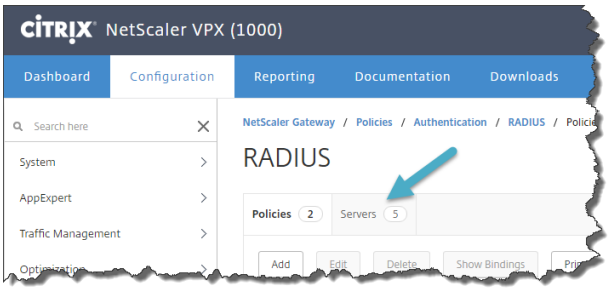
Netscaler configuration

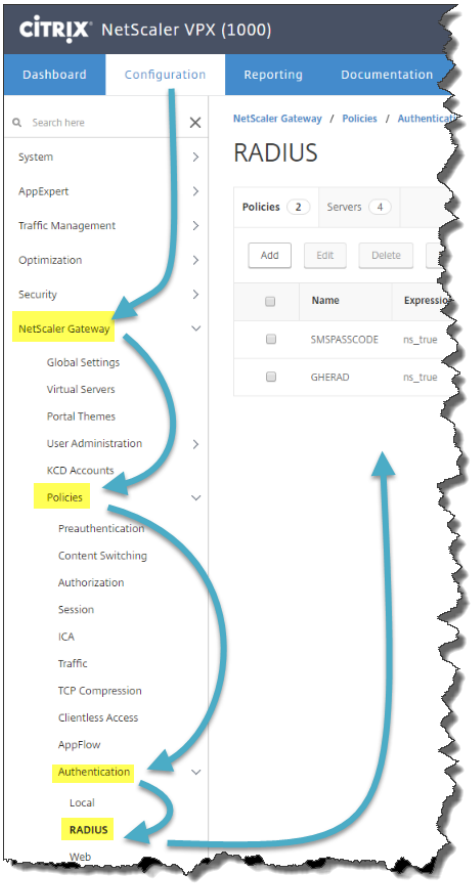
Contents

Configuration of the virtual server with a Radius authentication Server and Radius policy.

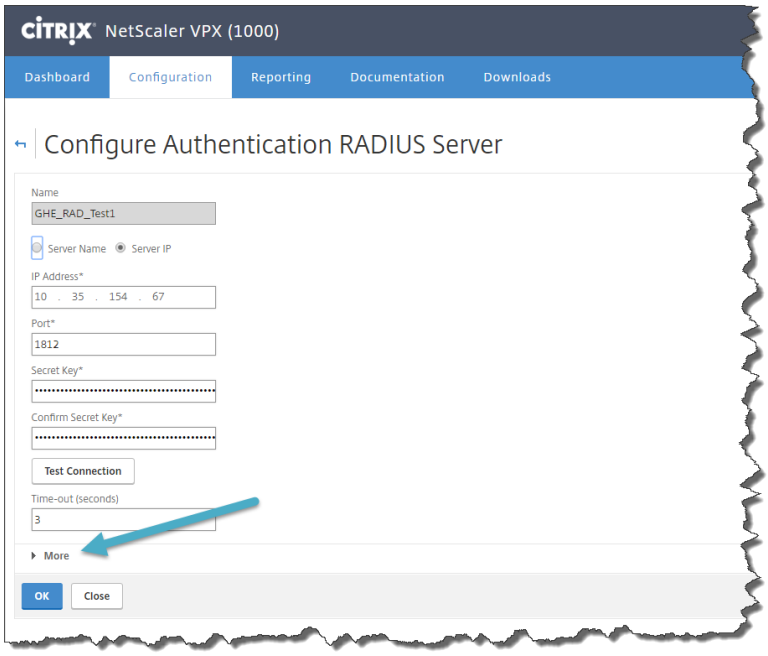
Create an Authentication server

Configure the Citrix Netscaler virtual server with a radius authentication Server. You can create a radius authentication server here “Configuration, Netscaler Gateway, Policies, Authentication, Radius". In the right section, please choose servers. Click Add (or modify an existing Radius authentication server)

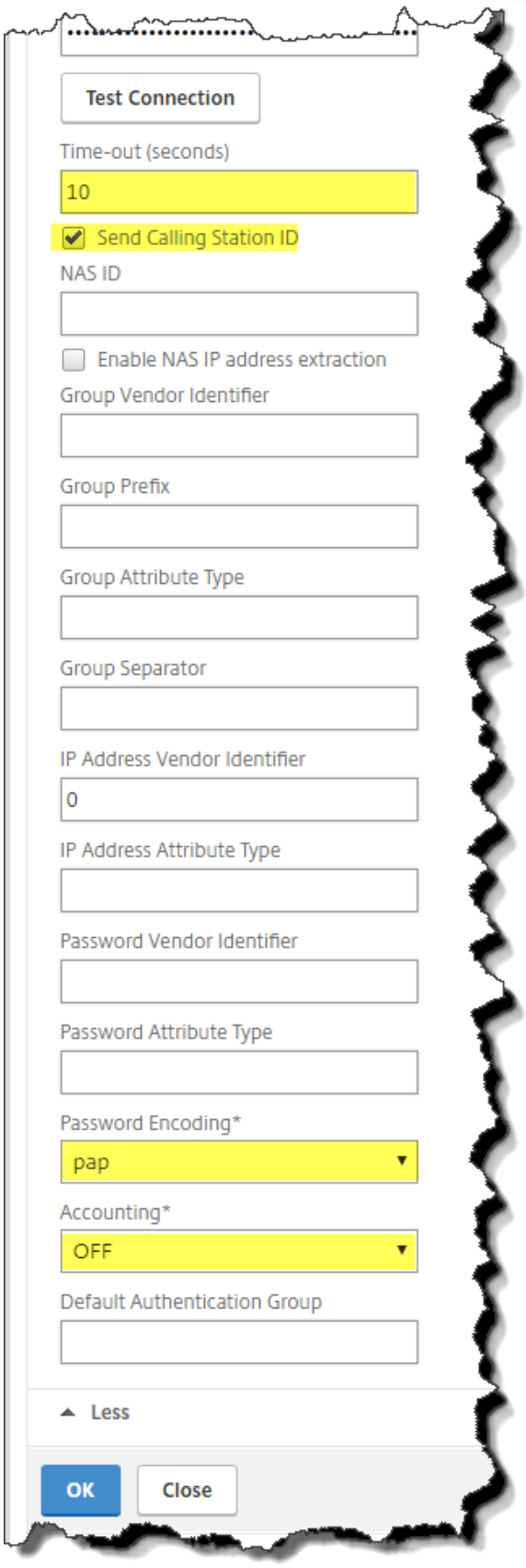




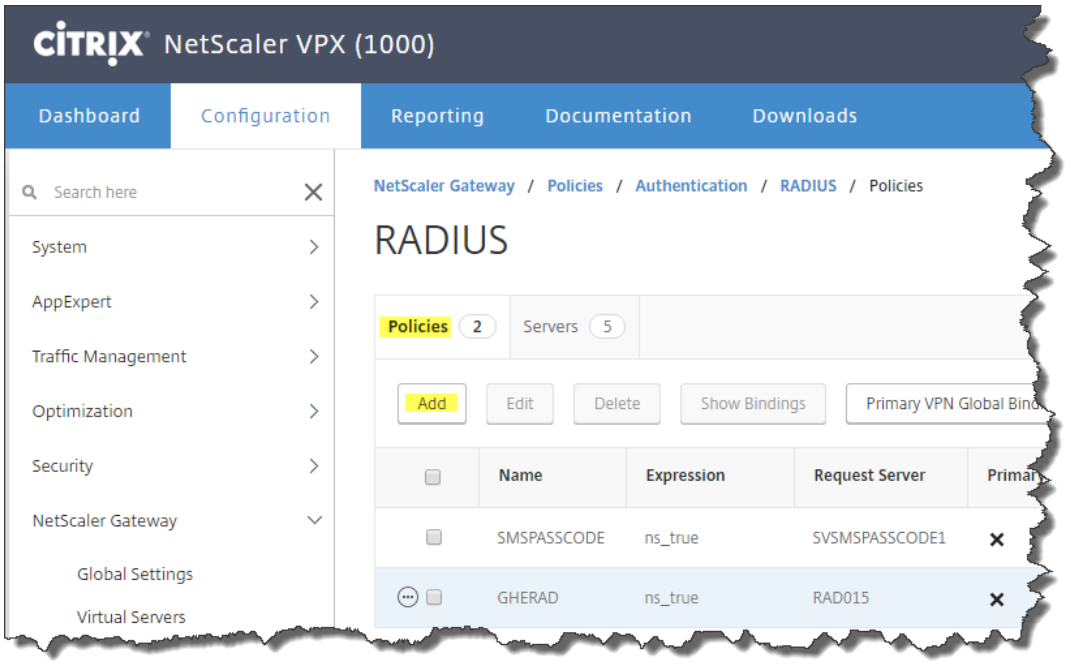
Please expand the view by clicking on “More”. The IP address is the IP of your Microsoft Radius server (NPS). The Shared secret must be the same secret as set in the Microsoft radius server (NPS) radius client (For configuration of the Microsoft radius server, please refer to SMS PASSCODE administrators guide.



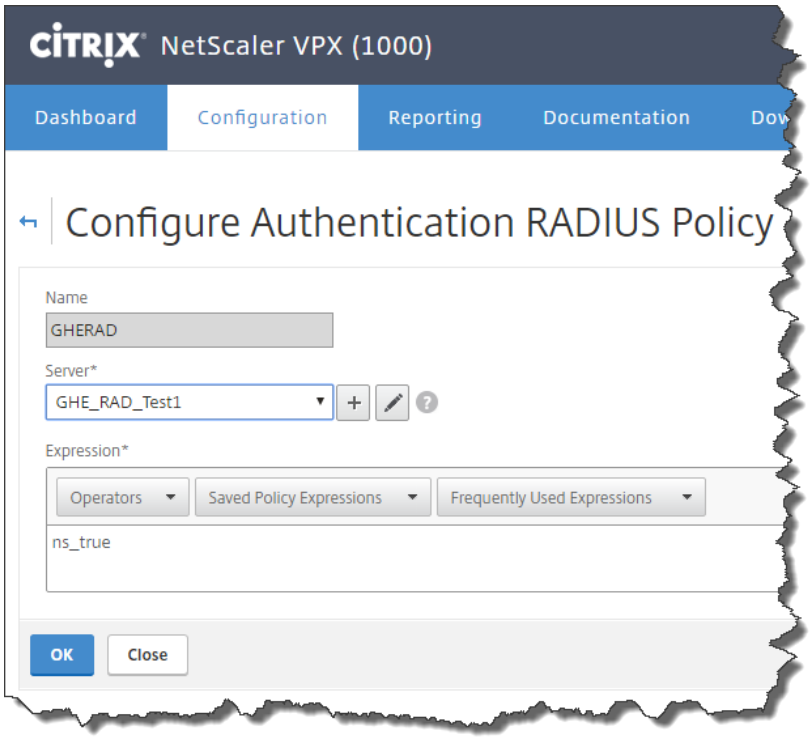
Time-out: The default value is 3 seconds, but we recommend 10 seconds, if there is no failover Radius server.
"Send Calling Station ID" should be check marked, if you want to use location aware authentication. It sends the source IP (End user IP) to the Radius server
Passcode Encoding: PAP
If you are not using "Accounting" then please set this to "Off"



Configure the Citrix Netscaler virtual server with a radius authentication policy. You can create a radius authentication policy here "Configuration, Netscaler Gateway, Policies, Authentication, Radius". Click Add (or modify an existing policy).



Now please bind the policy to the Radius Authentication server.

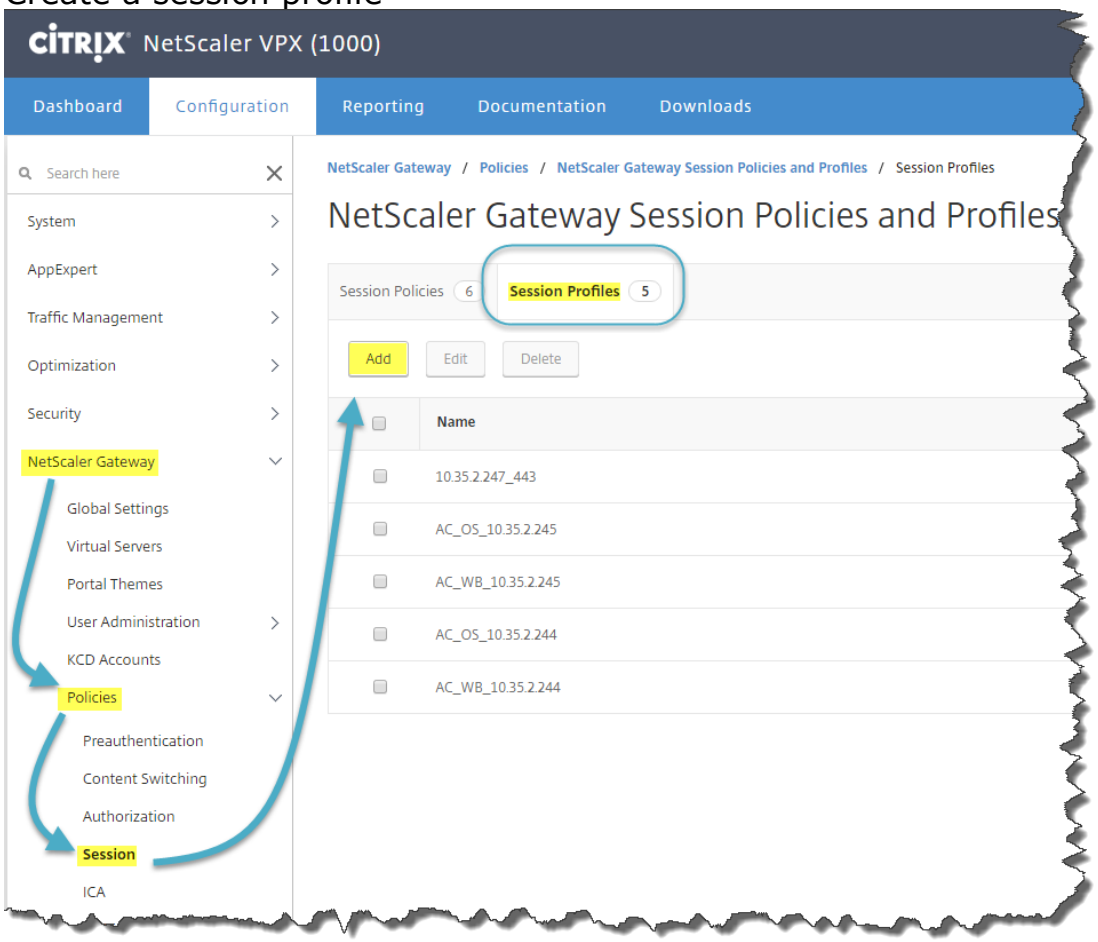


Configuration of the virtual server´s session policy and a Session Profile.

