

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).

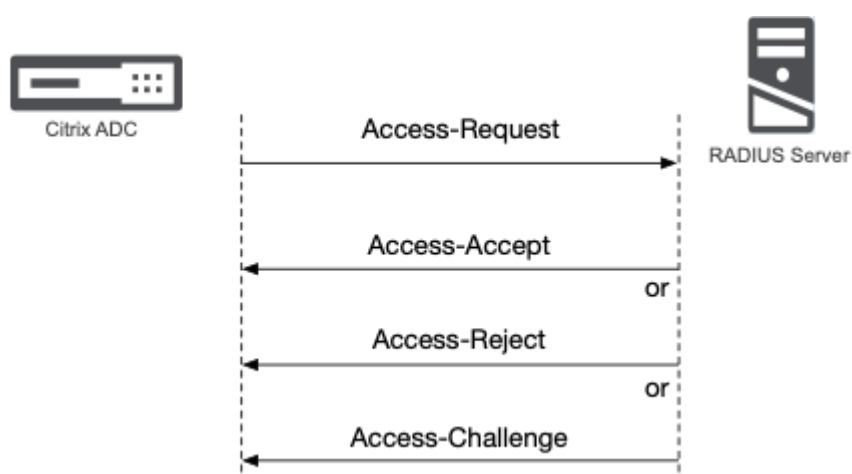
This article will cover how to configure Citrix ADC Gateway to use nFactor authentication for LDAP and RADIUS-based Multi-Factor Authentication and general troubleshooting techniques.

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

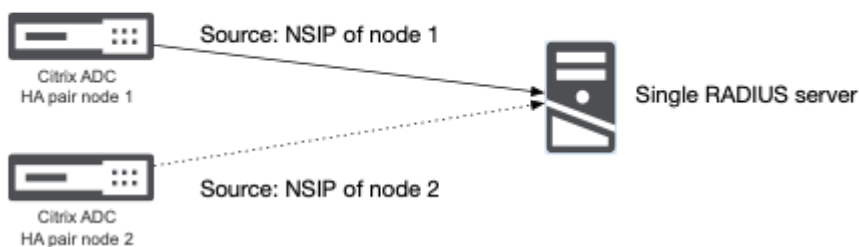
The RADIUS communication flow begins with an Access-Request packet from the client, in this case the Citrix ADC. The RADIUS server will then validate the client and authenticate the credentials received within the Access-Request. The server will then respond with an Access-Accept, Reject, or a Challenge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

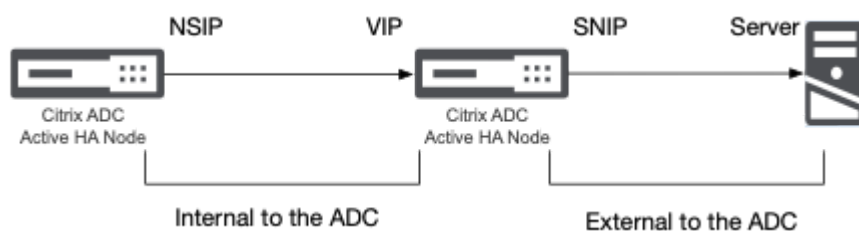
Default behaviour



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

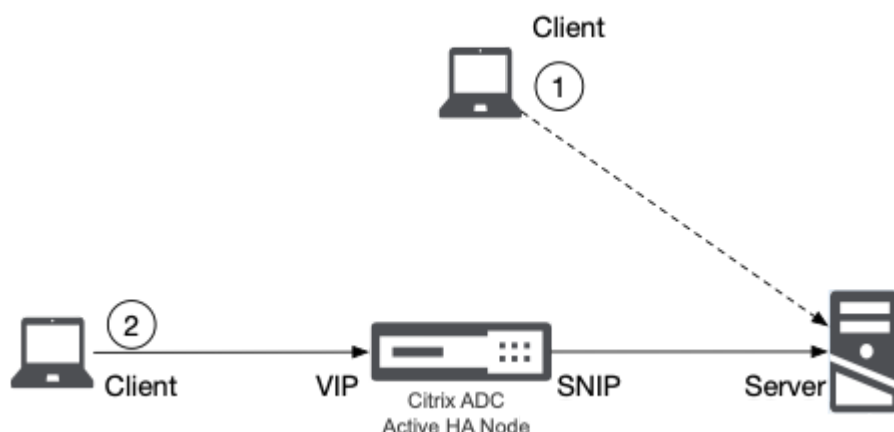
NTRadPing is a free third-party RADIUS test utility that allows you to manually generate RADIUS authentication requests and to observe the response. [You can download NTRadPing here:](#)

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

NTRadPing Test Utility

RADIUS Server/port: 1812

Reply timeout (sec.): 3 Retries: 6

RADIUS Secret key:

User-Name:

Password: ☐ CHAP

Request type: Authentication Request 0

Additional RADIUS Attributes:

NTRadPing 1.5 - RADIUS Server Testing Tool
 © 1999-2003 Master Soft SpA - Italy - All rights reserved
<http://www.dialways.com/>

MASTERSTOFT® **DIALWAYS**

RADIUS Server reply:

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.

