



SMSPassword

Citrix Netscaler

configuration guide v1.6
Juli 2018



Citrix **Net**Scaler

[1 A quick installation guide with Citrix Netscaler](#)

[Step 1. Run setup.exe](#)

[Step 2. Run the configuration utility:](#)

[Step 3. In Domain settings](#)

[Step 4. Open Active Directory Users and Computers](#)

[Step 5. Go back to the SMSPassword configuration tool.](#)

[5.1 SMSPassword A100 dispatcher](#)

[5.2 External SMS dispatcher mode](#)

[Step 6. Configure your netscaler.](#)

[Step 7. Configure your firewall](#)

[2 - Load balanced setup with Netscaler](#)

[Things to consider before starting:](#)

[To enable load balancing by using the netscaler configuration utility](#)

[Step 1 Setting up the A100 SMS dispatchers](#)

[Step 2 Installing the SMSPassword servers](#)

[Step 3 Installing the SMSPassword service](#)

[Step 4 Configure the Netscaler](#)

[General Disclaimer and Copyright Notice](#)

[Disclaimer](#)

[Copyright Notice](#)

1 A quick installation guide with Citrix Netscaler

For a minimal setup we need at least one server to run the SMSPassword-service. This can be an existing server. You have to consider the port that the SMSPassword-service uses. In this case port 1812 is defined for radius traffic. If this port is currently in use on the server, you can either configure RADIUS to use a different port, or use a different server.

For the purposes of this manual, we'll assume that the server is new and no required ports are in use;

Prepare a windows server;

- Create a (virtual) windows server (2008/2012/2016). Standard and datacenter editions are both supported.
- Configure a fixed IP address.
- Add the computer to the domain.
- Install .NET feature/framework 4.0 or newer.
- Optional: Disable the firewall/UAC.

Step 1. Run setup_smspassword.exe;

The installation is fairly straightforward, make sure to *Run as Administrator*. The only choice you have to make is your destination folder.

Step 2. Initial SMSPassword Configuration;

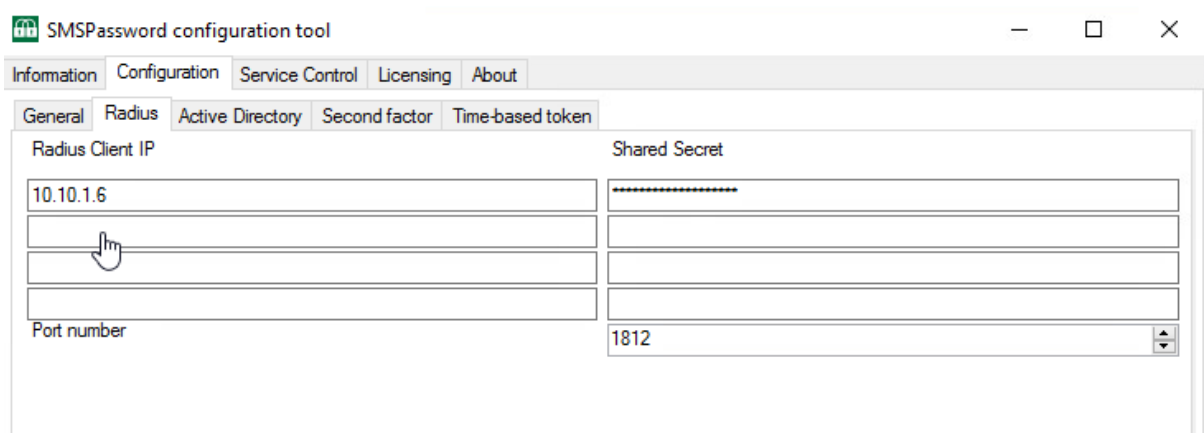
Run the configuration utility. This is where all configuration regarding SMSPassword is done. Open the Configuration tab.

Step 2a. General tab

Under General, enable Verbose logging. This will help with locating any issues during the installation process.

Step 2b. RADIUS tab

Under Radius, fill in your Netscaler NSIP address under *Radius Client IP*.



The screenshot shows the 'SMSPassword configuration tool' window with the 'RADIUS' tab selected. The 'Radius Client IP' field is filled with '10.10.1.6'. The 'Shared Secret' field is filled with a series of asterisks. The 'Port number' field is set to '1812'. The window has tabs for 'Information', 'Configuration', 'Service Control', 'Licensing', and 'About'. The 'Configuration' tab has sub-tabs for 'General', 'Radius', 'Active Directory', 'Second factor', and 'Time-based token'.

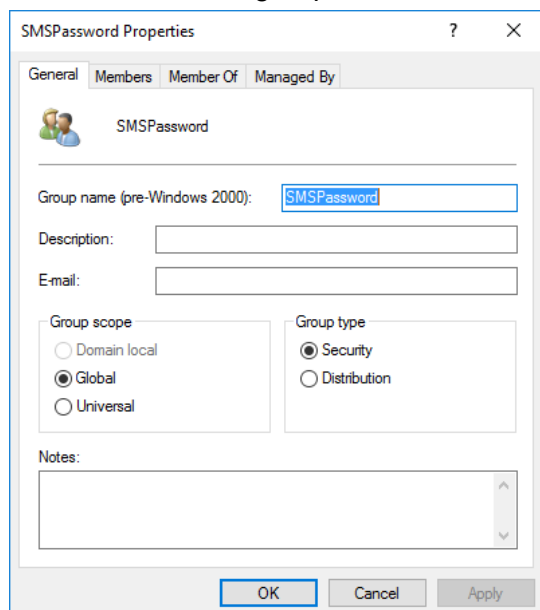
Make up a new password and enter it in the *Shared Secret* field. Make sure this password is saved in a place where other system administrators can find it. You will need this password later! You cannot recover the password from this tool, so it's very important to save it somewhere. (KeePass, etc.)

Step 2c. Active Directory tab

Fill in your full Domain DNS name (ex: gourami.local) under *Domain*. Leave the two other fields default: SMSPassword and mobile.

Step 4. Active Directory Group

Open *Active Directory Users and Computers*. Create a new global security group called 'SMSPassword'. Everyone who is going to use SMSPassword two-factor authentication has to be added to this group. SMSPassword supports nesting of AD Groups..



The screenshot shows the 'SMSPassword Properties' dialog box with the 'General' tab selected. The 'Group name (pre-Windows 2000):' field is filled with 'SMSPassword'. The 'Description' and 'E-mail' fields are empty. The 'Group scope' section has 'Global' selected. The 'Group type' section has 'Security' selected. The 'Notes' field is empty. The dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

4a. User Properties

Make sure your test user has the 'mobile' property filled and is a member of the previously created 'SMSPassword' group.

