



Netscaler configuration

Contents

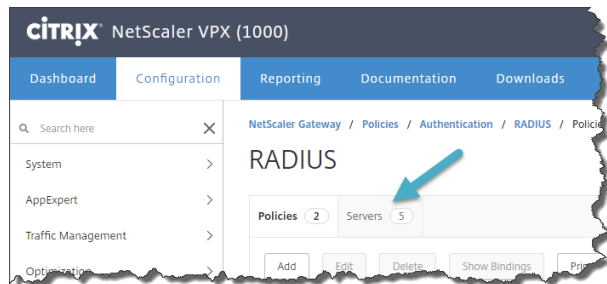
Netscaler configuration	0
Create an Authentication server	1
Creating the policy and profile	5
Bind the session policy to the virtual server.....	9
Use of the rewrite feature	16
Scenario 1.....	26
Scenario 2.....	27
Create Monitor.....	29
The Load Balancing Service Group.....	30
Load Balancing Virtual Server configuration.....	32
Network Policy Server	34
Configure iPad/iPhone for Web Interface	41



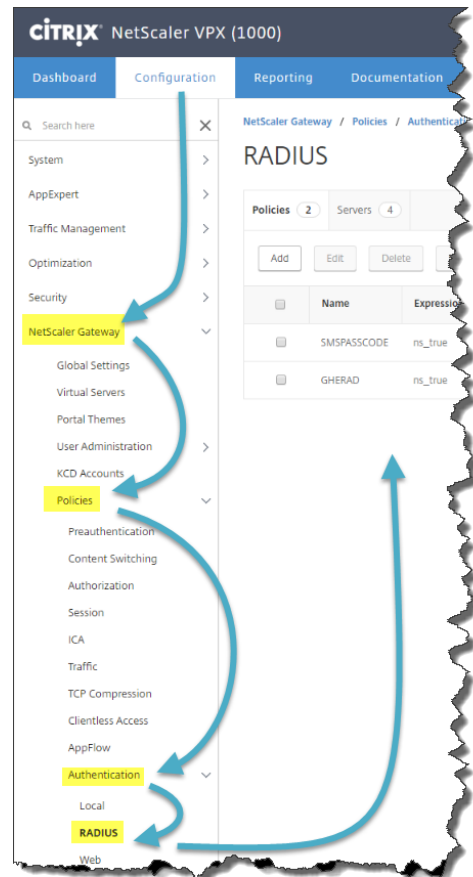
Configuration of the virtual server with a Radius authentication Server and Radius policy.

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.

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Configure Authentication RADIUS Server

Name
GHE_RAD_Test1

☐ Server Name ☒ Server IP

IP Address*
10 . 35 . 154 . 67

Port*
1812

Secret Key*
.....

Confirm Secret Key*
.....

Test Connection

Time-out (seconds)
3

More

OK Close



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 checked, 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"

Test Connection

Time-out (seconds)
10

☒ Send Calling Station ID

NAS ID

☐ Enable NAS IP address extraction

Group Vendor Identifier

Group Prefix

Group Attribute Type

Group Separator

IP Address Vendor Identifier
0

IP Address Attribute Type

Password Vendor Identifier

Password Attribute Type

Password Encoding*
pap ▼

Accounting*
OFF ▼

Default Authentication Group

▲ Less

OK Close



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).

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Search here

System > AppExpert > Traffic Management > Optimization > Security > NetScaler Gateway >

Global Settings Virtual Servers

NetScaler Gateway / Policies / Authentication / RADIUS / Policies

RADIUS

Policies 2 Servers 5

Add Edit Delete Show Bindings Primary VPN Global Bind

	Name	Expression	Request Server	Primary
<input type="checkbox"/>	SMSPASSCODE	ns_true	SVSMSPASSCODE1	✕
<input checked="" type="checkbox"/>	GHERAD	ns_true	RAD015	✕

Now please bind the policy to the Radius Authentication server.

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Configure Authentication RADIUS Policy

Name: GHERAD

Server*: GHE_RAD_Test1

Expression*: ns_true

OK Close



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

The screenshot shows the Citrix NetScaler VPX (1000) web interface. The left sidebar contains a navigation menu with the following items: System, AppExpert, Traffic Management, Optimization, Security, NetScaler Gateway (highlighted), Global Settings, Virtual Servers, Portal Themes, User Administration, KCD Accounts, Policies (highlighted), Preauthentication, Content Switching, Authorization, Session (highlighted), and ICA. The main content area displays the 'NetScaler Gateway Session Policies and Profiles' page. At the top, there are tabs for 'Session Policies' (6) and 'Session Profiles' (5), with the 'Session Profiles' tab selected and highlighted. Below the tabs are 'Add', 'Edit', and 'Delete' buttons. A table lists the session profiles with columns for a checkbox and 'Name'. The table contains five entries: 10.35.2.247_443, AC_OS_10.35.2.245, AC_WB_10.35.2.245, AC_OS_10.35.2.244, and AC_WB_10.35.2.244. A blue arrow points from the 'Session' item in the left sidebar to the 'Session Profiles' tab in the main content area.



NetScaler VPX (1000)

Dashboard
Configuration
Reporting
Documentation
Downloads

Create NetScaler Gateway Session Profile

Name*

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

☐ Display Home Page
☐ Override Global

Home Page
☐

URL for Web-Based Email
☐

Split Tunnel*
☐

Session Time-out (mins)
☐

Client Idle Time-out (mins)
☐

Clientless Access*
☐

Clientless Access URL Encoding*
☐

Clientless Access Persistent Cookie*
☐

Plug-in Type*
☐

Windows Plugin Upgrade
☐

Linux Plugin Upgrade
☐

MAC Plugin Upgrade
☐

AlwaysON Profile Name

☐

☐ Single Sign-on to Web Applications
☐

Credential Index*
☐

KCD Account

☐

Single Sign-on with Windows*
☐

Client Cleanup Prompt*
☐

☐ 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`.

