# CITRIX NETSCALER INTEGRATION GUIDE

## SecurEnvoy SecurAccess

### Abstract

This document will walk you through the basic steps to configure your Citrix NetScaler to use SecurEnvoy SecurAccess for Two-Factor Authentication

Document Version 1.22

Michael Urgero

murgero@securenvoy.com

# Contents

## Getting Started

The purpose of this document is to outline the general steps for the configuration of your Citrix NetScaler to use SecurEnvoy SecurAccess Two-factor Authentication Solution within your environment quickly and easily.

Both the SecurEnvoy SecurAccess Two-Factor Authentication Solution and the Citrix NetScaler have many features and optional configuration methods. We will not be covering all features and options in this guide. The intent of this guide is to provide instruction for the integration of SecurEnvoy SecurAccess Two-factor Authentication with your Citrix NetScaler to a production ready state.

### Things You Will Need

This document will assume that the reader is a network and systems administrator with administrative level access to the systems required for this implementation, listed below. If you do not currently have this level of access to the environment, you should obtain it before you continue.

To properly integrate SecurEnvoy SecurAccess with your Citrix NetScaler you will need the following;

- A working SecurEnvoy SecurAccess implementation.
- A working Citrix NetScaler (Version 11.1 48.10nc shown here)

### General Environment

The below assumptions are made during this document.

- Your Citrix NetScaler can be physical or virtual.
- You have deployed your Citrix NetScaler in a 1-Arm Configuration, which is the most common.
- You have already configured your Citrix NetScaler for use with Citrix StoreFront, including SSL Certificates.

### Other notable configurations

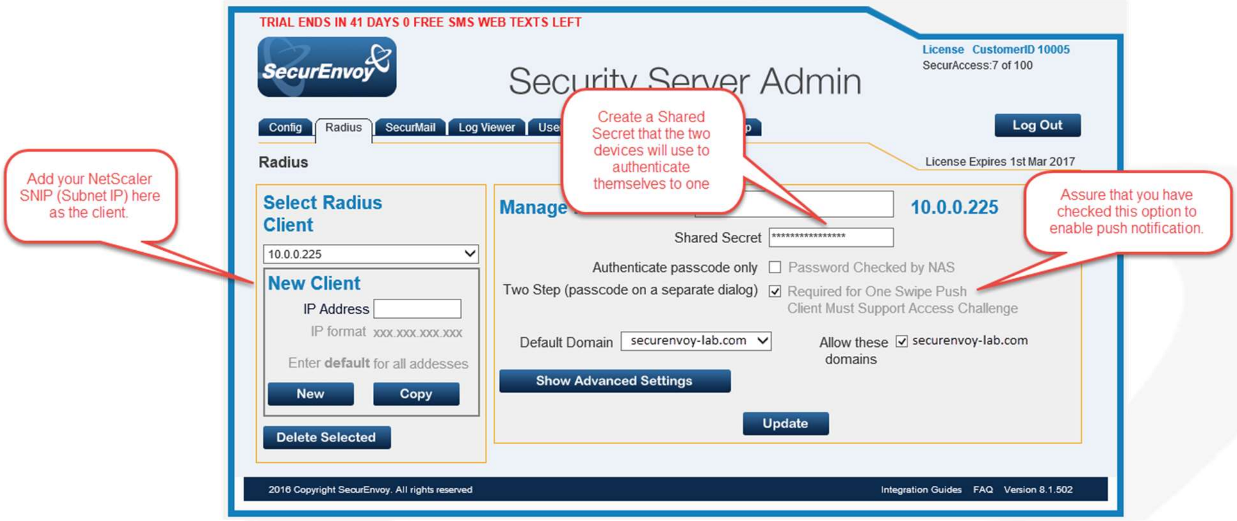
- If you are using two Citrix NetScalers and they are already configured for HA, this document will still apply properly.
- If you are using two SecurEnvoy SecurAccess Servers in your environment, you will need to follow a few additional optional steps notes in this guide.

| **SecurEnvoy Token Types Available for NetScaler** | |
|---|---|
| Real Time SMS or Email | ☑ |
| Preload SMS or Email | ☑ |
| Soft Token Code | ☑ |
| Soft Token Next Code | ☑ |
| Push Notifications (Apple, Android and Microsoft) | ☑ |
| Voice Call | ☑ |
| QR Code | ☒ |

## Prepare the SecurEnvoy SecurAccess Server

In this step, we will illustrate the critical components that you will need to perform to make sure that the SecurEnvoy SecurAccess Server is prepared.

