Sentry SSO with Netscaler

Contents

Introduction

This article explains how to integrate a Citrix Netscaler with Sentry.

It focusses on the setting up of Sentry and the modification of the login pages to support the Sentry integration.

It assumes knowledge of how to configure the Netscaler to use Sentry as a RADIUS authentication server. Details of these elements can be found in the existing integration guides Category:Netscaler

For this integration it is recommended that the Swivel Radius server is the only authentication required for this realm.

Overview

The integration works by

1. Configuring the Netscaler login page to redirect the user to Sentry to authenticate
2. User authenticates at Sentry
3. User is redirected back to the Netscaler login page with a claim
4. Netscaler login page is submitted with username and claim
5. Username and claim are validated via RADIUS
6. User gains access

Therefore the following steps are required

1. Configure Netscaler Login
2. Configure Sentry to work with Netscaler login page
3. Configure Sentry to accept RADIUS requests from Netscaler

Configure Netscaler Login

In order to make the Netscaler page work in the desired way once the page has loaded the page must detect if the user has been redirected to this page from Sentry or if the user have come directly.

If the user has come directly they need to be redirected to Sentry. If they have been directed from Sentry the login form needs to be populated and submitted.

This is the required snippet that needs adding to the head section of the login pages.

The only modification required is to change SENTRYURL for the actual public url of your sentry install.

Note the **applicationNameNoSAML=NetscalerVPN**. This is important as this application name must match the settings on Sentry

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
 window.location.replace("https://SENTRYURL/noSamlEndPoint?returnurlNoSAML="
 + window.location.href + "&applicationNameNoSAML=NetscalerVPN" );
}
var QueryString = function () {
 // This function is anonymous, is executed immediately and
 // the return value is assigned to QueryString!
 var query_string = {};
 var query = window.location.search.substring(1);
 var vars = query.split("&");
 for (var i=0;i<vars.length;i++) {
   var pair = vars[i].split("=");
        // If first entry with this name
   if (typeof query_string[pair[0]] === "undefined") {
     query_string[pair[0]] = pair[1];
        // If second entry with this name
   } else if (typeof query_string[pair[0]] === "string") {
     var arr = [ query_string[pair[0]], pair[1] ];
     query_string[pair[0]] = arr;
        // If third or later entry with this name
   } else {
     query_string[pair[0]].push(pair[1]);
   }
 }
   return query_string;
} ();

$(document).ready(setTimeout(function(){
  usernamePassedIn = QueryString["username"];
  passwordPassedIn = QueryString["password"];
  claimPassedIn = QueryString["claim"];
  if(typeof claimPassedIn == 'undefined') {
   redirect();
  } else {
```

```
   $('[name=passwd]').val(claimPassedIn);
   $('[name=login]').val(usernamePassedIn);
   //$('[name=passwd1]').val(claimPassedIn);
   document.getElementsByName("vpnForm")[0].submit();
}
},0));
</script>
</head>
```

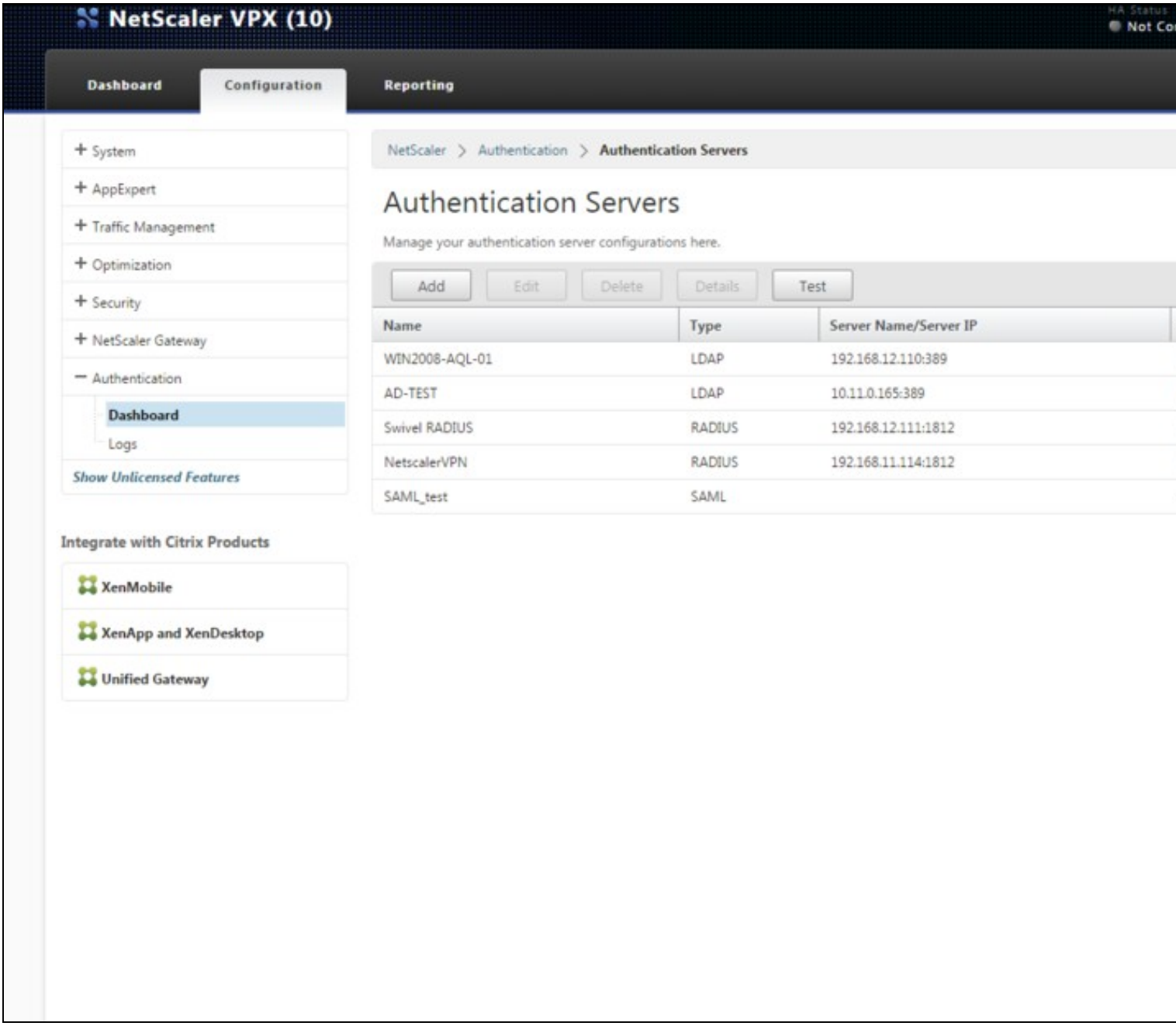
After setting the Script on the index page (in the script tag) you have to also add a form with three input fields as below