CITRIX® NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

← Configure 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
-----------------------	-------------------	----------	-------------------------------	----------------

Override Global

ICA Proxy*
ON ☒

Web Interface Address
https://Storefront1.sms.passcode/cit ☒

Web Interface Address Type*
IPV4

Web Interface Portal Mode*
NORMAL ☐

Single Sign-on Domain
sms ☒

Citrix Receiver Home Page
☐

Account Services Address
☐

OK Close



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

CITRIX® NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

← Create NetScaler Gateway Session Policy

Name*

Profile*
 + ✎

Expression*

Operators Saved Policy Expressions Frequently Used Expressions

Create Close



Bind the session policy to the virtual server

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Search here

System >
AppExpert >
Traffic Management >
Optimization >
Security >
NetScaler Gateway >
Global Settings
Virtual Servers
Portal Themes
User Administration >
KCD Accounts

NetScaler Gateway / NetScaler Gateway Virtual Servers

NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action

<input type="checkbox"/>	Name	State	IP Address	Port	Protocol	M
<input type="checkbox"/>	NS11	UP	10.35.2.247	443	SSL	
<input checked="" type="checkbox"/>	GHENS11	UP	10.35.2.246	443	SSL	
<input type="checkbox"/>	_XD_NS11	UP	10.35.2.245	443	SSL	
<input type="checkbox"/>	_XD_test ng	UP	10.35.2.244	443	SSL	

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

VPN Virtual Server

Basic Settings

Name	GHENS11	Maximum Users	0
IPAddress	10.35.2.246	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	UP	ICA Only	false
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-

Policies

Request Policies

6 Cache Policies

Done



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.

CITRIX® NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

VPN Virtual Server

Basic Settings

Name	GHENS11	Maximum Users	0
IPAddress	10.35.2.246	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	UP	ICA Only	false
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	true	Mac EPA Plugin Upgrade	-
DTLS	false	ICA Proxy Session Migration	false
AppFlow Logging	false	Enable Device Certificate	false

Certificate

1 Server Certificate >

No CA Certificate >

Basic Authentication +

Primary Authentication

1 RADIUS Policy >

Advanced Authentication

No SAML IDP Policy >

SSL Parameters

Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED
Enable DH Key Expire Size Limit	DISABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED
Enable Ephemeral RSA	ENABLED	Client Authentication	DISABLED	SSLv3	ENABLED
Refresh Count	0	Send Close-Notify	YES	TLSv1	ENABLED
Enable Session Reuse	ENABLED	PUSH Encryption Trigger	Always	TLSv11	ENABLED
Time-out	120	SNI Enable	DISABLED	TLSv12	ENABLED
SSL Redirect	DISABLED				

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

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

Choose Type

Policies

Choose Policy*

LDAP

Choose Type*

Secondary

Continue Cancel



Choose Type

Select or create a policy. Then Click Bind.

The screenshot shows the Citrix NetScaler VPX (1000) interface. The left sidebar displays the 'VPN Virtual Server' configuration page with 'Basic Settings' and 'Certificate' sections. The main area shows the 'Choose Type' dialog. The 'Policies' section has a 'Choose Policy' dropdown set to 'LDAP'. The 'Policy Binding' section has a 'Select Policy*' dropdown with a 'Click to select' button and a '+', a minus sign, and a pencil icon. A red box highlights the 'Click to select' button. The 'Binding Details' section has a 'Priority*' input field set to '100'. At the bottom are 'Bind' and 'Close' buttons.

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

The screenshot shows the Citrix NetScaler VPX (1000) interface. The left sidebar shows the 'NetScaler Gateway' section expanded, with 'Policies' and 'Session' sub-sections. The main area shows the 'NetScaler Gateway Session Policies and Profiles' page. The 'Session Policies' tab is selected, showing a list of policies. The 'ghe_test1' policy is highlighted. The 'Add', 'Edit', and 'Delete' buttons are visible at the top of the list.



Choose Client Experience

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

Configure 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 ☐

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

AlwaysON Profile Name

▼ + ✎ ☐

☐ Single Sign-on to Web Applications ☐

Credential Index*

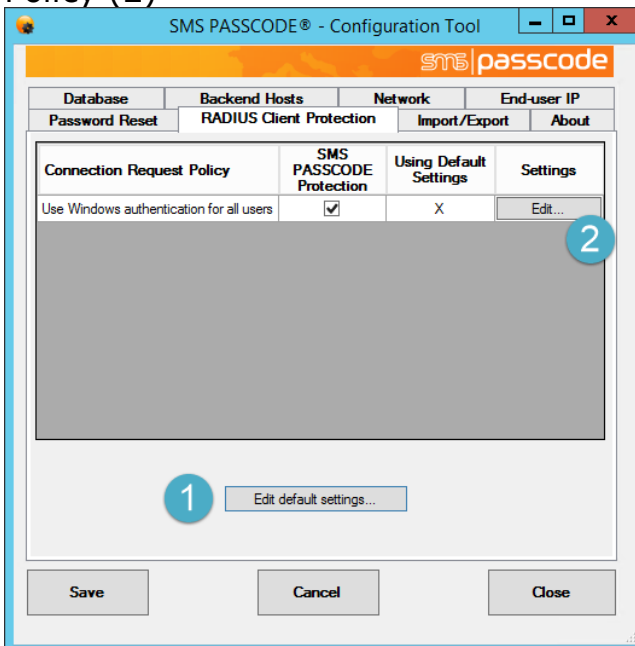
SECONDARY ☒

KCD Account

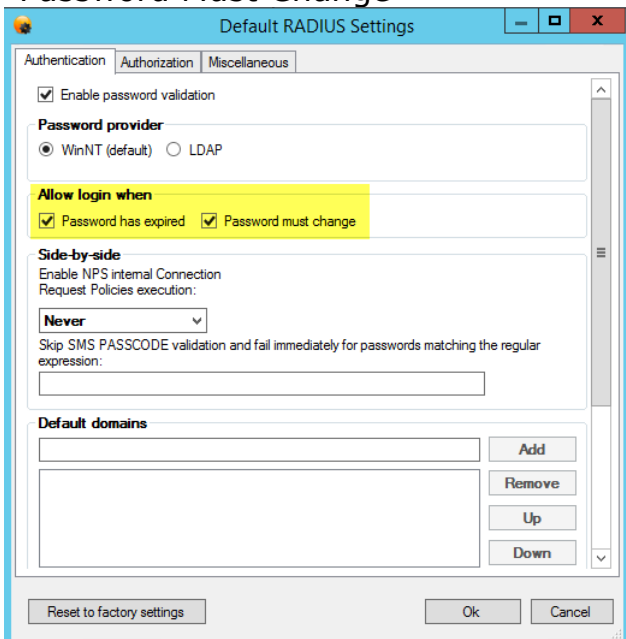


Settings in the SMS PASSCODE Configuration Tool

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.

