Steven Wright
November 10th 2021
DRAFT

Deployment Guide: Learn how to configure Citrix Gateway to use nFactor to authenticate against a RADIUS server for MFA

Overview

How to Configure Citrix Gateway to use nFactor to authenticate against a RADIUS server for Multi Factor Authentication (MFA).

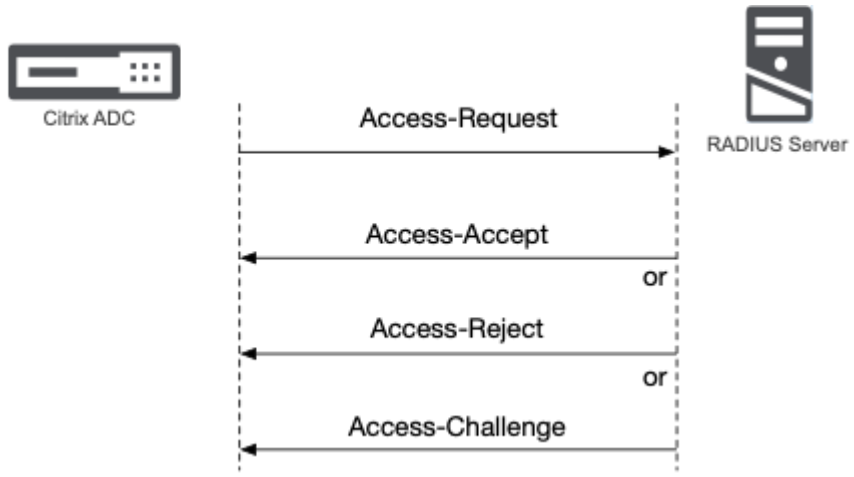
This article will cover how to configure Citrix ADC Gateway to use nFactor authentication for LDAP and RADIUS-based Multi-Factor Authentication and general troubleshooting techniques.

During this article, it is assumed that your Citrix ADC has an existing Citrix Gateway implementation and that RADIUS and LDAP servers are available.

This article also recommends connecting to your RADIUS and LDAP servers via a local load balancing virtual server, and assumes these have already been created. You can learn more about creating load-balancing virtual servers here and about configuring RADIUS persistence on a load balancer here.

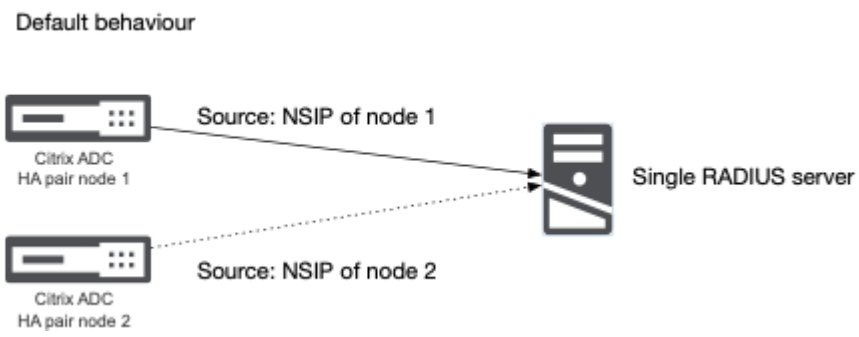
RADIUS Communication Overview

The RADIUS communication flow begins with an Access-Request packet from the client, in this case the Citrix ADC. The RADIUS server will then validate the client and authenticate the credentials received within the Access-Request. The server will then respond with an Access-Accept, Reject, or a Challenge asking for further details from the user.



RADIUS servers have a list of valid clients and a shared secret for each. A RADIUS server will usually ignore requests from invalid clients, but some implementations may return authentication failures. The shared secret is used to encrypt the password component of the credentials sent in the Access-Request; if the shared secret is incorrect, the server will always reject passwords as they will not decrypt to the correct value.

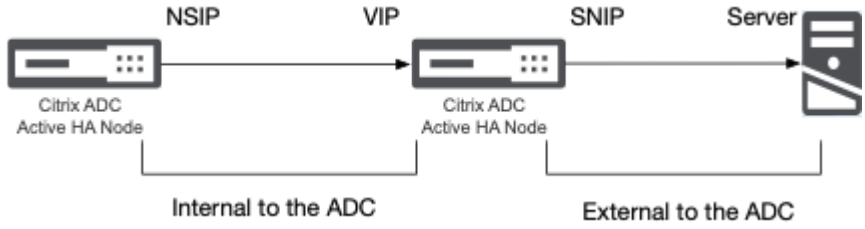
By default, Citrix ADC sends RADIUS authentication requests from the NSIP of the active HA node and targets a single RADIUS server.



To avoid defining the NSIP of both nodes in an ADC HA pair as valid clients on your RADIUS servers and to target one of several RADIUS servers to give resilience, Citrix recommends sending authentication requests via a local Load Balancing vServer.

When Citrix ADC sends RADIUS requests via a local Load Balancing vServer, the requests will leave the ADC via a SNIP. SNIPs are floating IP addresses and are only available on the current primary HA node.

The complete data flow when using a local Load Balancing (LB) vServer is that the NSIP of the current primary HA node will send a request to a local VIP associated with an LB vServer, and the LB vServer will then send the request to a RADIUS server from the HA pair's SNIP.



RADIUS Troubleshooting tools

While most RADIUS implementations are performed without, it can be helpful to understand the most common troubleshooting tools.

The "/tmp/aaad.debug" authentication debug pipe on the Citrix ADC

You can monitor authentication events on the Citrix ADC by entering the BSH shell with the command "shell" and then view the aaad.debug pipe with the command "cat /tmp/aaad.debug".

You can find more information on "aaad.debug" here: https://support.citrix.com/article/CTX114999

NTRadPing

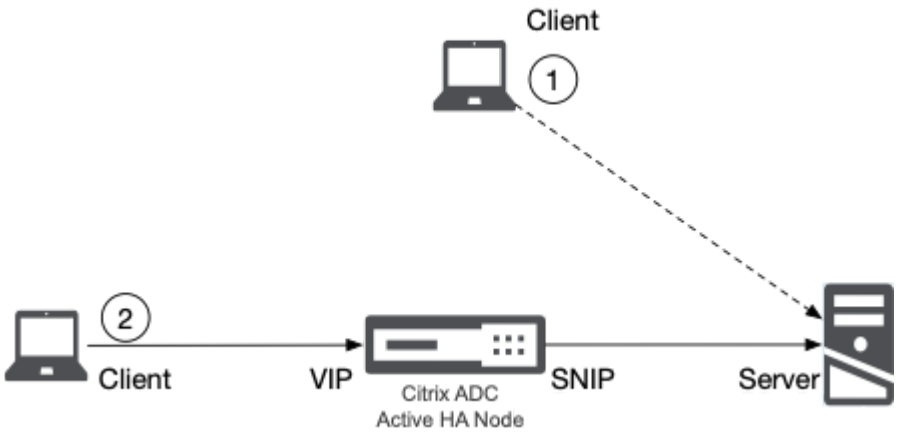
NTRadPing is a free third-party RADIUS test utility that allows you to manually generate RADIUS authentication requests and to observe the response. You can download NTRadPing here:

Using NTRadPing, you can send RADIUS authentication requests directly from your client to the RADIUS server and ensure that it is fully operational. Note that you will need to define your client's IP address and a shared secret on the RADIUS server so it is a valid client and, you may also need firewall rules to allow communication between your client to the RADIUS server.

Using NTRadPing, you can also send authentication requests to the LB vServer on the ADC, which it will forward to the RADIUS server. As these requests will originate, from the viewpoint of the RADIUS server,

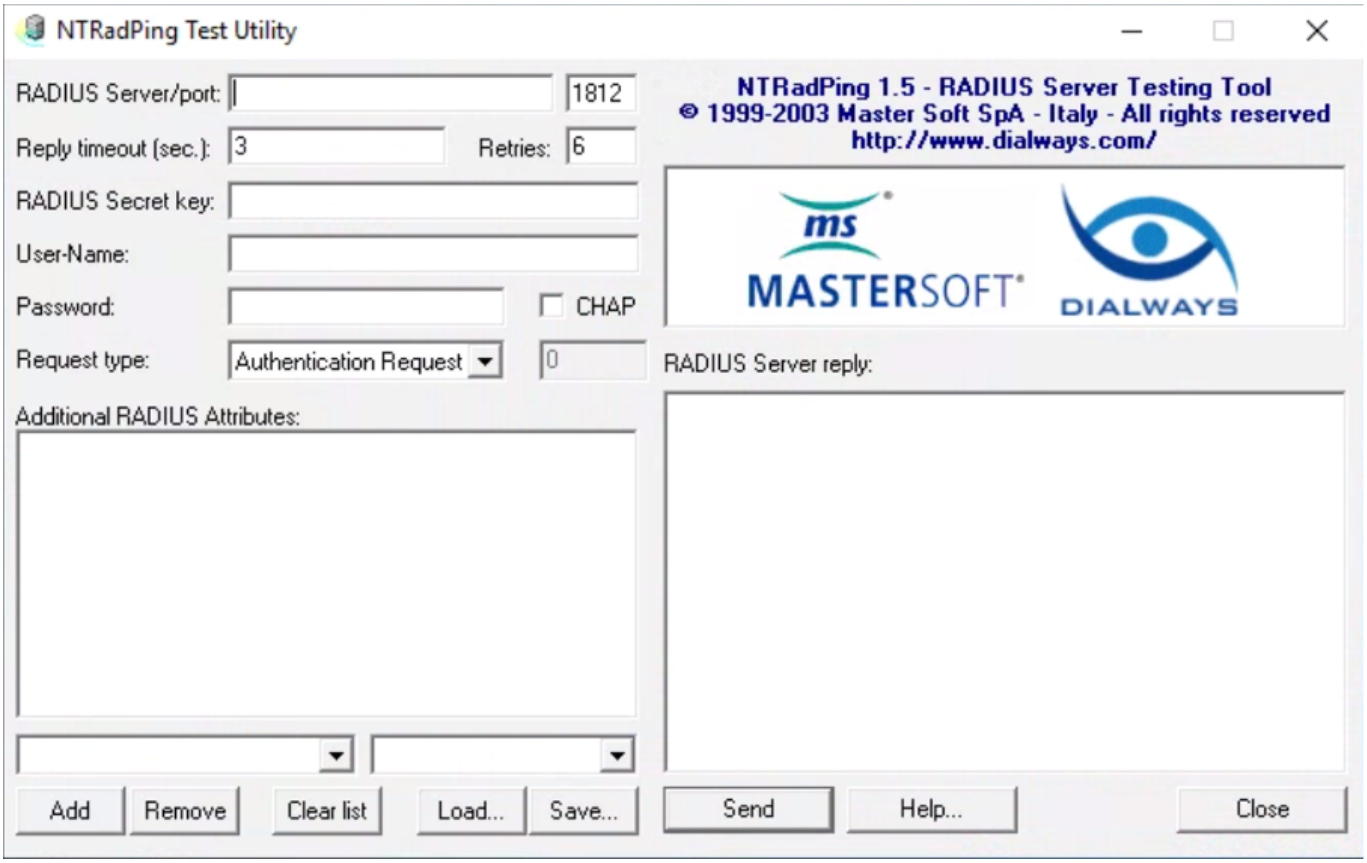
from the ADC, you need to use the same shared secret in NTRadPing as the ADC and, you may also need firewall rules to allow communication from your client to the ADC's RADIUS LB vServer.

In both cases, the test's purpose would be to isolate where a failure is occurring by testing each component separately. For example, suppose you diagnose that you can send successful requests via the ADC's RADIUS manually. In that case, you will know that the problem must be with something before that point, such as the RADIUS server definition on your ADC, and you can correctly focus your efforts.



NTRadPing consists of two files that you should extract into the same directory from its compressed zip. On launch, NTRadPing will prompt for:

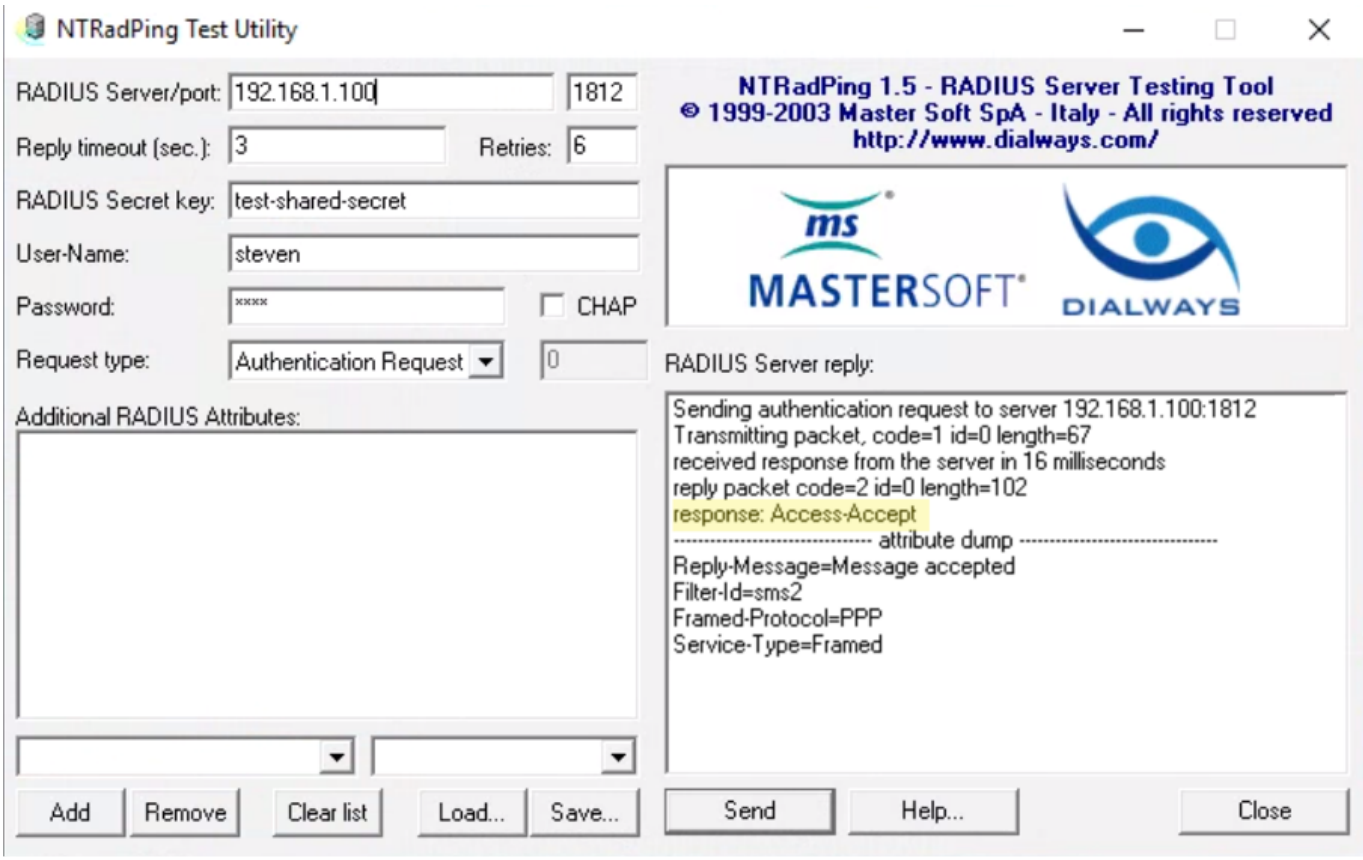
- The RADIUS server and port
- The RADIUS secret
- A username and password
- The Authentication request type



Depending on the test you are performing, you should use a RADIUS server IP address or that of the ADC's LB vServer. In both cases, you should use port 1812.

You will have set a RADIUS secret for your client if you are sending queries directly. If you are sending queries via the ADC's LB vServer to imitate authentication requests from Gateway, you should use the same shared secret as you have configured the ADC to use. The username and password fields should contain the credentials you expect the ADC to send to the RADIUS server on behalf of a user. Usually, the "password" field would contain the user's MFA token value.

Pressing "Send" will cause NTRadPing to send an authentication request from your client computer to the specified destination and, the server result (usually an Access-Accept or Access-Reject message) will be displayed in the right window.



WireShark

If you take a packet trace on the Citrix ADC during the authentication process, you can open that trace within WireShark and apply a display filter to examine the RADIUS request and response.

WireShark is the world's foremost and widely-used network protocol analyzer. WireShark is free and available without here.

You can find WireShark's RADIUS filter's here.

You can find the steps to take a packet trace on a Citrix ADC here.

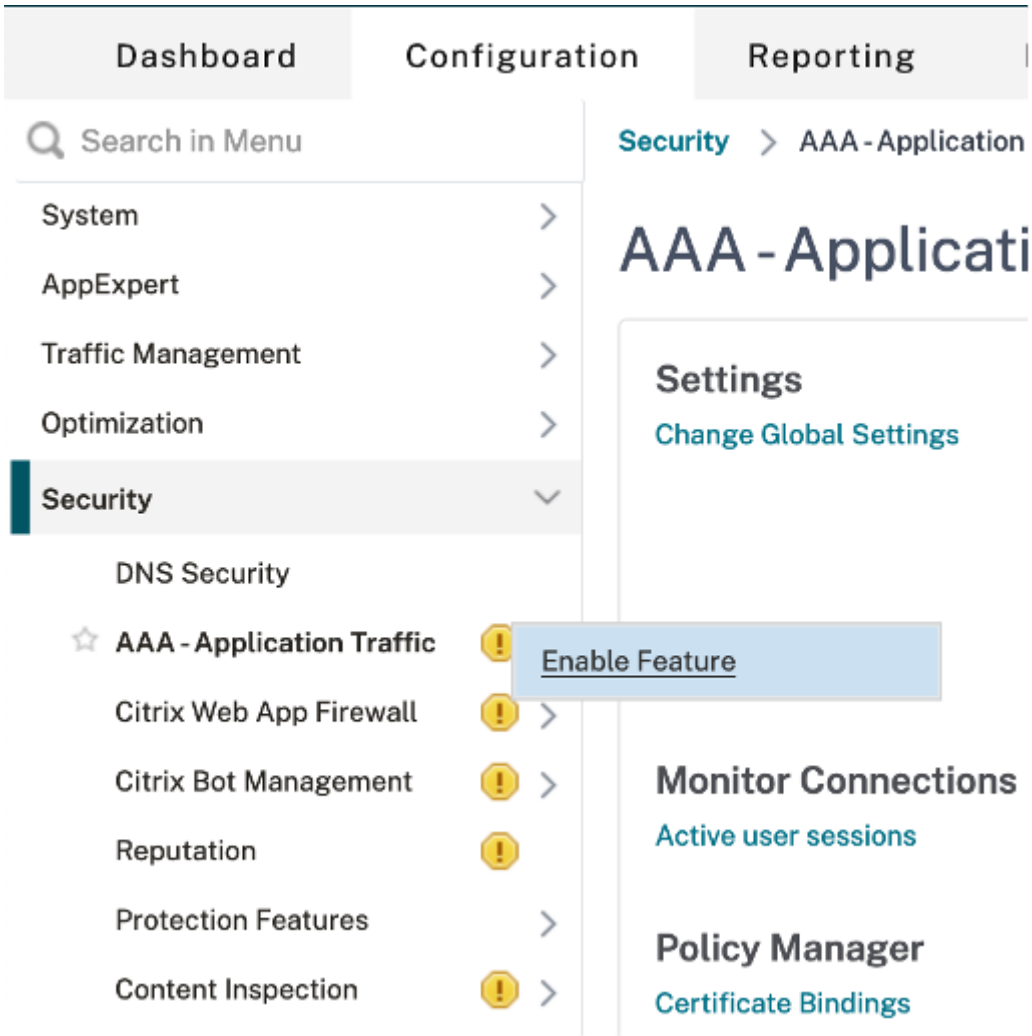
The RADIUS communication you observe within WireShark should consist of an Access-Request packet followed by a response of either Access-Accept, Access-Reject, or Access-Challenge. Missing responses often indicate a communication problem such as absent firewall rules or the RADIUS server not having a definition for the client.

GUI Instructions

Assuming that the configuration on your RADIUS servers is already complete, follow the following steps for the MFA authentication with Citrix Gateway:

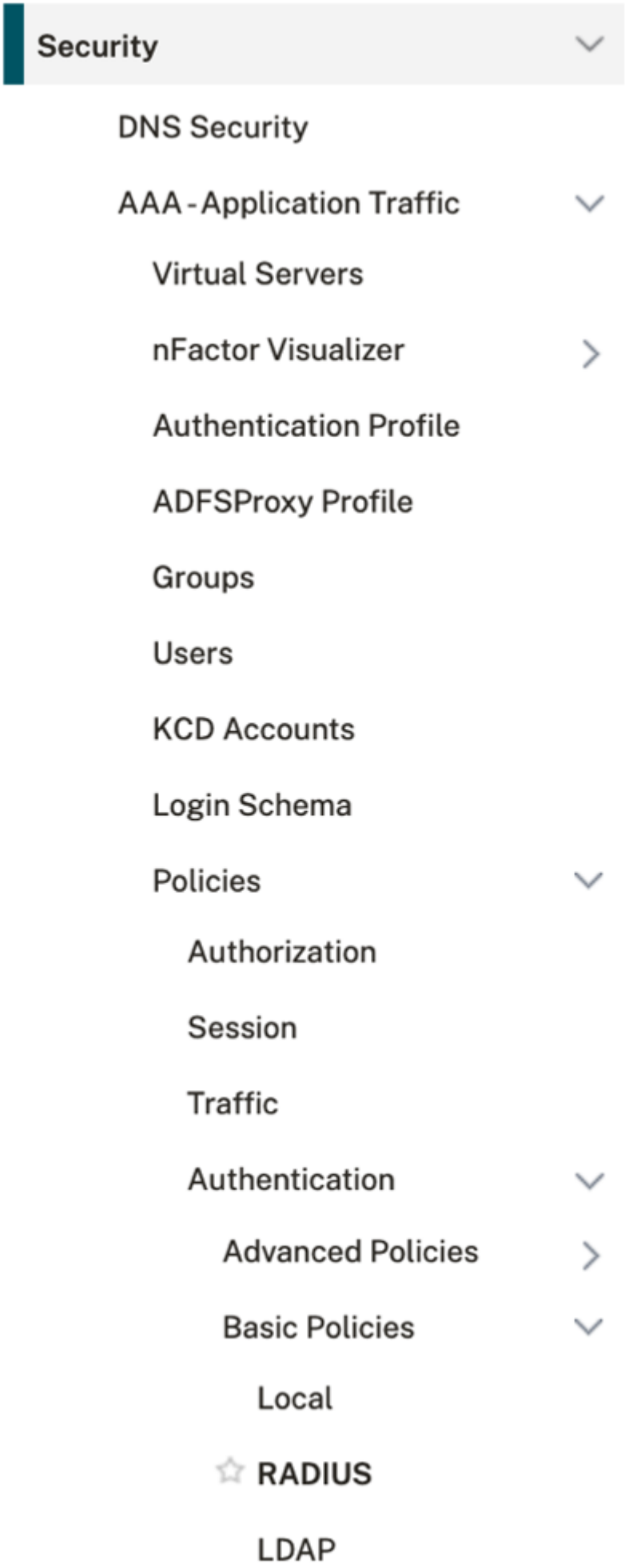
Enable the AAA feature

1. If AAA feature is not already enabled, navigate to, **Security > AAA – Application Traffic**, and right click to enable feature.

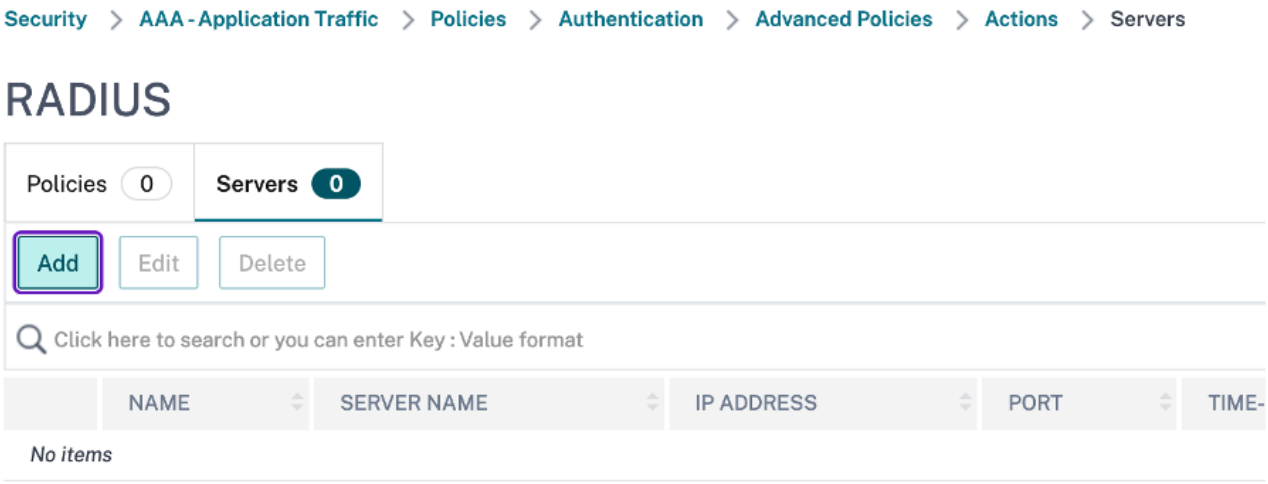


Add Authentication Servers

1. Select **Security > AAA – Application Traffic, Policies, Authentication, Base Policies, RADIUS**.

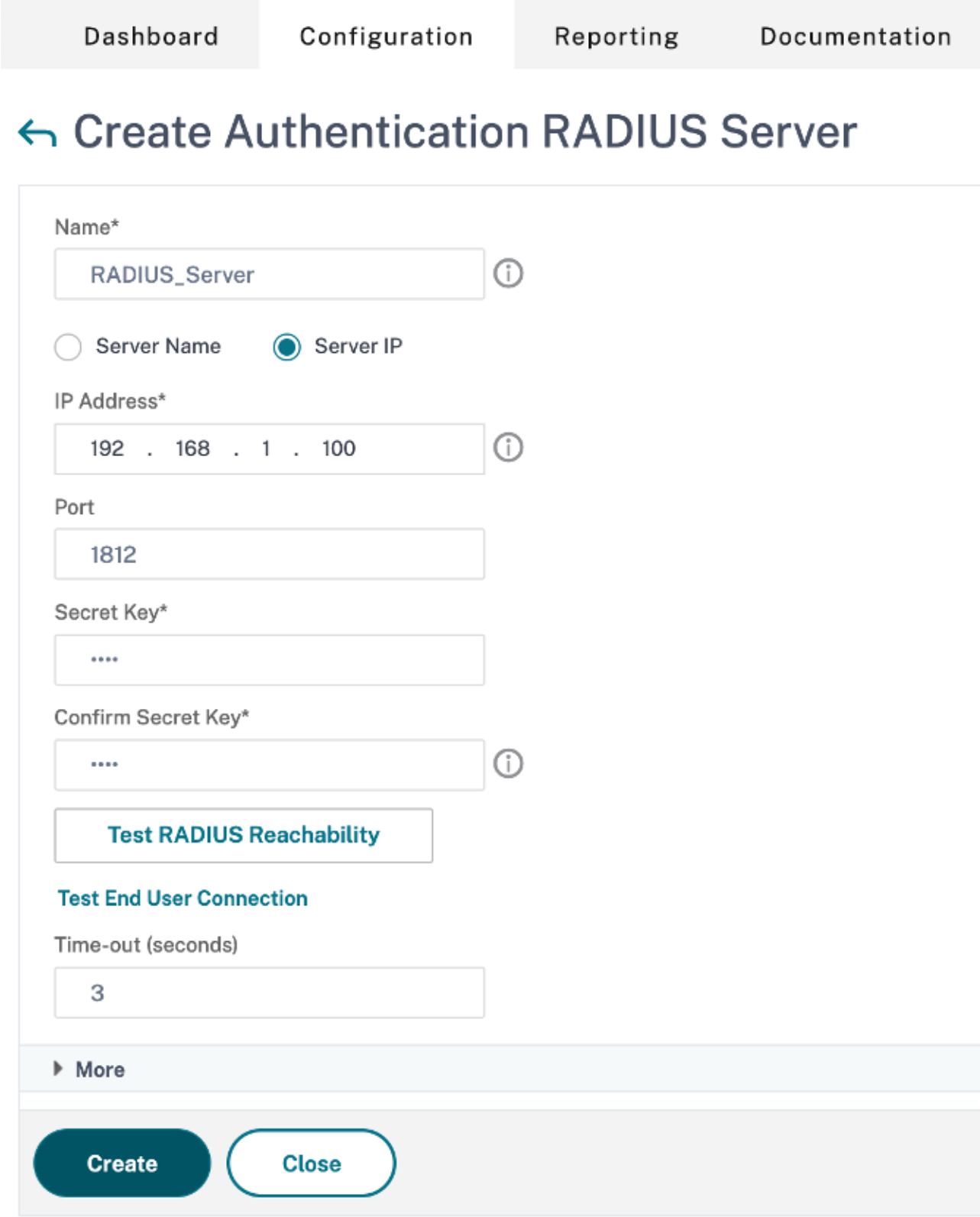


2. Select the Servers tab and then click "Add".

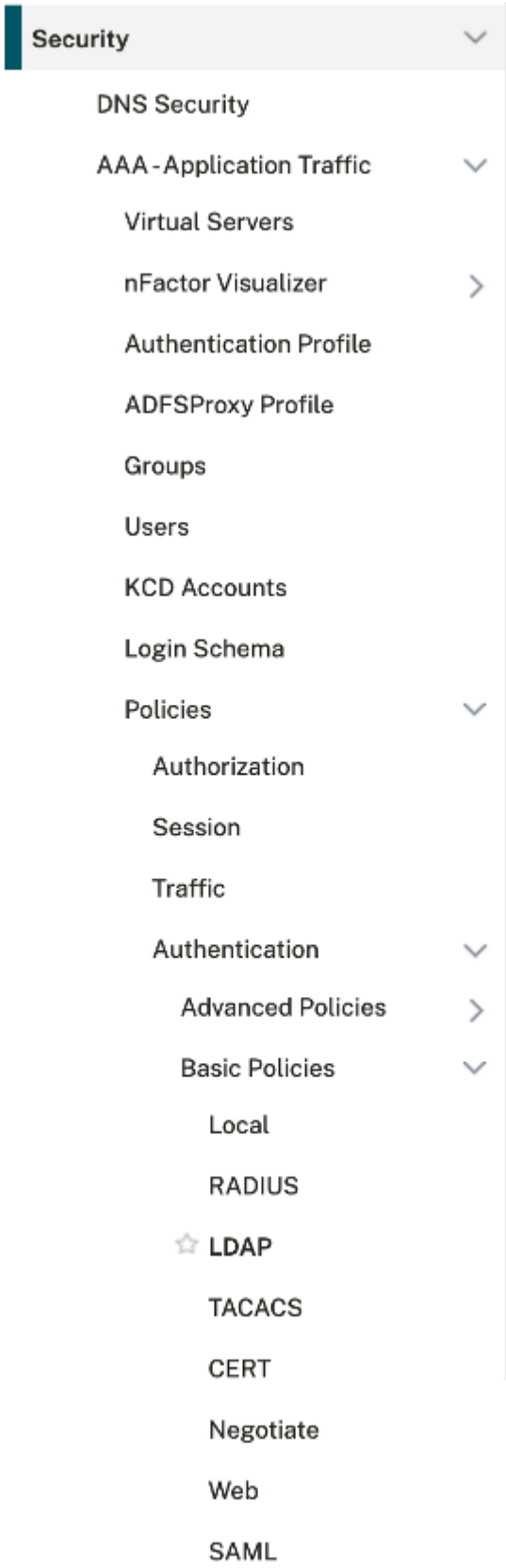


3. Populate details of your RADIUS server

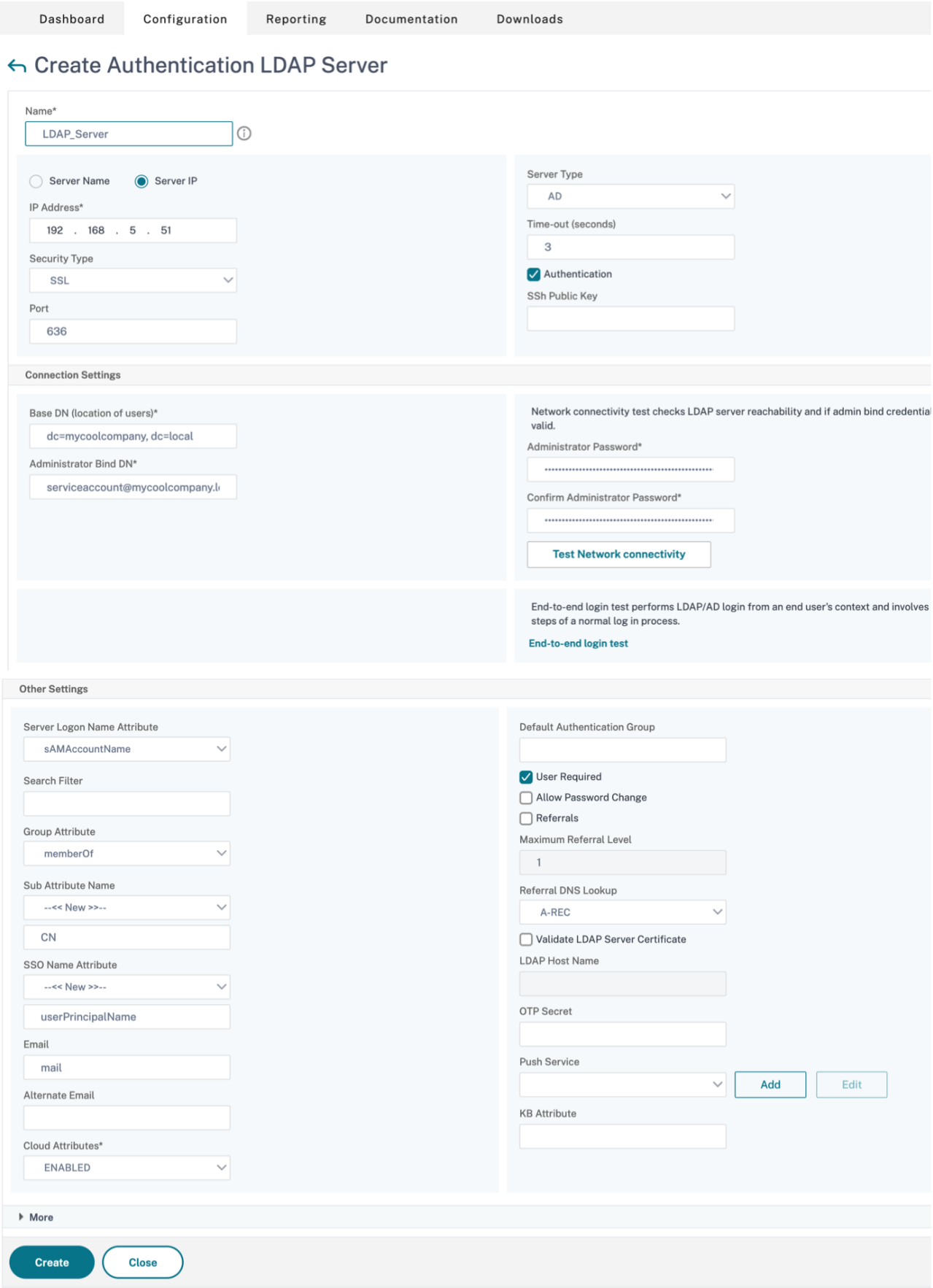
   As described in "RADIUS Communication Overview", Citrix recommends that you do not target an individual RADIUS server but, instead target a local Load Balancing (LB) vServer. As such, you should use the VIP of your RADIUS LB vServer as the Server IP on this page. The Secret Key should correspond to the value on your RADIUS server for the ADC's SNIP.