Always take note – our IP Addresses are from our internal lab. Yours will be different.



TRIAL ENDS IN 41 DAYS 0 FREE SMS WEB TEXTS LEFT

Security Server Admin

License CustomerID 10005
SecurAccess:7 of 100

License Expires 1st Mar 2017

Radius

Select Radius Client: 10.0.0.225

New Client
IP Address
IP format xxx.xxx.xxx.xxx
Enter **default** for all addesses

Manage 10.0.0.225

Shared Secret: ****************

Authenticate passcode only: □ Password Checked by NAS

Two Step (passcode on a separate dialog): ☑ Required for One Swipe Push
Client Must Support Access Challenge

Default Domain: securenvoy-lab.com

Allow these domains: ☑ securenvoy-lab.com

2016 Copyright SecurEnvoy. All rights reserved

Integration Guides FAQ Version 8.1.502

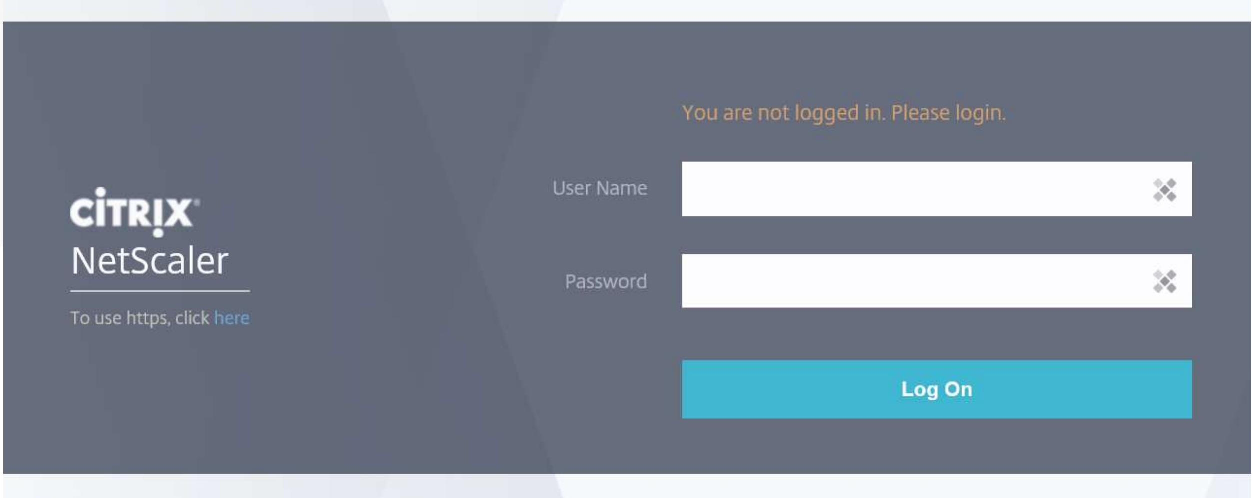
Add your NetScaler SNIP (Subnet IP) here as the client.

Create a Shared Secret that the two devices will use to authenticate themselves to one

Assure that you have checked this option to enable push notification.

Communication will RADIUS and is expected to be operating on the standard TCP Port 1812. The SecurEnvoy SecurAccess Server is the RADIUS host.

