

MICROSOFT NETWORK

document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security. WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

Limited Warranty - Copyright (c) 2010-2024 RCDevs Security SA. All Rights Reserved.

Microsoft Network Policy Server

NPS Network Policy Server RDS Remote Desktop Services RDWeb RDGateway Session Host RemoteApp Remote Application Remote Desktop Remote Desktop Gateway

1. Overview

In that documentation, we will explain how to configure OpenOTP multi-factor authentication on your Microsoft Network Policy Server. As a practical example, we will configure NPS with Microsoft Remote Access Server for VPN use.

For this recipe, you will need to have a WebADM, OpenOTP and Radius Bridge installed and configured. Please refer to <u>WebADM</u> <u>Installation Guide</u>, <u>WebADM Manual</u> and <u>Radius Bridge Manual</u> for instructions on these. Your Microsoft Network Policy Server and Remote Access Server should be installed and configured for VPN (PPTP, SSTP) use.

Note that only two multifactor authentication methods can be used to authenticate your Windows VPN client with OpenOTP: Simple push "Accept/Reject" or concatenated LDAP+OTP password. NPS supports RADIUS challenge, but Windows VPN Client does not, so you can not prompt additional credentials during the authentication request to ask for the OTP.

2. Configure MS VPN with NPS

Open the Routing and Remote Access console from your Windows VPN server



Right-click on your VPN > Properties



Click on Security tab



We will now change the Authentication Provider from Windows Authentication to RADIUS Authentication and click on Configure button.



On the following screen, configure the IP of your NPS server and a secret. Adjust the timeout according to the screenshot. If you are using Simple Push based authentication, it is important that the timeout exceeds the push timeout configured in WebADM.

				Ø	
Routing and Remote Access	YO-SSTP Properties		? ×		- a ×
	General Security IPv4	IPv6 IKEv2 PPP L	ogging	-	
Routing and Remote Access Server Status	The Authentication provide RADIUS Authentication	r validates credentials for rem	ote access clients		
VO-SSTP		1 1-1	2 ×	Server e Access Server Setup Wizard. To make	changes to the current
Administrator: Command Pr	Add RADIUS Server				- 🗆 X
Windows IP Configuration	Server name: Shared secret:	192.168.3.189	Change		^
Ethernet adapter Ethern	Time-out (seconds):	40 +			
Connection-specific Link-local IPv6 Add IPv4 Address. Subnet Mask Default Gateway.	Initial score: Port: Always use message au	30 + 1812 thenticator			
PPP adapter RAS (Dial)		lə	1		
Connection-specific		OK	Cancel		
Subnet Mask Default Gateway		ОК	Cancel		
Tunnel adapter isatap					
Media State Connection-specific		OK Cance	Apply		
Tunnel adapter isatap.{	6E06F030-7526-11D2	-BAF4-00500815A4B	0)::		
Media State Connection-specific	DNS Suffix .:	dia disconnected			
C:\Users\Administrator>	i				× .
¢ >					~
Done					11-51
= P 🛛 🤅 🖡	- <u></u>			^	₽ 4 ₂ 25/09/2019 ♀

3. NPS Configuration

3.1 Add your VPN server as RADIUS Client

On NPS your VPN server is configured as a Radius client.

Network Policy Server	RRAS Properties		
File Action View Help	Settings Advanced		
🦛 🐟 🙍 📅 🛛 🖬	Easter this BADUIC start		
NPS (Local)			
✓ I RADIUS Clients and Servers	Select an existing template:		
RADIUS Clients	v.	ur network.	n x
Remote RADIUS Server	Name and Address		
> Policies	Friendly name:		
Templates Management	VPN_Server		View Help
	Address (IP or DNS):		
	192.168.3.188 Venfy		
	Shared Secret		
	Select an existing Shared Secrets template:		
	None ~		rvor
	To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.		
	Manual Generate Shared secret:		nage
	Confirm shared secret:		
			bud servic
			Hide
	OK Cancel Apply		
		1	
	ROLES AND SERVER GROUPS Roles: 3 Server groups: 1 Servers total: 1		
	reares a perior diaman a servera reares		

The secret must be the same as the one you configured on your VPN server. Go back to your VPN properties and click on Authentication Methods button. Configure PAP as Authentication Method like below:

					1.0.2
Routing and Remote Access				- 0	×
File Action View Help		O-SSTP Properties	2 ×		
� ⇒ 2 🔟 🗶 🗉 Q 🛙		General Security IPv4 IPv6 IKEv2 PPP Li	paging		
Routing and Remote Access Server Status YO-SSTP Network Interfaces Remote Access Clients	YO-SSTP Routing and F This server has air	The Authentication provider validates credentials for remained demand dial routers.	te access clients	etup Wizard. To make changes to the current	^
및 Ponts 이 Remote Access Logging 이 포 IPv4 이 프 IPv6	Enable Direct/ You are currently u	The server authenticates remote systems by using the set the order shown below. Estensible authentication protocol (EAP) Select the EAP option if you are using Network Acce (NAP). Use NPS to configure all other NAP settings.	ected methods in	e rich remote access experience based on	
	DirectAccess by en corporate network, DirectAccess" op	Microsoft encrypted authentication version 2 (MS-CH Encrypted authentication (CHAP) Unencrypted password (PAP) Allow machine certificate authentication for IKEv2 Unauthenticated access Allow remote systems to connect without authenticate OK server anotac use to bind warr 35L (web caseler) Certificate: Default OK Cancel	AP v2) tion Cancel View	ioined clients can seamlessly connect to your tAccess" wizard by selecting the "Enable ode on the left.	
< > Done ₽	n <u>L</u> 3			へ 炉 4 ^{18.08} 日 19/09/2019	-

Apply the configuration. This concludes the VPN server part.

3.2 Add a new Remote RADIUS Server

Open the NPS console, we will now configure a Remote RADIUS Server. Right click on Remote RADIUS Server Group > New

			9 YO_SSTP	Pour relâcher vo	tre souris, appuyez sur : Control-
11 🖪	₹ ↔ 🖬	(i)	0 2 0 4	Ø	
Network	Policy Server				- 0 ×
File Acti	on View Help				
* • * 2					
NPS (L	ocal)		Remote RADIUS Server Groups		
V 🎽 RAI	DIUS Clients and Servers		Remote RADIUS server any ris allow you to specify where to for	ward connection requests when the lo	cal NPS server is configured as
1	Remote RADIUS Server Group	ns	a RADIUS proxy.		
v 🖉 Pol	icies	New	N		
Connection Request Poli Exp Network Policies Accounting	Export List	Name			
	View	crosoft Houting and Hemote Access Service Authentication Servers			
> 🛃 Ten	nplates Management	Refresh			
		Help			
		rich			
New					

Click Add button

	4) 🔟 🖞 🗑 4	
Network Policy Server		- 0 ×
File Action View Help		
NPS (Local) ADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Groups	Remote RADIUS Server Groups Remote RADIUS server groups allow you to specify where to forward connection requests when the a RADIUS proxy.	e local NPS server is configured as
Policies Connection Request Policies	Group Name	
Network Policies	New Remote RADIUS Server Group	
 Accounting Templates Management 	Group name:	
	RADIUS Servers: RADIUS Canada Printhe Wainhet Add	
	Photo Server Photos Photos	
	604	
	Remove	
	OK Cancel	
Aution: In an even	J	
Action: in progress		10.10
📲 P 🗆 健 🔚 🚪	🖌 🦣 👯 🕪 🗠 🛛	ヘ EP 4 19/09/2019 - 報

On the next page, add the IP address of your Radius Bridge.

Network Policy Server		- 🗆 ×
File Action View Help		
🗢 🌩 🖄 🔟 📓 🗊	Add RADIUS Server X	
🛞 NPS (Local)		
RADIUS Clients and Servers	Address Authentication/Accounting Load Balancing	equests when the local NPS server is configured as
RADIUS Clients	Select an existing Remote RADIUS Servers template:	
V Dolicies	None	
Connection Request Policies		
Accounting	Type the name or IP address of the RADIUS server you want to add.	
> 💐 Templates Management		
	Server: 192.168.3.54 Verfy	
	Ν	
	~	
	OK Cancel	
Action: In progress		
		18:18
🚛 🖓 🛄 🥃 🔜		수 팀 🗣 19/09/2019 🔞

On the next tab, you have to configure the secret, which must match a client definition in your RADIUS bridge clients.conf:

II 🖪 🔧 ↔ 🖸 🚇	48 💿 🕸 🗑 4		0
 Network Policy Server File Action View Help 			- 0 ×
🗢 🔿 🙍 🔟 🛙 💷	Add RADIUS Server		×
NPS (Local) RADIUS Clients and Servers RADIUS Clients and Servers Remote RADIUS Server Groups Policies Connection Request Policies Network Policies Remote Radius Server Serv	Address Authentication/Accounting Load Authentication port: Select an existing Shared Secrets template None Shared secret: Confirm shared secret: Request must contain the message auth Accounting Accounting Accounting port: Use the same shared secret for auther Select an egisting Shared Secrets ter None Shared secret: Confirm shared secret:	d Balancing	requests when the local NPS server is configured as
		UK Lancel	-
Action: In progress]]		
		3	
		2	19/09/2019 🔞

NPS server IP needs to configured as Radius client in /opt/radius/conf/clients.conf :

```
client NPS_Server {
    ipaddr = 192.168.3.189
    secret = testing123
}
```

On the Load Balancing tab, you need to configure the timeouts like below. Again they must exceed the push timeout:

	W YO_SSTP	Pour relacher votre souris, appuyez sur : Control-
	4) 🖲 🖞 🗑 4	2
Network Policy Server File Action View Help		- 0 ×
💠 🔿 🙍 🔟 🖬	Add RADIUS Server X]
 NPS (Local) RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Groups Connection Request Policies Network Policies Accounting Templates Management 	Address Authentication/Accounting Load Balancing The priority of ranking indicates the status of a server. A primary server has a priority of 1. Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority. Priority: 1 Weight: 50 Advanced settings Advanced settings Number of seconds without response before request is considered dropped: 40 1 Maximum number of dropped requests before server is identified as unavailable: 3 40 Number of seconds between requests when server is identified as unavailable: 40 40	requests when the local NPS server is configured as
Action: In progress	OK Cancel	^ テ⊋ 4 <u>,</u> 18:22 19/09/2019 ₹

Click Ok twice when your configuration is done.

	U YO_SSTP	
		0
Network Policy Server		- 0 ×
File Action View Help		
🕈 🔿 📶 🔛 🕅		
 NPS (Local) RADIUS Clients and Servers 	Remote RADIUS Server Groups	
RADIUS Clients Remote RADIUS Server Groups Policies Connection Request Policies Network Policies Accounting Templates Management	a RADIUS prov.	n meliocal nino server is comigured as
	Group Name	
	New Remote RADIUS Server Group X	
	Group name:	
	OpenOTP	
	RADIUS Servers:	
	RADIUS Server Priority Weight Add	
	192.168.3.54 1 50 Edit	
è.	Remove	
	OK Crowd	
	UN Carba	
]	
Action: In progress		
📲 🔎 🗆 🥭 🔚 🛛		へ 空 ds 18-24 19/09/2019 - 報



3.3 Connection request Policies

Now we need to configure a Connection Request Policy in order to forward authentication request to Radius Bridge. Right click on Connection Request Policy > New

		0 0 0 4		10			
				<u></u>		-	
Network Policy Server					-	D	~
File Action View Help							
🥐 🕸 🔽 🔟 🔟 🕅							
🚱 NPS (Local)		Connection Request Policies					
RADIUS Clients and Servers		Connection ownuest policies allow up uto	darinnata ubalhar on	martino manuale a	re opposited locally or forwarded to rea	ate RADIII	10
RADIUS Clients	Ner Groups	servers.	ocargenate in realien co		to proceeded to carry or rotheradou to ret		
V Policies	iver oroups						
Connection Rec	A Dullate	Policy Name	Status	Processing Order	Source		
Network Policie	New D	Use Windows authentication for all users	Disabled	1	Remote Access Server(VPN-Dial up)		
Accounting	Export List	Microsoft Routing and Remote Access Service	Policy Disabled	2	Remote Access Server(VPN-Dial up)		
> 🛒 Templates Managel	View >						
	Refresh						
	11.4						
	Help						
		Use Windows authentication for all users					
		Conditions - If the following conditions are met:					
		Condition Value					
		NAS Port Type Virtual (VPN)					
		Settings - Then the following settings are applied:					
							_
		Setting	Value				
		Accounting Provider Name	Microsoft Routing and	Remote Access S	ervice Authentication Servers		
		Authentication Provider Bemote BADII IS to Windows User Managing	Local Computer				
		Override Authentication	Disabled				
New		1					
						0.70	
	e 👝 📥	🦄 🐺 🔊 📼 🛽			^ 惊 4∎ 19/0	9/2019	(4)
					12/1		-

Name your policy, define the Type of Network access server to Remote Access Server and then click Next.

