

# 

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. RCDevs. All further trademarks of 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.

www.rcdevs.com

Remote Desktop Services Windows RDWeb RDGateway NPS

# How To Configure MS Remote Desktop Services and RDWeb portal with OpenOTP

## Note

OpenOTP plugin for Remote Desktop Web portal works on Windows Server 2012, 2016, 2019 & 2022.

# 1. Prerequisites

#### 1.1 Remote Desktop Services Infrastructure

In this post, we will assume an existing Remote Desktop Services infrastructure installed and available. This post will not cover how to set up RDS. Please refer to the Microsoft documentation and/or the TechNet blog for details about how to install and configured Microsoft documentation.

#### 1.2 WebADM/OpenOTP/Radius Bridge

For this recipe, you will need to have WebADM/OpenOTP installed and configured. If you would like to have Push Login Mode then Radius Bridge needs to be configured. Please, refer to <u>WebADM Installation Guide</u>, <u>WebADM Manual</u> and <u>Radius Bridge</u> to do it.

## 2. How to Secure RDWeb Access with OpenOTP

#### 2.1 RDWeb Authentication Workflow (Challenge Mode)



- 1. User Access to RDWeb login page, provide Username/Password. Credentials are sent to Kerberos.
- 2. Credentials are validated between RDWeb and Kerberos services.
- 3. If credentials are correct then a Kerberos ticket is provided to RDWeb for this user.
- 4. Once the first validation with Kerberos is ok, an OpenOTP login request is sent from the OpenOTP RDWeb Plugin installed on RDWeb server to OpenOTP server.
- 5. If LDAP Credentials are validated by OpenOTP server, then a challenge request is sent by OpenOTP to the RDWeb and will allow the user to provide the OTP.
- 6. The user is prompted to enter his OTP. The OTP is sent back to the OpenOTP server through the OpenOTP RDWeb plugin.
- 7. OpenOTP validates the OTP provided by the User.
- 8. If the OTP is validated by OpenOTP server then the authentication is a success.
- 9. The user has logged on the RDWeb interface and is able to download RDP files.

2.2 RDWeb Authentication Workflow (Push Login Mode)



- 1. The user initiates an RDP session with an RDP file previously downloaded from the RDWeb server.
- 2. The RDP connection start through the RDP client. The RDP client contacts the RDGateway. The RDGateway communicate with NPS to check users policies and resources allowed for this user.
- 3. At this step, the first validation with Kerberos is in progress.
- 4. A Kerberos ticket is created for this user and send back to NPS.
- 5. NPS act as a PROXY RADIUS too. Once NPS has received the Kerberos validation, a RADIUS *Access-Request* is sent to Radius Bridge by NPS.
- 6. The Radius *Access-Request* is translated into a SOAP *Login request* by Radius Bridge product to be managed by OpenOTP server. OpenOTP will validate LDAP credentials and send a push login request to the user' mobile.
- 7. If LDAP Credentials are validated by OpenOTP server, then a push login request is sent RCDevs Push servers.
- 8. RCDevs Push Servers communicate with Google/Apple Push services.
- 9. Google/Apple services. send the push notification on the user's mobile OpenOTP.
- 10. The user receives the push login request on his phone and has to Accept or Reject the login attempt.

- 11. The response from the mobile is sent to WAProxy server and WAProxy forward the mobile response to OpenOTP server.
- 12. OpenOTP manages the response and accept or reject the login attempt according to the mobile response.
- 13. OpenOTP sends a SOAP access accept request to Radius Bridge.
- 14. Radius Bridge translates the SOAP request into a RADIUS request. The response is sent to NPS. NPS receives the authorization from the RADIUS server to allow the connection for this user. The user is successfully authenticated in 2FA.
- 15. RDGateway allows the user to access to Session Hosts according to policies configured on NPS for this user and resources allowed.

# 3. OpenOTP Plugin for RDWeb Installation

OpenOTP plugin for Microsoft RDS has to be installed on every RDWeb servers you have. You have to download the plugin on RCDevs Website at the following links OpenOTP Plugin for RDWeb Gateway.

## 🛕 Note

Administrative/elevated permissions are necessary on any workstation to correctly set up and/or change the OpenOTP Plugin for RDWeb's configuration. Please, run the Windows PowerShell as Administrator. Right click on the Windows PowerShell then select Run as Administrator.



Extract files from the archive on your RDS server(s), run the MSI file in the Windows PowerShell as Administrator and click on Next.



Accept the End-User License Agreement and click on **Next**.

|   |   | - ogi cement  | concromy   | ``   | security                   | soluti |
|---|---|---|--|--|----------------------------|--------|
| RCDEVS Open   | nOTP-RDWel  | D LICENS  | E AGREEM   | ENT  |                            | ^      |
| RCDevs Open<br>Copyright<br>reserved.                                 | nOTP RDWeb<br>(c) 2010-2  | 0 Access<br>2019 RCD                                    | e ("OpenOT<br>evs SA,                                  | P-RDWeb")<br>All right                               | 3                          |        |
| IMPORTANT:<br>distributin<br>accept all<br>present Ope<br>If you do n | READ CAR<br>ng the Soi<br>the follo<br>enID Licen<br>not agree, | EFULLY:<br>Etware P<br>owing te<br>nse Agre<br>, do not | By using<br>roduct y<br>rms and<br>ement("A<br>install | , copying<br>ou<br>condition<br>greement"<br>and use | or<br>s of th<br>).<br>the | e ~    |
| If you do n   | not agree,  | , do not  | install  | and use  | the                        | ~      |

On the next page, choose your default folder location and click on  ${\tt Next}$  .

| OpenOTP-RDWeb (64 bit) Setur     This feature requires 2KB on your     hard drive. It has 1 of 1     subfeatures selected. The     subfeatures require 4202KB on you     hard drive. | Select the way you<br>Click the icons in th | want features to be insta<br>the tree below to change th | led.   | rity solu       |
|--|---|--|--|-----------------|
| Browse   |   | enOTP-RDWeb (64 bit) Se                                  | This feature requires 2KB on hard drive. It has 1 of 1 subfeatures selected. The subfeatures require 4202KB or hard drive. | your<br>on your |

On this page, you have to configure one of your WebADM servers URL. If you are running a WebADM cluster, then both OpenOTP URLs should be automatically retrieve in the Auto mode. If your OpenOTP URL(s) can not be automatically retrieve, then configure URL(s) manually like below :

| nfiguration 1/5<br>Setup server URLs, default domain, login text and dient ID |           |
|---|-----------|
|   |           |
| Auto     Manual   |           |
| WebADM URL:   |           |
| https://192.168.3.64  | Configure |
| Server URL: (mandatory)   |           |
| https://192.168.3.64:8443/openotp/  | •         |
| additional Server URL: (optional)   |           |
| https://192.168.3.65:8443/openotp/  | •         |
| Login Text: (optional)  |           |
| Work Resources  | •         |
| <u>Client ID: (optional)</u>  |           |
| RDWeb   | •         |
|   |           |
|   |           |
|   |           |
|   |           |

On the next page, the WebADM CA certificate is automatically retrieved and configured if you have chosen the Auto mode to return OpenOTP URL(s). Every other settings are optional. If you'd like to use a client certificate for enhanced security, please use this next screen to provide the detail. Clicking on the question marks (?) will provide additional help during the installation procedure.

| ₿ OpenOTP-RDWeb (64 bit) Setup ×   |
|--|
| Configuration 2/5  |
| Setup security using a PKI.  |
| The following settings are generally not required.<br>They are applicable only if you have set the Server URL with HTTPS in the previous step. |
| Certificate Authority File: (optional)   |
| C:\Program Files\RCDevs\OpenOTP RDWeb Access\ca.crt  |
| Certificate <u>Fi</u> le: (optional)   |
| 0  |
| Certificate Password: (optional)   |
|  |
| Confirm Password:  |
|  |
| Back Next Cancel   |

Click Next and the next page allows you to configure failover with OpenOTP, SOAP request timeout and UPN Mode. Keep the default configuration if you are not sure of what you need. Click on Next.

| RCDevs OpenOTP-RDWeb (64 bit) Setup<br><b>Configuration 3/5</b><br>Setup preferences for this machine. | ×<br>RCDevs<br>security solutions |
|--|-----------------------------------|
| The following settings are for advanced configurations.<br>You should keep the default values here.    |                                   |
| SOAP Timeout: (Default 30)   |                                   |
|  | U                                 |
| Server Selection Policy: (optional)  |                                   |
| Ordered (Default)  | × 🕚                               |
|  |                                   |
|  |                                   |
|  |                                   |
|  |                                   |
| Back   | Next Cancel                       |