Creating the policy and profile

If you already have a session policy and a session profile, then please skip forward to the next section (Bind the session policy to the virtual server)

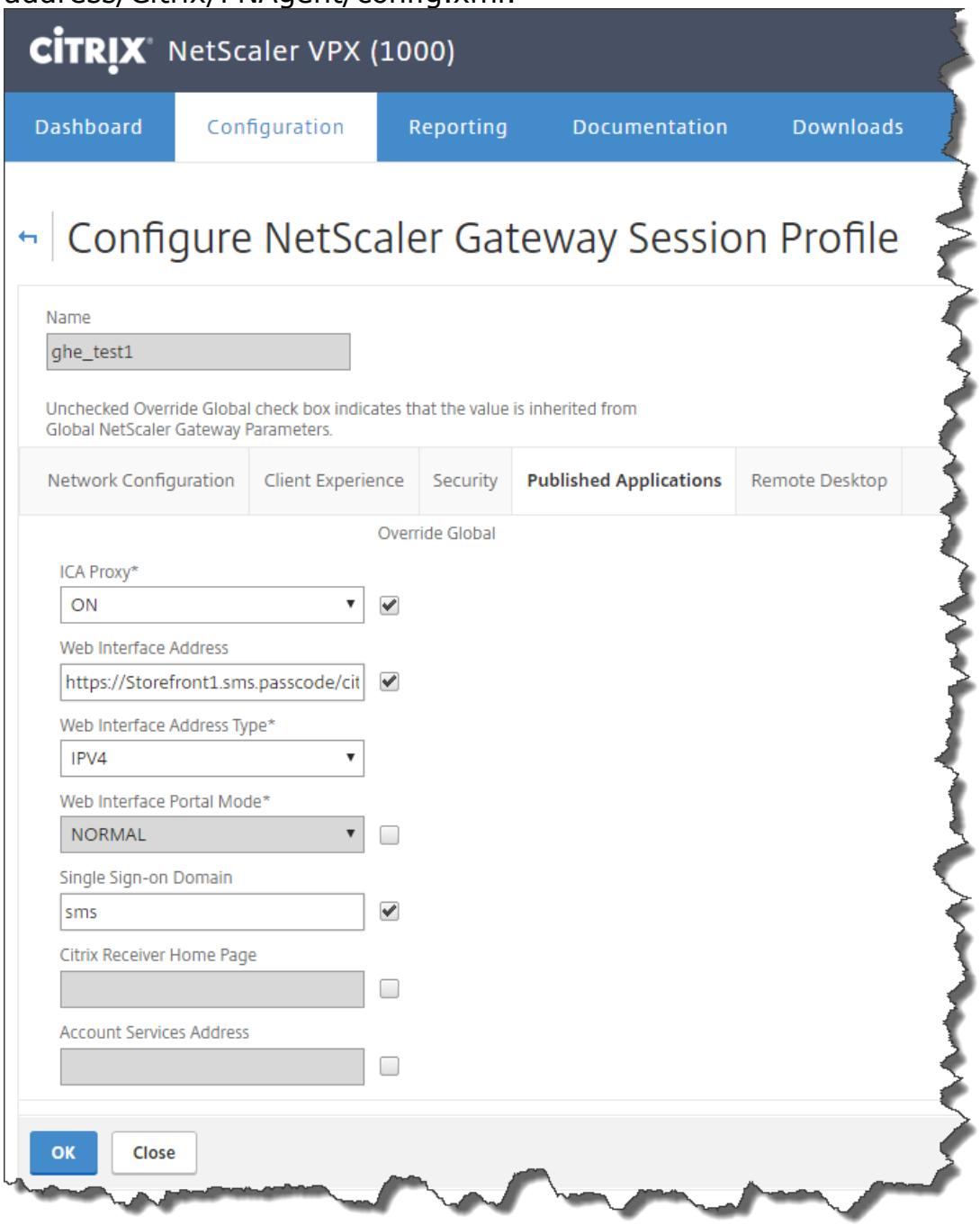
Create a session profile



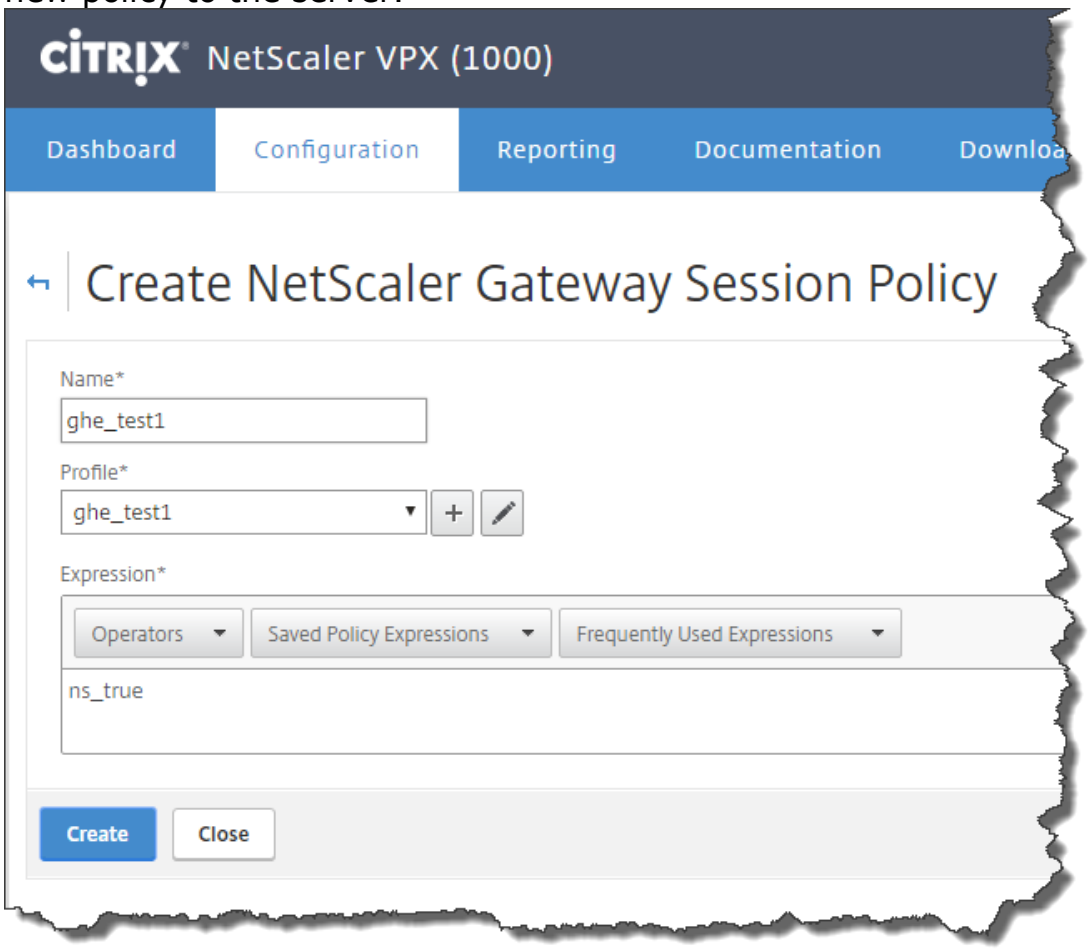
censornet.


CITRIX NetScaler VPX (1000)
Dashboard
Configuration
Reporting
Documentation
Downloads
Create NetScaler Gateway Session Profile
Name*
GHE_Test1
Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.
Network Configuration
Client Experience
Security
Published Applications
Remote Desktop
Accounting Policy
Override Global
Display Home Page
Home Page
URL for Web-Based Email
Split Tunnel*
OFF
Session Time-out (mins)
30
Client Idle Time-out (mins)
Clientless Access*
Allow
Clientless Access URL Encoding*
Obscure
Clientless Access Persistent Cookie*
DENY
Plug-in Type*
Windows/MAC OS X
Windows Plugin Upgrade
Always
Linux Plugin Upgrade
Always
MAC Plugin Upgrade
Always
AlwaysON Profile Name
Single Sign-on to Web Applications
Credential Index*
PRIMARY
KCD Account
Single Sign-on with Windows*
OFF
Client Cleanup Prompt*
ON
Advanced Settings
Create
Close

If you are publishing a Citrix Web Interface and not Storefront, then the Web Interface Address should most likely look like this: http//IP address/Citrix/PNAgent/config.xml.

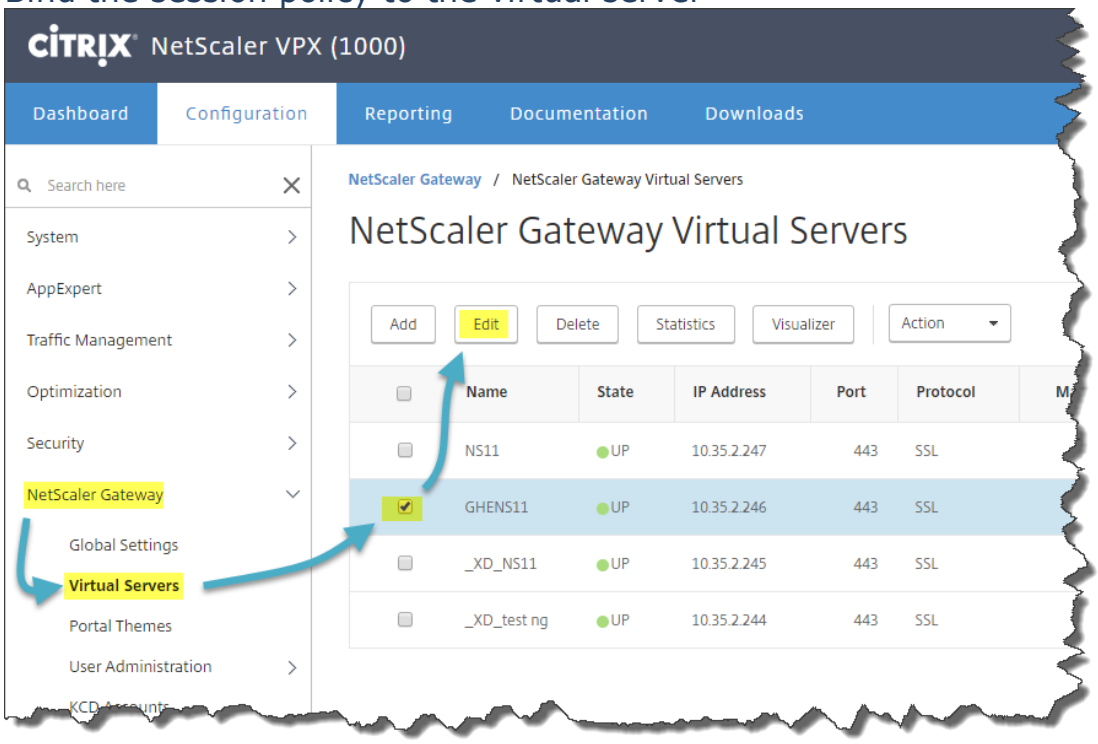


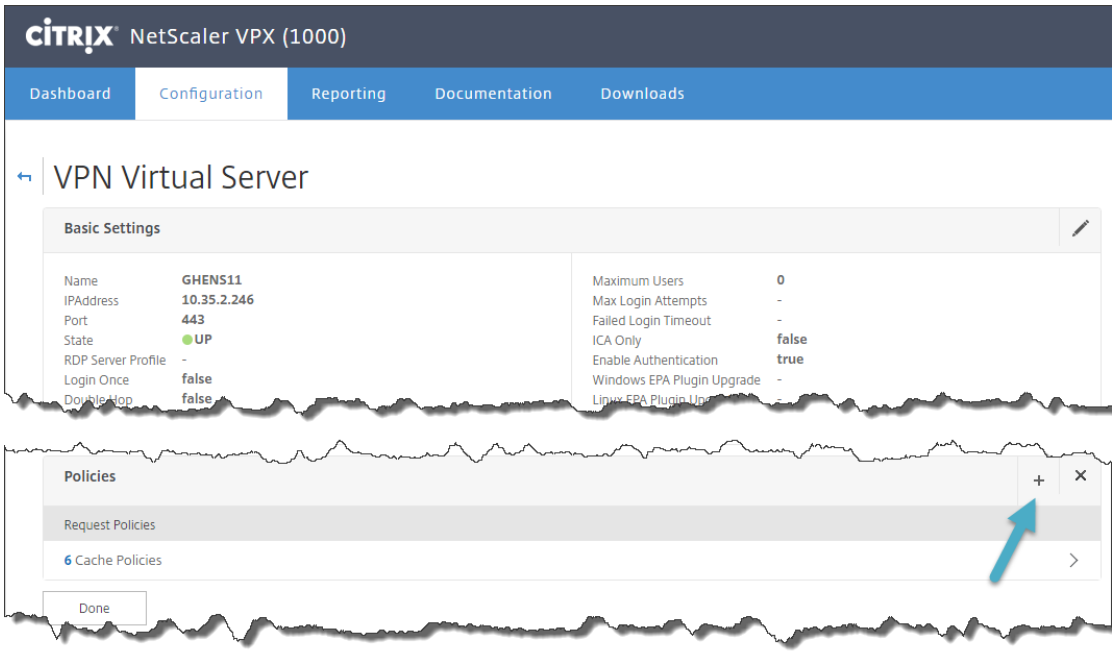
Now please create the session policy, and then you will be ready to bind your new policy to the server.



censornet.

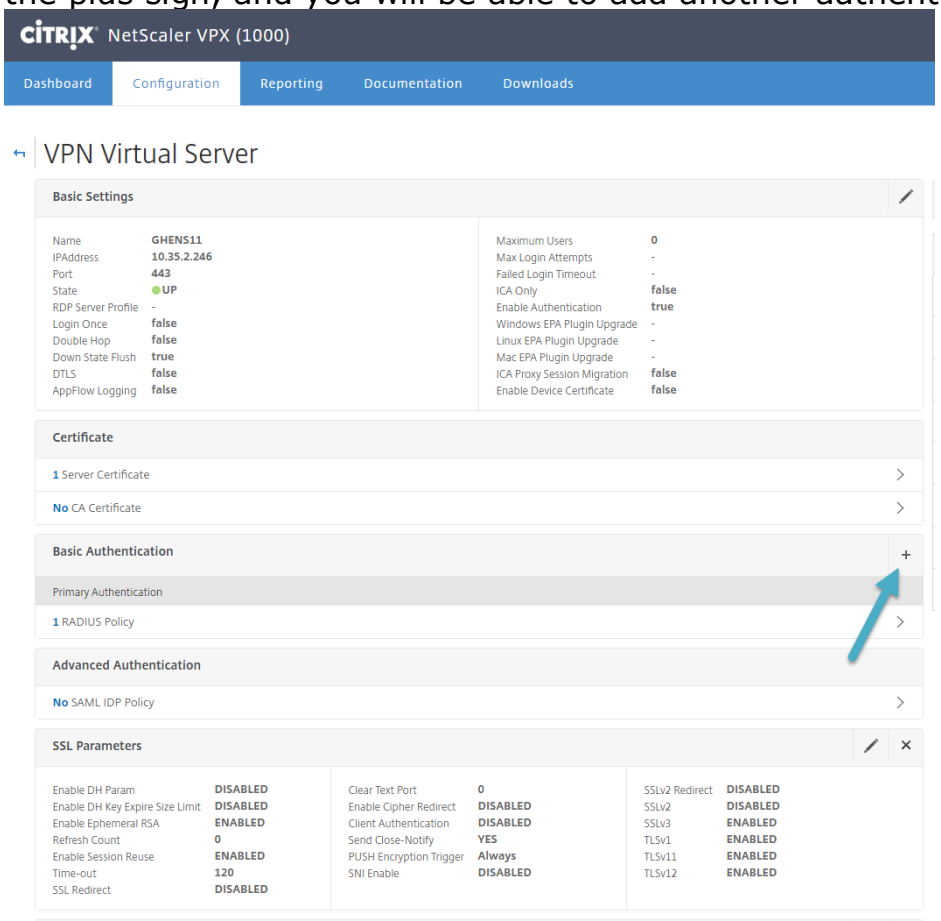
Bind the session policy to the virtual server



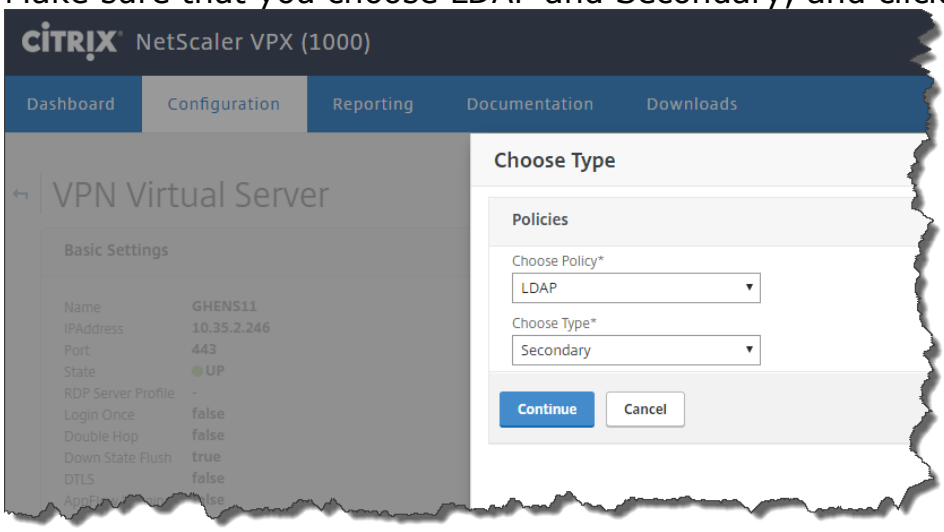


Radius and LDAP authentication, to allow for Password change (optional)

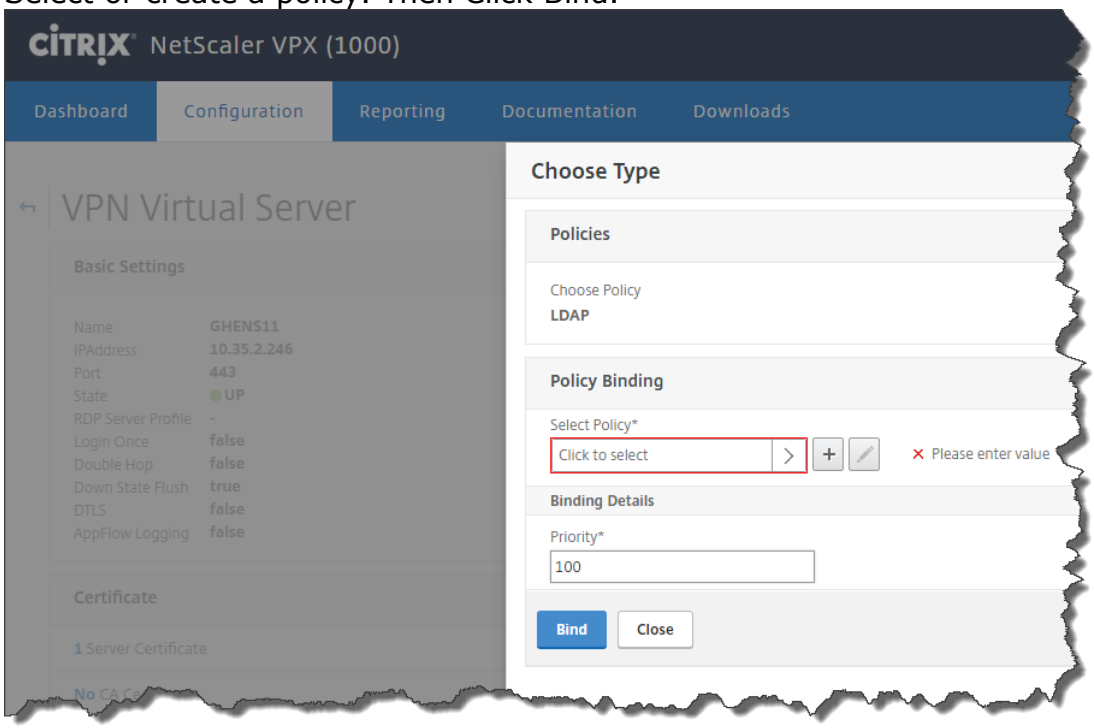
Please navigate to the virtual server. Find the Basic authentication section. Click the plus sign, and you will be able to add another authentication.



