Check Point
SOFTWARE TECHNOLOGIES LTD.
WELCOME TO THE FUTURE OF CYBER SECURITY

Azure MFA Authentication for RAS VPN users

About this guide

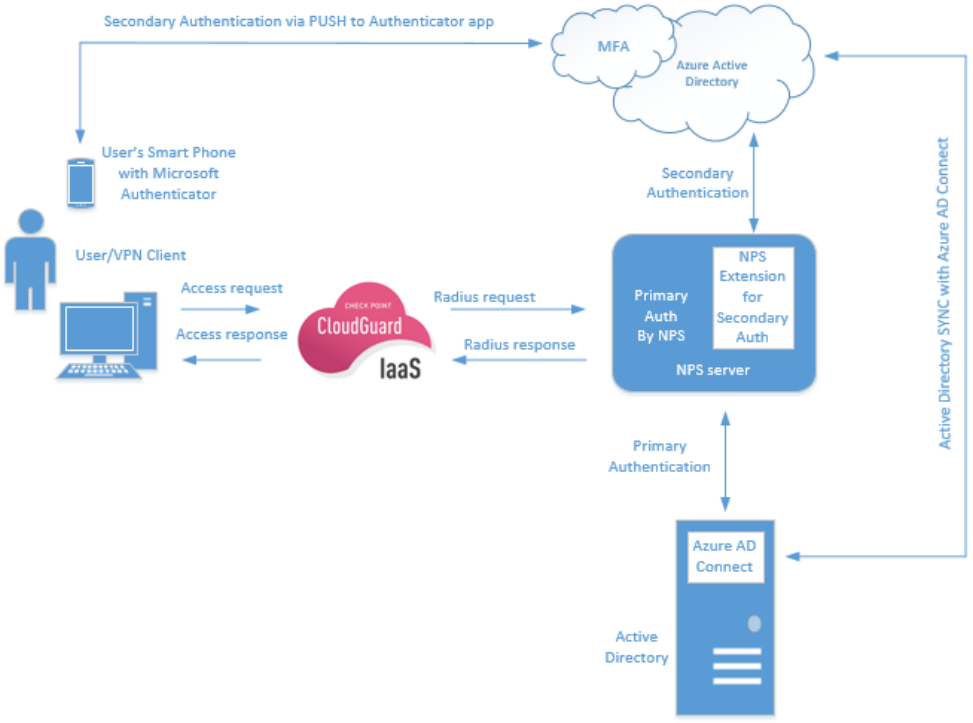
This is guide will describe the full setup configuration of a Azure MFA using the Microsoft Authenticator App in combination with an Active Directory on-premises synced with Azure Active Directory.

The scope is based on VPN remote access on premises that will be moved to Azure Cloud Iaas. The authentication is Active directory credentials in combination with Azure MFA.

Azure MFA for RAS VPN to use Multifactor authentication.

Introduction

User will connect via Endpoint security VPN client to VPN Gateway, enter his Active Directory – UPN (User Principal Name) credentials as primary authentication method and when he has been allowed by the Primary authentication method, the Secondary Authentication method will push a notification to the user in order to “Approve” or “Reject” his access authorization.