On the next page, you can configure a custom message when users need assistance.

| 🛃 OpenOTP-RDWeb (64 bit) Setup                               | ×      |
|--|--------|
| Configuration 4/5<br>Setup user assistance information.      |        |
| The following settings are assistance information for users. |        |
| Support Information: (optional) Ctrl+Enter for new line      |        |
| Back N   | Cancel |

Click on Next. On that page, you can configure the reverse-proxy address(es) of your reverse-proxy if you are accessing RDWeb portal through a reverse-proxy. This is usefull for WebADM in order to know the real end-user IP in WebADM logs instead of the reverse-proxy IP(s). It is also usefull for WebADM if you want to use the Per-Network Extra Policies feature in your RDWeb client policy.

| OpenOTP-RDWeb (64 bit) Setup Configuration 5/5 |      | PC    | ×                 |
|--|------|-------|-------------------|
| Setup RDWeb specific configuration info        | s    | Se Se | ecurity solutions |
| Authorized Proxies IPs (optional) :            |      |       |                   |
| 192.168.3.1                                    |      | 0     |                   |
|  |      |       |                   |
|  |      |       |                   |
|  |      |       |                   |
|  |      |       |                   |
|  |      |       |                   |
|  |      |       |                   |
|  |      |       |                   |
|  | Back | Next  | Cancel            |

Click on Next and Install.



Installation is complete. Click on Finish.



# 🛕 Plugin Installation

Repeat this procedure on every RDWeb servers!

You are now able to log in on your RDWeb server with OpenOTP. Go to your RDWeb page and please enter your credentials:

|                        |  | RD Web Access |
|------------------------|--|---------------|
| Work Resourc           | es<br>onnection  |               |
|                        |  | Help          |
|                        | Domain\user name: ad.rcdevs.com\administrator<br>Password:<br>Security<br>Warning: By logging in to this web page, you confirm<br>that this computer complies with your organization's<br>security policy.     |               |
|                        | Sign in<br>To protect against unauthorized access, your RD Web<br>Access session will automatically time out after a period<br>of inactivity. If your session ends, refresh your browser<br>and sign in again. |               |
| Windows Server 2012 R2 |  | Microsoft     |

# ▲ WebADM Authentication Policy

Here, WebADM is configured with the authentication policy LDAP + OTP but, LDAP credentials are not checked by WebADM/OpenOTP but by Windows. In any case, OpenOTP will only check the OTP password.

Enter your OTP password on the next screen and click on **Submit**.



#### And you are logged on:

| Work Resourc             | 2S<br>nnection | RD Web Access   |
|--------------------------|----------------|-----------------|
| RemoteApp and Desktops   |                | Help   Sign out |
| Current folder: /        |                |                 |
| 📑 🛷 🖭                    |                |                 |
| Calculator Paint WordPad |                |                 |
|                          |                |                 |
|                          |                |                 |
|                          |                |                 |
|                          |                |                 |

It's done for the RDWeb.

## 3.1 Enable MFA for the RDWeb Apps.

If you have Remote applications accessible through RDWeb portal, and you want to secure these applications access with OpenOTP, you have to install OpenOTP Plugin for Windows Login.

|  |  |   |        |      | RD Web Access |
|--|--|---|--------|------|---------------|
| Work Resources<br>RemoteApp and Desktop Connection |  |   |        |      |               |
| Current folder: /                                  | RemoteApp<br>Starting your app<br>Server Manager | - | • ×    | Help | Sign out      |
| Manager<br>Server Manager                          | Configuring remote session                       |   | Cancel |      |               |
|  |  |   |        |      |               |







To enable Multi-Factor Authentication (MFA) for every connection, even if you close the published app, follow these steps:

To ensure MFA is required for every connection, you need to activate the

set time limit for logoff of remoteapp sessions option. This can be done under the host machine
(Windows server).

#### **Configuration Steps :**

> Login with an administrator account, press "Window" + "R" to launch the "Run" window.

| Ø             | Run X   |  |  |  |  |
|---------------|---|--|--|--|--|
|               | Type the name of a program, folder, document, or Internet resource, and Windows will open it for you. |  |  |  |  |
| <u>O</u> pen: | [ v   |  |  |  |  |
|               | 😵 This task will be created with administrative privileges.   |  |  |  |  |
| -             |   |  |  |  |  |
|               | OK Cancel Browse  |  |  |  |  |
| 1.            |   |  |  |  |  |

> Enter "gpedit.msc" and press "Enter" to enter the local group policy editor.

| File Action   View Help   Image: Computer Policy   Image: Computer Configuration   Image: Compu  | 9   | Local  | Group Policy Editor                                  | _ <b>D</b> X |
|--|---|--|--|--------------|
| <ul> <li>Concerne Configuration</li> <li>Software Settings</li> <li>Mathematicative Templates</li> <li>Software Settings</li> <li>Softw</li></ul> | File Action View Help   |  |  |              |
| <ul> <li>Local Computer Configuration</li> <li>Computer Configuration</li> <li>Windows Settings</li> <li>Software Settings</li> <li>Software Settings</li> <li>Mindows Settings</li> <li>Administrative Templates</li> </ul>   | (* *) 💽 🔛 🛃 🖬   |  |  |              |
|  | <ul> <li>Local Computer Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Administrative Templates</li> <li>User Configuration</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Windows Settings</li> <li>Administrative Templates</li> </ul> | Local Computer Policy     Select an item to view its description.     Extended      Standard | Name<br>Computer Configuration<br>User Configuration |              |
|  |   |  |  |              |

Find I Computer Configurations-> Administrative Templates-> Windows Components-> Remote Desktop Services-> Remote Desktop Connection Host-> Session Time Limits.



> Select "Set Time Limit for Logoff of RemoteApp Sessions", right click to select "Edit".



> Select "Enabled", and select a time at the options for "End a disconnected session", and then click "OK" to apply the configurations.

| Set time limit for logoff of RemoteApp sessions       Previous Setting       Next Setting         Not Configured       Comment:       Image: Comment:       Image: Comment:         Disabled       Supported on:       At least Windows Server 2008       Image: Comment:         Options:       Help:       Image: Comment:       Image: Comment:         Not Configured       Supported on:       At least Windows Server 2008       Image: Comment:         Options:       Help:       Image: Comment:       Image: Comment:         Not Configured       Supported on:       Help:       Image: Comment:         Options:       Help:       Image: Comment:       Image: Comment:         Image: Comment:       Supported on:       Help:       Image: Comment:         Image: Comment:       Help:       Image: Comment:       Image: Comment:         Image: Comment:       Help:       Image: Comment:       Image: Comment:         Image: Comment:       Help:       Image: Comment:       Image: Comment:         Image: | Set time limit for logoff of Remote     | app sessions   | _   |   | $\times$          |
|--|---|--|---|---|-------------------|
| Not Configured       Comment: <ul> <li>Disabled</li> <li>Supported on:</li> <li>At least Windows Server 2008</li> </ul> Options:       Help:         RemoteApp session logoff delay:       This policy setting allows you to specify how long a user's RemoteApp session will remain in a disconnected state after closing all RemoteApp programs before the session is logged off from the RD Session Host server.         By default, if a user closes a RemoteApp program, the session is disconnected from the RD Session Host server, but it is not logged off.         If you enable this policy setting, when a user closes the last running RemoteApp program associated with a session, the   | Set time limit for logoff of RemoteA    | pp sessions Previous Setting   | Next Setting  |   |                   |
| O Disabled       At least Windows Server 2008         Options:       Help:         RemoteApp session logoff delay:       This policy setting allows you to specify how long a user's RemoteApp programs before the session is logged off from the RD Session Host server.         By default, if a user closes a RemoteApp program, the session is disconnected from the RD Session Host server, but it is not logged off.         If you enable this policy setting, when a user closes the last running RemoteApp program associated with a session, the   | Not Configured     Comment:     Enabled |  |   |   | ~                 |
| Options:       Help:         RemoteApp session logoff delay:       This policy setting allows you to specify how long a user's RemoteApp session will remain in a disconnected state after closing all RemoteApp programs before the session is logged off from the RD Session Host server.         By default, if a user closes a RemoteApp program, the session is disconnected from the RD Session Host server, but it is not logged off.         If you enable this policy setting, when a user closes the last running RemoteApp program associated with a session, the   | O Disabled Supported on:                | At least Windows Server 2008   |   |   | < >               |
| RemoteApp session logoff delay:       This policy setting allows you to specify how long a user's         RemoteApp session will remain in a disconnected state after         closing all RemoteApp programs before the session is logged off         from the RD Session Host server.         By default, if a user closes a RemoteApp program, the session is         disconnected from the RD Session Host server, but it is not         logged off.         If you enable this policy setting, when a user closes the last         running RemoteApp program associated with a session, the  | Options:                                | Help:  |   |   |                   |
| RemoteApp session will remain in a disconnected state until the<br>time limit that you specify is reached. When the time limit<br>specified is reached, the RemoteApp session will be logged off<br>from the RD Session Host server. If the user starts a RemoteApp<br>program before the time limit is reached, the user will reconnect<br>to the disconnected session on the RD Session Host server.<br>If you disable or do not configure this policy setting, when a user<br>closes the last RemoteApp program, the session will be<br>disconnected from the RD Session Host server but it is not  | RemoteApp session logoff delay:         | This policy setting allows you to<br>RemoteApp session will remain<br>closing all RemoteApp program<br>from the RD Session Host server<br>By default, if a user closes a Ren<br>disconnected from the RD Sessi<br>logged off.<br>If you enable this policy setting,<br>running RemoteApp program a<br>RemoteApp session will remain<br>time limit that you specify is rea<br>specified is reached, the Remote<br>from the RD Session Host server<br>program before the time limit is<br>to the disconnected session on<br>If you disable or do not configu<br>closes the last RemoteApp prog<br>disconnected from the RD Sessi | specify how long a<br>in a disconnected sta<br>s before the session i<br>hoteApp program, th<br>on Host server, but it<br>when a user closes t<br>ssociated with a sessi<br>in a disconnected sta<br>iched. When the time<br>App session will be l<br>f. If the user starts a R<br>reached, the user with<br>the RD Session Host<br>re this policy setting,<br>ram, the session will<br>on Host server but it | user's<br>ate after<br>is logged o<br>e session is<br>is not<br>he last<br>ion, the<br>ate until the<br>elimit<br>logged off<br>emoteApp<br>ill reconnect<br>server.<br>when a us<br>be<br>is not | e<br>e<br>t<br>er |