```
<form action="/cgi/login">
    <input id="login" name="login" data-swivel="username">
    <input id="passwd" name="passwd" data-swivel="password">
    <input id="passwd1" name="passwd1" data-swivel="claim">
</form>
```

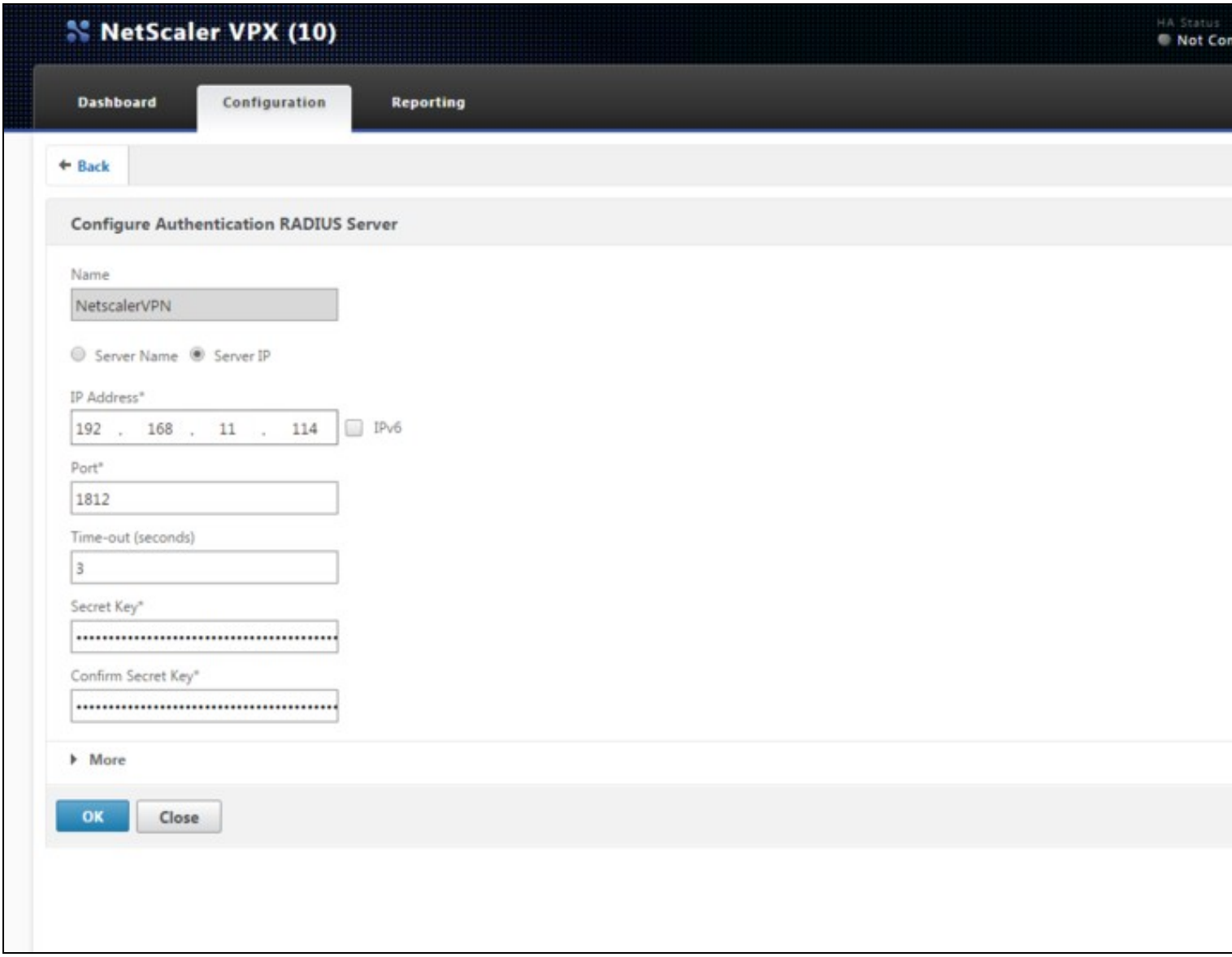
This form has to be in the body of the page (in between <body> and </body>) The login page can be found on your Netscaler server usually at the path /netscaler/ns_gui/vpn/index.html

Configuring Netscaler

After you have successfully modified the login page, you should configure the Netscaler by adding a new Radius server. To do so you have to click on the Authentication -> Dashboard.

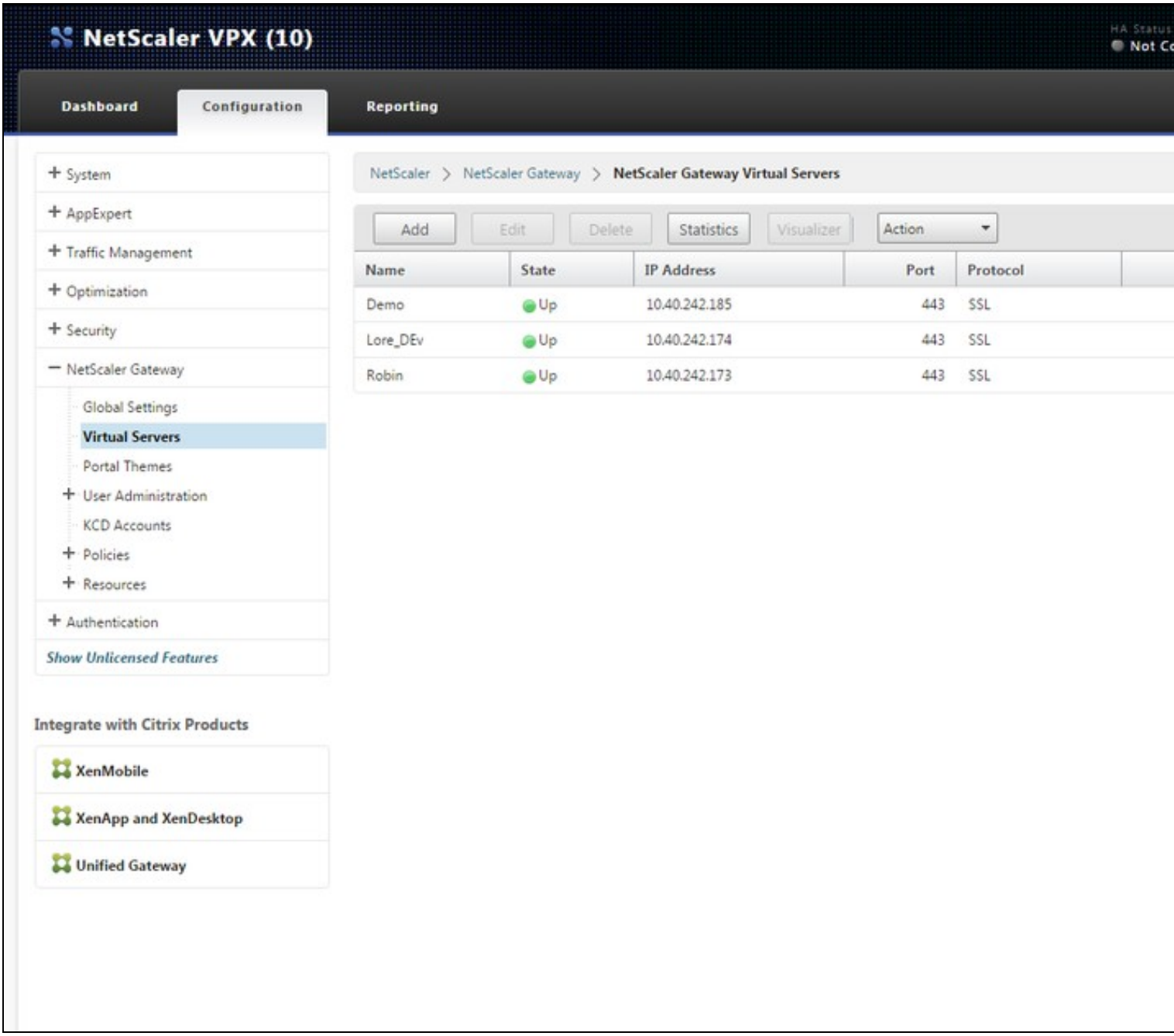


Click on the "Add" button and Add a RADIUS Server by adding an IP Address or Server Name Port, Time-out and secret (Secret should be the same as on the Sentry Core). It should look similar to the screenshot below:

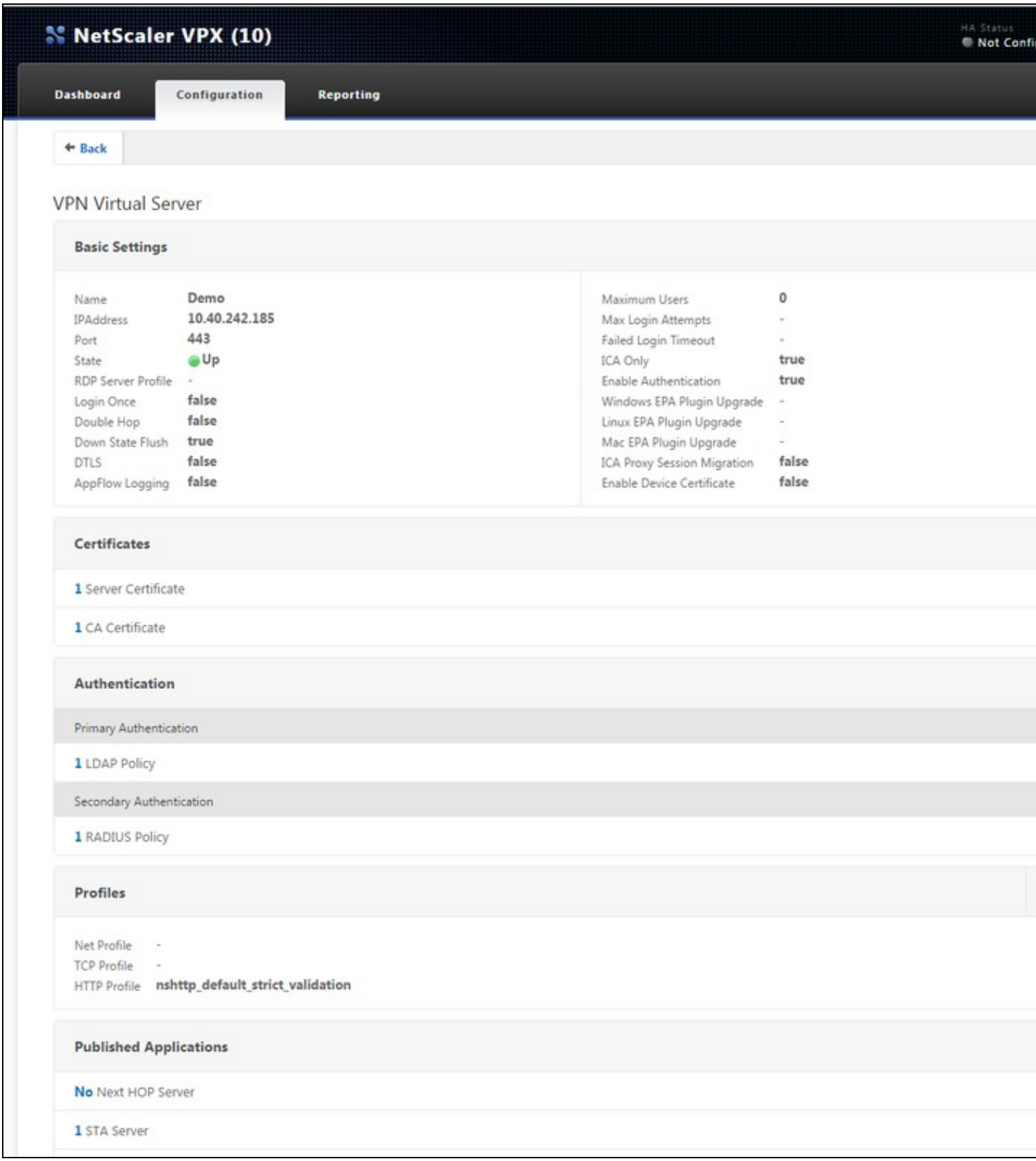


After you have added a radius server you should be able to see if Netscaler can connect to it (if you have created it prior to this) on the Authentication Servers screen in the Status column.

To set up the authentication servers to your Virtual Server or to create a Gateway Virtual Server you have to click on NetScaler Gateway -> Virtual Server

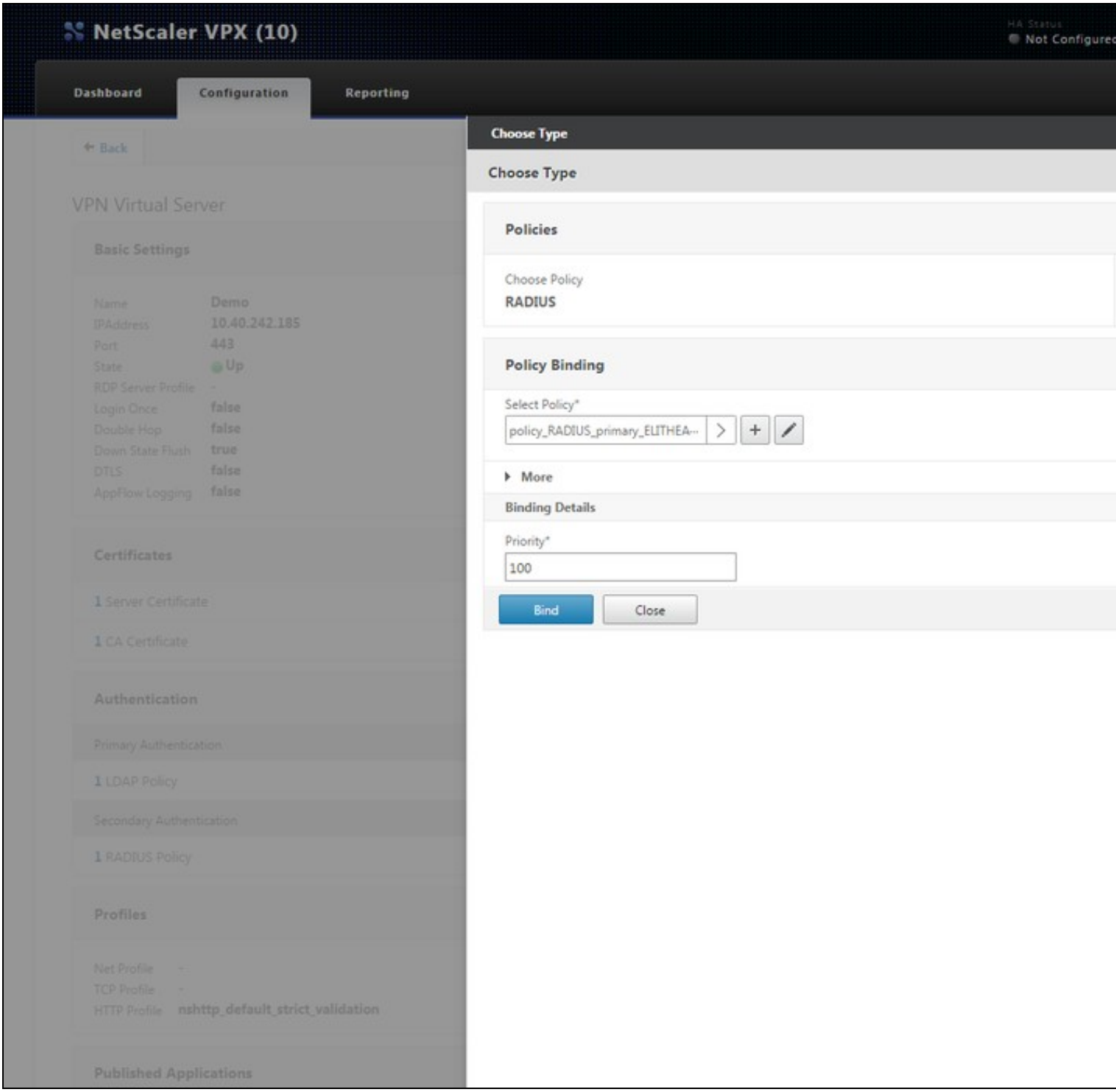


On this screen (as above) you should be able to to edit or Add a new Gateway Virtual Server to Add a new server you have to click on the "Add" button, to edit the server you have to select the server by clicking on it once and clicking on the "Edit" button. In this example we are editing the already created Virtual server.