NTRadPing Test Utility

RADIUS Server/port: 192.168.1.100 1812

Reply timeout (sec.): 3 Retries: 6

RADIUS Secret key: test-shared-secret

User-Name: steven

Password: CHAP ☐

Request type: Authentication Request 0

Additional RADIUS Attributes:

NTRadPing 1.5 - RADIUS Server Testing Tool
© 1999-2003 Master Soft SpA - Italy - All rights reserved
<http://www.dialways.com/>

ms MASTERSOFT® **DIALWAYS**

RADIUS Server reply:

Sending authentication request to server 192.168.1.100:1812
Transmitting packet, code=1 id=0 length=67
received response from the server in 16 milliseconds
reply packet code=2 id=0 length=102
response: Access-Accept
----- attribute dump -----
Reply-Message=Message accepted
Filter-Id=sms2
Framed-Protocol=PPP
Service-Type=Framed

Add Remove Clear list Load... Save... Send Help... Close

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.](#)

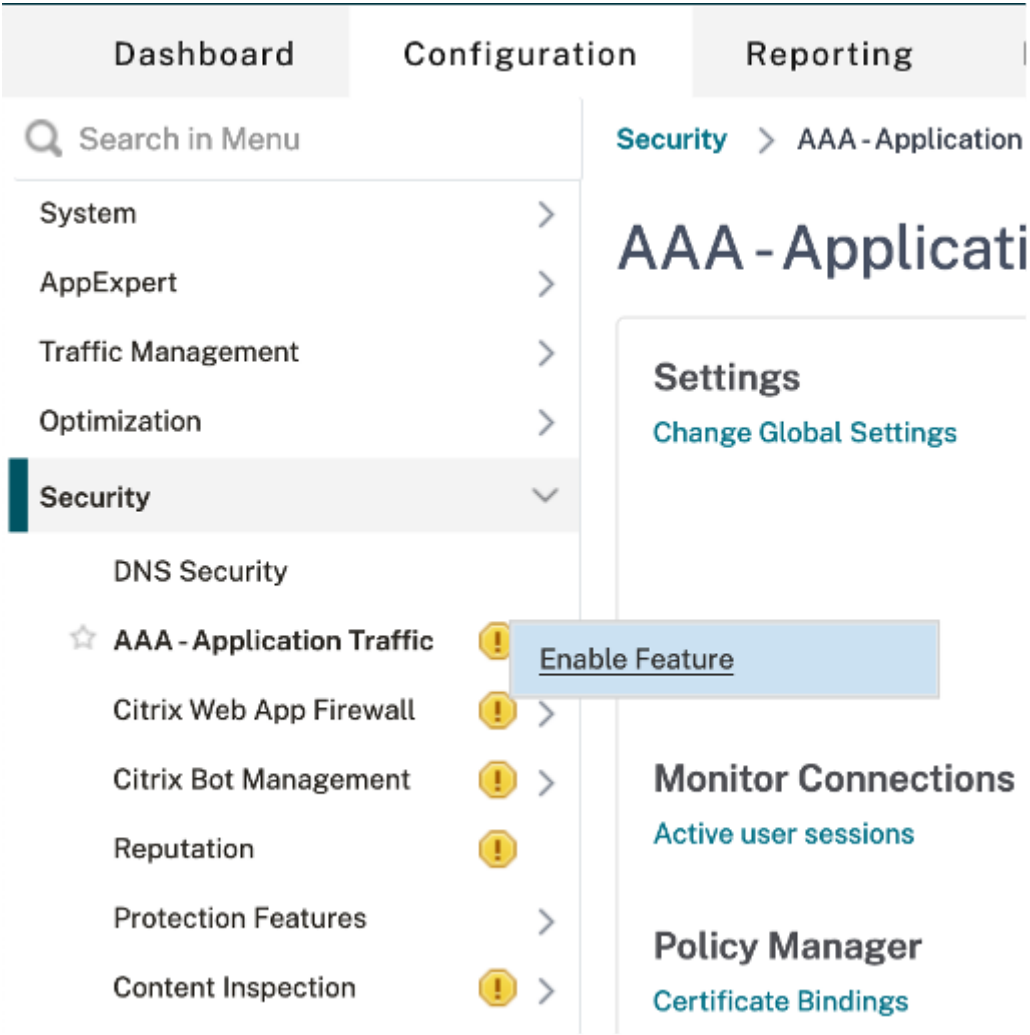
The RADIUS communication you observe within WireShark should consist of an Access-Request packet followed by a response of either Access-Accept, Access-Reject, or Access-Challenge. Missing responses often indicate a communication problem such as absent firewall rules or the RADIUS server not having a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