Now you can use the gpupdate /force command in PowerShell to forcibly update Group Policy.

# 4. How to configure RDGateway with NPS and OpenOTP over RADIUS

# A Push Login is mandatory in that scenario

The RDS scenario with NPS, OpenOTP and Radius Bridge can only work with the push login infrastructure. NPS didn't manage the RADIUS challenge, that's why it's mandatory to use the Push login.

## 4.1 Workflow



- 1. The user initiates an RDP session with an RDP file previously downloaded from the RDWeb server.
- 2. The RDP connection starts through the RDP client. The RDP client contacts the RDGateway. The RDGateway communicate with NPS to check users policies and resources allowed for this user.
- 3. At this step, the first validation with Kerberos is in progress.
- 4. A Kerberos ticket is created for this user and send back to NPS.
- 5. NPS act as a PROXY RADIUS too. Once NPS has received the Kerberos validation, a RADIUS *Access-Request* is sent to Radius Bridge by NPS.
- 6. The Radius *Access-Request* is translated into a SOAP *Access request* by Radius Bridge product to be managed by OpenOTP server. OpenOTP will validate LDAP credentials and send a push login request to the user's mobile.
- 7. If LDAP Credentials are validated by OpenOTP server, then a push login request is sent RCDevs Push servers.
- 8. RCDevs Push Servers communicate with Google/Apple Push services.
- 9. The user receives the push login request on his phone and has to Accept or Reject the login attempt.
- 10. The response from the mobile is sent to WAProxy server and WAProxy forward the mobile response to OpenOTP server.
- 11. OpenOTP manages the response and accept or reject the login attempt according to the mobile response.
- 12. OpenOTP sends a « SOAP access accept » request to Radius Bridge.

- 13. Radius Bridge translates the SOAP request into a RADIUS request. The response is sent to NPS. NPS receives the authorization from the RADIUS server to allow the connection for this user. The user is successfully authenticated in 2FA.
- 14. RDGateway allows the user to access to Session Hosts according to policies configured on NPS for this user and resources allowed.

#### 4.2 RDGateway Configuration

We will start by configuring the RDGateway component. Open the RD Gateway manager console.

Right click on Connection Authorization Policies > Create New Policy > Wizard.



You will be prompted to the following screen:



Select Create an RD CAP and an RD RAP option and click Next.

Provide a name for your RD CAP.





Select your user group and a computer group membership.

| Create New Authorization Policies V   | Vizard X  |
|---|---|
| Authorization Policies<br>Connection Authorization Policy<br>Requirements<br>Device Redirection<br>Session Timeout                                | Select at least one supported Windows authentication method. If you select both methods, users that use either method will be allowed to connect.   |
| RD CAP Summary<br>Resource Authorization Policy<br>User Groups<br>Network: Resource<br>Allowed Ports<br>RD RAP Summary<br>Confirm Policy Creation | Add the user groups that will be associated with this RD CAP. Users who are members of these groups can connect to this RD Gateway server. User group membership (required): SUPPORT20\Domain Admins Add Group Remove                       |
|   | Optionally, you can add computer groups that will be associated with this RD CAP. Client computers that are members of these groups can connect to this RD Gateway server.  Client computer group membership (optional):  Add Group  Remove |
|   | < Previous Next > Freeh Cancel  |



| File | Action View Help<br>Action View Help<br>Create New Authorization Policies<br>Set Session   | Waard  | ×                        |
|------|--|--|--------------------------|
|      | Authorization Policies<br>Connection Authorization Policy<br>Requirements<br>Device Redirection<br>Session Trimeout<br>RD CAP Summary<br>Resource Authorization Policy<br>User Groups<br>Network Resource<br>Alowed Ports<br>RD RAP Summary<br>Confirm Policy Creation | Specify timeout and reconnection settings for remote sessions. |                          |
| <    |  | < Previou  | 8 Next > Freihall Cancel |





| Create New Authorization Policies With   | roups   | ×     |
|--|---|-------|
| Authorization Policies<br>Connection Authorization Policy<br>Requirements<br>Device Redirection<br>Session Timeout<br>RD CAP Summary<br>Resource Authorization Policy<br>User Groups<br>Network Resource<br>Allowed Ports<br>RD RAP Summary<br>Confirm Policy Creation | Add the user groups that will be associated with this RD RAP. Users who are members of these groups can connect to network resources remotely through RD Gateway.<br>If you have just configured a RD CAP by using this wizard, the same user group that you associated with the RD CAP will be specified. To specify another group, click the group that you want to remove, click. Remove, and then click Add Group.<br>User group membership (required):<br>SUPPORT20/Domain Admins<br>Add Group<br>Remove |       |
|  | < Previous Next > Eastb C   | ancel |





| Create New Authorization Policies Wiz  | tard   | ×                    |
|--|--|----------------------|
| RD RAP Settin  | gs Summary   |                      |
| Authorization Policies<br>Connection Authorization Policy<br>Requirements<br>Device Redirection<br>Session Timeout<br>RD CAP Summary<br>Resource Authorization Policy<br>User Groups<br>Network Resource<br>Allowed Ports<br>RD RAP Summary<br>Confirm Policy Creation | You have specified that an RD RAP with the following settings be created:  If the user is a member of any of the following user groups: SUPPORT20\Domain Admins then the user can connect remotely through RD Gateway to any computer on the network and the user can connect to these network resources (computers) through the following ports: Default port: 3389 |                      |
|  | < Previous   | Next > Finish Cancel |



The configuration wizard is now finished.

Now click right on your server name under RD Gateway Manager console and select **Properties**.



