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

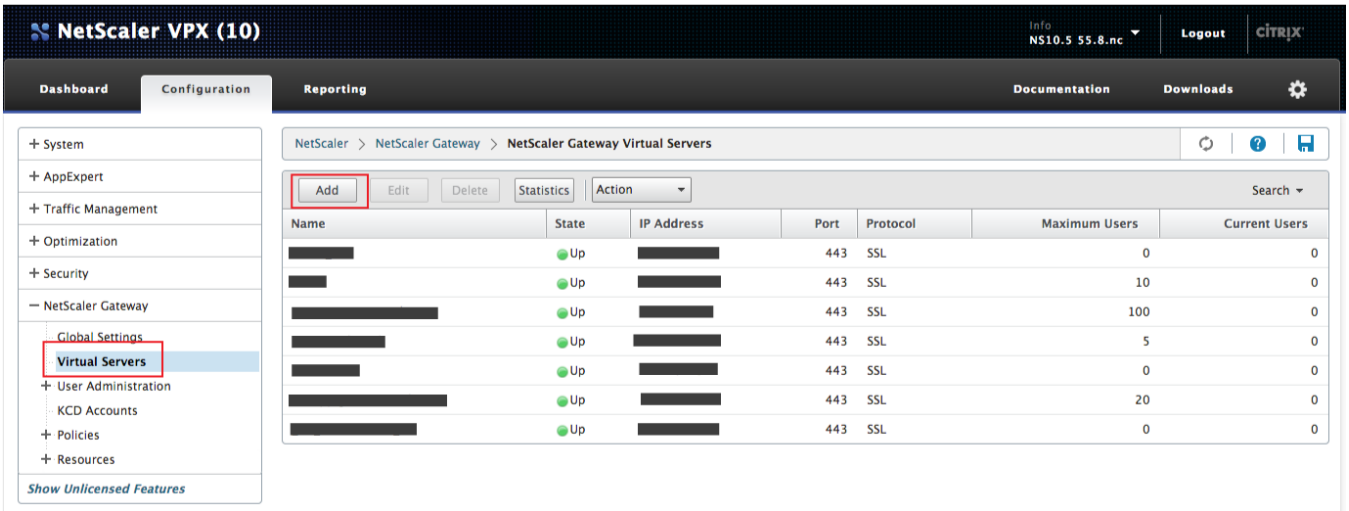
2. Have the Public Address for VIP

    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



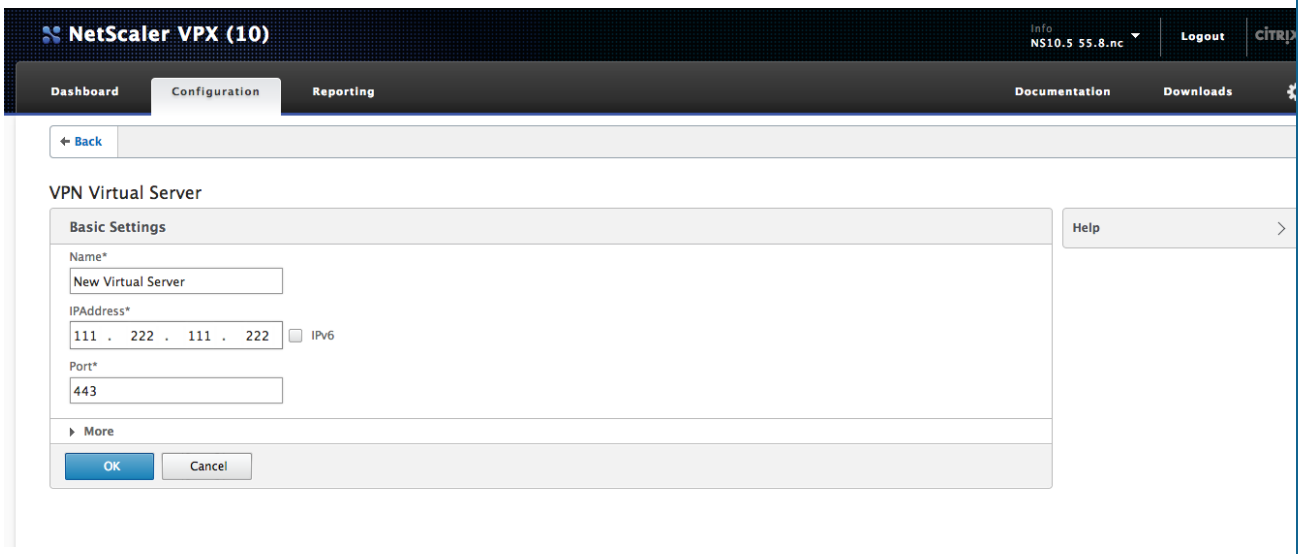
A **VPN Virtual Server** is required for this integration

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

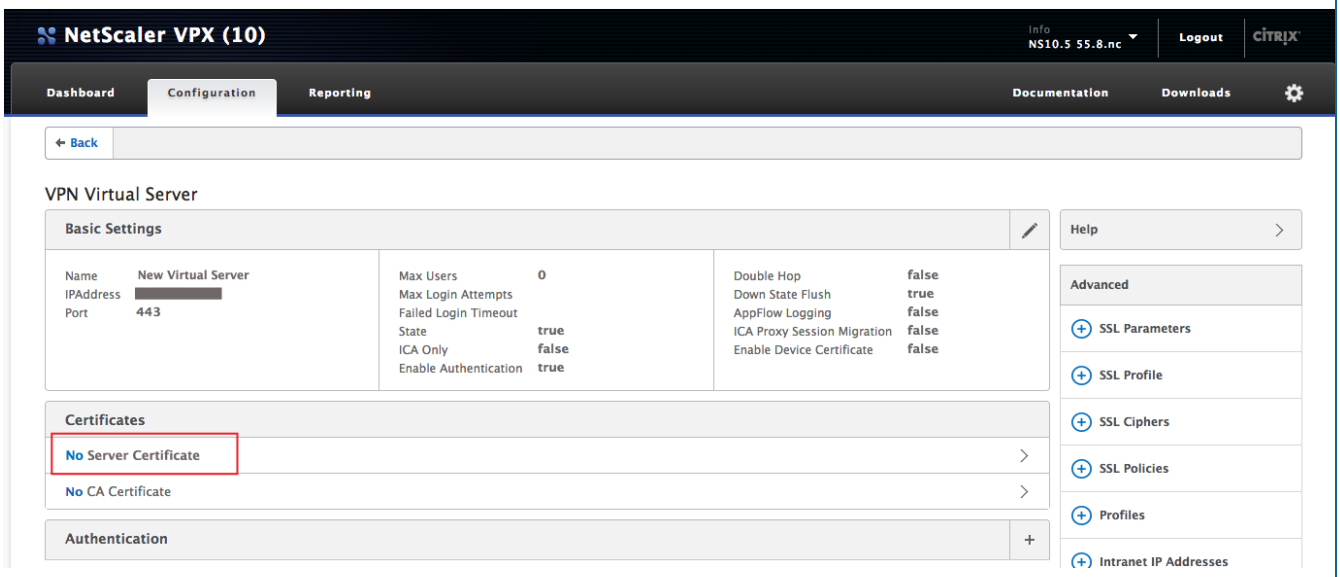
    See below for Virtual Server creation steps

New VPN Virtual Server



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

Server Certificate

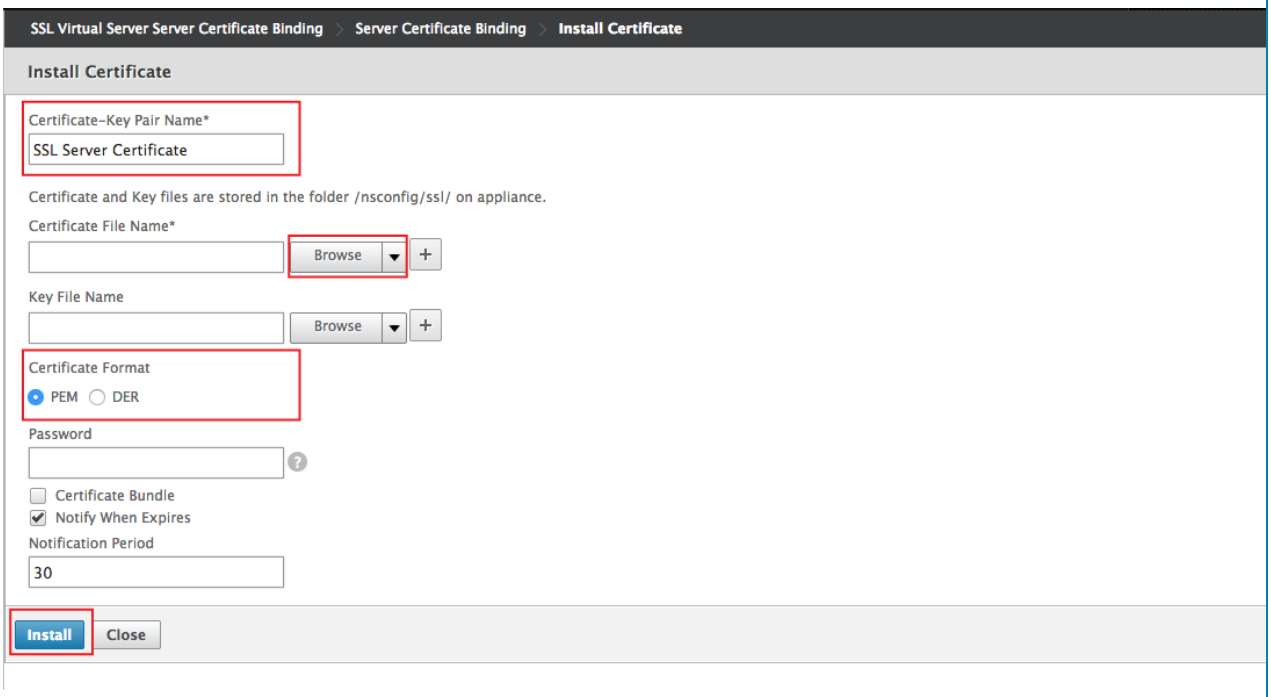


3. Open the Virtual Server, and click on the **Server Certificate** option

4. Select the SSL Certificate to be used from the **Select Server Certificate** dropdown; or click the **+** to install the certificate (see below)

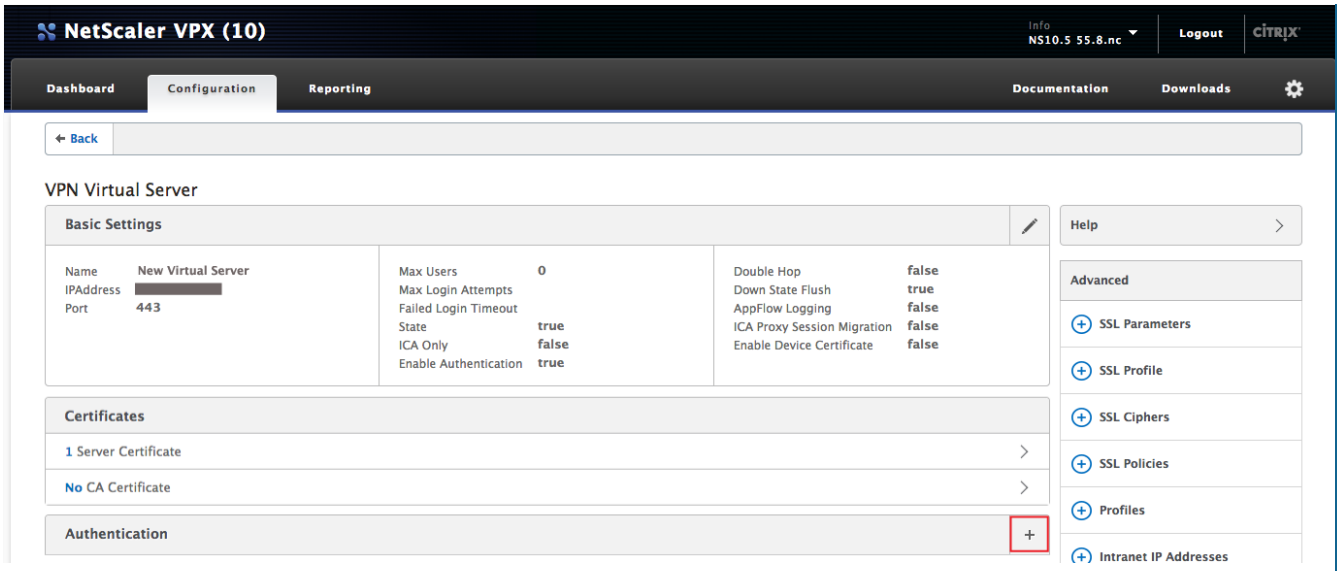
5. Once the SSL Certificate is selected, click **Bind**

Install Certificate

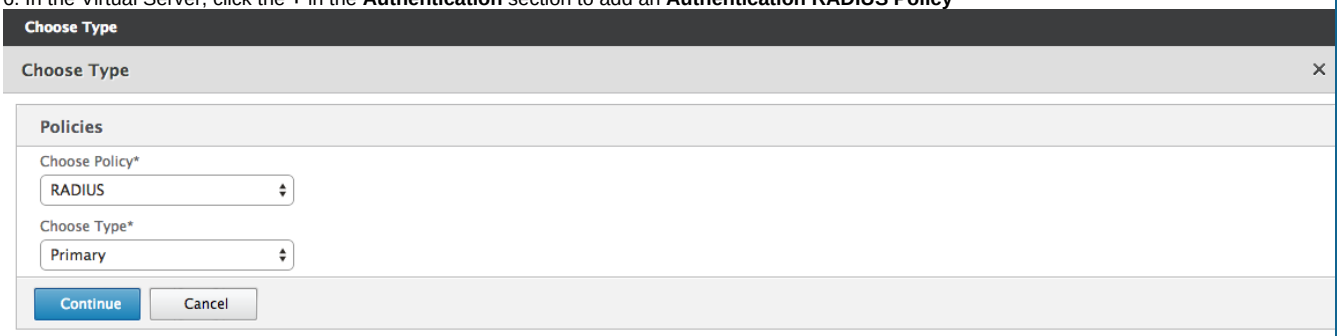


1. Provide a **Certificate Key-Pair Name** for the SSL Identity Certificate
2. Click **Browse** in the **Certificate File Name** section, and select the SSL Certificate
3. Select **PEM** or **DER** from the **Certificate Format** options
4. Click **Install**

RADIUS Authentication Policy



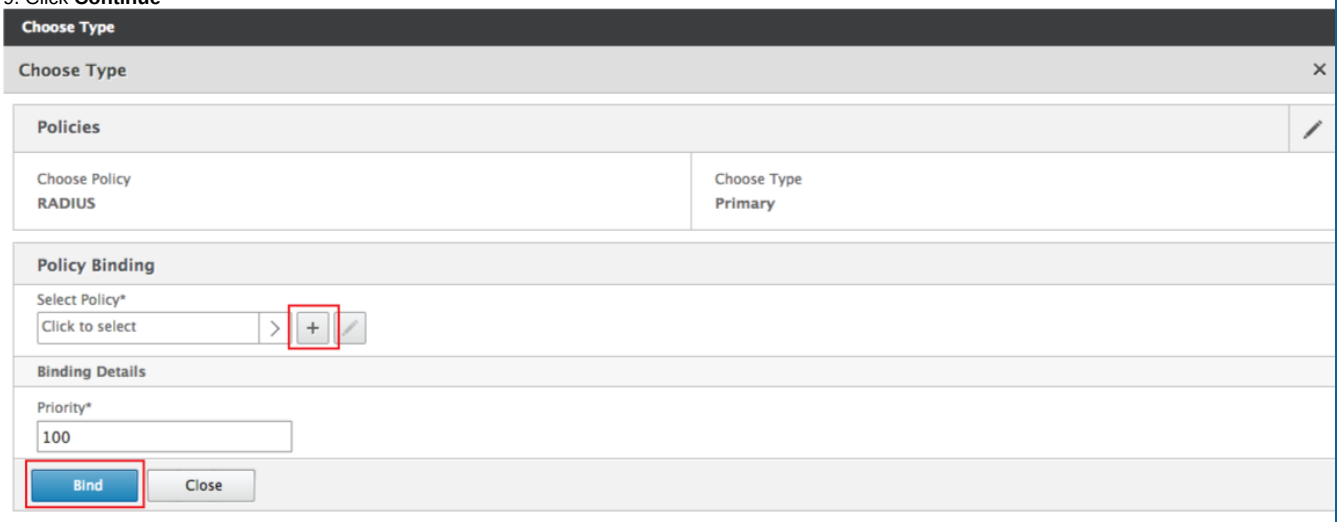
6. In the Virtual Server, click the **+** in the **Authentication** section to add an **Authentication RADIUS Policy**



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

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

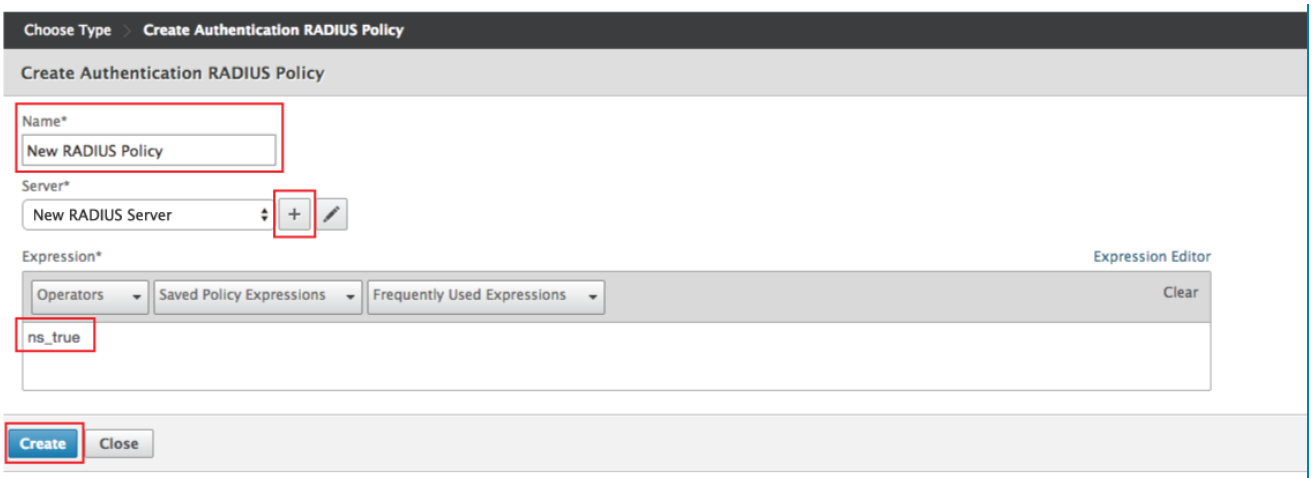
9. Click **Continue**



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**

Create Authentication RADIUS Policy



12. Provide a **Name** for the new RADIUS policy

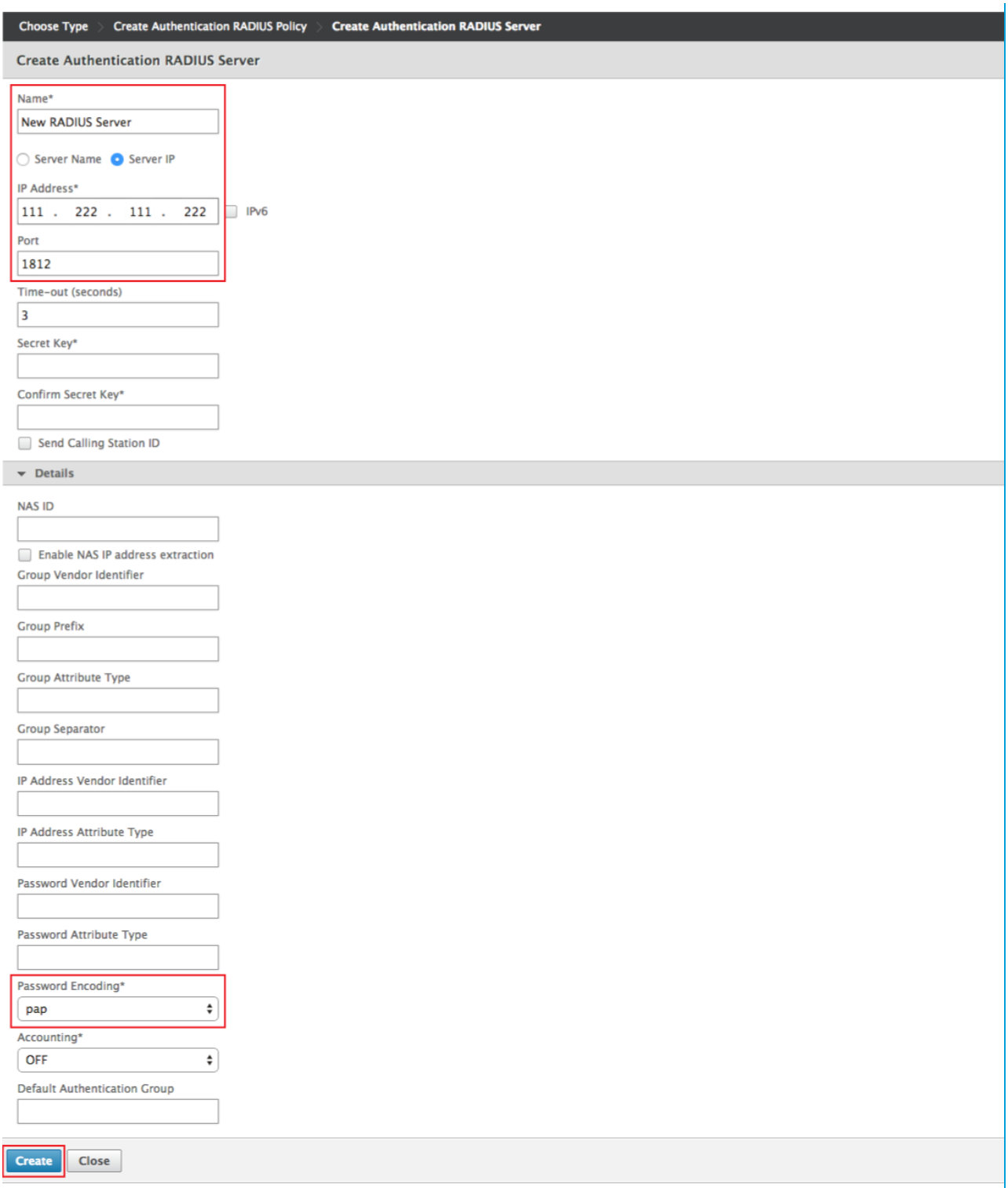
13. Click the **+** in the **Server** section to create a new RADIUS server

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



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**