

## Contents

Install high level steps I took.....	2
AD.....	2
Check Point .....	2
Client PC.....	3
Assumptions.....	3
Azure AD Connect .....	5
Why use Azure AD Connect? .....	5
Network Policy Server extension for Azure .....	6
Azure AD .....	7
Self Service password resets .....	7
User MFA settings .....	7
Setup users account (Self enroll) .....	8
<b>Testing with NTRADPING .....</b>	<b>9</b>
<b>Setting up a Check Point 750 SMB .....</b>	<b>9</b>
<b>** NOTE **</b> .....	<b>10</b>
<b>Testing with SecureClient.....</b>	<b>10</b>

## **Scenario**

Customer would like to do 2FA for their remote access VPN solution on SMB and Enterprise gateway, they are a Microsoft shop with On-Prem AD and AzureAD.

Customer would like to have the option for SMS, email or SmartPhone App to perform the 2FA, they however do NOT want to use hardware tokens.

## **Hardware / Software used**

1 x 750 (R77\_85)

1 x 3200 (R80.40)

1 x Windows 2019 AD and NPS

1 x Windows 10 PC

## Install high level steps I took

### AD

1. Create new public DNS domain
2. Added domain as a "Custom domain name" in AzureAD
3. Created 2019 AD domain on prem
4. Installed NPS onto AD server
5. \*\* STOP AND TEST RADIUS \*\*
6. Installed Azure AD Connect and began AD sync to cloud
7. Installed "Network Policy Server extension for Azure" on top of NPS

### Check Point

1. Factory wipe of a SMB 750
2. Installed latest firmware
3. Enabled VPN blade
4. Setup radius connection

## Client PC

1. Install Windows 10
2. Download and install Check Point VPN client (SecureClient)
3. Create VPN site
4. Test connection

## **Steps**

### Assumptions -

1. You have an active Azure sub with a p2 subscription, this is required for AzureAD 2fa
2. Active Directory is installed and working
3. Windows 10 Host is installed and working
4. You have all applicable licenses for Check Point and Microsoft
5. You created a "Custom Domain" under AzureAD that matches your onprem domain, to ensure syncin of hash's the UPN's for AzureAD and On-Prem AD must be the same.

We will pick this up after step #3, so AD is installed and working. Nothing special was done to get AD working, it is a standard 2019 deployment with DNS, NPS and AD installed. This was a new deployment so during the DCPROMO command a new forest was created.

1. On the AD server, open the NPS manager
2. Under Radius Clients and Servers, right click "Radius Clients" and select New, from here you can fill in the information for the host that will be sending the radius request.
3. Under the root of the window click "NPS (Local)" and select "Configure VPN or Dial-Up"
4. Select the 2<sup>nd</sup> option, VPN and click next
5. Add any additional radius clients and click next

6. Under groups you can either choose a specific AD group or use "Domain Users" for all users in AD
7. Under "Connection Request Policies" you can edit the newly created policy by double clicking it
8. Change "Type of network access server" from "Remote Access Server(VPN-Dial up)" to "Unspecified"
9. Under "Conditions", delete "NAS Port Type" and add a new condition e.g. "Day and time restrictions"
10. Everything else can be left as default
11. Now under "Network Policies" edit the newly created policy
12. Again, change "Type of network access server" from "Remote Access Server(VPN-Dial up)" to "Unspecified"
13. Under condition, delete "NAs Port Type" and add a new condition e.g. "User Groups"
14. Under Constraints, edit the authentication methods and match to supported types. For testing I just enabled everything. DO NOT do this in production, as PAP / SPAP are not encrypted.
15. All other settings can be left as default

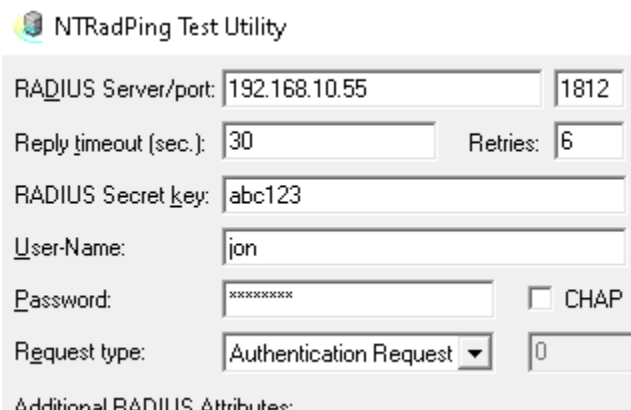
**STOP HERE – Download NTRADPING FROM HERE -**

<https://www.novell.com/coolsolutions/tools/downloads/ntradping.zip>

This is an oldschool app, but great for doing basic testing of a radius server

Once you have the app, configure it (very simple)

Radius server = there NPS is installed



NTRadPing Test Utility

RADIUS Server/port: 192.168.10.55 1812

Reply timeout (sec.): 30 Retries: 6

RADIUS Secret key: abc123

User-Name: jon

Password: xxxxxxx ☐ CHAP

Request type: Authentication Request 0

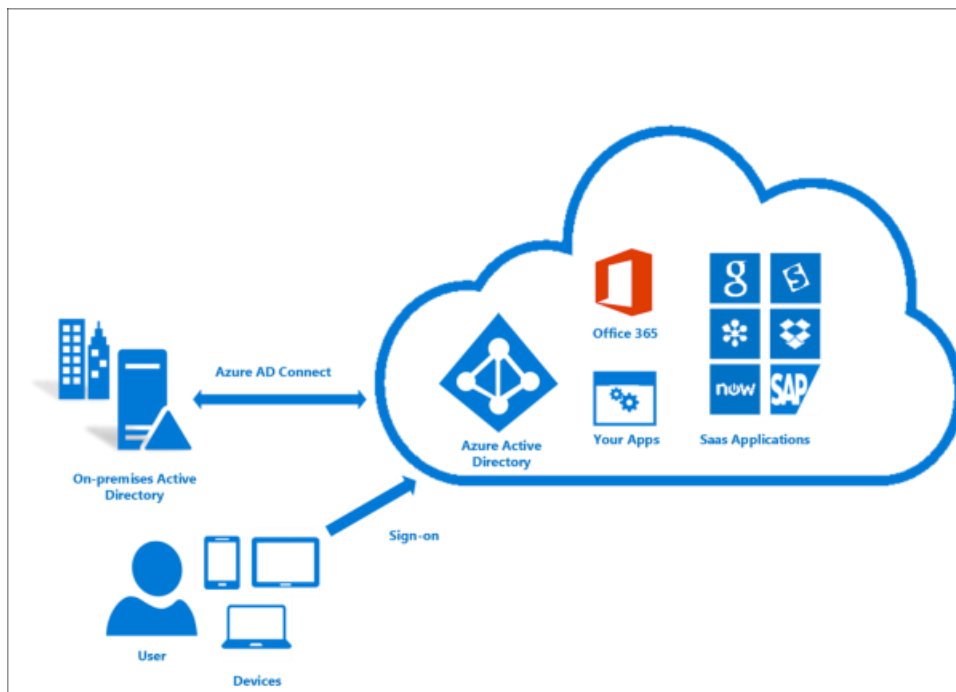
Additional RADIUS Attributes:

and hit SEND, if everything works you will see a response from the radius server that says....

response: Access-Accept

At this point, the users will authenticate to AD using a static password.

## Azure AD Connect



### Why use Azure AD Connect?

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. Users and organizations can take advantage of:

- Users can use a single identity to access on-premises applications and cloud services such as Office 365.
- Single tool to provide an easy deployment experience for synchronization and sign-in.
- Provides the newest capabilities for your scenarios. Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync. For more information, see [Hybrid Identity directory integration tools comparison](#).

1. Login to the Azure portal, and click on Azure Active Directory on the left.
2. Scroll down to "Properties" and click it
3. Copy the "Directory ID" to a notepad for later use
4. Click on Users
5. Click on "New User"
6. Create a new user under the "custom domain" and assign it "Global Administrator" roles
7. Login to your local AD server
8. Download the MSI from - <https://www.microsoft.com/en-us/download/details.aspx?id=47594>
9. Once downloaded, install it
10. During the install process it will ask for your AzureAD admin account and your On-Prem Admin account.
11. If everything is good, the process will end with ADConnect syncing your on-prem AD to Azure

## Network Policy Server extension for Azure

The Network Policy Server (NPS) extension for Azure MFA adds cloud-based MFA capabilities to your authentication infrastructure using your existing servers. With the NPS extension, you can add phone call, text message, or phone app verification to your existing authentication flow without having to install, configure, and maintain new servers.

This extension was created for organizations that want to protect VPN connections without deploying the Azure MFA Server. The NPS extension acts as an adapter between RADIUS and cloud-based Azure MFA to provide a second factor of authentication for federated or synced users.

8. **NAS/VPN Server** receives requests from VPN clients and converts them into RADIUS requests to NPS servers.
9. **NPS Server** connects to Active Directory to perform the primary authentication for the RADIUS requests and, upon success, passes the request to any installed extensions.
10. **NPS Extension** triggers a request to Azure MFA for the secondary authentication. Once the extension receives the response, and if the MFA challenge succeeds, it completes the authentication request by providing the NPS server with security tokens that include an MFA claim, issued by Azure STS.
11. **Azure MFA** communicates with Azure Active Directory to retrieve the user's details and performs the secondary authentication using a verification method configured to the user.

1. Login to the AD Server
2. Download the MSI from - <https://aka.ms/npsmfa>
3. Install
4. Run Windows PowerShell as an administrator.
5. Change directories.
6. `cd "C:\Program Files\Microsoft\AzureMfa\Config"`
7. Run the PowerShell script created by the installer.
8. `.\AzureMfaNpsExtNConfigSetup.ps1`
9. Sign in to Azure AD as an administrator.
10. PowerShell prompts for your tenant ID. Use the Directory ID GUID that you copied from the Azure portal in the prerequisites section.
11. PowerShell shows a success message when the script is finished.
12. Reboot the Server

At this point every RADIUS request sent to the NPS server will be sent to AzureAD for MFA

## Azure AD

There are a few items that should be enabled within AzureAD to ensure self enrollement to MFA

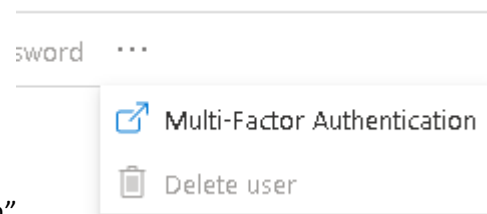
### Self Service password resets

1. Login to Azure portal
2. Click on "Azure Active Directory"
3. Click on "Password reset"
4. Change settings to "All" if no groups are defined or needed.

### User MFA settings

1. Click on Users
2. "All Users"

3. Then along the top click "Multi-Factor Authentication"
4. Tick the users that you want to enable MFA for



5. Then click enable

At this point 2fa will be enabled but not working as Azure does not know the phone numberr or email of the user

## Setup users account (Self enroll)

1. Open a new browser window, ideally in private mode
2. Goto - <https://myprofile.microsoft.com/>
3. Login as the user



### More information required

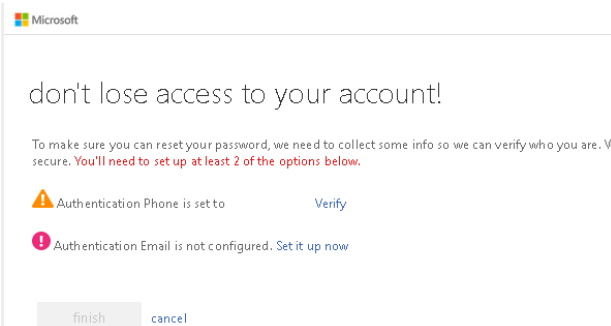
Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)

4. First login will show this -
5. Then you will need to fill in a phone number and/or an email, this will be where the 2fa PIN will



be sent -



## Testing with NTRADPING

So now that everything should be working we can test the MFA sms function.

1. Start up NTRADPING, it should saved your config from earlier testing
2. Click SEND
3. If everything works the server reply should look now this -

RADIUS Server reply:

```
Sending authentication request to server 192.168.10.55:1812
Transmitting packet, code=1 id=1 length=43
received response from the server in 1907 milliseconds
reply packet code=11 id=1 length=98
response: Access-Challenge
----- attribute dump -----
Reply-Message=Enter Your Microsoft verification code
State=230d1ee0-ccf8-4b9d-a0d8-e6b1eea36158
```

4. As you should see, the “Reply-Message” should say “Enter your microsoft verification code”
5. Within a few seconds you should also get an SMS with your OTP

## Setting up a Check Point 750 SMB

The VPN setup of a 750 (or any embedded device) is the same process

1. Login via webui
2. Click on VPN
3. Click on Remote Access – Blade Control
4. Turn on remote access
5. In the bottom section, turn on “Check Point VPN Clients”
6. On the left select “Authentication Servers”
7. Configure a new radius server using the shared key setup in the early steps

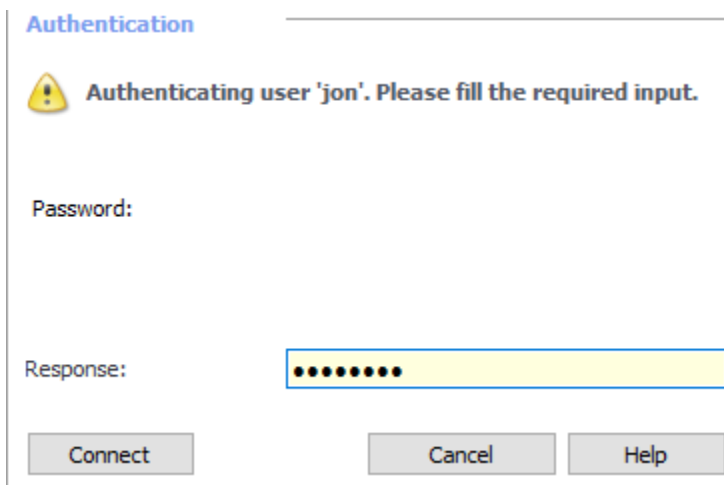
**\*\* NOTE \*\***

DO NOT CONFIGURE RADIUS AND AD AUTHENTICATION, IF YOU DO AD WILL ALWAYS AUTH FIRST AND THIS FLOW CAN NOT BE CHANGED BY DESIGN.


**Testing with SecureClient**

Finally we will test with the actual VPN client

1. Create a VPN site in your client
2. Set the authentication type as “Challenge Response”
3. Connect to vpn when asked
4. Enter you AD username and click connect



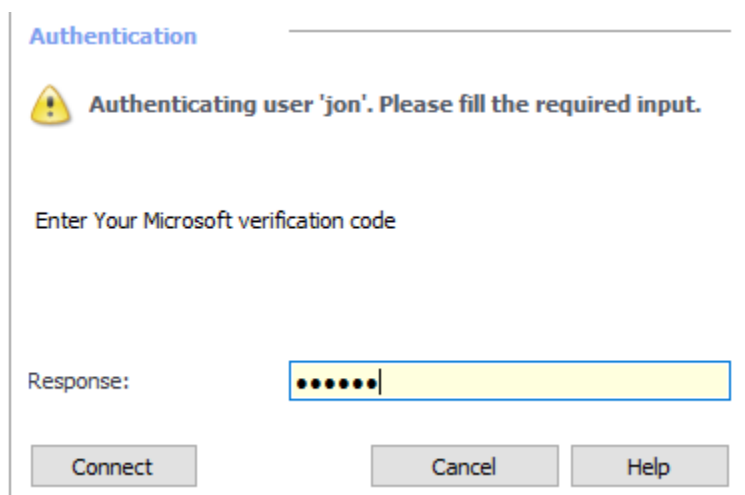
**Authentication**

 **Authenticating user 'jon'. Please fill the required input.**


Password:

Response:

5. You will be asked a Response – enter your windows password
6. You will notice the login screen will change to “Enter your Microsoft verification code”



**Authentication**

 **Authenticating user 'jon'. Please fill the required input.**

Enter Your Microsoft verification code

Response:

At this point 2FA is now complete and will allow the users to access the network.