SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Citrix Netscaler Integration Guide

SecurAccess Integration Guide

Version 1.0 – 09/18

Citrix Netscaler Integration Guide

Contents

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA solution integrates with Citrix Netscaler appliance through the use of RADIUS Server for authorisation and access control.

The software used for the integration process is listed below:

Citrix Netscaler VPX (1000)® NS12.1 48.13.nc
SecurEnvoy SecurAccess Release v9.3.502

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configuration may have other methods to accomplish the same task than those described.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- A SecurAccess MFA server installed, configured and working on a system with:
  - Windows Server 2003 or higher.
  - An LDAP or Lightweight Directory Service database of users

  Note: Please see SecurEnvoy's SecurAccess version 9.3 deployment guide on how to setup MFA server solution (On the www.securenvoy.com website)

- A Citrix Netscaler (Physical, Virtual) running version 12.0 and above, (previous versions of Netscaler may work but have not been tested with full functionality)

- This guide assumes that Citrix Netscaler has been installed and previously configured to authenticate users successfully with a username and password through LDAP.

- Familiarity with the following technologies:
  - RADIUS configuration
  - Citrix Netscaler Administration Interface

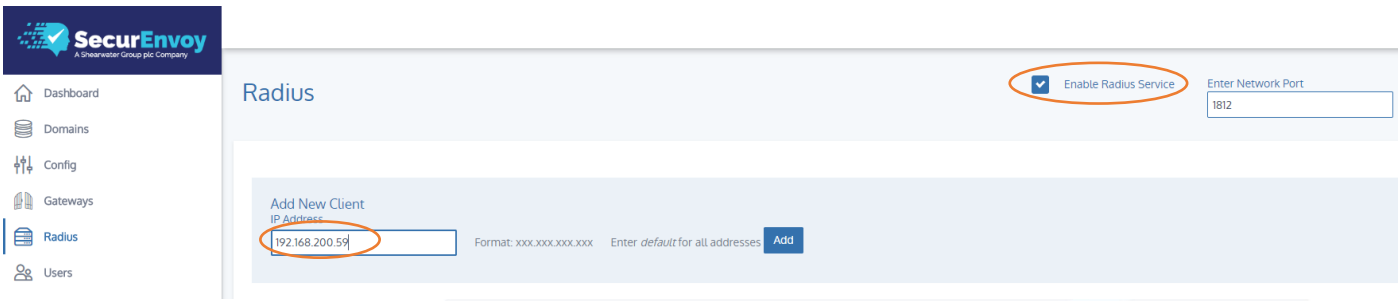
1.4 Authentication

The following section describes the steps required to configure both the Netscaler appliance to authenticate users via RADIUS through the SecurEnvoy SecurAccess Solution.

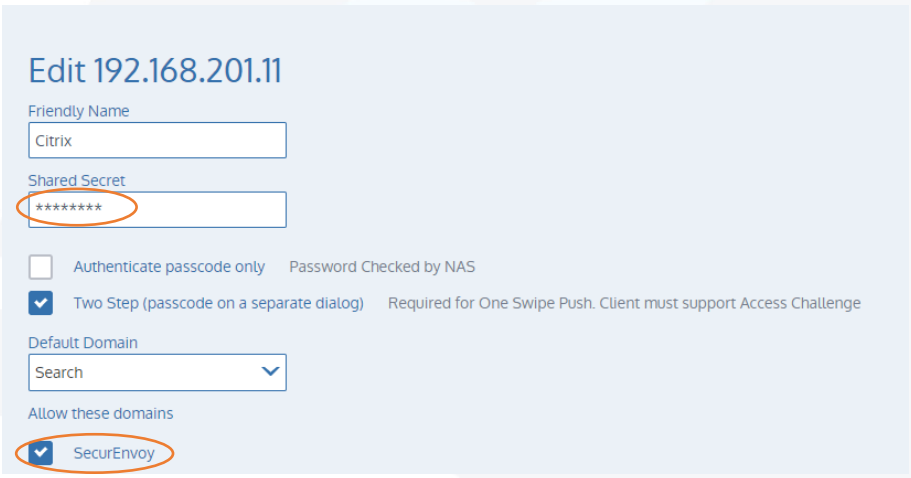
1.41 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the Pulse connect Secure appliance as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the IP address of the Netscaler Appliance and click "Add"