0		- A V
Pretwork Policy Server		- U ^
File Action View Help		
•• 200 00	al la la harri na la la	-
NPS (Local) IADIUS Clients and Ser RADIUS Clients Remote RADIUS Ser Policies	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	onwarded to remote RADIUS
Connection Reques		
Network Policies	Policy name:	er(VPN-Dial up)
Accounting	VPN_to_OpenOTP	er(VPN-Dial up)
> remplates Managemen	Natural second as without	
	Tremonic connection memory 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.	
	Tune of network access server	
	Banata Assass Secure (AP) (Indus)	
	(Nenicle Access Server(Vr.Nr.Das.up)	
	Vendor specific:	
	C2	
		ervers
	Previous Next Finish Cancel	
Action: In progress		
		18:28
- p 🗇 🔁	- 📖 🦛 🐩 🦻 📇 🧃	19/09/2019

On the next page, define your Access Conditions.

Network Policy Server		- 0 ×
File Action View Help		
* * 2 🔟 🖬 🖬		
NPS (Local)	New Connection Request Policy X	
RADIUS Clients and Sen RADIUS Clients and Sen	Specify Conditions	forwarded to remote RADIUS
Remote RADIUS Ser	Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A	
v I Policies	minimum of one condition is required.]
Connection Reques		1
Network Policies	ielect condition X	er(VPN-Dial up)
> Templates Managemer	Select a condition, and then click Add.	er(vr wolaiup)
	User Name	
	User Name	
	typically contains a realm name and a user account name.	
	Connection Properties	i i i i i i i i i i i i i i i i i i i
	Access Client IPv4 Address The Access Client IPv4 Address condition specifies the IPv4 address of the Access Client that is requesting access	
	from the RADIUS client.	· · · · · · · · · · · · · · · · · · ·
	Access Client IPv6 Address	
	from the RADIUS client.	
	Framed Protocol	
	The Framed Protocol condition restricts the policy to only clients specifying a certain transing protocol for incoming packets, such as PPP or SLIP.	
	Add Cancel	
Ļ		
	Add D Edit Remove	
		ervers
	Previous Neid Finish Cancel	
		J
Action: In progress		
Action: In progress		된 de

On my side, I only defined the NAS Port Type to VPN (Virtual). This means the policy is applied to VPN connections.

Network Policy Server File Action View Help				- 0 X
NPS (Local) RADIUS Clients and Ser RADIUS Clients and Ser RADIUS Clients and Ser RADIUS Clients Remote RADIUS Ser Policies Connection Reques Network Policies Accounting	lew Connection Request Specify Specify the minimum o elect condition	Policy Conditions conditions that determine whether this connection request policy is evaluat f one condition is required. NAS Port Type	ted for a connection request.	Ionwarded to remote RADIUS a er(VPN-Dial up) er(VPN-Dial up)
 Self Templates Managemer Self Self 	NAS Identifier NAS Identifier The NAS Identifier can use pattern in NAS IPv4 Addr The NAS IPv6 Addr The NAS IPv6 Addr The NAS IPv6 Addr BBL NAS IPv6 Addr The NAS IPv6 Addr T	Specify the access media types required to match this policy. Common dai-up and VPN turnel types Async (Modem) Sync (T1 Line) Vestal (VPN) Common 802.1X connection turnel types Eithernet FDDI Token Ring Wreless - IEEE 802.11 Others ADSL-DMT - Asymmetric DSL Carrierless Amplitude Phase Modulation Agenc (Modem) Cable OK: Cancel	er (NAS). You use pattern u can use phone lines,	
		Previous Next	Finish Cancel	ervers
Action: In progress				19:37

			U	
Network Policy Server				- 0 ×
File Action View Help				
🗢 🔿 🙇 📷 🛛 👘 💡				-
NPS (Local)	New Connection Request Policy		×	
V 🔤 RADIUS Clients and Ser	Enacify Conditions			
RADIUS Clients	Specify Conditions			orwarded to remote RADIUS
Remote RADIUS Ser	Specify the conditions that de minimum of one condition is r	stermine whether this connection request polic required.	ty is evaluated for a connection request.	Α.
Connection Reques				
Network Policies	Contribution			er(VPN-Dial up)
No Accounting	Conditions.			er(VPN-Dial up)
> 🛃 Templates Managemer	Londton Value			
	Witual (VPN)			
	Condition description:			
		Add.	Edit Remiève	
				ervers
		Previous Next	t Finish Cancel	
				-
Action: In progress				
Action: In progress				· 뛰 4

Click **Next** when all of your conditions are defined.