4. Select **Security > AAA – Application Traffic, Policies, Authentication, Base Policies, LDAP**. Then, select the "**Servers**" tab and click "**Add**".

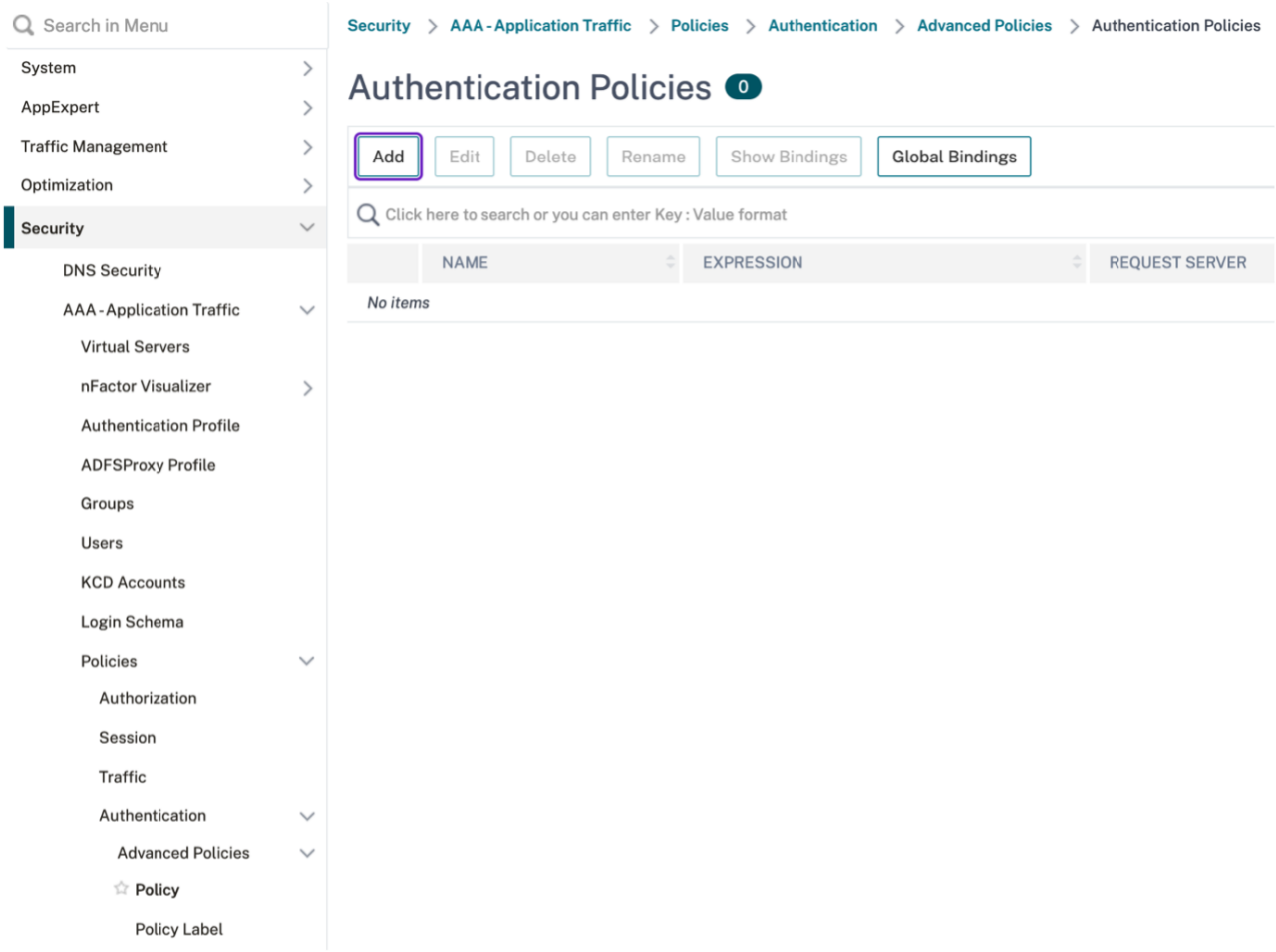


5. Populate details of your LDAP target
   Like RADIUS, Citrix recommends that you use a local Load Balancing (LB) vServer as the destination. As such, you should use the VIP of your LDAP LB vServer as the Server IP on this page.

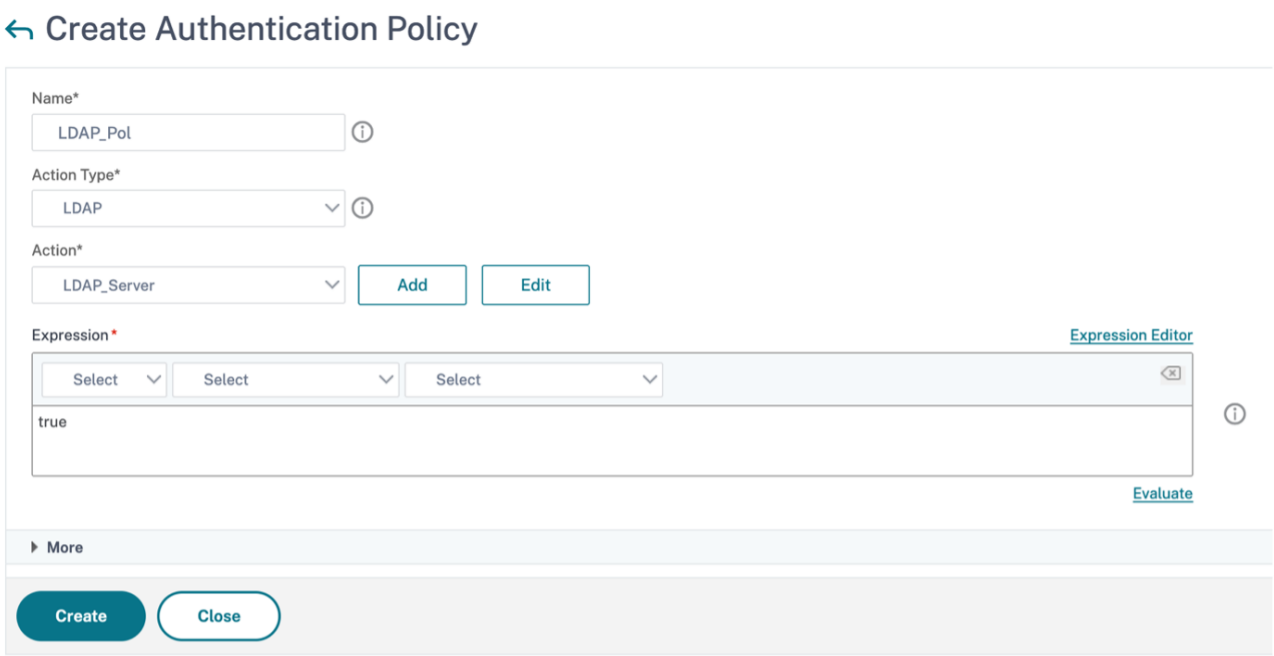


Add Advanced Authentication Policies

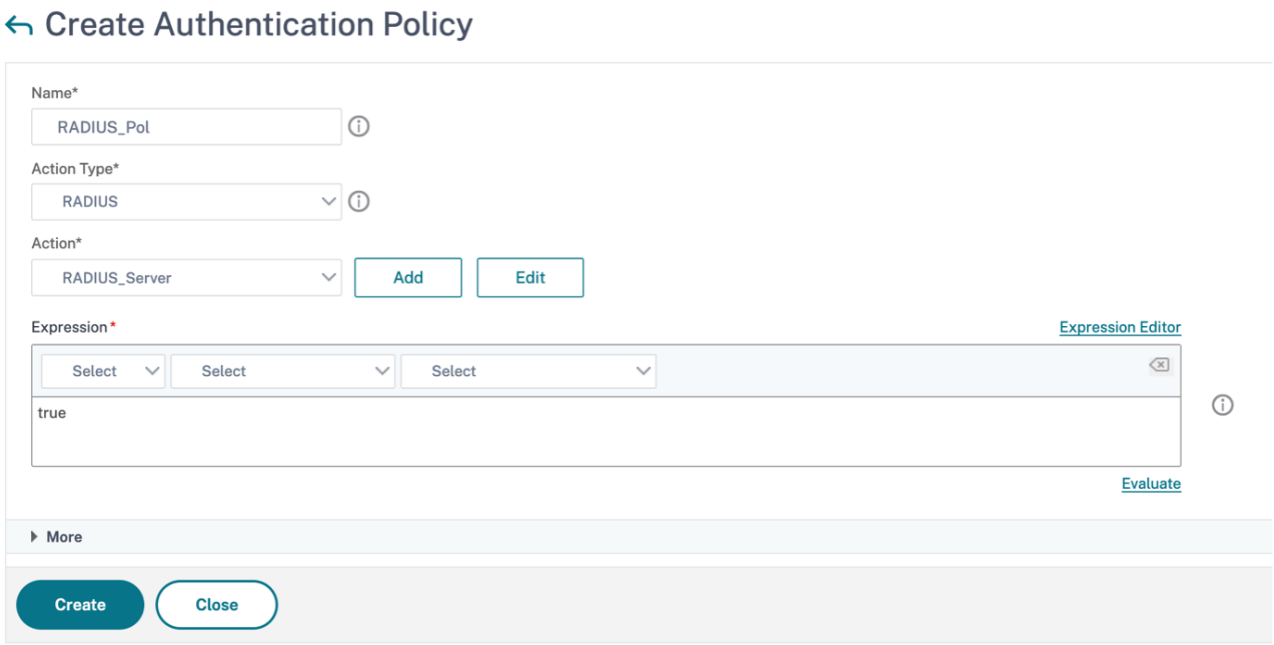
1. Select, **Security > AAA – Application Traffic, Policies, Authentication, Advanced Policies, Policy**. Then, click "**Add**".



2. Populate the policy details as shown and then click "**Create**".

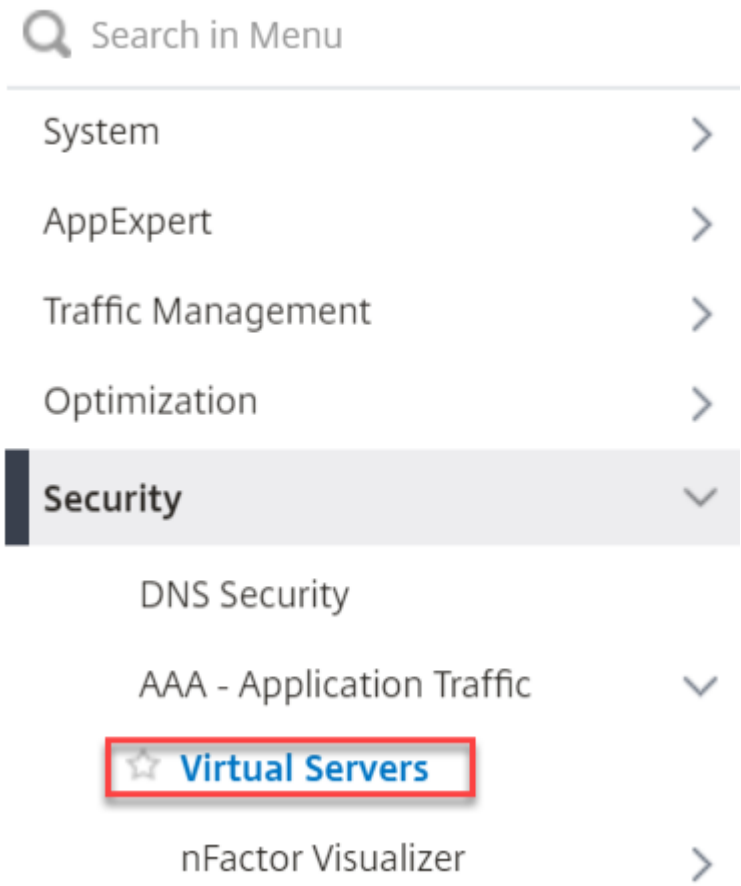


3. Repeat the step above to create another policy for RADIUS and then click "**Create**".

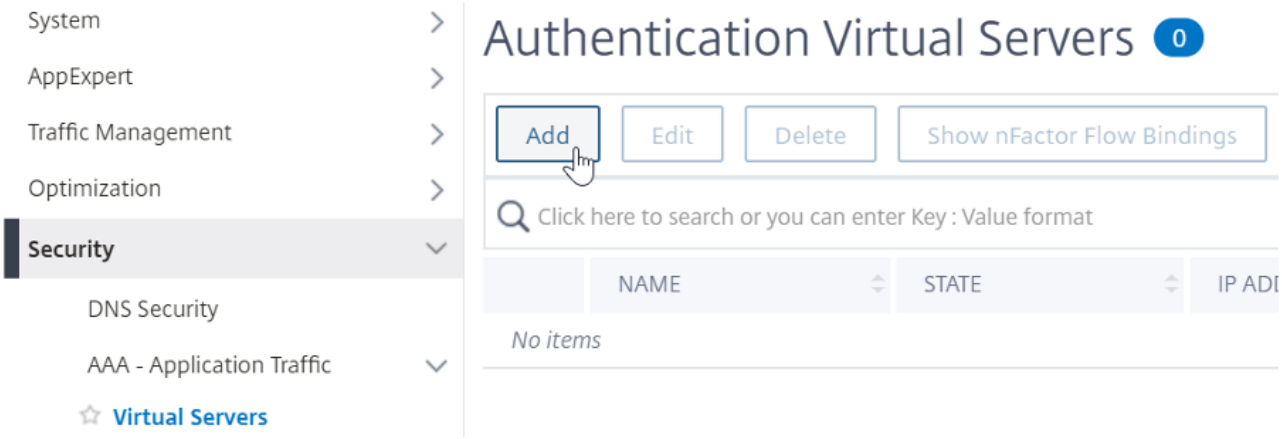


Create a AAA vServer

1. Navigate to **Configuration > Security > AAA - Application Traffic > Virtual Servers**.

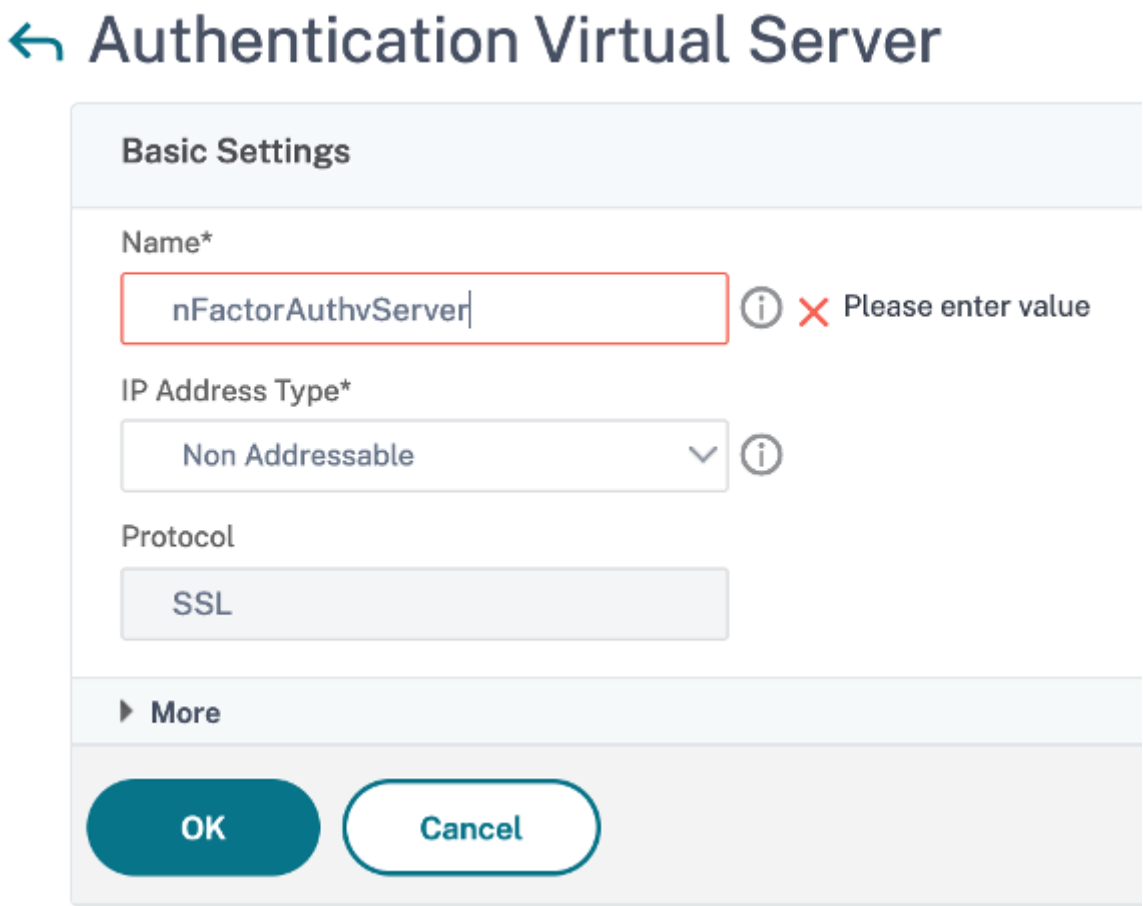


2. Click "**Add**" to create an authentication virtual server.

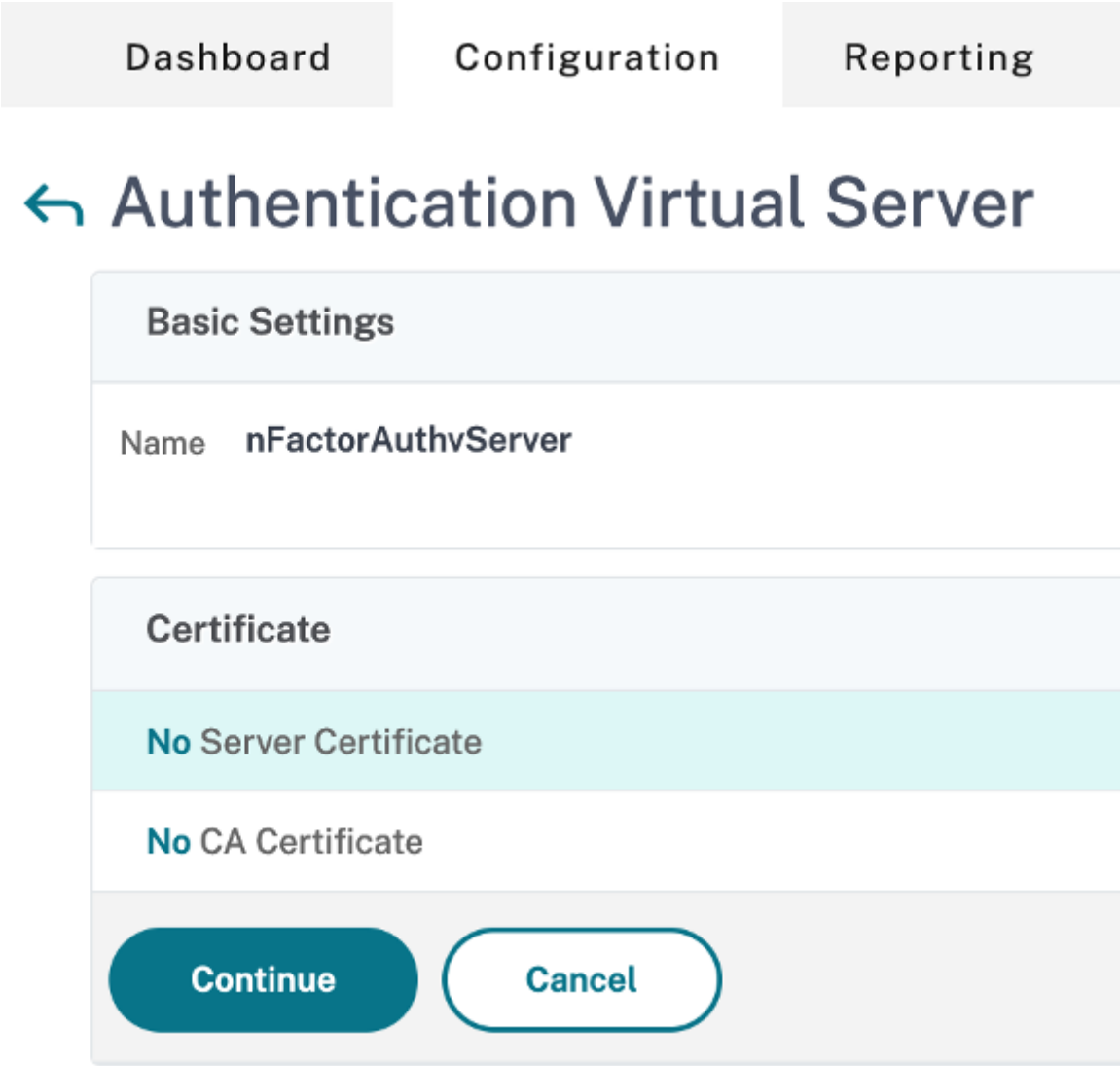


3. Enter the following information and click OK.

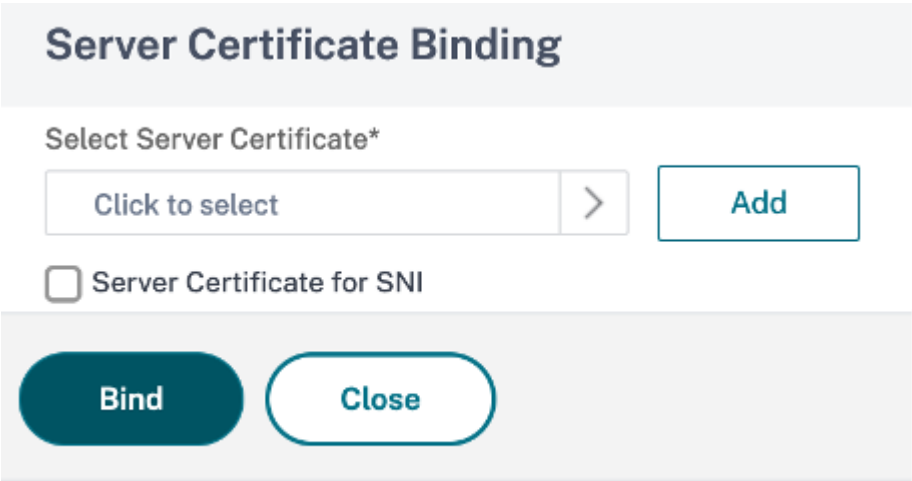
   - Name - Name for the AAA virtual server.
   - IP address Type - Change the IP address Type to Non Addressable as this virtual server is used only for Citrix Gateway.



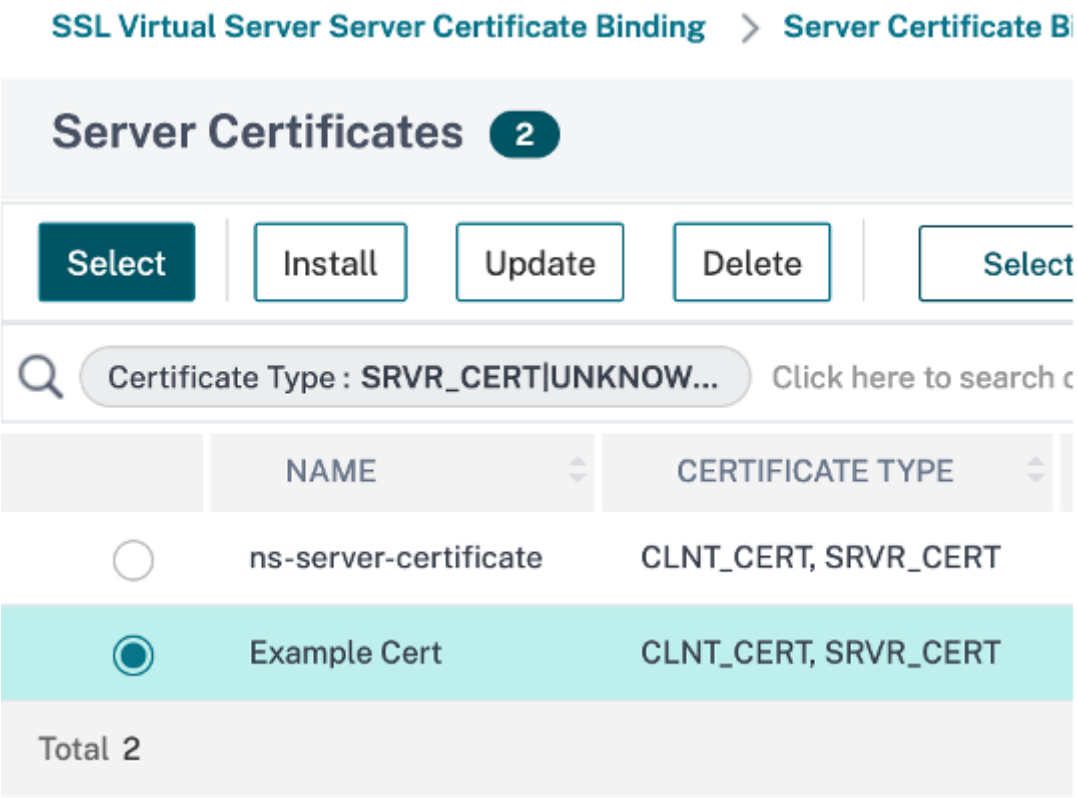
4. Under Certificate, select "No Server Certificate".



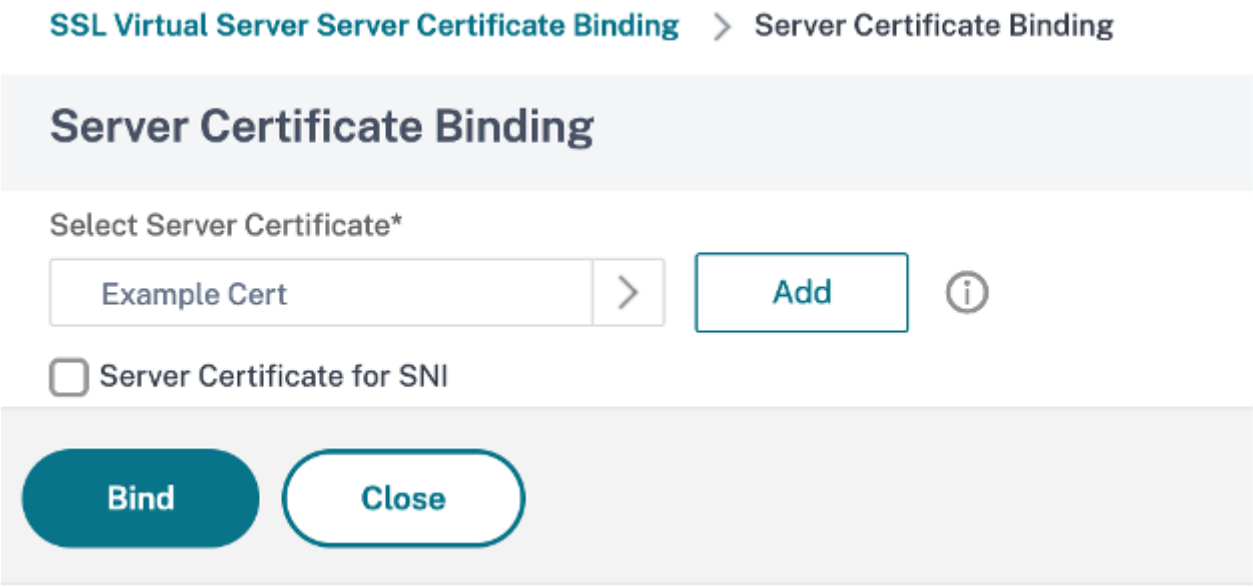
5. Click "**Click to select**" to select the server certificate



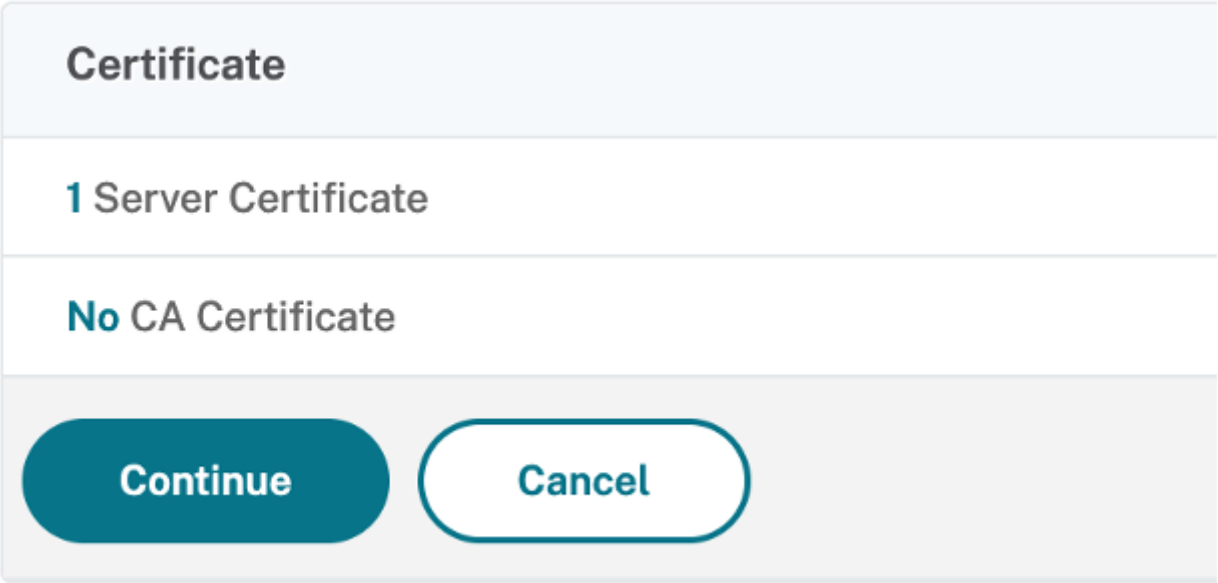
6. Click the radio button next to a certificate for the AAA Virtual Server, and then click "**Select**". The chosen certificate doesn't matter because this server is not directly accessible.


SSL Virtual Server Server Certificate Binding
Server Certificate B
Server Certificates 2
Select
Install
Update
Delete
Select
Certificate Type : SRVR_CERT|UNKNOW...
Click here to search c
NAME
CERTIFICATE TYPE
ns-server-certificate
CLNT_CERT, SRVR_CERT
Example Cert
CLNT_CERT, SRVR_CERT
Total 2

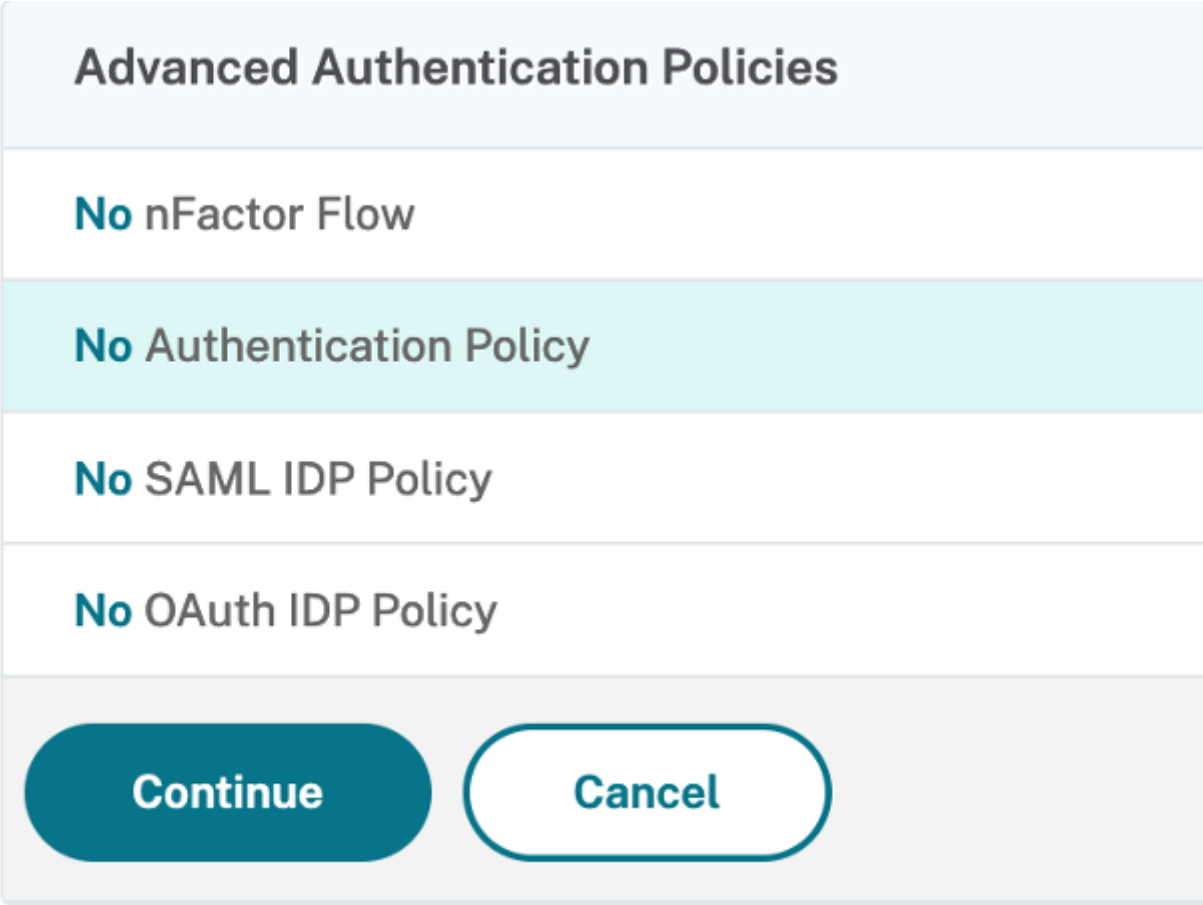
7. Click "**Bind**".


SSL Virtual Server Server Certificate Binding
Server Certificate Binding
Server Certificate Binding
Select Server Certificate*
Example Cert
Add
Server Certificate for SNI
Bind
Close

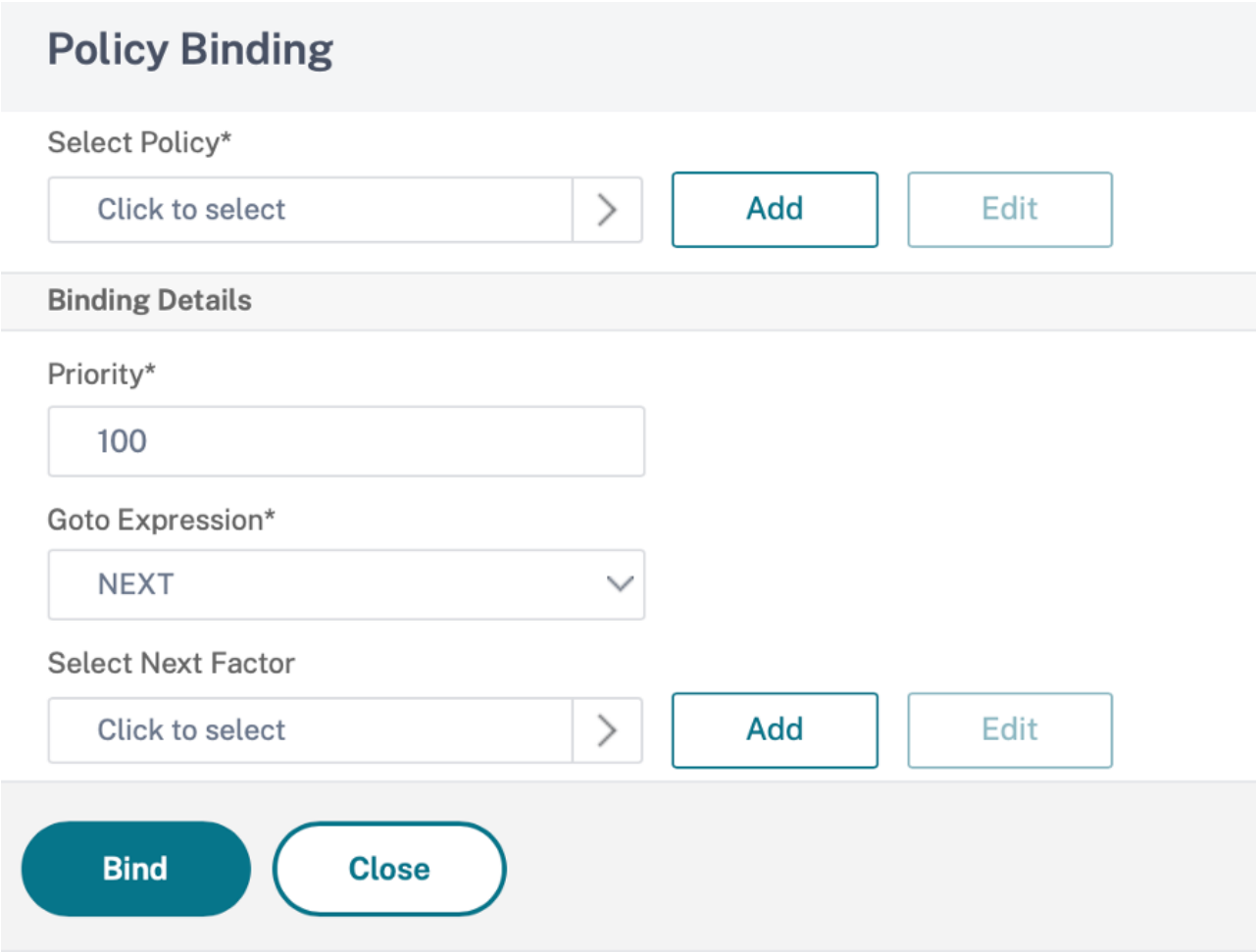
8. Click "**Continue**" to close the Certificate section.



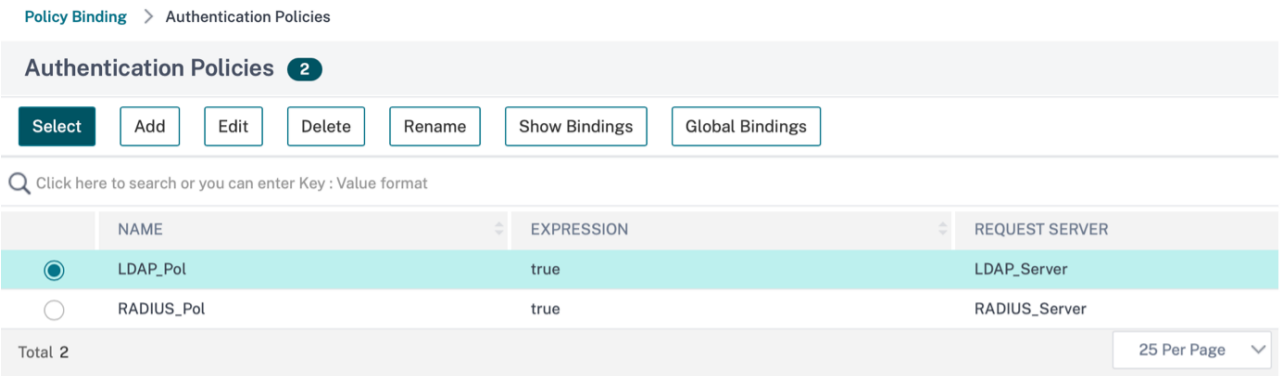
9. Click "**No Authentication Policy**" within "**Advanced Authentication Policies**".



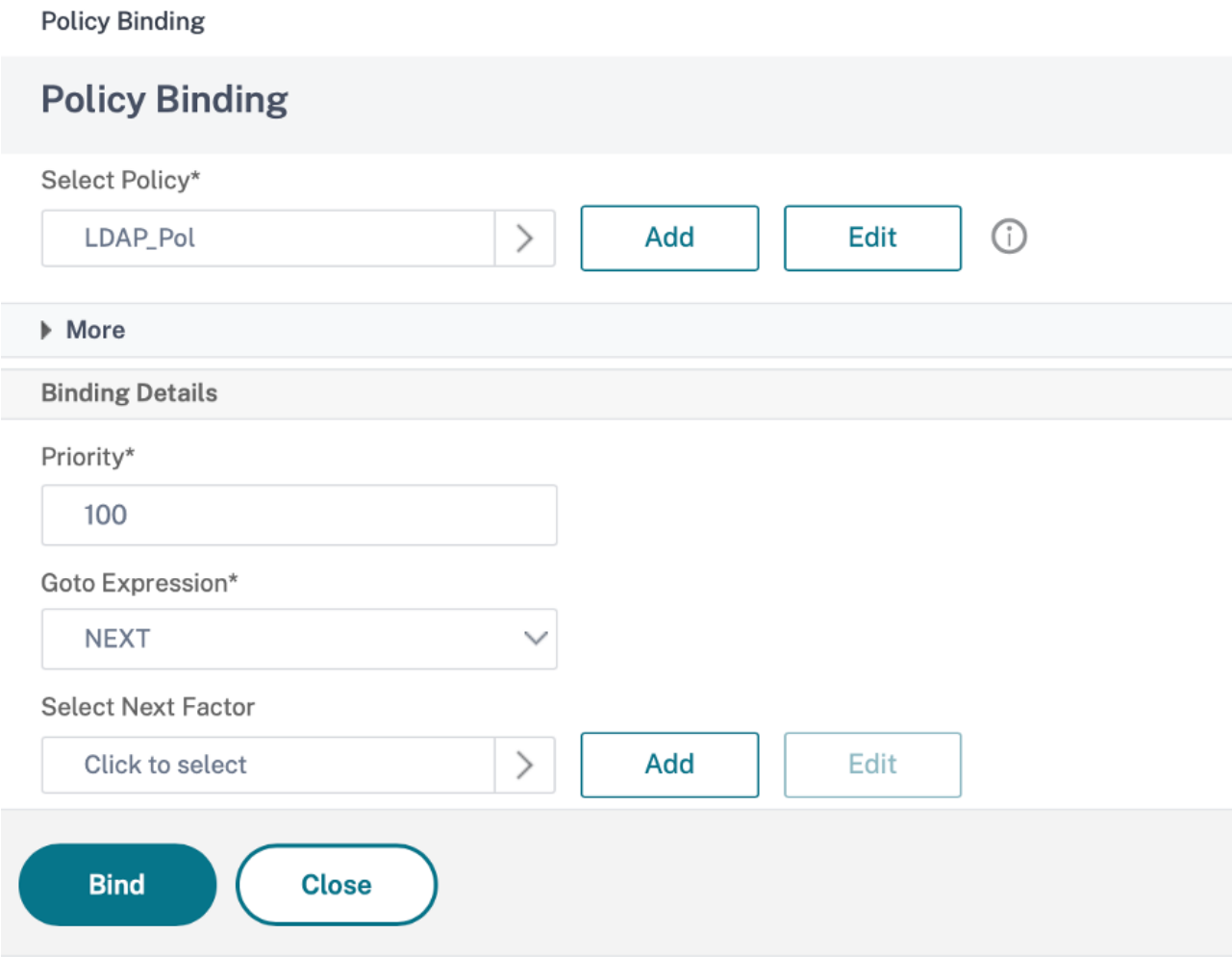
10. Click "**Click to select**" under the field for "**Select Policy**".



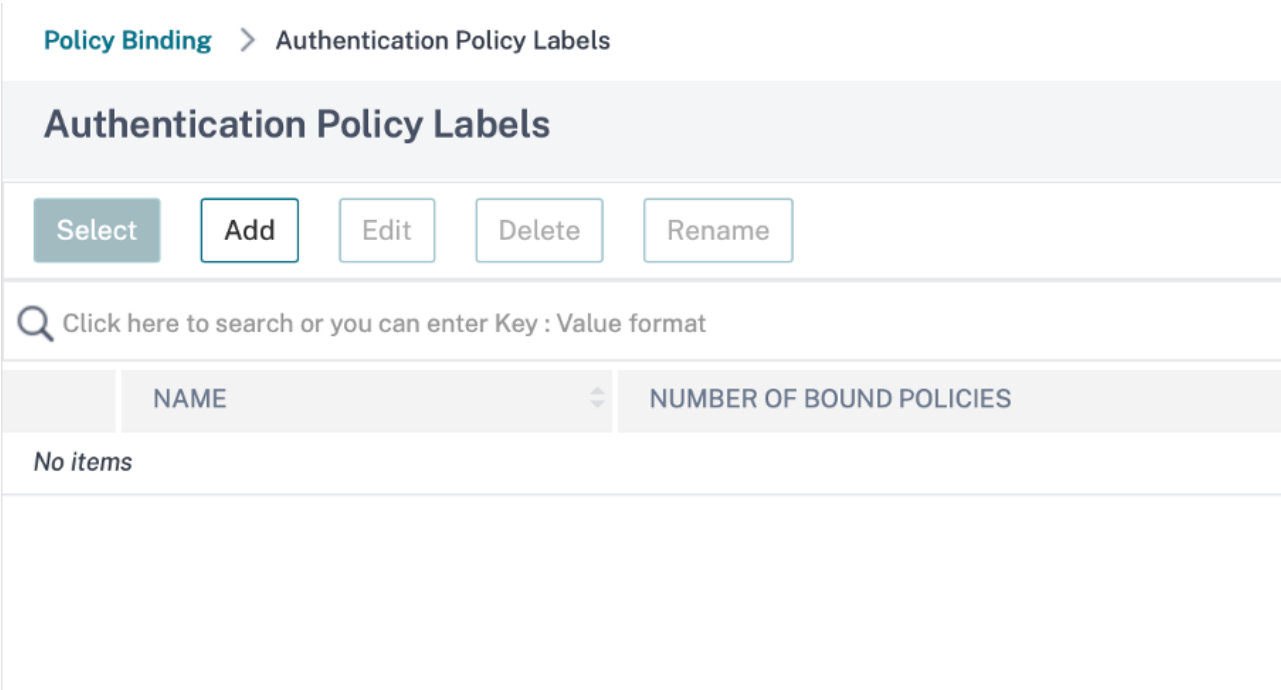
11. Select the "**LDAP_Pol**" policy and click "**Select**".



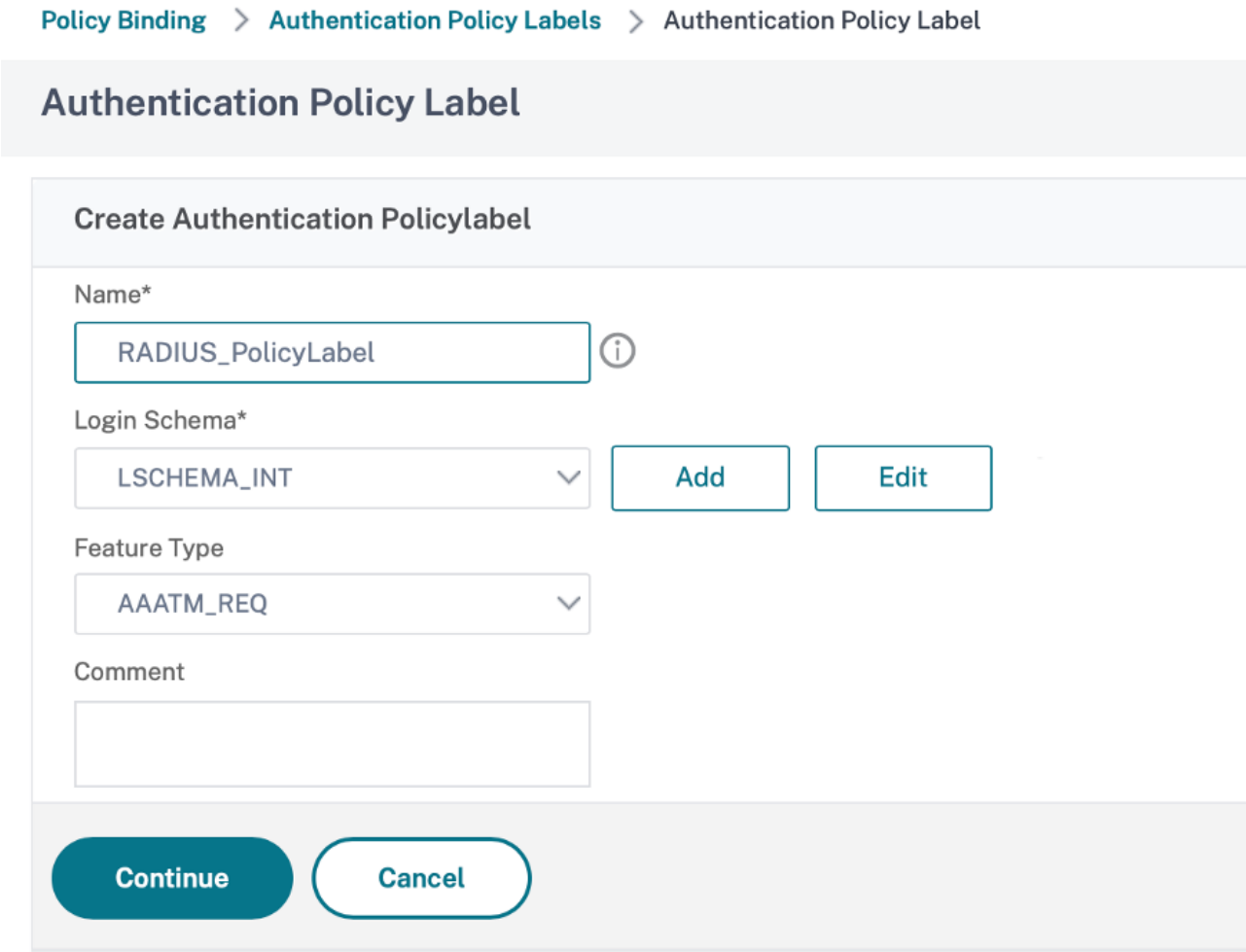
12. Click "**Click to select**" under the field for "**Select Next Factor**".



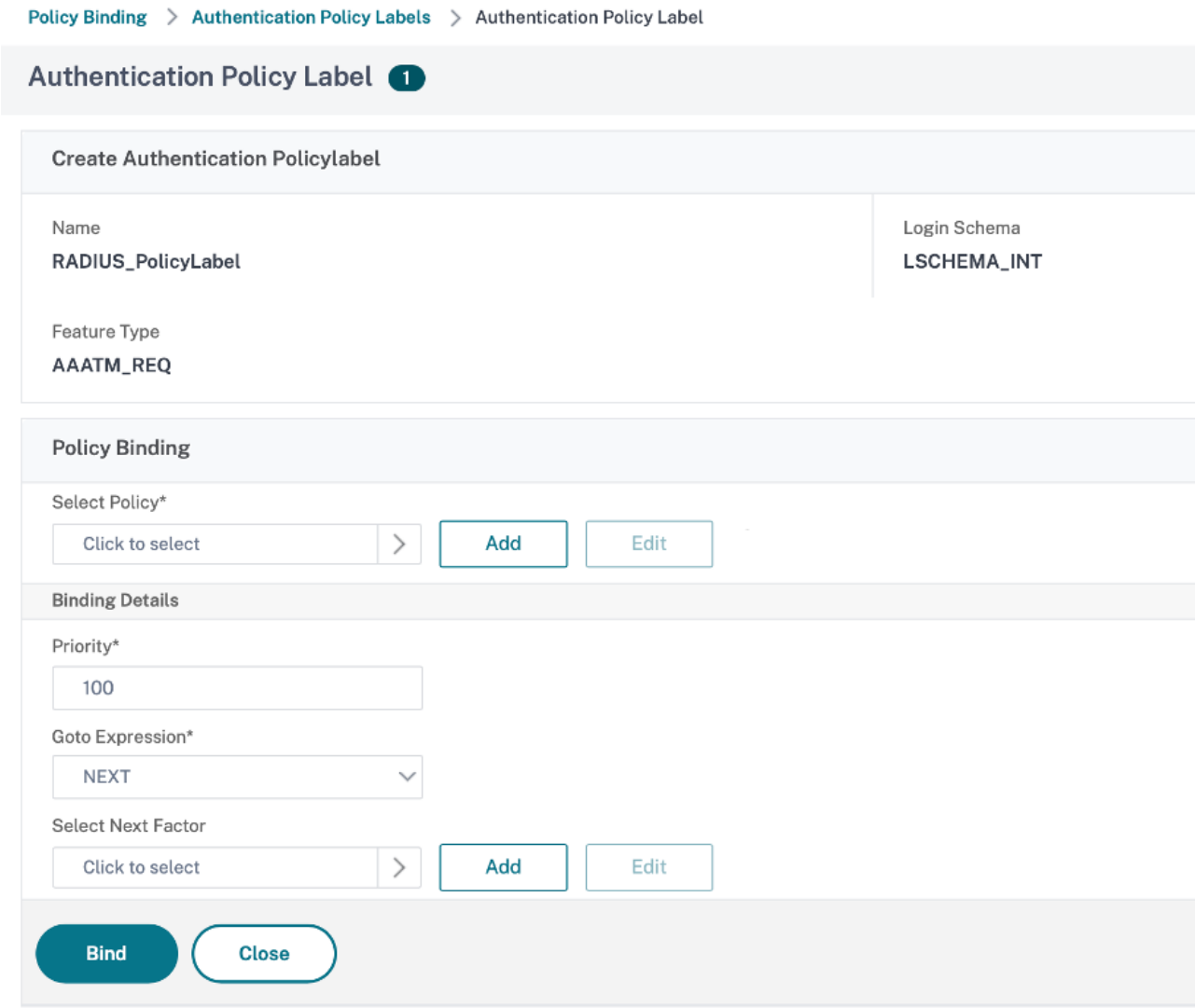
13. Click "**Add**" within "**Authentication Policy Labels**".



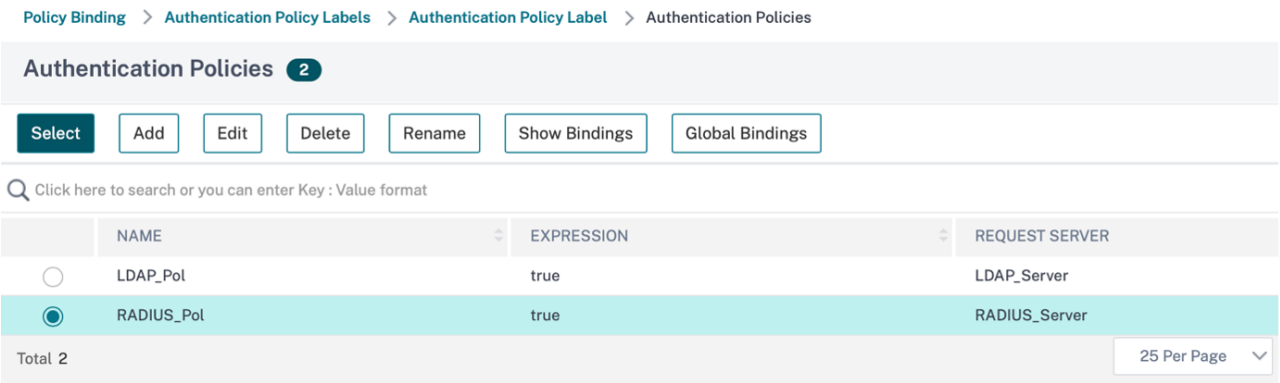
14. Enter a name for the Policy Label we will use to trigger RADIUS authentication and click "**Continue**".



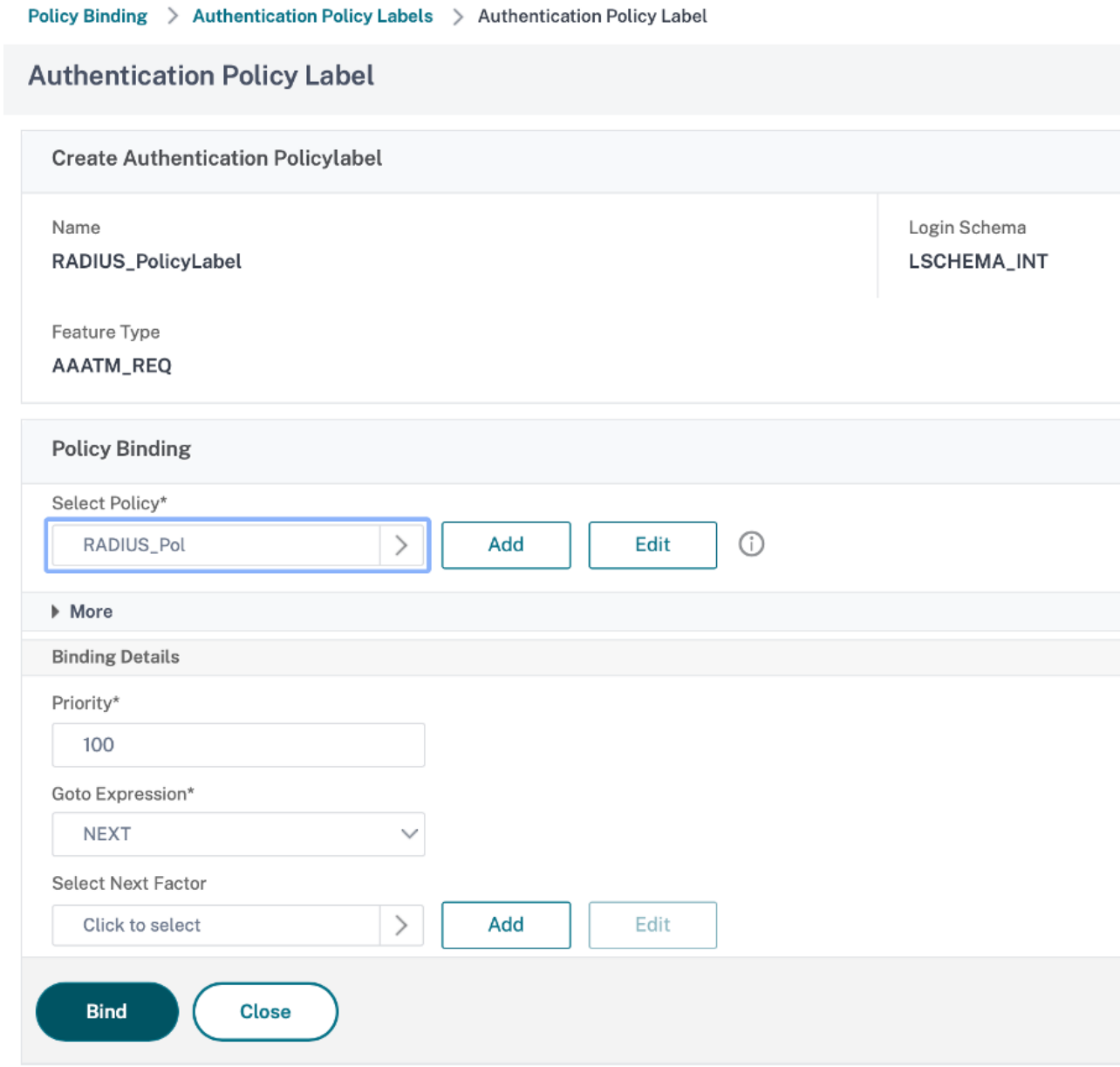
15. Click "**Click to select**" under the field for "**Select Policy**".



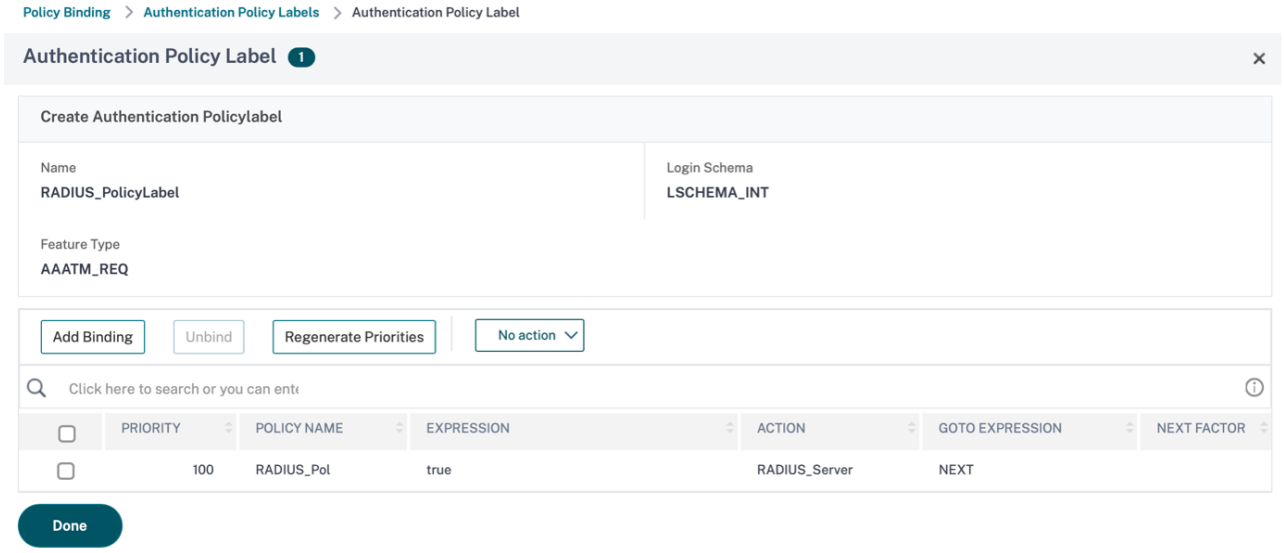
16. Select the "**RADIUS_Pol**" policy and click "**Select**".



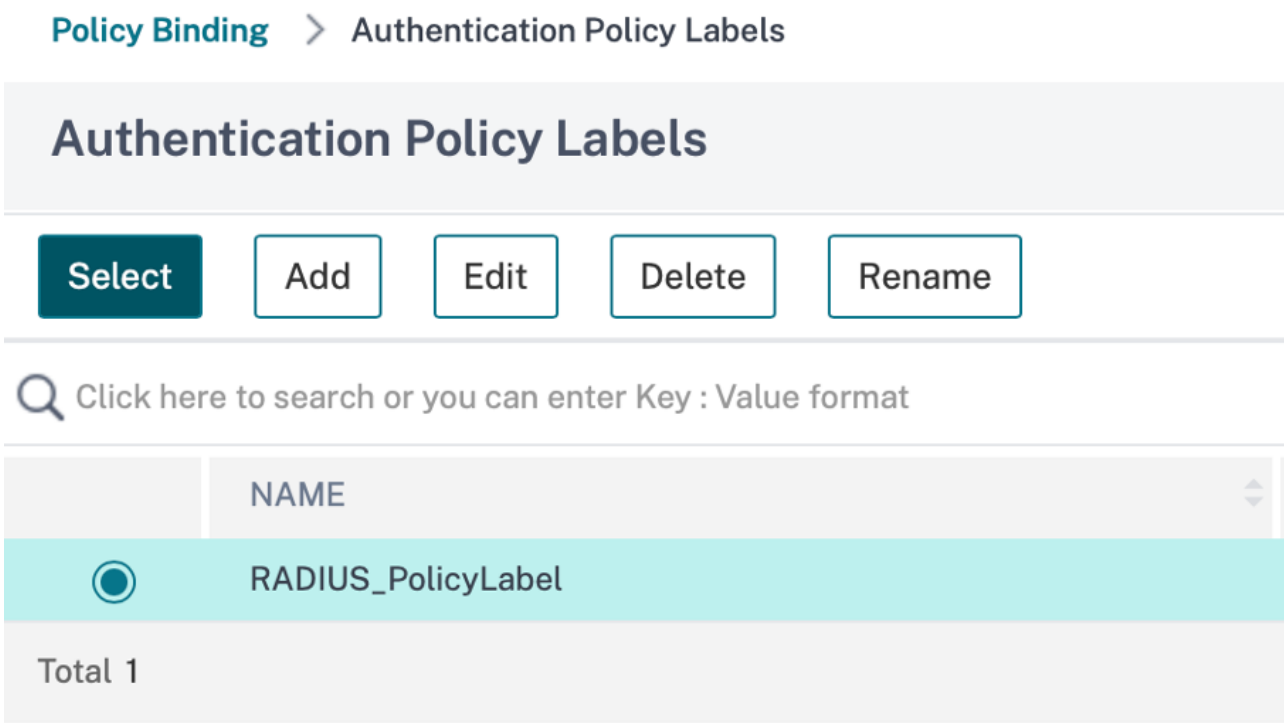
17. Click "**Bind**" at the bottom of the "**Create Authentication Policy Label**" screen.



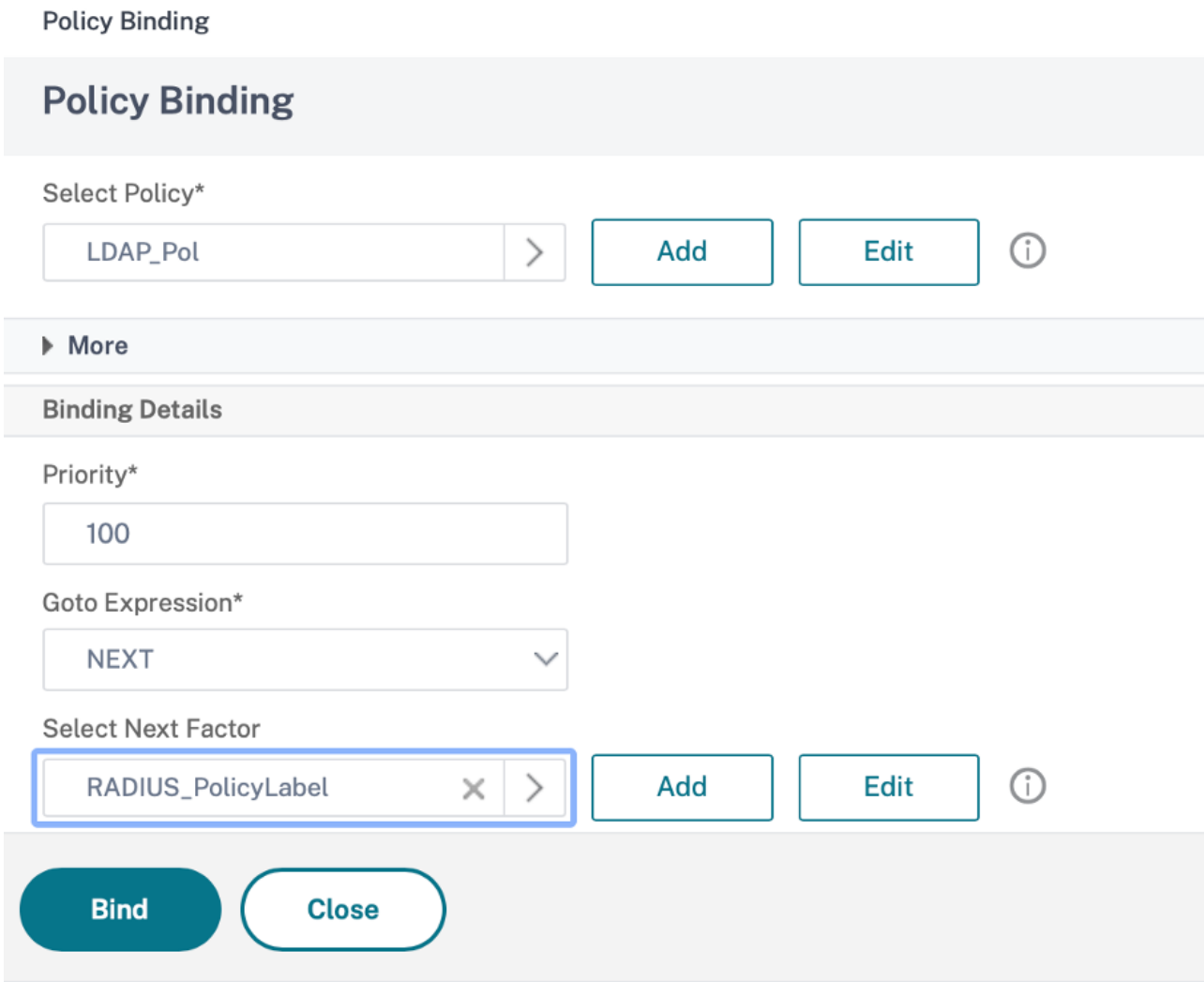
18. Click "**Done**" at the bottom of the "**Authentication Policy Label**" screen.



19. Click "**Select**".

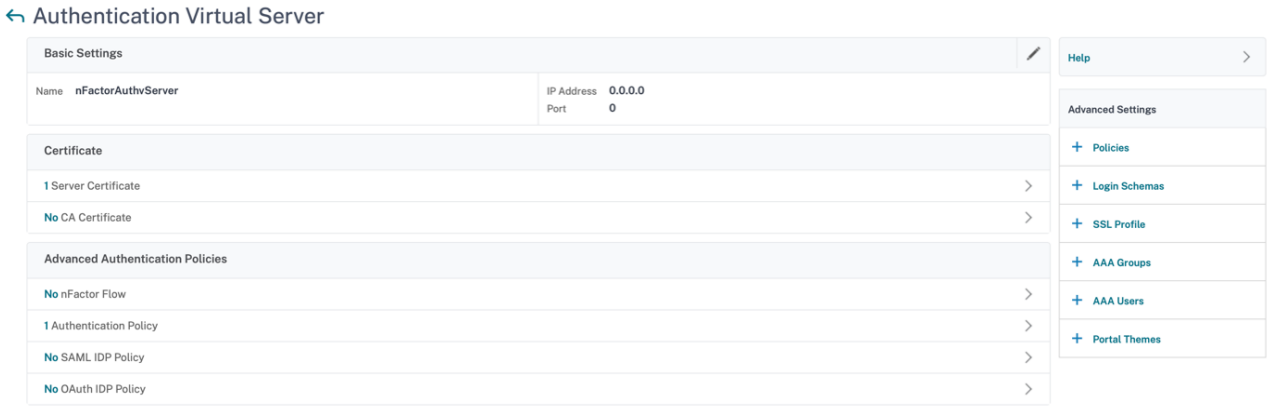


20. Click "**Bind**" at the bottom of the "**Policy Binding**" screen.

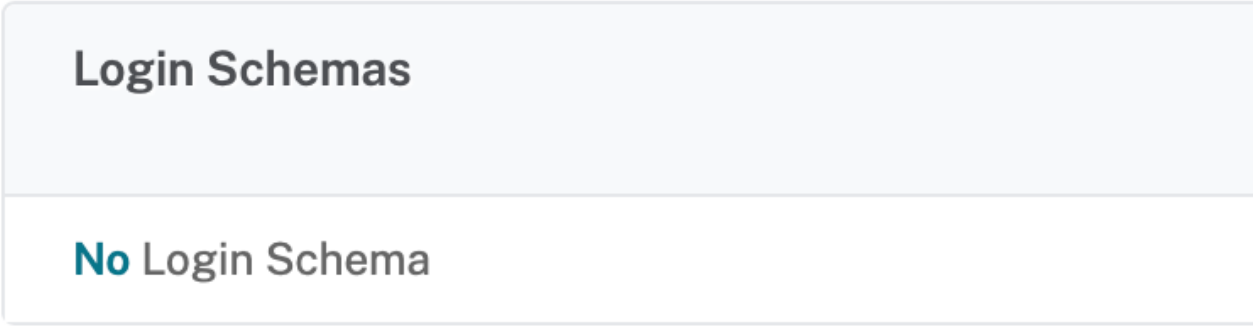


Apply a Login Schema that presents the user with a username, password, and passcode field

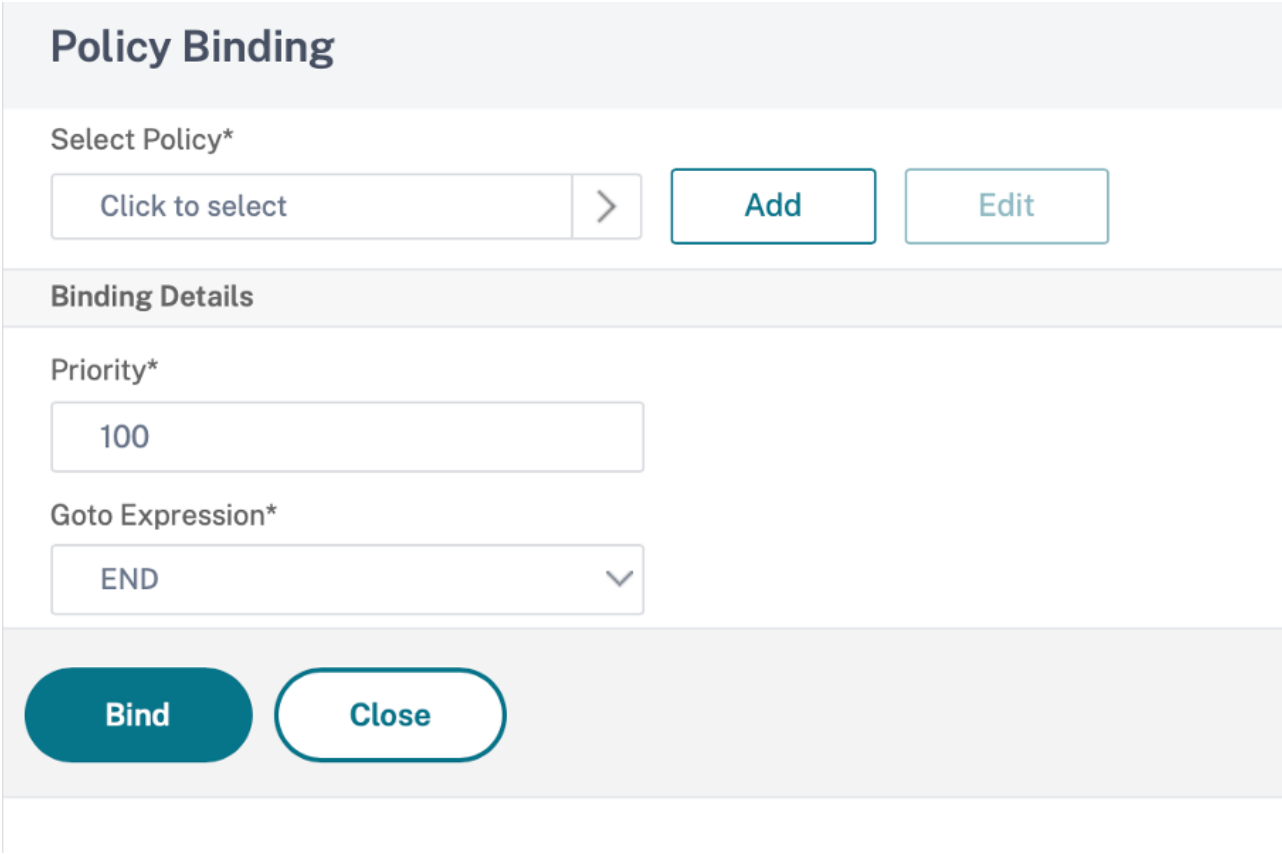
1. Click "**Login Schemas**" in the right-hand side "**Advanced Settings**" menu.



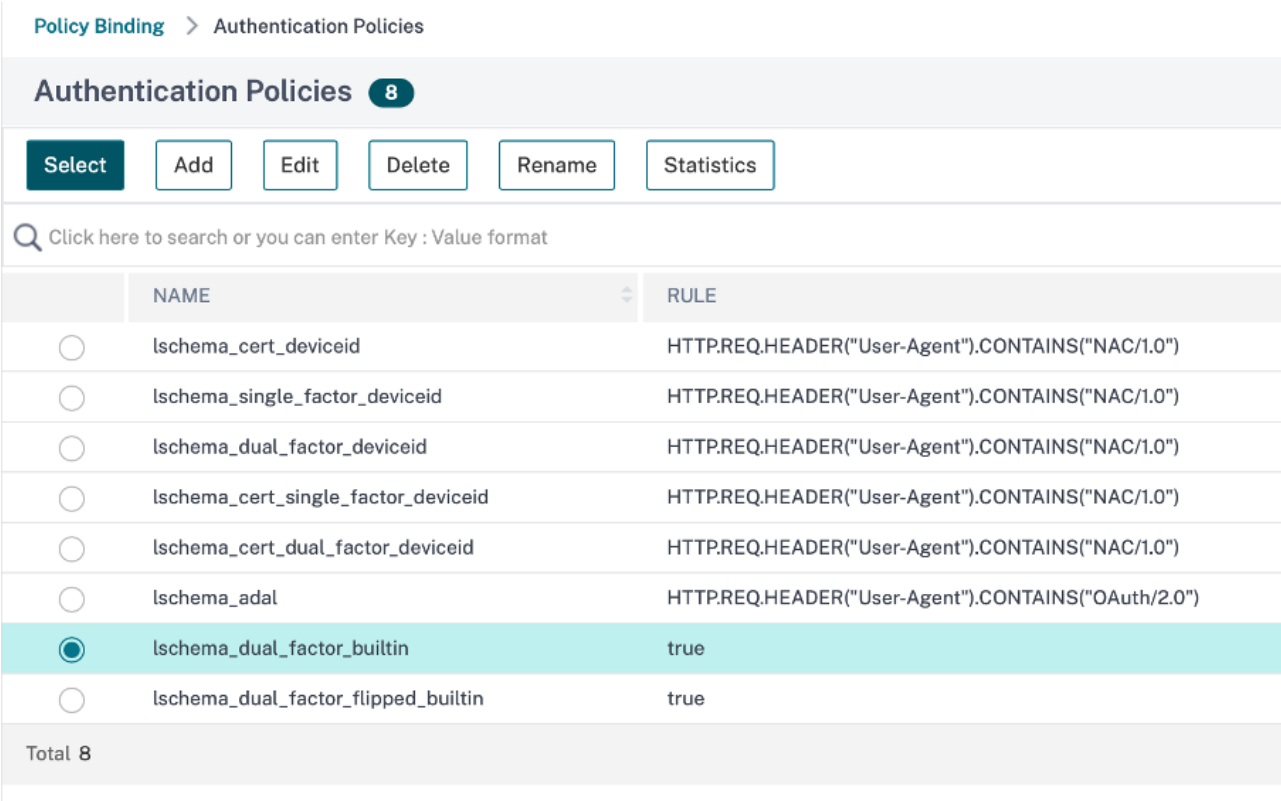
2. Click "**No Login Schema**" to present a window to select the schema.



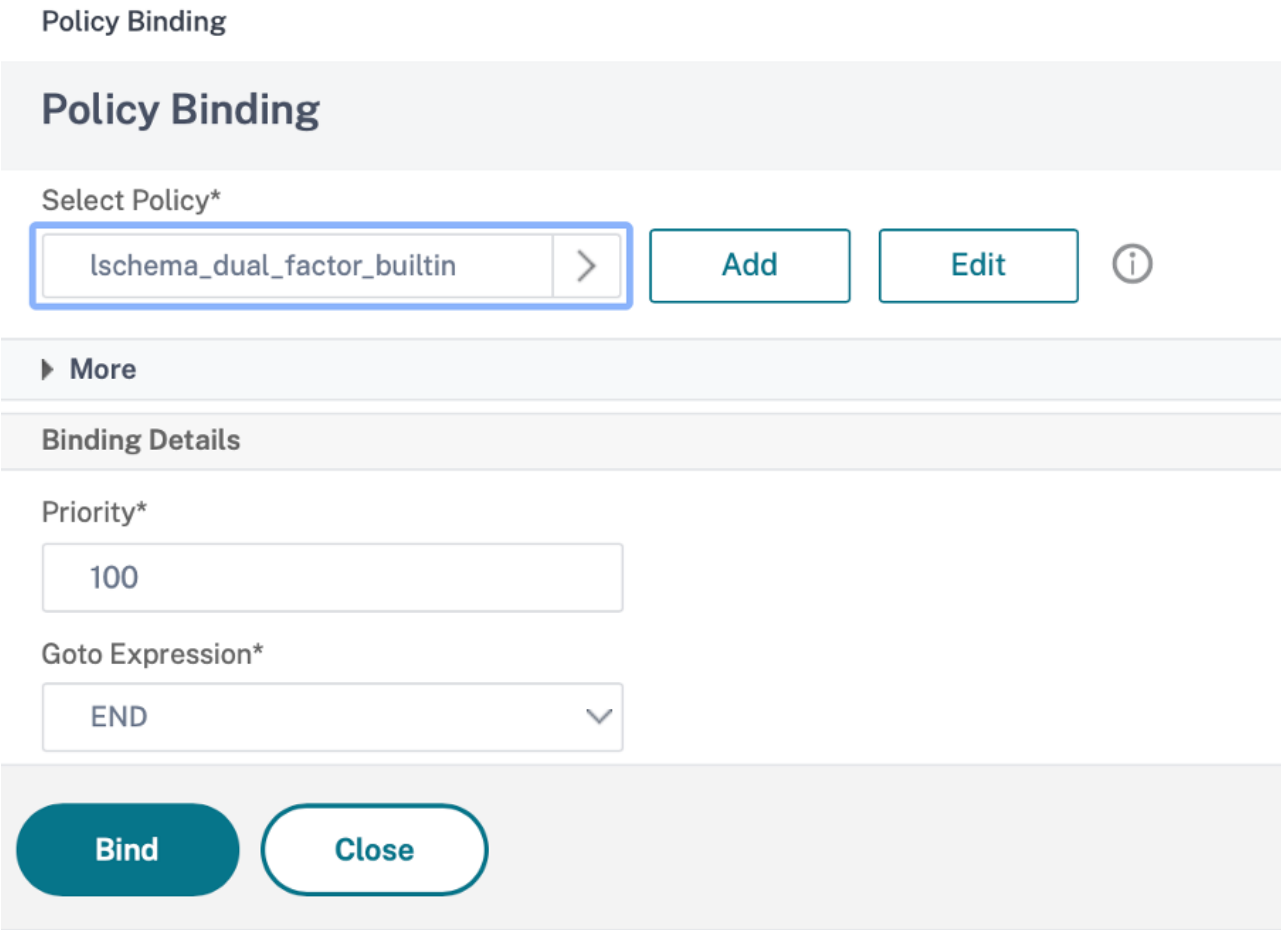
3. Click "**Click to Select**" under "**Select Policy**".



4. Select the built-in "**lschema_dual_factor_builtin**" policy and click "**Select**".



5. Click "**Bind**" and select "**Done**" to exit the AAA vServer configuration menu.

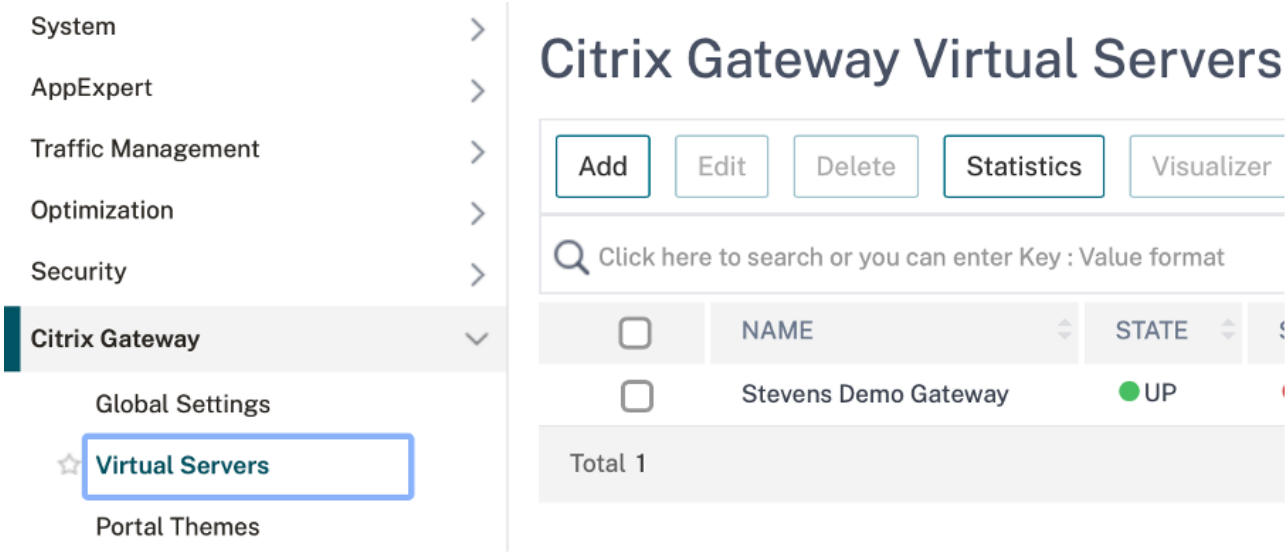


> **Note:** The "lschema_dual_factor_builtin" policy was added in ADC 13.0 firmware. If you are using an earlier release then you will need to create a policy. You can find instructions explaining how to create

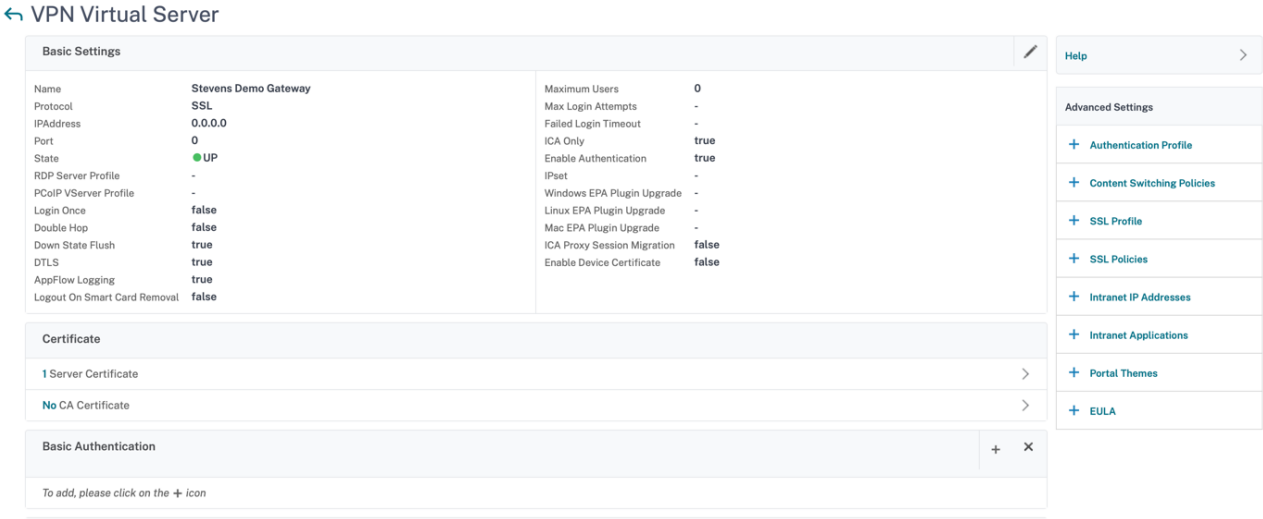
> a policy here.

Configure your Gateway vServer to use the new AAA server

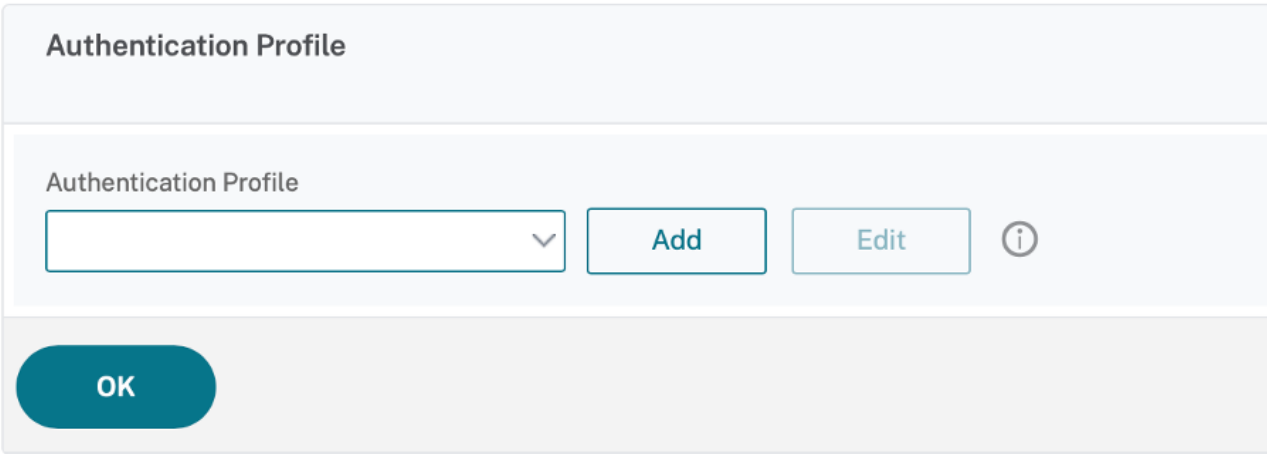
1. Select "**Citrix Gateway, Virtual Servers**", then select your Gateway vServer and click "**Edit**".



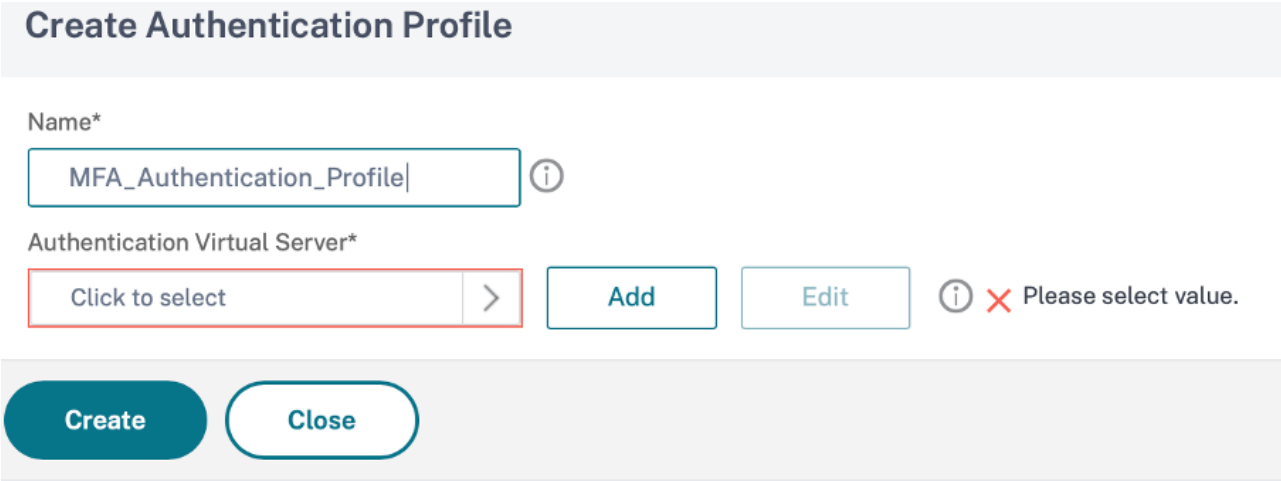
2. Select "**Authentication Profile**" in the right-hand side "**Advanced Settings**" menu.



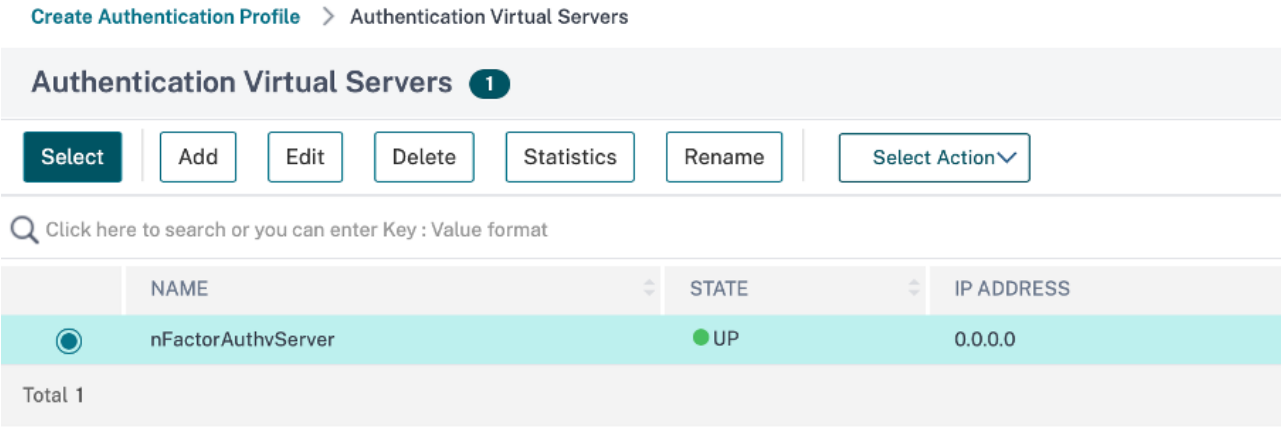
3. Select "**Add**" within the "**Authentication Profile**" section.



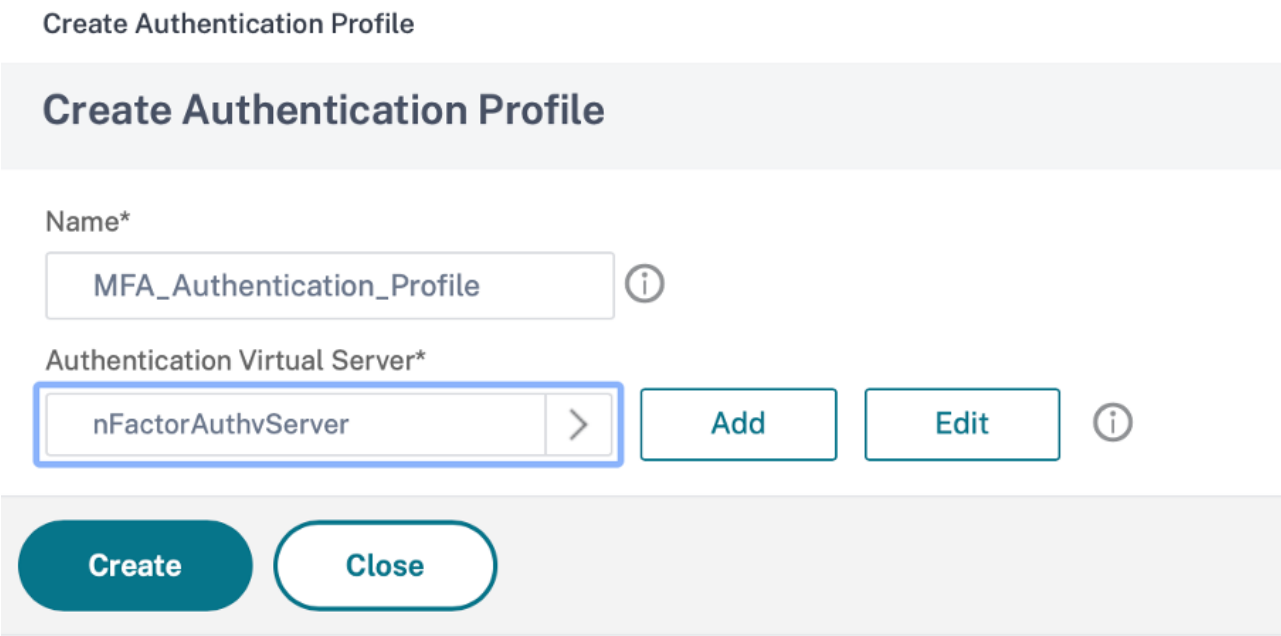
4. Enter a name for the new authentication profile as show and then click "**Click to select**" under "**Authentication Virtual Server**".



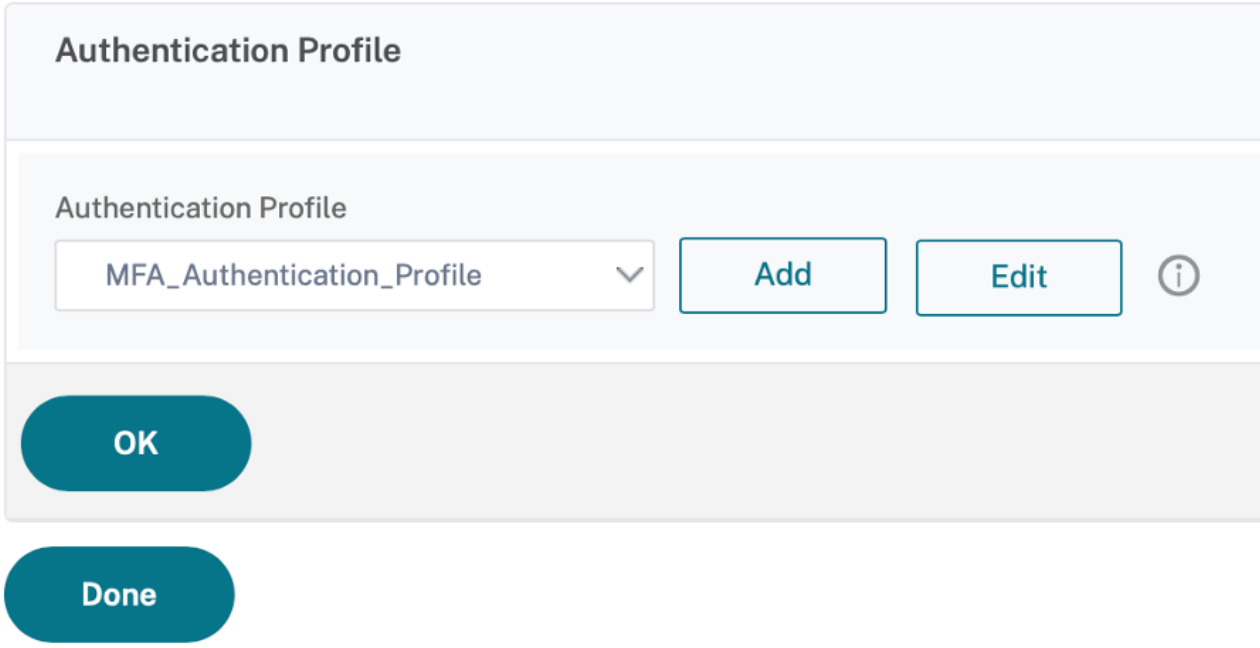
5. Select the AAA vServer that we created earlier and click "**Select**".



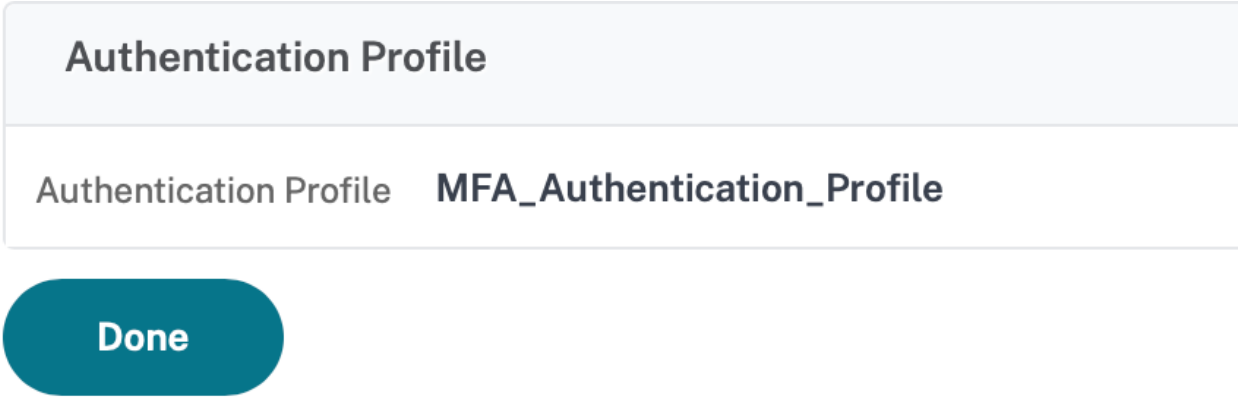
6. Click "**Create**".



7. Click "**OK**".

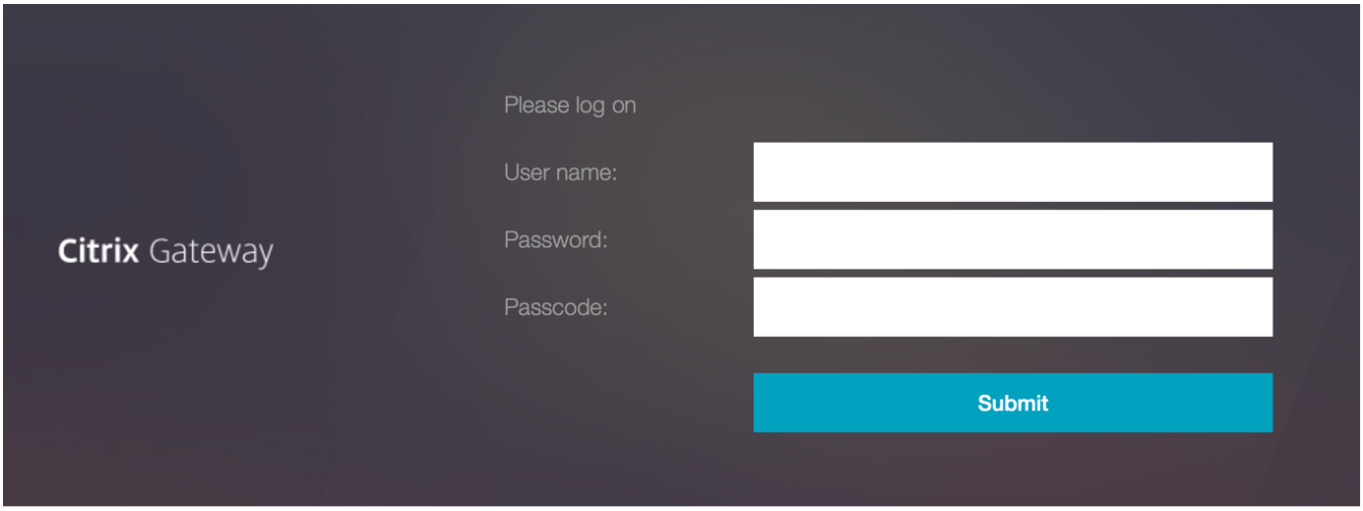


8. Click "**Done**".



Perform testing

You are now ready to use Multi-Factor Authentication on your Citrix Gateway vServer.



Should you encounter any authentication challenges, please refer to the troubleshooting section of this document.

CLI Instructions

If you prefer to configure the ADC using the CLI, the following configuration script will complete all necessary steps.

```
# 1. Enable AAA
en ns feature aaa

# 2. Creating LDAP Server
add authentication ldapAction LDAP_Gateway -serverIP LDAP_LB_IP -
serverPort 636 -ldapBase "DC=citrix,DC=lab" -ldapBindDn
readonly@citrix.lab -ldapBindDnPassword -ldapLoginName sAMAccountName -
groupAttrName memberOf

# 3. Creating LDAP Policy
add authentication Policy pol_LDAP_Gateway -rule true -action LDAP_Gateway

# 4. Creating RADIUS Server
add authentication radiusAction RADIUS_Server -serverIP 192.168.1.100 -
serverPort 1812 -radKey sharedsecret

# 5. Create RADIUS Policy
add authentication Policy RADIUS_Pol -rule true -action RADIUS_Server

# 6. Create a PolicyLabel triggering the RADIUS Policy
add authentication policylabel RADIUS_PolicyLabel -loginSchema LSCHEMA_INT

# 7. Create the AAA virtual server
add authentication vserver nFactorAuthvServer SSL 0.0.0.0

# 8. Bind an SSL certificate to the AAA virtual server
bind ssl vserver nFactorAuthvServer -certkeyName "Example Cert"

# 9. Bind the LDAP policy and RADIUS PolicyLabel to the AAA virtual server
bind authentication vserver nFactorAuthvServer1 -policy LDAP_Pol -priority
100 -nextFactor RADIUS_PolicyLabel -gotoPriorityExpression NEXT

# 10. Bind the builtin Login Schema for dual factor authentication to the
AAA virtual server
bind authentication vserver nFactorAuthvServer -policy
lschema_dual_factor_builtin -priority 100 -gotoPriorityExpression END

# 11. Create an Authentication Profile attached to the AAA virtual server
add authentication authnProfile MFA_Authentication_Profile -authnVsName
nFactorAuthvServer

# 12. Configure your existing Gateway virtual server to use the
Authentication Profile
set vpn vserver "Steven Demo Gateway" -authnprofile
"MFA_Authentication_Profile"
```