Under the **SSL Certificate** tab, select your Certificate signed by your CA or select a self-signed certificate. On my side, I select a certificate issued by my internal CA.

| File Action View Help  |   |  |   |  |   |   |       |   |
|--|---|--|---|--|---|---|-------|---|
| RD Gateway Manager     RD 2 (Local)     Gonection Authorization Policies     Gonection Authorization Policies     Monitoring | Policies Import Cert No certificate to Certificate to Show al Show al | RDS2 Properties<br>Server Fam<br>General<br>Cetificate is nee<br>messaging. Cetificate<br>es are currently instal<br>a certificate. s<br>the RD Gateway se<br>Issued 8<br>vorders CA<br>oredevs. RDS2 y<br>etficate<br>cetificates in (Local | Audtin<br>SSL Certificate<br>ded for secure commiscate is automatically<br>eway to function cor-<br>led.<br>alect the certificate<br>river, select the cert<br>winter the certificate<br>orcodevs.com Service<br>Computer/Personal<br>incare mito me rur us<br>pool Computer/Personal | Comparison of HTT<br>munication of HTT<br>bound to the co<br>rectly, you must a<br>that you want to.<br>ifficate, and then<br>that you want to.<br>ifficate, and then<br>wated Purpose<br>if Authentication<br>if Authentication<br>at Authentication<br>if Authentication<br>at Authent | SL Bridging<br>port Settings<br>PS/UDP lateness a<br>ringured HTTP and<br>elect an existing SS<br>and then click Vie<br>click Import.<br>Expiration Date<br>V11/2020<br>7/12/2019 | Messaging<br>RD CAP Store<br>Ind for NAP<br>UDP pots.<br>3L certificate or<br>w Certificate. To impor<br>Remark<br>Valid Certificate<br>Valid Certificate | × × × | Actions<br>RDS2 (Local)  Conot manage this se<br>Export policy and confi<br>Import policy and conf<br>Properties<br>View  Refresh<br>Help |
| ¢  | >   |  |   |  | ОК Са   | ncel Apply  |       | FNC 220 AM  |



My certificate will now be used to trust the Gateway.

Now, go to RD CAP Store and choose the location of your NPS server. On my side, NPS is installed on the same server.

| RD Geteway Manager<br>File Action View Help   |   | - 6 ×  |
|---|---|--|
| 🗢 🔶 📶 🖬 🔟   |   |  |
| RD Gateway Manager     BDS (Loca)     Policies     Connection Authorization Policies     Resource Authorization Policies     Monitoring | RDS2 Properties         Server Fam       Audting       SSL Bridging       Messaging         General       SSL Certificate       Transport Settings       RD CAP Store         Specify whether to use Remote Desktop connection authorization policies (RD CAPs) stored on the local or central server that is running Network Policy Server (NPS).            Local server nurning NPS <ul> <li>Use RD Gateway Manager to manage RD CAPs.</li> <li>Central server nurning NPS</li> <li>Use the central Network Policy Server snap-in to manage RD CAPs and to enforce health policies for clients.</li> </ul> Enter a name or IP address for the server nurning NPS:       Order       DNS Name       Second S | Actions       RDS2 (Local)       X     Do not manage this se       Export policy and confi       Import policy and conf       Yroperties       View       Refresh       Help |
| ٤ ،   |   | 1  |
|   |   | ENG 3:41 AM  |

Under the Server Farm tab, add your current RD Gateway server(s).



The configuration of RD Gateway is now finished!

## 4.3 NPS Configuration

#### 4.3.1 Remote RADIUS Server Groups

We will now configure the NPS component. NPS manages which user is able to log in on which resource, the authentication method...

First, we will configure a Remote RADIUS Server Group and edit the default group TS GATEWAY SERVER GROUP.



Right click > Properties on theTSGatewayServerGroup. Under the General tab, clickAddbutton to add a RADIUSServer.192.168.3.54is my Radius Bridge server installed on my OpenOTP/WebADM server.

| Network Policy Server   |  | - 0 X  |
|---|--|--|
|   |  |  |
| <ul> <li>NPS (Local)</li> <li>ADUIS Clients and Servers         <ul> <li>RADIUS Clients</li> <li>Remote RADIUS Server Groups</li> <li>Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul> </li> </ul> | Remote RADIUS Server       X         Add RADIUS Server       X         Address       Authentication/Accounting       Load Balancing         Select an existing Remote RADIUS Servers template:       V         None       V         Type the name or IP address of the RADIUS server you want to add.         Server:       192 168 3 54         Verfy | when the local NPS server is configured as a |
|   | OK Cancel  |  |
| 🕶 0 m 🐔 🖿 🖡   |  | ENG 4:31 AM                                  |

On the Authentication/Accounting tab, configure your Radius secret.

| Network Policy Server   |   | - 6 X  |
|---|---|--|
| File Action View Help   |   |  |
| 💠 🔿 🙍 📷 📓 🗊   |   |  |
| <ul> <li>MPS (Local)</li> <li>MPS (Local)</li> <li>RADIUS Clients and Servers</li> <li>RADIUS Clients</li> <li>Remote RADIUS Server Groups</li> <li>Policies</li> <li>Templates Management</li> </ul> | Remote RADIUS Server Groups         Add RADIUS Server       ×         Address       Authentication/Accounting       Load Balancing         Address       Authentication pot:       1812         Select an existing Shared Secrets template:       None       ×         Shared secret:       •       •         Confirm shared secret:       •       •         Conting       Accounting       •         Accounting poot:       1813       •         Use the same shared secret for authentication and accounting.       Select an existing Shared Secrets template:         None       •       1813         Use the same shared secret for authentication and accounting.       Select an existing Shared Secrets template:         None       •       •         Shared secret:       •       •         Confirm shared secret:       •       •         Provad network access server start and stop notifications to this server       • | when the local NPS server is configured as a |
|   | < OK Cancel   | 3  |
| 🖷 A 🗆 🗲 🗖 💺   | 93 🚯 🔜 🕾  | ∧ 덮 4,8 ENG 4:33 AM<br>FR 1/11/2019 록        |

Under the Load Balancing tab, configure your timeout value and the priority if you configure more than 1 server.

|  | C YO_SSTP   | Pour relâcher votre souris, appuyez sur : Control-  |
|--|---|---|
|  |   |   |
| Image: Server     File     Action     View     Help       Image: Server     File     Action     View     Help       Image: Server     RADIUS Clients and Servers     Image: RADIUS Clients       Image: RADIUS Clients     Image: RADIUS Clients       Image: RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clients     Image: Remote RADIUS Server Groups       Image: Remote RADIUS Clien | Add RADIUS Server      Address Authentication/Accounting Load Balancing      The priority of ranking indicates the status of a server. A primary server has a priority of      The violity of ranking indicates how often request are series to a specific server in a group of servers that have the same priority.      Priority:      The violity:      Th | requests when the local NPS server is configured as |
|  | Maximum number of dropped requests before server is 3 Identified as unavailable: Number of seconds between requests when server is identified 40 as unavailable: OK Cancel  |   |
|  |   | -   |
| Action: In program   | ]   |   |
| Action: in progress  |   |   |
| 📲 🔎 🗆 🖉 🔚 📗  |   | ·  문 네a 18:22 등                                     |
|  |   | 19/09/2019  |
|  |   |   |

Once the configuration is done, click  ${\tt Save}$  and  ${\tt Ok}$  .

At this step, you can also configure the Radius Client and his secret on Radius Bridge Server to allow NPS to communicate with Radius Bridge.

vi /opt/radiusd/conf/clients.conf

At the end of this file you should have your NPS Server configured like below:

```
client NPS {
    ipaddr = 192.168.3.119
    secret = testing123
}
```

Your Radius Server is now configured at the NPS level.

#### 4.3.2 Connection Request Policies

We will now create a new Connection Request Policy.

| 11 8 3 ↔ 5   |                 | 624  |              |                     | 0   |                      |     |
|--|-----------------|--|--------------|---------------------|---|----------------------|-----|
| Network Policy Server  |                 |  |              |                     |   | - 6                  | ×   |
| File Action View Help  |                 |  |              |                     |   |                      |     |
| 🗢 🌩 🖄 🔟 🔟 🔟  |                 |  |              |                     |   |                      |     |
| NPS (Local)  | ( )             | Connection Request Policies  |              |                     |   |                      |     |
| RADIUS Clients and Server     RADIUS Clients     Remote RADIUS Server     Policies     | r Groups        | Connection request policies allow you to servers.  | designate wh | ether connection re | quests are processed locally or forwarded | to remote RADIUS     |     |
| Connection Reques  |                 | Silcy Name   | Status       | Processing Order    | Source                                    |                      |     |
| <ul> <li>Network Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul> | New D           | TS GATEWAY AUTHORIZATION POLICY  | Enabled      | 1                   | Remote Desktop Gateway                    |                      |     |
|  | Export List     | Use Windows authentication for all users   | Disabled     | 1000000             | Unspecified                               |                      |     |
|  | anagemer View > |  |              |                     |   |                      |     |
|  | Refresh         |  |              |                     |   |                      |     |
|  | Help            |  |              |                     |   |                      |     |
|  |                 | Condition Value<br>Day and time restrictions Sunday 00:00-24:0<br>Settings - Then the following settings are applied | 0 Monday 00  | :00-24:00 Tuesday 0 | 00.00-24.00 Wednesday 00.00-24.00 Th      | /reday 00:00-24:00 . | 1.0 |
|  |                 | Setting Value<br>Authentication Provider Local Computer  |              |                     |   |                      |     |
|  |                 |  |              |                     |   |                      |     |