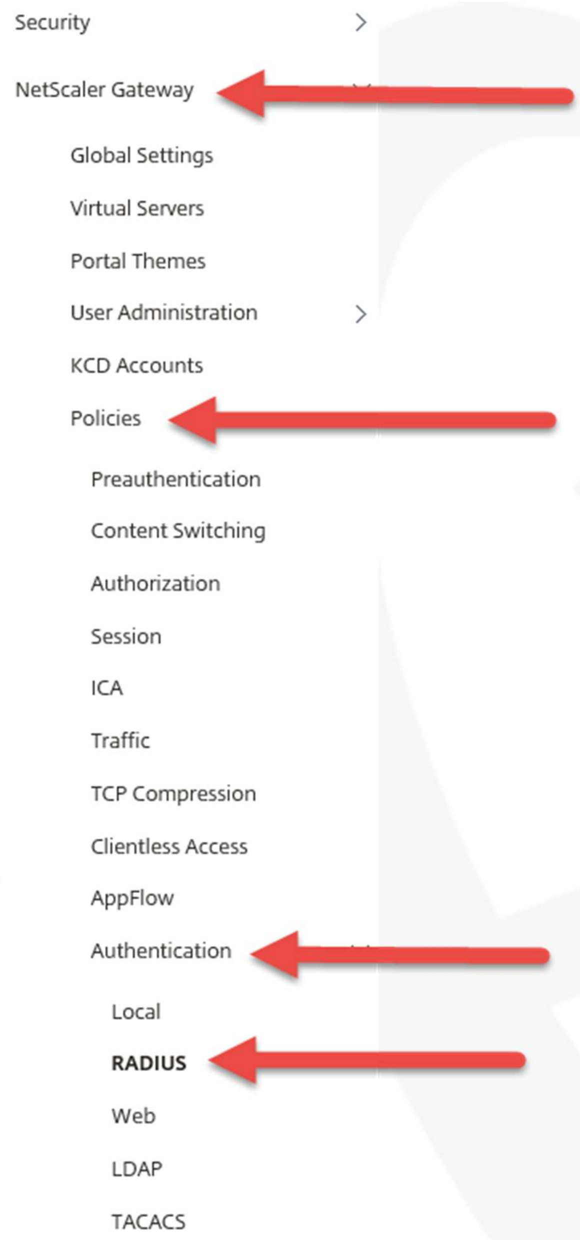
## Let’s get logged into the Citrix NetScaler



You are not logged in. Please login.

To use https, click here

Authentication with an admin account is required.



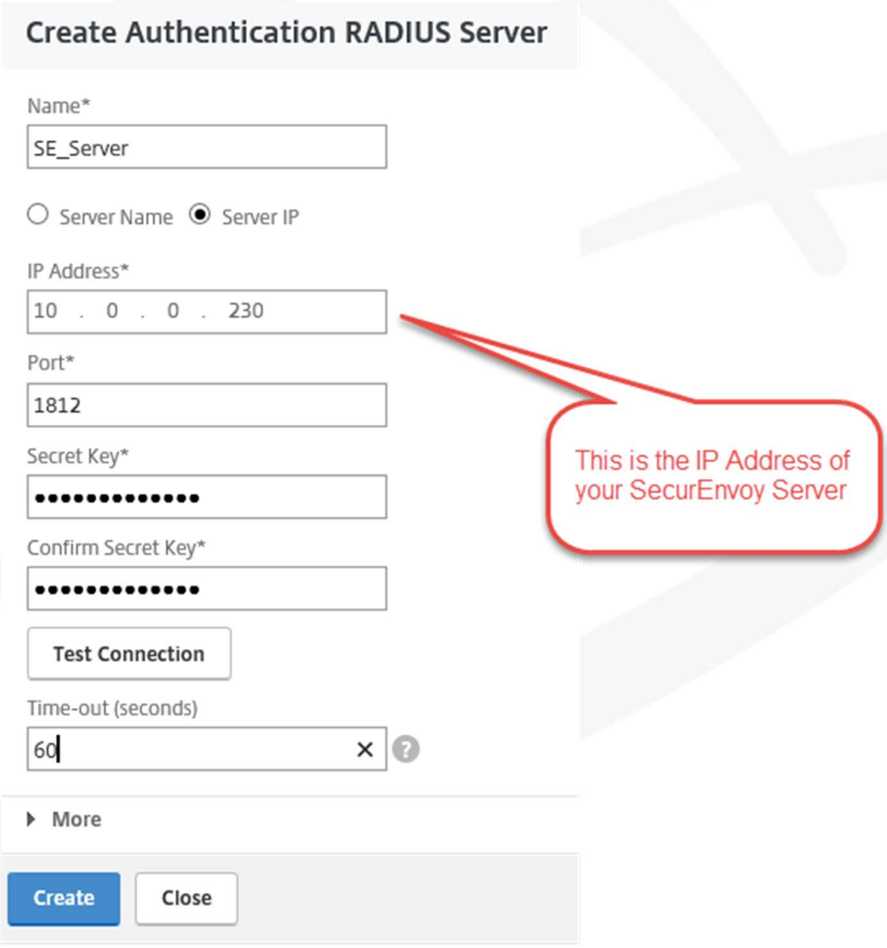
We will be creating a RADIUS Authentication Policy. Navigate using the left tree to the RADIUS Authentication Policy Section shown here.