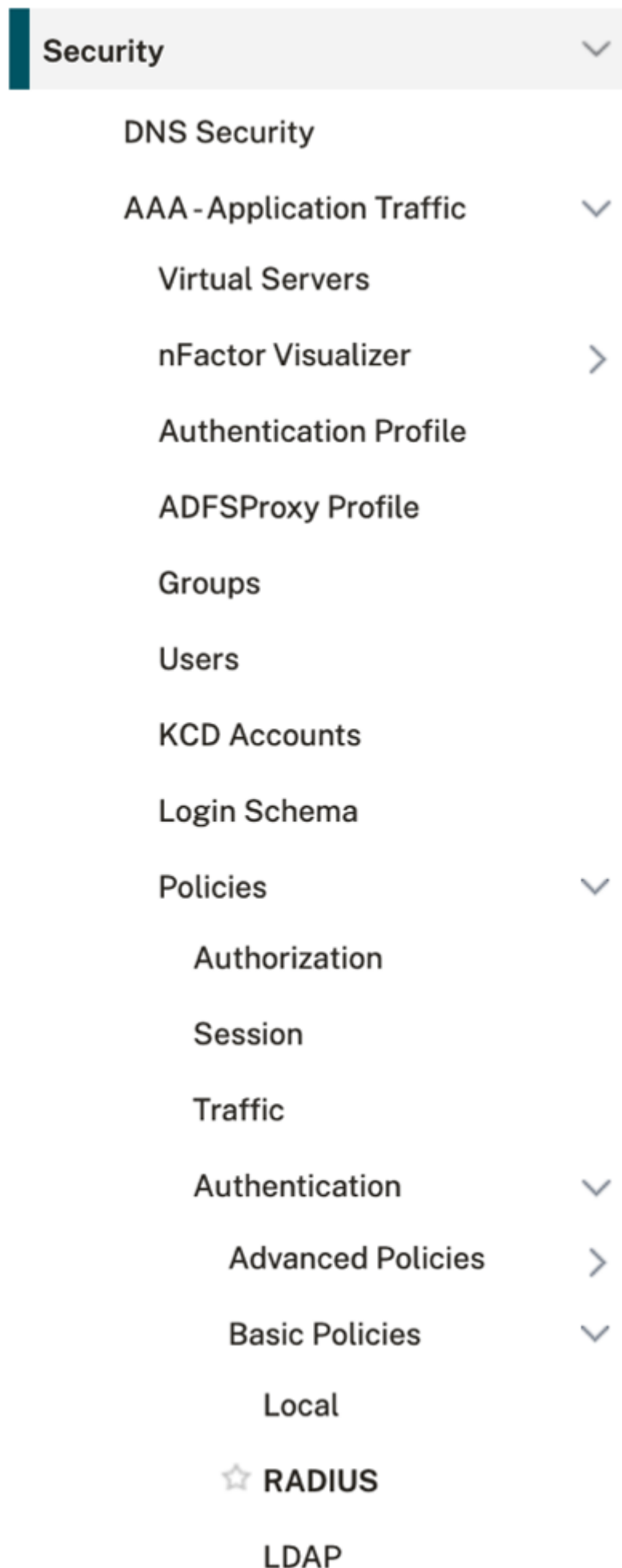
Enable the AAA feature

- 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".

Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > Servers

RADIUS

Policies 0

Servers 0

Add

Edit

Delete

Q

Click here to search or you can enter Key : Value format

	NAME	SERVER NAME	IP ADDRESS	PORT	TIME-
No items					

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.