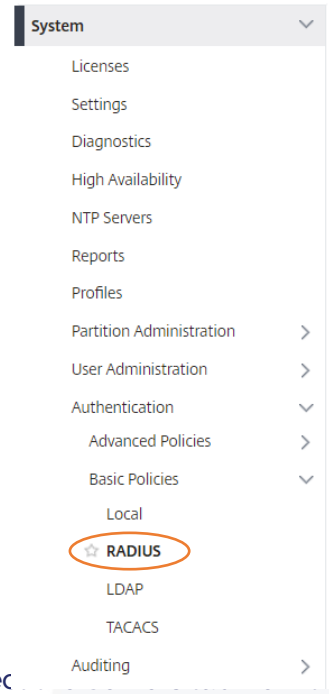


- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update

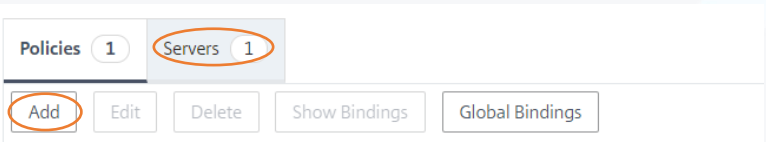


1.42 Setup RADIUS – Netscaler

Navigate to System\Authentication\Basic Policies\RADIUS within the Netscaler administration portal.



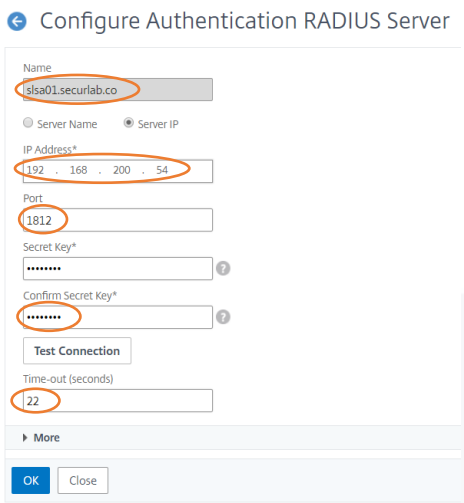
Selec e config window and click Add to define a new RADIUS Authentication Server.



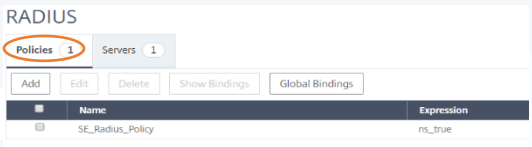
Select RADIUS Server from the drop-down list and select New Server, to configure a new authentication Server.

On presentation of the RADIUS Server dialogue box, complete the details as highlighted below, making sure you enter the shared secret password set in the last section.

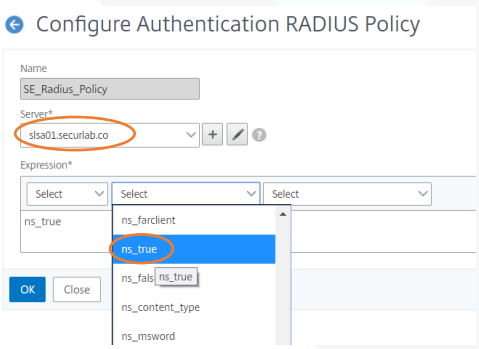
Name: Provide the Server with a unique, but identifiable name
Server Name or Sever IP
IP Address: Set the IP address of the SecurAccess Server
Port: Make sure the port number matches the port set on the SecurAccess RADIUS page
Shared Key: Make sure the Shared key matches the key defined in the last section
Timeout: Timeout should be higher than the timeout set in SecurAccess for PUSH notifications



Click OK to apply the settings.



