

Citrix NetScaler RADIUS OTP Configure Guide

Introduction

Use this guide to configure Citrix NetScaler to utilize a SecureAuth IdP Mobile One-time Password (OTP) as the user's password via RADIUS.

When the OTP password is accepted, the Access Gateway will send forward a successful authentication to the configured resources.

Prerequisites

1. Have a properly licensed and configured Access Gateway

Access Gateway Enterprise Edition or equivalent is required

2. Have the Public Address for VIP

NAT works as well

3. Have [RADIUS Service](#) configured on [SecureAuth IdP](#) with OATH realm to support **OTP only**

4. Have the SecureAuth IdP OTP app installed on mobile devices, and have mobile devices registered with SecureAuth IdP

Citrix NetScaler Configuration Steps

The screenshot shows the Citrix NetScaler VPX (10) Configuration page. The breadcrumb navigation is: NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers. The 'Add' button is highlighted with a red box. The table below shows the list of Virtual Servers.

Name	State	IP Address	Port	Protocol	Maximum Users	Current Users
[Redacted]	Up	[Redacted]	443	SSL	0	0
[Redacted]	Up	[Redacted]	443	SSL	10	0
[Redacted]	Up	[Redacted]	443	SSL	100	0
[Redacted]	Up	[Redacted]	443	SSL	5	0
[Redacted]	Up	[Redacted]	443	SSL	0	0
[Redacted]	Up	[Redacted]	443	SSL	20	0
[Redacted]	Up	[Redacted]	443	SSL	0	0

A **VPN Virtual Server** is required for this integration

1. Log into the Citrix NetScaler AGEE admin console, and select **Virtual Servers** under **NetScaler Gateway**

2. Select the appropriate Virtual Server to use for this integration, or click **Add** to create a new one

See below for Virtual Server creation steps

New VPN Virtual Server

NetScaler VPX (10) Info NS10.5 55.8.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

VPN Virtual Server

Basic Settings Help >

Name*
New Virtual Server

IPAddress*
111 . 222 . 111 . 222 IPv6

Port*
443

▶ More

OK Cancel

1. Set a **Name** for the new Virtual Server
2. Provide the **IP Address**
3. Provide the **Port** number
4. Click **OK**

Server Certificate

NetScaler VPX (10) Info NS10.5 55.8.nc Logout CITRIX

Dashboard Configuration Reporting Documentation Downloads

← Back

VPN Virtual Server

Basic Settings Help >

Name	New Virtual Server	Max Users	0	Double Hop	false
IPAddress		Max Login Attempts		Down State Flush	true
Port	443	Failed Login Timeout		AppFlow Logging	false
		State	true	ICA Proxy Session Migration	false
		ICA Only	false	Enable Device Certificate	false
		Enable Authentication	true		

Certificates

No Server Certificate >

No CA Certificate >

Authentication +

Advanced

- + SSL Parameters
- + SSL Profile
- + SSL Ciphers
- + SSL Policies
- + Profiles
- + Intranet IP Addresses

3. Open the Virtual Server, and click on the **Server Certificate** option

SSL Virtual Server Server Certificate Binding > Server Certificate Binding

Server Certificate Binding

Select Server Certificate*

Click to select > +

Server Certificate for SNI

Bind Close

4. Select the SSL Certificate to be used from the **Select Server Certificate** dropdown; or click the **+** to install the certificate (see below)
5. Once the SSL Certificate is selected, click **Bind**

Install Certificate

SSL Virtual Server Server Certificate Binding > Server Certificate Binding > Install Certificate

Install Certificate

Certificate-Key Pair Name*

SSL Server Certificate

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*

Browse +

Key File Name

Browse +

Certificate Format

PEM DER

Password

Certificate Bundle

Notify When Expires

Notification Period

30

Install Close

1. Provide a **Certificate Key-Pair Name** for the SSL Identity Certificate
2. Click **Browse** in the **Certificate File Name** section, and select the SSL Certificate
3. Select **PEM** or **DER** from the **Certificate Format** options
4. Click **Install**

RADIUS Authentication Policy

← Back

VPN Virtual Server

Basic Settings				Help	
Name	New Virtual Server	Max Users	0	Double Hop	false
IPAddress		Max Login Attempts		Down State Flush	true
Port	443	Failed Login Timeout		AppFlow Logging	false
		State	true	ICA Proxy Session Migration	false
		ICA Only	false	Enable Device Certificate	false
		Enable Authentication	true		

Certificates	
1 Server Certificate	>
No CA Certificate	>

Authentication	
	+

6. In the Virtual Server, click the + in the **Authentication** section to add an **Authentication RADIUS Policy**

Choose Type

Choose Type

Policies

Choose Policy*
RADIUS

Choose Type*
Primary

Continue Cancel

7. Select **RADIUS** from the **Choose Policy** dropdown

8. Select **Primary** from the **Choose Type** dropdown

9. Click **Continue**

Choose Type

Choose Type

Policies

Choose Policy RADIUS	Choose Type Primary
-------------------------	------------------------

Policy Binding

Select Policy*
Click to select > +

Binding Details

Priority*
100

Bind Close

10. Click to + in the **Select Policy** section to create a new RADIUS policy

11. Once the policy and profile are created (steps 12-21 below), click **Bind**

Choose Type > Create Authentication RADIUS Policy

Create Authentication RADIUS Policy

Name*
New RADIUS Policy

Server*
New RADIUS Server +

Expression* Expression Editor

Operators Saved Policy Expressions Frequently Used Expressions Clear

ns_true

Create Close

12. Provide a **Name** for the new RADIUS policy
13. Click the **+** in the **Server** section to create a new RADIUS server
14. Select the newly created RADIUS server (steps 17-21 below) from the **Server** dropdown
15. Create an **ns_true** Expression
16. Click **Create**

Create Authentication RADIUS Server

Create Authentication RADIUS Server

Name*
New RADIUS Server

Server Name Server IP

IP Address*
111 . 222 . 111 . 222 IPv6

Port
1812

Time-out (seconds)
3

Secret Key*

Confirm Secret Key*

Send Calling Station ID

▼ Details

NAS ID

Enable NAS IP address extraction

Group Vendor Identifier

Group Prefix

Group Attribute Type

Group Separator

IP Address Vendor Identifier

IP Address Attribute Type

Password Vendor Identifier

Password Attribute Type

Password Encoding*
pap

Accounting*
OFF

Default Authentication Group

Create Close

17. Provide a **Name** for the new RADIUS server
18. Provide the **Server Name** or IP Address
19. Set the **Port** to **1812** (as configured on SecureAuth IdP)
20. Select **pap** from the **Password Encoding** dropdown
21. Click **Create**