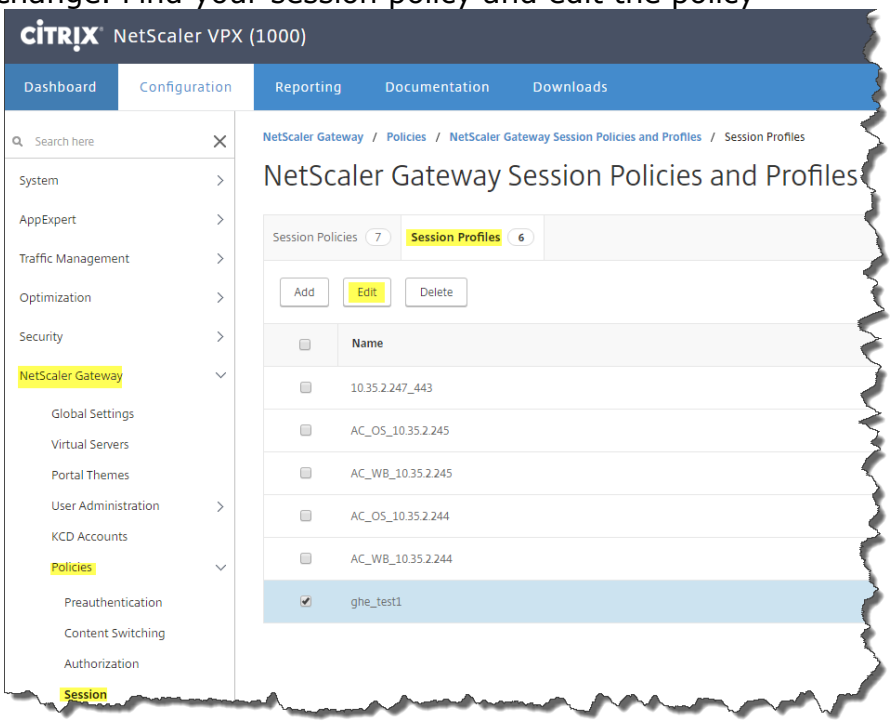
Make sure that you choose LDAP and Secondary, and click continue



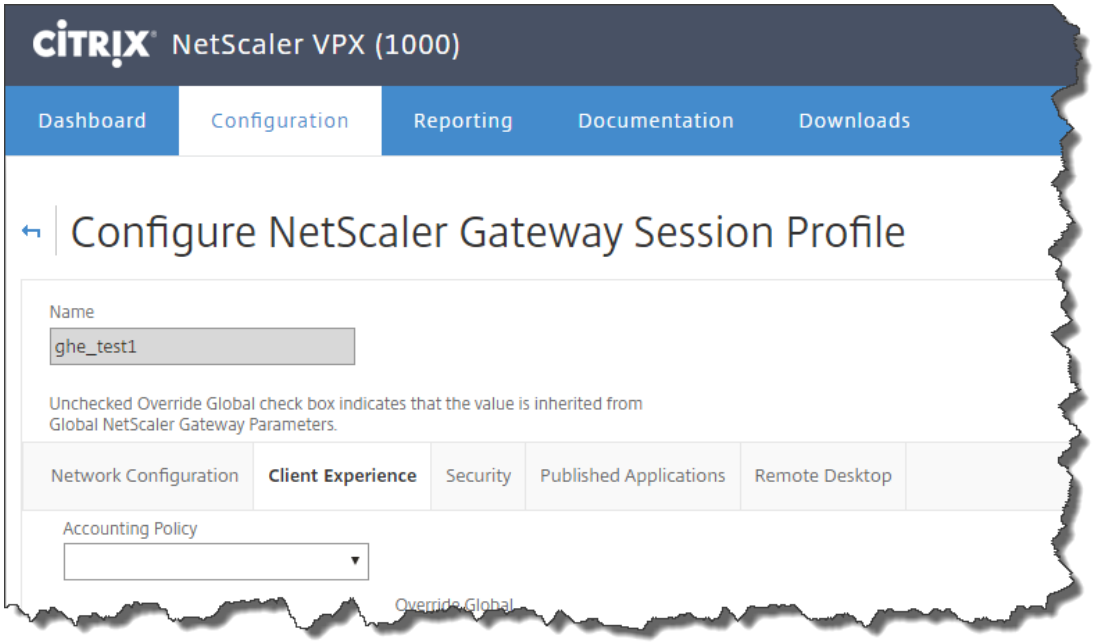
Choose Type
Select or create a policy. Then Click Bind.



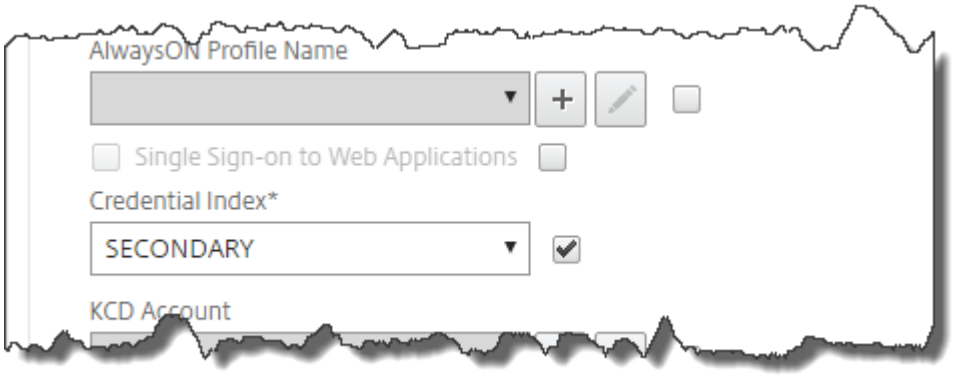
Please make sure that the session policy which redirects to Web Interface/Storefront is using SECONDARY Credential Index to make sure that SSO is working after password change. Find your session policy and edit the policy



Choose Client Experience

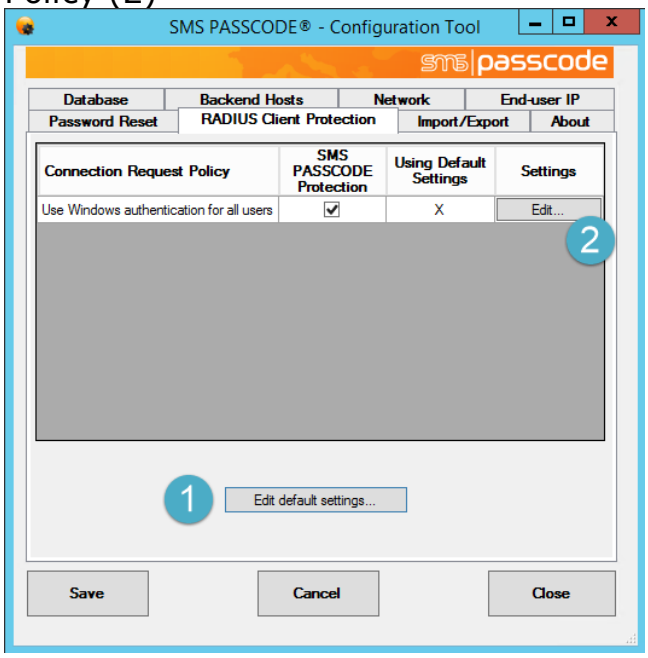


Find the Credential Index, and checkmark the checkmark box to overwrite, the default setting, and then choose SECONDARY. Now please save this.

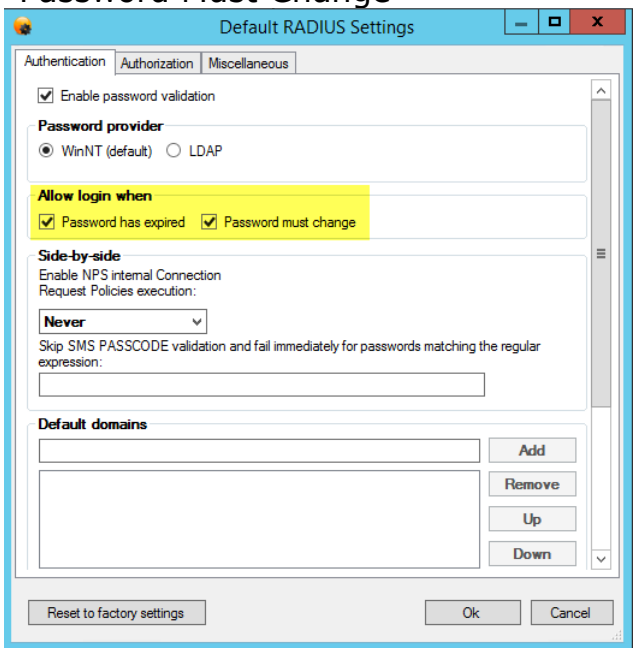


Settings in the SMS PASSCODE Configuration Tool

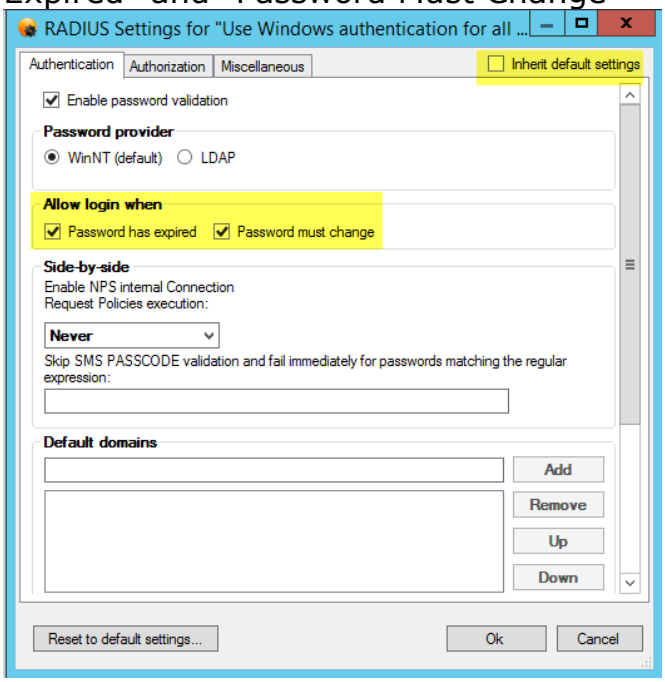
Please make sure to allow radius login with an expired password in the SMS PASSCODE configuration tool. This can be configured either as default or for a specific Connection Request Policy,
The default settings (1) and the settings for a specific Connections Request Policy (2)



In the section for Allow login when Checkmark the “Password has Expired” and “Password Must Change”



For a specific Connection Request policy, you uncheck the Inherit default settings. In the section for Allow login when Checkmark the "Password has Expired" and "Password Must Change"



Hide the secondary password field

When using both Radius and LDAP e.g. if you allow for Password change, you must use the rewrite feature in Netscaler to avoid two password fields shown. The Netscaler will automatically use the primary password in the secondary if you leave this field blank. If you do not have license to use the Rewrite feature, then you can edit login.js Please do not edit the login.js if you use the Rewrite feature.

If you are using Netscaler 12 and at the same time is using the new Netscaler 12 theme, then please pay attention to the following section.

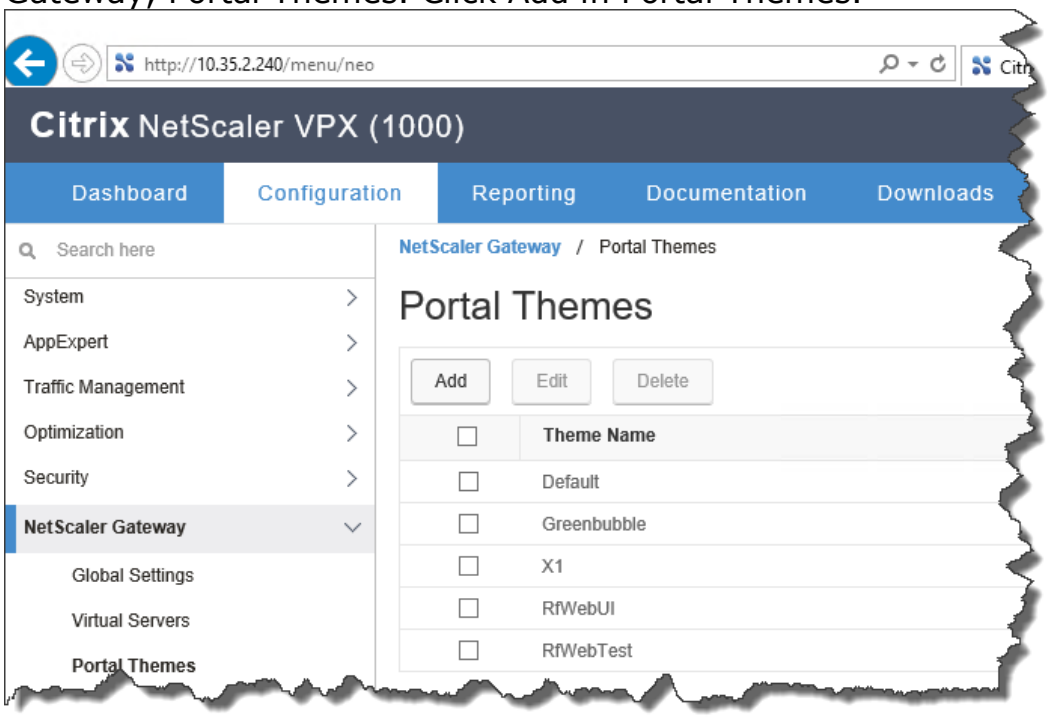
If you are not using the new theme in Netscaler 12, then please pay attention to the re-write section.

If you are using both kind of themes, then please pay attention to both the following section and the re-write section.

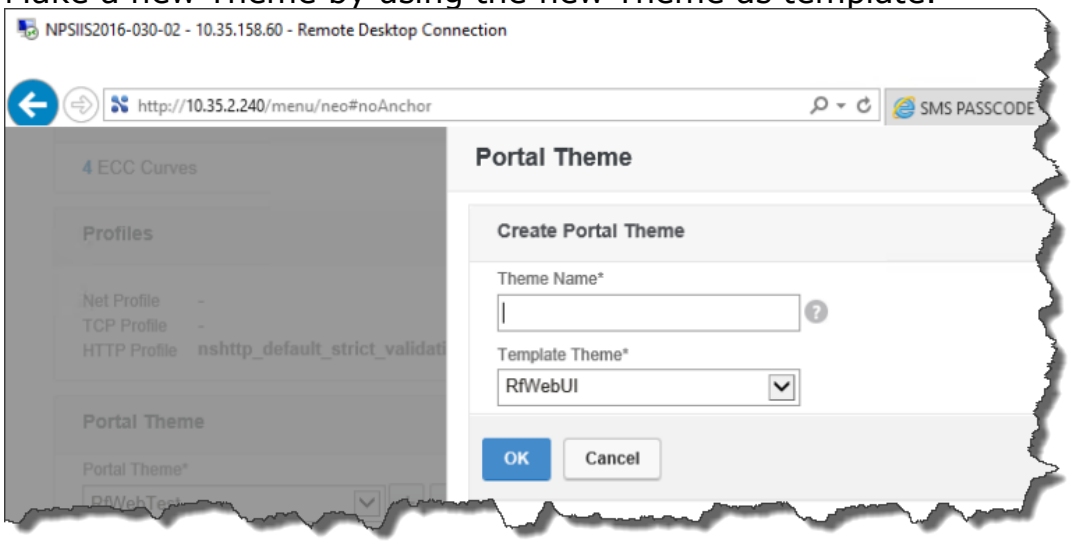
censornet.