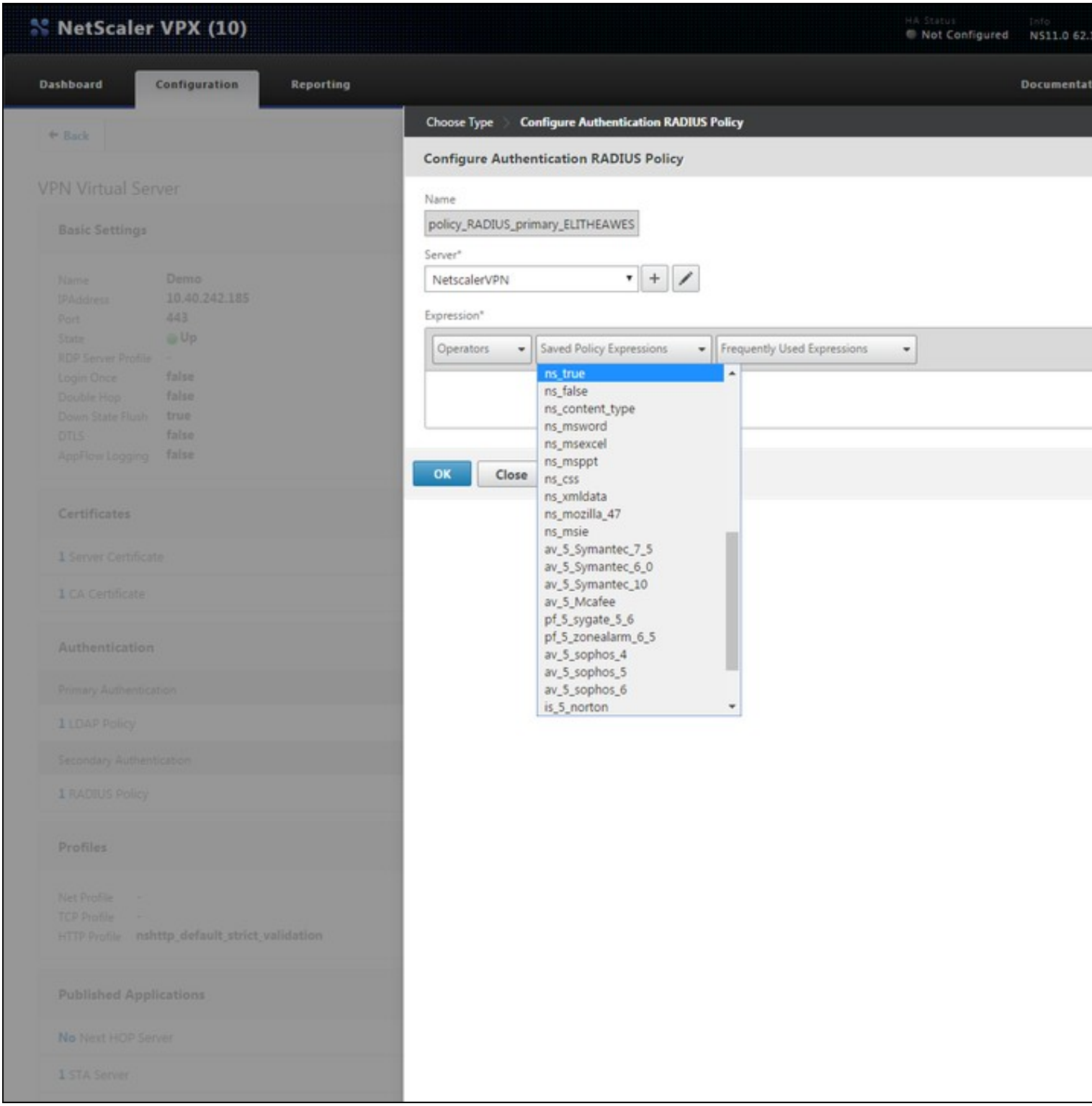


You will see a screen similar to the one above, you have to set the Primary Authentication method to be your newly created Radius Server. To Do so you have to click on "+" on the Primary Authentication. On the new window that pops up you have to select the Policy as being RADIUS and type as being Primary.

On the next page you have to select the policy. You can click on the arrow button like on the screenshot below, and select your created Radius Server.



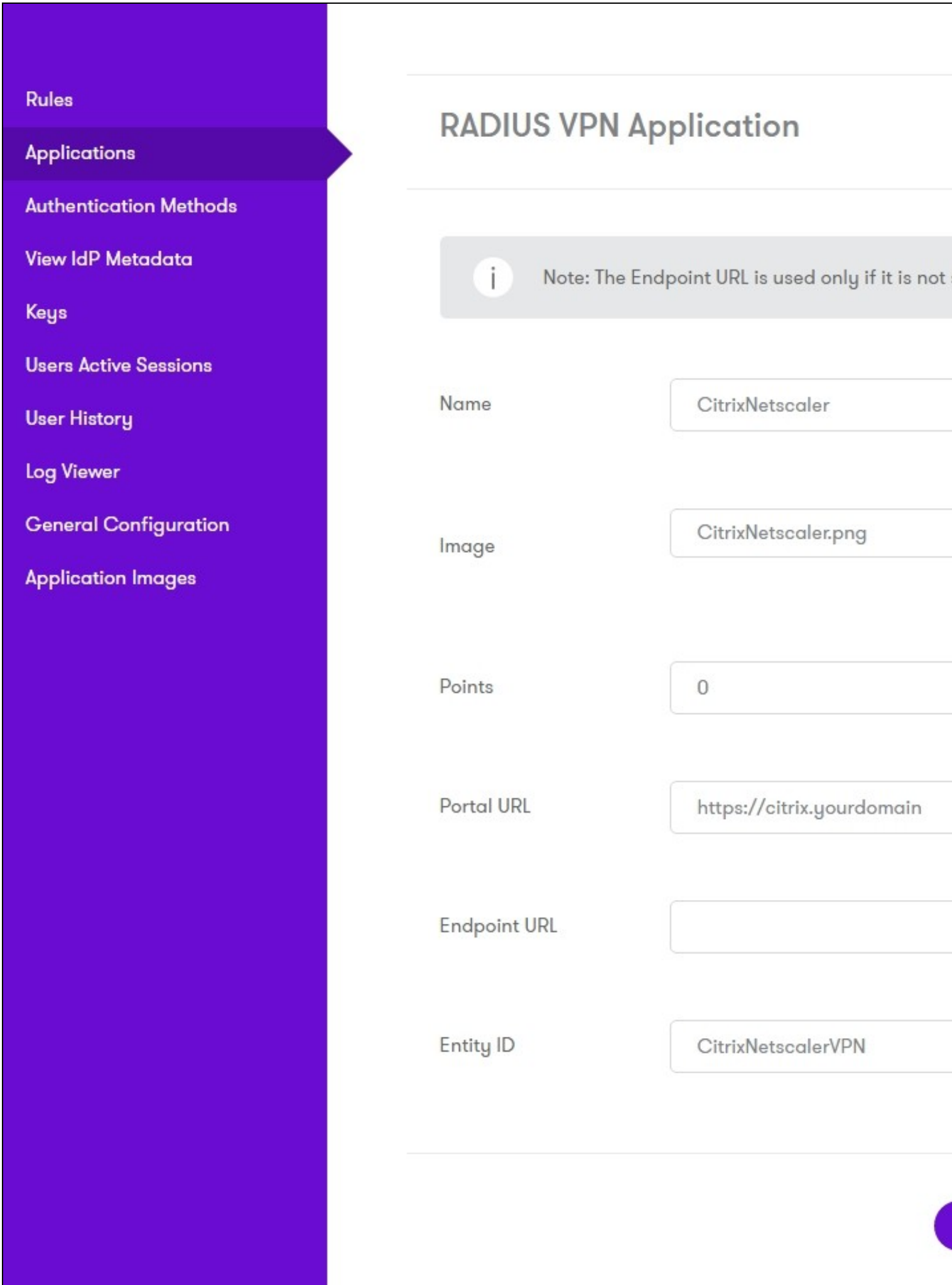
After selecting the radius you have to click on the edit button (pencil) and on the edit screen you have to change the Expression to "ns_true" which might be selectable from the Saved Policy Expressions column as you can see from the screenshot below.