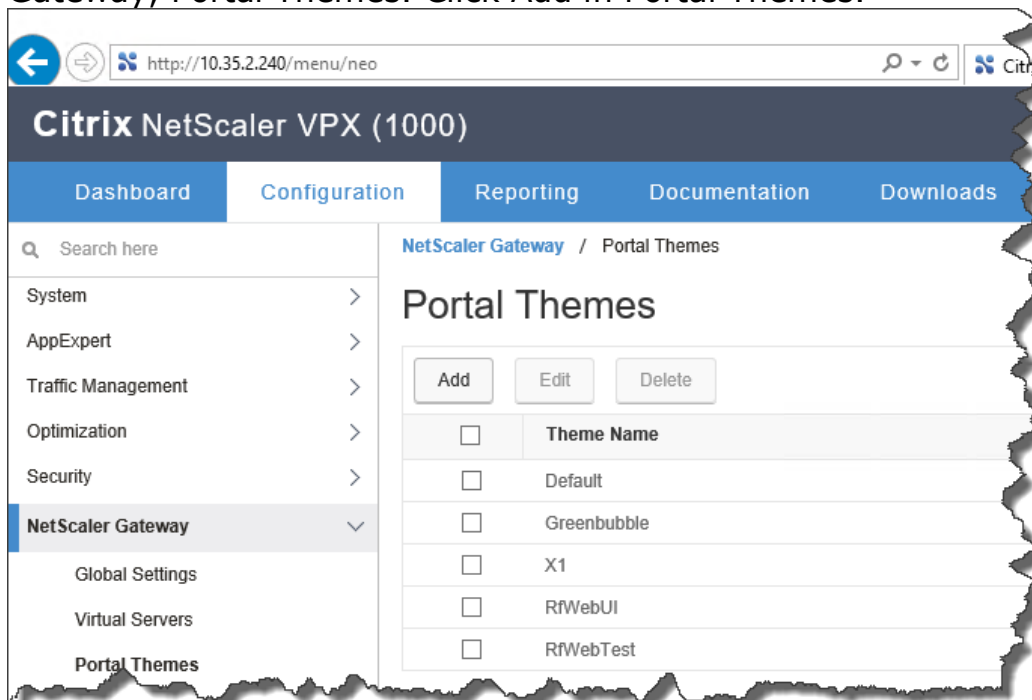
If you are not using the new theme in Netscaler 12, then please pay attention to the re-write section.

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

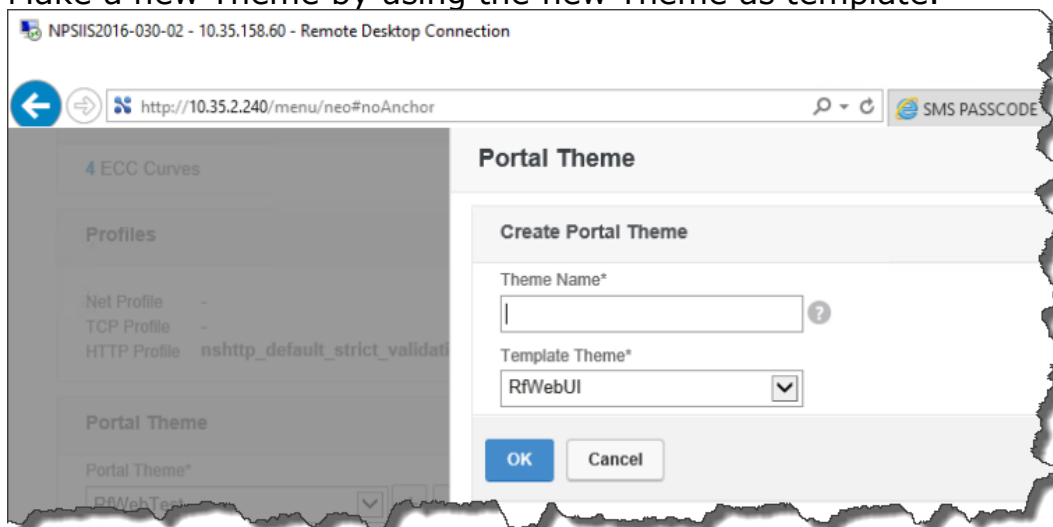


For Netscaler 12 with new Netscaler 12 Theme.

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.





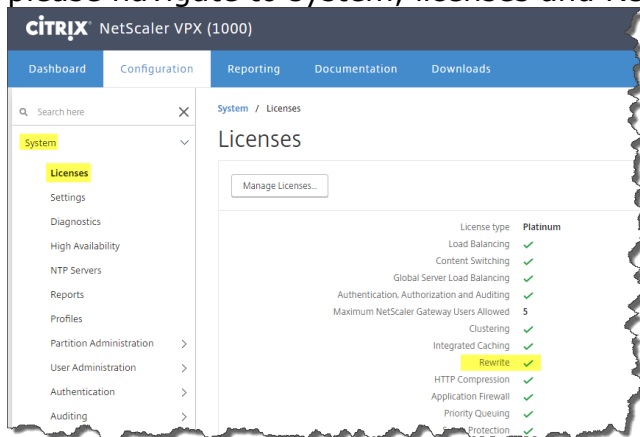
Make sure that your theme is the new theme and save your running configuration. Be patient, for some reason this change can take a couple of minutes to update. Drink a cup of coffee and then test it.

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.

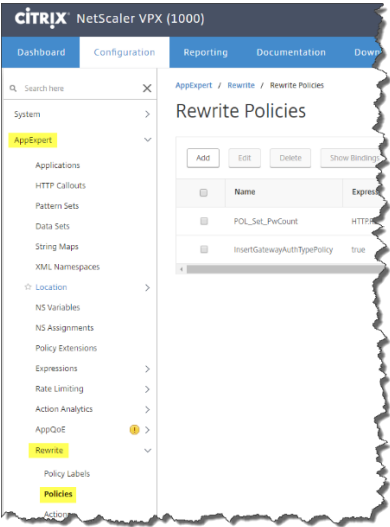
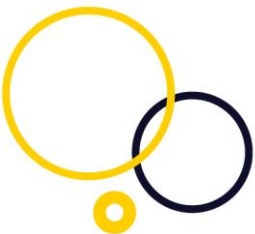
```
add rewrite action RWA-RES-REMOVE_2ND_PASSWORD replace_all "HTTP.RES.BODY(99999)"
"\r\n\r\n"+\n"<style type=\\\"text/css\\\">\r\n\r\n"+\n\"[for=\\\"passwd1\\\"] { display:
none;}\\r\n\r\n"+\n\"#passwd1 { display: none;
}\\r\n\r\n"+\n\"</style>\r\n\r\n"+\n\"\\r\n\r\n"+\n\"</body>\r\n\r\n"+\n\"</html>\r\n\r\n\" -search
"text(\n</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.



NetScaler VPX (1000)

Dashboard
Configuration
Reporting

Create Rewrite Policy

Name*

Action*

▼
+
✎

Log Action

▼
+
✎

Undefined-Result Action*

Expression*

Operators ▼

Saved Policy Expressions ▼

Frequency ▼

Press Control+Space to start the expression and then type '!' to

Comments

Create

Close

Please configure like this:
Type: INSERT_HTTP_HEADER.



Header name: Set-Cookie

Expression: "pwcount=0"

The screenshot shows the Citrix NetScaler VPX (1000) Configuration page. The main page is titled 'Create Rewrite Policy' and has a sidebar with 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The 'Configuration' tab is active. The main content area shows the 'Create Rewrite Policy' form with fields for Name, Action, Log Action, Undefined-Result Action, and Expression. The 'Configure Rewrite Action' dialog is open, showing the following details:

- Name: Set_PWCount
- Type: INSERT_HTTP_HEADER
- Use this action type to insert a header.
- Header Name*: Set-Cookie
- Expression: "pwcount=0"
- Comments: (empty)

The dialog has 'OK' and 'Close' buttons at the bottom.

The Rewrite policy needs an expression:



```
HTTP.REQ.HOSTNAME.CONTAINS("ng.smspsscode.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
```

NetScaler VPX (1000)

HA Sta...
Not ...

Dashboard
Configuration
Reporting
Documentation
Downloads

Create Rewrite Policy

Name*

Action*

Set_PWDCount
+

Log Action

+

Undefined-Result Action*

-Global-undefined-result-action-

Expression*

Operators
Saved Policy Expressions
Frequently Used Expressions

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

Evaluate

Comments

Create
Close



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"

[Choose Type](#) / [Configure Rewrite Policy](#) / [Configure Rewrite Action](#)

Configure Rewrite Action

Name

InsertGatewayAuthHeader

Type

INSERT_HTTP_HEADER ▼

Use this action type to insert a header.

Header Name*

X-Citrix-AM-GatewayAuthType

Expression

Operators ▼

Saved Policy Expressions ▼

Frequently Used Expressions ▼

"SMS"

In string expressions, string constants and expressions can be concatenated with "+" operator. Please make sure that string

Comments

OK

Close



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

CITRIX NetScaler VPX (1000)

DashboardConfigurationReportingDocumentationDownloads

[←](#) Configure Rewrite Policy

Name

InsertGatewayAuthTypePolicy

Action*

InsertGatewayAuthHeader

+

Log Action

+

Undefined-Result Action*

-Global-undefined-result-action-

Expression*

Operators

Saved Policy Expressions

Frequently Used Expressions

true

Comments

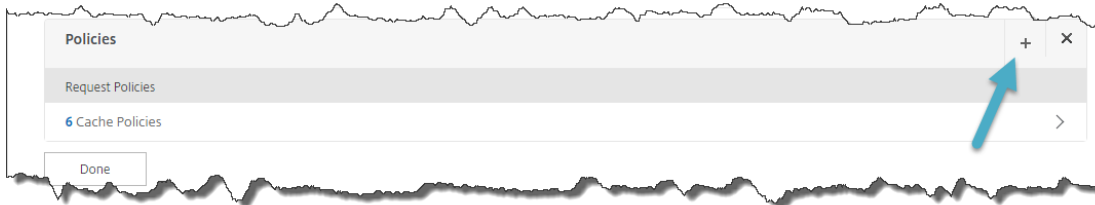
?

OK

Close



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.

Choose Type

Policies

Choose Policy*

Rewrite ▼

Choose Type*

Response ▼

Continue **Cancel**



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

CITRIX® NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

VPN Virtual Server

Basic Settings

Name	GHENS11
IP Address	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

Certificate

1 Server Certificate

No CA Certificate

Basic Authentication

Primary Authentication

1 RADIUS Server

Choose Type

Choose Policy

Rewrite

Policy Binding

Select Policy*

GHE_PWD_COUNT

More

Binding Details

Priority*

100

Goto Expression*

END

Bind Close

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

Policies	+	×
Request Policies		
6 Cache Policies		
Response Policies		
2 Rewrite Policies		

Done



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.

The image shows the 'Configure Authentication RADIUS Server' page in the Netscaler GUI. The page has a breadcrumb trail: 'VPN Virtual Server Authentication RADIUS Policy Binding / Configure Authentication RADIUS Server'. The main title is 'Configure Authentication RADIUS Server'.

Fields on the page include:

- Name: GHE_RAD_Test1
- Server Name (radio button) / Server IP (radio button, selected)
- IP Address*: 10 . 35 . 154 . 67
- Port*: 1812
- Secret Key*: [Redacted]
- Confirm Secret Key*: [Redacted]
- Test Connection button
- Time-out (seconds): 10
- ☒ Send Calling Station ID
- NAS ID: [Redacted]
- ☐ Enable NAS IP address extraction
- Group Vendor Identifier: [Redacted]
- Group Prefix: [Redacted]
- Group Attribute Type: [Redacted]
- Group Separator: [Redacted]
- IP Address Vendor Identifier: 0
- IP Address Attribute Type: [Redacted]
- IP Address Vendor Identifier: [Redacted]

A 'RADIUS Settings' dialog box is open, showing the 'Authorization' tab. The 'Inherit default settings' checkbox is unchecked. The 'Authorization enabled' checkbox is checked. The 'Authorization attribute properties' section includes:

- Max size of attributes: 2048
- Vendor code: 1
- Attribute number: 99
- Prefix: CTXSUserGroups=
- Separator: :

The 'Restrict groups collected into the authorization attribute' section has a 'Restrict to groups:' list with 'Add', 'Remove', 'Up', and 'Down' buttons. At the bottom of the dialog are 'Reset to default settings...', 'Ok', and 'Cancel' buttons.

Blue arrows indicate the mapping of fields between the main page and the dialog box:

- From 'Group Vendor Identifier' to 'Vendor code'.
- From 'Group Prefix' to 'Prefix'.
- From 'Group Attribute Type' to 'Attribute number'.
- From 'Group Separator' to 'Separator'.



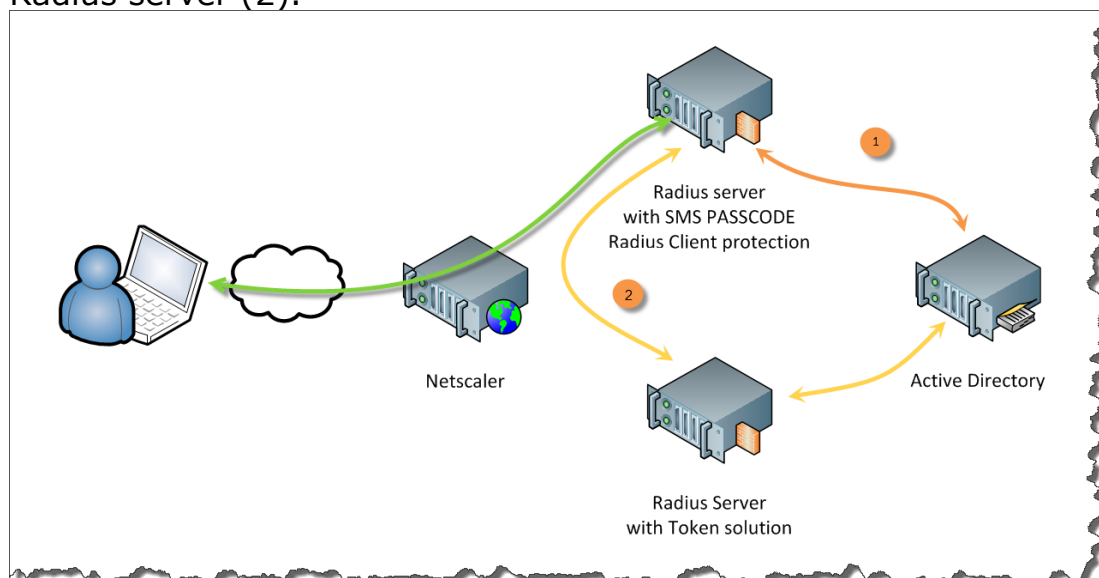
For further information regarding the authorization pane in the SMS PASSCODE configuration tool, please refer to the SMS PASSCODE administrators guide.

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

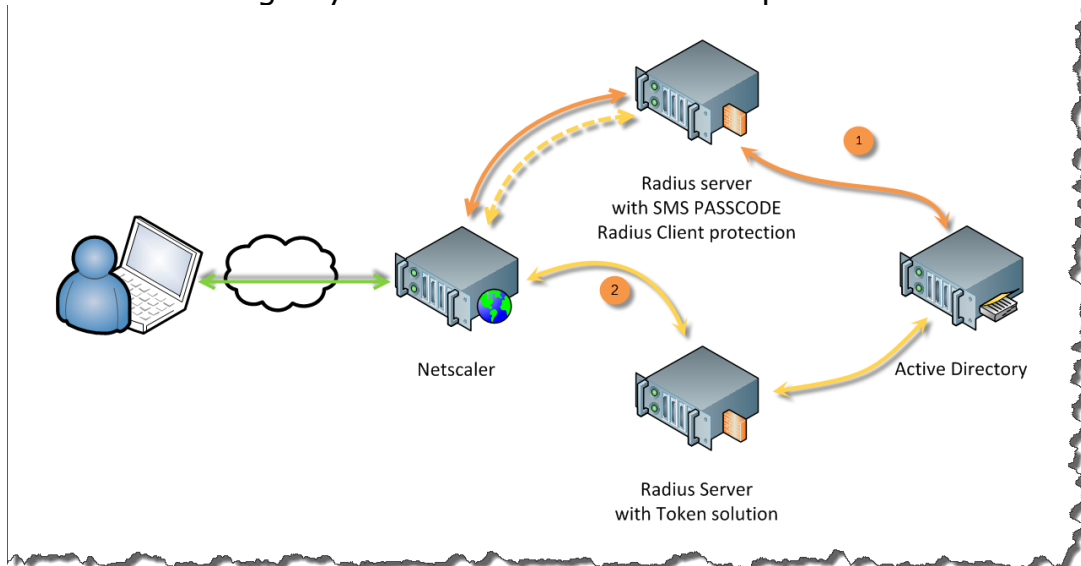
regular
token

^\\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.



CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

VPN Virtual Server

Basic Settings

Name	GHENS11	Maximum Users	0
IPAddress	10.35.2.246	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	UP	ICA Only	false
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	true	Mac EPA Plugin Upgrade	-
DTLS	false	ICA Proxy Session Migration	false