## RADIUS Authentication Policy

The SecurEnvoy SecurAccess Authentication Policy needs to be created and will replace the authentication policy that you currently have, usually LDAP.

### Create the Authentication Server

You will need to create an authentication server to define the RADIUS communication.



Create Authentication RADIUS Server

Name*: SE_Server

○ Server Name ● Server IP

IP Address*: 10 . 0 . 0 . 230

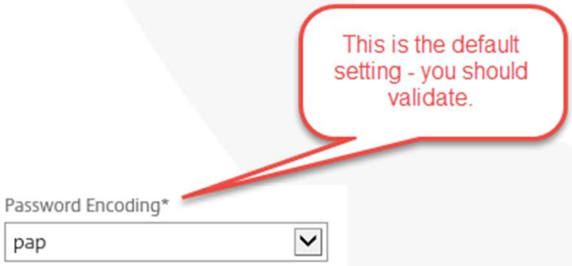
Port*: 1812

Secret Key*: ••••••••••••••

Confirm Secret Key*: ••••••••••••••

Time-out (seconds): 60

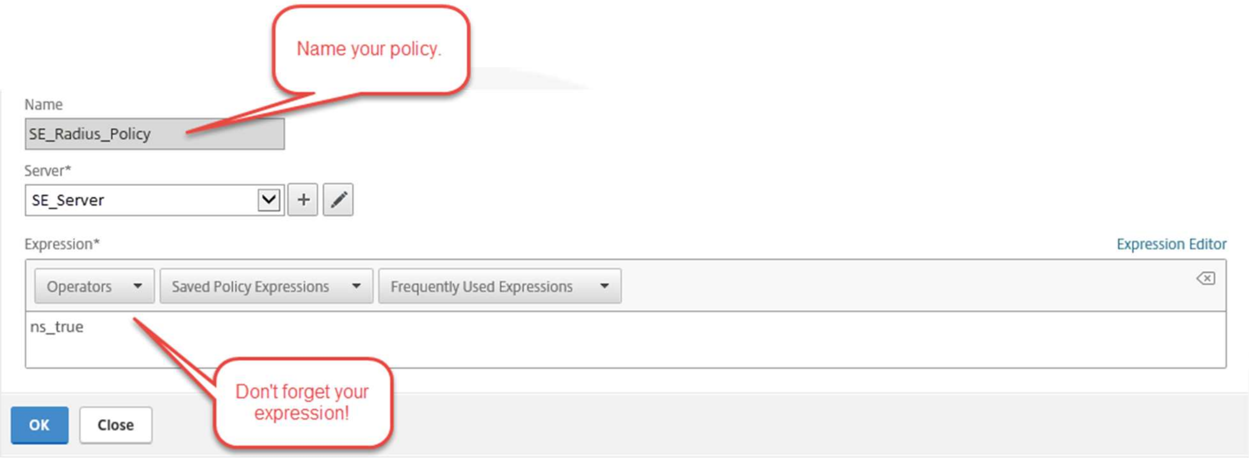
This is the IP Address of your SecurEnvoy Server



This is the default setting - you should validate.

Password Encoding*: pap

Don’t forget to click ‘More’ and verify that the Password Encoding is set to pap.



Name your policy.