Name your policy and select Remote Desktop Gateway as Type of network access server.

| II 8 3 00   |  | 0   |
|---|--|---|
| Network Palicy Server<br>File Action View Help  |  | - 6 )   |
| 📥 🔿 📷 🛛 📾   |  |   |
| NPS (Local)  ADJUS Clients and Serv  RADJUS Clients  RADJUS Clients  Remote RADJUS Serv  Policies  Connection Request | New Connection Request Policy Specify Connection Request Policy Name and C You can specify a name for your connection request policy and the type of c   | Connection Type varded to remote RADIUS onnections to which the policy is applied.                          |
| Network Policies  | Balan arms   |   |
| Accounting  | OpenOTP Connection Policy  |   |
|   | Select the type of network access server that sends the connection request to NPS. You can set<br>type or Vendor specific, but neither is required. If your network access server is an 802.1X suffer<br>select Unspecified. | ect ether the network access server<br>riloating switch or wreless access point,<br>00 Thursday 00.00-24.00 |
|   | L₂   |   |
|   | Erevonus.  | Eynah Cancel  |
| Action: In progress   |  |   |
| = P 🗆 🌔   | 🗧 🔚 😘 🦻 🛶 🗠  | ∧   |
|   |  | 11 11/2013  |

Click Next.

You have now to specify conditions of this policy.

|  | (a) Y   | /O_RDS2                                     | Pour relâcher                | votre souris, appuyez sur : Contro |
|--|---|---|------------------------------|------------------------------------|
| II 5                                       |   |   | 0                            |                                    |
| Network Policy Server                      |   |   |                              | - 0 ×                              |
| Ella Action View Halo                      |   |   |                              |                                    |
| the Action view risp                       |   |   |                              |                                    |
|  |   |   |                              |                                    |
| NPS (Local)                                | New Connection Request Policy                             |   | ~                            |                                    |
| RADIUS Clients and Serv     BADIUS Clients | Specify Conditions  |   |                              | varded to remote RADIUS            |
| Remote RADIUS Sen                          | Spacify the conditions that determine whether             | this connection request policy is evaluate  | d for a connection request   |                                    |
| v I Policies                               | minimum of one condition is required.                     | this connection request policy is evaluat   | ed for a connection request. | <u>`</u>                           |
| Connection Request                         |   |   |                              |                                    |
| Network Policies                           | Select condition  |   | ×                            |                                    |
| Accounting                                 | Chairman Mar and the shift had                            |   |                              |                                    |
| > 🛒 remplates Managemen                    | Select a condition, and then click Add.                   |   |                              |                                    |
|  | The NAS Identifier condition specifies a character string | that is the name of the network access s    | erver (NAS). You             |                                    |
|  | can use pattern matching syntax to specify NAS names.     |   |                              |                                    |
|  | NAS IPv4 Address  | on 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 s    | string that is the IPv6 address of the NAS. | You can use                  |                                    |
|  | NASPortType   |   |                              |                                    |
|  | The NAS Port Type condition specifies the type of media   | a used by the access client, such as anal   | og phone lines,              | 00 Thursday 00:00-24:00            |
|  | SUN, tunnels or virtual private networks, IEEE 802.11 w   | irreless, and Ethernet switches.            |                              |                                    |
|  |   |   |                              |                                    |
|  |   |   | ~                            |                                    |
|  | L   | N   |                              |                                    |
|  |   | ß   | Add Cancel                   |                                    |
|  |   | G [   | Add Cancel                   |                                    |
|  |   |   | Add Cancel                   |                                    |
|  |   | ka [  | Add Cancel                   |                                    |
|  |   | Lo Lo                                       | Add Cancel                   |                                    |
|  |   | L3 [  | Add Cancel                   |                                    |
|  |   | Add   | Add Cancel                   |                                    |
|  |   | Add   | Add Cancel                   |                                    |
|  |   | Add   | Add Cancel                   |                                    |
|  |   | Add   | Add Cancel                   |                                    |
| uction: In progress                        |   | Add   | Add Cencel                   |                                    |
| ction: In progress                         |   | Add   | Add Cancel                   | 1. ENG 4.50 AM                     |
| kction: In progress<br>Ħ                   |   | Add   | Add Cancel                   | d. €NG 4:50 AM<br>FR 1/11/2019 ₽   |
| Action: In progress                        |   | Add   | Add Cancel                   | d. ENG 4:50 AM<br>FR 1/11/2019 ₽   |

Select NAS port Type and then Virtual (VPN) as value.

| Ⅱ 恶 飞 ↔   |  | 0   |
|---|--|---|
| Network Policy Server   |  | - 6 X   |
|   |  |   |
|   | New Connection Request Policy  | ×   |
| RADIUS Clients and Serv<br>RADIUS Clients<br>Remote RADIUS Serv<br>Policies<br>Connection Request | Specify Conditions Specify the conditions that determine whether this connection request policy is evalu minimum of one condition is required. | varded to remote RADIUS<br>ated for a connection request. A |
| Network Policies  | Conditions:  |   |
| Accounting  | Condition Value  |   |
|   | S NAS Port Type Virtual (VPN)  |   |
|   | Condition description:   | 00 Thursday 00:00-24:00                                     |
|   | La Add   | Edt., Remove  |
|   | Previous Next  | Finish Cancel   |
|   |  |   |
|   |  |   |
| Action: In progress   |  |   |
| Action: In progress   |  | ^ 洰 4, ENG 4:50 AM  |

Click **Next** and on the next page, select your Radius Server group previously configured.

| Network Policy Server   File Action View Help   Help Image: Constraint of the policy Server New Constraint of the policy Server   RADIUS Clients and Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Constraint of the policy Server Image: Constraint of the policy Server   Image: Const   | nection Request Policy<br>Specify Com<br>The connection req<br>remote RADIUS ser<br>icy conditions match the con<br>actions match the con<br>actions for the context of | nection Request Forwarding<br>Lest can be authenticated by the local server or it can be forw<br>ver group.<br>nection request, these settings are appled.<br>Specify whether connection requests are processed locally, ar<br>RADIUS servers for authentication, or are accepted without as | arded to RADIUS servers in a                         | - O ×                   |
|---|---|--|--|-------------------------|
| Proficies     Accounting     Accounting     Templates Management     Accounting     Account | section Request Policy     Specify Con     The connection request Policy     The connection request Policy     The connection request Policy     Section Policy     Therefore Policy     Section Polic                 | nection Request Forwarding<br>wer group.<br>nection request, these settings are appled.<br>Specify whether connection requests are processed locally, ar<br>RADIUS servers for authentication, or are accepted without as  | arded to RADIUS servers in a                         | varded to remote RADIUS |
| <ul> <li>NPS (Local)</li> <li>RADIUS Clients and Sev<br/>RADIUS Clients and Sev<br/>RADIUS Clients<br/>Remote RADIUS Sen<br/>Connection Request<br/>Accounting<br/>Accounting<br/>Templates Management     </li> </ul>  | nection Request Policy Specify Con The connection request Policy The connection request Policy The connection request Policy The connection request Policy The connection T            | nection Request Forwarding<br>set can be authenticated by the local server or it can be forw<br>ver group.<br>nection request, these settings are appled.<br>Specify whether connection requests are processed locally, ar<br>RADIUS servers for authentication, or are accepted without as  | × arded to RADIUS servers in a reforwarded to remote | varded to remote RADIUS |
| Accounting     Metwork Policies     F the policy     Accounting     Templates Management     Settingg     Corva     Reque     Accounting   | icy conditions match the con<br>a:<br>arding Connection<br>rat<br>athentication   | nection request, these settings are applied.<br>Specify whether connection requests are processed locally, at<br>RADIUS servers for authentication, or are accepted without at   | re forwarded to remote                               |                         |
| Forwa<br>Reque  | arding Connection<br>est<br>athentication   | Specify whether connection requests are processed locally, ar<br>RADIUS servers for authentication, or are accepted without a  | re forwarded to remote                               |                         |
|   | counting  | Authenticate requests on this server Forward requests to the following remote RADIUS server g TS GATEWAY SERVER GROUP Accept users without validating oredentials  | uthentication:                                       | 00 Thunday 00:00-24:00  |
|   |   | Previous Next  | Front Cancel   |                         |
| Action: In progress   | L 3   | <u> </u>   | ^ 단  | 450 AM<br>FR 1/11/2019  |