Next page we finally define the Authentication mechanism for the requests. On the Authentication tab switch to

Forward requests to the following RADIUS server group for authentication and choose the Server group we defined earlier.



The accounting part can be kept by default because Radius Bridge does not support RADIUS accounting. Click Next.

On the next page, there is one small but important setting to be considered. If you wish to implement Network Policies (for example user/group specific netowork access rules) in NPS, you must configure the following RADIUS attribute set to **True**. This attribute means NPS sends the defined Network Policies back to VPN server. Without it all Network Policies are ignored.

Network Policy Server			- 0 ×
File Action View Help			
	New Connection Research Deliver		~
NPS (Local)	New Connection Request Policy		^ <u>_</u>
RADIUS Clients and Ser ADIUS Clients	Configure S	Settings	orwarded to remote RADIUS
Remote RADIUS Ser	NPS applies settin	gs to the connection request if all of the connection request policy conditions for t	the policy are
✓ ■ Policies	matched.		
Connection Reques			
Accounting	Configure the settings for this netwo If conditions match the connection is	rk policy. equest and the policy grants access, settings are applied.	er(VPN-Dial up) er(VPN-Dial up)
> 🜉 Templates Managemer	Cattings:		
	Specify a Realm Name		
	Attribute	To send additional attributes to RADIUS clients, select a Vendor Specific attribute, then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients	s. See
	RADIUS Attributes	your RADIUS client documentation for required attributes.	
	Standard		
	Z Vendor Specific	Attributes:	
		Name Vendor Value	
		Remote-RADIUS to-Windows-User-Mapping RADIUS Standard True	- A
		AddEdtRemove	
		D ₂	ervers
		Previous Next. Finish	Cancel
L			
Action: In progress			10.00
🛯 🗢 🖉	ê 📄 🔚 🗞	27 😥 🗠 🧃	^ 문 4 19/09/2019 특衡

Click Next and finish.

	@ YO_SSTP	Pour relâcher votre souris, appuyez sur : Control-X
II E		0
Network Policy Server File Action View Help		- 0 X
💠 🔿 🗾 🔟 🔟		
NPS (Local) RADIUS Clients and Ser RADIUS Clients RADIUS Clients Remote RADIUS Ser Policies Connection Reques	Completing Connection Request Policy Wizard	onwarded to remote RADIUS
Network Policies	You have successfully created the following connection request policy:	er(VPN-Dial up)
> Templates Managemen	VPN_to_OpenOTP	er(VPN-Dial up)
	Policy conditions:	
	Condition Value	
	NAS Port Type Virtual (VPN)	
	Policy settings:	
	Condition Value	
	Authentication Provider Forwarding Request	
	Remote-RADIUS-to-Windows-User-Mapping True	
	To close this wizard, click Finish.	
		ervers
	Previous Next. Fin	ish Cancel
Action: In progress		
a 2 0 (🗧 🔚 🍡 💱 👂 📼 🛽	∧ 〒 d _■ 18:58 19/09/2019 ₹

4. VPN client configuration

On the VPN Client configuration we need to configure PAP as supported protocol. Edit your VPN Connection Properties and configure it as below :

2	Network Connections	- 0 X
1 🔮 🕈 Control Panel 🔸 Netw	ork and Internet Network Connections	✓ ♂ Search Ne P
Organize Start this connection Rename	this connection Delete this connection Change settings of this connection	s: • 🔟 🕯
Ethernet0 ad.rcdevs.com Intel(R) 82574L Gigabit Network C	VPN Connection Disconnected WAN Miniport (PPTP) VPN Connection Properties	
	General Options Security Networking Sharing	
	Type of VPN:	
	Automatic 🗸	
	Advanced settings	
	Optional encryption:	
	A theritation	
	O Use Extensible Authentication Protocol (EAP)	
	w l	
	Properties	
	 Allow these protocols EAP-MSCHAPv2 will be used for IKEv2 VPN type. Select any of these protocols for other VPN types. 	
	Unencrypted password (PAP)	
	Challenge Handshake Authentication Protocol (CHAP)	
	A trendicially use my Workeye loope name and	
	password (and domain. # any)	
	OK Cancel	
	Activat Go to Sy Windows	te Windows stem in Control Panel to activate s.
items 1 item selected		10

That concludes the VPN client configuration.