Name

SE_Radius_Policy

Server*

SE_Server

Expression*

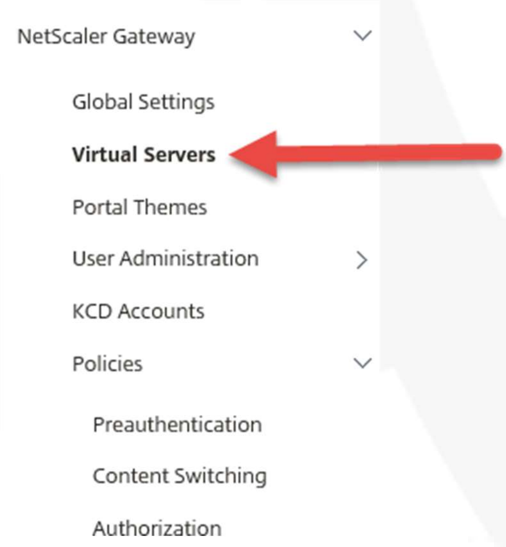
ns_true

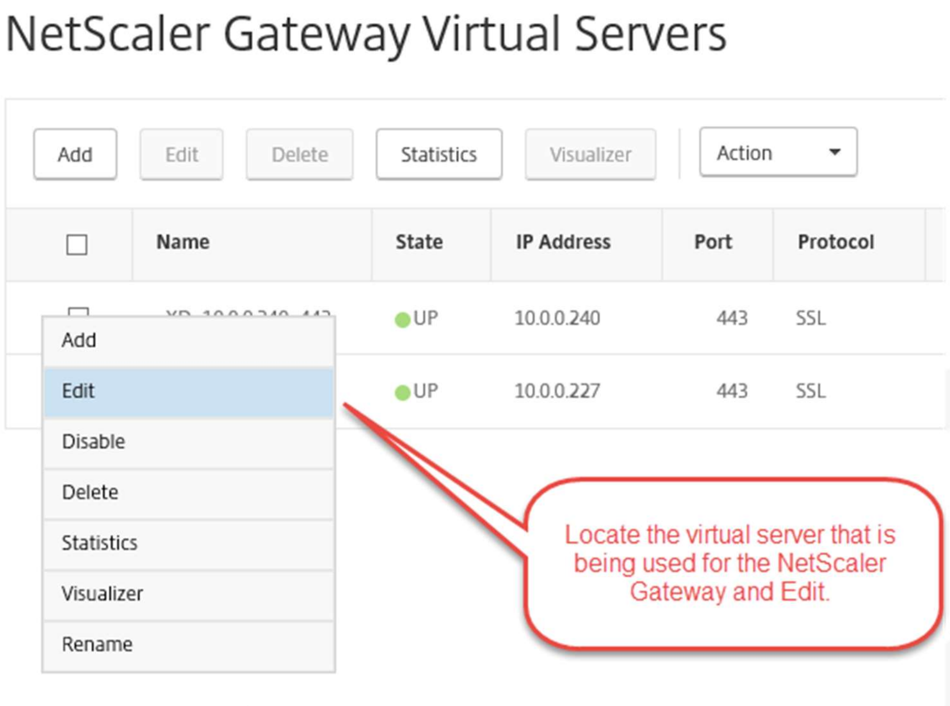
Don't forget your expression!

Once you have created the authentication policy, defined your SecurEnvoy Server, verified pap and your expression, you're nearly done.

All we need to do now is use this policy as opposed to your existing LDAP one.

Navigate up to Virtual Servers as shown.

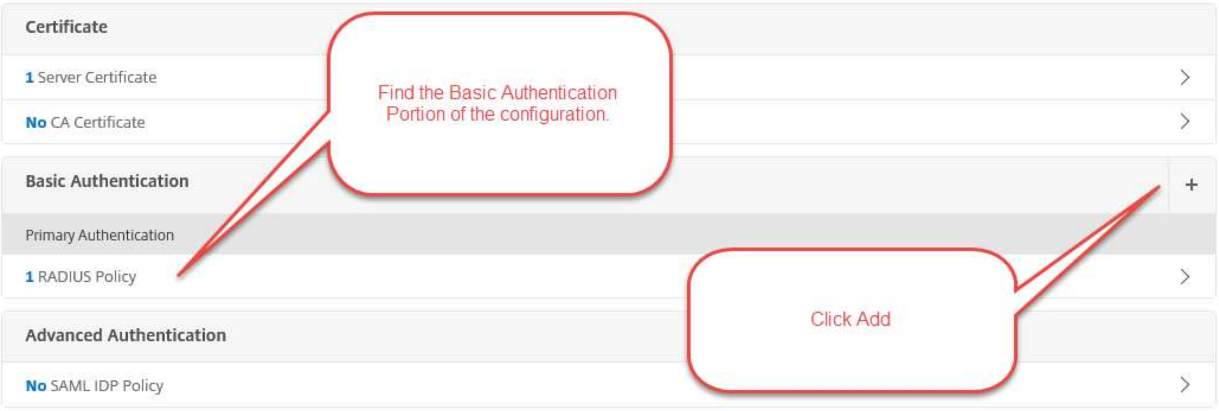




NetScaler Gateway Virtual Servers

| ☐ | Name | State | IP Address | Port | Protocol |
|---|---|---|---|---|---|
| ☐ | XD_10.0.0.240_443 | ● UP | 10.0.0.240 | 443 | SSL |
|  |  | ● UP | 10.0.0.227 | 443 | SSL |