| 11 8 3, ↔  |  | 2 (  |                         |
|--|--|--|-------------------------|
| Network Policy Server  |  |  | - 6 X                   |
| File Action View Help  |  |  |                         |
| 🗢 🏟 🙇 📷 🛛 🖬 ,  |  |  | 7                       |
| NPS (Local)     ADJUS Clients and Serv     RADIUS Clients     RADIUS Clients     Remote PADIUS Sen | New Connection Request Policy Configure S  | Settings   | varded to remote RADIUS |
| Policies     Connection Request     Network Policies   | matched.   | gs to the connection request if all of the connection request policy conditions for the policy are                           |                         |
| Accounting   | Configure the settings for this netwo<br>If conditions match the connection r<br>Settings: | rk policy.<br>equest and the policy grants access, settings are applied.   |                         |
|  | Specify a Realm Name   | Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the lat. |                         |
|  | RADIUS Attributes  | Attribute: Called-Station-Id ~   |                         |
|  | Vendor Specific  | Find Replace With Add  |                         |
|  |  | Edit<br>Remove<br>Move Up  | 00 Thunday 00:00-24:00  |
|  |  | Move Down  |                         |
|  |  | bg.  |                         |
|  |  | Previous Next Finals Cancel  |                         |
|  |  |  |                         |
| Action: In progress  |  |  | 4 ENG 5:06 AM           |
|  |  |  | FR 1/11/2019            |

| Network Policy Server   |  |  | - 6                     |
|---|--|--|-------------------------|
| File Action View Help   |  |  |                         |
| 💠 🔿 🙍 📷 🔒 📖 🔔   |  |  |                         |
| NPS (Local)     ADIUS Clients and Serv     RADIUS Clients     RADIUS Clients     Remote RADIUS Serv     Policies     Connection Request | New Connection Request Policy Completing C   | Connection Request Policy Wizard           | varded to remote RADIUS |
| <ul> <li>Network Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul>  | You have successfully created the foll<br>OpenOTP_Connection_Policy<br>Policy conditions:                | lowing connection request policy:          |                         |
|   | Condition Value  |  |                         |
|   | (NAS Port Type Virtual (VPN)   |  |                         |
|   | Policy settings:<br>Condition Value<br>Authentication Provider Forw<br>Authentication Provider Name TS G | e<br>arding Request<br>ATEWAY SERVER GROUP | 00 Thumday 00:00-24:00  |
|   | To close this wizard, click Finish.  |  |                         |
| Action: In progress   |  | Previous Not P                             | nieh Cancel             |
| E 🖉 🗆 🌔   | 🗖 🔚 🤧 👂  | » 🥁 📼                                      | ヘ 記 👍 ENG 5:06 AM       |

Click on Finish button.

My connection request policy is now created and activated.

|  | \$ B Z 4   |                                 |                     | 0   |                      |   |
|--|--|---------------------------------|---------------------|---|----------------------|---|
| Network Policy Server<br>File Action View Help   |  |                                 |                     |   | - 0                  | × |
| 🗢 🔿 📶 🗳 🔟  |  |                                 |                     |   |                      |   |
| NPS (Local)     NO (Local)     ADJUS Clients and Servers     RADIUS Clients     RADIUS Clients     Remote RADIUS Server Groups     Policies     Competing Request Policies | Connection Request Policies Connection request policies allow you to servers. Policy Name  | designate who<br>Status         | ether connection re | quests are processed locally or forwa                           | rded to remote RADIU | S |
| <ul> <li>Network Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul>   | OpenOTP_Connection_Policy<br>TS GATEWAY AUTHORIZATION POLICY<br>Use Windows authentication for all users                               | Enabled<br>Disabled<br>Disabled | 1<br>2<br>1000000   | Remote Desktop Gateway<br>Remote Desktop Gateway<br>Unspecified |                      |   |
| l⊋   | TS GATEWAY AUTHORIZATION POLICY<br>Conditions - If the following conditions are met:<br>Condition Value<br>NAS Port Type Virtual (VPN) |                                 |                     |   |                      |   |
|  | Settings - Then the following settings are applie<br>Setting Value<br>Authentication Provider Local Computer                           | d:                              |                     |   |                      |   |
| # P © 6 🖬 💺  | 9 👂 🖌 🗠  |                                 |                     | ~ 뒫 4   | ENG 5:10 AM          | 1 |

## 4.3.3 Network Policies

We will now configure a Network Policy through the NPS console. Right click on **Network Policies** > **New**.



Name your Network Policy, select Remote Desktop Gateway as Type of network access server and then click Next.

| II 8 → ↔   |   |   |
|--|---|---|
| Network Palicy Server<br>File Action View Help   |   | - 0 ×   |
| 💠 🔿 🙍 🛅 🖬 🔐  |   | _   |
| NPS (Local)  RADIUS Clients and Serv  RADIUS Clients  RADIUS Clients  Remote RADIUS Serv  Policies                                   | New Network Policy         >           Specify Network Policy Name and Connection Type            You can specify a name for your network policy and the type of connections to which the policy is applied.         >  | under which they can or   |
| <ul> <li>Policies</li> <li>Connection Request</li> <li>Network Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul> | Policy name:<br>Network_OpenOTP_Policy  | Type Source<br>coess Remote Desktop Gat<br>coess Unspecified<br>coess Unspecified |
|  | Network connection method<br>Select the type of network access server that sends the connection request to NPS. You can select either the network access server<br>type or Vendor specific, but nether is required. If your network access server is an 802 1X authenticating switch or wireless access point,<br>select Unspecified. |   |
|  | Remote Desktop Gateway ~ ~<br>O Vendor specific:  | 00 Thursday 00:00-24:00   |
|  | l≱  |   |
|  | Previoual Next Pesalty. Cancel  | CHAP v2 OR MS-CHAP  |
| Action: In progress  |   |   |
| # > © (e   | n 🔁 💁 🔽 🔤 🔤 👘   | C 4 ENG 5:12 AM<br>FR 1/11/2019   |

On the following screen, you have to specify conditions.

| 000<br>H H 3 11 1  |   | W YO_RDS2  | Pour relâch  | er votre souris, appuyez sur : Control |
|--|---|--|--|--|
| 1 6 4 00   |   |  | C <sup>2</sup>   |  |
| Network Policy Server<br>File Action View Help   |   |  |  | - 6 X                                  |
| 🗢 🔿 🙍 📷 👔 👘  |   |  |  | -                                      |
| NP5 (Local)     ADIUS Clients and Serv     RADIUS Clients     RADIUS Clients     Remote RADIUS Serv     Policies | New Network Policy  Specify Conditions  Specify the conditions that determ of one condition is required.  | ine whether this network policy is evaluated for a   | connection request. A minimum  | under which they can or                |
| Connection Request   | Colored and Diversion   |  |  | rype Source                            |
| Accounting   | Select a condition, and then click Add.   |  |  | cess Unspecified<br>cess Unspecified   |
|  | Windows Groups           The Vindows Groups condition specifies the groups           Machine Groups           The Machine Groups condition specifies the distribution of the groups           User Groups condition specifies that the Day and time restrictions           Day and Time R | at the connecting user or computer must belong to<br>the connecting computer must belong to one of the<br>e connecting user must belong to one of the select<br>and times when connection attempts are and are r<br>re the NPS server is located.<br>Add | ane of the selected<br>He selected groups.<br>ed groups.<br>Not allowed. These<br>Add:Cancel<br>EdtRemove. | 00 Thursday 00:00-24:00                |
|  |   | Previous Next  | Prost: Cancel  | CHAP v2 OR MS-CHAP                     |
| 1  |   |  |  |  |
| Action: in progress  |   |  |  | INC SALAM                              |
|  | 🗖 🔄 🕃 💽 🔤   | 8-1<br>-   | ~ 단  | FR 1/11/2019                           |
|  |   |  |  |  |

| ingure the conditions to<br>onditions match the cor<br>nection request, NPS s | This network policy. Inection request, NPS uses this policy to authorize the connection request, kips this policy and evaluates other policies, if additional policies are config | . If conditions do not match the<br>jured. |
|---|---|--|
| elect condition   | Heer Groups   | ×  |
| elect a condition, and t  | her   | ,  |
| Windows Gro<br>The Windows (<br>groups.                                       | Specify the group membership required to match this policy.<br>Groups   | of the selected                            |
| Machine Grou<br>The Machine G   | IPS SUPPORT20\Domain Admins   | ected groups.                              |
| User Groups<br>The User Grou<br>Day and time restriction                      | ps<br>ons   | pups.                                      |
| Day and Time<br>Day and Time<br>restrictions are                              | s R<br>Re<br>s ba Add Groups Remove   | lowed. These                               |
| Connection Properties   | ОК  | Cancel Add Cancel                          |
|   | Add   | Edit Remove                                |

