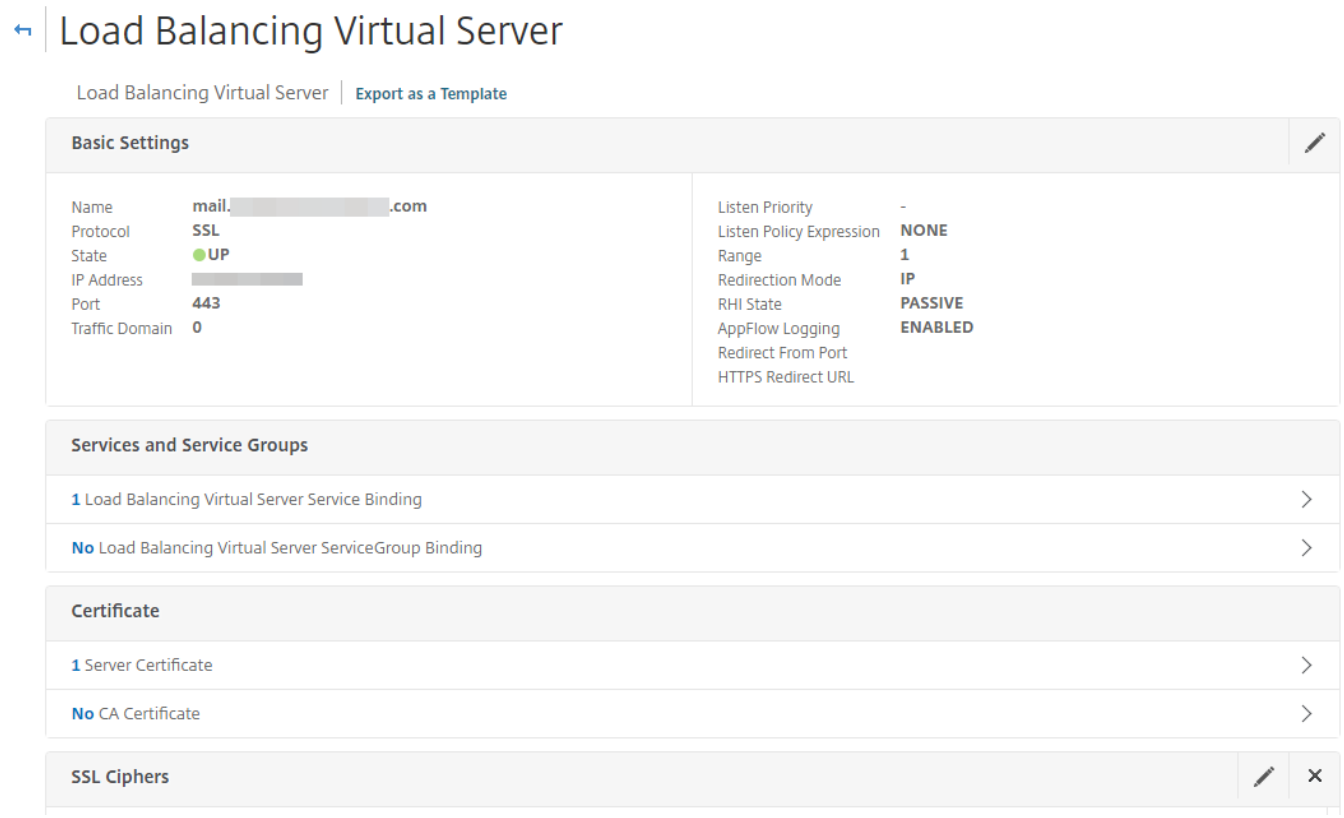
- Add load balancing virtual server
- Add AAA authentication virtual server
- Add traffic policy for OWA logout

Prerequisites

- SecureAuth IdP configured realm (See SecureAuth IdP configuration steps)

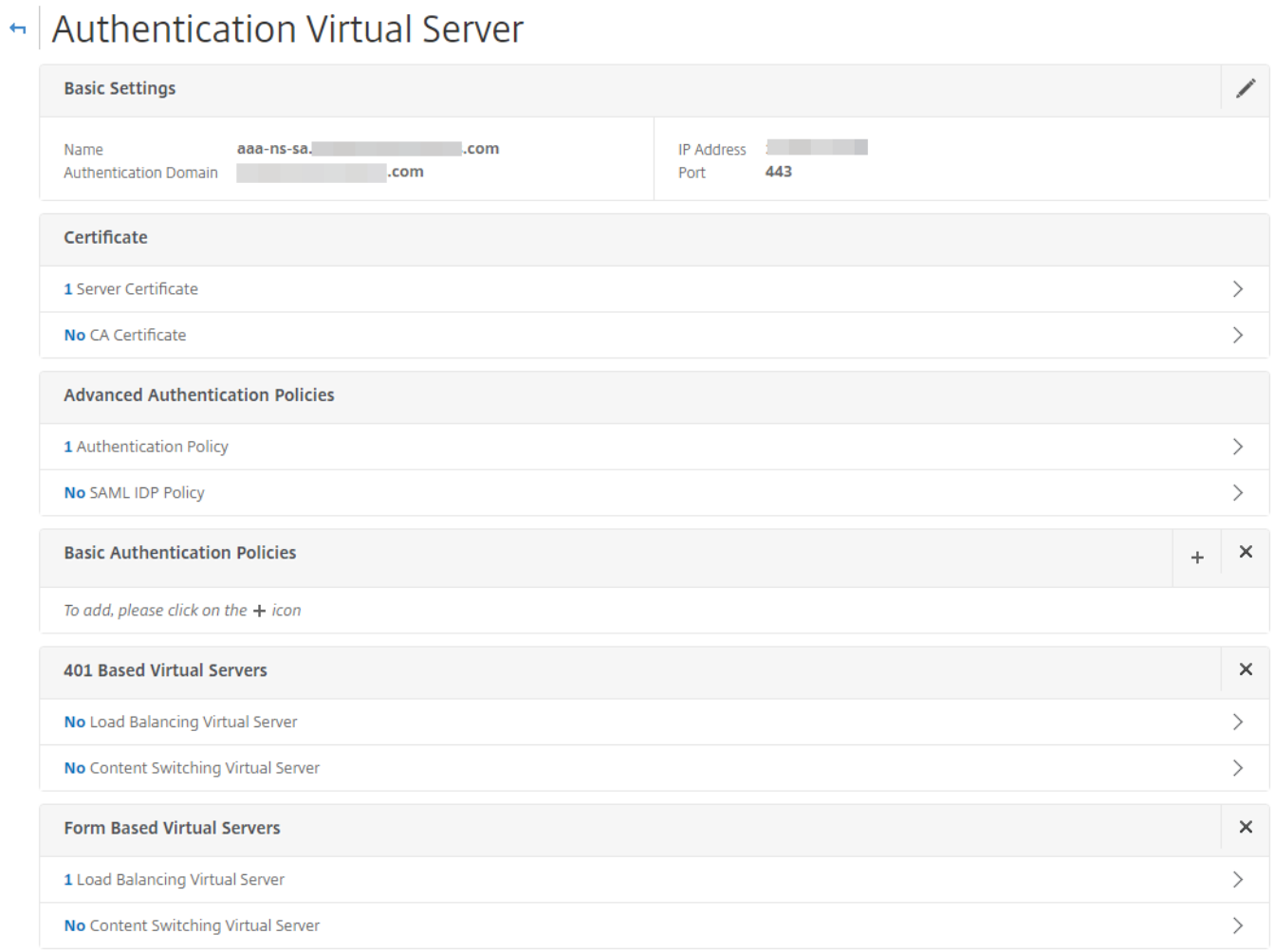
Load balancing virtual server

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

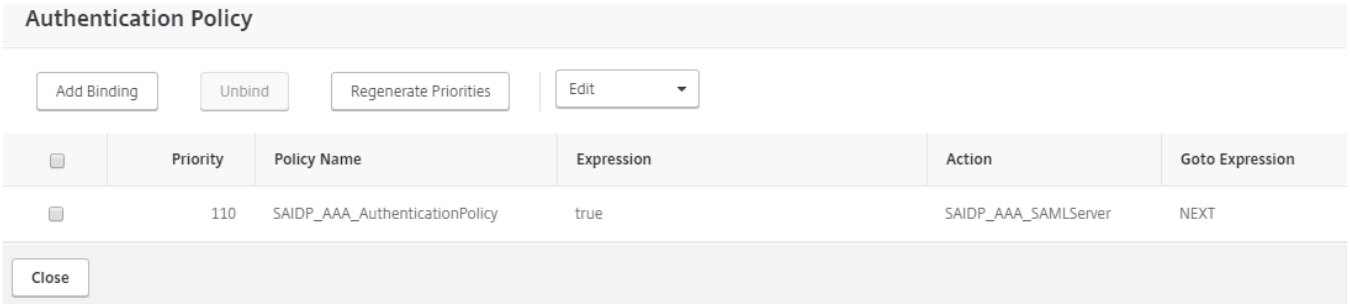


AAA authentication virtual server

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



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

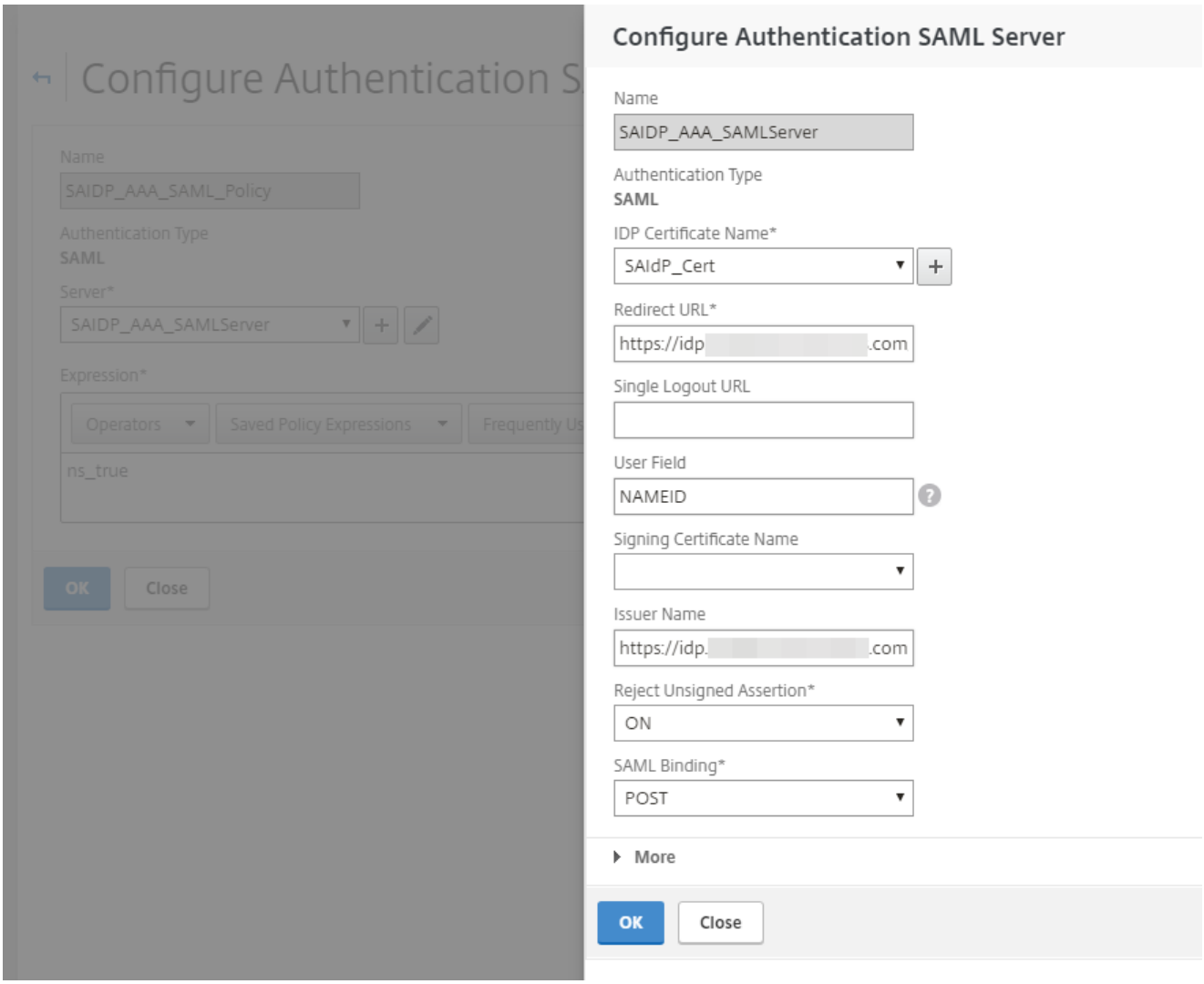


4. To use SecureAuth IdP, make the following entries:

   a. Set **IDP Certficiate Name** to use the SecureAuth IdP certificate.

   b. Set the **Redirect URL** to point to the SecureAuth IdP SAML realm.

   c. Set **User Field** to **NAMEID**.