Locate the virtual server that is being used for the NetScaler Gateway and Edit.



Certificate

1 Server Certificate

No CA Certificate

Basic Authentication

Primary Authentication

1 RADIUS Policy

Advanced Authentication

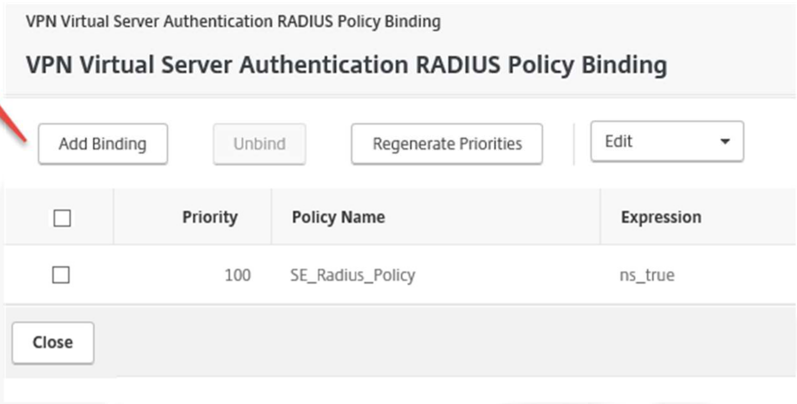
No SAML IDP Policy

Find the Basic Authentication Portion of the configuration.

Click Add

We always recommend adding the RADIUS Policy before removing the authentication policy you already have here.

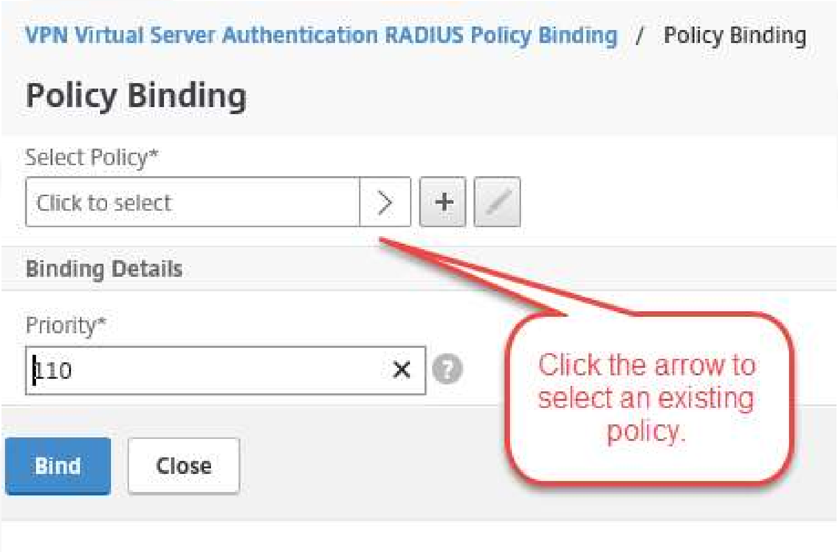
Click Add Binding.