You should have 3 following conditions configured in your Network Policy. For the Calling Station ID condition, put UserAuthType:(PWICA) value.

| Candhiana C   | 1.1.1. D.W.   |           |
|---|---|-----------|
| rview Conditions Cons                               | straints Settings   |           |
| nfigure the conditions for t                        | this network policy.  |           |
| conditions match the conn                           | nection request, NPS uses this policy to authorize the connection request. If conditions do not m | natch the |
| nnection request, NPS sk                            | tips this policy and evaluates other policies, if additional policies are configured.             |           |
|   |   |           |
| Condition   | Value   |           |
| User Groups   | SUPPORT20\Domain Admins   |           |
| NAS Port Type                                       | Virtual (VPN)   |           |
| Calling Station ID                                  | UserAuthType:(PWICA)  |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
|   |   |           |
| ndition description -                               |   |           |
| ndition description:                                |   |           |
| ndition description:<br>e Calling Station ID condri | tion specifies the network access server telephone number dialed by the access client.            |           |
| ndition description:<br>e Calling Station ID condit | tion specifies the network access server telephone number dialed by the access client.            |           |
| ndition description:<br>e Calling Station ID condit | tion specifies the network access server telephone number dialed by the access client.            |           |
| ndition description:<br>e Calling Station ID condit | tion specifies the network access server telephone number dialed by the access client.            |           |
| ndition description:<br>e Calling Station ID condi  | tion specifies the network access server telephone number dialed by the access client.            | Berrun    |
| ndition description:<br>e Calling Station ID condi  | tion specifies the network access server telephone number dialed by the access client.            | Remove    |
| ndition description:<br>e Calling Station ID condit | tion specifies the network access server telephone number dialed by the access client.            | Remove    |
| ndition description:<br>e Calling Station ID condit | tion specifies the network access server telephone number dialed by the access client.            | Remove    |
| ndition description:<br>e Calling Station ID condi  | tion specifies the network access server telephone number dialed by the access client.            | Remove    |

Once you have the 3 previous conditions configured, click  ${\tt Next}$  .

I configured this policy to allow the access so here I select Access Granted :

| 11 8 3 ↔ 1  |  |   |
|---|--|---|
| Network Policy Server<br>File Action View Help  |  | - 0 ×   |
| 🗢 🔿 🙍 📷 👔 🔐   |  |   |
| NPS (Local)     ADIUS Clients and Serv     RADIUS Clients and Serv     RADIUS Clients     Remote RADIUS Serv     Policies     Consection Request  | New Network Policy  Specify Access Permission  Configure whether you want to grant network access or deny network access if the connection request policy.   | matches this                                  |
| Connection Request     Connection Reques | Access granted     Grant access if client connection attempts match the conditions of this policy.     Access denied     Deny access if client connection attempts match the conditions of this policy.     Access is determined by User Dial-in properties (which overside NPS policy)     Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy. | coess Remote Desktop Gat<br>coess Unspecified |
|   | D₂   | 00 Thursday 00:00-24:00                       |
|   | Previous Next Pinaih C   | CHAP v2 OR MS-CHAP                            |
| Action: In progress   |  |   |
| # ^ 🗆 🤅   | 🗖 💺 🛂 🔊 🔤 🗁  | ヘ 記 de ENG 5:54 AM<br>FR 1/11/2019            |

I keep these settings by default.

| 1.5. 3.0   | ଔYO_RDS2 Pour reliad<br>ସାୟା ବିଙ୍ଶା ଅଧ୍ୟ  | her votre souris, appuyez sur : Contro                             |
|--|---|--|
| Network Policy Server<br>File Action View Help   |   | - 0 ×  |
| 💠 🔿 🙇 📷 👔 👘  |   | -  |
| NPS (Local)     ADJUS Clients and Serv     RADIUS Clients and Serv     Remote RADIUS Serv     Policies     Constraints Remote Reserved | New Network Policy         >           Image: Configure Authentication Methods         Configure and co | under which they can or  |
| Connection Request   | EAP types are negotiated between NPS and the client in the order in which they are lated. EAP Types: Movee Up   | coess Remote Desktop Gat<br>coess Unspecified<br>coess Unspecified |
|  | Add     Edt.     Plentove       Less secure aufhertication methods:     Microsoft Encrypted Authentication version 2 (MS/CHAP+v2)       Ø User can change password after t has expired       Ø Microsoft Encrypted Authentication (MS/CHAP)       Ø User can change password after t has expired       Encrypted authentication (RAP, SPAP)       Ø Hencorypted authentication (PAP, SPAP)       Ø Hencorypted authentication (PAP, SPAP)   | 00 Thursday 00:00-24:00  |
|  | Previous Next Provide   | CHAP V2 OR MS-CHAP   |
| Action: In progress  |   |  |
|  | े 🔜 🔚 💱 🔂 🖷 🗠 🗠   | FR 1/11/2019   |

I keep these settings by default.

| 1 8 3 0   |  | @ YO_RDS2   | D Pour reach  | er votre souris, appoyez sur : Contr |
|---|--|---|---|--------------------------------------|
| Network Policy Server<br>File Action View Help  |  |   |   | - 0 ×                                |
| Physic (Local)     RADIUS Clients and Serv     RADIUS Clients     Remote RADIUS Serv     Policies       | New Network Policy  Configure  Constraints are a  constraint is not r  | Constraints<br>dditional parameters of the network polic<br>natched by the connection request, NPS as | X<br>that are required to match the connection request. If a<br>tomatically rejects the request. Constraints are option | under which they can or              |
| Connection Request<br>Connection Request<br>Participation Request<br>Accounting<br>Templates Management | If you do not want to configure constraints, click Next. Configure the constraints for this network policy. If all constraints are not matched by the connection request, network access is denied. Constraints: |   | Type Source<br>coess Remote Desktop Gat<br>coess Unspecified<br>coess Unspecified                                       |                                      |
|   | Constraints<br>Session Timeout<br>Celled Station ID<br>Day and time<br>restrictions<br>NAS Port Type   | Specify the maximum time in minutes th<br>is deconnected<br>Disconnect after the maximum iden<br>1    | at the server can remain idle before the connection   | 00 Thursday 00:06-24:00              |
|   |  |   | à   |                                      |
|   |  | Previo  | us Ned Pranh Cancel   | CHAP V2 OR MS-CHAP                   |
| Action: In progress   |  |   |   | ENG 556 AM                           |
|   | e 🔚 🍕 -  | 📚 🖮 🔤   | ~ 탄   | FR 1/11/2019                         |

Here is a summary of my Network Policy.

|   |   | ~ |
|---|---|---|
| Con   | npleting New Network Policy   |   |
| ou have successful  | y created the following network policy:   |   |
| letwork_OpenOT  | P_Policy  |   |
| olicy conditions:   |   |   |
| C   | alue  |   |
| Condition   |   |   |
| User Groups S   | UPPORT20\Domain Admins  |   |
| User Groups S<br>NAS Port Type  | UPPORT20\Domain Admins<br>Intual (VPN)  |   |
| User Groups S<br>NAS Port Type Calling Station ID   | UPPORT20\Domain Admins<br>irtual (VPN)<br>IserAuthType:(PWICA)  |   |
| User Groups S<br>NAS Port Type N<br>Calling Station ID  | UPPORT20\Domain Admins<br>Irtual (VPN)<br>IserAuthType:(PWICA)  |   |
| User Groups S<br>NAS Port Type C<br>Calling Station ID  | :UPPORT20\Domain Admins<br>irtual (VPN)<br>IserAuth Type:(PWICA)  |   |
| User Groups S<br>NAS Port Type Calling Station ID   | :UPPORT20\Domain Admins<br>irtual (VPN)<br>IserAuthType:(PWICA)   |   |
| User Groups S<br>NAS Port Type C<br>Calling Station ID C<br>Olicy settings:   | :UPPORT20\Domain Admins<br>irtual (VPN)<br>IserAuthType:(PWICA)   |   |
| User Groups S<br>NAS Port Type C<br>Calling Station ID U<br>Olicy settings:<br>Condition  | UPPORT20\Domain Admins<br>Intual (VPN)<br>IserAuthType:(PWICA)<br>Value   |   |
| User Groups S<br>NAS Port Type Calling Station ID C<br>Calling Station ID C<br>Colicy settings:<br>Condition<br>Authentication Meth                             | IUPPORT20\Domain Admins Intual (VPN) IserAuthType:(PWICA) Value Value MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2  | 2 |
| Condition User Groups NAS Port Type Calling Station ID Olicy settings: Condition Authentication Meth Access Permission  | IUPPORT20\Domain Admins Intual (VPN) IserAuthType:(PWICA) Value Value MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 Grant Access                             | 2 |
| Condition<br>User Groups<br>NAS Port Type<br>Calling Station ID<br>Colicy settings:<br>Condition<br>Authentication Meth<br>Access Permission<br>Framed-Protocol | UPPORT20\Domain Admins<br>Intual (VPN)<br>IserAuthType:(PWICA)<br>Value<br>od MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2<br>Grant Access<br>PPP           | 2 |
| Condition User Groups NAS Port Type Calling Station ID Olicy settings: Condition Authentication Meth Access Permission Framed-Protocol Service-Type             | UPPORT20\Domain Admins<br>Intual (VPN)<br>IserAuthType:(PWICA)<br>Value<br>od MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2<br>Grant Access<br>PPP<br>Framed | 2 |