For Netscaler 12 with new Netscaler 12 Theme.

The Netscaler 12 with the new themes for Netscaler 12 will not hide the secondary password field, as described above. You can do this in another way. First step is to make a copy of the theme. Please navigate to Netscaler Gateway, Portal Themes. Click Add in Portal Themes.



Make a new Theme by using the new Theme as template.

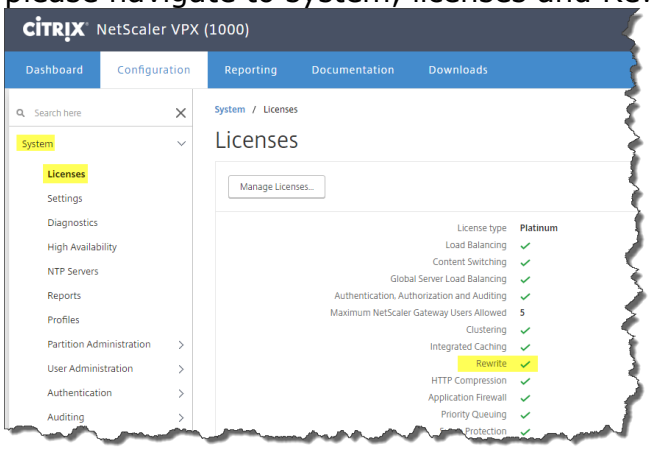


Make sure that your theme is the new theme and save your running configuration. Be patient, for some reason this change can take a couple of minutes to update. Drink a cup of coffee and then test it.
Now run this in a Netscaler command prompt. This will configure rewrite policy for your. Perhaps do some name check on the Netscaler Gateway Virtual Server.

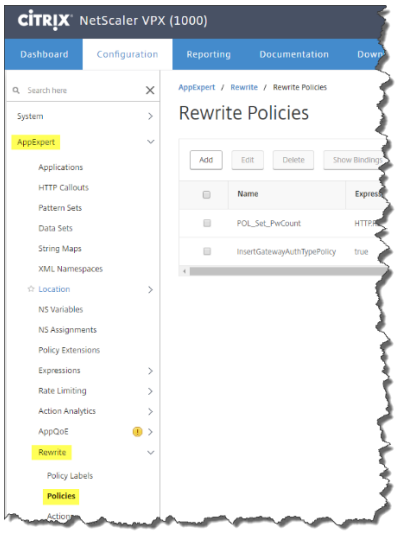
```
add rewrite action RWA-RES-REMOVE_2ND_PASSWORD replace_all "HTTP.RES.BODY(99999)"
"\"\\r\\n\"+\n\"<style type=\\\"text/css\\\">\\r\\n\"+\n\"[for=\\\"passwd1\\\"] { display:
none;}\\r\\n\"+\n\"#passwd1 { display: none;
}\\r\\n\"+\n\"</style>\\r\\n\"+\n\"\\r\\n\"+\n\"</body>\\r\\n\"+\n\"</html>\\r\\n\"" -search
"text(\"</body>\n</html>\")"
add rewrite policy RWP-RES-REMOVE_2ND_PASSWORD
"HTTP.REQ.URL.PATH_AND_QUERY.SET_TEXT_MODE(IGNORECASE).EQ(\"/logon/LogonPoint/index.html\")
" RWA-RES-REMOVE_2ND_PASSWORD
bind vpn vserver <NSGW VSERVER> -policy RWP-RES-REMOVE_2ND_PASSWORD -priority 80 -
gotoPriorityExpression NEXT -type RESPONSE
```

Use of the rewrite feature

Your Netscaler must be licensed to use rewrite to use this approach. To verify this, please navigate to system, licenses and Rewrite must have a green checkmark.

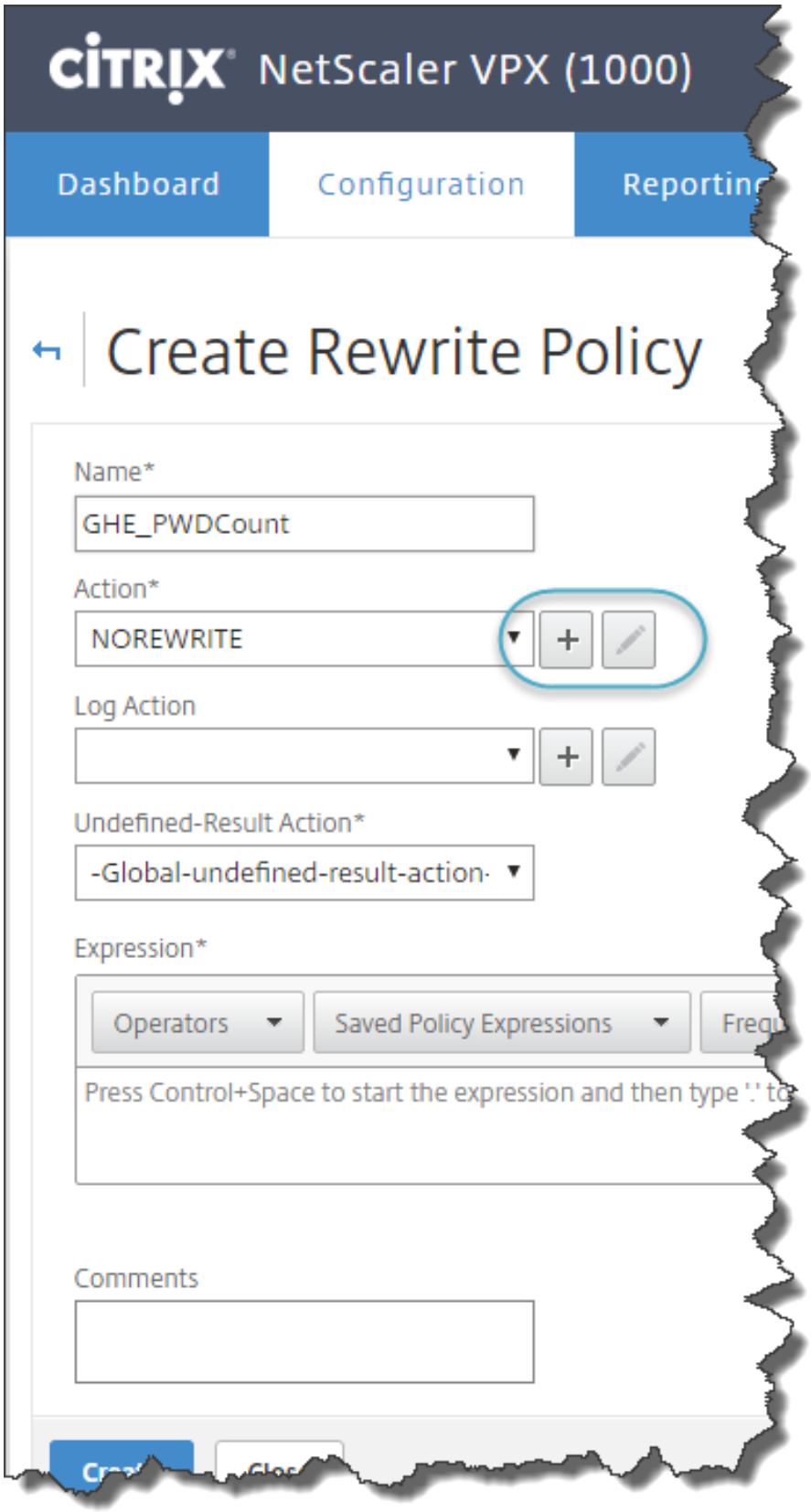


To create a rewrite policy and rewrite action please navigate to AppExpert -> Rewrite -> Policies. Click Add to add a new policy. In the new policy, you need to add an Action.



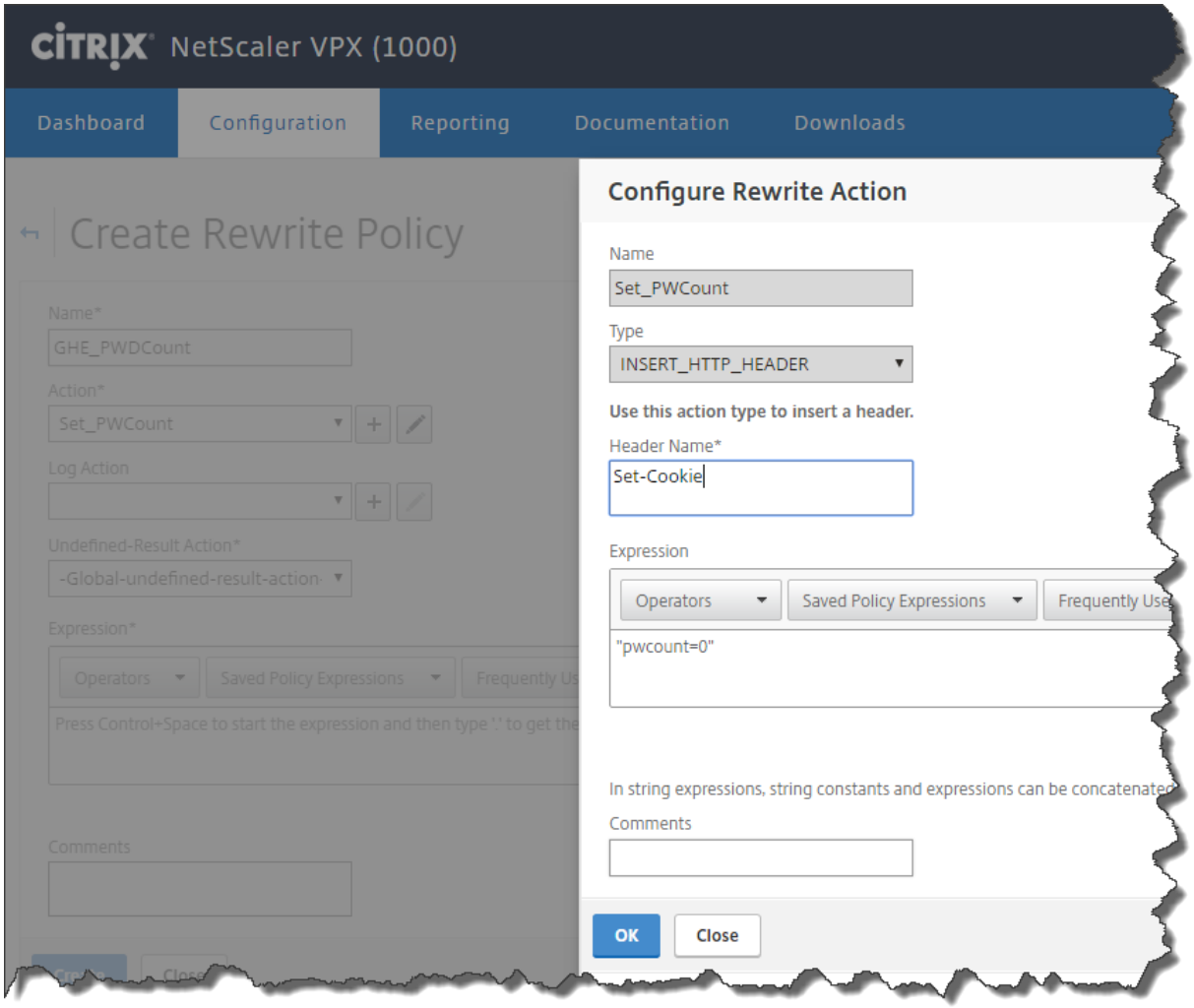
Please assign an Action or create an Action. Click the plus sign to create a new action.

censornet.



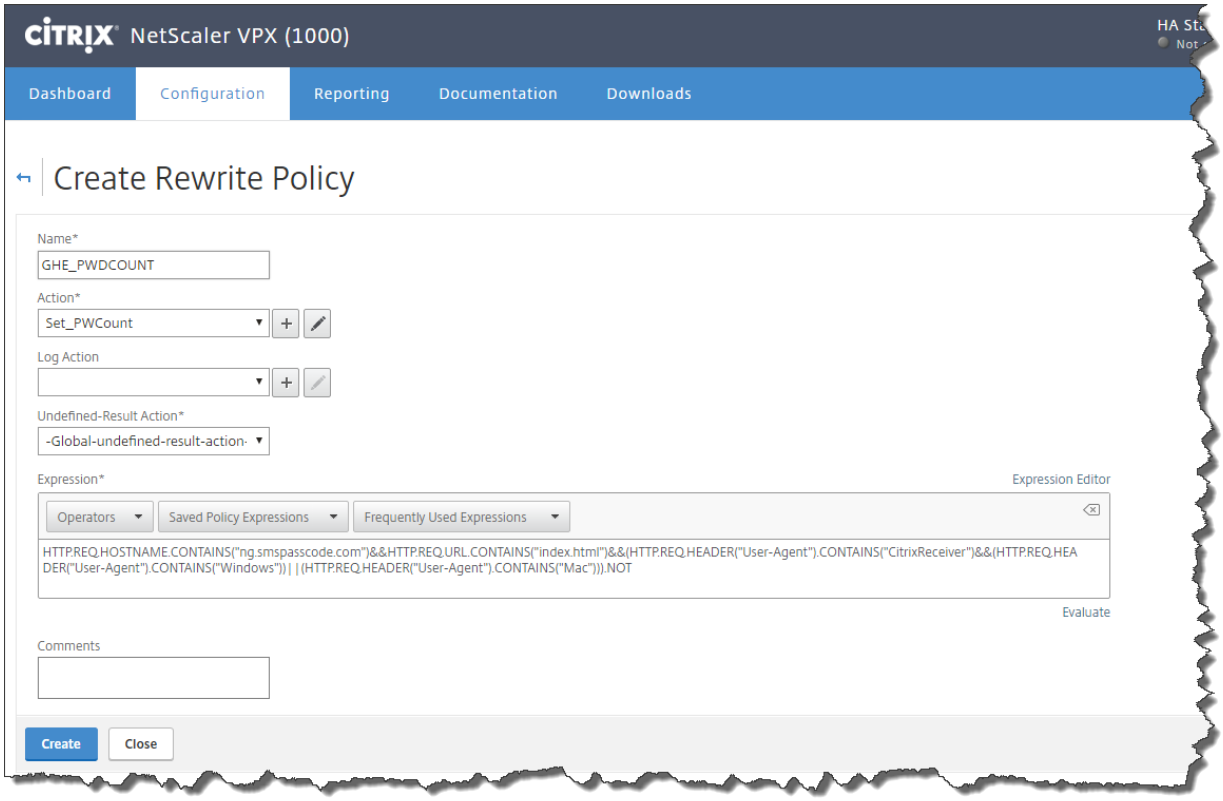
Please configure like this:
Type: INSERT_HTTP_HEADER.