VPN Virtual Server Authentication RADIUS Policy Binding

### VPN Virtual Server Authentication RADIUS Policy Binding

| □ | Priority | Policy Name | Expression |
|---|---|---|---|
| □ | 100 | SE_Radius_Policy | ns_true |



VPN Virtual Server Authentication RADIUS Policy Binding / Policy Binding

### Policy Binding

Select Policy*

Click to select

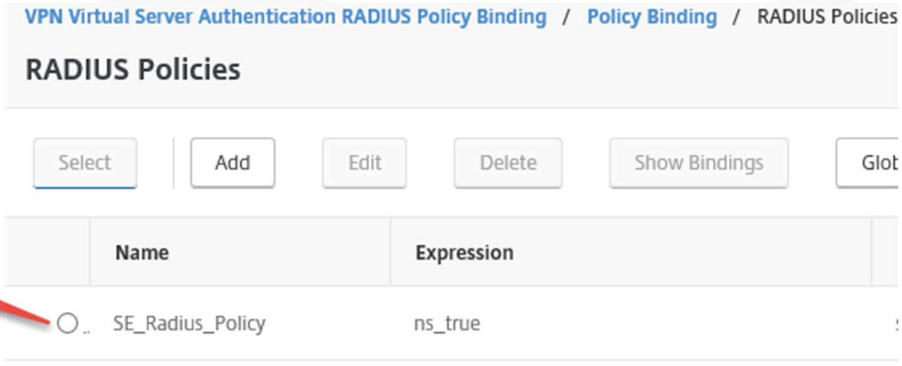
Binding Details

Priority*

110

Click the arrow to select an existing policy.

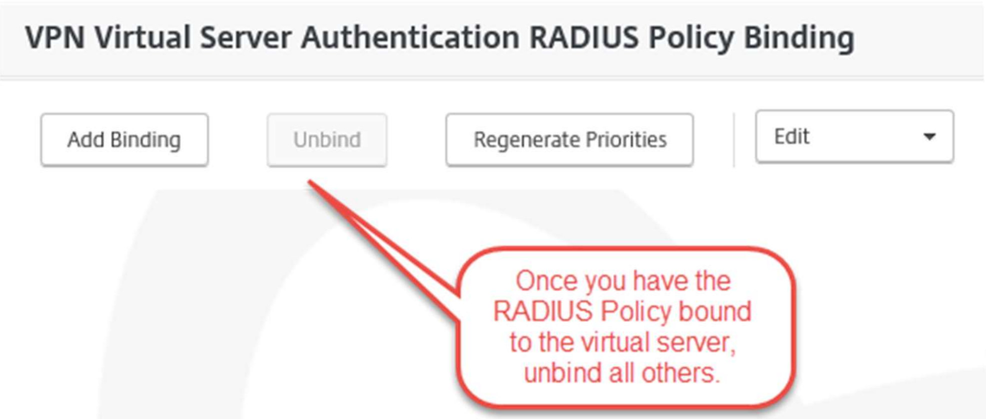
Select your policy that you created previously.



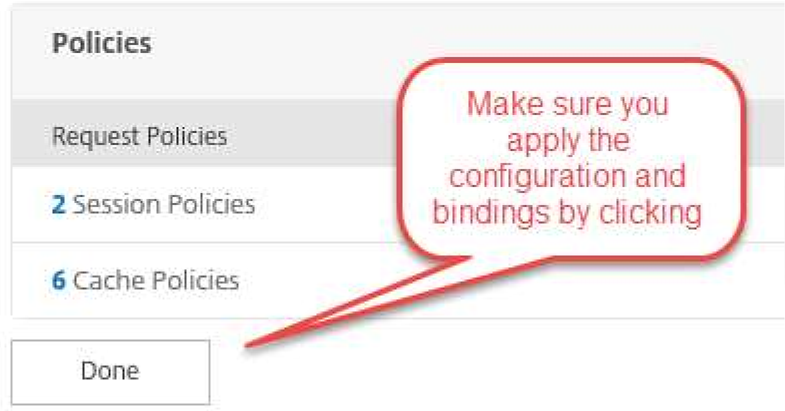
VPN Virtual Server Authentication RADIUS Policy Binding / Policy Binding / RADIUS Policies

### RADIUS Policies

| | Name | Expression |
|---|---|---|
| ○ | SE_Radius_Policy | ns_true |



Once you have the RADIUS Policy bound to the virtual server, unbind all others.



Make sure you apply the configuration and bindings by clicking

## What’s Next

Now that you have the SecurEnvoy SecurAccess Two-Factor Authentication configuration completed, you can logoff the Citrix NetScaler.

Opening your browser and navigate to the Citrix NetScaler Access Gateway URL – myapps.company.com

## Support for Your Trial

We’re happy to help you get things setup and running. If you have any questions or need help with your trial, please reach out to us – we would be happy to help.