Dashboard


Configuration

Reporting

Documentation

← Create Authentication RADIUS Server


Name*



☐ Server Name

☒ Server IP


IP Address*



Port

Secret Key*

Confirm Secret Key*



Test RADIUS Reachability

Test End User Connection

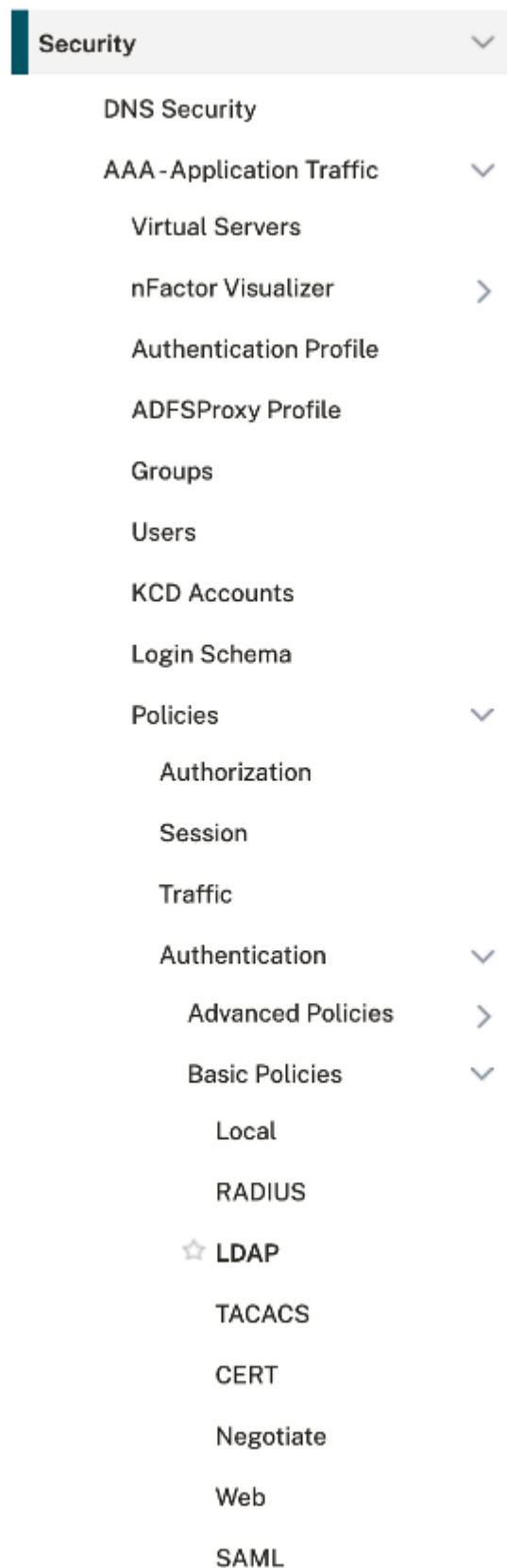
Time-out (seconds)

► More

Create

Close

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.

Dashboard
Configuration
Reporting
Documentation
Downloads

← Create Authentication LDAP Server

Name*
 ⓘ

☐ Server Name
☒ Server IP

IP Address*

Security Type

Port

Server Type

Time-out (seconds)

☒ Authentication

Ssh Public Key

Base DN (location of users)*

Administrator Bind DN*

Network connectivity test checks LDAP server reachability and if admin bind credential valid.
Administrator Password*

Confirm Administrator Password*

End-to-end login test performs LDAP/AD login from an end user's context and involves steps of a normal log in process.

Server Logon Name Attribute

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Email

Alternate Email

Cloud Attributes*

Default Authentication Group

☒ User Required

☐ Allow Password Change

☐ Referrals

Maximum Referral Level

Referral DNS Lookup

☐ Validate LDAP Server Certificate

LDAP Host Name

OTP Secret

Push Service

KB Attribute

More

Add Advanced Authentication Policies

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

Search in Menu

- System >
- AppExpert >
- Traffic Management >
- Optimization >
- Security** >
 - DNS Security
 - AAA - Application Traffic >
 - Virtual Servers
 - nFactor Visualizer >
 - Authentication Profile
 - ADFSProxy Profile
 - Groups
 - Users
 - KCD Accounts
 - Login Schema
 - Policies >
 - Authorization
 - Session
 - Traffic
 - Authentication >
 - Advanced Policies >
 - Policy**
 - Policy Label

Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policies

Authentication Policies 0

[Add](#) [Edit](#) [Delete](#) [Rename](#) [Show Bindings](#) [Global Bindings](#)

Click here to search or you can enter Key : Value format

	NAME	EXPRESSION	REQUEST SERVER
No items			

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

← Create Authentication Policy

Name*
 ⓘ

Action Type*
 ⓘ

Action*
 [Add](#) [Edit](#)

Expression* [Expression Editor](#)
 ⓘ

[Evaluate](#)

► More

[Create](#) [Close](#)

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

← Create Authentication Policy

Name*

Action Type*

RADIUS

▼

Action*

RADIUS_Server

▼

Add

Edit

Expression*

Select

▼

Select

▼

Select

▼

true

[Expression Editor](#)

[Evaluate](#)