5. WebADM Client Policy

As mentioned, Windows VPN client doesn't support RADIUS Challenge. For this reason, you have to create a WebADM client policy for your VPN, disabling the challenge mode support for the requests from MS VPN server.

Loginon WebADM Admin GUI > Admin tab > Client Policy



Click on Add Client button, name your client policy and click Proceed button:

	Mandatory attributes		
Container	cn=Clients,cn=WebADM,dc=yorcdevs,dc=com	±.	Select
Common Name	Microsoft NPS		
WebADM Object Type	WebADM Client Policy (Client)		
	Optional attributes		
Description / Note			
WebADM Settings	You can edit this attribute once object is created.		

Click on Create Object :

object creation for cn=l	Microsoft NPS,cn=Clients,cn=We
Attribute	Value
DN	cn=Microsoft NPS,cn=Clien
Common Name	Microsoft NPS
WebADM Object Type	Client

You are now on the configuration page of your client policy. Scroll down to find the **Forced Application Policies** section :



Enable the setting and click **Edit** button:

In the Application box on the top left, select MFA Authentication Server switch the

Challenge Mode Supported setting to No:

Web Alight Enterprise Edition Copyright © 2010-2019 RCDove SA, Ad Rights	v1.7.6-2	
# Home Admin Cluster Create	Search Import Databases Statistics Applications About	Logout
	Application Settings	
Applications	Authentication Policy	
✓ MFA Authentication Server	Login Mode (LDAPOTP (Default) \$	
Shared Session Server SSH Public Key Server QR Login & Signing Server OpenID & SAML Provider	The login mode (required login factors) should be ajusted via Client - LDAPOTP: Require both LDAP and OTP passwords. - LDAPU2F: Require both LDAP and FIDO response. - LDAPMFA: Require LDAP and either OTP or FIDO. - LDAP: Require LDAP password only. - OTP: Require OTP password only.	Policies.
	OTP Type TOKEN (Default) \$	
	- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Toker - SMS: SMS one-time password (On-demand or Prefetched). - MAIL: Email one-time password (On-demand or Prefetched). - LIST: Pre-generated OATH OTP password list (to be printed). - PROXY: Forward requests to another RADIUS server (for migratic OTP Failback TOKEN Failback OTP Type to be used as secondary authentication method SMS/MAIL OTPs are delayed for MobileTimeout seconds before be LASTOTP let users use the last validated OTP which expires after i Use DISABLED to disabled failback if there is a configuration by de	n.
	OTP PIN Prefix Yes No (default)	
	When enabled a static prefix has to be prepended to any OTP pass	word in the form [PIN][OTP].
	Challenge Mode Supported O Yes (default) O No	
	OpenOTP assumes concatenated OTP passwords when disabled a Note: Challenge is required for Simple-Push, FIDO, OATH-OCRA a Mobile Response Timeout 30 (Default) # Time to wait for mobile response with Token Simple Push before sw Changing the default value requires to adjust client timeouts (ex. R	es norsupport it. with simpleLogin requests. nd on-demand SMS/Mail OTP. itching to a fallback method. ADIUS request timeout) accordingly!

On the same page you can also configure **Push** Login setting to **yes** if you have a push login infrastructure available and wish to use this method.

Scroll down to apply the configuration, and you will be redirected to the client policy configuration page. You should have the following :



For OpenOTP match the policy with NPS and your VPN, you must configure the IP addresses of your VPN and NPS servers in the Client Name Aliases setting. On my side, both are running on the same server so I configured only one IP address:

Web Copyright	0 2010-2011	erprise	Edition	v1.7.7									X	🔤 🗔 🏶 🗔
# Home	Admin	Cluster	Create	Search	Import	Databases	Statistics	Applications	About	Logout				
						Object Settin	ngs for <u>CN=N</u>	licrosoft NPS,0	N=Clients	CN=WebA	DM,DC=yorcdevs			
				0	Disable C When dis Default D This dom	client abled, client re omain ain is automati Name	oquests using	les No (defa this client polic t when no domain	ult) y will be ref in is provid	used. led.				
					Friendly o	lient name or : me Aliases	short descrip	tion to be used 1	or %CLIEN	IT% in user	messages.			
					Comma-s	eparated list o	falternative	client IDs.						
					UID Attrib Restricted	utes d list of LDAP I	ogin attribute	s replacing the	attributes c	onfigured via	a uid_attrs in webadn	Edit		

Press Apply to save your client policy.