AppFlow Logging	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

<input type="checkbox"/>	Priority	Policy Name	Expression
<input type="checkbox"/>	100	GHERAD	ns_true
<input type="checkbox"/>	110	TokenDinosaurSolution	ns_true



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

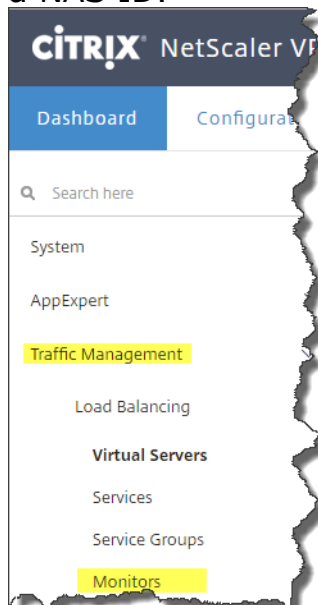
Create Monitor

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.



CITRIX® NetScaler VPX (1000)

Dashboard Configuration Reports

Create Monitor

Name*
GHE_LB_MON

Type*
RADIUS

Standard Parameters Special Parameters

Response Codes

2

User Name*
test1\testuser2010

Password*
....

RADIUS Key*
.....

NAS ID
NSProbeUser

NAS IP

Create Close



The Load Balancing Service Group.

Give the Load Balancing Service Group a name and make sure the Protocol is Radius. Please click OK.

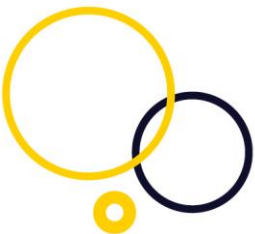
Once you save the Load Balancing Service Group, you will have the possibility to add Service Group Members.

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.

The screenshot shows the Citrix NetScaler VPX (1000) Configuration page for a Load Balancing Service Group. The page has a dark blue header with the Citrix logo and the text "NetScaler VPX (1000)". Below the header are three tabs: "Dashboard", "Configuration", and "Reporting". The "Configuration" tab is selected. The main content area is titled "Load Balancing Service Group" with a back arrow icon. Below the title is a "Basic Settings" section. The settings include:

- Name*: GHE_LB_SG
- Protocol*: RADIUS
- Traffic Domain: (empty dropdown)
- Cache Type*: SERVER
- AutoScale Mode: (empty dropdown)
- Cacheable: ☐
- State: ☒
- Health Monitoring: ☒
- AppFlow Logging: ☒
- Monitoring Connection Close Bit: (empty dropdown)
- Number of Active Connections: (empty input field)

At the bottom of the form are two buttons: "OK" and "Cancel".



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

CITRIX® NetScaler VPX (1000)

DashboardConfigurationReportingDocumentationDownloads

← Load Balancing Service Gro

Basic Settings

Name

GHE_LB_SG

Protocol

RADIUS

State

ENABLED

Effective State

DOWN

Traffic Domain

0

Service Group Members

No Service Group Member

OK

Create Service Group Member

☒ IP Based

☐ Server Based

IP Address/IP Address Range*

10

.

35

.

154

.

67

☐ IPv6

Port*

1812

Weight

1

Server Id

Hash Id

☒ State

Create

Close