Header name: Set-Cookie
Expression: “pwcount=0”

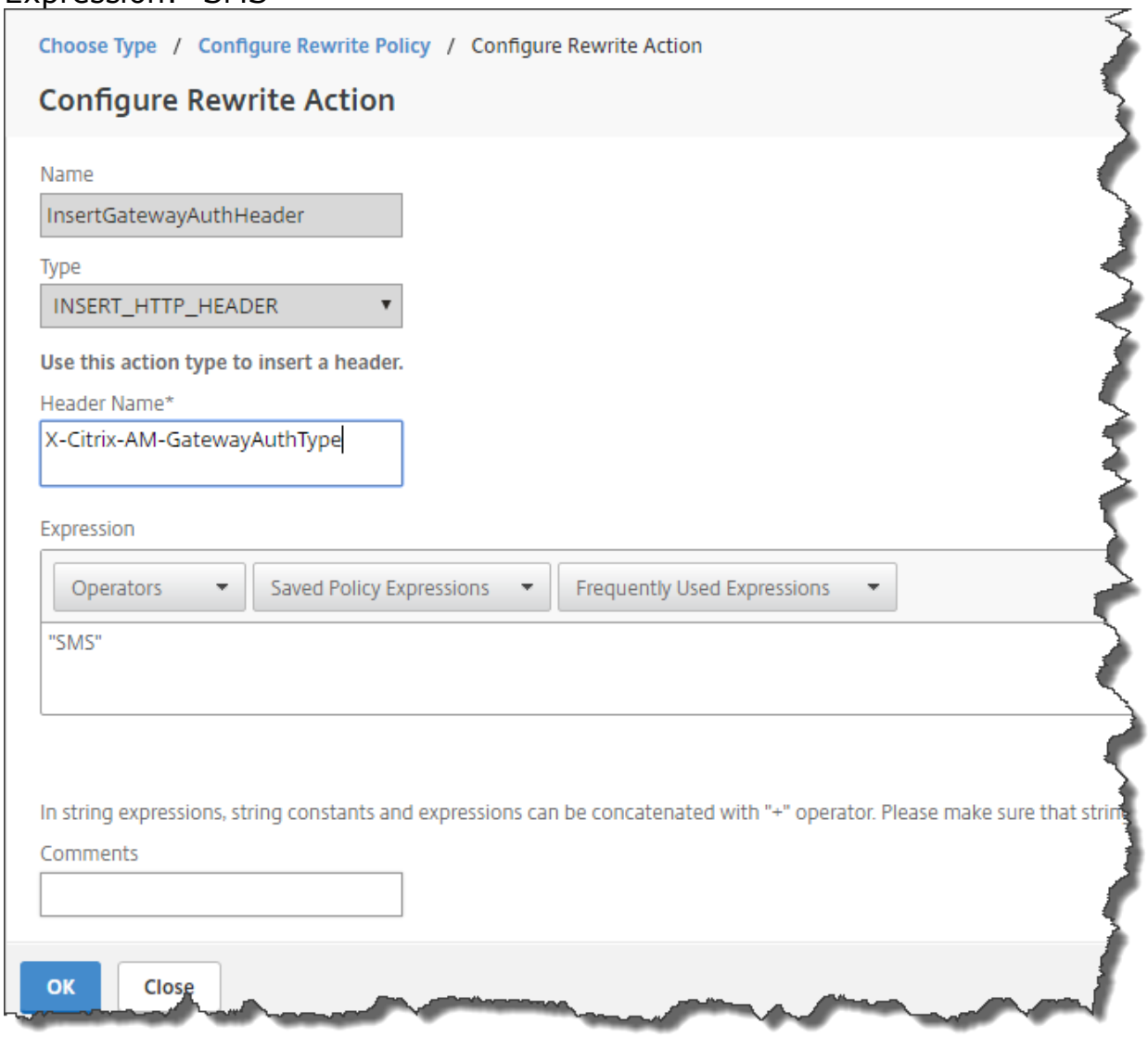


The Rewrite policy needs an expression:

HTTP.REQ.HOSTNAME.CONTAINS("ng.smspasscode.com") && HTTP.REQ.URL.CONTAINS("index.html")&&(HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")&&((HTTP.REQ.HEADER("User-Agent").CONTAINS("Windows"))||(HTTP.REQ.HEADER("User-Agent").CONTAINS("Mac")))).NOT

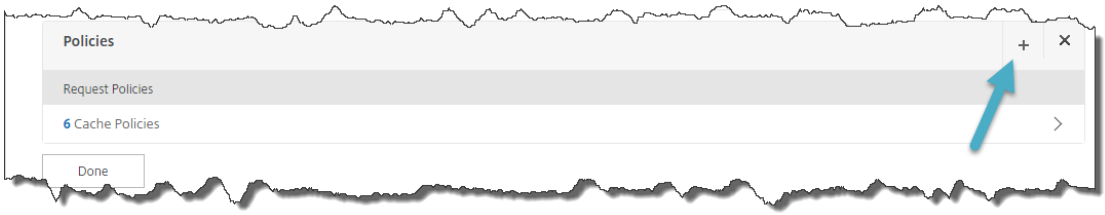


Now please make a new Rewrite policy with a new rewrite action. This will leave you with two rewrite policies.
Type: Insert_HTTP_HEADER
Header Name: X-Citrix-AM-GatewayAuthType
Expression: “SMS”



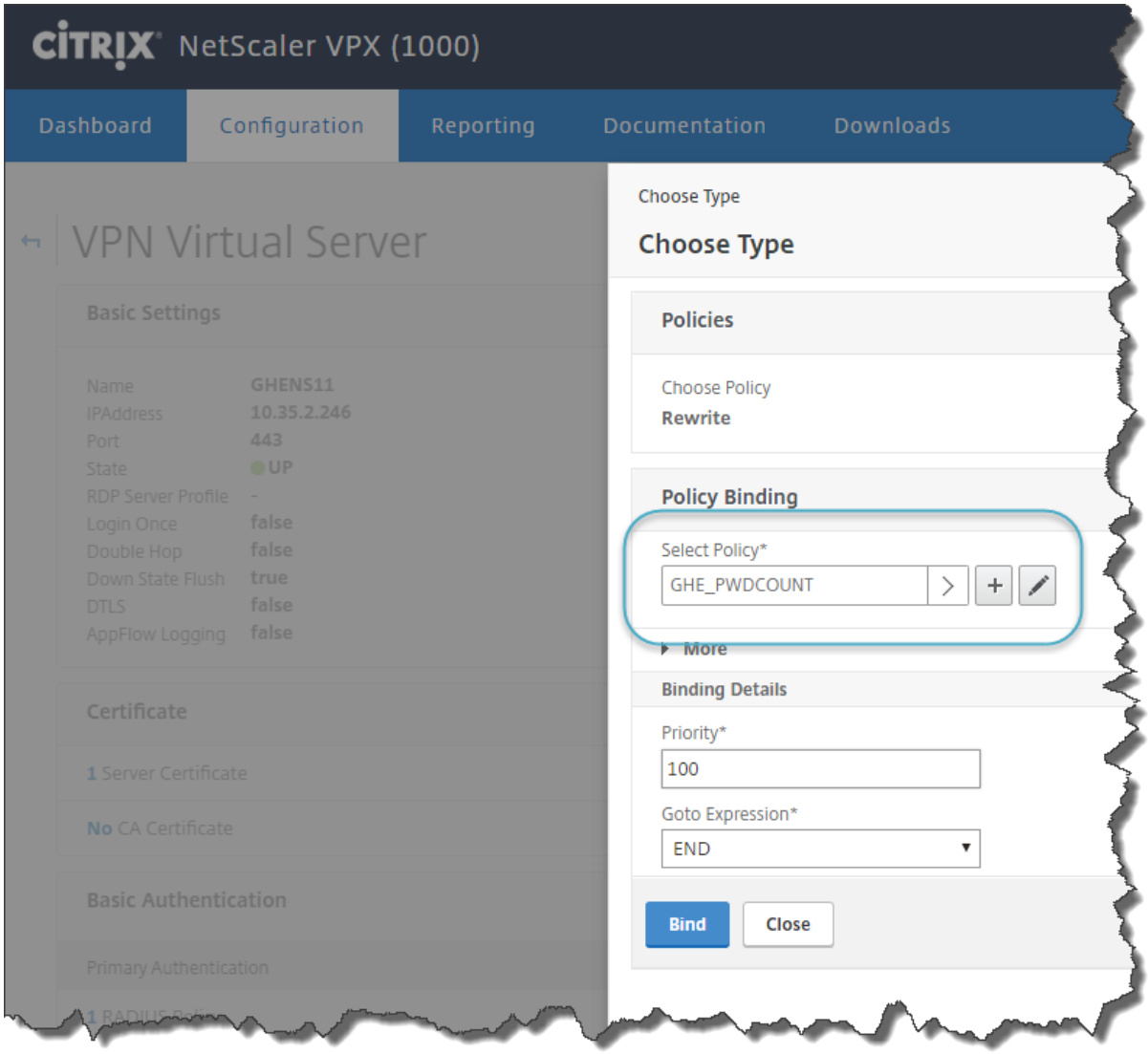
Bind the action to the policy. Save and bind the policy to the virtual server.

Please bind both rewrite policies to the virtual server.
Navigate to the virtual server, and add a policy in the Policies section. Please click the plus sign as shown below.

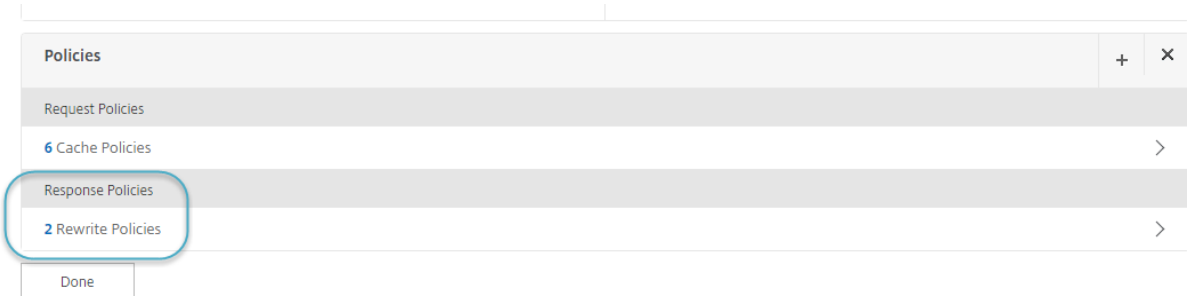


Choose a Rewrite Policy and make the Type Response.

Now please make a policy binding and select the rewrite policy.

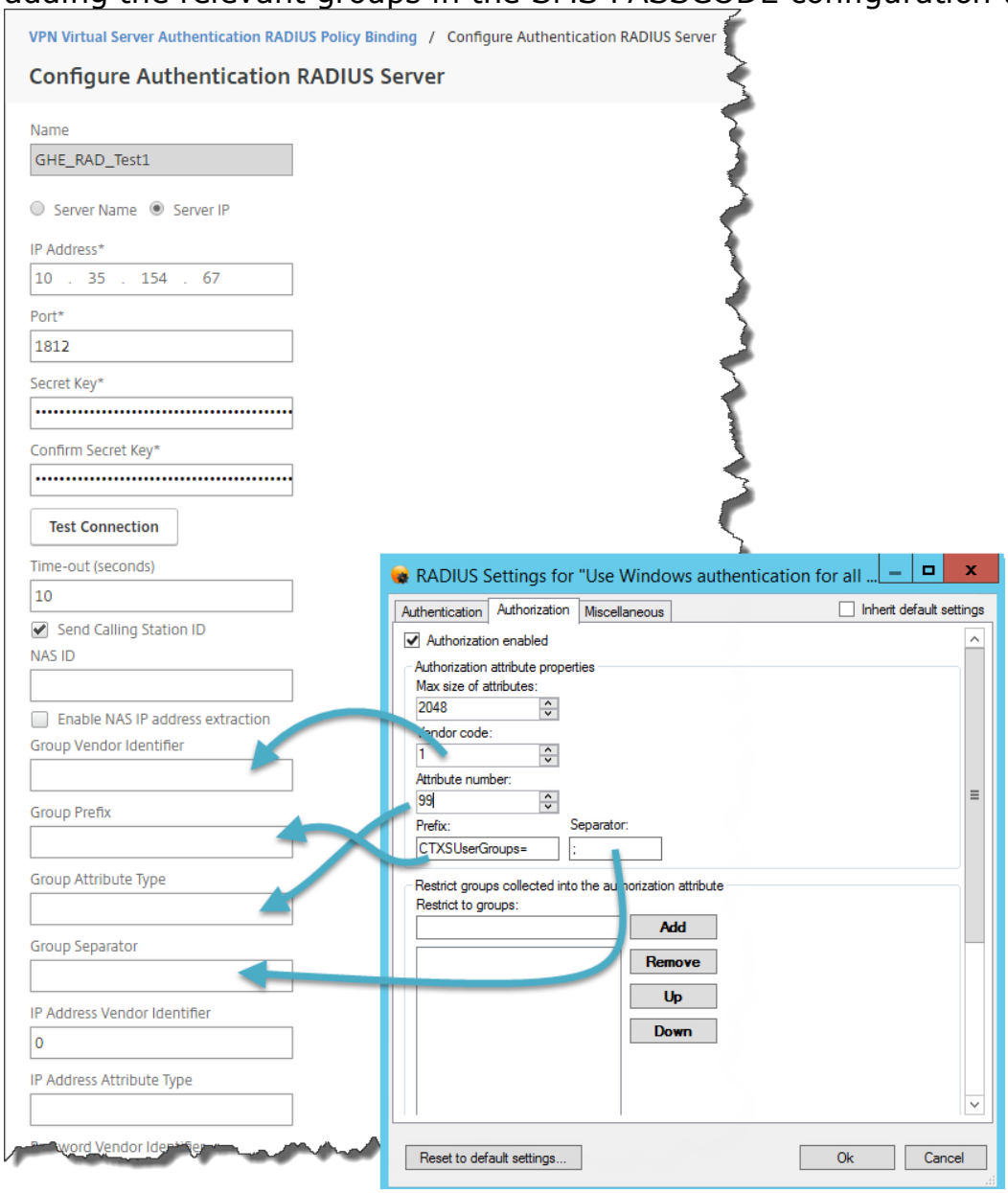


Now please bind both the rewrite policies to the virtual server.
The result should be like this:



Authorization with Radius and SMS PASSCODE MFA

Please note that you should only configure authorization if you need authorization. Not sure? then test without.
If you need to extract groups with Radius, please make sure that you match Vendor code in SMS PASSCODE MFA with Group Vendor identifier in the Netscaler, Attribute number with Group attribute type, prefix with group prefix, and separator with group separator.
It is highly recommended to limit the group search to relevant groups, by adding the relevant groups in the SMS PASSCODE configuration tool.



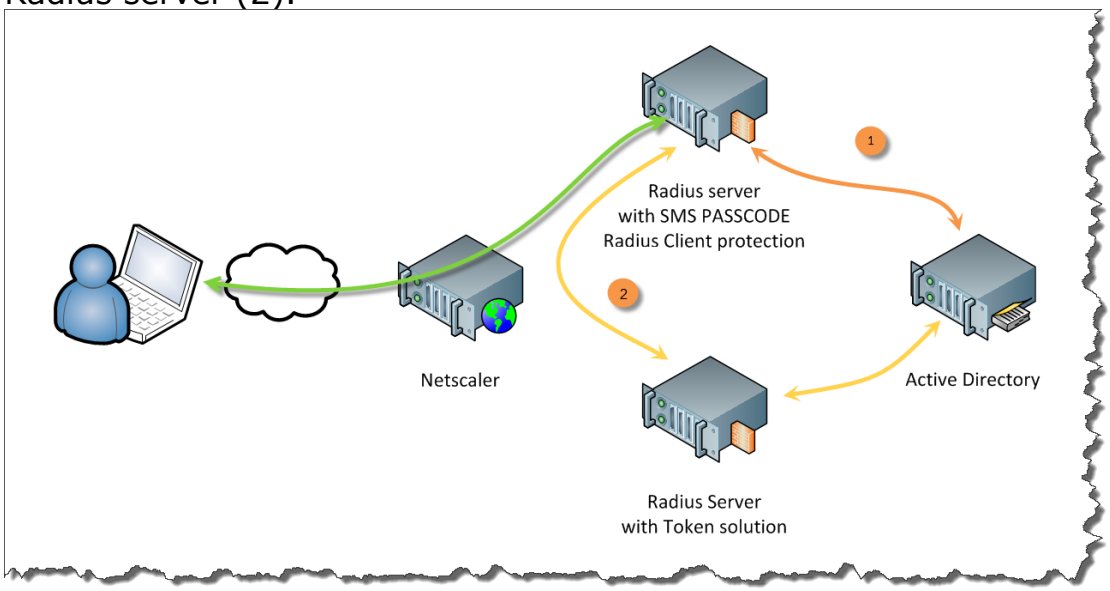
For further information regarding the authorization pane in the SMS PASSCODE configuration tool, please refer to the SMS PASSCODE administrators guide.

Configure SMS PASSCODE MFA for co-existence with a token solution

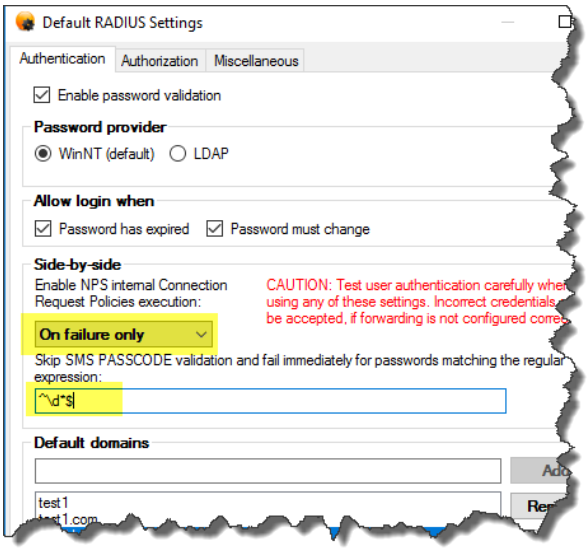
SMS PASSCODE MFA can co-exist with token solutions like RSA.

Scenario 1

Your token solution uses radius authentication. You configure radius forwarding from the SMS PASSCODE MFA radius server to the Token solution radius server. This is the most common scenario. SMS PASSCODE MFA users are resolved directly from the Radius server (1) that forwards the Token Users to the Token Radius server (2).



In the SMS PASSCODE configuration tool, you set a expression that denies the code. In example this expression.: for numbers: The Side-by-Side mode configured as "On failure

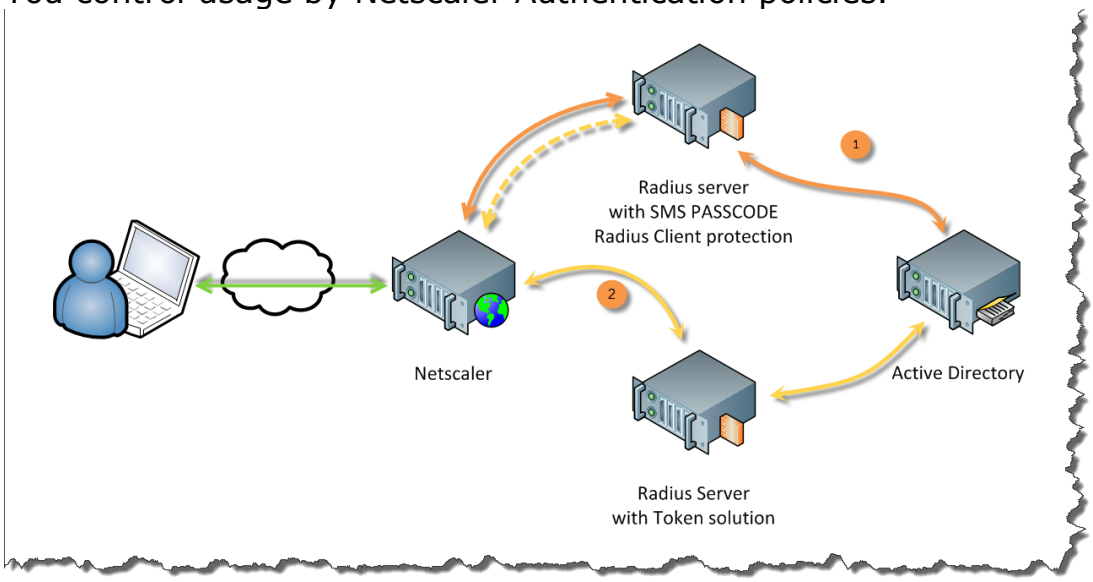


regular token

^\d*$ must be only"

Scenario 2

You control usage by Netscaler Authentication policies.

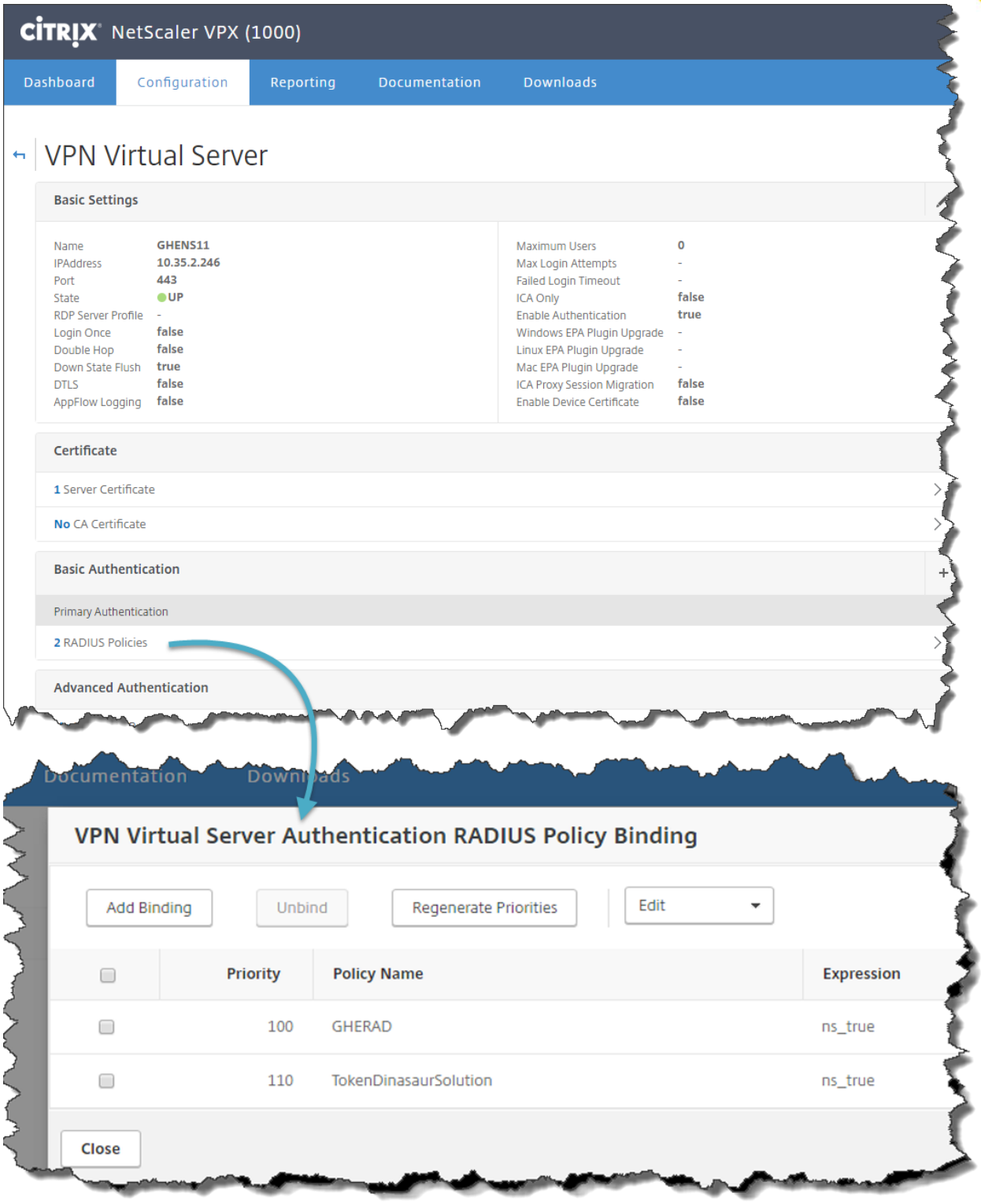


You add 2 Authentication policies, one for SMS PASSCODE MFA Radius and one for the Token solution authentication. The SMS PASSCODE MFA authentication policy must be inserted before (lower number) the Token solution authentication policy.

When a user is logs on (1), the user authenticates at the SMS PASSCODE MFA Radius server. The Token solution user (2) is logging on; the user is at first authenticated with the SMS PASSCODE MFA Radius authentication policy, which denies the user access, because the user is not a SMS PASSCODE MFA User. An Access-Deny is then sent back to the Netscaler, and the Netscaler will now try the next in line authentication policy, which is the Token solution authentication policy. Now the user will be able to gain access.

To configure this please navigate to the virtual server and edit the binding. See screenshot at the next page.

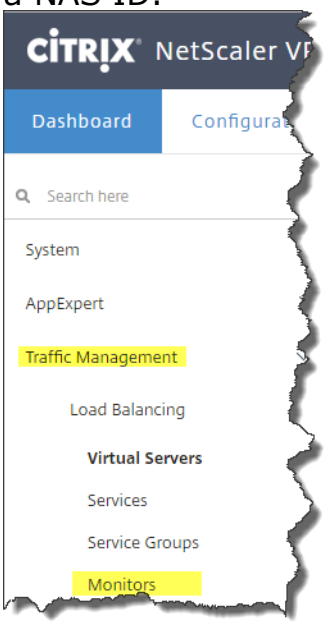
censornet.

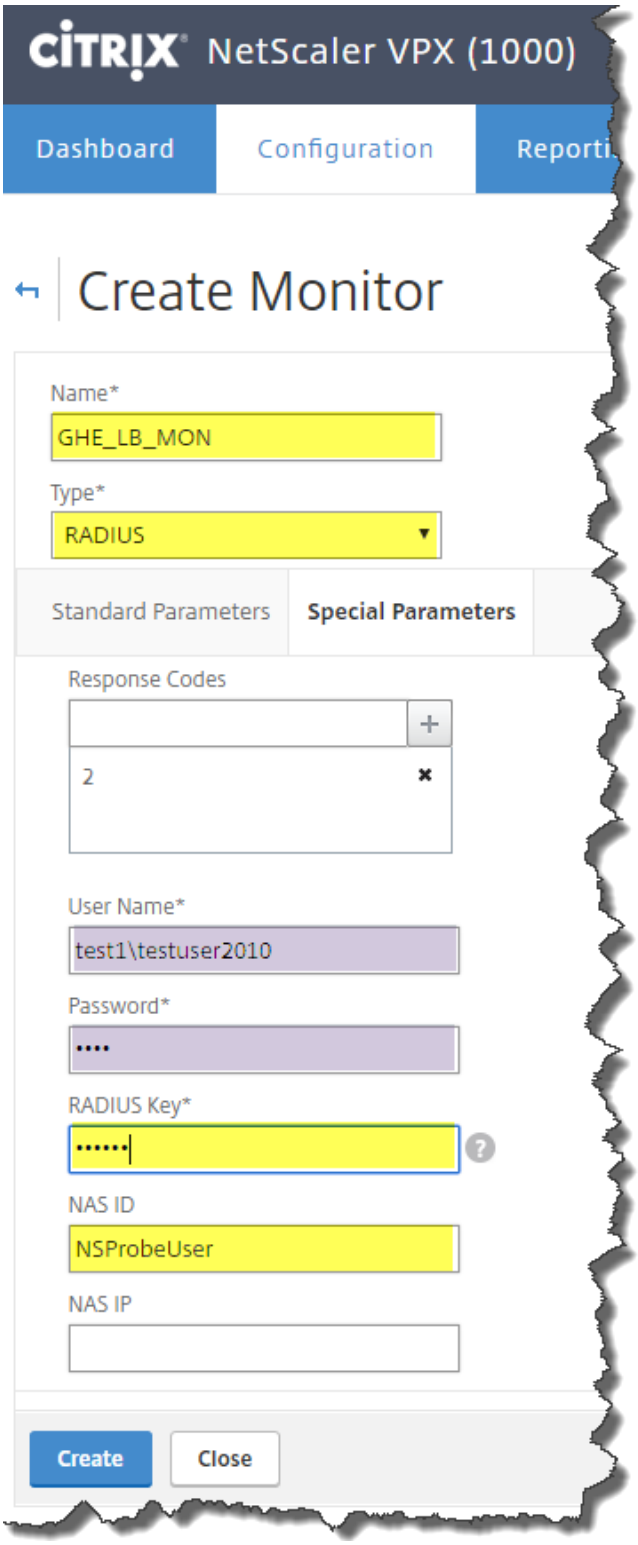

CITRIX NetScaler VPX (1000)
Dashboard
Configuration
Reporting
Documentation
Downloads
VPN Virtual Server
Basic Settings
Name GHENS11
IPAddress 10.35.2.246
Port 443
State UP
RDP Server Profile -
Login Once false
Double Hop false
Down State Flush true
DTLS false
AppFlow Logging false
Maximum Users 0
Max Login Attempts -
Failed Login Timeout -
ICA Only false
Enable Authentication true
Windows EPA Plugin Upgrade -
Linux EPA Plugin Upgrade -
Mac EPA Plugin Upgrade -
ICA Proxy Session Migration false
Enable Device Certificate false
Certificate
1 Server Certificate
No CA Certificate
Basic Authentication
Primary Authentication
2 RADIUS Policies
Advanced Authentication
Documentation
Downloads
VPN Virtual Server Authentication RADIUS Policy Binding
Add Binding
Unbind
Regenerate Priorities
Edit
Priority
Policy Name
Expression
100 GHERAD ns_true
110 TokenDinasaurSolution ns_true
Close

Configure a Load Balancing environment for use with SMS PASSCODE MFA Radius servers.

Create Monitor

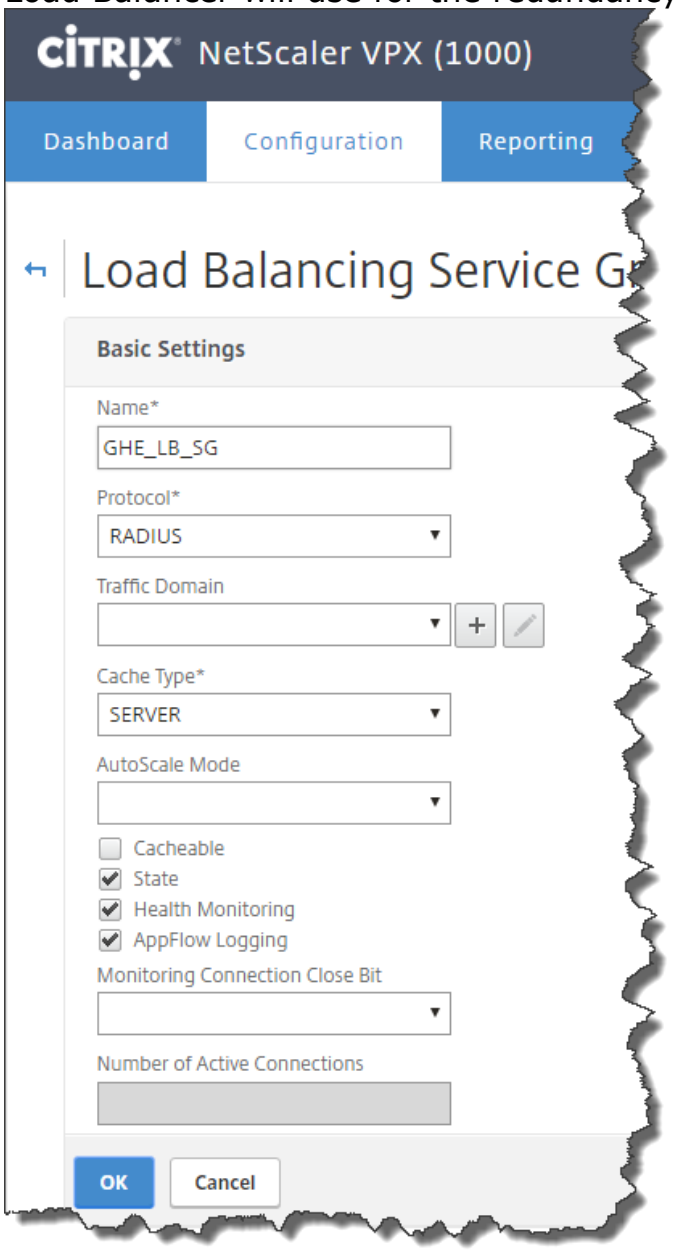
Please navigate to the Traffic Management.
When setting up a Netscaler with e.g. 2 radius servers for redundancy, it is important to use Load Balancing instead of configuring 2 radius servers in the primary authentication.
For a start please create the Monitor. Navigate to Traffic management, Load Balancing, Monitors.
Please give the Load Balancing Service Group a name of your own choice, and make sure that the type is RADIUS. User name and password can be configured but can also be left out.
Radius key must be the same shared secret as the shared secret configured in the NPS radius client.
Please make sure to configure a NAS ID.



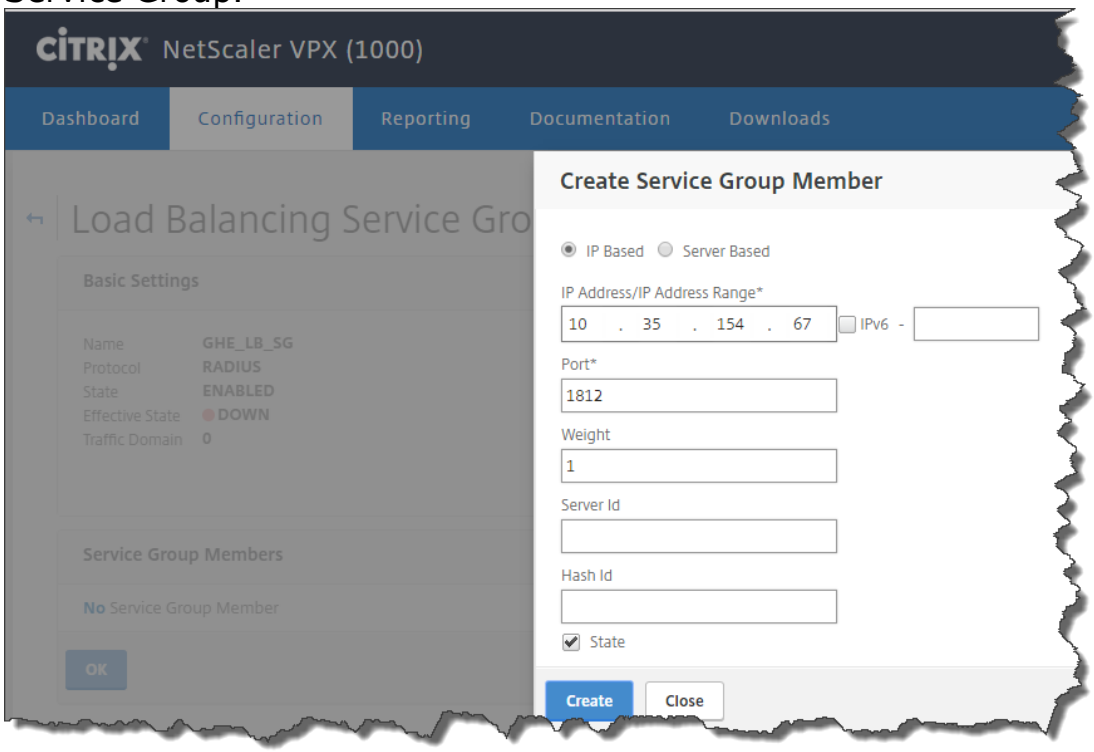


The Load Balancing Service Group.

Give the Load Balancing Service Group a name and make sure the Protocol is Radius. Please click OK.
Once you save the Load Balancing Service Group, you will have the possibility to add Service Group Members.
Server group member binding contains the two radius servers with SMS PASSCODE MFA Radius client protection. It´s these two Radius servers that the Load Balancer will use for the redundancy configuration.



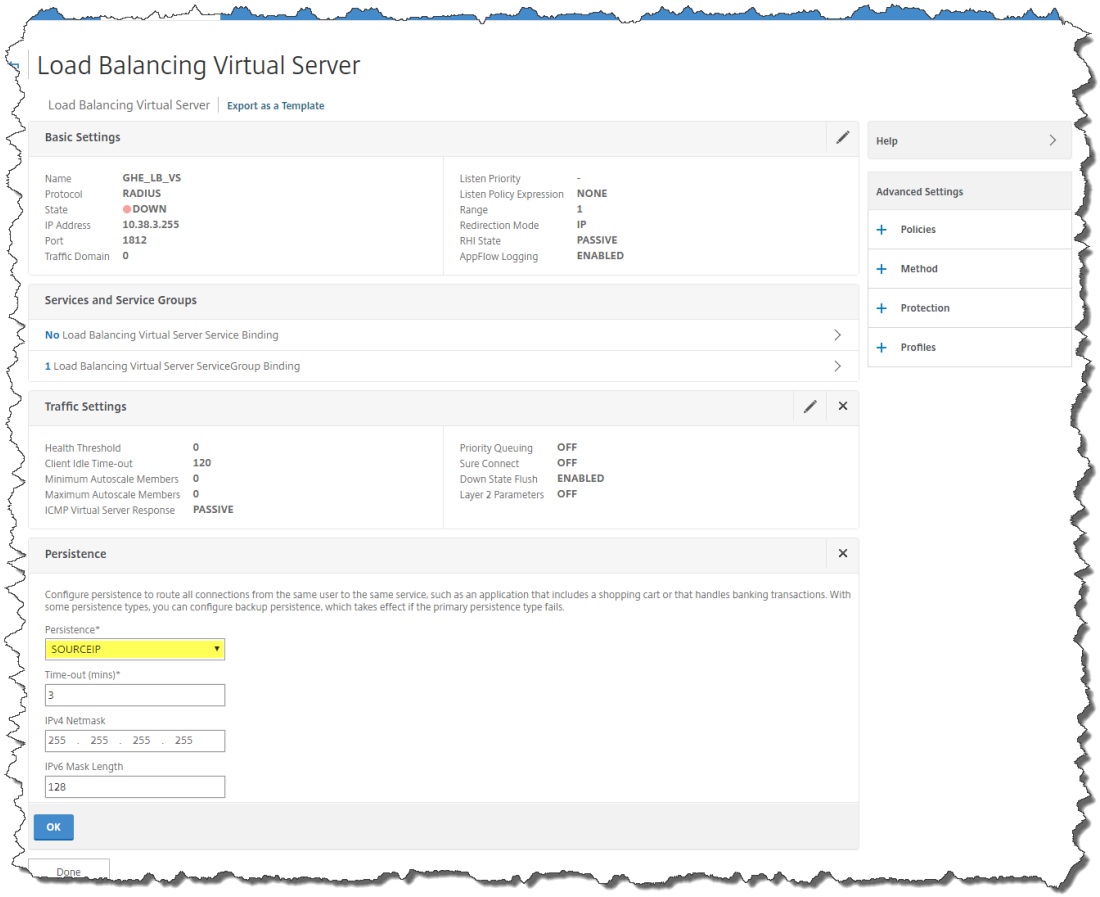
Add your radius servers as Service Group members to the Load Balancing Service Group.



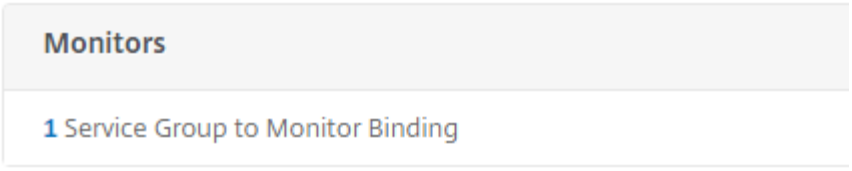
Load Balancing Virtual Server configuration

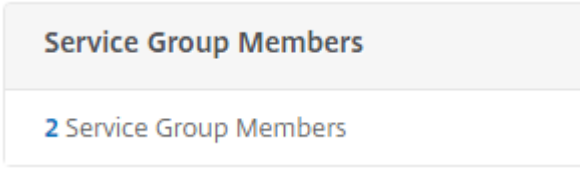
Configure the Load Balancing Virtual Server. The name is optional. Please ensure that the protocol is RADIUS. IP address type should be IP Address and the port is 1812. The IP address configured is the IP address, that you need to configure as the IP address the Virtual Server´s radius IP address, instead of the actual Radius servers.

In the Persistence section, you must ensure to configure persistence with SUOURCEIP.

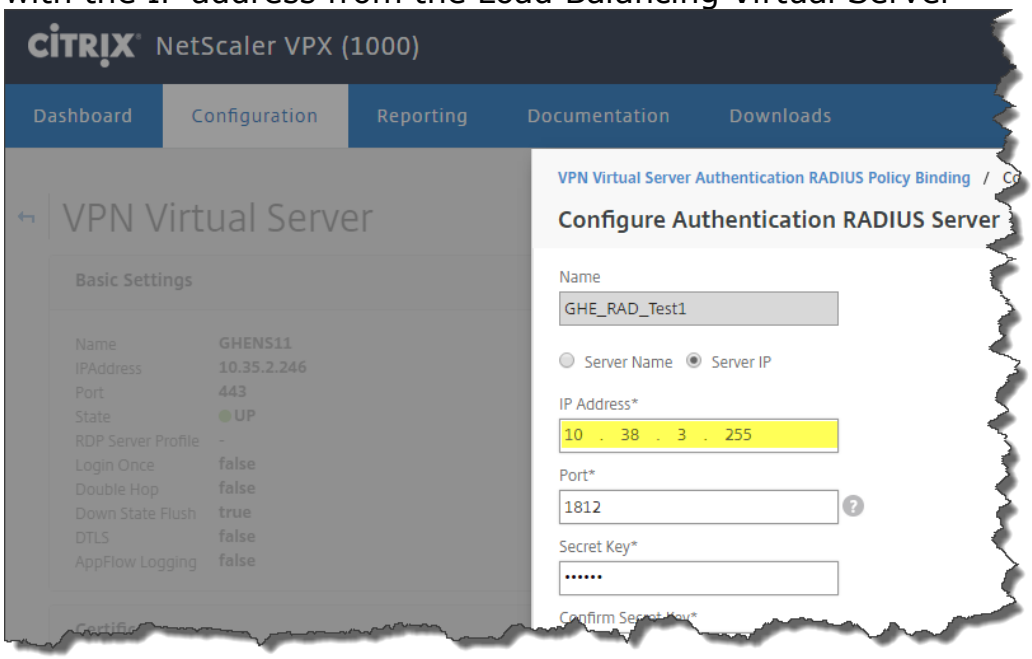


Please also add the Service Group members and the Monitor.



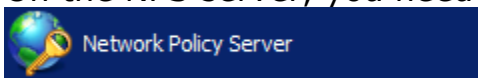


When finished please make sure that the VPN Virtual server has been configured with the IP address from the Load Balancing Virtual Server

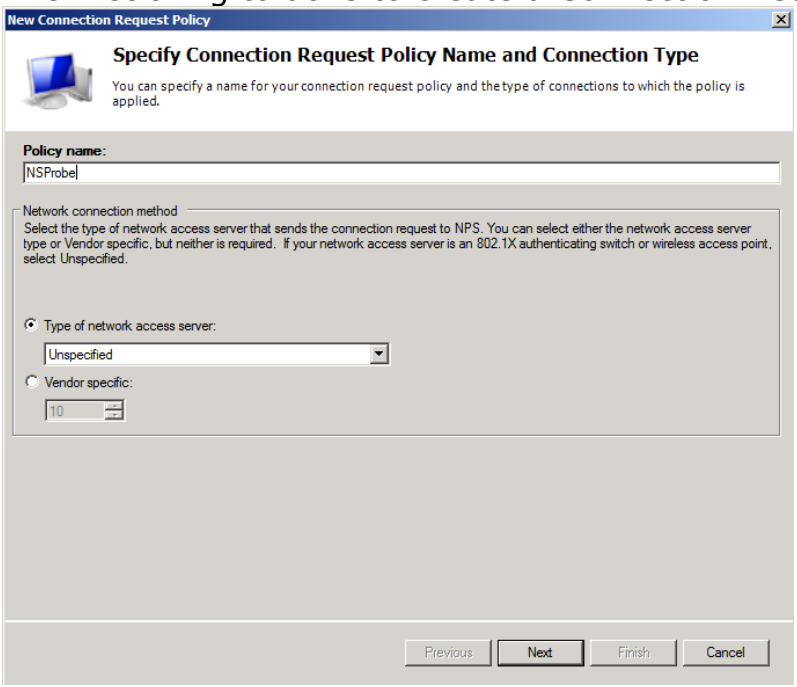


Network Policy Server

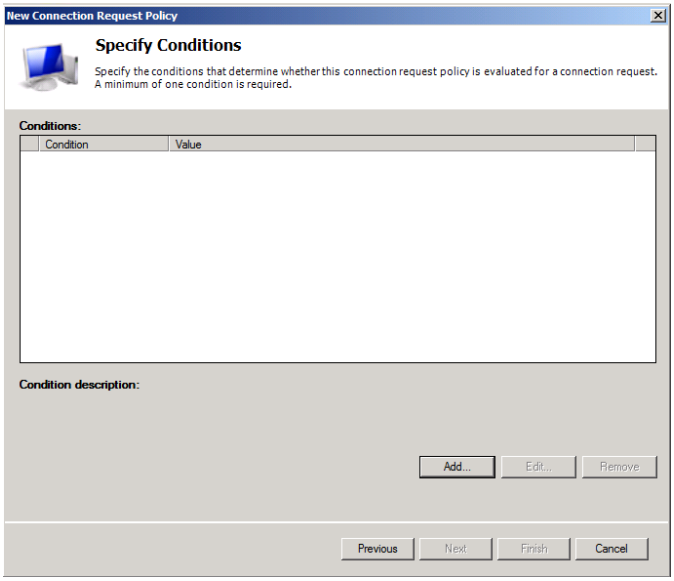
On the NPS server, you need to start the Net policy server manager



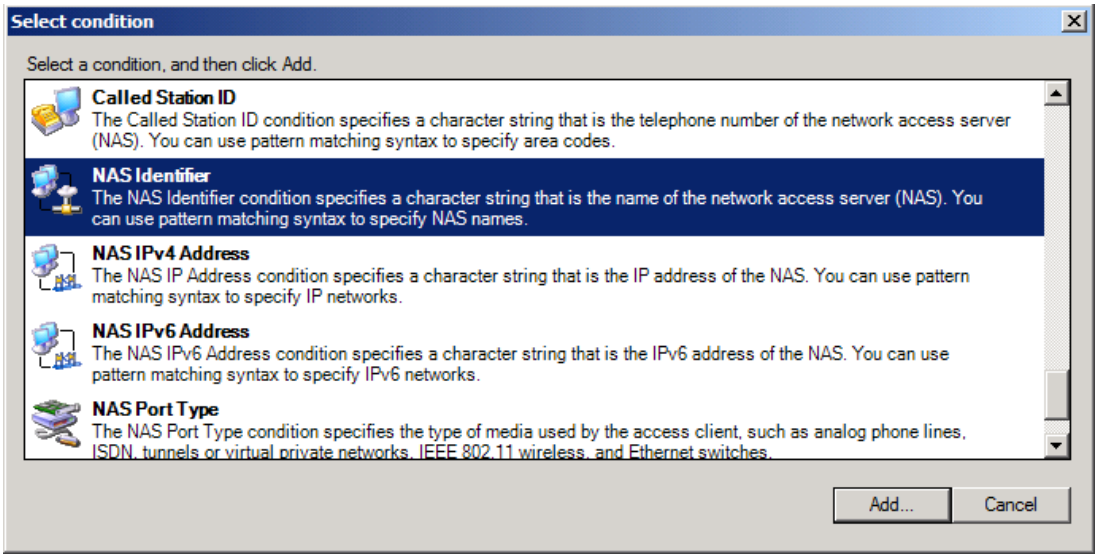
The first thing to do is to create a Connection Request Policy



Add a condition.

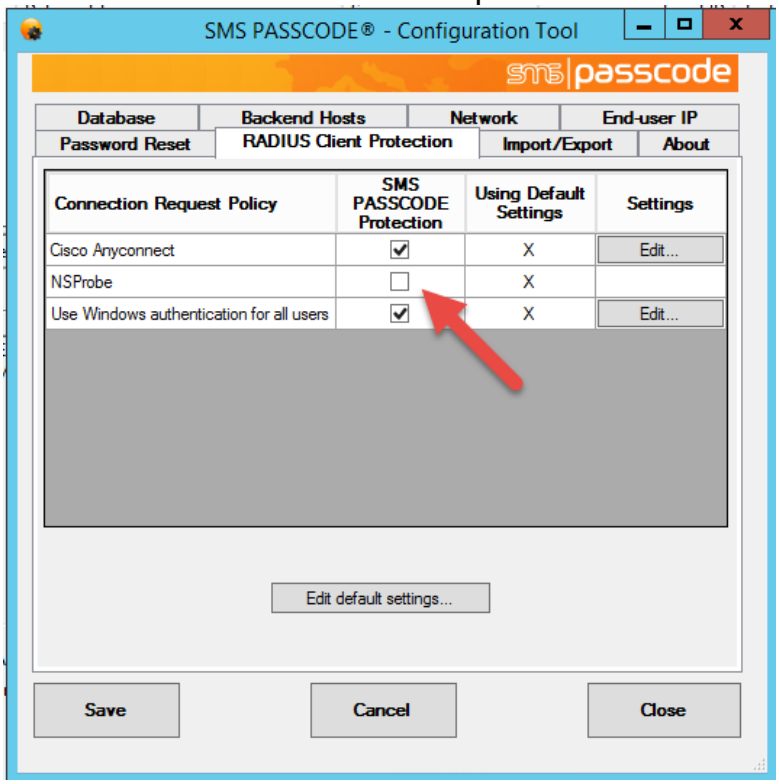


The condition must be NAS ID



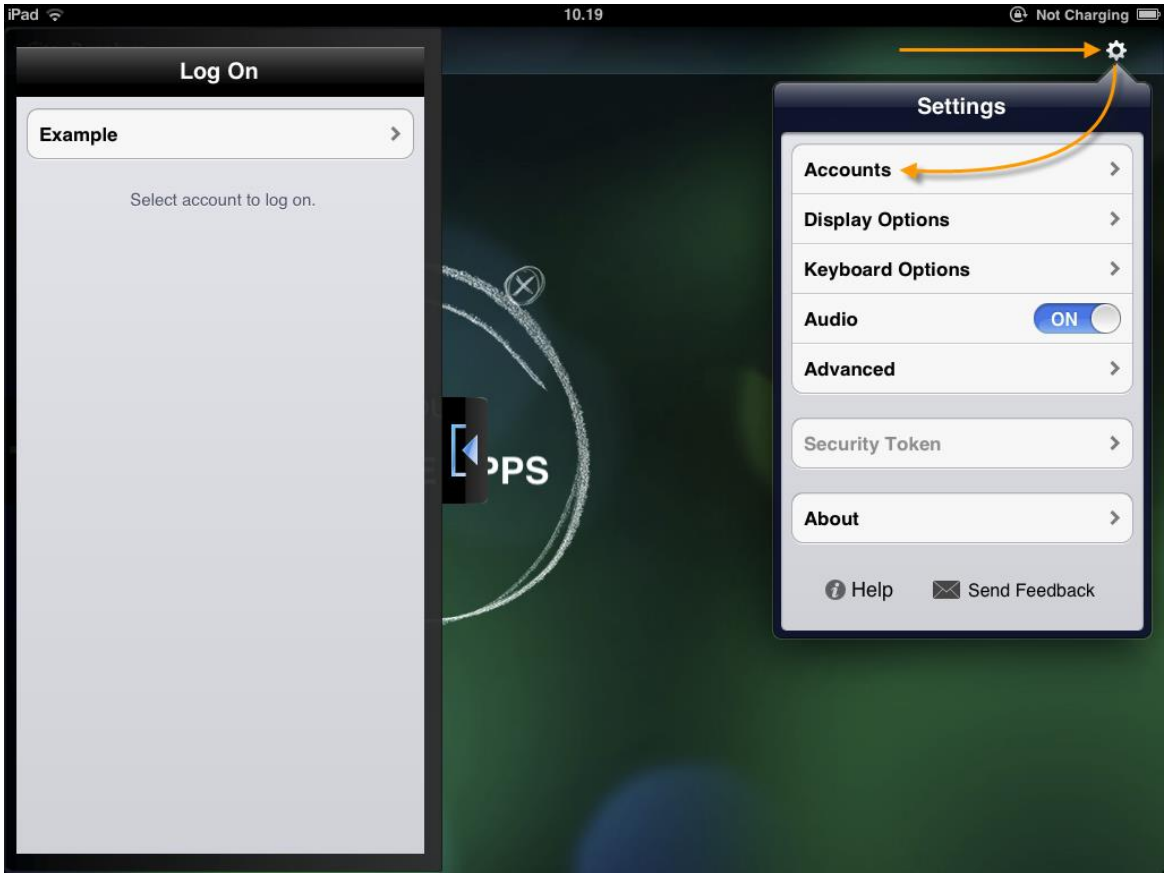
The value must the same as you specified in the NAS ID in the Netscaler´s Load Balancer. Click ok, and then finish the guide as next next next finish.

Now you can specify the MFA by-pass, by unchecking the policy that only the Probe user can use. This will prevent a flood of events in the event log.

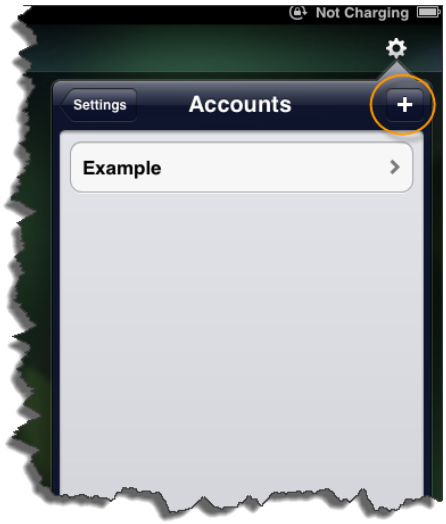


Configure settings for the “Citrix receiver for iPad/iPhone” with Citrix receiver 5.6+.

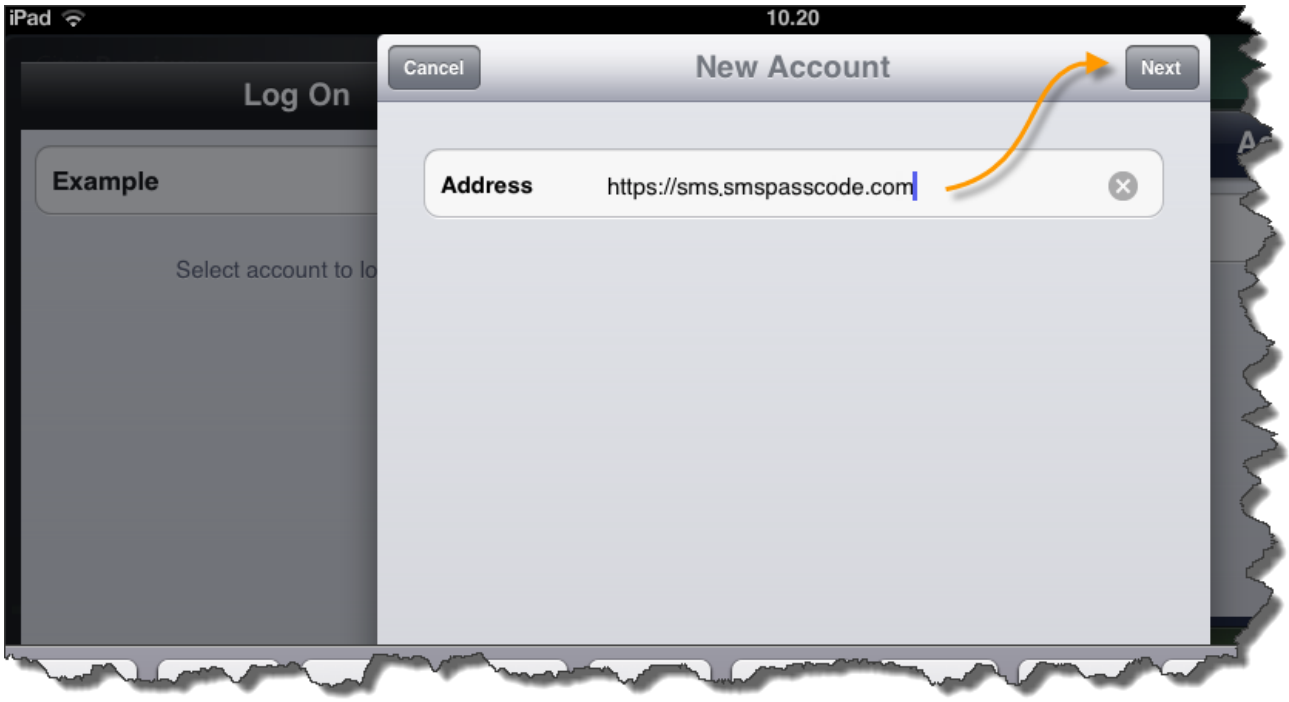
To configure the Citrix Receiver, please open it, navigate to settings, and choose Accounts from the menu.



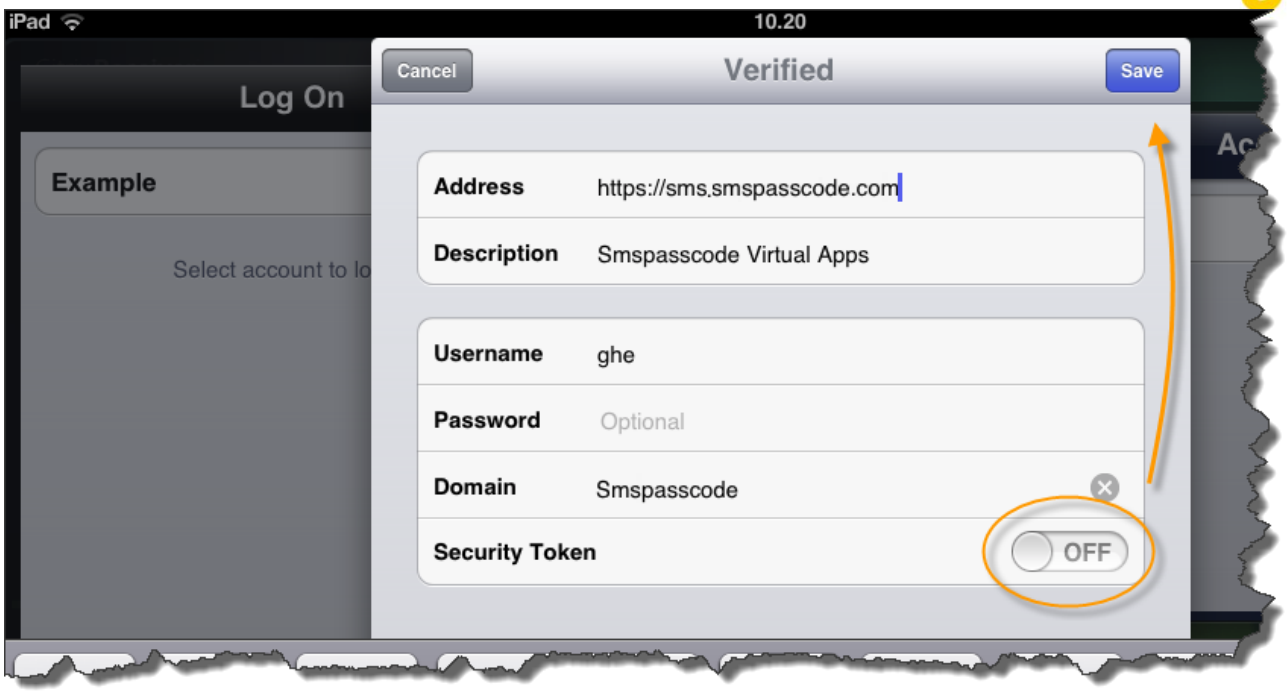
To add an account please click on the + sign.



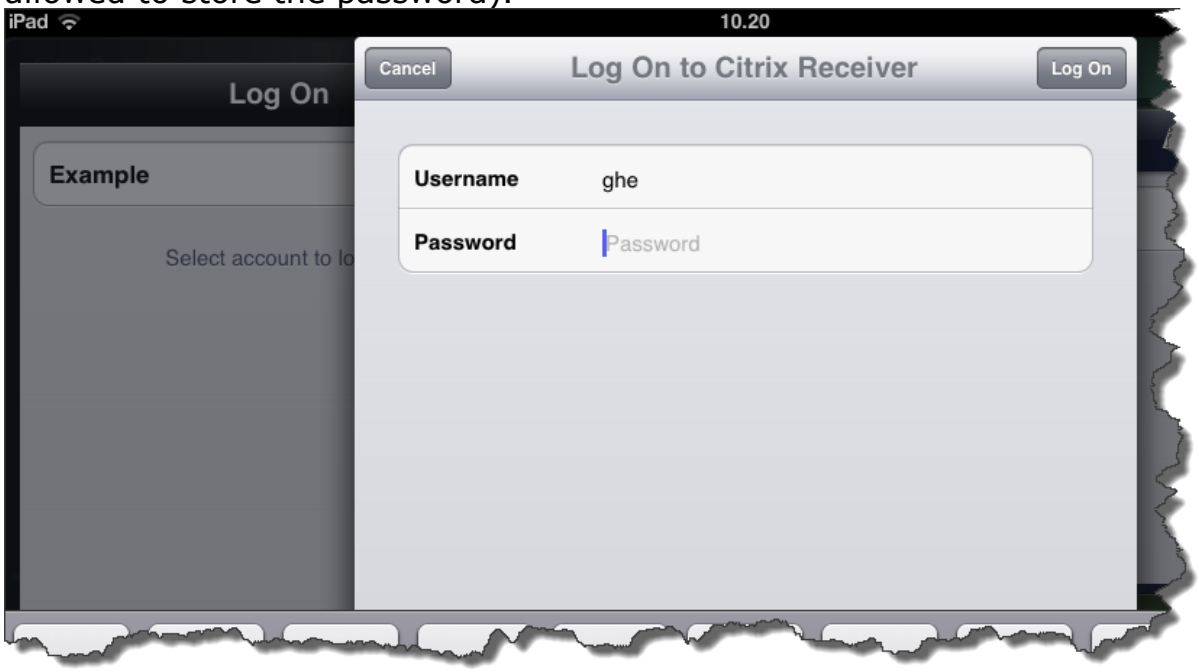
Now enter the URL of your Citrix Access Gateway Enterprise Edition / Netscaler, and click on Next.



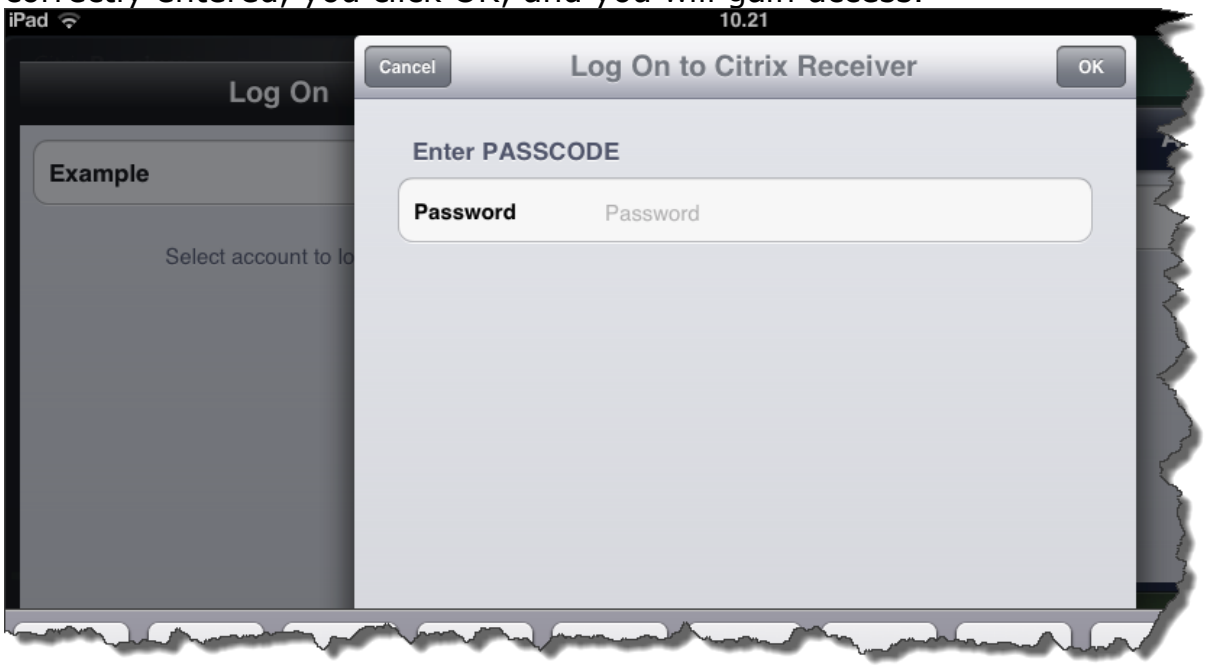
Fill in the information; leave Security Token as OFF, and save the configuration.



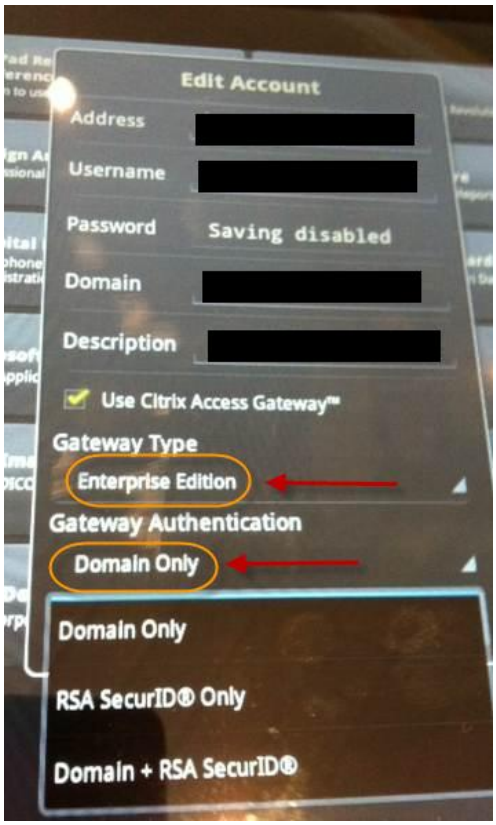
Now you are ready to use your Citrix Receiver. Your experience should look like this (This window will show if the password has not been saved or if it is not allowed to store the password).



You should now receive your One Time Passcode, and enter this. If the code correctly entered, you click OK, and you will gain access.



If you are using Citrix Receiver for Android, the configuration should look like this:



Configure iPad/iPhone for Web Interface

To authenticate over the web interface with Citrix receiver for iPad requires:

- Citrix Receiver for iPad version 4.2 or newer
- Citrix Web Interface version 5.4 or newer

When you authenticate with Citrix Receiver for iPad over the web interface the SMS PASSCODE
If the web site is configured with ns_true in policies, then this will work out of the box.

censornet.