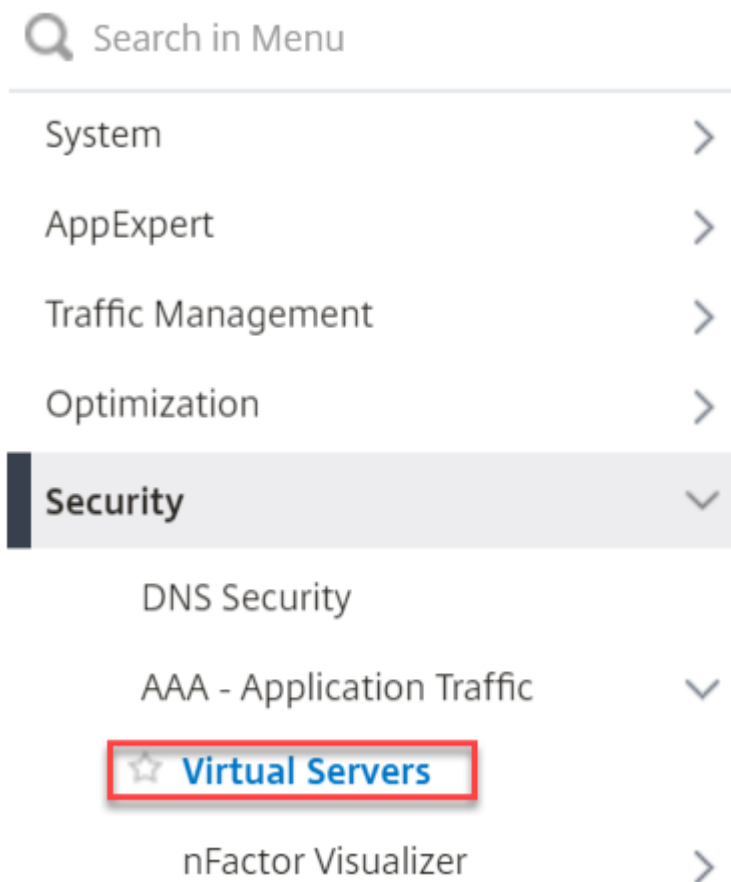
► More

Create

Close

Create a AAA vServer

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



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

The screenshot shows the 'Authentication Virtual Servers' management page. On the left is a navigation menu with categories: System, AppExpert, Traffic Management, Optimization, Security (selected), and Virtual Servers (indicated by a star). Under 'Security', there are sub-items: DNS Security, AAA - Application Traffic, and Virtual Servers. The main content area is titled 'Authentication Virtual Servers' with a blue circle containing the number '0'. Below the title are four buttons: 'Add', 'Edit', 'Delete', and 'Show nFactor Flow Bindings'. A search bar with a magnifying glass icon contains the text 'Click here to search or you can enter Key : Value format'. Below the search bar is a table with columns: NAME, STATE, and IP ADI. The table currently displays 'No items'.

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.

← Authentication Virtual Server

The screenshot shows the 'Basic Settings' section of the 'Authentication Virtual Server' configuration dialog. It contains the following fields:

- Name***: A text input field containing 'nFactorAuthvServer'. To the right of the field is an information icon (i) and a red 'X' with the text 'Please enter value'.
- IP Address Type***: A dropdown menu currently set to 'Non Addressable'. To the right of the dropdown is an information icon (i).
- Protocol**: A dropdown menu currently set to 'SSL'.

Below the 'Basic Settings' section is a 'More' section with a right-pointing arrow. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

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

Dashboard

Configuration

Reporting

← Authentication Virtual Server

Basic Settings

Name nFactorAuthvServer

Certificate

No Server Certificate

No CA Certificate

Continue

Cancel

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

Server Certificate Binding

Select Server Certificate*

Click to select

>

Add

☐ Server Certificate for SNI

Bind

Close

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.

Server Certificates 2

Select

Install

Update

Delete

Select

Certificate Type : SRVR_CERT|UNKNOWN... [Click here to search c](#)

	NAME	CERTIFICATE TYPE
<input type="radio"/>	ns-server-certificate	CLNT_CERT, SRVR_CERT
<input checked="" type="radio"/>	Example Cert	CLNT_CERT, SRVR_CERT

Total 2

7. Click "Bind".

Server Certificate Binding

Select Server Certificate*

Example Cert

>

Add

☐ Server Certificate for SNI

Bind

Close

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

Certificate

1 Server Certificate

No CA Certificate

Continue **Cancel**

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

Advanced Authentication Policies

No nFactor Flow

No Authentication Policy

No SAML IDP Policy

No OAuth IDP Policy

Continue **Cancel**

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

Policy Binding

Select Policy*

Click to select

>

Add

Edit

Binding Details

Priority*

100

Goto Expression*

NEXT

Select Next Factor

Click to select

>

Add

Edit

Bind

Close

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

Policy Binding > Authentication Policies

Authentication Policies 2

Select

Add

Edit

Delete

Rename

Show Bindings

Global Bindings

Click here to search or you can enter Key : Value format

	NAME	EXPRESSION	REQUEST SERVER
<input checked="" type="radio"/>	LDAP_Pol	true	LDAP_Server
<input type="radio"/>	RADIUS_Pol	true	RADIUS_Server