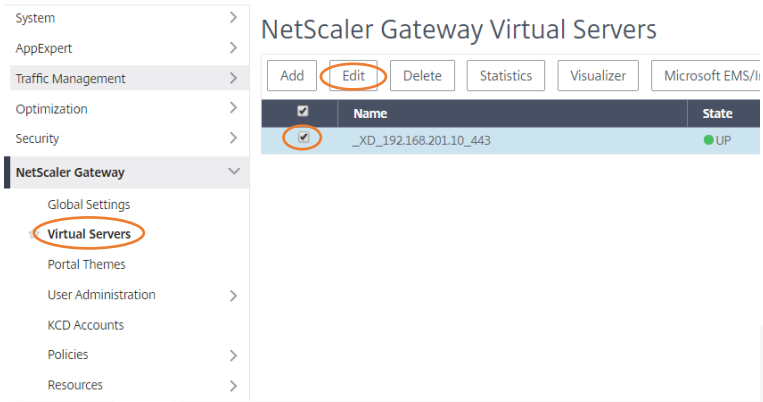
We will now need to define a policy against the newly created RADIUS Server.
Click on the Policies tab and select Add to create a new policy.



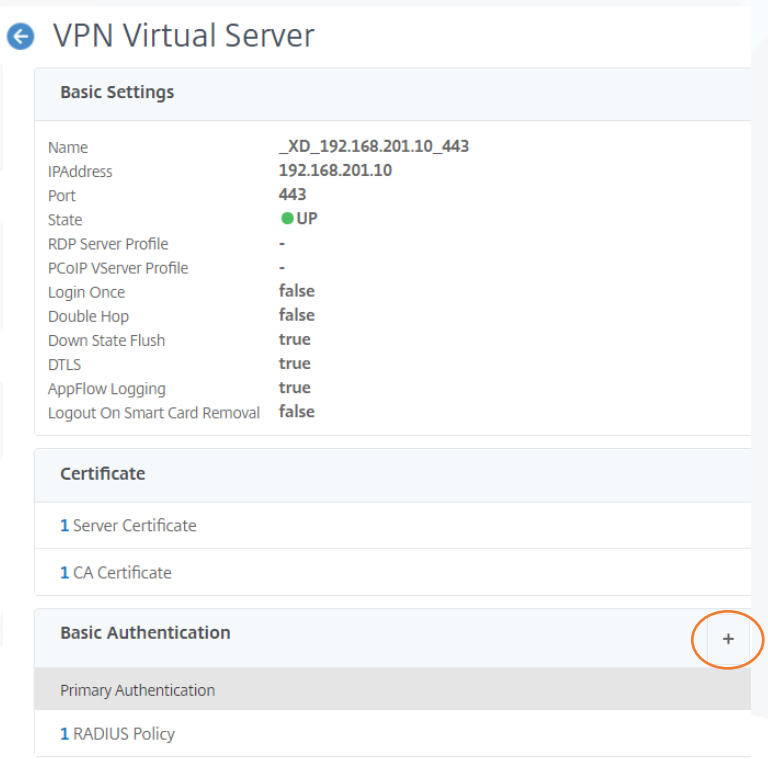
Name: Set a name for the Policy
Server: Select drop down list and select the server we created in the last step.
Expression: Select middle drop-down list and select ns_true and click OK to complete.

1.43 Virtual Server – Authentication Policy

Once we have defined both the RADIUS Authentication server and policy, we will assign to the existing Virtual Server.
Navigate to Netscaler Gateway\Virtual Servers and select the existing Virtual Server that is authenticating users through AD username and password.
Click Edit

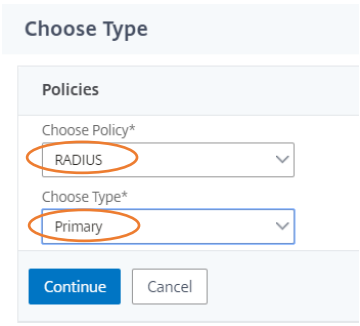


We will now look to edit the Basic Authentication Policy and change the existing LDAP policy to a RADIUS method.