Configuration is now complete.

With this policy, when your users will try to log in from the VPN client, they must use the push login to be able to log in (if push login infrastructure is configured with OpenOTP) or use LDAP and OTP passwords concatenation :

- > LDAP Username : Administrator
- > LDPA Password : password
- > OTP:123456
- > LDAP Password+OTP concatenation : password123456

6. OpenOTP logs

6.1 Push login logs

[2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] New openotpSimpleLogin SOAP request [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Username: administrator [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Password: xxxxxxxx [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Source IP: 192.168.3.189 [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] > Options: RADIUS,-U2F [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Enforcing client policy: Microsoft NPS (matched client IP) [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Registered openotpSimpleLogin request [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Resolved LDAP user: CN=Administrator,CN=Users,OU=TESTING,DC=yorcdevs,DC=com (cached) [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Resolved LDAP groups: group policy creator owners, domain admins, enterprise admins, schema admins, administrators, denied rodc password replication group [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Started transaction lock for user [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found user fullname: Administrator [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found 46 user settings: LoginMode=LDAPOTP,OTPType=TOKEN,PushLogin=Yes,ExpireNotify=MAIL,ChallengeMode=No,ChallengeTin 1:HOTP-SHA1-6:QN06-T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,SecureMail=No,MailMode=Ondemand,Prei [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found 5 user data: TokenType,TokenKey,TokenState,TokenID,TokenSerial [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Found 1 registered OTP token (TOTP) [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Challenge mode disabled (checking concatenated passwords) [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] Requested login factors: LDAP & OTP [2019-09-19 16:50:33] [192.168.3.54] [OpenOTP:8ENCNNEB] LDAP password Ok [2019-09-19 16:50:34] [192.168.3.54] [OpenOTP:8ENCNNEB] Sent push notification for token #1 [2019-09-19 16:50:34] [192.168.3.54] [OpenOTP:8ENCNNEB] Waiting 27 seconds for mobile response [2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] Received mobile authentication response from 192.168.3.192 [2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] > Session: SeNAdV4FltKKVKIJ [2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] > Password: 16 Bytes [2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] Found authentication session started 2019-09-19 16:50:33 [2019-09-19 16:50:37] [192.168.3.56] [OpenOTP:8ENCNNEB] PUSH password Ok (token #1) [2019-09-19 16:50:37] [192.168.3.54] [OpenOTP:8ENCNNEB] Updated user data [2019-09-19 16:50:37] [192.168.3.54] [OpenOTP:8ENCNNEB] Sent login success response

6.2 Concatenated LDAP password and OTP logs

[2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] New openotpSimpleLogin SOAP request [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Username: administrator [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Password: xxxxxxxxxxxxxx [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Source IP: 192.168.3.189 [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] > Options: RADIUS,-U2F [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Enforcing client policy: Microsoft NPS (matched client IP) [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Registered openotpSimpleLogin reguest [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Resolved LDAP user: CN=Administrator,CN=Users,OU=TESTING,DC=yorcdevs,DC=com (cached) [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Resolved LDAP groups: group policy creator owners, domain admins, enterprise admins, schema admins, administrators, denied rodc password replication group [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Started transaction lock for user [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found user fullname: Administrator [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found 46 user settings: LoginMode=LDAPOTP,OTPType=TOKEN,PushLogin=No,ExpireNotify=MAIL,ChallengeMode=No,ChallengeTim 1:HOTP-SHA1-6:QN06-T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,SecureMail=No,MailMode=Ondemand,Prei [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found 5 user data: TokenType,TokenKey,TokenState,TokenID,TokenSerial [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Found 1 registered OTP token (TOTP) [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Challenge mode disabled (checking concatenated passwords) [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Requested login factors: LDAP & OTP [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] LDAP password Ok [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] TOTP password Ok (token #1) [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Updated user data [2019-09-19 16:37:23] [192.168.3.54] [OpenOTP:232F08T0] Sent login success response

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved