

Using RD Gateway with Azure Multifactor Authentication

We have a client that uses RD Gateway to allow users to access their RDS deployment from outside their corporate network. They have about 1000+ users. Their users access the RDS environment from mostly unmanaged devices including many different flavors of tablets. The client was worried about these unmanaged devices being stolen or lost and potentially providing an intruder with access to their RDS environment.

In researching solutions to this problem (and given the breadth of the types of unmanaged clients they wanted to support) we looked at using multifactor authentication together with RD Gateway to create an authentication sequence that would require two forms of identification in order to gain access to the RDS environment:

1. Something only the user knows - his username/password combo
2. A one-time password

If some of you are not very familiar with the growing need for two factor authentication, read [“The increasing need for two factor authentication”](#), by Orin Thomas, contributing editor for [Windows IT Pro](#) and a Windows Security MVP.

We explored some different multifactor authentication offerings and homed in on Microsoft Azure Multifactor Authentication (Azure MFA) for three reasons. First, the price point is excellent compared to some other competing solutions. Second, Azure MFA can complete the second layer of authentication via cell phone or smart device (a device that most people already have) instead of requiring a hard token. Third, Azure MFA can also be set to require a unique PIN that only the user knows. No matter what device is used to access the RDS deployment, the user will need more than his user credentials (which are often cached) to get in.

A Remote Desktop login request to RD Gateway that includes Azure MFA looks like this:

1. User logs into RD Web Access and double clicks a RemoteApp (or desktop connection)
2. The user's login credentials for the website are used to validate the user (Web SSO), so no need to give them again.
3. The user then gets an SMS text message on their smart device that provides them a 6 digit numeric code (the one-time password).
4. The user replies to the text message by inputting this 6 digit code and adding their unique pre-defined PIN to the end of the sequence – Azure MFA includes the option to require the user know a predefined unique PIN as well, so that replies to a text message have to come from the user.
5. The user is authenticated, and the RemoteApp (or desktop connection) opens.

Note: SMS txt authentication isn't the only way that Azure MFA can communicate with users. In a separate upcoming article we'll cover the various authentication options Azure MFA provides

which will include for example authentication by phone call and also using an App on a smartphone.

Because the RD Gateway / Azure MFA solution met the customer's requirements on paper, we decided to run a test pilot. First, we implemented Azure MFA with an RDS environment that only had one RD Gateway server (it was not highly available). Then we implemented with multiple RD Gateway servers in a high availability configuration. The setups both worked well, but the setup was different for these scenarios. In this article we will walk through setting up Azure MFA with one RD Gateway. In our next article we will explore highly available configurations.

How Azure MFA Works With RD Gateway

Let's look closer at how MFA works with RD Gateway to provide two factor authentication. First, in order to understand the setup steps you will go through, you need to know how RD Gateway works to authenticate users.

RD Gateway and NPS

RD Gateway uses NPS (Network Policy Services), a Windows Server 2012 in-box feature, to maintain Network Policies (in the RD Gateway Manager interface these policies are called RD Connection Access Policies, or RD CAPs). In general, RD Gateway (and NPS) work together to authenticate a user like this:

1. The user login credentials gets sent to RD Gateway.
2. NPS checks the credentials against its Network Policies to see if the user is allowed to access RD Gateway. (This is the RD CAP check in RD Gateway speak).

If the credentials are allowed by NPS, then

3. RD Gateway checks the user credentials against its Resource Authorization Policies (RD RAPs are housed in an XML file on the RD Gateway server) to see if the user is allowed to access the requested endpoint and allows or denies the connection.

Adding Azure MFA

When you add in Azure MFA, then a user gets authenticated like this:

1. The user login credentials gets sent to RD Gateway.
2. NPS checks the credentials against its Network Policies to see if the user is allowed to access RD Gateway. (This is the RD CAP check in RD Gateway speak).

If the credentials are allowed by NPS, then:

3. The login request is sent to MFA Server
4. MFA Server communicates with the end user (by SMS text, phone call, mobile app or OATH token) asking them to reply by repeating the sent letter/number sequence back, and adding their unique PIN to the end if MFA is setup to require a personal PIN.
5. MFA receives the user's reply, checks the response. If the response is correct, then MFA sends an "accept" response to RD Gateway.

If RD Gateway gets an Accept response from MFA, then:

6. RD Gateway checks the user credentials against its RD RAPs to see if the user is allowed to access the requested endpoint and allows or denies the connection.

Injecting Azure MFA into the Authentication Sequence

When you have one RD Gateway server running with a locally running NPS service (the default configuration), you have to have some way to get the MFA server into the communication sequence. As shown in Figure 1, you do this by tricking RD Gateway - you configure RD Gateway to use a centralized NPS server but you point it to the MFA server. The communication works like this:

1. RDG gets the initial user login request
2. RD Gateway forwards the RADIUS request through NPS to MFA server.
3. MFA server forwards if right back to NPS on the RD Gateway server
4. RD Gateway validates the user credentials and does the RD CAP check.
5. NPS then sends an ACCEPT or REJECT to MFA server.
6. On ACCEPT, MFA will perform the two factor authentication sequence with the user (via phone call, text or mobile app). If the user returns the correct letter / number sequence, it sends an ACCEPT to RD Gateway.
7. Finally RD Gateway will check the RD RAP and either allow or deny the connection.

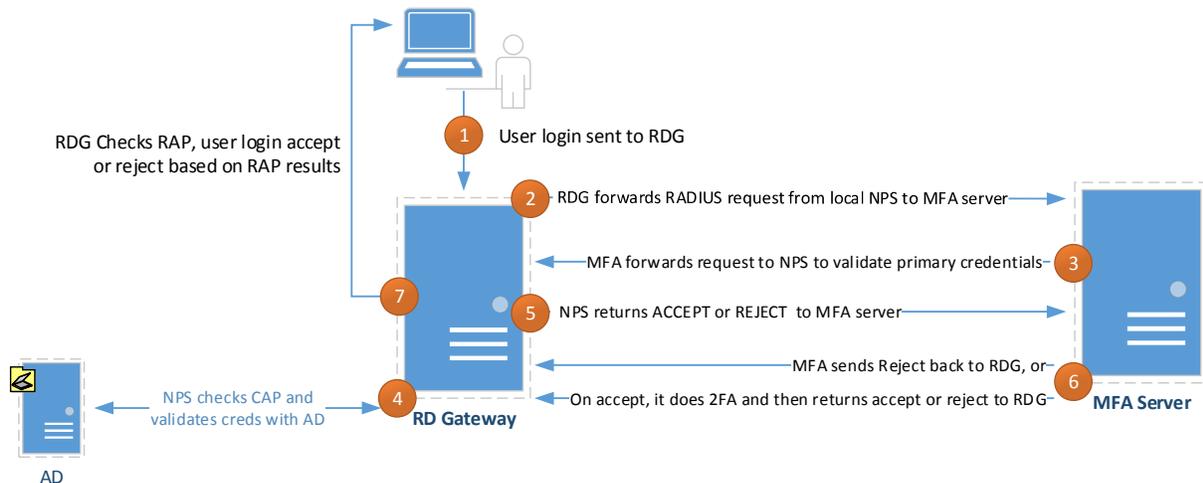


Figure 1: You trick RD Gateway into thinking it is using a centralized NPS.

Implementing an On Premise Azure MFA Server with RD Gateway

Azure MFA can be used in cloud driven scenarios, but it can also be used with on premise applications, and that is what we are concentrating on here - we will show you how to set up an on premise Azure MFA server to provide multifactor authentication to an on premise RD Gateway implementation.

First, here are the things you will need to proceed:

- A working RDS environment, including RD Gateway (running NPS locally)
- A working RD Web Access website with published RemoteApps or desktops
- An Azure account configured with billing information. This article assumes you have already set this up. If you have not, then sign Up For Azure here: <https://account.windowsazure.com/SignUp>
- A domain joined server (physical or VM) designated to be the Azure MFA on premise server
- A cell phone to respond to Azure MFA SMs text requests
- A client test device (a PC or tablet for example) preferably with Internet Explorer

Now we will walk through these main setup steps:

1. Install pre-requisites on the designated Azure MFA server
2. Create a Multifactor Authentication Provider in Azure
3. Download and install the on premise MFA server software
4. Configure MFA Server, RD Gateway and NPS
5. Setup a Test User in Azure MFA Server and do some testing

Pre-Requisites

The on premise Azure MFA Server (from here on out called “MFA Server”) install requires the .NET Framework 3.5 Features, and it will not auto-install it during the setup so you need to install it first. From Server Manager, select the Add Roles and Features option, select .NET 3.5 Framework Features and click Install (shown in Figure 2).

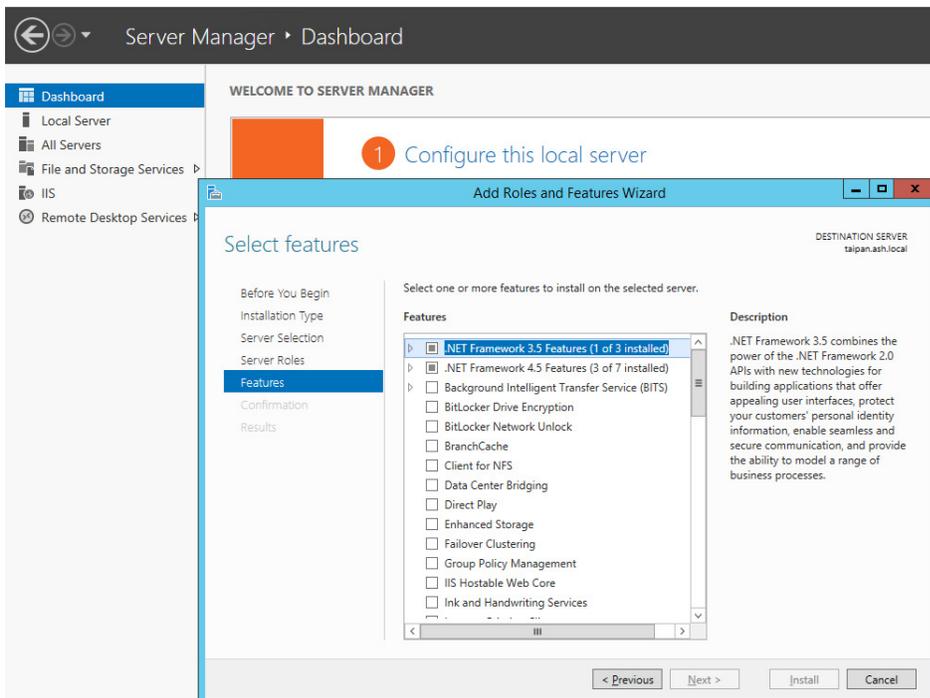


Figure 2: Install the .NET Framework 3.5 Features

Create a Multifactor Authentication Provider in Azure

Next, create a Multifactor Authentication Provider in Azure. Follow these steps:

1. From the MFA server, log into the Microsoft Azure Management Portal: <https://manage.windowsazure.com/>.
2. In the left hand column, scroll to the bottom and click the “+New” button (shown in Figure 3.)

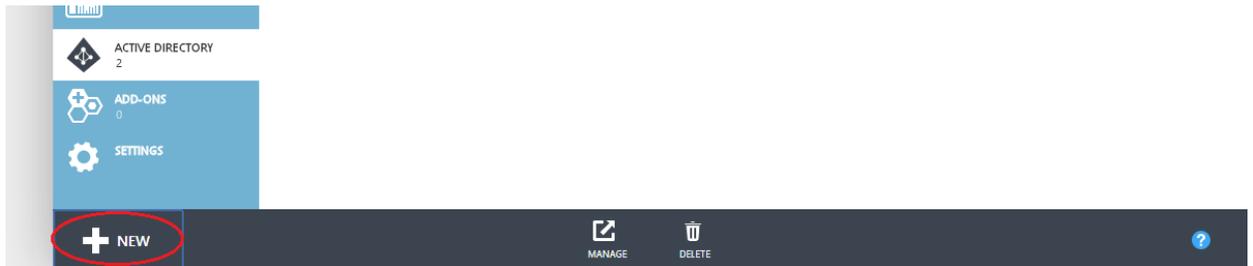


Figure 3: Create a new Multifactor Authentication provider in Azure

3. Figure 4 shows five columns from which you will select properties of the new MFA provider. Select App Services in the first column, select Active Directory in the second column, and select Multifactor Auth Provider in the third column. Then click the Quick Create button. Fill out the form that appears.

For the Usage Model you have two options:

- Per Enabled User means you pay a fixed fee for every user account that is configured to use MFA. Each user gets an unlimited amount of authorizations.
- Per Authentication means you pay a fixed fee per 10 authentications. The amount of users is unlimited.

Both models have possible use cases. You need to figure out which model to go with in advance, as you cannot change the Usage Model once you create the MFA provider.

The Directory options allow you to connect this MFA provider to an Azure Active Directory. Because this implementation will use an on premise MFA Server that will be joined to the on premise domain, leave the option set to “Do not link a directory”.

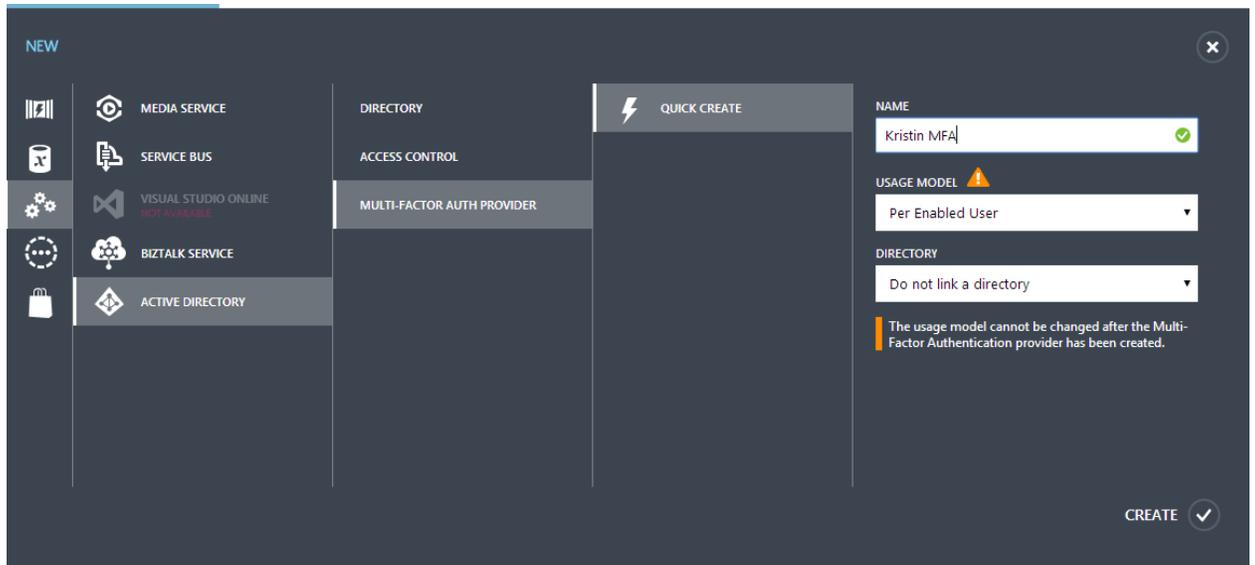


Figure 4: Choose the MFA provider properties from the designated five columns.

4. From the Azure main page you should see your MFA provider created. Select it and then click the “manage” icon at the bottom of the page as shown in Figure 5.

The screenshot displays the Azure portal interface. On the left is a navigation pane with various service categories. The main area shows a table of Multi-Factor Authentication Providers. The table has columns for NAME, STATUS, USAGE MODEL, SUBSCRIPTION, and DIRECTORY. One provider, 'VirtualKristin MFA', is highlighted in blue and circled in red. Below the table, at the bottom of the page, there is a dark bar with a 'NEW' button, a 'MANAGE' button (circled in red), and a 'DELETE' button. The 'MANAGE' button is the target for the next step in the process.

NAME	STATUS	USAGE MODEL	SUBSCRIPTION	DIRECTORY
VirtualKristin MFA	Active	Per Enabled User	Visual Studio Premium with MS...	Default Directory

Figure 5: Select the MFA provider and then click Manage to access the MFA Management portal

Download and Install the On Premise Azure MFA Server Software

The Windows Azure Multifactor Authentication management portal will open in a new browser tab, shown in Figure 6.

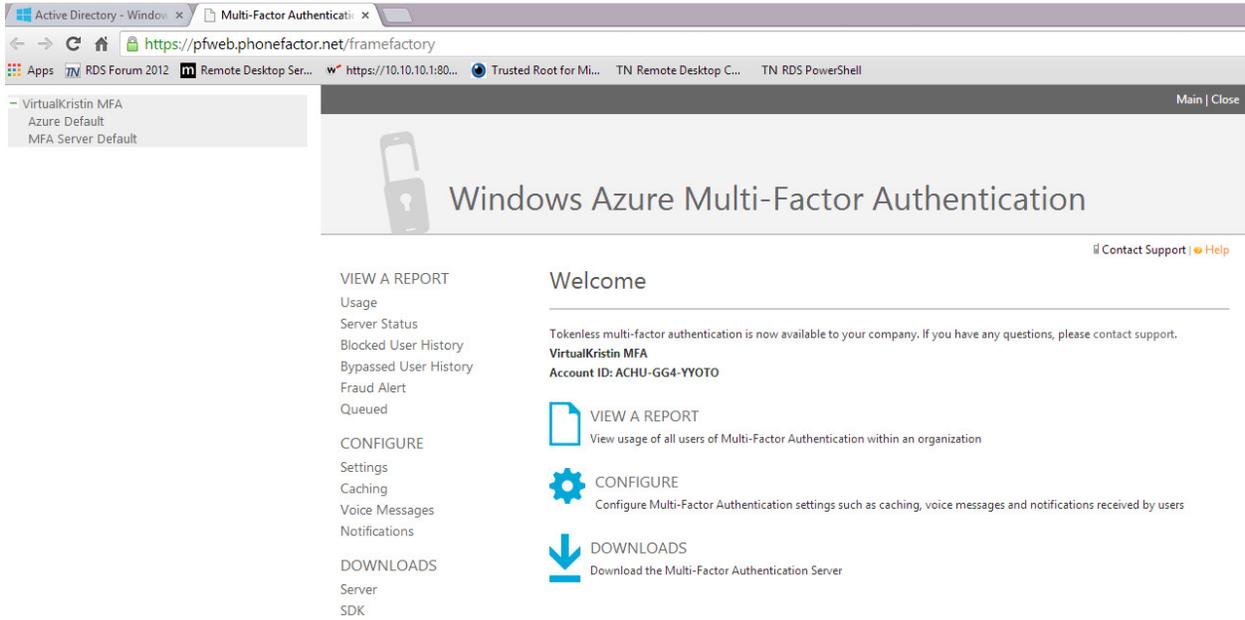


Figure 6: The Windows Azure Multifactor Authentication management portal

Follow these steps to download and install the Azure MFA software.

1. On this tab click the DOWNLOADS button. You will get the screen shown in Figure 7.

Windows Azure Multi-Factor Authentication

VIEW A REPORT
Usage
Server Status
Blocked User History
Bypassed User History
Fraud Alert
Queued

CONFIGURE
Settings
Caching
Voice Messages
Notifications

DOWNLOADS
Server
SDK

Downloads Server

Download a copy of the Multi-Factor Authentication Server. Be sure to install directly on the server to be protected.

MULTI-FACTOR AUTHENTICATION SERVER (version 6.1.1) [Release notes](#)

The Multi-Factor Authentication Server supports the following platforms:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008, SP1, SP2
- Windows Server 2003 R2
- Windows Server 2003, SP1, SP2
- Windows 8.1, all editions
- Windows 8, all editions
- Windows 7, all editions
- Windows Vista, all editions, SP1, SP2
- Windows XP, all editions, SP2, SP3

1 [Download](#)

2 [Generate Activation Credentials](#)

[Back](#)

Do you want to run or save **MultiFactorAuthenticationServerSetup.exe** (114 MB) from **pfweb.phonefactor.net**?

Figure 7: Download the software, then generate activation credentials.

2. Click the small Download link right above the Generate New Activation Credentials button. Save the download file, then run it.
3. Meanwhile go back to the webpage and click the Generate New Activation Credentials button. The activation credentials are only good for 10 minutes. Enter the activation credentials on the Activate screen of the install shown in Figure 8. If your credentials expire before you enter them, click the Generate New Activation Credentials button again to get a new set.

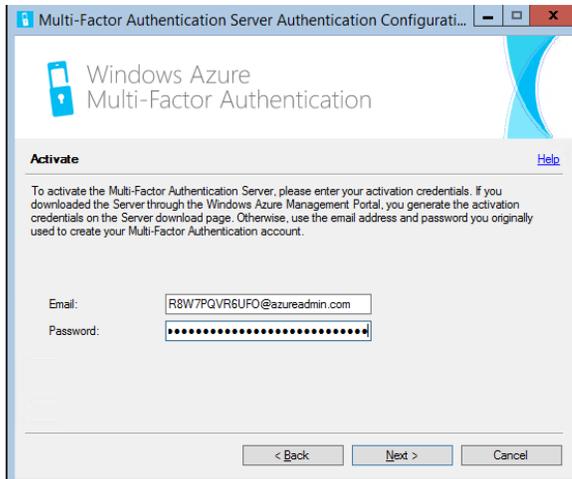


Figure 8: Specify the activation credentials during the MFA setup

TIP: During the activation process the Phone Factor online service is contacted (Microsoft bought Phone Factor, and made Azure Multifactor Authentication so you may see Phone Factor in documents or some GUI screens still). For this to work you need to be able to make connection to the outside on port 443. In scenarios where your server running MFA is using a Proxy Server, run the following command to make use the MFA service leverage your proxy server too:

netsh WinHTTP Set Proxy proxy-server="FQDN_of_Proxy_Server:8080"

Otherwise you could run into the following error shown in Figure 9:

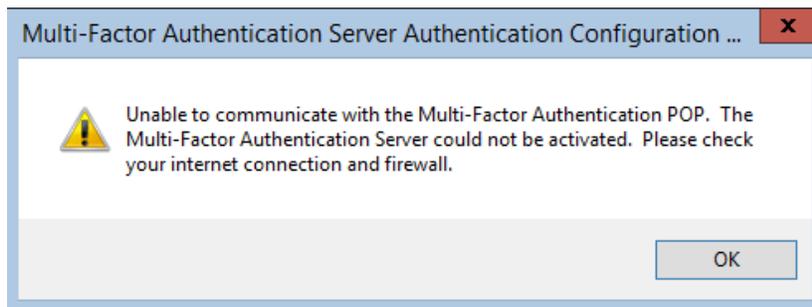


Figure 9: Error indicating the MFA Service could not be reached

Configure RD Gateway Server, NPS and MFA Server

Now you need to configure RD Gateway, NPS, and MFA Server to communicate with each other.

Configure RD Gateway

First, you fake out RD Gateway and configure it to use a Central RD CAP store, but you point it to the new MFA server. Follow these steps:

1. Open RD Gateway Manager, right click the server name, and select Properties.
2. Select the RD CAP Store tab (shown in Figure 10).
3. Select the Central server running NPS option.
4. Enter the name or IP address of the MFA server and click Add.
5. Enter a shared secret in the corresponding popup box and click OK.

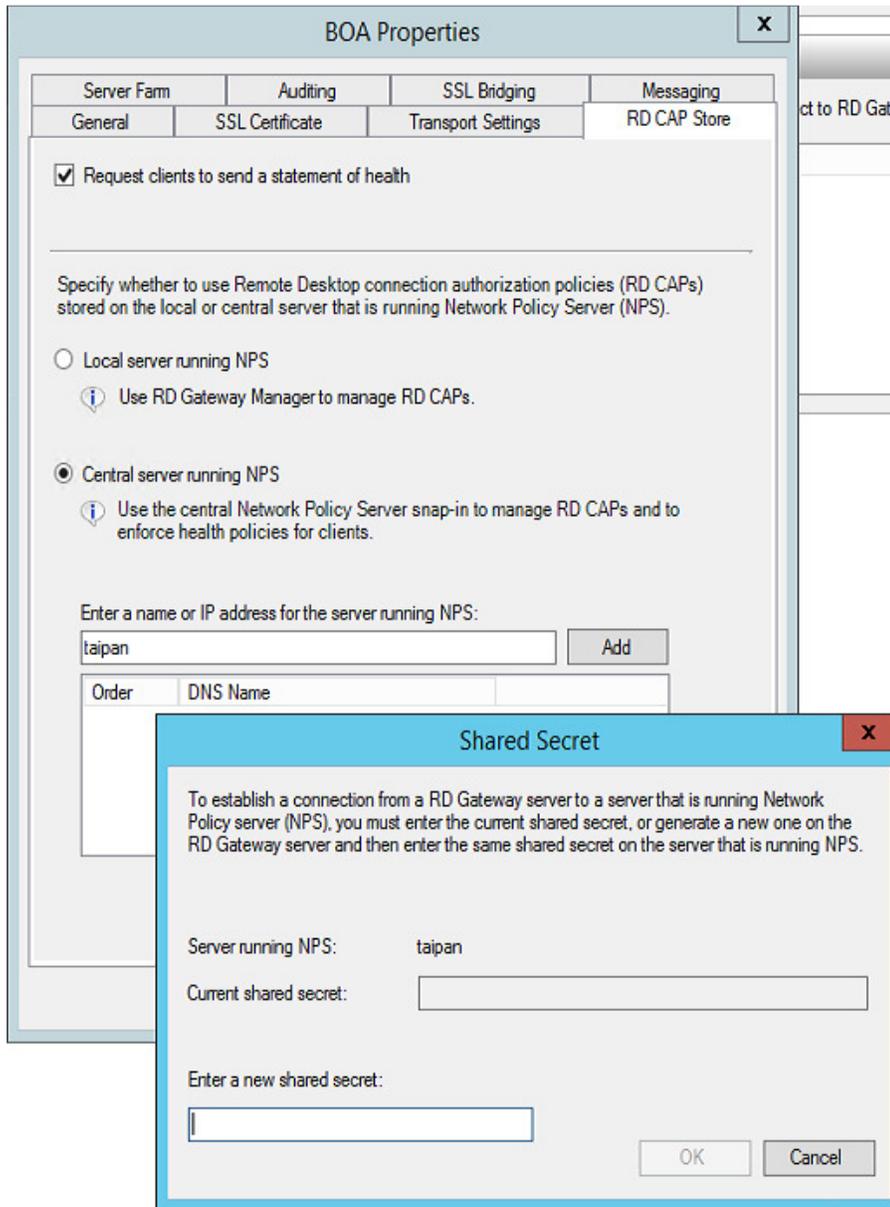


Figure 10: Configuring RD Gateway to use central NPS

Make NPS and MFA Talk To Each Other

Now you need to configure NPS (located on the RD Gateway server) and MFA server to talk to each other. NPS and MFA server both use a RADIUS client and RADIUS server to communicate with each other. So you configure a RADIUS client and a RADIUS server (depicted in Figure 11) on each server like this:

- On the RD Gateway server, in NPS you configure two Connection Request Policies:
 - The first will send communication to MFA Server via a Remote RADIUS Server Group
 - The second will receive communication from MFA server via a RADIUS client
- On the MFA server you configure:
 - A RADIUS client to receive communication from the NPS server
 - A RADIUS Target to send communication to the NPS server

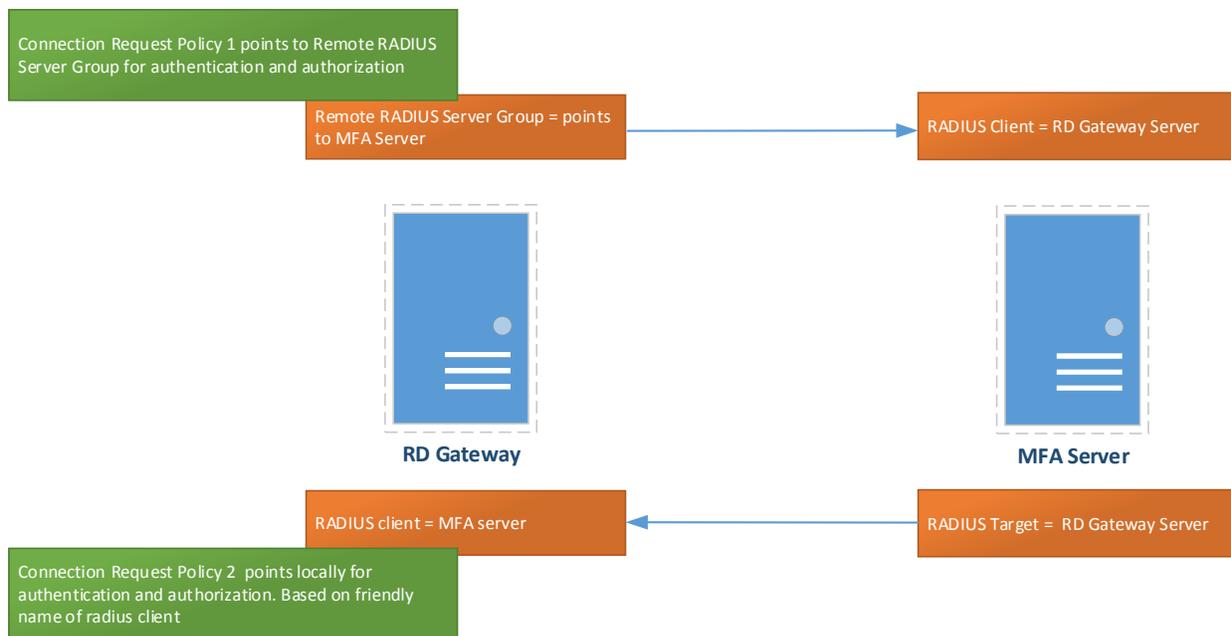


Figure 11: NPS and MFA server use RADIUS servers and clients to communicate with each other.

Configure NPS

First, you need to prevent NPS from timing out before MFA's authentication has completed. Follow these steps (shown in Figure 12):

1. In NPS, expand the RADIUS Clients and Servers menu and select Remote RADIUS Server Groups.
2. When you setup RD Gateway it creates an entry here named "TS GATEWAY SERVER GROUP". Right click this group and select Properties.
3. Select the MFA server listed and select Edit.
4. Select the Load Balancing tab.

5. Change the “Number of seconds without response before request is considered dropped” and the “Number of seconds between requests when server is identified as unavailable” to 30-60 seconds.

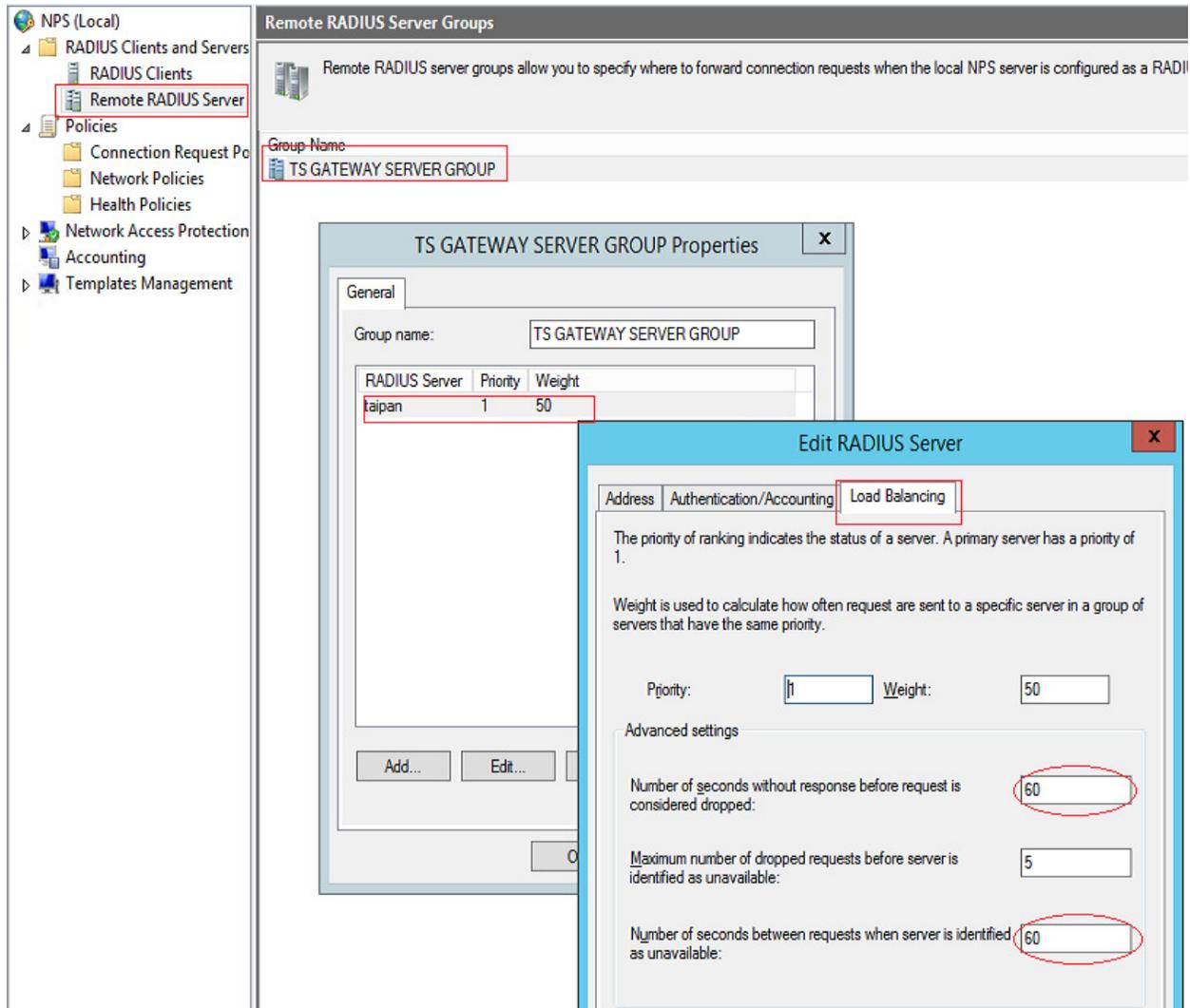


Figure 12: Adjust the RADIUS server settings in NPS.

Next you need to configure NPS to receive RADIUS authentications from MFA server. So you create a RADIUS client. Follow these steps:

1. In the left column, right click RADIUS Clients and choose New.
2. Add a Friendly Name and the address of the MFA server as shown in Figure 13.
3. Add a shared secret and click OK.

The screenshot shows the 'New RADIUS Client' dialog box with the following fields and options:

- Settings** / **Advanced** tabs
- Enable this RADIUS client**
- Select an existing template:** (dropdown menu)
- Name and Address** section:
 - Friendly name:** PUT FRIENDLY NAME HERE
 - Address (IP or DNS):** PUT ADDRESS OF MFA SERVER HERE (with a **Verify...** button)
- Shared Secret** section:
 - Select an existing Shared Secrets template:** None (dropdown menu)
 - Text: 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:** (password field with 8 dots)
 - Confirm shared secret:** (password field with 8 dots)
- OK** and **Cancel** buttons at the bottom.

Figure 13: Create a RADIUS client in NPS.

Next, configure two Connection Request Policies in NPS - one to forward requests to the Remote RADIUS Server Group (which is set to forward to MFA server), and the other to receive requests coming from MFA server (to be handled locally).

The easiest way to do this is to use the existing policy that was created when you created an RD CAP in RD Gateway. Follow these steps:

1. In NPS expand the Policies section in the left side of the screen and then select Connection Request Policies. You should see a policy already created there, called TS GATEWAY AUTHORIZATION POLICY.
2. Right click this policy and select Duplicate Policy.

Note: In order to easily tell what each policy is doing, I rename my policies like this:

- I rename "TS GATEWAY AUTHORIZATION POLICY" to "To MFA"
- I rename "Copy of TS GATEWAY AUTHORIZATION POLICY" to "From MFA"

3. Double click the new duplicate policy and select the Conditions tab.

4. Add a Client Friendly Name as shown in Figure 14. Use the same Friendly name you set for the RADIUS client you created earlier.

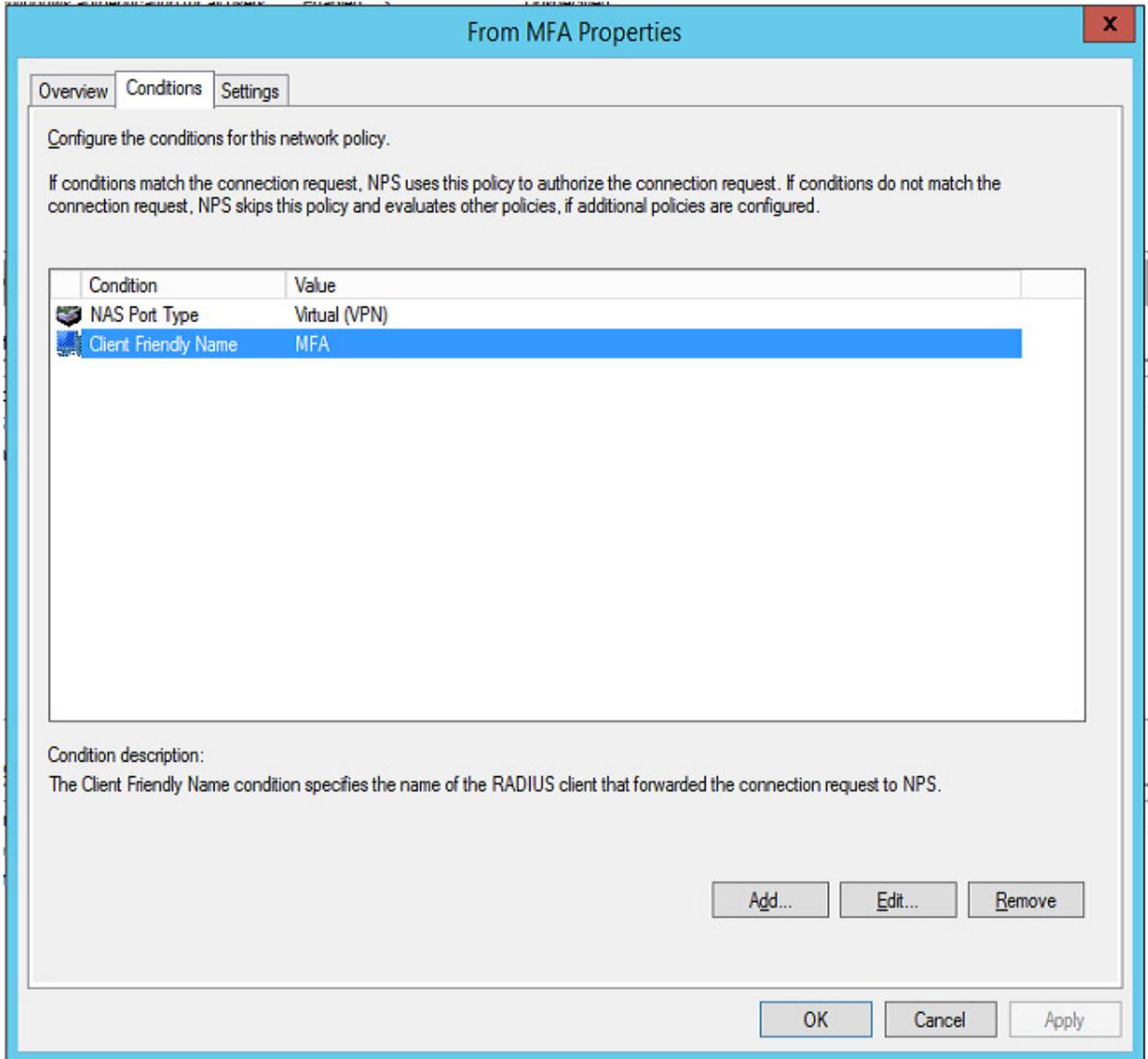


Figure 14: Add a Client Friendly Name to the existing TS GATEWAY AUTHORIZATION POLICY.

- Now select the Settings tab and change the Authentication Provider to “Authenticate requests on this server” as shown in Figure 15.

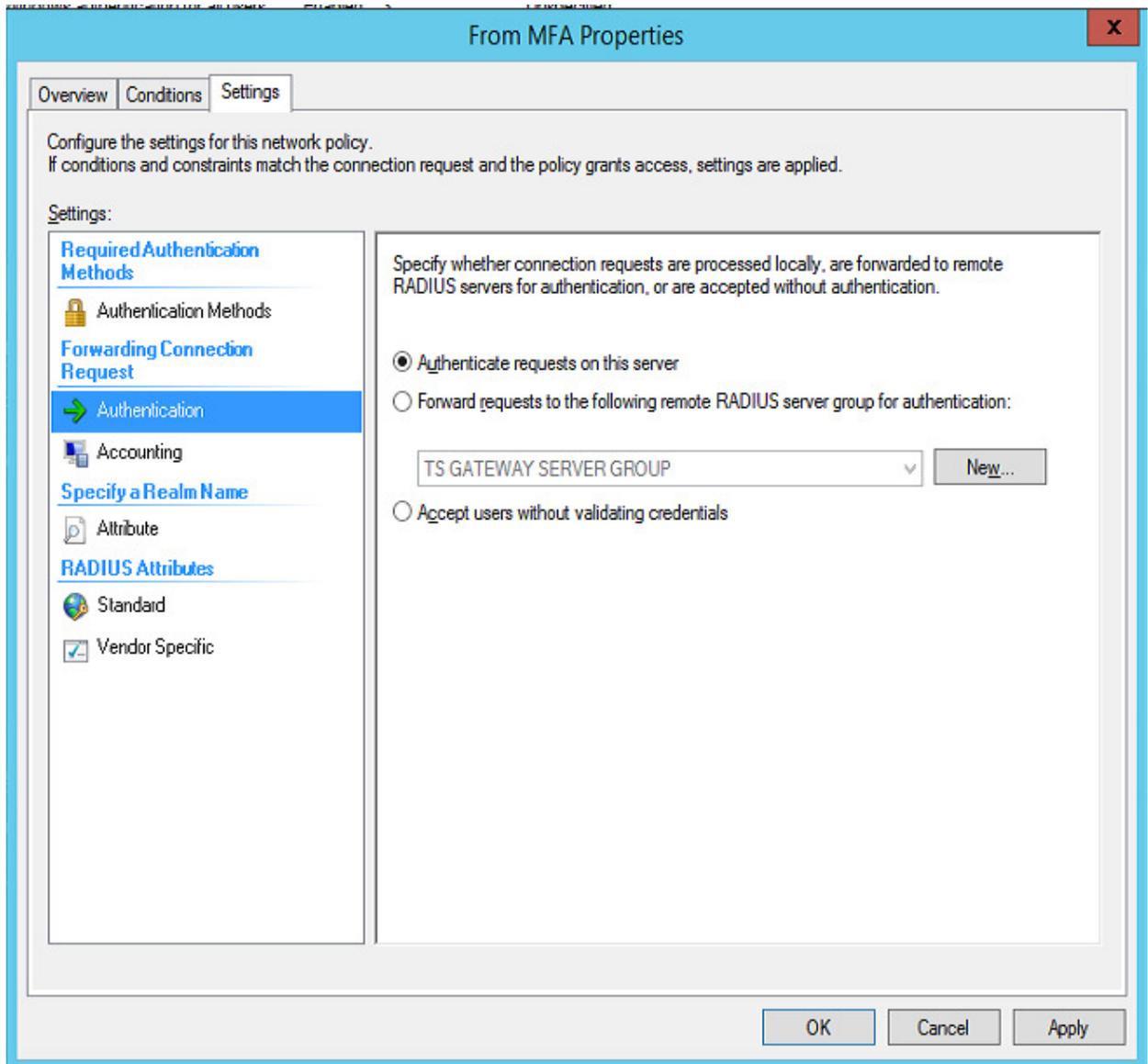


Figure 15: Change the policy to authenticate requests locally.

6. Select Accounting and make sure the “Forward accounting requests...” check box is not checked. Then click OK. When you are done, your policy settings should show up on the main interface as shown in Figure 16.

The screenshot shows the NPS (Local) console with the 'Connection Request Policies' window open. The left pane shows the tree view with 'Connection Request Policies' selected. The main pane displays a table of policies and the configuration for the selected 'From MFA' policy.

Policy Name	Status	Processing Order	Source
From MFA	Enabled	1	Remote Desktop Gateway
To MFA	Enabled	2	Remote Desktop Gateway
Use Windows authentication for all users	Enabled	3	Unspecified

From MFA

Conditions - If the following conditions are met:

Condition	Value
NAS Port Type	Virtual (VPN)
Client Friendly Name	MFA

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Override Authentication	Disabled

Figure 16: Overview of the NPS policy settings of the “From MFA” policy

7. Make sure that this policy (the copy of the original) is ordered first, ahead of the original policy.

- You should not have to make any changes to the original policy but double check to make sure that it contains settings as shown in Figure 17.

Connection Request Policies

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to a remote RADIUS server.

Policy Name	Status	Processing Order	Source
From MFA	Enabled	1	Remote Desktop Gateway
To MFA	Enabled	2	Remote Desktop Gateway
Use Windows authentication for all users	Enabled	3	Unspecified

To MFA

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	TS GATEWAY SERVER GROUP
Authentication Provider Name	TS GATEWAY SERVER GROUP
Authentication Provider	Forwarding Request

Figure 17: Make sure the original policy has the settings outlined here.

Configure MFA Server

Now you need to configure the MFA Server software with a RADIUS target and client. Follow these steps:

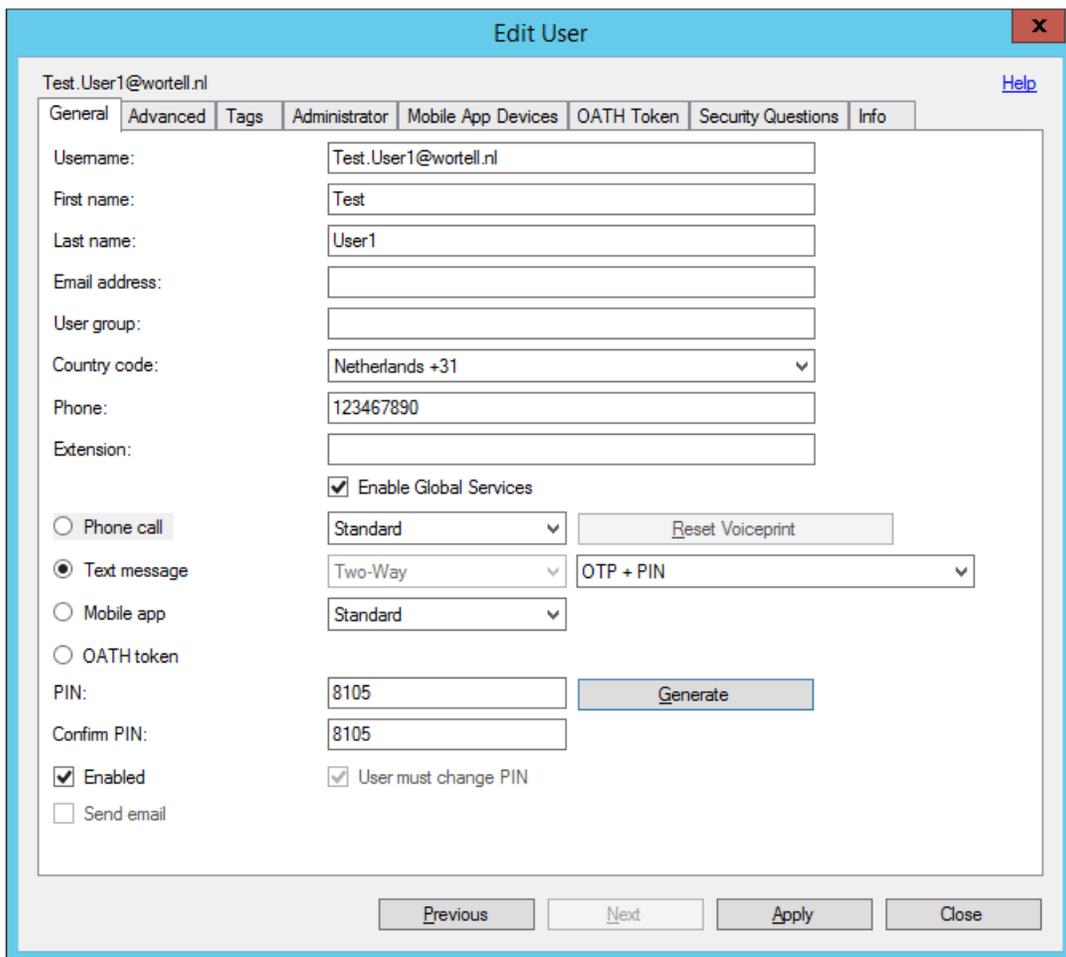
- On the MFA server open the Multifactor Authentication Server and click the RADIUS Authentication icon.
- Check the Enable RADIUS authentication checkbox.
- On the Clients tab, click the Add... button.
- Add the RD Gateway / NPS server IP address, and a shared secret. The shared secret needs to match the one added to the Central CAP Store configuration in RD Gateway Manager.
- Click the Target tab and choose the RADIUS server(s) radio button.

6. Click Add and enter the IP address, shared secret and ports of the NPS server. The shared secret must match the one configured for the RADIUS client of the NPS server.

Testing

To able to test the scenario you need to add a Test User to MFA and configure it with an authentication method. Here's how to do it:

1. On the MFA server open the Multi-Factor Authentication Server and select the Users icon.
2. Click the Import Users from Active Directory button.
3. Drill down in the container hierarchy to the user account you want to test with, select the user account and click Import.
4. Double click the newly created user account (as shown in Figure 18).



The screenshot shows the 'Edit User' window for 'Test.User1@wortell.nl'. The window has a blue title bar and a 'Help' link in the top right. Below the title bar are tabs for 'General', 'Advanced', 'Tags', 'Administrator', 'Mobile App Devices', 'OATH Token', 'Security Questions', and 'Info'. The 'General' tab is active. The form contains the following fields and options:

- Username: Test.User1@wortell.nl
- First name: Test
- Last name: User1
- Email address: (empty)
- User group: (empty)
- Country code: Netherlands +31 (dropdown)
- Phone: 123467890
- Extension: (empty)
- Enable Global Services
- Authentication method: Phone call (Standard), Text message (Two-Way, OTP + PIN), Mobile app (Standard), OATH token
- PIN: 8105 (Generate button)
- Confirm PIN: 8105
- Enabled, User must change PIN
- Send email

At the bottom of the window are buttons for 'Previous', 'Next', 'Apply', and 'Close'.

Figure 18: Configure the test user's settings.

On the General tab:

- Enter the country code and the phone number of the cell phone you will use to test with.
 - Select the Text Message option. Then select OTP + PIN from the corresponding dropdown menu to the right.
 - Enter a PIN or click the Generate button to generate a new pin code.
5. Select the Enabled check box, and click Apply to save the configuration.

To test the scenario perform the following steps:

1. From your test client device open Internet Explorer and browse to the RD Web Access website, and login with a test account.
2. Open a Remote App or Remote Desktop. On the client the dialog shown in Figure 19 will remain open until the two factor authentication has been completed:

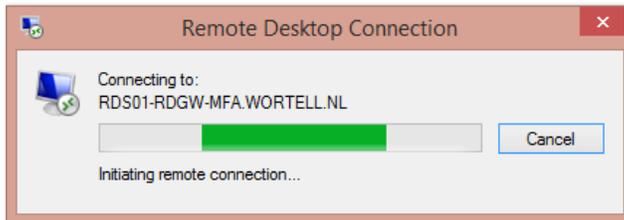


Figure 19: Launch the RDP session

3. You will receive a text message from MFA server as shown in Figure 20.

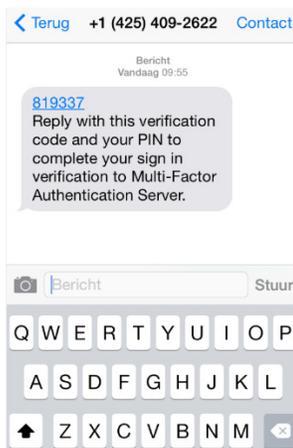


Figure 20: You should receive a text message from MFA server.

4. Reply to the text by typing the One Time Password in the initial text message and add the unique user PIN to the end of your response.

5. If you type in the correct information the multifactor authentication will complete successfully and the session will open.

Troubleshooting

When we were working with this installation, we did not set things up right the first time (or the second). So we had to troubleshoot our pilot. Unfortunately we did not find very much to help us. The event logs were our friend however.

When you make a successful connection (complete with UDP channels through RD Gateway), you will get 16 event log entries in the RD Gateway operational event log. It is located at:

Event Viewer / Applications and Services Logs / Microsoft / Windows / TerminalServices-Gateway / Operational

These 16 entries correspond to the successful connection like this:

1. User met CAP policy requirements and can connect to RD Gateway
2. User met RAP policy requirements and can connect to RD Connection Broker
3. The user connected to RD Connection Broker using HTTP
4. The user connected to RD Connection Broker using UDP
5. The user connected to RD Connection Broker using UDP Proxy
6. The user connected to RD Connection Broker using UDP (second channel)
7. The user connected to RD Connection Broker using UDP Proxy (second channel)
8. The user disconnected to RD Connection Broker using HTTP
9. The user disconnected to RD Connection Broker using UDP
10. The user disconnected to RD Connection Broker using UDP
11. User met RAP policy requirements and can connect to RD Session Host
12. The user connected to RD Session Host using HTTP
13. The user connected to RD Session Host using UDP
14. The user connected to RD Session Host using UDP Proxy
15. The user connected to RD Session Host using UDP (second channel)
16. The user connected to RD Session Host using UDP Proxy (second channel)

What we found was that if you have a problem with misconfigured policies in NPS, you most likely will get an event log error at step one. The event log will say that you did not meet CAP requirements even if you do.

If you run into this, check your policies. If you are sure they are correct, then make sure your CAP works if you use a local NPS (switch the RD Gateway CAP store setting back to Local). If it works when you choose the Local option then we recommend you redo your policies. Remove the policies you have edited or created in NPS. Then redo the Central CAP setting in RD Gateway Manager (put it back to Local, then change it again to Central). Doing this will recreate required starting pieces in NPS, and you can recreate and edit policies from there.

Q&A

Q: Are there other ways to configure the communication in NPS that will work?

A: Yes, there are multiple ways to setup the communication in NPS that will work. For example, we got this working also by:

- Leaving RD Gateway with a local NPS instead of faking it out.
- Adding two RADIUS clients in NPS, one for the RD Gateway server and one for the MFA server.
- Configuring two Connection Request Policies to handle communication from NPS to MFA server (one by friendly name and the other by IP address).
- Configuring two Connection Request Policies to handle communication from MFA server to NPS (one by friendly name and the other by IP address).

But this configuration turned out to be pretty touchy. We were able to repeatedly break this installation and the only repair that would work was to undo the policies in NPS and start over.

We are going to walk through other possible configuration scenarios in our next article when we talk about RD Gateway and Azure MFA high availability scenarios.

Q: Why do I need to change the timeouts for the Remote RADIUS Server Group in NPS from 5 seconds to 30-60 seconds?

A: Because it takes time to perform primary authentication with RD Gateway and then to perform two factor authentication before returning a response to RDG, the RADIUS timeouts in NPS need to be increased to 60 seconds.

Q: How does Azure know to bill me when I deploy Azure MFA on premise?

A: You get billed through the Multi-Factor Auth Provider created in Azure. The MFA Server reports the number of enabled users to the MFA cloud service, which reports billing to the Azure commerce systems.

Q: What piece of Azure MFA takes care of sending the text messages to cell phones?

A: All second-factor authentications are performed through the MFA cloud service. That service performs the phone calls, text messages and push notifications (mobile app). When using the on premise MFA Server, the server requests the authentication from the cloud service.

Q: When I get a TXT message from Azure MFA with my OTP, it comes from what seems to be random phone numbers. How are users supposed to know that this is legit? Is there a way to identify this other than the friendly name in the MFA setup?

A: Azure uses multiple SMS providers today, each with a pool of numbers that the SMS messages are sent from. Microsoft is bringing an SMS short code into production very shortly and then most of the SMS traffic in the US will be sent from that short code so there will be some consistency in place soon. You can also customize the SMS message that is sent by going into Company Settings → SMS Text.

Q: How does an on premise Azure MFA server communicate with Azure MFA cloud services?

A: The MFA Server communicates to the MFA cloud service over port 443 outbound. Figure 21 shows a high-level architecture that shows the MFA Server on-premises, Azure AD and the MFA cloud service.

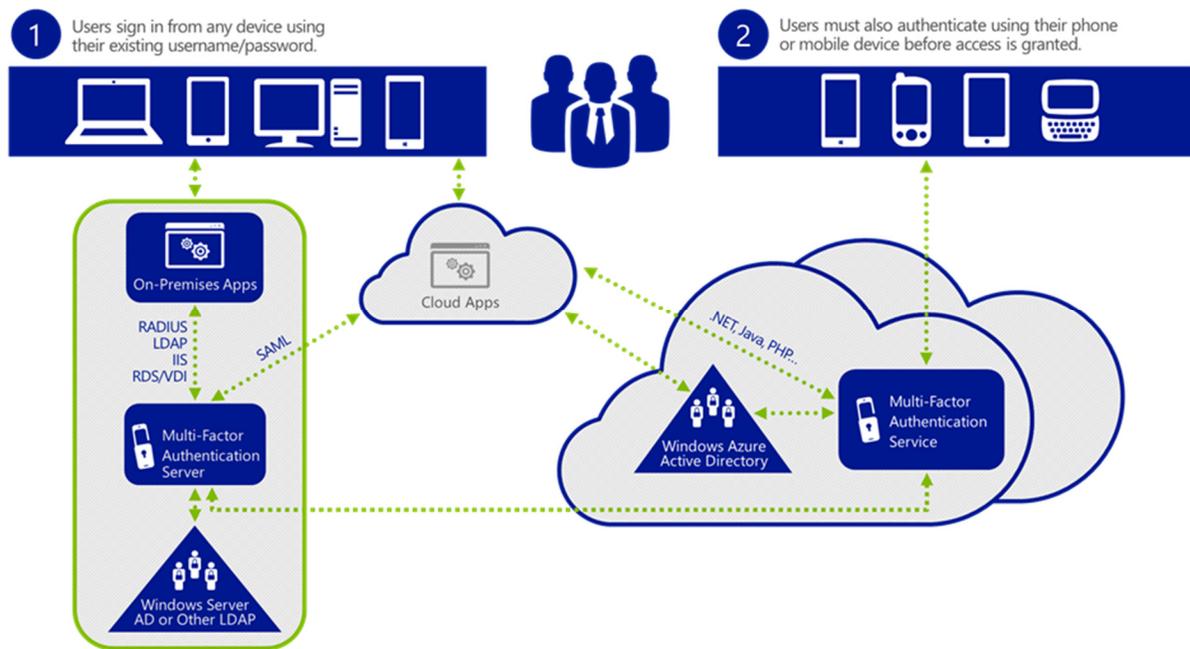


Figure 21: MFA High Level architecture

Other Helpful Articles

- [Getting started with Windows Azure Multi-Factor Authentication](#)
- [RADIUS Authentication](#)
- [Remote Desktop Gateway and Azure Multi-Factor Authentication Server using RADIUS](#)

Summary

This setup is a simple one – a single RD Gateway and single on premise Azure MFA server – great for testing a concept, but what about a more real world solution? In upcoming articles we will show you how to configure a highly available solution including multiple RD Gateways, multiple MFA Servers. We will also explore various Azure MFA authentication methods such as phone call, and mobile app options. Check RDSGurus.com for updates!