Total 2

25 Per Page

17 / 28

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

Policy Binding

Policy Binding

Select Policy*

LDAP_Pol

>

Add

Edit

► More

Binding Details

Priority*

100

Goto Expression*

NEXT

▼

Select Next Factor

Click to select

>

Add

Edit

Bind

Close

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

Policy Binding

>

Authentication Policy Labels

Authentication Policy Labels

Select

Add

Edit

Delete

Rename

Click here to search or you can enter Key : Value format

NAME

▼

NUMBER OF BOUND POLICIES

No items

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

Policy Binding > Authentication Policy Labels > Authentication Policy Label

Authentication Policy Label

Create Authentication Policylabel

Name*

RADIUS_PolicyLabel

i

Login Schema*

LSHEMA_INT

▼

Add

Edit

Feature Type

AAATM_REQ

▼

Comment

Continue

Cancel

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

[Policy Binding](#) > [Authentication Policy Labels](#) > Authentication Policy Label

Authentication Policy Label 1

Create Authentication Policylabel

Name

RADIUS_PolicyLabel

Login Schema

LSCHEMA_INT

Feature Type

AAATM_REQ

Policy Binding

Select Policy*

Click to select



Add

Edit

Binding Details

Priority*

100

Goto Expression*

NEXT



Select Next Factor

Click to select



Add

Edit

Bind

Close

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

[Policy Binding](#) > [Authentication Policy Labels](#) > [Authentication Policy Label](#) > Authentication Policies

Authentication Policies 2

Select

Add

Edit

Delete

Rename

Show Bindings

Global Bindings

Click here to search or you can enter Key : Value format

	NAME	EXPRESSION	REQUEST SERVER
<input type="radio"/>	LDAP_Pol	true	LDAP_Server
<input checked="" type="radio"/>	RADIUS_Pol	true	RADIUS_Server
Total 2			25 Per Page

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

[Policy Binding](#) > [Authentication Policy Labels](#) > Authentication Policy Label

Authentication Policy Label

Create Authentication Policylabel

Name

RADIUS_PolicyLabel

Login Schema

LSCHEMA_INT

Feature Type

AAATM_REQ

Policy Binding

Select Policy*

RADIUS_Pol

>

Add

Edit

► More

Binding Details

Priority*

100

Goto Expression*

NEXT

▼

Select Next Factor

Click to select

>

Add

Edit

Bind

Close

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

[Policy Binding](#) > [Authentication Policy Labels](#) > Authentication Policy Label

Authentication Policy Label 1

×

Create Authentication Policylabel

Name

RADIUS_PolicyLabel

Login Schema

LSCHEMA_INT

Feature Type

AAATM_REQ

Add Binding

Unbind

Regenerate Priorities

No action ▼

🔍 Click here to search or you can ent

<input type="checkbox"/>	PRIORITY	POLICY NAME	EXPRESSION	ACTION	GOTO EXPRESSION	NEXT FACTOR
<input type="checkbox"/>	100	RADIUS_Pol	true	RADIUS_Server	NEXT	

Done

19. Click "Select".

Policy Binding

>

Authentication Policy Labels

Authentication Policy Labels

Select

Add

Edit

Delete

Rename

Click here to search or you can enter Key : Value format

	NAME
<input checked="" type="radio"/>	RADIUS_PolicyLabel

Total 1

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

Policy Binding

Select Policy*

LDAP_Pol

>

Add

Edit

i

More

Binding Details

Priority*

100

Goto Expression*

NEXT

▼

Select Next Factor

RADIUS_PolicyLabel

×

>

Add

Edit

i

Bind

Close

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.

← Authentication Virtual Server

Basic Settings		Help
Name	nFactorAuthvServer	
IP Address	0.0.0.0	
Port	0	
Certificate		
1 Server Certificate		
No CA Certificate		
Advanced Authentication Policies		
No nFactor Flow		
1 Authentication Policy		
No SAML IDP Policy		
No OAuth IDP Policy		
		Advanced Settings
		+ Policies
		+ Login Schemas
		+ SSL Profile
		+ AAA Groups
		+ AAA Users
		+ Portal Themes

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

Login Schemas

No Login Schema

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

Policy Binding

Select Policy*

Click to select

>

Add

Edit

Binding Details

Priority*

100

Goto Expression*

END

Bind

Close

4. Select the built-in "Ischema_dual_factor_builtin" policy and click "Select".

Policy Binding > Authentication Policies

Authentication Policies 8

Select Add Edit Delete Rename Statistics

Click here to search or you can enter Key : Value format

	NAME	RULE
<input type="radio"/>	Ischema_cert_deviceid	HTTP.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0")
<input type="radio"/>	Ischema_single_factor_deviceid	HTTP.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0")
<input type="radio"/>	Ischema_dual_factor_deviceid	HTTP.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0")
<input type="radio"/>	Ischema_cert_single_factor_deviceid	HTTP.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0")
<input type="radio"/>	Ischema_cert_dual_factor_deviceid	HTTP.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0")
<input type="radio"/>	Ischema_adal	HTTP.REQ.HEADER("User-Agent").CONTAINS("OAuth/2.0")
<input checked="" type="radio"/>	Ischema_dual_factor_builtin	true
<input type="radio"/>	Ischema_dual_factor_flipped_builtin	true

Total 8

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

Policy Binding

Policy Binding

Select Policy*

Ischema_dual_factor_builtin > Add Edit ⓘ

► More

Binding Details

Priority*

100

Goto Expression*

END ▼

Bind Close

Note: The "Ischema_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**".

The screenshot shows the Citrix Gateway Virtual Servers management interface. On the left, a sidebar menu lists various categories: System, AppExpert, Traffic Management, Optimization, Security, Citrix Gateway (selected), Global Settings, Virtual Servers (highlighted with a blue box), and Portal Themes. The main content area is titled 'Citrix Gateway Virtual Servers' and contains buttons for Add, Edit, Delete, Statistics, and Visualizer. Below these buttons is a search bar with the text 'Click here to search or you can enter Key : Value format'. A table lists the virtual servers, with one entry 'Stevens Demo Gateway' shown as 'UP'. A summary bar at the bottom indicates 'Total 1'.

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

← VPN Virtual Server

The screenshot displays the configuration page for a VPN Virtual Server. The 'Basic Settings' section shows details for 'Stevens Demo Gateway', including Protocol (SSL), IP Address (0.0.0.0), Port (0), and State (UP). It also lists various authentication and security settings like 'Maximum Users', 'Max Login Attempts', 'Failed Login Timeout', 'ICA Only', 'Enable Authentication', 'IPset', 'Windows EPA Plugin Upgrade', 'Linux EPA Plugin Upgrade', 'Mac EPA Plugin Upgrade', 'ICA Proxy Session Migration', and 'Enable Device Certificate'. The 'Certificate' section shows '1 Server Certificate' and 'No CA Certificate'. The 'Basic Authentication' section has a '+' icon to add new profiles. On the right, the 'Advanced Settings' menu is visible, with 'Authentication Profile' selected and highlighted.

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

The screenshot shows the 'Authentication Profile' configuration dialog. It features a dropdown menu for selecting an authentication profile, followed by 'Add' and 'Edit' buttons. An information icon (i) is also present. At the bottom, there is a large 'OK' button.

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

Create Authentication Profile

Name*



Authentication Virtual Server*



Please select value.

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

[Create Authentication Profile](#) > Authentication Virtual Servers

Authentication Virtual Servers 1

Click here to search or you can enter Key : Value format

	NAME	STATE	IP ADDRESS
<input checked="" type="radio"/>	nFactorAuthvServer	● UP	0.0.0.0
Total 1			

6. Click "**Create**".

[Create Authentication Profile](#)