| Network Policy Server  |  |   | - a ×   |  |  |
|--|--|---|---|--|--|
| File Action View Help  |  |   |   |  |  |
|  |  |   |   |  |  |
| NP19 (Local)     Allocal     ADUUS Clients and Servers     ADUUS Clients     RADIUS Clients     Remote RADIUS Server Groups     Policies     Connection Request Policies | Network Policies  Network policies allow you to designate who is authorized to conn cannot connect.  Policy Name   | ect to the network and the circumstances u  | inder which they can or   |  |  |
| <ul> <li>Connection Kequest Policies</li> <li>Accounting</li> <li>Templates Management</li> </ul>  |  | Disabi 1 Deny Ac<br>Enabled 2 Grant Ac<br>Disabi 999999 Deny Ac<br>Disabi 1000000 Deny Ac | cess Remote Desktop Gat<br>Remote Desktop Gat<br>cess Unspecified<br>cess Unspecified |  |  |
|  | Connections to other access servers  |   |   |  |  |
|  | Condition Value<br>Day and time restrictions Sunday 00:00-24:00 Monday 00:00-24:00 Tu  | uesday 00:00-24:00 Wednesday 00:00-24:0   | 10 Thursday 00:00-24:00   |  |  |
|  | Settings - Then the following settings are applied:  |   |   |  |  |
|  | Setting         Value           Access Permission         Derry Access           Authentication Method         MS-CHAP v1 OR MS-CHAP v1 (User can char<br>Framed-Protocol           PPP         Service-Type           Framed         Framed | nge password after it has expired) OR MS C  | CHAP v2 OR MS-CHAP  |  |  |
|  |  |   |   |  |  |

The NPS configuration is done. I should be able now to log in on a Session Host through my RD Gateway and NPS over RADIUS protocol.

## 4.4. Login Test with MFA Push Login

I start the default RDP client tool from Microsoft. In the advanced configuration, I configure my RD Gateway server address.



I will now try to log in remotely on my AD server, so I configured my AD server address:

|             |                |  |                             | YO_ADFS                           | Pour relâcher votre souris, appuyez sur : Control- |
|-------------|----------------|--|-----------------------------|-----------------------------------|--|
| 11 6        | Э,             | ↔ 🖸                                      |                             | 李 圖 4                             | 0  |
|             |                |  |                             |                                   |  |
| Recycle Bin | chare-yo adfo  |  |                             |                                   |  |
| Recycle bin | share-yo_aurs  | 10 10 10 10 10 10 10 10 10 10 10 10 10 1 | Rem                         | ote Desktop Connection            |  |
|             | _              |  | Remot                       | e Desktop                         |  |
|             | <b>2</b>       | 3  | 🐼 Conn                      | ection                            |  |
|             | ibrahim (max)  |  |                             |                                   |  |
|             |                | Gener                                    | al Display Local            | Resources Programs Experier       | nce Advanced                                       |
| 6           | 1              | Logo                                     | n settings<br>Enter the nar | ne of the remote computer.        |  |
| Google      | OpenOTP_C      |  | Computer:                   | YO_AD-DC vorcievs.com             |  |
| Chrome      |                |  | Liner name:                 |                                   | frateur.   |
|             |                |  | User name.                  |                                   | ualeur   |
|             |                |  | You will be a               | sked for credentials when you cor | inect.   |
|             |                |  | Allow me                    | to save credentials               |  |
|             |                | Conr                                     | ection settings             |                                   |  |
| <b>R</b>    |                |  | Save the cur                | rent connection settings to an RD | P file or open a                                   |
| TeamViewer  | OpenOTP_C      |  | Saved Conne                 | Save As.                          | Open   |
|             |                |  |                             |                                   | - Com an 2012 D2                                   |
| 4           | 6              |  |                             |                                   | Act vate Windows                                   |
| Wireshark   | libopenotp.dll | 🛞 на                                     | le Options                  | Connec                            | Help Ge o System in Control Panel                  |
|             |                |  |                             |                                   | wondows/Server 2012 R2 Standard                    |
|             |                | 1000                                     |                             |                                   | Build 9600   |
|             | <b>a</b> 2     |  | 9                           | ø 👃                               | ► 😼 🖓 🕼 FRA 11/01/2019                             |
|             |                |  |                             |                                   |  |
|             |                |  |                             |                                   |  |

In the meantime, I've started my Radius Bridge component in debug mode with the following command to see in live the radius request sent by NPS:

#### /opt/radiusd/bin/radiusd debug

Listening on auth address \* port 1812 bound to server default Listening on auth proto tcp address \* port 1812 bound to server default Listening on auth address \* port 1645 bound to server default Listening on acct address \* port 1813 bound to server default Listening on acct address \* port 1646 bound to server default Listening on status address \* port 18120 bound to server default Listening on command file /opt/radiusd/temp/radiusd.sock Ready to process requests

I perform the login now through my RDP client. I'm prompted to enter my Credentials:



I press OK after providing my credentials, and then I see the RADIUS request coming on my Radius Bridge debug console:

| (0) Received Access-Request Id 24 fror | n 192.168.3.119:60706 to | 192.168.3.54:1812 length 143 |
|--|--------------------------|------------------------------|
|--|--------------------------|------------------------------|

- (0) Service-Type = Voice
- (0) User-Name = "NETBIOSYORCDEVS\\administrateur"
- (0) Called-Station-Id = "UserAuthType:PW"
- (0) MS-Machine-Name = "YO\_SQL2.yorcdevs.com"
- (0) MS-Network-Access-Server-Type = Terminal-Server-Gateway
- (0) NAS-Port-Type = Virtual
- (0) Proxy-State = 0xfe800000000000000c9e592a48d7b3d5c0000001b
- (0) # Executing section authorize from file /opt/radiusd/lib/radiusd.ini
- (0) authorize {
- (0) eap: No EAP-Message, not doing EAP
- (0) [eap] = noop
- (0) pap: WARNING: No "known good" password found for the user. Not setting Auth-Type
- (0) pap: WARNING: Authentication will fail unless a "known good" password is available
- (0) [pap] = noop
- (0) [openotp] = ok
- (0) } # authorize = ok
- (0) Found Auth-Type = OTP
- (0) # Executing group from file /opt/radiusd/lib/radiusd.ini
- (0) Auth-Type OTP {
- rlm\_openotp: Found NPS Terminal-Server-Gateway request (password not requested)
- rlm\_openotp: Sending openotpNormalLogin request
- rlm\_openotp: OpenOTP authentication succeeded
- rlm\_openotp: Reply message: Authentication success
- rlm\_openotp: Sending Access-Accept
- (0) [openotp] = ok
- (0) } # Auth-Type OTP = ok
- (0) Login OK: [NETBIOSYORCDEVS] (from client any port 0)
- (0) Sent Access-Accept Id 24 from 192.168.3.54:1812 to 192.168.3.119:60706 length 0
- (0) Reply-Message := "Authentication success"
- (0) Proxy-State = 0xfe800000000000000029e592a48d7b3d5c0000001b
- (0) Finished request

Waking up in 9.9 seconds.

(0) Cleaning up request packet ID 24 with timestamp +9

Ready to process requests

I now received the push login request on my phone:



I approve the login request, and I am logged on my remote server:



# 5. Another scenario

# Another scenario is also possible which consist on protect each session hosts with the OpenOTP Credential Provider for Windows login. The 2FA login will be performed by each session hosts instead of a centralized component.

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