The left screenshot shows the 'John Smith Properties' dialog box with the 'Telephones' tab selected. The 'Mobile' field is highlighted with a yellow box and contains the number '44123123456'. The right screenshot shows the same dialog box with the 'Member Of' list selected. The list shows 'Domain Users' as the primary group, and 'smspassword' is listed as a member of the 'Domain Users' group. The 'smspassword' entry is highlighted with a yellow box.

Step 5. Go back to the SMSPassword configuration tool.

Under the tab Configuration, under 'SMS', configure your SMS dispatcher mode.

5.1 SMSPassword A100 dispatcher

If you use the SMSPassword A100 SMS dispatcher, follow the included manual.

5.2 External SMS dispatcher mode

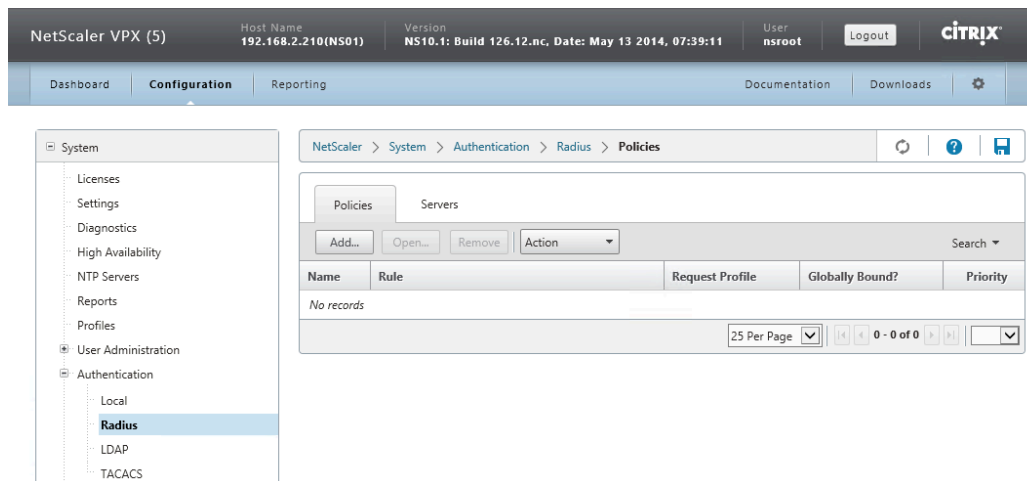
This can be an external dispatcher like BlukSMS or MessageBird. Enter the correct URL and fill in your account's username and password. Send a test SMS to see if your configuration is correct.

Also make sure that you can reach the URL on the computer running SMSPassword. It might be necessary to open some firewall ports.

Save your settings by pressing the save config button. A file called smspassword.cfg is created in the same folder as smspasswordconfig.exe.

Step 6. Configure your netscaler.

-Log on to your Citrix Netscaler, and go to 'System', 'Authentication', 'Radius'.



-Press 'Add...' to add an authentication policy.

-In the Name field enter: smspassword_ap

-Under server, press New  New...

-In the box 'Create Authentication Server', type as name: smspassword

-In the IP address use your fixed IP address of the server running the SMSPassword service.

-Fill in the shared secret created in step 2. Twice...

-The rest should be like this; Password encoding: Pap, port and timeout 1812 and 100.

-Press Create

-Go back to the configure authentication Policy box,

-Under named expressions, select the second drop down, go all the way down, and select True value.

-Press the green plus to add an expression, an ns_true value appears in the expression box.

Create Authentication Policy

Name*

Authentication Type

Server [New...](#) [Modify...](#)

Expression

Expression

ns_true

Match Any Expression ☐ AND ☐ OR

Named Expressions [Add Expression](#)

Preview Expression

[Help](#) [Create](#) [Close](#)

-Press create

-Bind you radius policy to your where you need it; for example your Netscaler Gateway Virtual Server;

Configure NetScaler Gateway Virtual Server

Name* IP Address*

Protocol* Port*

☐ Network VServer Range Failed Login Timeout

☐ SmartAccess Mode ☒ Basic Mode ☐ AppFlow Logging ☒ Down state flush ☐ Double Hop

Max Users Max Login Attempts

[Certificates](#) [Authentication](#) [Bookmarks](#) [Policies](#) [Intranet Applications](#) [Intranet IPs](#) [Published Applications](#) [Advanced](#)

User Authentication

If your NetScaler Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.

☒ Enable Authentication

Authentication Policies

[Primary](#) [Secondary](#) [Group Extraction](#)

Priority	Policy Name	Expression	Profile
100	New Policy...		
	ac_idap		
	smspassword_ap		

Details

No details available.

[Insert Policy](#) [Unbind Policy](#) [Regenerate Priorities](#) [Modify Policy](#)

Comments

[Help](#) [OK](#) [Close](#)

Don't forget to save your changes.

Step 7. Configure your firewall

If you have a firewall in your environment, you'll need to open some ports:

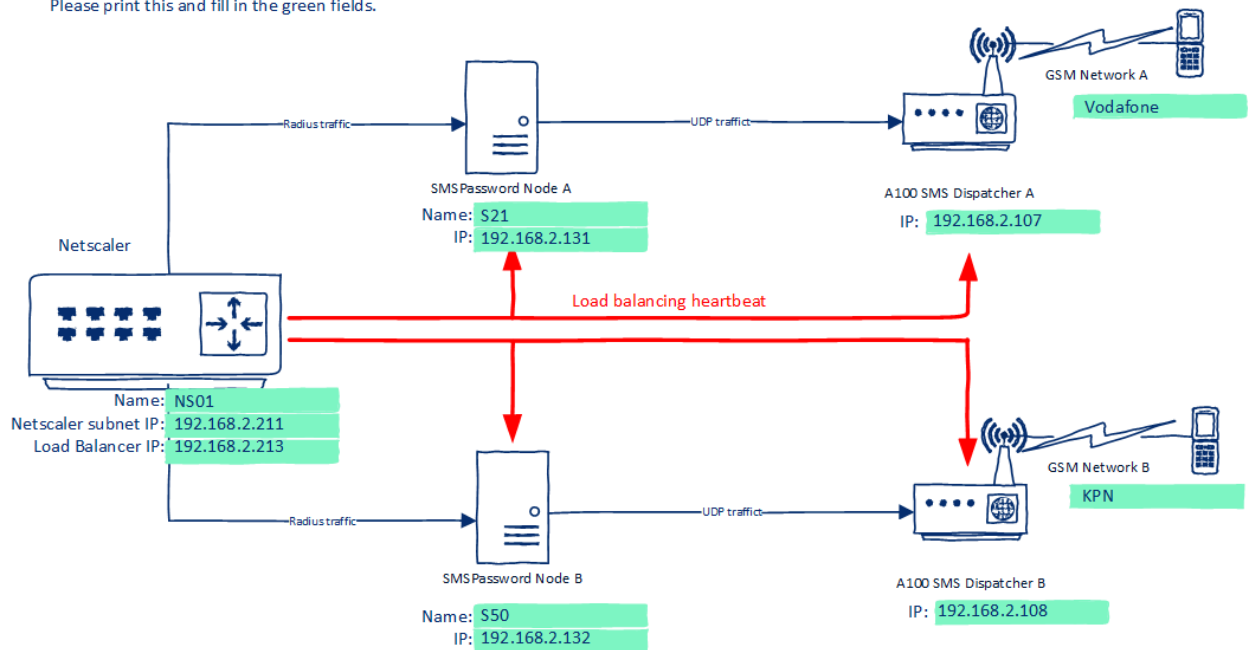
- From the netcaler to all servers running the SMSPassword service, port 1812 has to be open for radius traffic. Unless you have chosen to run the Radius service on a different port.
- The computer running the SMSPassword service should be able to contact your SMS dispatcher service.

2 - Load balanced setup with Netscaler

When setting up a load balanced configuration you need to remember a lot of IP addresses. To make things easier for you, we created a network drawing. Below you find a filled in example. In this manual we are going to use the IP addresses as shown in the drawing below.



SMSPassword load balancer setup sheet.
Please print this and fill in the green fields.

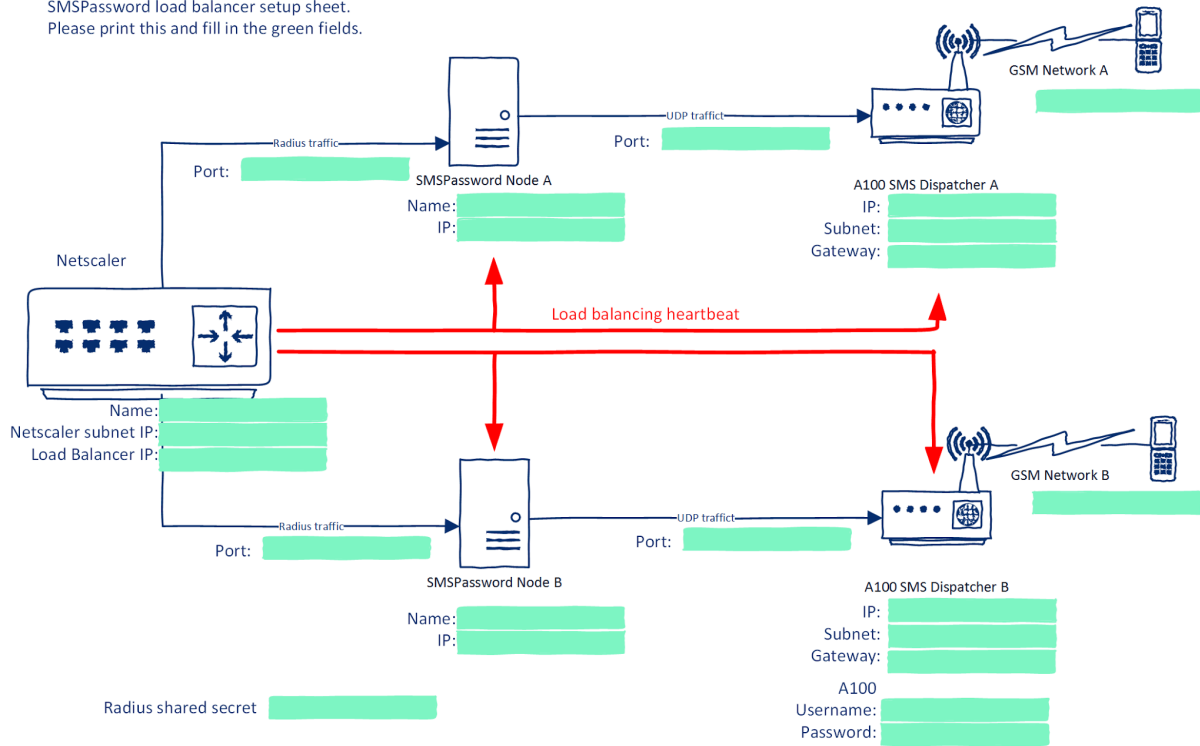


Filled in example network drawing

It's highly recommended that you fill in the empty network drawing before you start configuring everything. This will give you a good idea of what you are doing, and makes configuring a redundant SMSPassword setup even easier. Below you find the empty network drawing. Print this out, and fill in the green fields.



SMSPassword load balancer setup sheet.
Please print this and fill in the green fields.



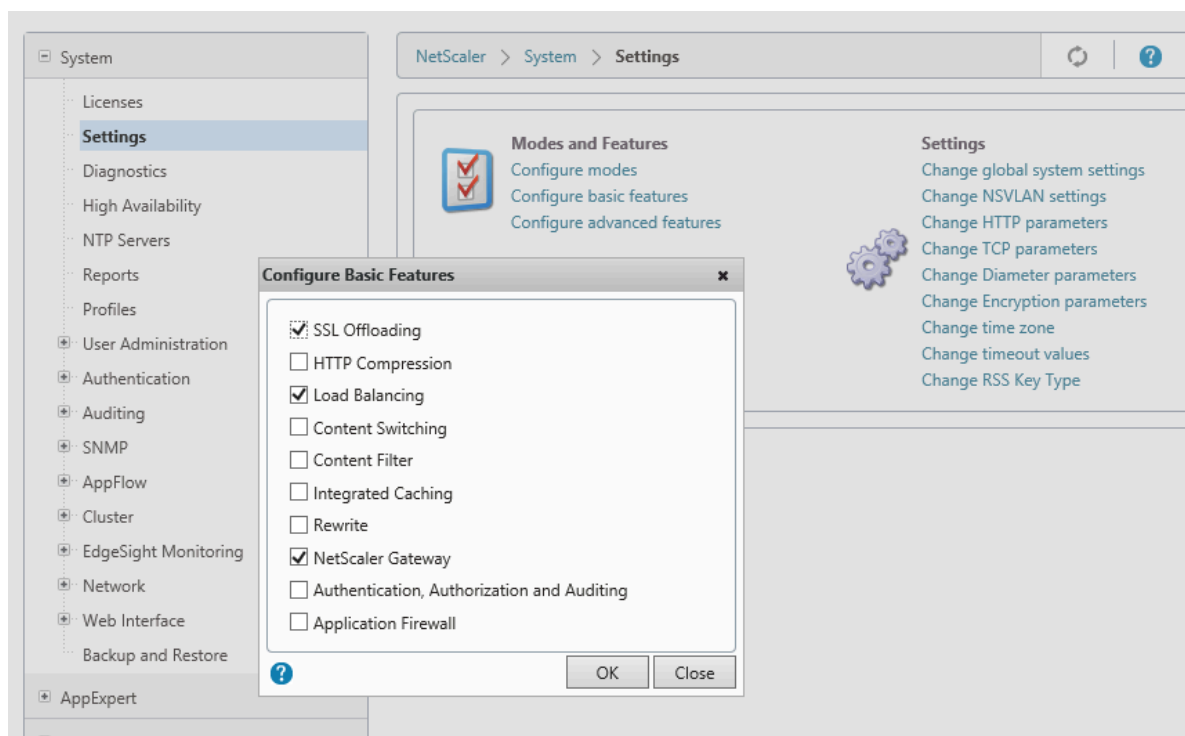
Template network drawing, print out and fill in

Things to consider before starting:

- Load balancing Radius is supported from Netscaler 9.2 and higher.
- In this tutorial we assume that everything is in one open network. Most production environments are not. Please, consider firewalls and subnets in your setup. Ask your network manager.
- Ensure the load balancing feature is enabled in Netscaler;

To enable load balancing by using the netscaler configuration utility

1. In the navigation pane, expand **System**, and then click **Settings**.
2. In the details pane, under **Modes and Features**, click **Change basic features**.
3. In the **Configure Basic Features** dialog box, select the **Load Balancing** check box, and then click **OK**.
4. In the Enable/Disable Feature(s)? message box, click **Yes**.



Step 1 Setting up the A100 SMS dispatchers

Configure the two A100 SMS dispatchers as described in the separate manual. It's recommended that you use a small sticker, and write 'SMSPassword dispatcher A' on device designated as NodeA, and write 'SMSPassword dispatcher B' on the device designated as NodeB.

fill in the correct time zone for each SMS dispatcher a

SMSPassword dispatcher A:

- Network Configuration, IP Address: 192.168.2.107
- Fill in the correct subnet mask
- Enter the correct time zone, Preference, Time Zone

- Choose you reboot time different from the other dispatchers
- We use 192.168.2.**131** as SMS server. This is the server running the actual SMSPassword service.
- As SMS server port we use 44444
- client ID is 11
- We used 'sms' as password.

SMS Sender	☒ Enable ☐ Disable
SMS Server IP	192.168.2.131
SMS Server Port	44444
SMS Client ID	11
Password	...
HTTP Port	80

SMSPassword dispatcher B:

- is given IP adress 192.168.2.**108**
- Fill in the correct subnet mask
- Enter the correct time zone, Preference, Time Zone
- Choose you reboot time different from the other dispatchers
- We use 192.168.2.**132** as SMS server. This is the server running the actual SMSPassword service.
- As SMS server port we use 44444
- client ID is 11
- We used 'sms' as password.

SMS Sender	☒ Enable ☐ Disable
SMS Server IP	192.168.2.132
SMS Server Port	44444
SMS Client ID	12
Password	...
HTTP Port	80

As described in the A100 manual, test to see if you can send SMS messages from both nodes.

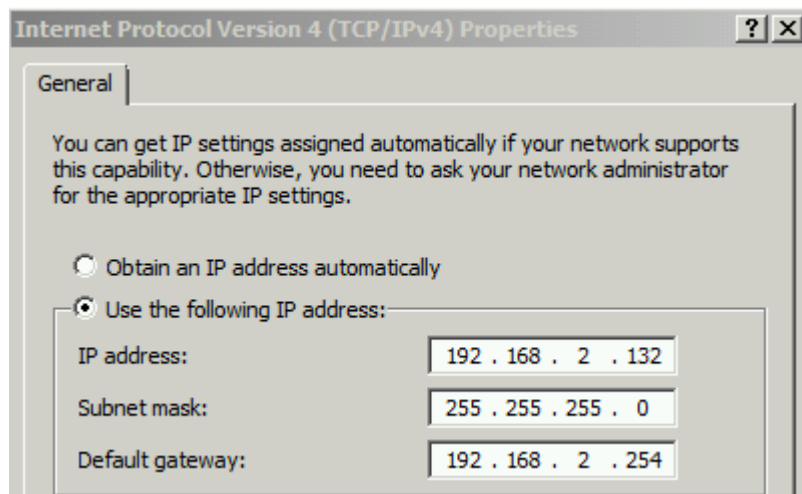
Step 2 Installing the SMSPassword servers

Find two servers that meet the requirements for SMSPassword. These can be two existing servers. For example, the Storefront servers. Make sure that your radius port (1812 default) is not already in use! In this example we use new servers.

Configure the servers to have static IP addresses:

For SMSPassword NodeA: 192.168.2.131

For SMSPassword NodeB: 192.168.2.132



The windows firewall can block ports; in our configuration example we completely disabled the windows firewall. You can also open the ports you need (default is 1812).

Make sure you can reach the SMS A100 dispatcher from every node.

From the SMSPassword NodeA server you should: ping 192.168.2.107

From the SMSPassword NodeB server you should: ping 192.168.2.108

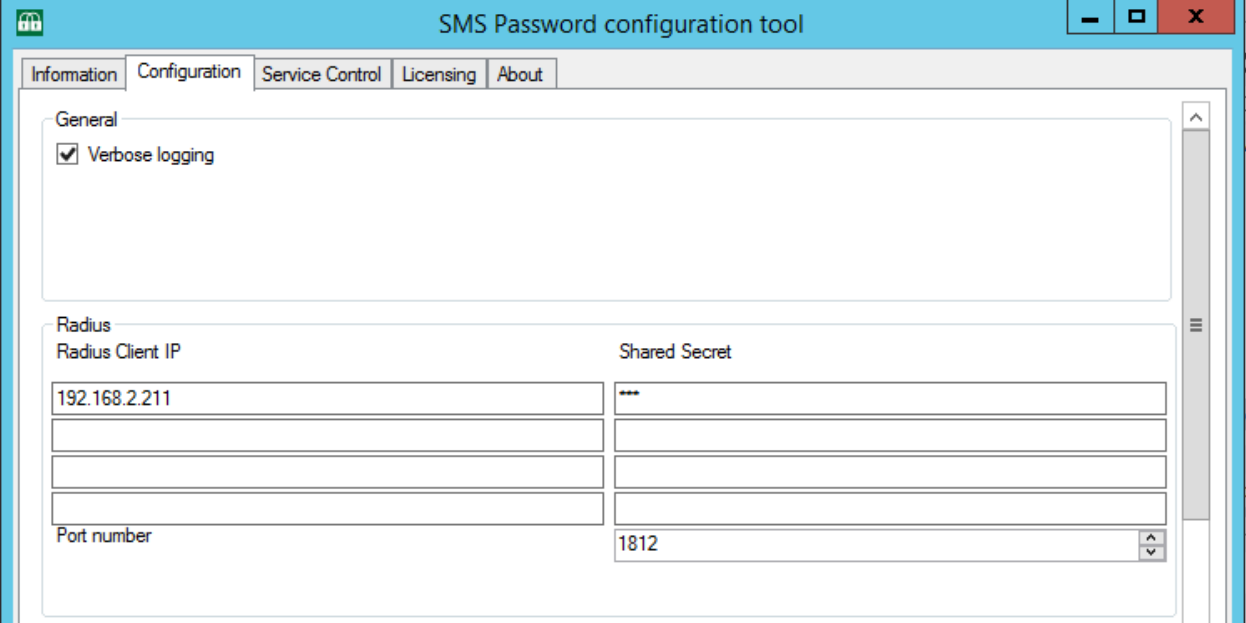
Make sure you join each of the servers to the domain.

Step 3 Installing the SMSPassword service

Install the software and run the configuration utility;

Both nodes should configure the Netscaler subnet IP as radius client. By default, Netscaler uses the NSIP to communicate with Radius. When you use a load balancing virtual server, Netscaler uses the SNIP as the Radius client IP.

In this example we are going to use a load balancing virtual server, so fill in the Netscaler subnet IP as the Radius Client IP:



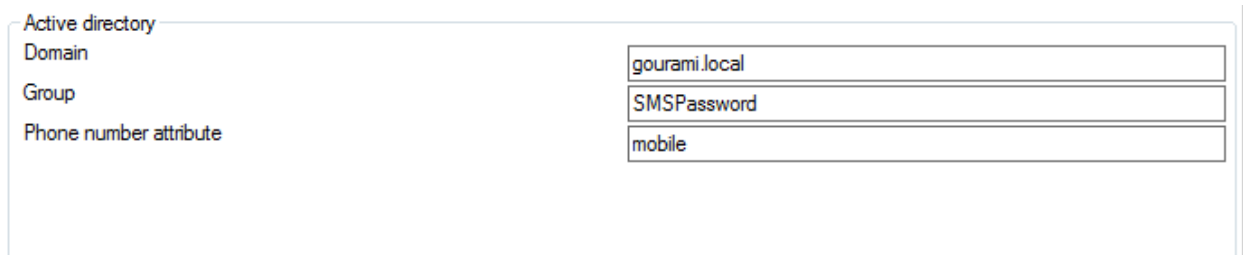
The screenshot shows the 'SMS Password configuration tool' window with the 'Configuration' tab selected. The 'Radius' section is expanded, showing the following fields:

Radius Client IP	Shared Secret
192.168.2.211	***

Below the table, the 'Port number' is set to 1812.

In this example, we use 'sms' as [Radius Shared Secret](#). You are free to use any password you like. Please make sure you document it for future use. Also, make sure to configure the same [Radius Shared Secret](#) in the Netscaler, in your Radius connector.

You should configure the same Active Directory information on both nodes:



The screenshot shows the 'Active directory' section with the following fields:

Domain	gourami.local
Group	SMSPassword
Phone number attribute	mobile

It's best practice to use the same setting for the one-time password on both nodes.

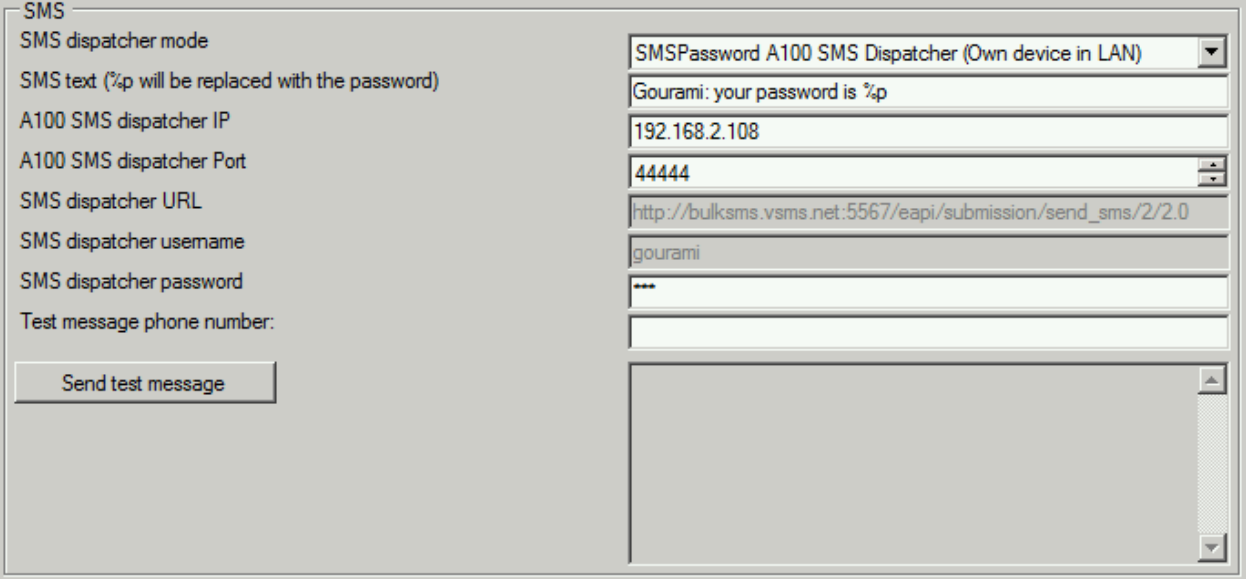
On SMSPassword NodeA service we are going to configure the SMS device like so:

SMS	
SMS dispatcher mode	SMSPassword A100 SMS Dispatcher (Own device in LAN) ▼
SMS text (%p will be replaced with the password)	Gourami: your password is %p
A100 SMS dispatcher IP	192.168.2.107
A100 SMS dispatcher Port	44444 ▲▼
SMS dispatcher URL	http://bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0
SMS dispatcher username	gourami
SMS dispatcher password	***
Test message phone number:	
Send test message	

Consult the network drawing; SMSPassword NodeA is using SMS dispatcher A. So, for this node, we are going to use the SMS dispatcher 192.168.2.**107**. In our example it sends using UDP port 44444. And, for this test we used 'sms' as password.

It's recommended to send a test SMS. Please consider the notation of the number. Some network operators expect a full international number.

On SMSPassword NodeB service we are going to configure the SMS device like so:



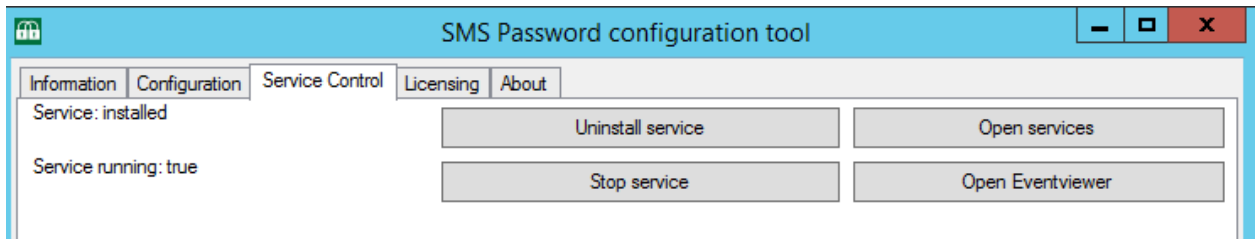
The screenshot shows a configuration window titled "SMS" with the following fields and values:

Field	Value
SMS dispatcher mode	SMSPassword A100 SMS Dispatcher (Own device in LAN)
SMS text (%p will be replaced with the password)	Gourami: your password is %p
A100 SMS dispatcher IP	192.168.2.108
A100 SMS dispatcher Port	44444
SMS dispatcher URL	http://bulksms.vsms.net:5567/eapi/submission/send_sms/2/2.0
SMS dispatcher username	gourami
SMS dispatcher password	***
Test message phone number:	

Below the fields is a "Send test message" button and a large empty text area for the test message content.

Consult the network drawing; SMSPassword NodeB is using SMS dispatcher B. So, for this node, we are going to use the SMS dispatcher 192.168.2.**108**. In our example it sends using UDP port 44444. And, for this test we used 'sms' as password.

It's recommended to send a test SMS. Please consider the notation of the number. Some network operators expect a full international number.

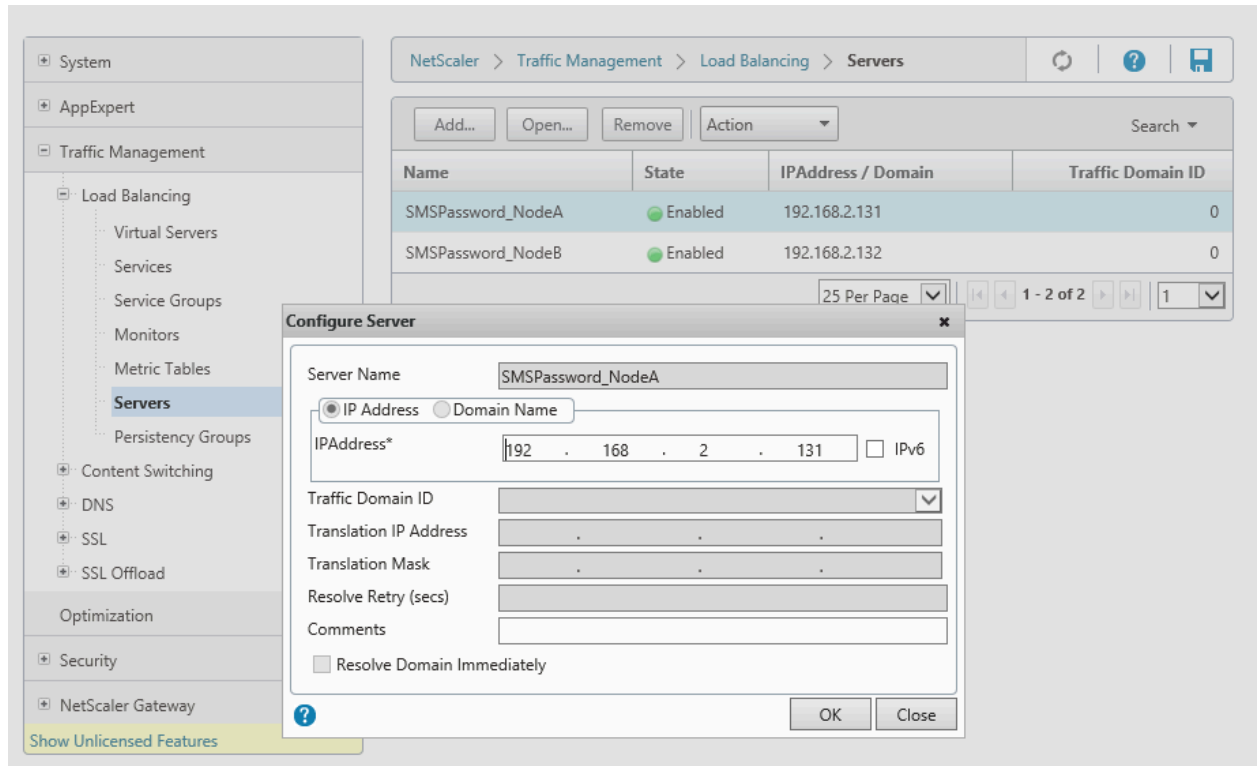


When you are done configuring both the SMSPassword nodes, make sure you install and start the service on both nodes.

Step 4 Configure the Netscaler

Please notice that radius load balancing is supported from Netscaler 9.2 and higher. Make sure you have enabled the load balancing feature of the netscaler.

The first thing to do is to add the two SMSPassword servers in the Netscaler. Go to traffic management, Load Balancing, Servers. Add our two SMSPassword servers with the IP addresses shown in the picture below.



Save the configuration

Make sure you can reach both of the SMSPassword servers from the Netscaler, by pinging them from the commandline of the Netscaler. It happens often that firewalls block this because the Netscalers are often in a DMZ.

Create a custom monitor, go to traffic management, load balancing, monitors, and click add. Name the monitor SMSPassword_RadiusMonitor as shown below.

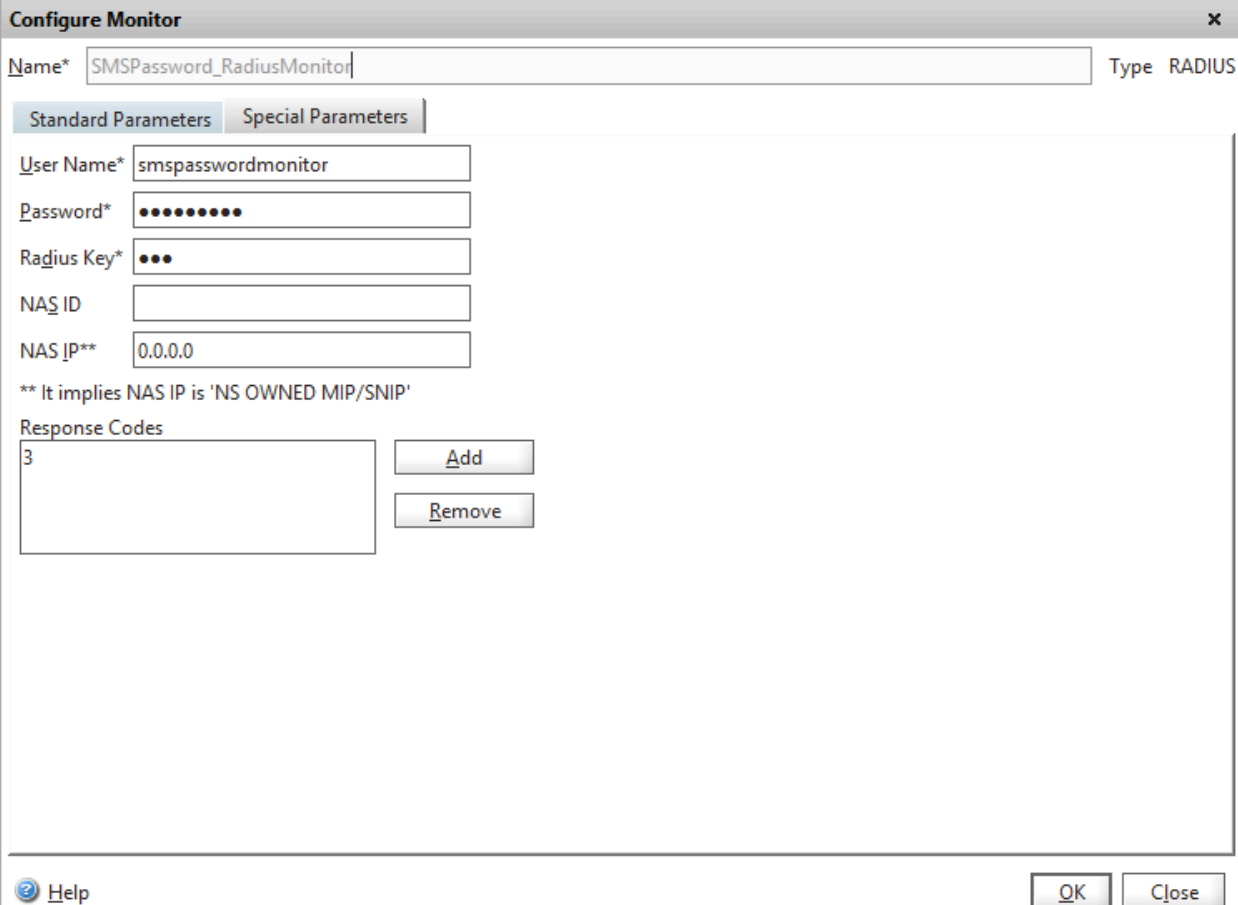
NetScaler > Traffic Management > Load Balancing > Monitors

Buttons: Add... Open... Remove Action Search

Name	State	Type
Configure Monitor Name* SMSPassword_RadiusMonitor Type RADIUS Standard Parameters Special Parameters Interval 5 Seconds Response Time-out 2 Seconds Down Time 30 Seconds Deviation Seconds Retries 3 SNMP Alert Retries 0 Success Retries 1 Failure Retries 0 ☒ Enabled ☐ Reverse ☒ LRTM (Least Response Time using Monitoring) ☐ TOS TOS Id 0 Destination IP . . . ☐ IPv6 Destination Port Dynamic Time-out Dynamic Interval Resp Time-out Threshold Action NONE Custom Header ☐ Treat back slash as escape character Net Profile ☐ Transparent ☐ Secure ☐ IP Tunnel Help OK Close		

! Some users reported better results when using a 10 second interval, with a response time-out of 6 seconds.

Go to the special parameters tab and fill in:



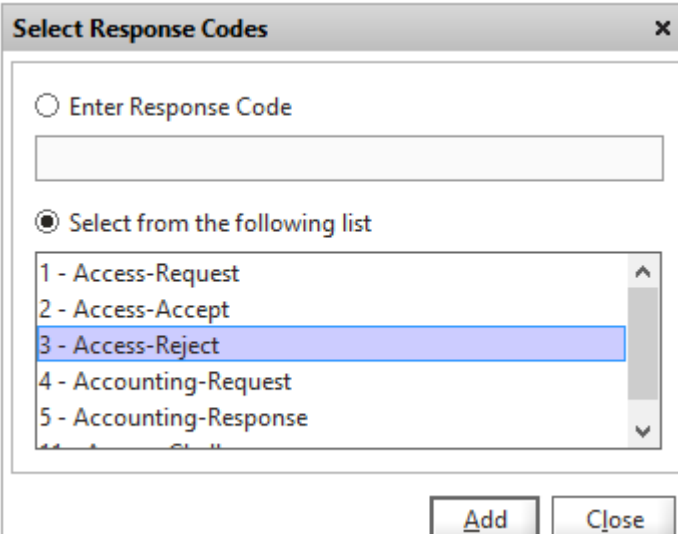
The 'Configure Monitor' dialog box is shown with the 'Special Parameters' tab selected. The 'Name*' field contains 'SMSPassword_RadiusMonitor' and the 'Type' is 'RADIUS'. The 'User Name*' field contains 'smspasswordmonitor', 'Password*' is masked with dots, and 'Radius Key*' is masked with three dots. The 'NAS ID' field is empty, and 'NAS IP**' contains '0.0.0.0'. A note states: '** It implies NAS IP is 'NS OWNED MIP/SNIP''. Under 'Response Codes', the number '3' is entered in a list box, with 'Add' and 'Remove' buttons to its right. The bottom of the dialog has a 'Help' icon and 'OK' and 'Close' buttons.

As username fill in: smpasswordmonitor

(this has match exactly and thus lower case!)

Password: smpasswordpassword

Radius key: in this example we use 'sms', but you can configure your own.



The 'Select Response Codes' dialog box is shown. It has two radio buttons: 'Enter Response Code' (unselected) and 'Select from the following list' (selected). Below the second radio button is a list box containing the following items: '1 - Access-Request', '2 - Access-Accept', '3 - Access-Reject' (which is highlighted with a blue background), '4 - Accounting-Request', and '5 - Accounting-Response'. At the bottom of the dialog are 'Add' and 'Close' buttons.

Press add, next to response codes. Select 3 - Access-Reject, and press add.

Press create to create the monitor.

Add a Load Balancing Virtual Server

Go to Traffic Management, Virtual Servers and select 'add'.

As name use SMSPassword_LoadBalancing_VirtualServer

As IP address use 192.168.2.213 (see network drawing)

Configure Virtual Server (Load Balancing)

Name*

SMSPassword_LoadBalancing_VirtualServer

Protocol*

RADIUS

☐ Network VServer

Range

1

☐ Enable DNS64

☐ Bypass AAAA Requests

State

UP

Disable

☒ AppFlow Logging

IP Address Based

IP Pattern Based

IP Address*

192 . 168 . 2 . 213

Port*

1812

Traffic Domain ID

Services

Service Groups

Policies

Method and Persistence

Advanced

Profiles

SSL Settings

Activate All

Deactivate All

Find

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight
--------	--------------	------------	------	----------	-------	--------	----------------

Add...

Open...

Remove

Comments

Help

OK

Close

Go to advanced and select the following options;

Configure Virtual Server (Load Balancing)

Name* SMSPassword_LoadBalancing_VirtualServer ☒ IP Address Based ☐ IP Pattern Based

Protocol* RADIUS IP Address* 192 . 168 . 2 . 213

☐ Network VServer Range 1 Port* 1812

☐ Enable DNS64 ☐ Bypass AAAA Requests Traffic Domain ID

State ☒ UP ☐ Disable ☒ AppFlow Logging

Services | Service Groups | Policies | Method and Persistence | **Advanced** | Profiles | SSL Settings

LB Method

Method Round Robin New Service Startup Request Rate PER_SECOND

Increment Interval 1

Persistence

Persistence RULE Persistence NONE

Time-out (min) 5 Time-out (min) 2

Rule CLIENT.UDP.RADIUS.USERNAME

IPv4 Netmask 255.255.255.255 IPv6 Mask Length 128

Comments

Help OK Close

LB method: Round Robin

Persistence: Rule

Timeout: 5

Rule: CLIENT.UDP.RADIUS.USERNAME

Go to service groups and add a new **service group**;

Name it SMSPassword_ServiceGroup

Protocol: Radius

Create Service Group

Service Group Name* SMSPassword_ServiceGroup Protocol* RADIUS

Traffic Domain ID

Service Group State ☒ ENABLED ☒ Enable Health Monitoring ☐ AppFlow Logging

Members Monitors Profiles Advanced SSL Settings

Specify Member(s)

☐ IP Based ☒ Server Based

SMSPassword_NodeA
SMSPassword_NodeB

Port

Weight 1

Server ID "None"

Hash ID

☒ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
SMSPassword_...	192.168.2.131	1812	1	"None"		☒ UP
SMSPassword_...	192.168.2.132	1812	1	"None"		☒ UP

Comments

Under the tab 'members', select 'Server Based'. Select the two SMSPassword nodes, fill in as port '1812', and press 'add' to add them to the configured members as shown above.

Go to the tab 'monitors' and select and add the SMSPassword_RadiusMonitor.

Service Group Name* Protocol*

Traffic Domain ID

Service Group State ☒ ENABLED ☒ Enable Health Monitoring ☐ AppFlow Logging

Members Monitors Profiles Advanced SSL Settings

Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp

Configured

Monitors	Weight	State	Passive
SMSPassword_RadiusM...	1	☒	☐

Comments

Press create to create the service group. Press the floppy icon to save the Netscaler configuration so far.

You can test the monitor by stopping the SMSPassword service on one of the nodes, and check to see if it shows as down in the Netscaler. If the member state doesn't show as 'up'/green, check the firewall.

Add the **radius server**;

Go to system, authentication, radius, and select the servers tab. Add a radius server.

Configure Authentication RADIUS Server

Name
SMSPassword_LBVS_Radius

☐ Server Name ☒ Server IP

IP Address*
192 . 168 . 2 . 213 ☐ IPv6

Port*
1812

Time-out (seconds)
300

Secret Key*
.....

Confirm Secret Key*
.....

► More

OK Close

As name use SMSPassword_LBVS_Radius

IPadress: 192.168.2.213

Port: 1812

Secret key ([Radius Shared Secret](#)): 'sms'

Confirm secret key([Radius Shared Secret](#)): 'sms'

Password encoding: pap

Timeout: 300

Accounting: OFF

Add the radius authentication policy:

Go to system, authentication, radius, and select the policies tab. Add an authentication policy.

Configure Authentication Policy

Name*

Authentication Type

Server New... Modify...

Expression

Expression
ns_true

Match Any Expression

Named Expressions Add Expression

Preview Expression

Help

Use as name: SMSPassword_Radius_AuthPol

Select as type: Radius

Server: Select the SMSPassword_Radius_LBVS

Add as expression: ns_true

Press create. Save the Netscaler config.

Now go to your Netscaler Gateway virtual server under 'Netscaler Gateway', 'Virtual Servers'. Open your gateway virtual server, and go to the authentication tab. Select; insert policy. And select the SMSPassword_Radius_AuthPol.

Configure NetScaler Gateway Virtual Server

Name*: citrix.gourami.eu IP Address*: 192 . 168 . 2 . 212

Protocol*: SSL Port*: 443

☐ Network VServer Range 1 Failed Login Timeout

☐ SmartAccess Mode ☒ Basic Mode ☐ AppFlow Logging ☒ Down state flush ☐ Double Hop Max Users 0

Max Login Attempts

Authentication | Certificates | Bookmarks | Policies | Intranet Applications | Intranet IPs | Published Applications | Advanced

User Authentication

If your NetScaler Gateway is to be deployed in a manner where user authentication is not desired, you may turn off authentication below. Please apply this option with CAUTION.

☒ Enable Authentication

Authentication Policies

Primary Secondary Group Extraction

Priority	Policy Name	Expression	Profile
100	SMSPassword_Radius_AuthPol	ns_true	SMSPassword_Radius_LBVS

Details : SMSPassword_Radius_AuthPol Find

Type: RADIUS Request Profile: SMSPassword_Radius_LBVS Rule: ns_true

Insert Policy Unbind Policy Regenerate Priorities Modify Policy

Comments

Help OK Close

Save your configuration.

Test your configuration by logging on to your Netscaler.

General Disclaimer and Copyright Notice

Disclaimer

Whilst every care has been taken by SMSPassword Software to ensure that the information contained in this document is correct and complete, it is possible that this is not the case. SMSPassword Software provides the information "as is", without any warranty for its soundness, suitability for a different purpose or otherwise. To the maximum extent permitted by applicable law, SMSPassword Software is not liable for any damage which has occurred or may occur as a result of or in any respect related to the use of this information. SMSPassword Software may change or terminate this document at any time without further notice and shall not be responsible for any consequence(s) arising therefrom. Subject to this disclaimer, SMSPassword is not responsible for any contributions by third parties to this information.

Copyright Notice

Copyright © on software and all Materials 1998-2015 SMSPassword Software. SMSPassword and the SMSPassword Logo are either registered trademarks or service marks of SMSPassword in Europe, the United States and other countries. All other product and company names mentioned may be trademarks and/or service marks of their respective owners.