After setting the Expression click OK. Set Priority to 100 and click Bind. Now your Netscaler should be set up.

Configuring Sentry Login

The Netscaler VPN needs to be added to Sentry as an Application.


Rules
Applications
Authentication Methods
View IdP Metadata
Keys
Users Active Sessions
User History
Log Viewer
General Configuration
Application Images
RADIUS VPN Application
Note: The Endpoint URL is used only if it is not
Name
CitrixNetscaler
Image
CitrixNetscaler.png
Points
0
Portal URL
https://citrix.yourdomain
Endpoint URL
Entity ID
CitrixNetscalerVPN

The following entries are required.

- **Name:** This must match the name in the redirect url, eg NetscalerVPN
- **Image:** CitrixNetscaler.png (Selected by default)
- **Points:** Number of points required to access the VPN, refer to Sentry User guide
- **Portal URL:** This is the URL of the Netscaler login page configured to work with Sentry
- **Endpoint URL:** N/A
- **Entity ID:** Should match Name.

Configuring Sentry RADIUS

To complete the integration the Netscaler VPN must be added as a NAS on the Sentry server.

The key settings are

- Identifier Must match the Name on Sentry login, eg NetscalerVPN
- Hostname Must match IP of Netscaler VPN

Two stage auth, Check Password with repository should be set to NO

SSO

For RADIUS VPN applications the login page will be displayed although Sentry has been configured with SSO enabled. That attribute just applies for SAML applications.

Authentication with AD/LDAP and Radius

To be able to authenticate with both AD/LDAP and Radius when logging in you have to add few minor changes. You have to modify the script which you have added at this step

You have to uncomment one line:

```
//$('[name=passwd1]').val(claimPassedIn);
```

by removing double forward slashes in front of the $ sign, so it would look like below:

```
$('[name=passwd1]').val(claimPassedIn);
```

You also have to change the password line above the uncommented code from.

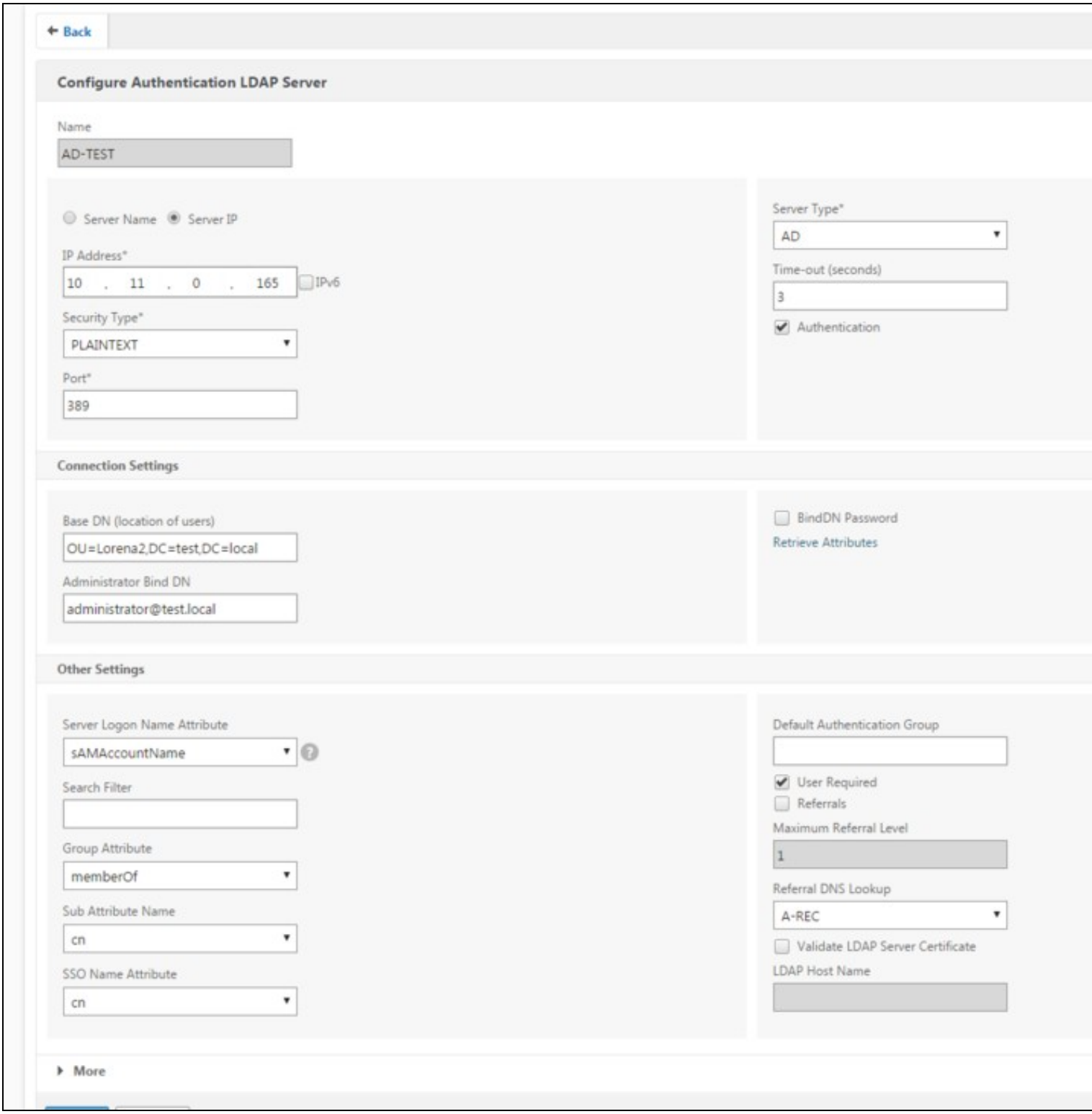
```
 $('[name=passwd]').val(claimPassedIn);
```

To the line below, in the password field we will pass now the password and the claim in the password#2 which we have uncommented above.

```
$('[name=passwd]').val(passwordPassedIn);
```

You have to re-upload/update the page to the Netscaler.

After updating the page, you have to configure AD/LDAP on the NetScaler. Fallow to the Authentication -> Dashboard and click on Add. You have to enter your AD/LDAP settings and the page should resemble to something similar to the screenshot below.



After adding an AD/LDAP you can check if NetScaler can connect to it (Status has to be Up on the Authentication Servers page)

You have to go to the Virtual Server and modify the settings for your virtual server to set AD/LDAP to be the primary authentication method and RADIUS to be Secondary. Follow the same steps to add the authentication methods as on here except that the Expression for AD-TEST should be "REQ.HTTP.HEADER User-Agent NOTCONTAINS Receiver" and Expression for RADIUS should be also "REQ.HTTP.HEADER User-Agent NOTCONTAINS Receiver".

This way when you will try to authenticate the password will be checked with AD/LDAP server and the One Time Code will be checked with the RADIUS Server (Sentry Core)

Testing

- Goto to Netscaler login url
- User redirected to Sentry, user should be prompted for credentials
- Supply credentials

Should see Sentry logs including

```
Login successful for user: username
SSO_CLAIM_CREATED_FOR_USER, username
```

- User should be redirected to Netscaler VPN
- User should gain access

Logs should include

```
NetscalerVPN:Processing user username as channel CLAIM
NetscalerVPN:Login successful for user: username
```

Troubleshooting

The scripts on the login page work by injecting values into the login page and submitting this page. To work therefore the standard login page must have a form called vpnForm that has an input field called login for the username and an input field called passwd for the password as shown in the javascript.

By "called" the html must have the name attribute set to this value