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.

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

Protocol*

IP Address Type*

IP Address*

Port*

Traffic Domain

Range

Redirection Mode*

☒ Virtual Server State

☐ RHI State

☒ AppFlow Logging

Listen Priority

Listen Policy Expression Expression Editor

Press Control+Space to start the expression and then type ':' to get the next set of options

Evaluate

Comments

▲ Less



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

Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings

Name	GHE_LB_VS	Listen Priority	-
Protocol	RADIUS	Listen Policy Expression	NONE
State	DOWN	Range	1
IP Address	10.38.3.255	Redirection Mode	IP
Port	1812	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED

Services and Service Groups

No Load Balancing Virtual Server Service Binding

1 Load Balancing Virtual Server ServiceGroup Binding

Traffic Settings

Health Threshold	0	Priority Queuing	OFF
Client Idle Time-out	120	Sure Connect	OFF
Minimum Autoscale Members	0	Down State Flush	ENABLED
Maximum Autoscale Members	0	Layer 2 Parameters	OFF
ICMP Virtual Server Response	PASSIVE		

Persistence

Configure persistence to route all connections from the same user to the same service, such as an application that includes a shopping cart or that handles banking transactions. With some persistence types, you can configure backup persistence, which takes effect if the primary persistence type fails.

Persistence*

SOURCEIP

Time-out (mins)*

3

IPv4 Netmask

255 . 255 . 255 . 255

IPv6 Mask Length

128

OK

Done

Help

Advanced Settings

Polices

Method

Protection

Profiles

Please also add the Service Group members and the Monitor.

Monitors

1 Service Group to Monitor Binding

Service Group Members

2 Service Group Members



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

CITRIX NetScaler VPX (1000)

Dashboard Configuration Reporting Documentation Downloads

VPN Virtual Server

Basic Settings

Name	GHEN511
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

Configure Authentication RADIUS Server

Name: GHE_RAD_Test1

☐ Server Name ☒ Server IP

IP Address*: 10.38.3.255

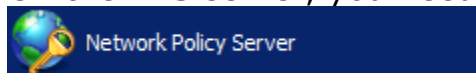
Port*: 1812

Secret Key*:

Confirm Secret Key*:

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

New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name: NSProbe

Network connection method: Unspecified

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server: Unspecified

☐ Vendor specific: 10

Previous Next Finish Cancel



Add a condition.

New Connection Request Policy

Specify Conditions
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Condition	Value

Condition description:

Buttons: Add... Edit... Remove

Navigation: Previous Next Finish Cancel

The condition must be NAS ID

Select condition

Select a condition, and then click Add.

- Called Station ID**
The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.
- NAS Identifier**
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.
- NAS IPv4 Address**
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.
- NAS IPv6 Address**
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.
- NAS Port Type**
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

Buttons: Add... Cancel

The value must be 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.



NAS Identifier

Specify the name of the network access device that sent the access request message.

NSProbe

OK Cancel

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.

SMS PASSCODE® - Configuration Tool

Database Backend Hosts Network End-user IP
Password Reset RADIUS Client Protection Import/Export About

Connection Request Policy	SMS PASSCODE Protection	Using Default Settings	Settings
Cisco Anyconnect	<input checked="" type="checkbox"/>	X	Edit...
NSProbe	<input type="checkbox"/>	X	
Use Windows authentication for all users	<input checked="" type="checkbox"/>	X	Edit...

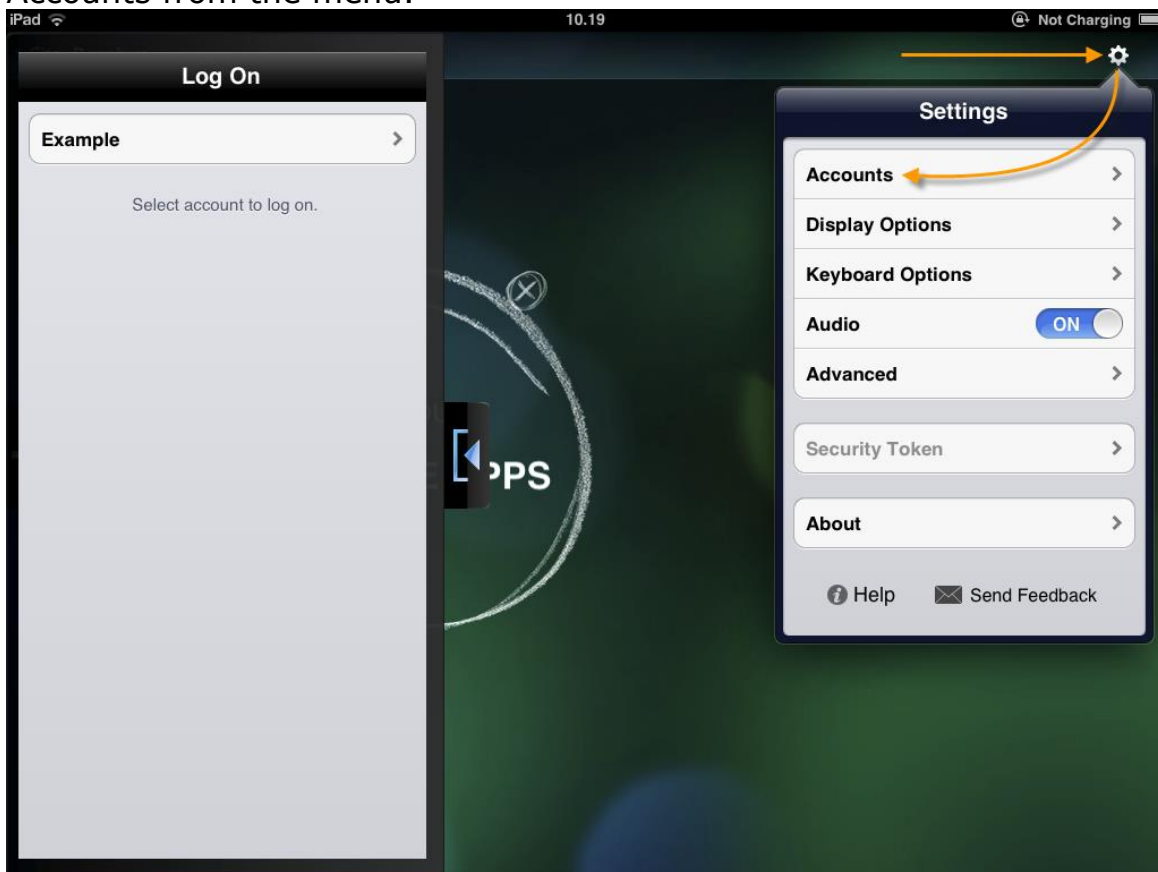
Edit default settings...

Save Cancel Close

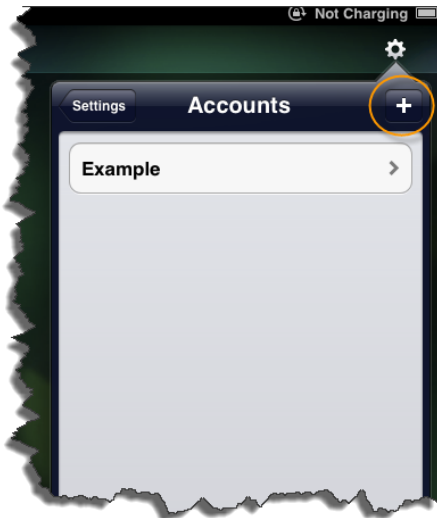


Configure settings for the "Citrix receiver for iPad/iPhone" with Citrix receiver 5.6+.

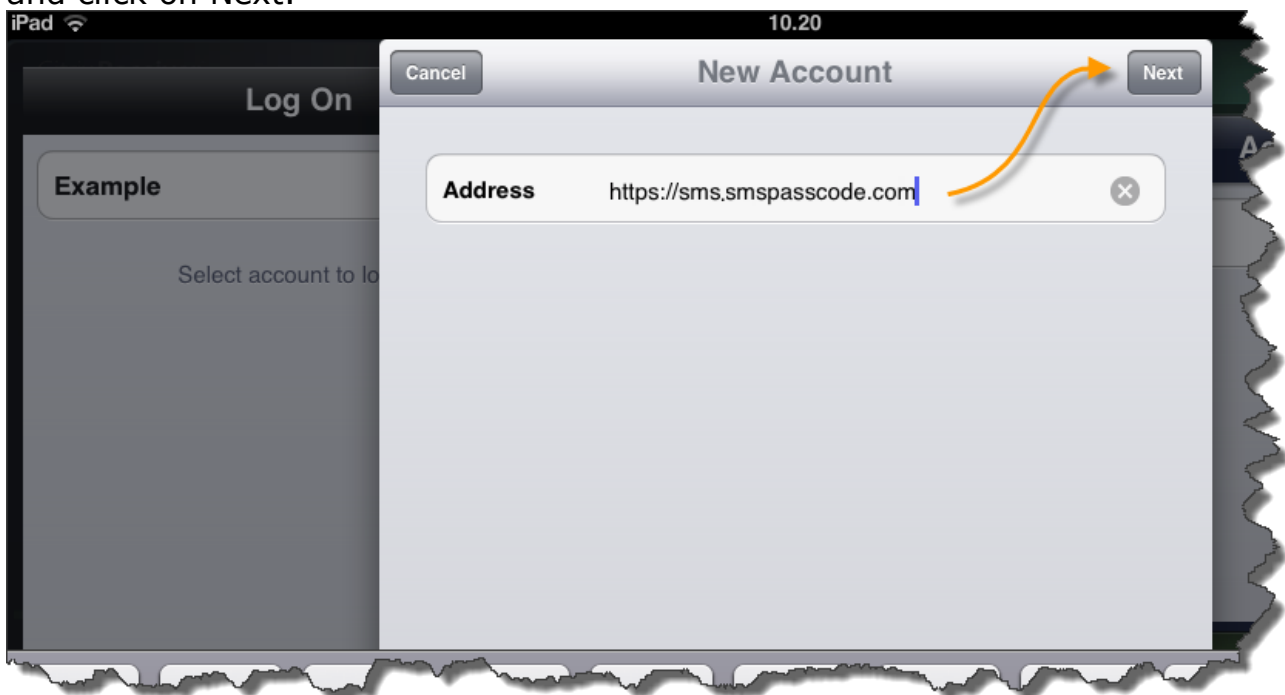
To configure the Citrix Receiver, please open it, navigate to settings, and choose Accounts from the menu.



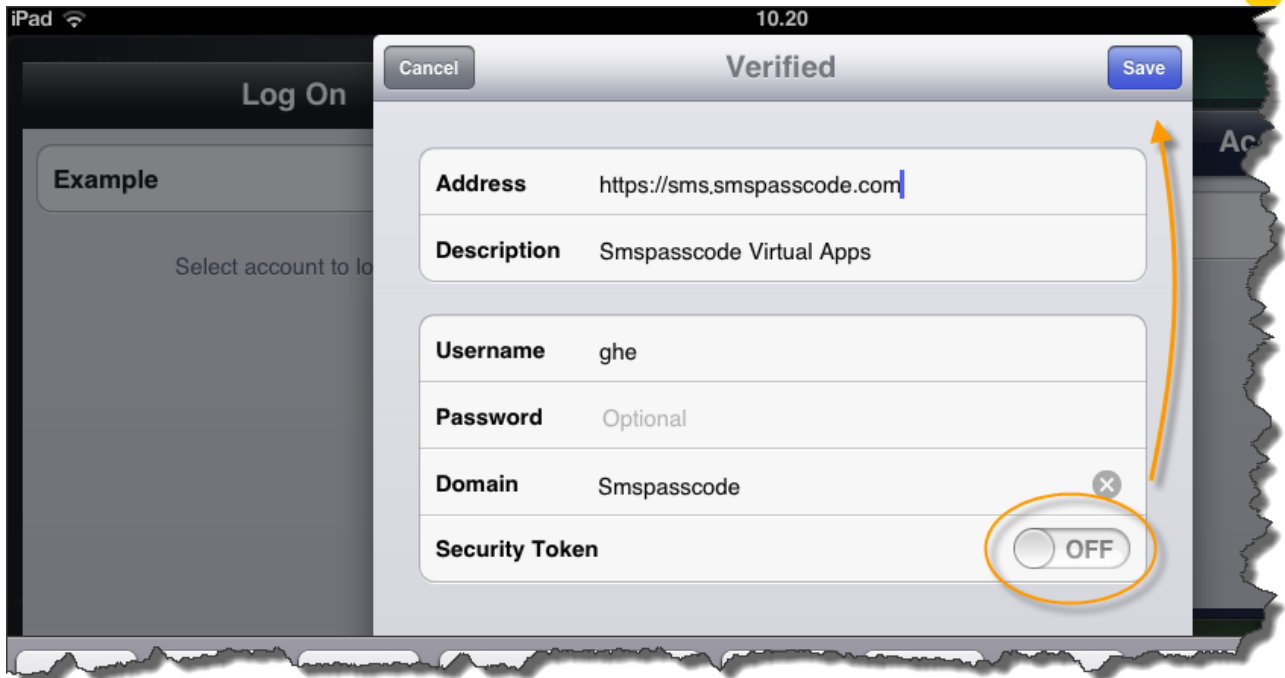
To add an account please click on the + sign.



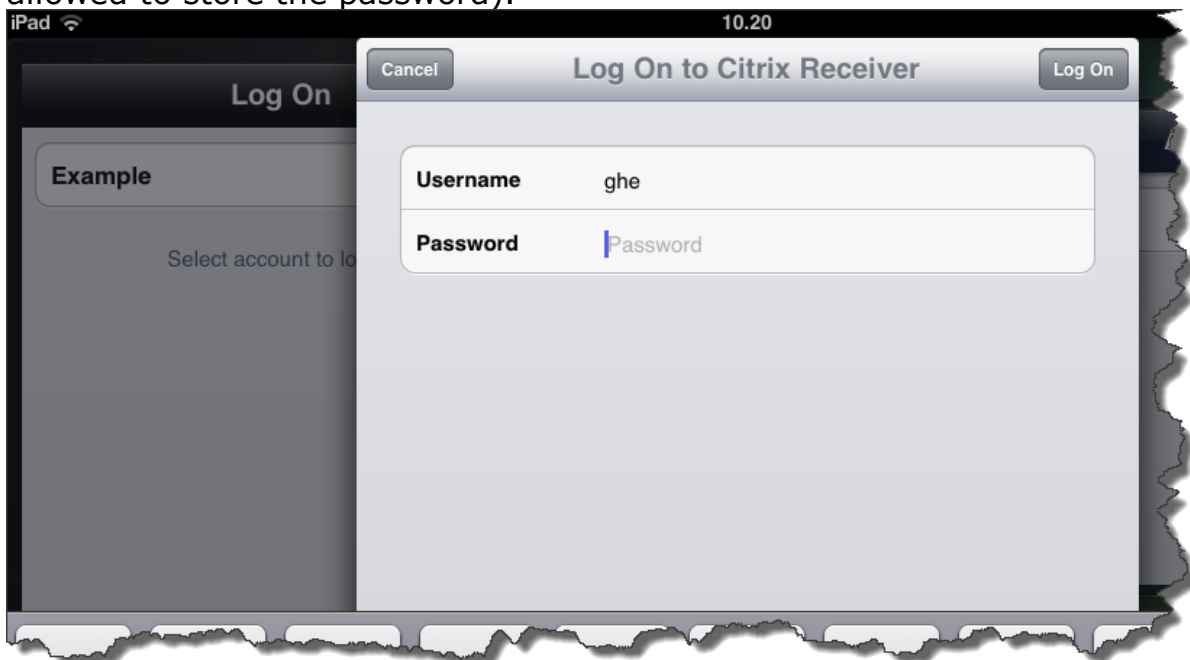
Now enter the URL of your Citrix Access Gateway Enterprise Edition / Netscaler, and click on Next.



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

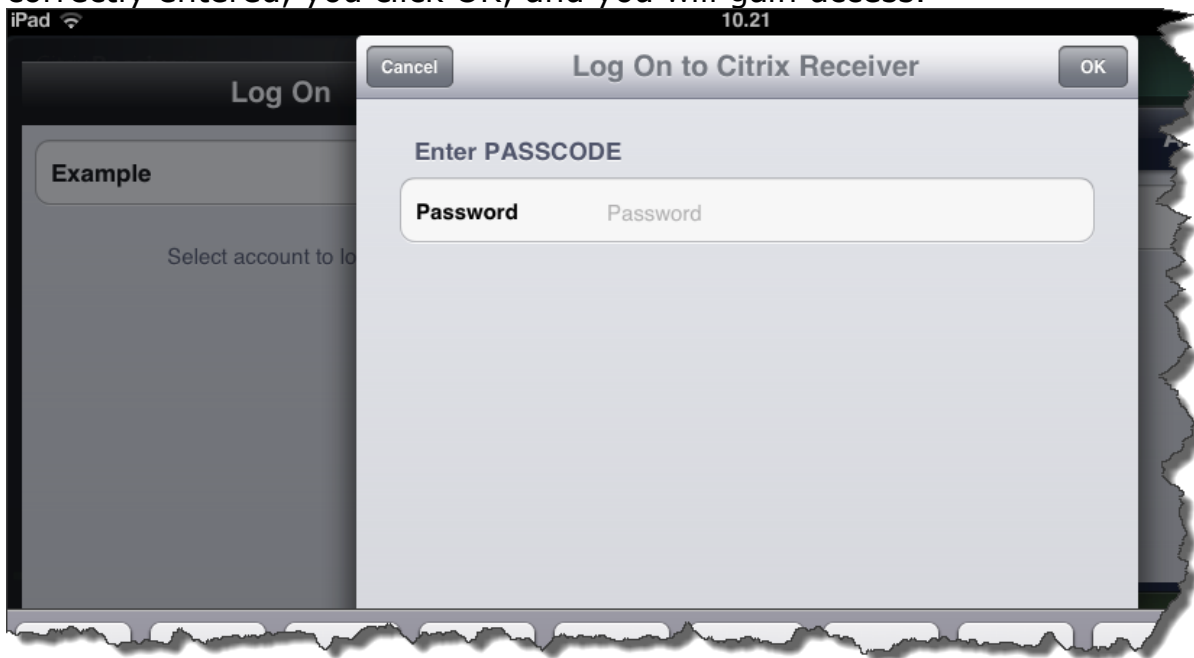


Now you are ready to use your Citrix Receiver. Your experience should look like this (This window will show if the password has not been saved or if it is not allowed to store the password).





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.