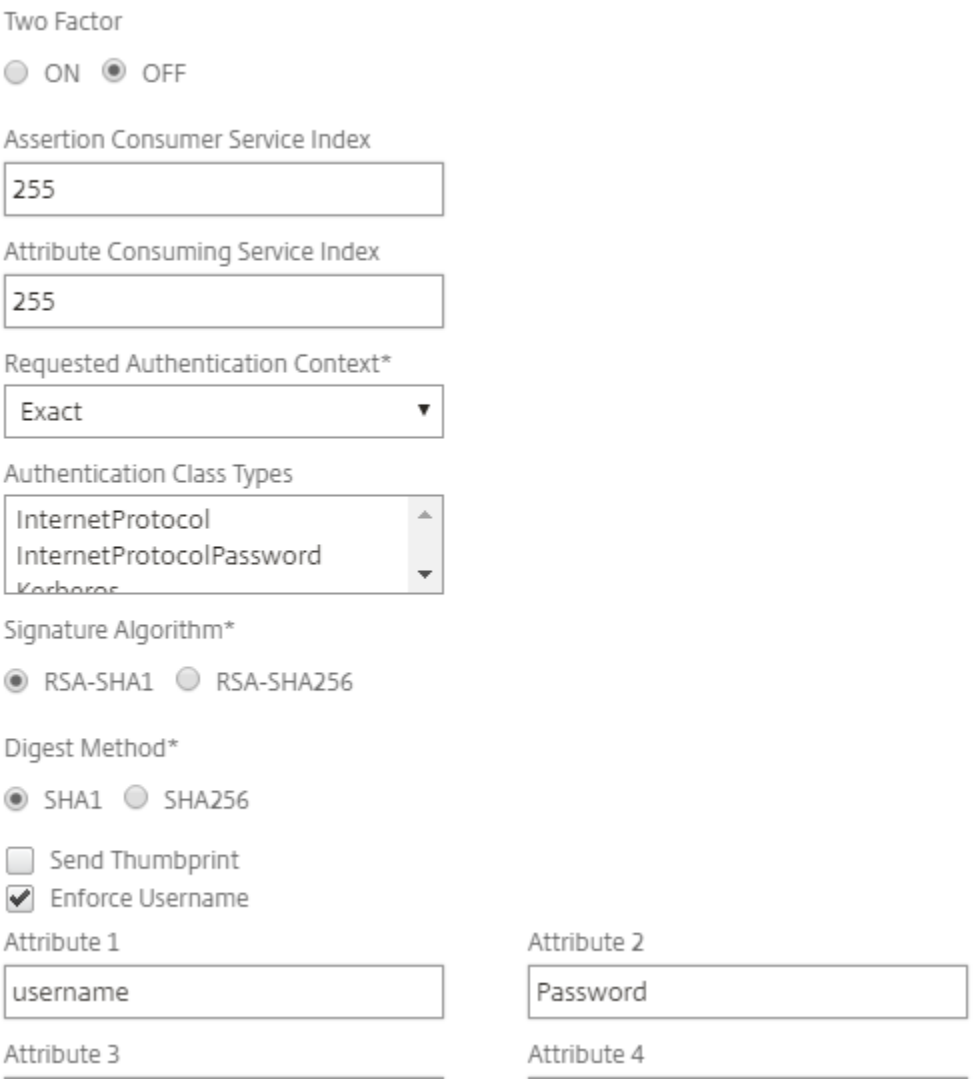
5. Expand **More** and continue to make the following entries:

    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.



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:

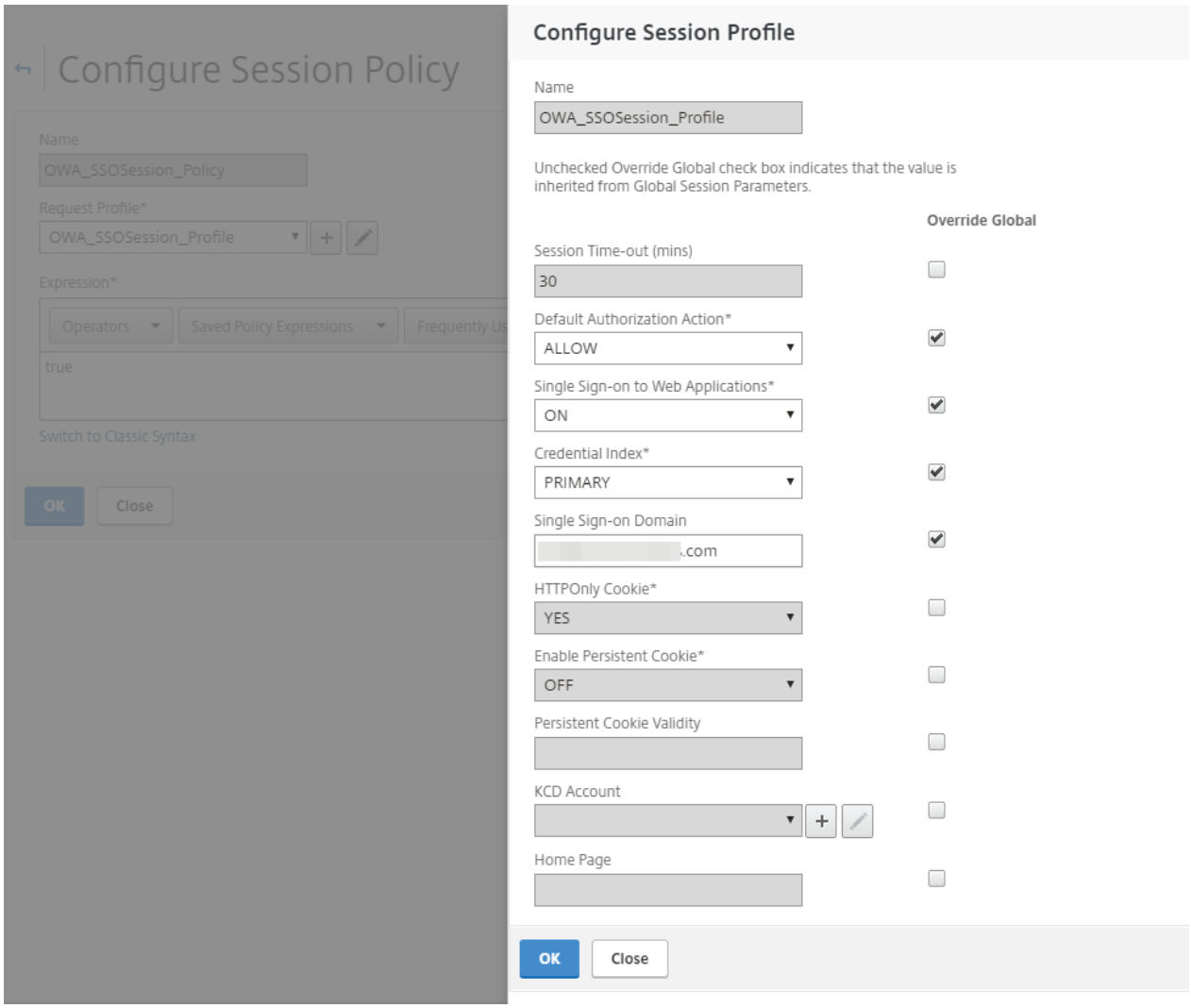
a. Set **Single Sign-on to Web Applications** to **ON**.

b. Set the domain name in the **Single Sign-on Domain** field.

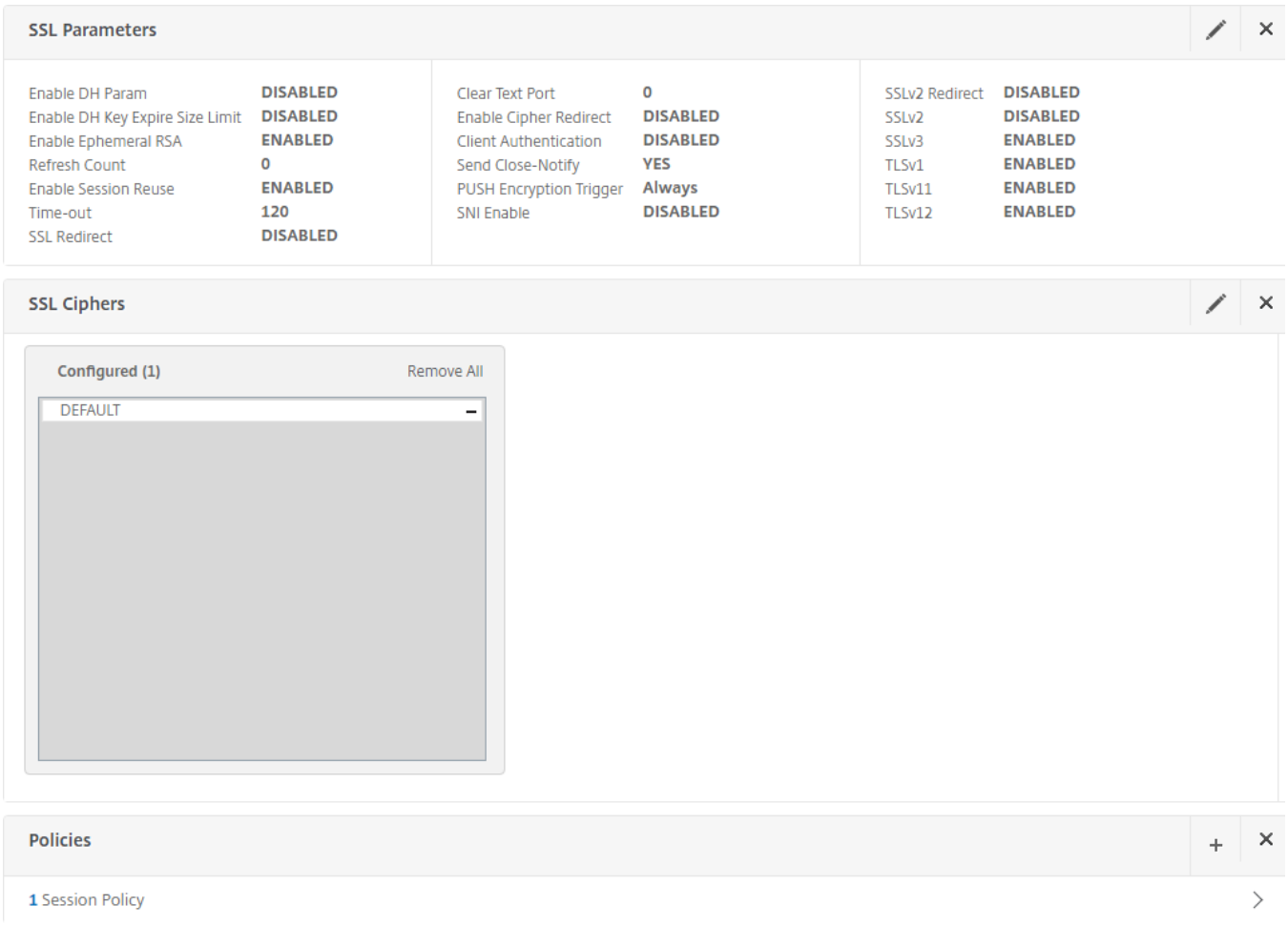
c. If you are using a Content Switching VIP, ensure the following configurations are set:

i. Set **Enable Persistent Cookie** to **ON**.

ii. Set the **Persistent Cookie Validity** to **30**.



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



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)
    ```

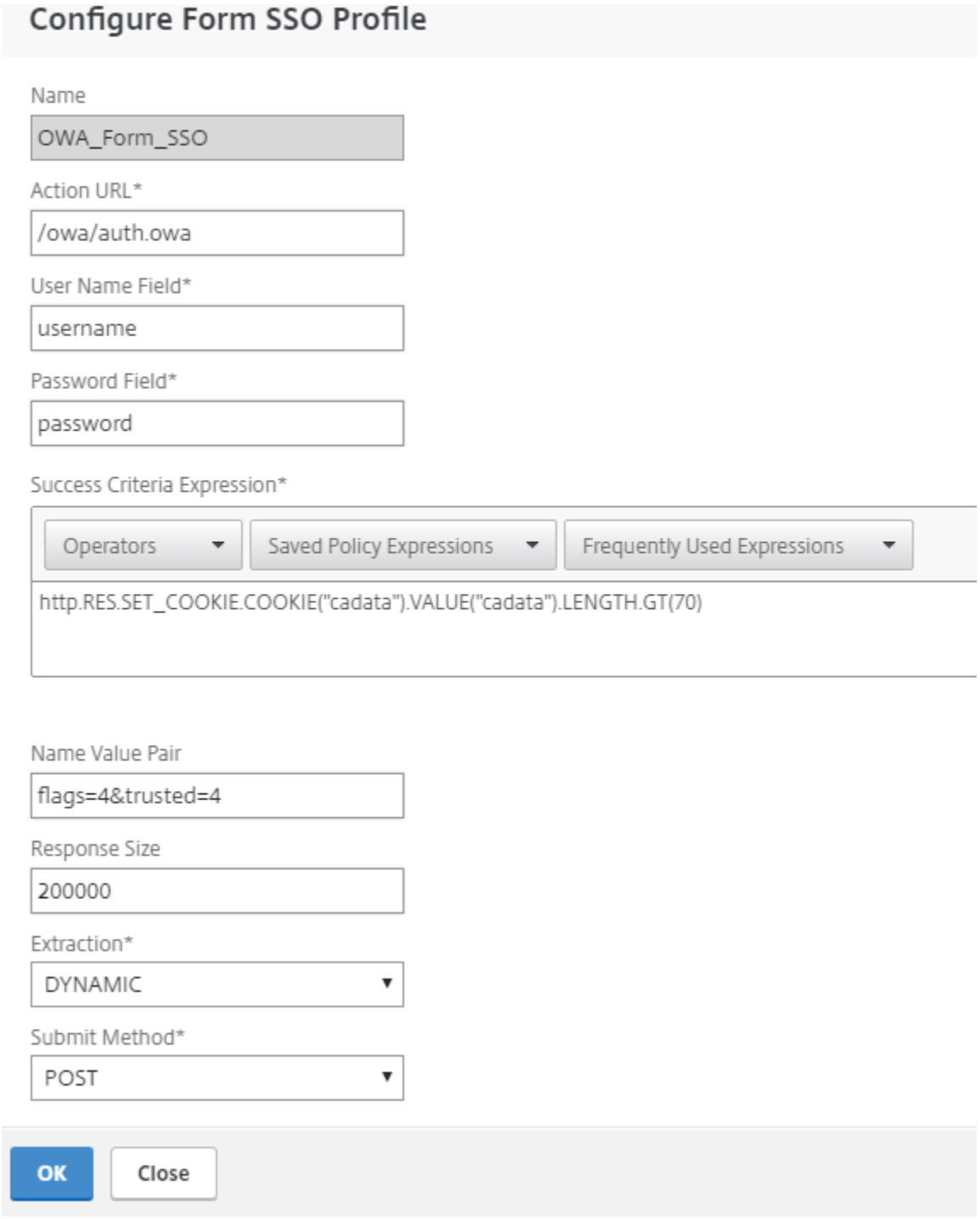
    e. Set the **Name Value Pair** to the following:

    ```
    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.**



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**.

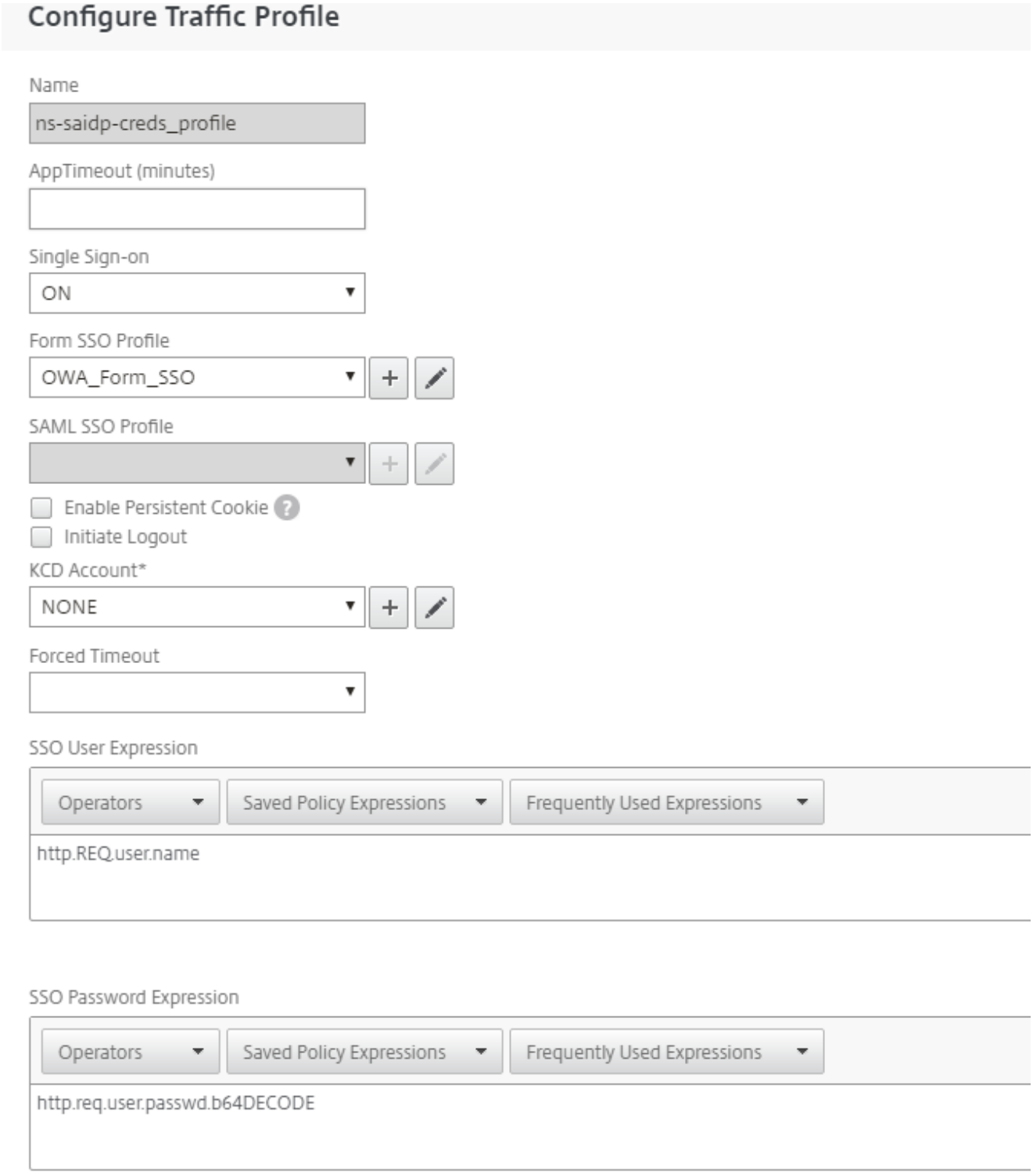
   b. Set **Form SSO Profile** to **OWA_Form_SSO**.

   c. Set **KCD Account** to **NONE**.

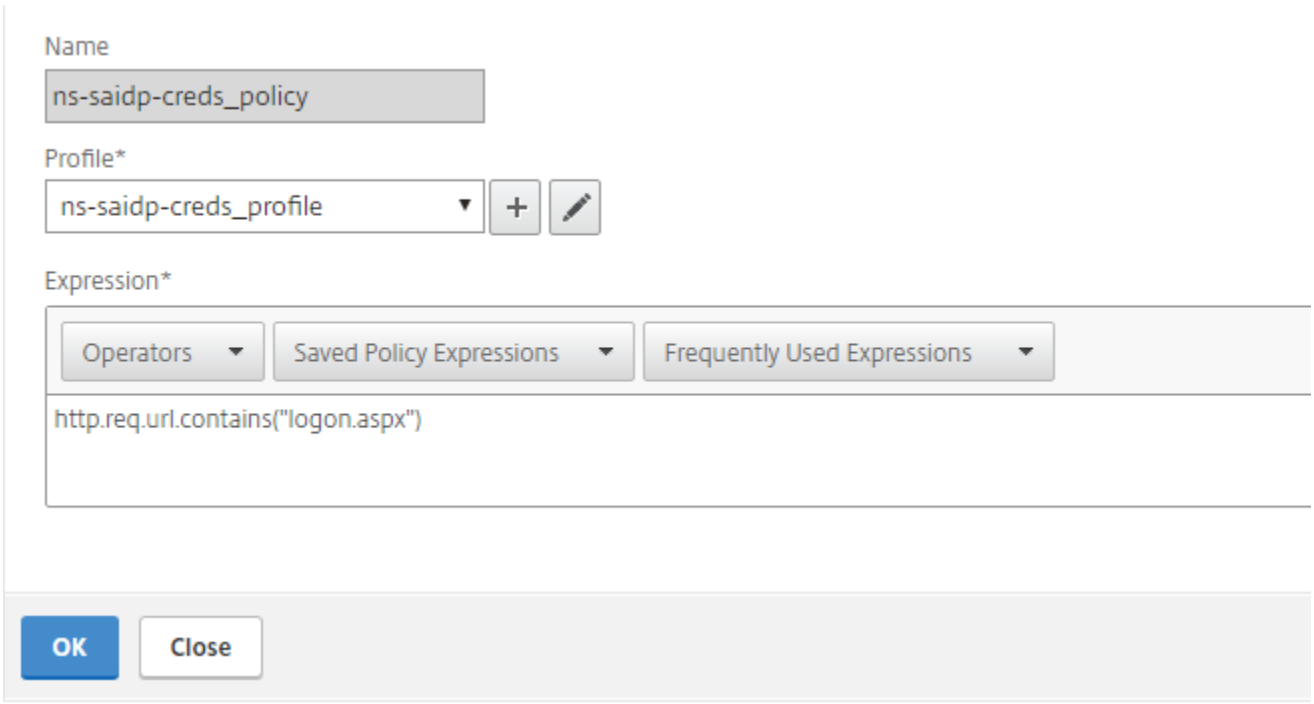
   d. Use the command-line to create the SSO user and password expressions required for the traffic profile. (Creating them through the GUI is not available, so, use the command-line.) Run the following command-line parameters:

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

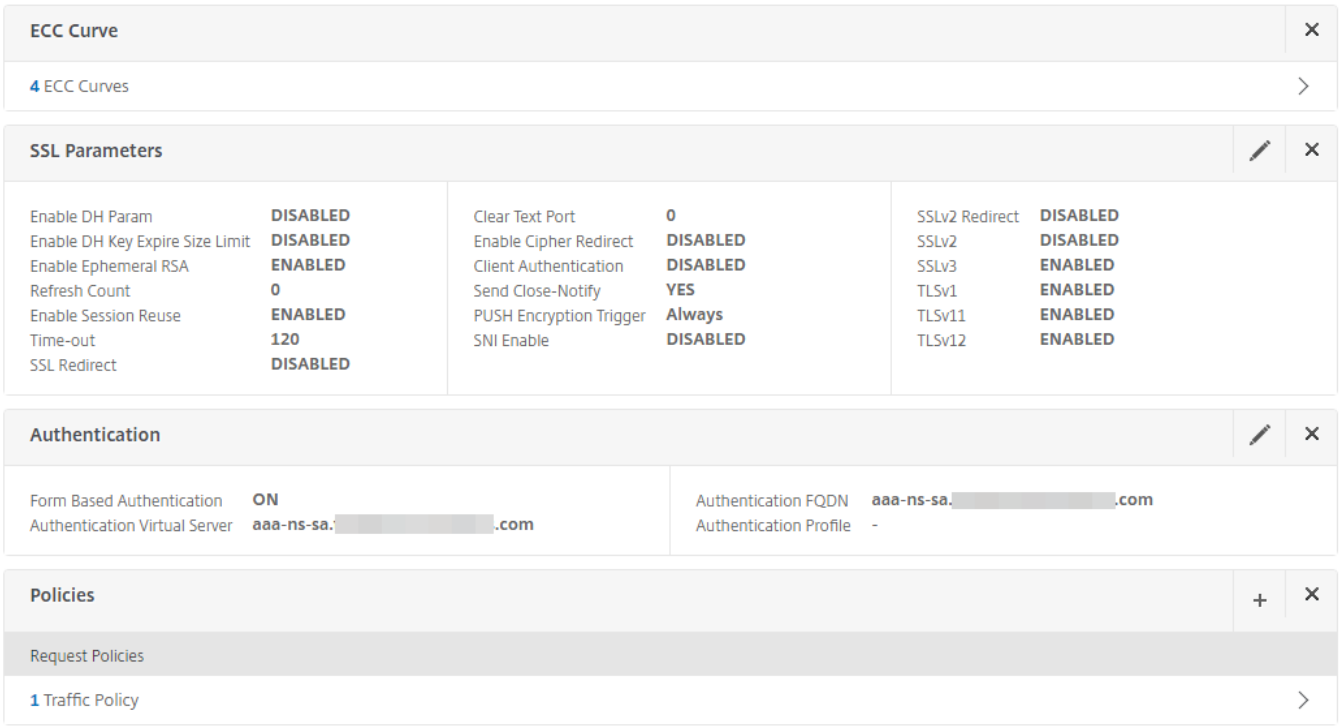
For issues with executing the commands, seek help from either a Citrix Admin or contact Citrix Technical Support.



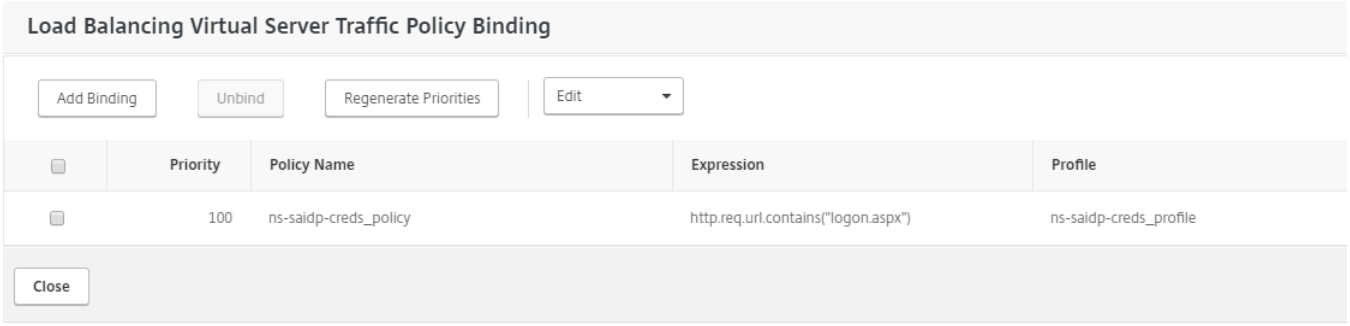
10. Go back to the **Configure Form SSO Profile** section and add the Form SSO profile you just created.
11. Create a traffic policy and attach the profile you created in step 9.



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

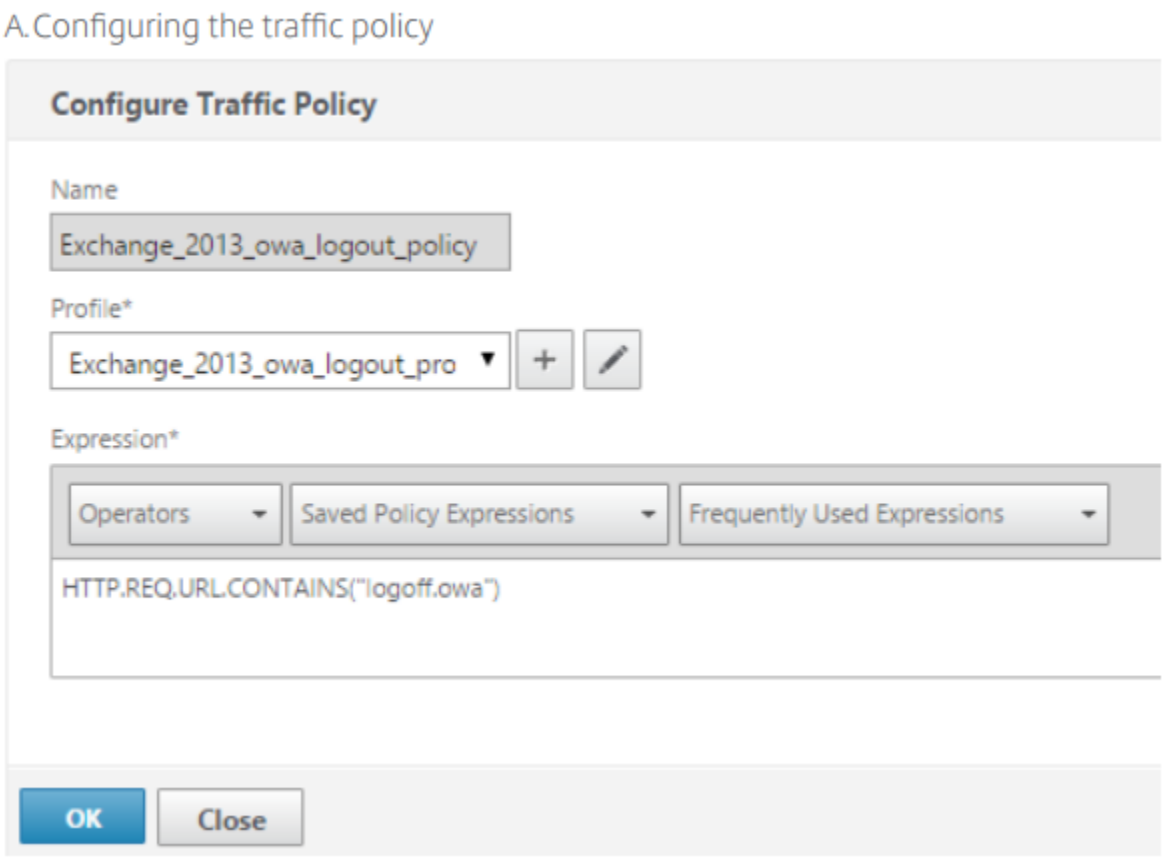


13. Bind the traffic policy to the NetScaler OWA virtual server and save the settings.



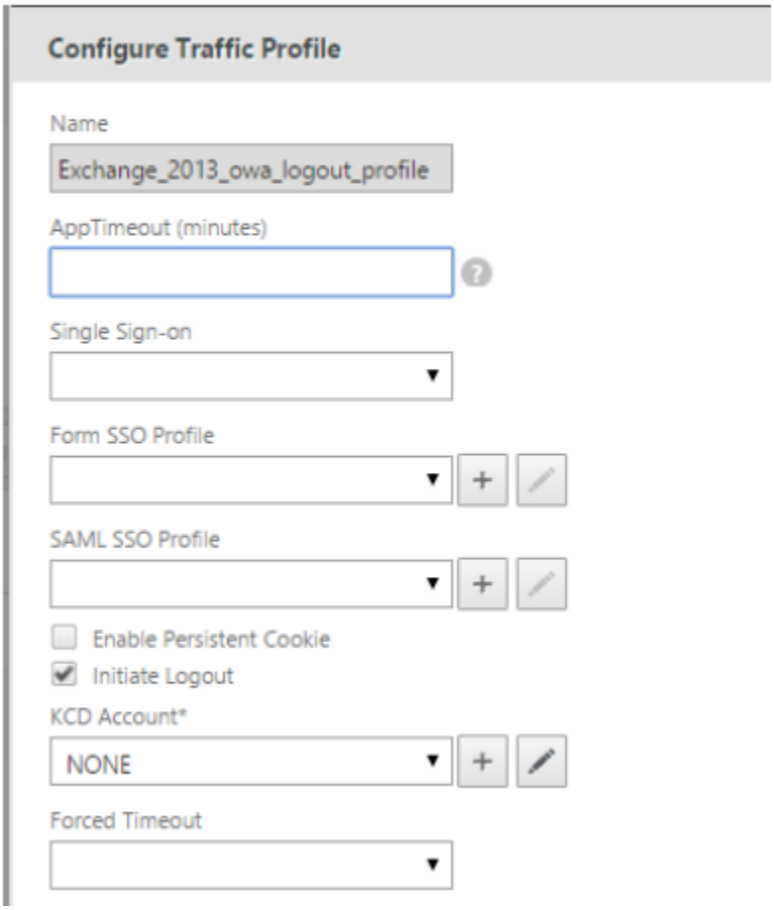
Traffic policy for OWA logout

14. Create a new traffic policy for OWA logout.



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

B. Configuring the traffic profile



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

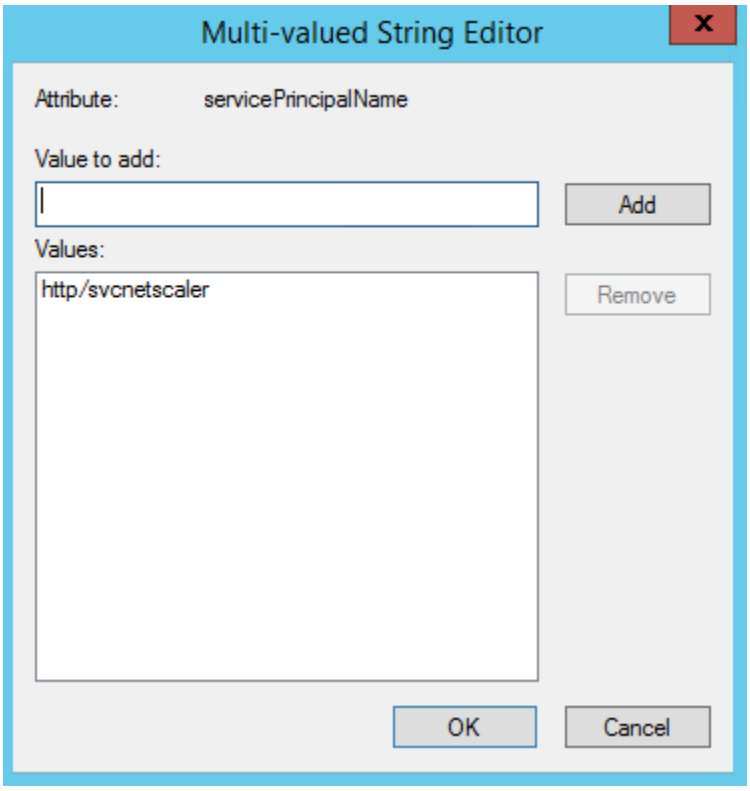
- SecureAuth IdP configured realm (See SecureAuth IdP configuration steps)
- NetScaler Traffic virtual server created in the previous section
- NetScaler AAA server created in the previous section

Active Directory configuration

1. Create a service account with the following entries:

    a. Use the **servicePrincipalName** attribute.

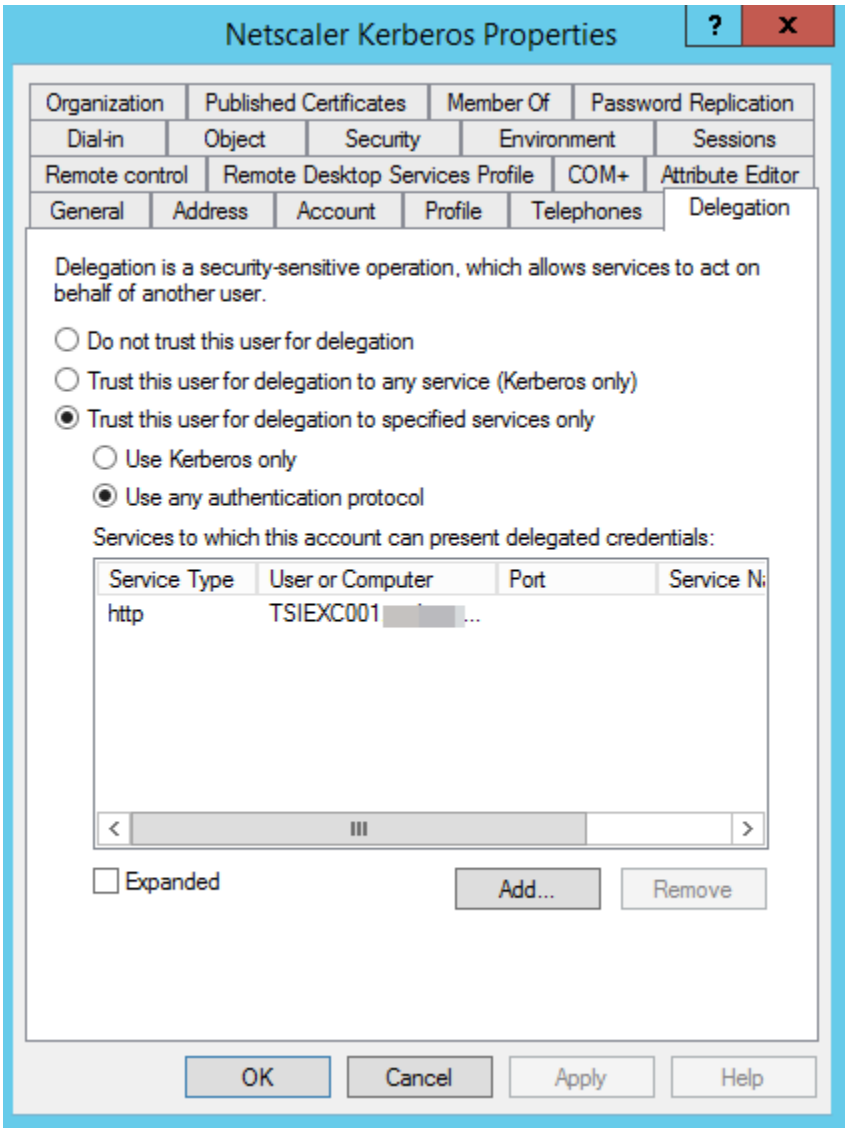
    b. Set the **Values** as http/account_name.



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.

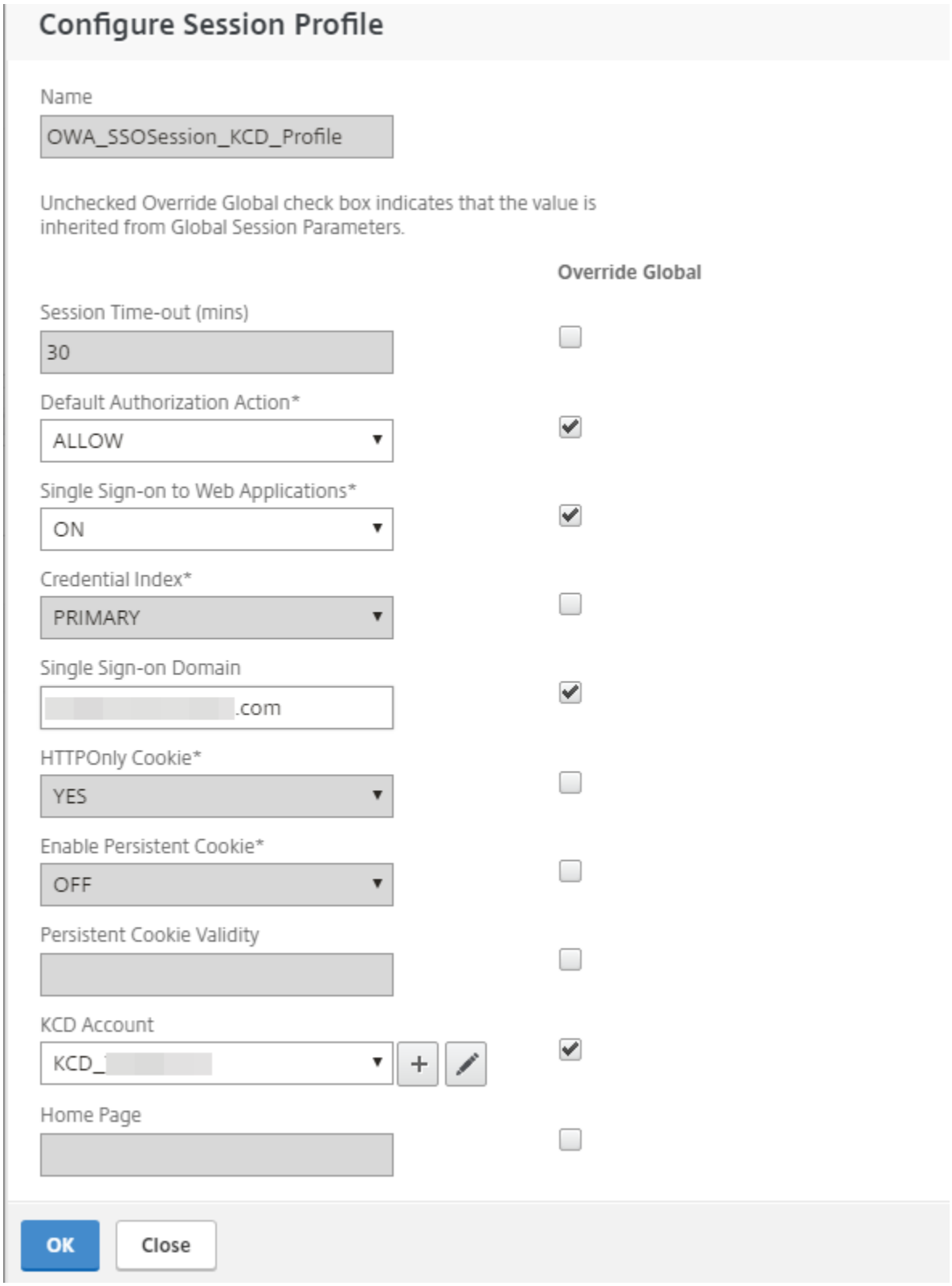
4. Configure a session profile with the following entries and ensure the applicable **Override Global** check box is selected:

    a. Set **Default Authorization Action** to **ALLOW**.

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

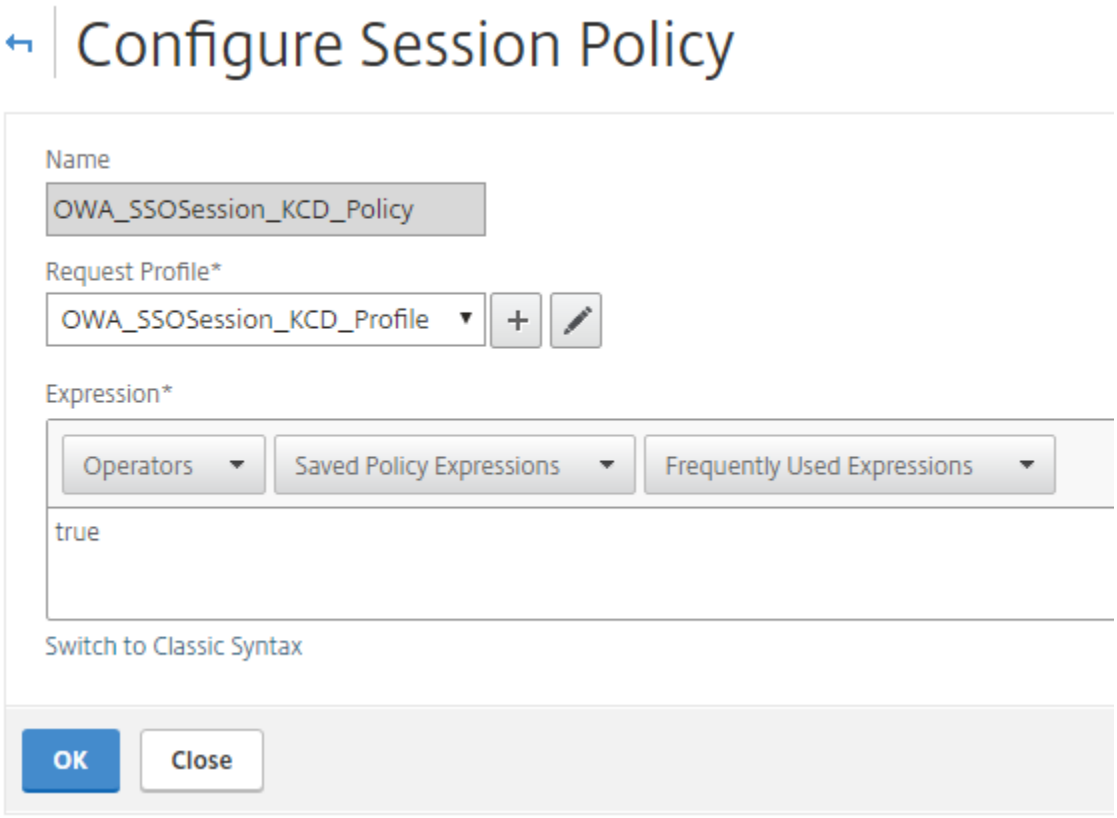
    c. Type the **Single Sign-on Domain** name.

    d. Select the applicable **KCD Account**.



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.



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.

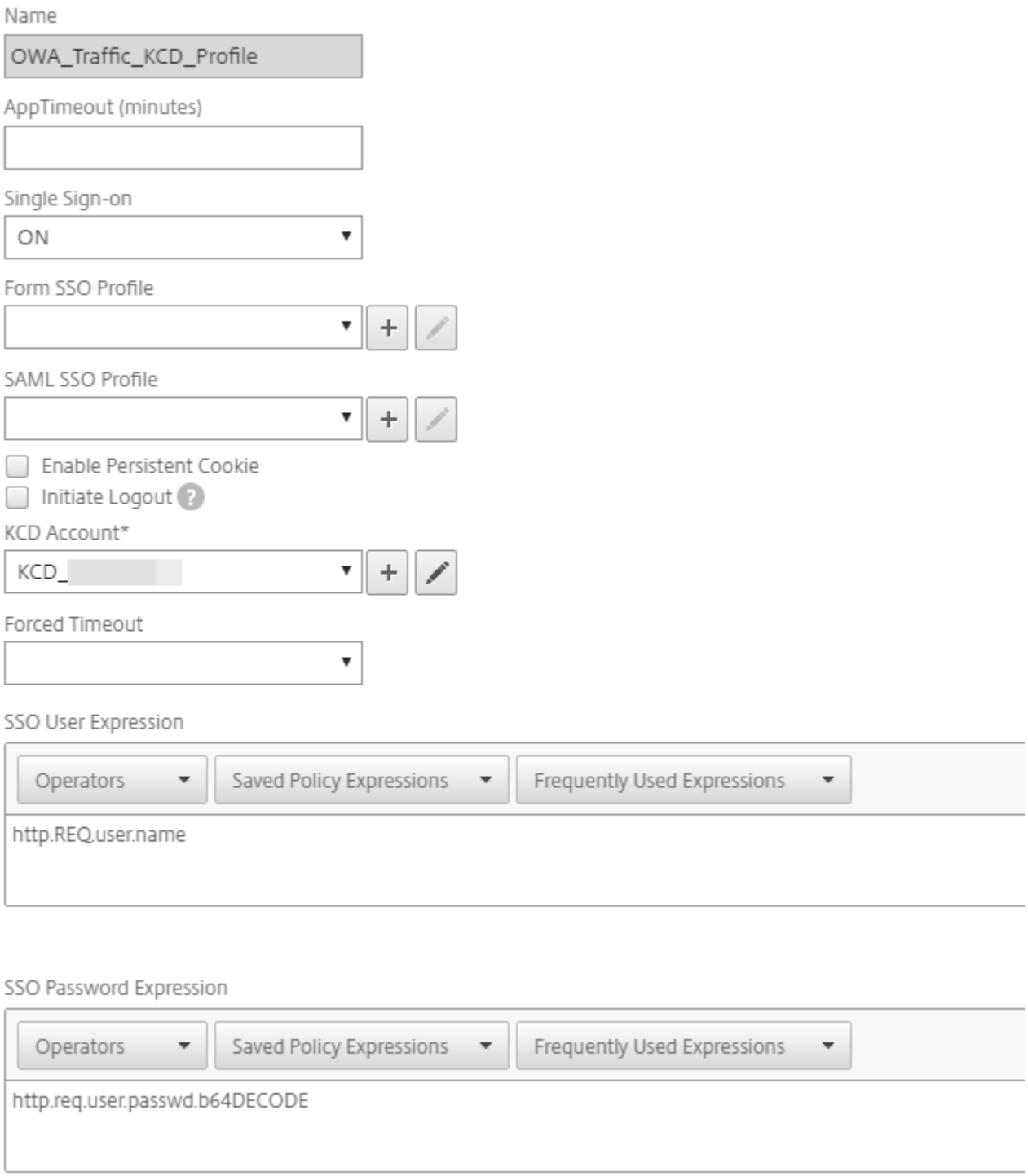
   a. Set **Single Sign-on** to **ON**.

   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:

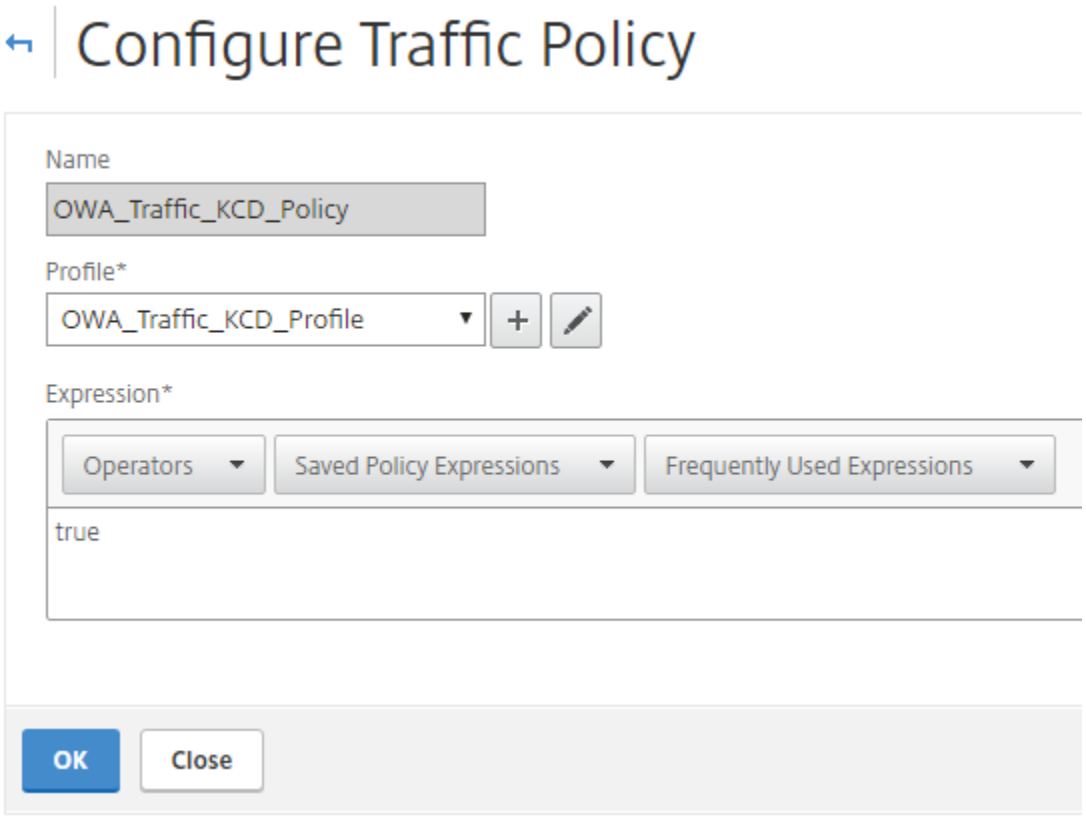
   ```
   set tm trafficAction OWA_Traffic_KCD_Profile -sso on -userExpression http.REQ.user.name
    -passwdExpression http.req.user.passwd.b64DECODE
   ```

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

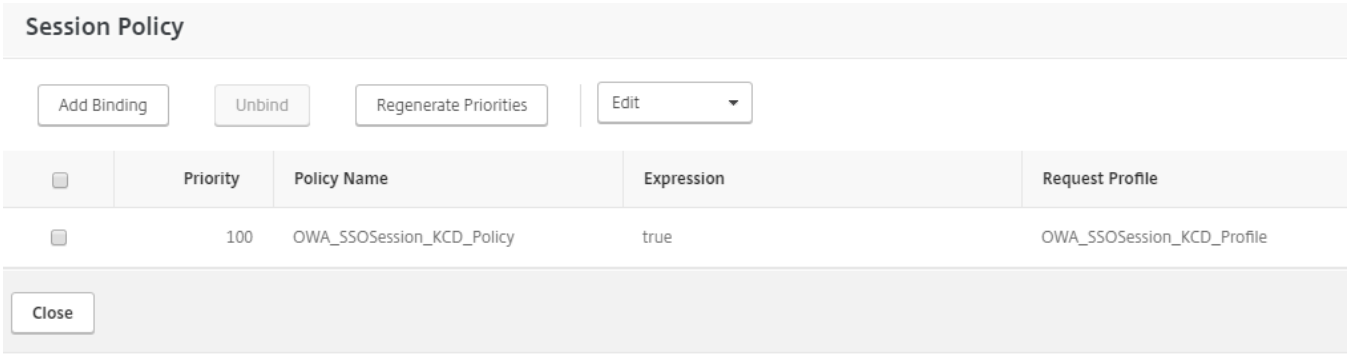


7. In the **Configure Traffic Policy** section, make the following entry:

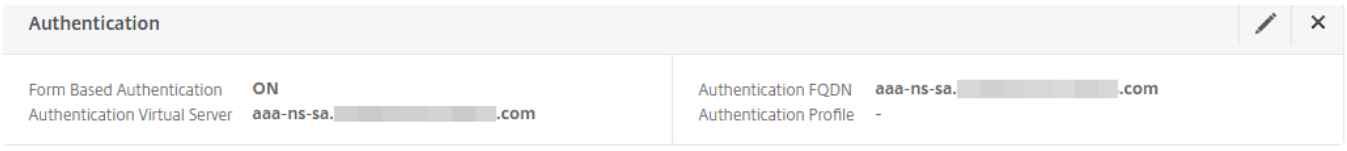
    a. Set **Profile** to the one you just created in step 6.



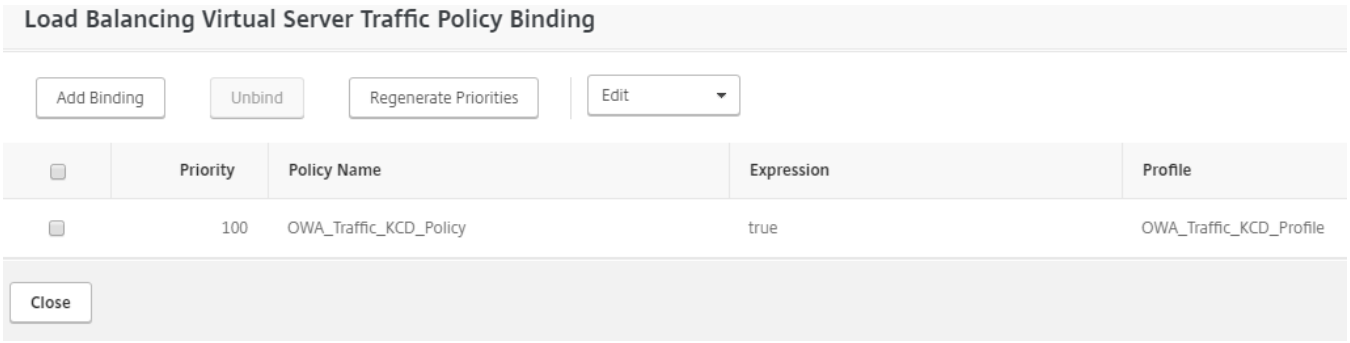
8. In the **Session Policy** section, add the session policy you created in steps 4-5 to the AAA server that will be used for OWA authentication.



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



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



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

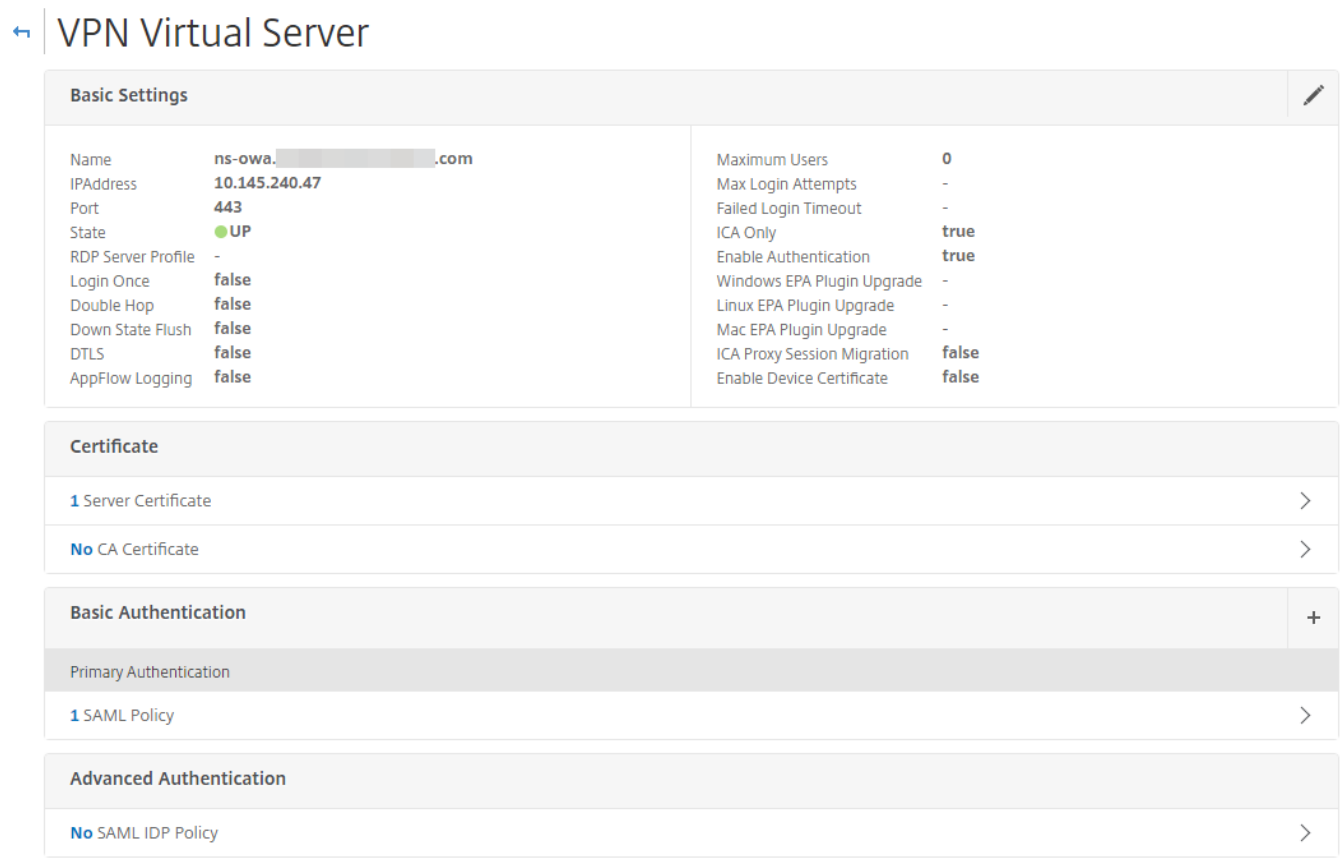
This section describes how to configure NetScaler Gateway for SecureAuth IdP SAML and OWA on Exchange Server 2013 or 2016 form-based authentication and includes

Prerequisites

- SecureAuth IdP realm SAML settings (See SecureAuth IdP configuration steps)

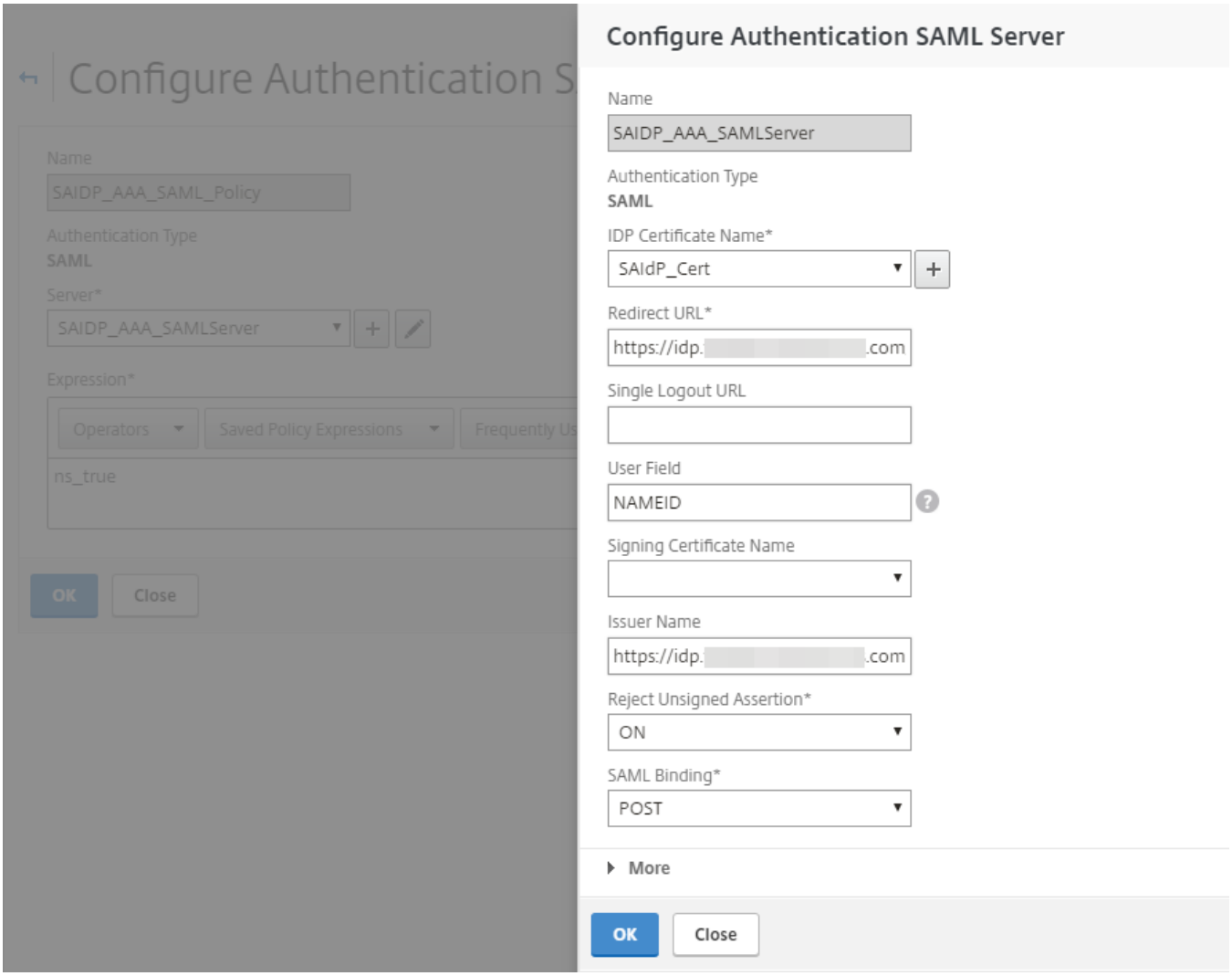
VPN virtual server configuration

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



2. Add the server certificate for SSL.

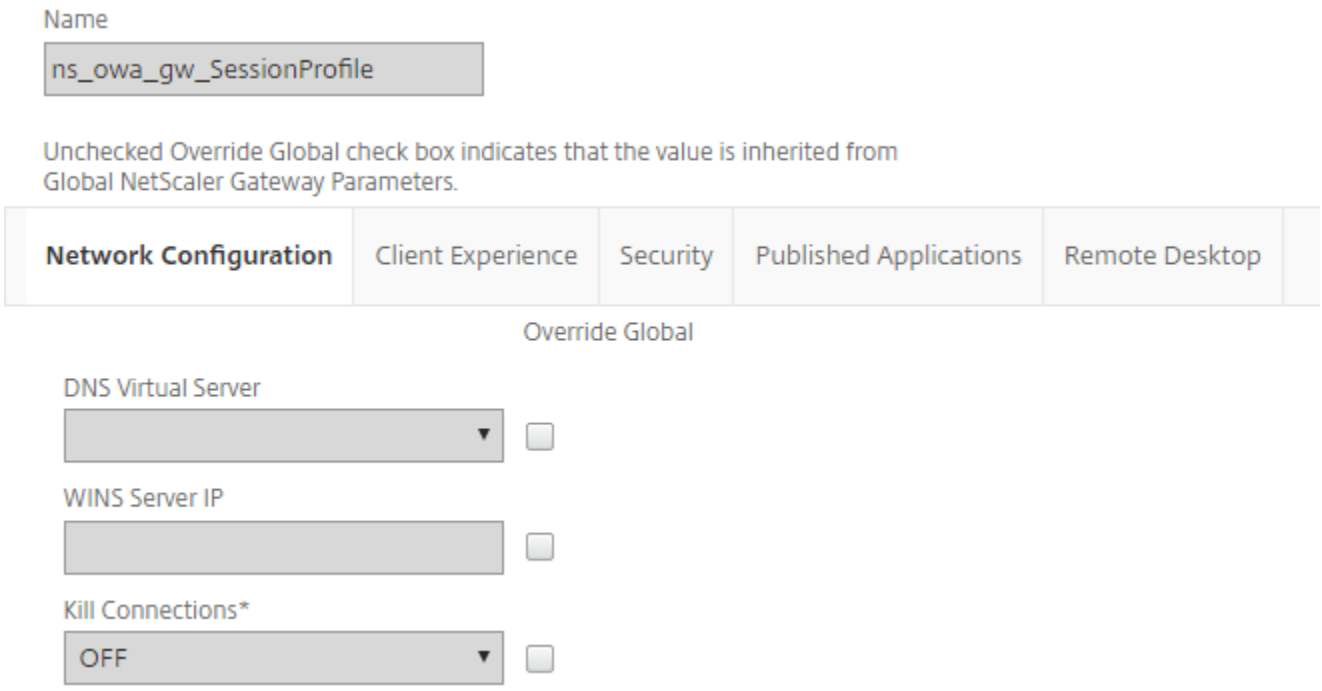
3. In the Basic Authentication section, specify the SAML server that was configured with SecureAuth IdP.



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.

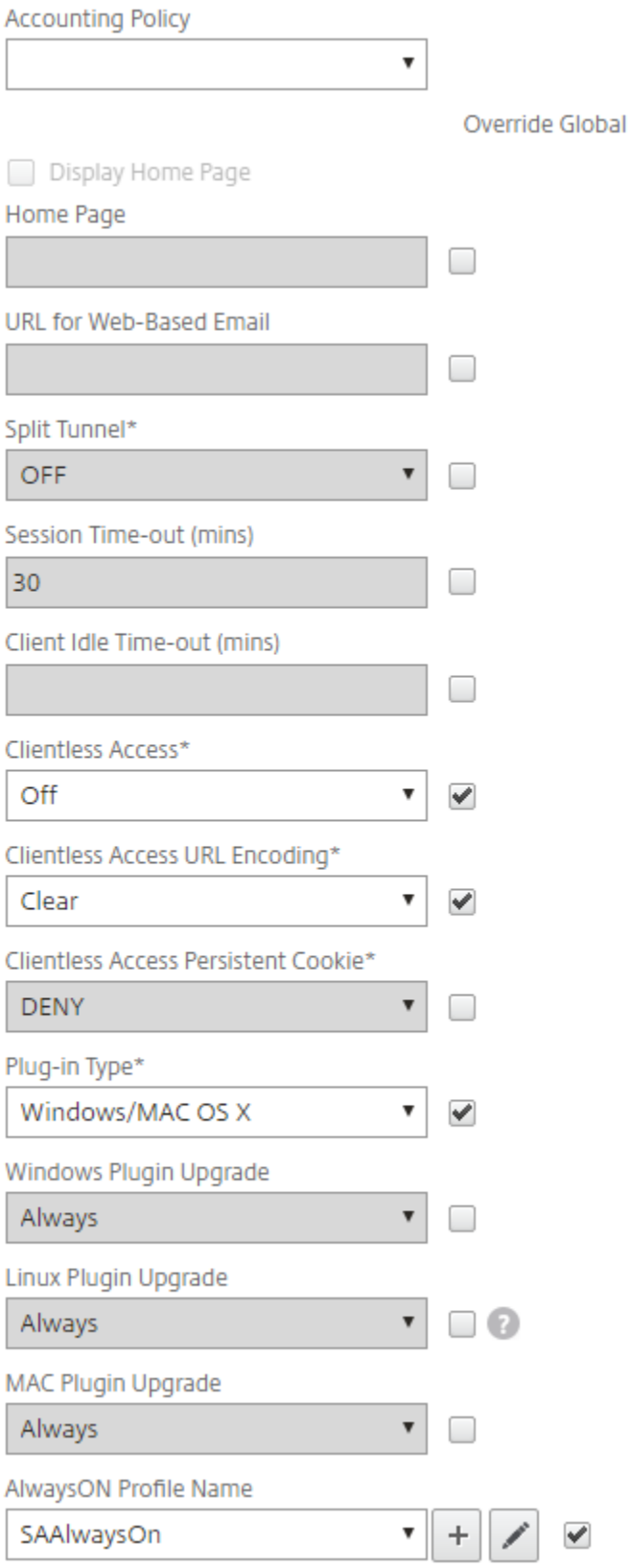


a. Set **Clientless Access** to **Off**.

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**.

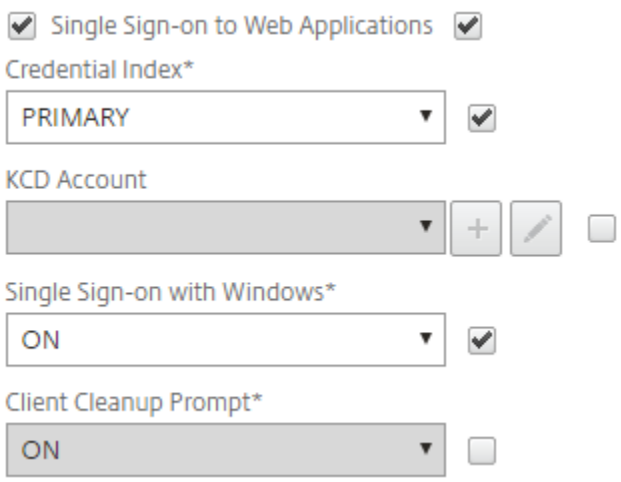


5. Scroll down and continue to make these entries and ensure the applicable **Override Global** check box is selected:

    a. Select the **Single Sign-on to Web Applications** check box.

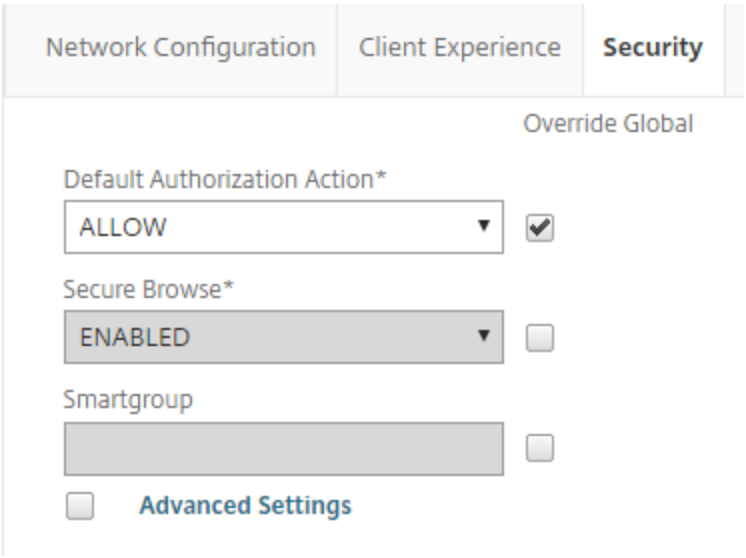
    b. Set **Credential Index** to **PRIMARY**.

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



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

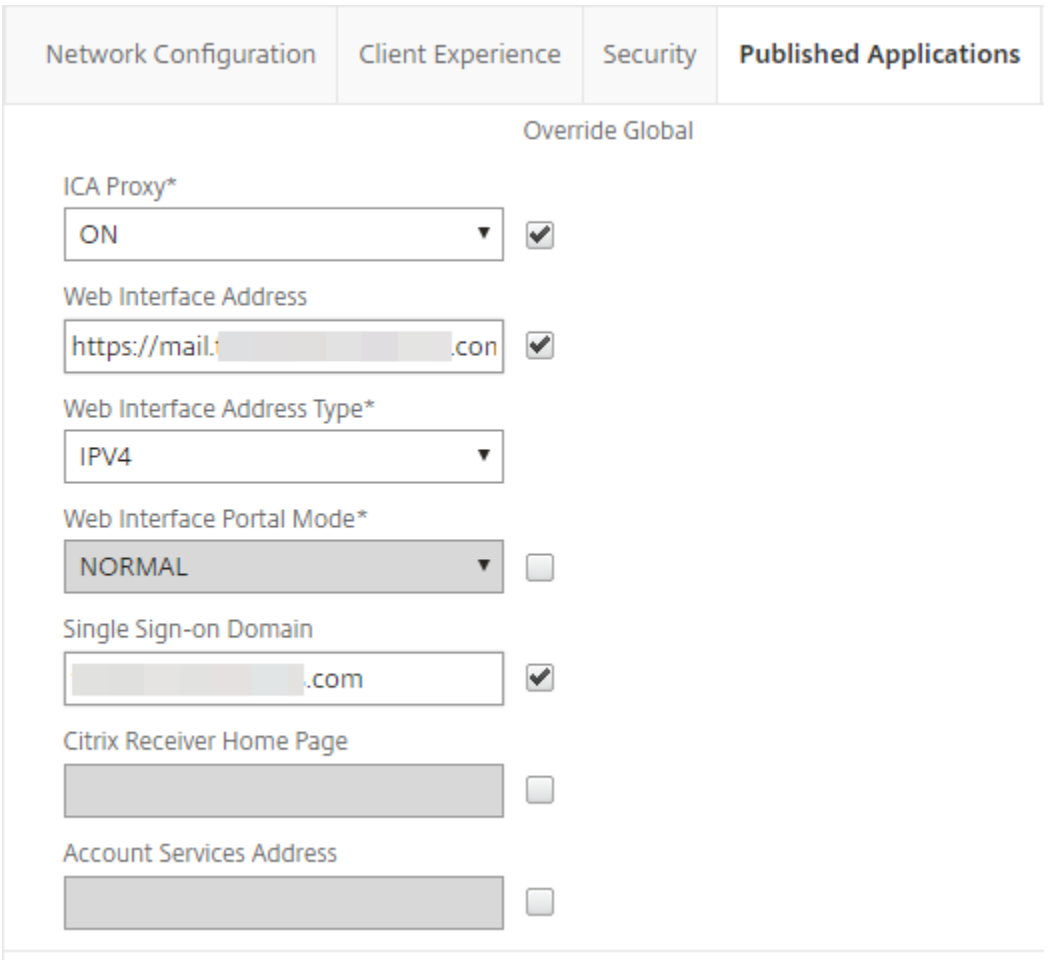
a. Set **Default Authorization Action** to **ALLOW** and ensure the **Override Global** check box is selected.



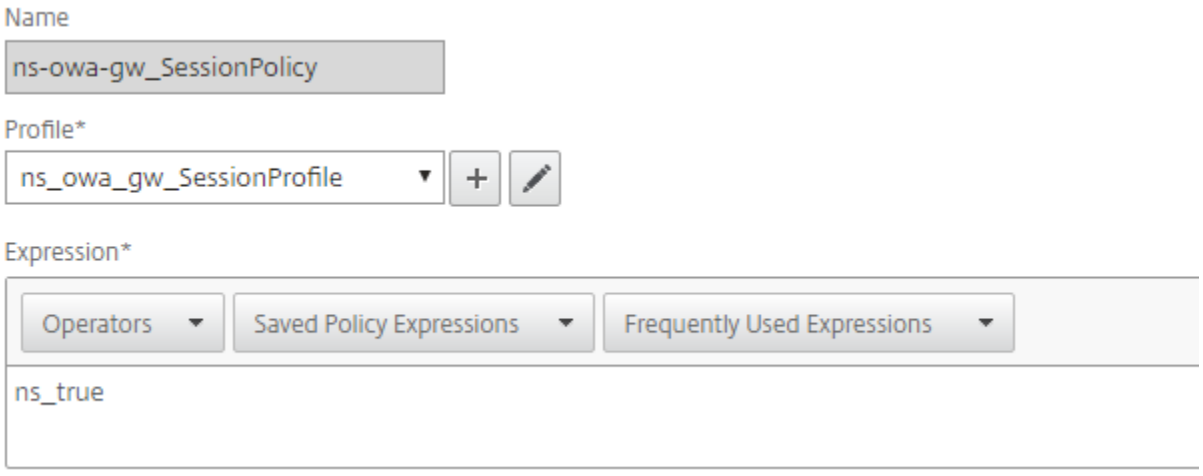
7. On the **Published Applications** tab, make the following entry:

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



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



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

   a. Set the **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:

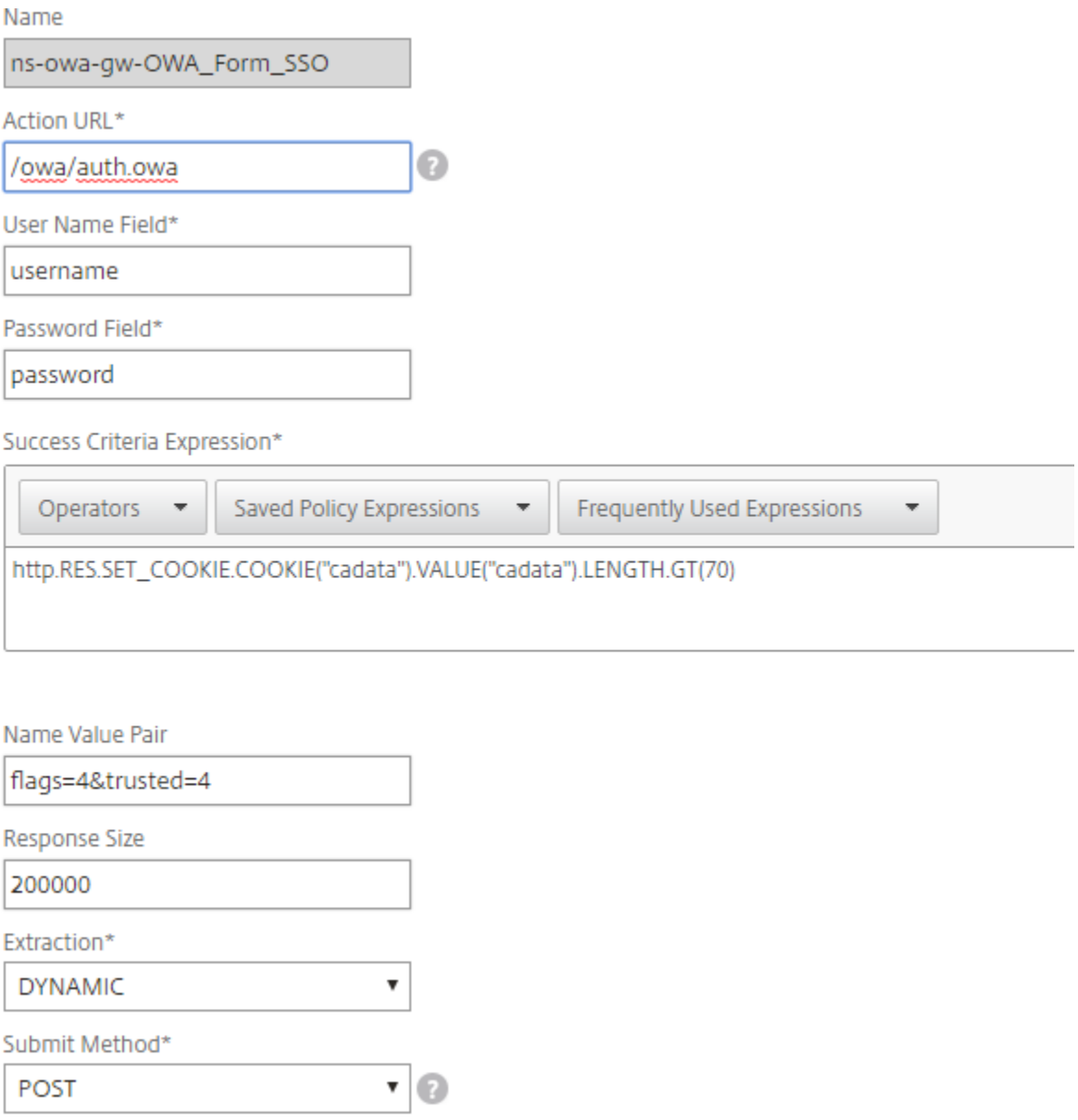
```
flags=4&trusted=4
```

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**.



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**.

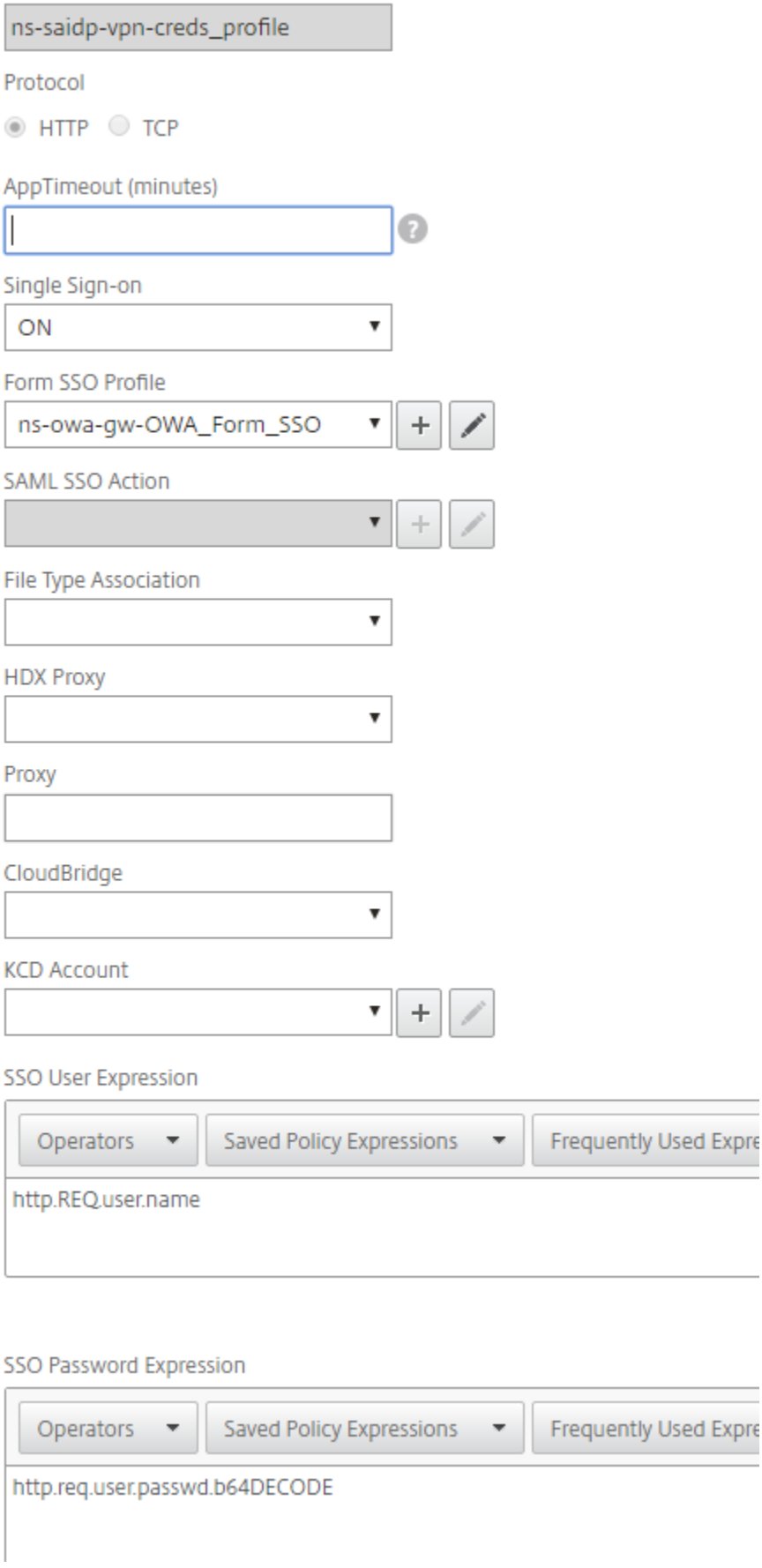
c. Set **Form SSO Profile** to **ns-owa-gw-OWA_Form_SSO**.

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:

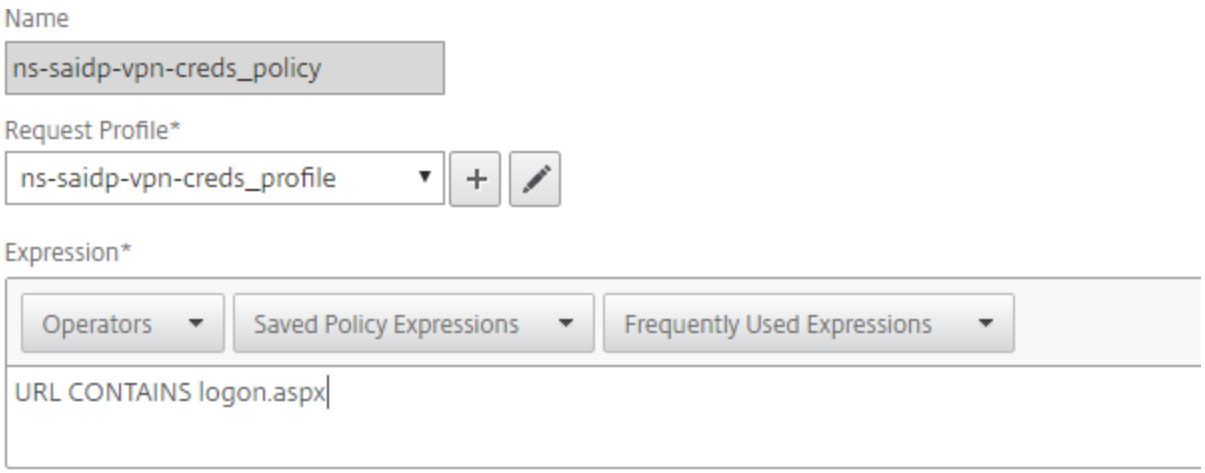
```
add vpn trafficAction ns-saidp-vpn-creds_profile HTTP -SSO ON -formsSOAction ns-owa-gw-OWA_Form_SSO
 -userExpression http.REQ.user.name -passwdExpression http.req.user.passwd.b64DECODE
```

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



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.



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

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:

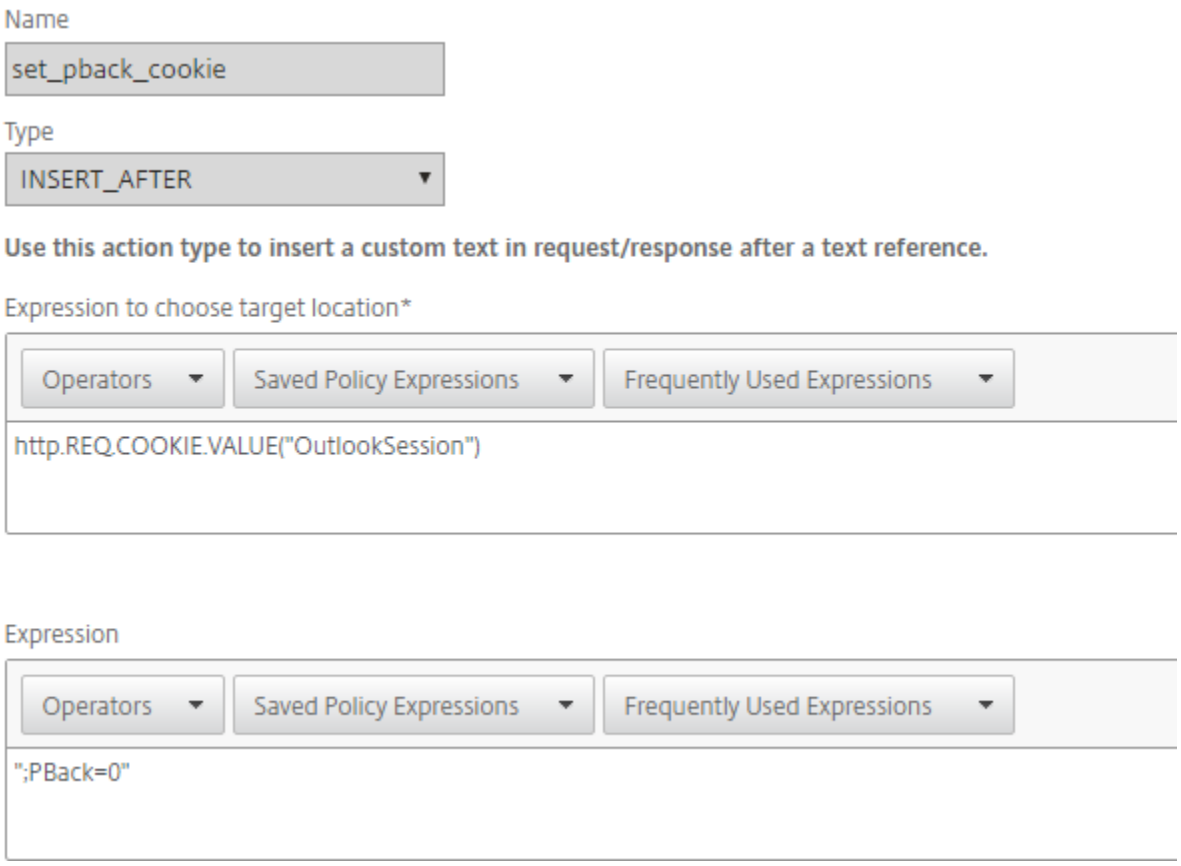
    a. Create the rewrite action.

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

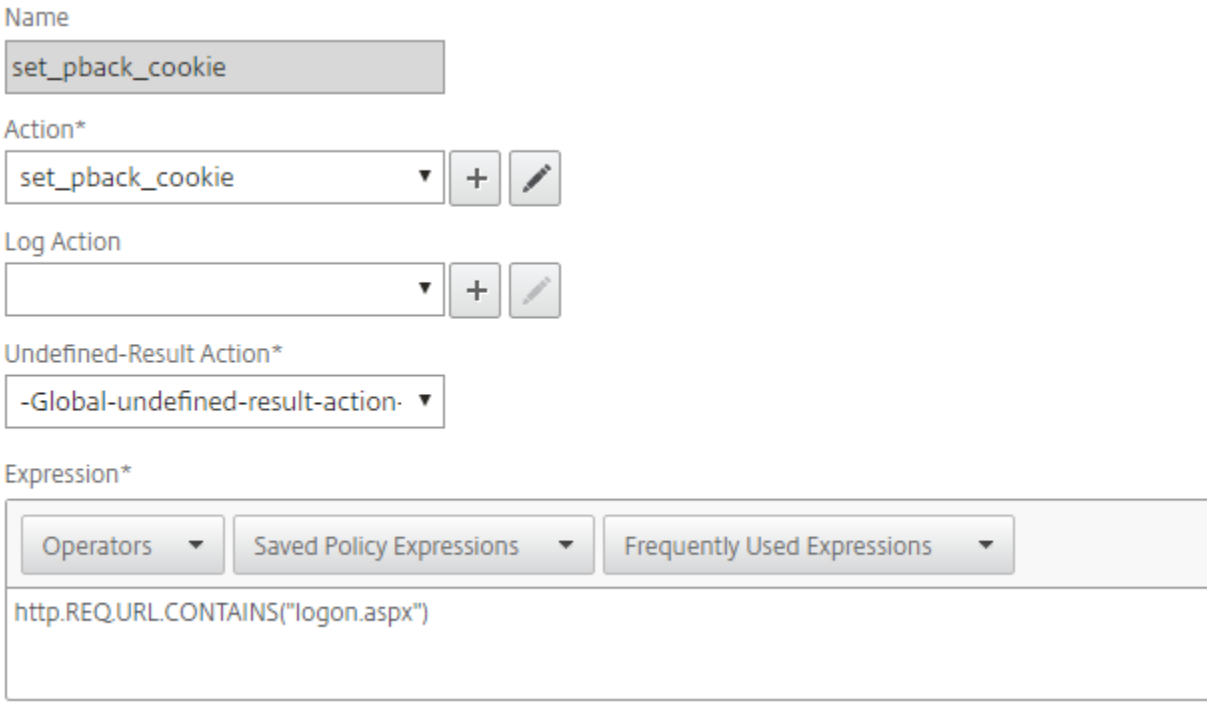
    ```
    http.REQ.COOKIE.VALUE("OutlookSession")
    ```

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

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



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



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.