Create Authentication Profile

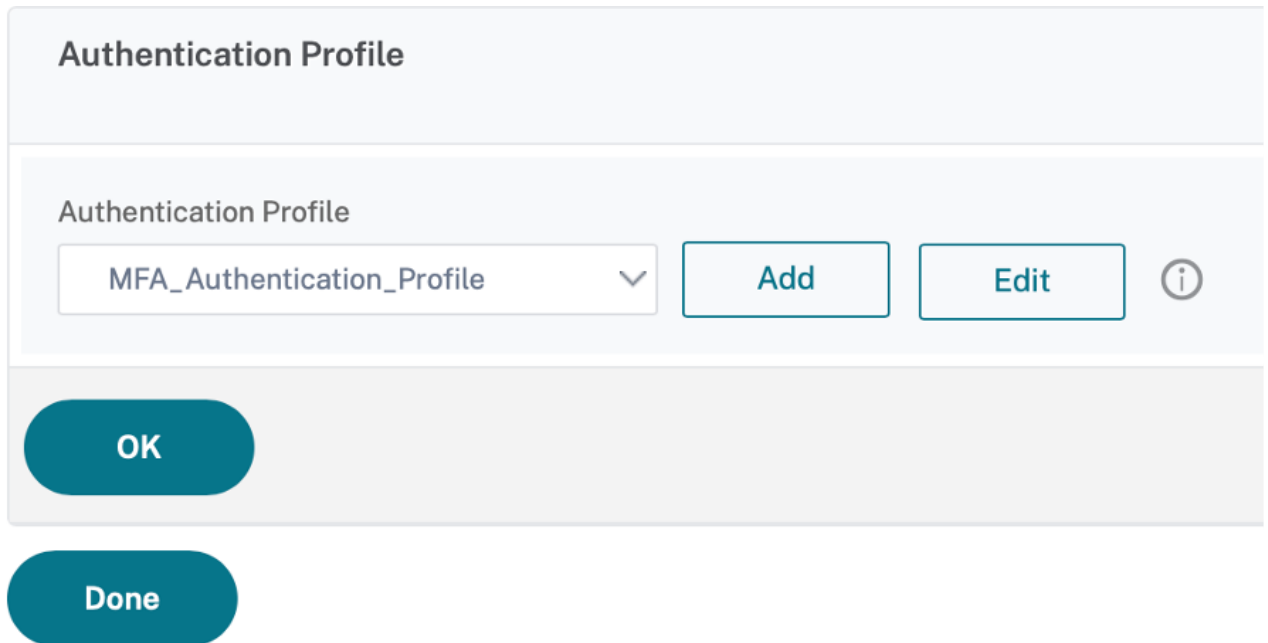
Name*



Authentication Virtual Server*



7. Click **"OK"**.



Authentication Profile

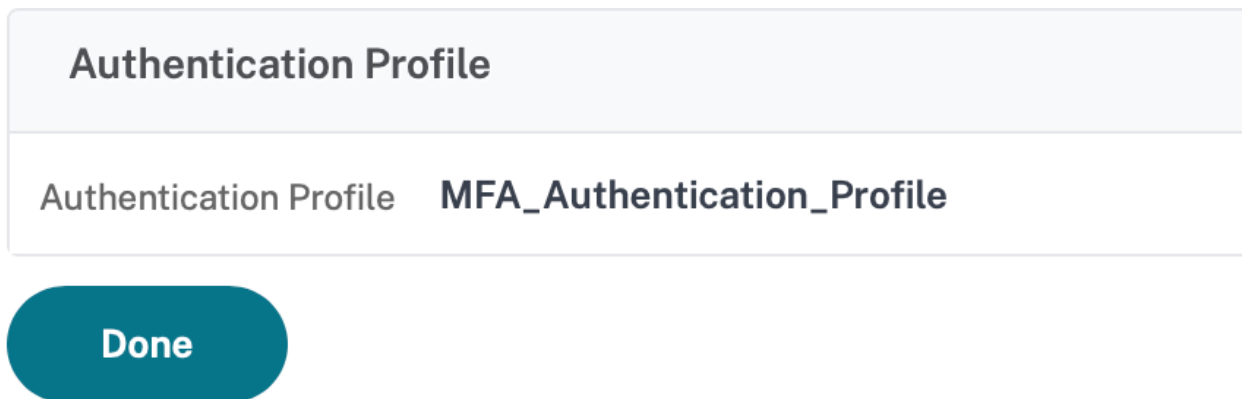
Authentication Profile

MFA_Authentication_Profile ▼ Add Edit ⓘ

OK

Done

8. Click **"Done"**.



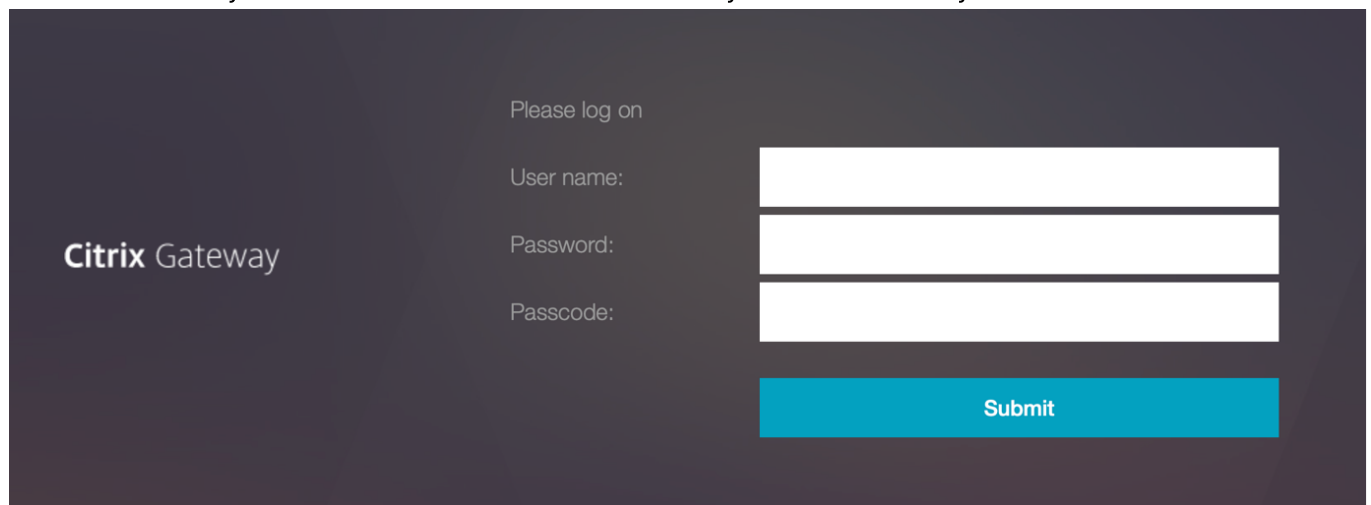
Authentication Profile

Authentication Profile MFA_Authentication_Profile

Done

Perform testing

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



Citrix Gateway

Please log on

User name:

Password:

Passcode:

Submit

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"
```