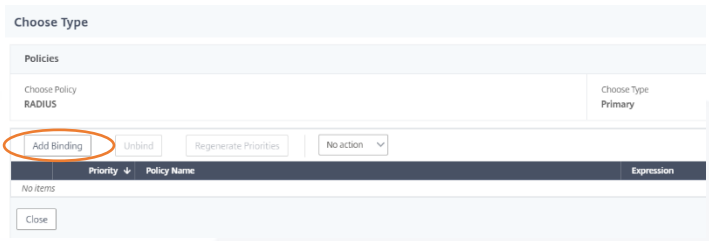


Locate and click on the plus sign to add a new authentication policy

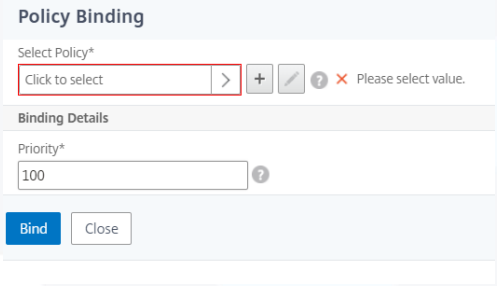
Select RADIUS policy and Primary Type and select Continue.



Select Add Binding



And select the RADIUS policy by selecting the Policy drop-down list and clicking Bind

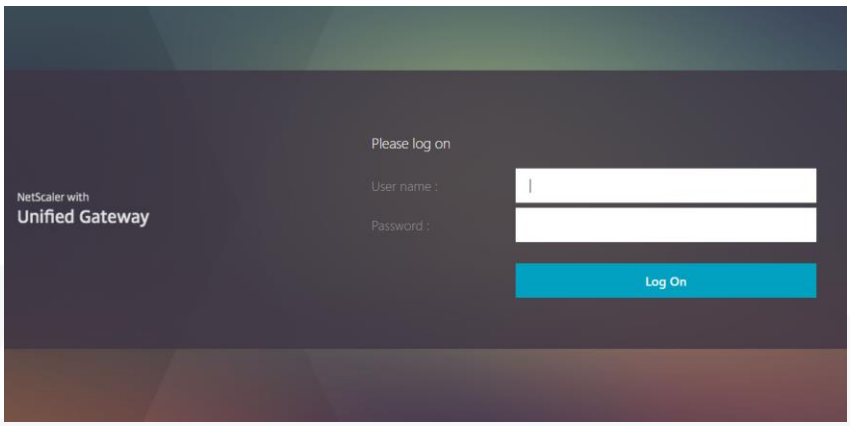


B
e sure to remove the existing LDAP Authentication server from the Virtual Server and click the Save button at the top right of the screen.

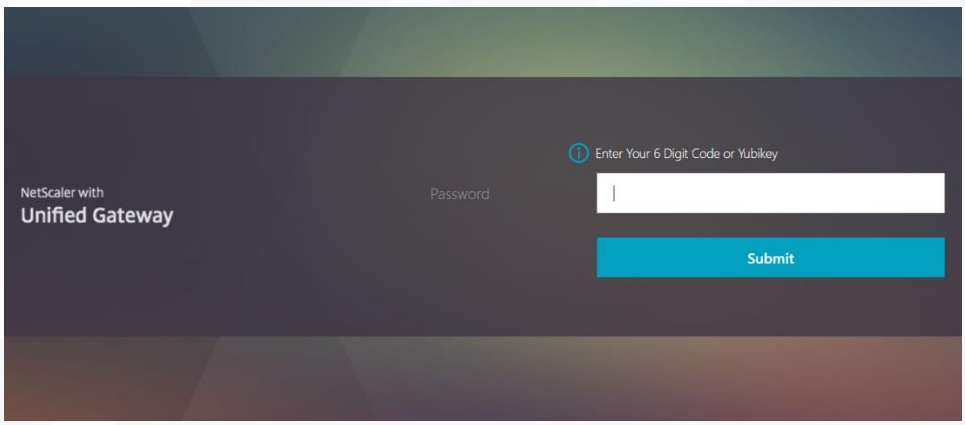
1.5 Client Logon

The following section describes the login process and demonstrates what will be presented back to the user.

- Browse to your Netscaler Virtual IP or hostname
- Enter in your username from Active Directory or Local Directory Service account
- Enter your domain password and click Log On



- Dependent on the authentication type you have configured within SecurAccess, you will either receive a PUSH notification to your Apple or Android phone or presented with a login page requesting the 6-digit token (Received via SMS or Email)
- Enter the one-time code received or enter the code from the soft token or Yubikey.



Once entered, you will be taken to your Citrix StoreFront Server.

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com