Version 3, March 2020
Patrick Willekens

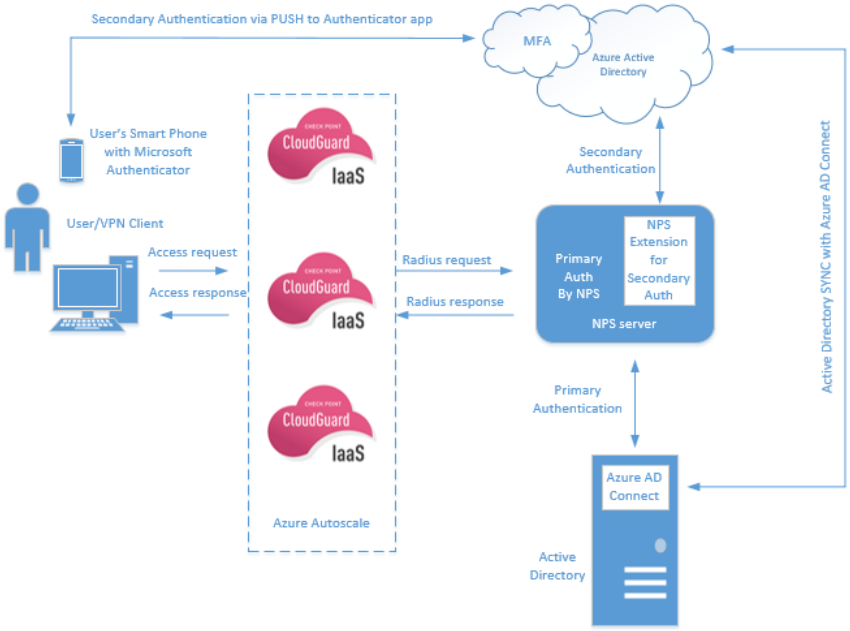
Table of Contents

[Protected] Distribution or modification is subject to approval

1. Overview

The scope is based on the move from on-Premises VPN gateways to VPN IaaS gateways into Azure. The gateways will be deployed following the “Azure auto scale” in order to provide scalability and SLA guarantee from 99.9%.

Azure Active Directory and/or SAML 2.0 authentication for RAS VPN are not yet supported into version starting from R80.xx, therefore will the primary Authentication method be “Active Directory” on-premises via “Express route” and synced with Azure Active Directory to provide Azure MFA.



2. General configuration

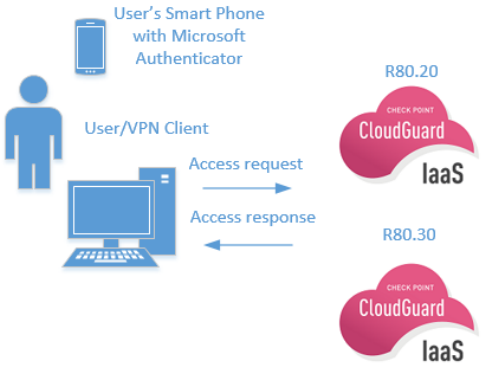
- The configuration has been fully deployed and tested in Azure.
- The RAS VPN has been successfully tested on Cloudguard IaaS R80.20 and Cloudguard IaaS R80.30.
- Active Directory and NPS server has been installed on Window Server 2008R2.

2.1. The authentication flow includes the following components

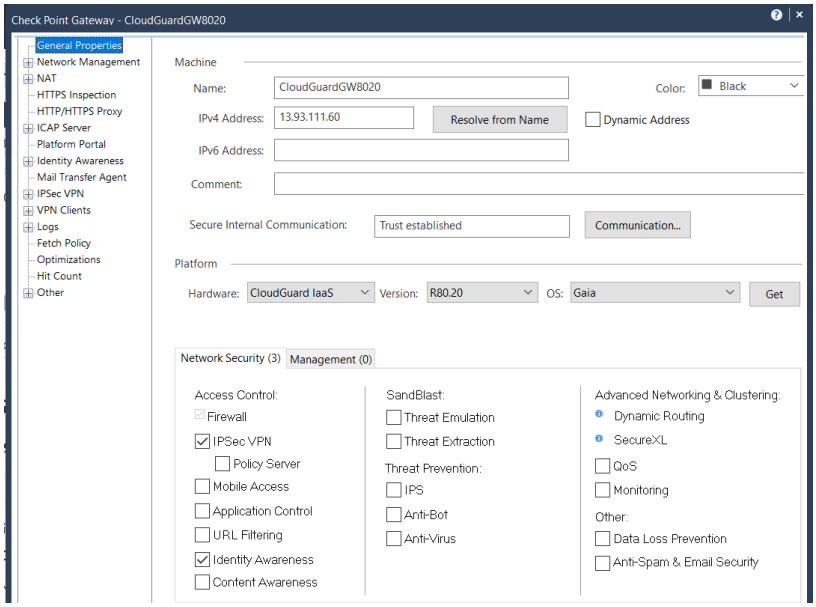
1. **NAS/VPN Server (Cloudguard IaaS)** receives requests from VPN clients (Endpoint Security) and converts them into RADIUS requests to NPS servers.
2. **NPS Server** connects to Active Directory to perform the primary authentication for the RADIUS requests and, upon success, passes the request to any installed extensions.
3. **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.
4. **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.

3. CloudGuard Iaas

The CloudGuard Iaas gateways has been deployed into Virtual Machines in Azure with two NIC's. Two IaaS Gateways has been deployed in parallel as standalone, one R80.20 version and one R80.30 version.

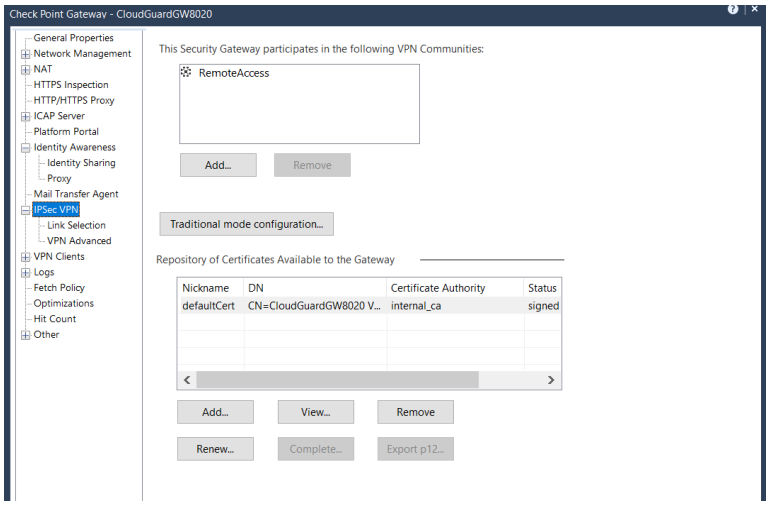


3.1. General settings

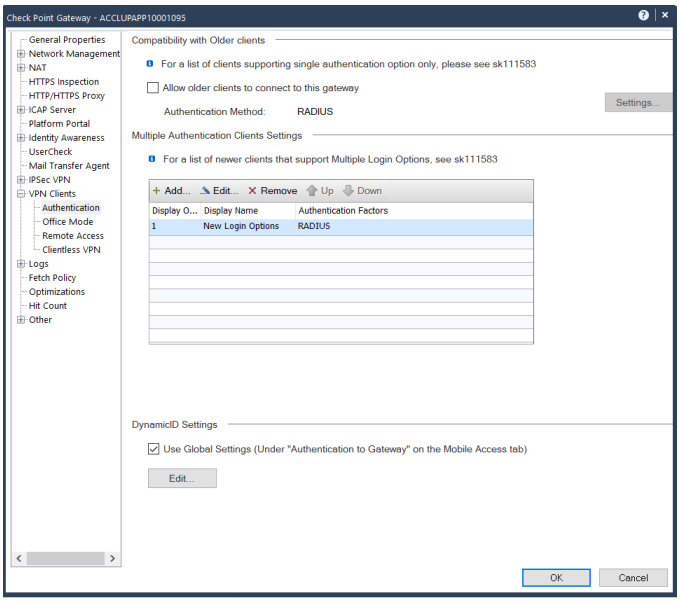


We enabled "IPSec VPN" blade and the "Identity Awareness" blade. IPsec VPN for the RAS VPN and the Identity Awareness in order to retrieve the Users/Groups from the Active Directory in order to include them into the Security Policies.

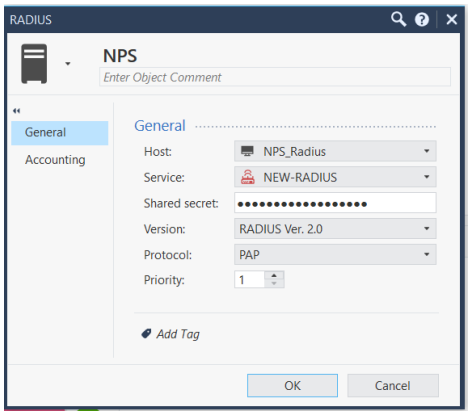
3.2. IPSec VPN setings



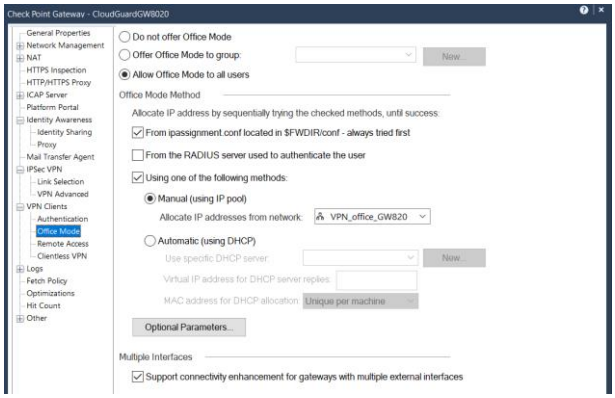
The Authentication tab is set to “**RADIUS**”



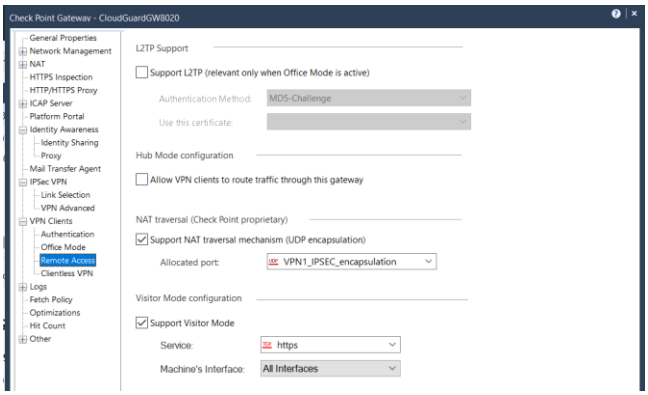
The radius server settings are using “New-RADIUS” and Radius V2 with “PAP”.



Office Mode is set to all users and the DHCP scope is given and defined into the Firewall.
We can use an external DHCP server or retrieve IP from Radius NSP server.

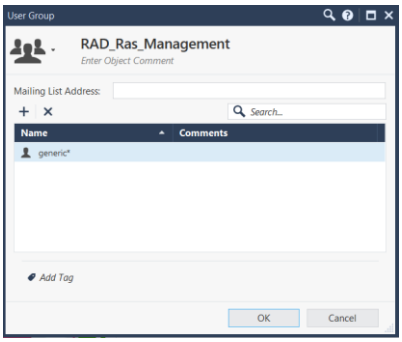


In our case the requirements were to use IPSec and/or Https protocol for the Endpoint Security VPN client.



3.3. Radius configuration on Smartcenter

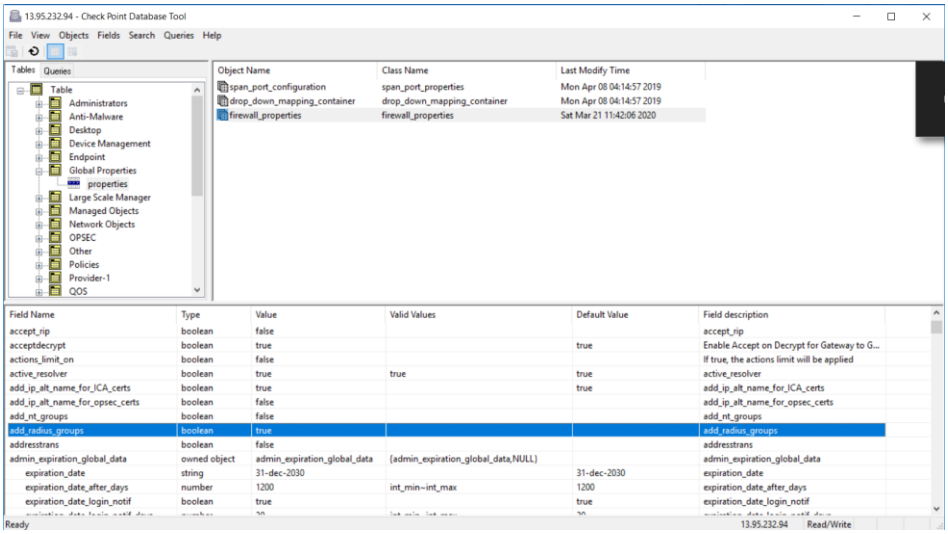
Create an empty group with the name *"RAD_yourattributename."* This needs to match the attribute name in AD group.



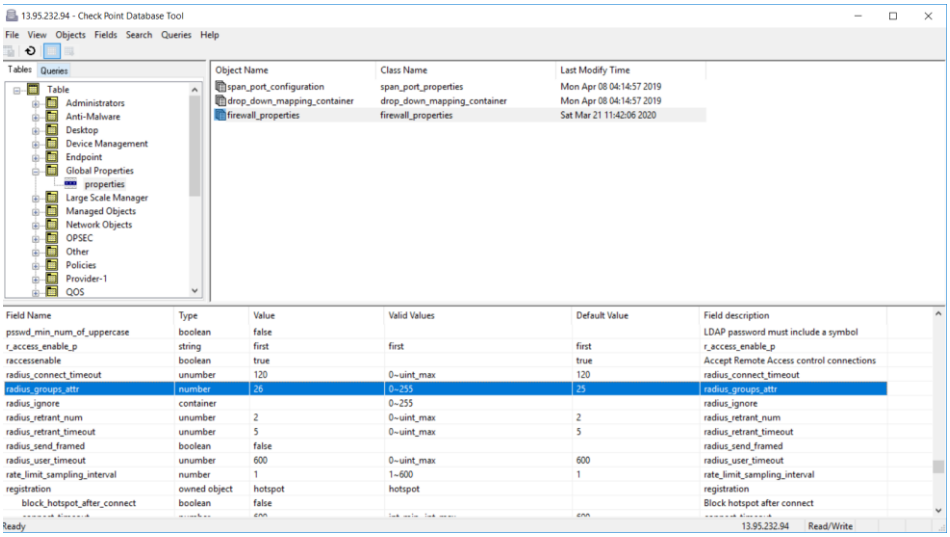
Publish your changes and close SmartConsole. **It is recommended to take backup of your SMS prior to making the following changes.**

Open GuiDB Edit

Change “**add_radius_groups”** value under ***Global Properties > Properties > firewall_properties*** to **true**.



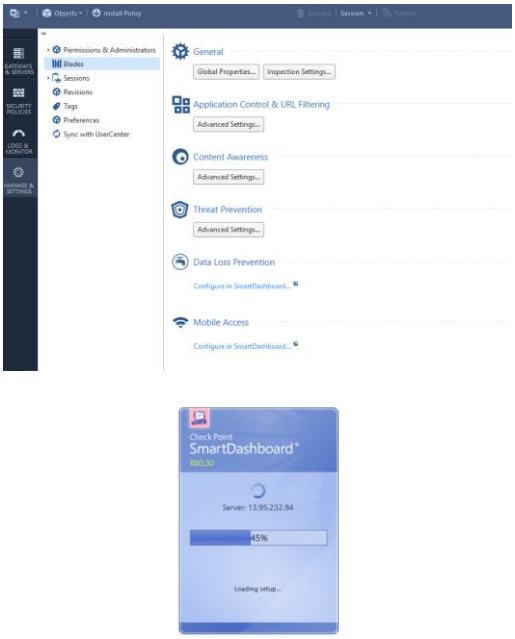
Change the “**radius_groups_atttr”** from **25** to **26**.



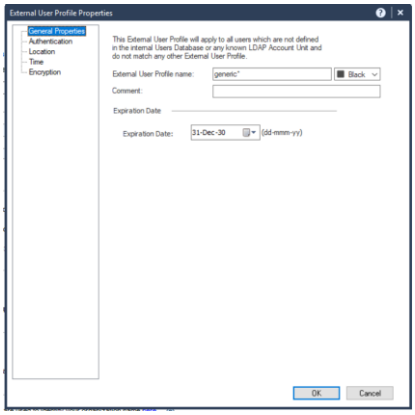
Save your changes and exit GUIDB edit.

[Protected] Distribution or modification is subject to approval

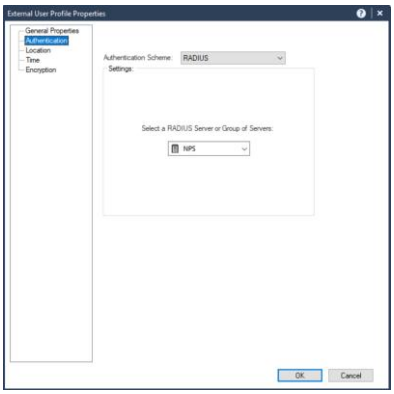
Reopen SmartConsole. Click on “Manage and Settings” followed by “Blades” and then click “Configure in SmartDashboard.” The legacy SmartDashboard client will open.



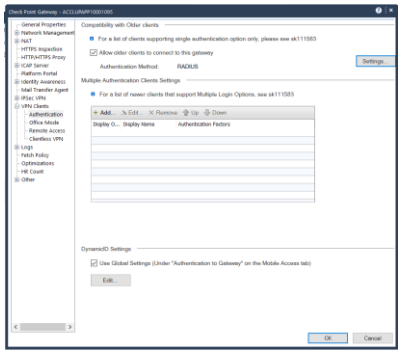
Click on the user icon in the Object Explorer in the bottom left. Then right click “External User Profiles” and select “New External User Profile > Match all users”.



Select “Authentication” and change the Authentication Scheme to RADIUS. Then select the RADIUS server object you created.

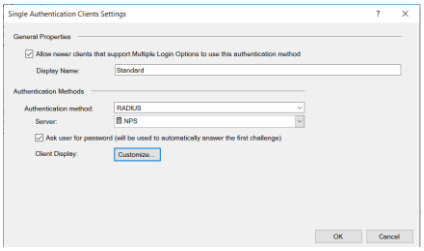


Click “OK” and save your changes. Then close the SmartDashboard window. In SmartConsole, open the gateway object for your Remote Access VPN Gateway.
Select “VPN Clients” and expand the menu. Then click “Authentication”.



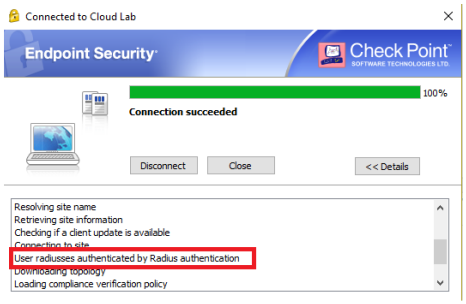
This guide will utilize the single authentication only option with RADIUS as the authentication method. Check the box “Allow older clients to connect to this gateway” and then click “Settings”.

Change the authentication method to RADIUS and select the server you created as the server. Check the box that says “Ask user for password (will be used to automatically answer the first challenge”. If you leave this unchecked, your end user will be prompted for a username, then a password and they will need to complete two prompts instead of one.



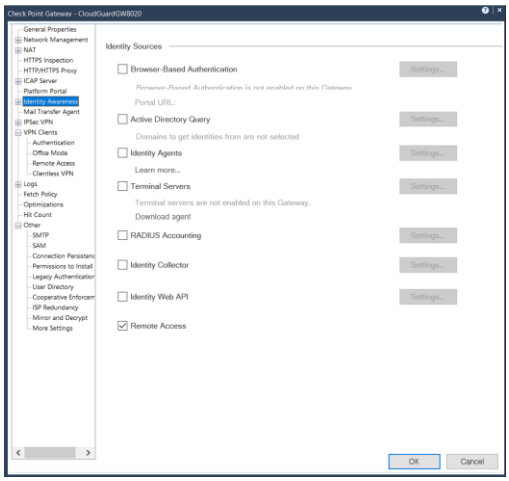
Click “OK” on each open window and install policy to the Remote Access gateway.

Your users should now be able to authenticate via their Active Directory Credentials and RADIUS:

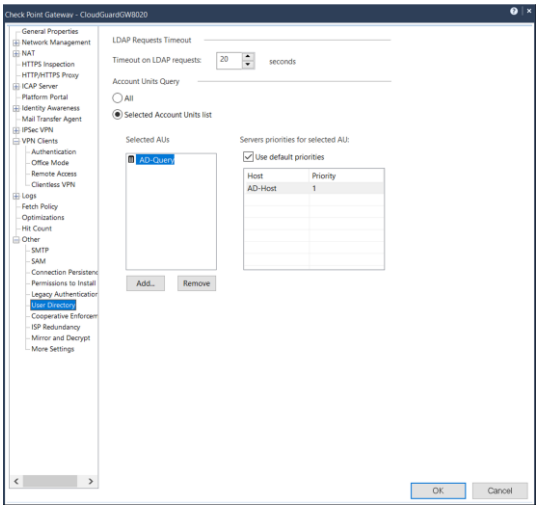


3.4. Identity Awareness settings

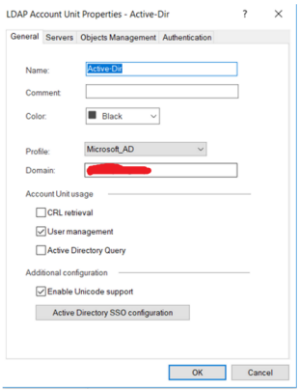
In order to retrieve the Active Directory Users and Groups to use them into the Security Policies, we enabled Identity Awareness blade. Identity based “Access control” is providing roaming users access to applications independent of the network they are connected to or the site they are located in.



3.5. The User Directory

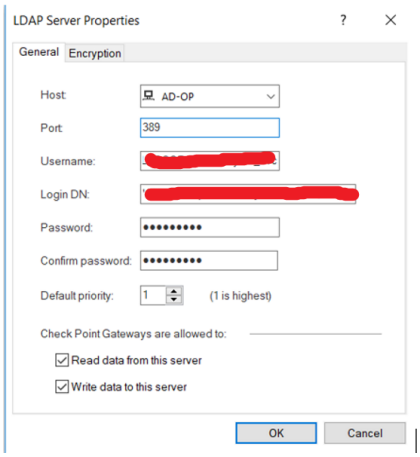


3.6. The LDAP Account Unit configuration

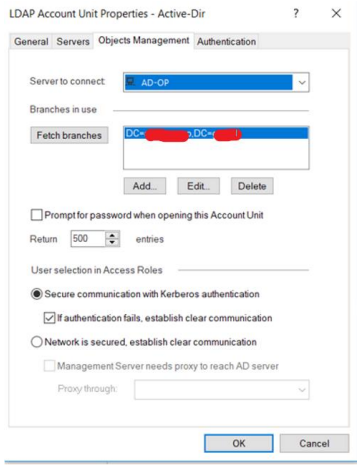


Domain = “domain.xxx”

Choose the AD host you already defined upfront and fill the field such as Username, Login DN and Password.



- In our case the Username = *domain\account*
- The Login DN= *'CN=account,OU=Users,DC=domain,DC=xxx*

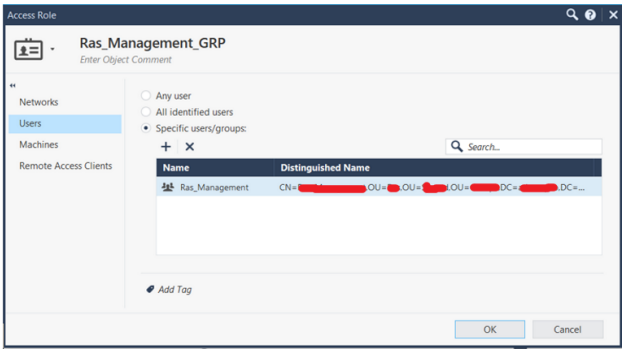


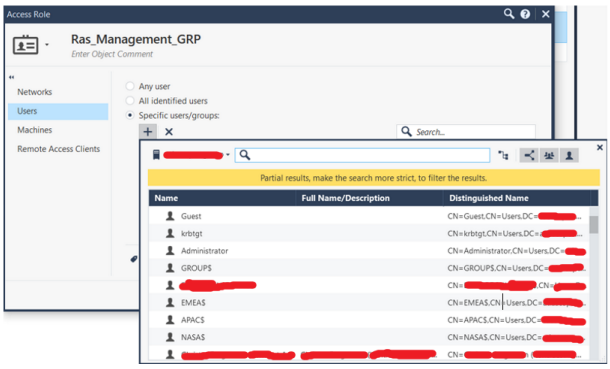
Fetch branches to verify your communication with Active Directory

[Protected] Distribution or modification is subject to approval

3.7. The Acces Role

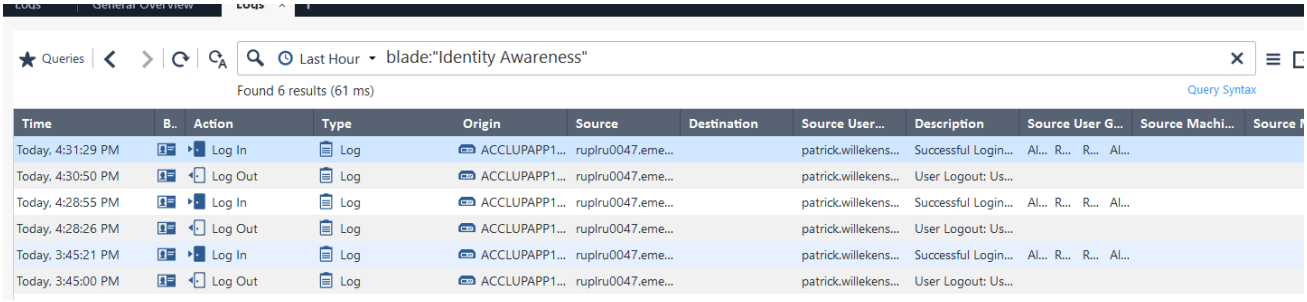
In order to have a security rule base defined on the AD groups, make an access Role and add the Groups that we allowed.





We should enable “Application control” on the GW and so we can secure and monitor, applications, bandwidth and use.

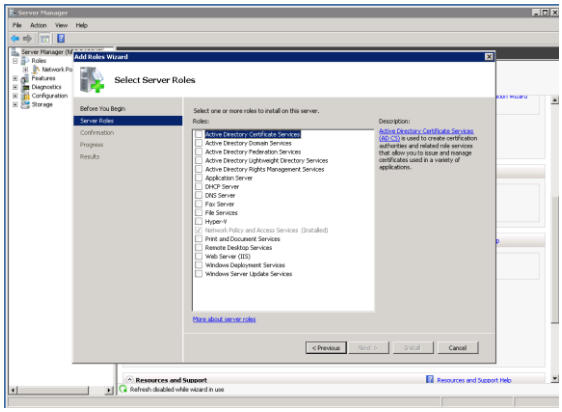
The security rule base, will not use the Legacy access anymore, but with an “Access roles” in order to filter and log properly all users who logon via VPN.

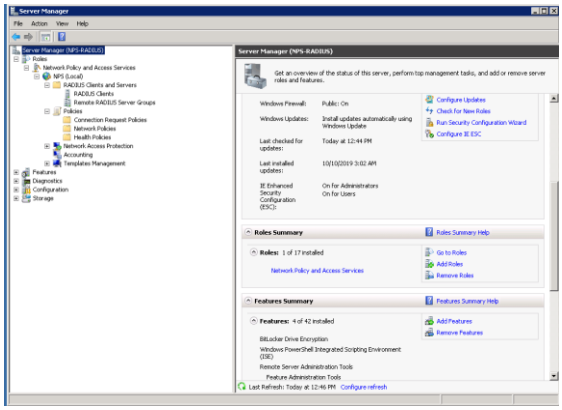


[Protected] Distribution or modification is subject to approval

4. NPS Server

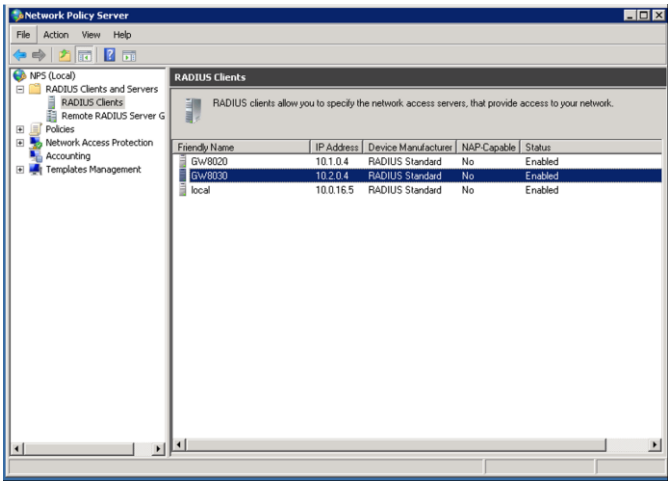
The NPS installed on Windows 2008R2 server. The NPS server has been added as a "**role**" via the server Manager.





4.1. Configure of the NPS server

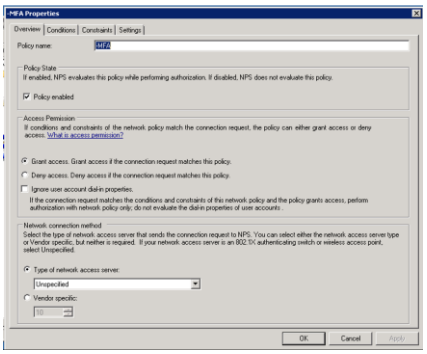
Add the IP address(es) of your VPN gateway(s) to you "Radius clients".



NOTE : It's important to join the NPS server to the "Active Directory Domain" (see Policy Conditions)

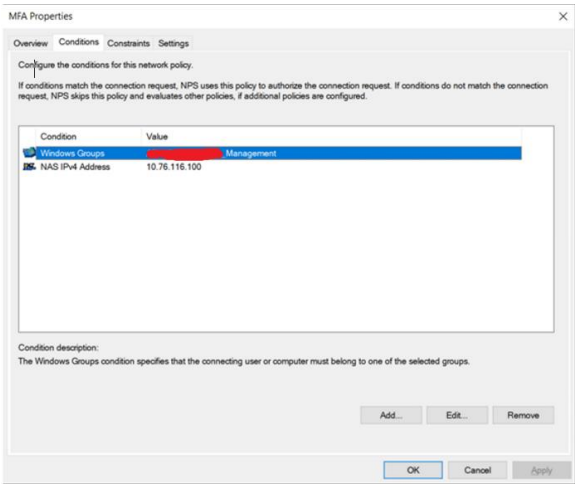
4.2. Configure of the NPS Policy

In the "*Overview*" we give the policy a "*name*" and leave Type of Network Access Server to **undefined**.

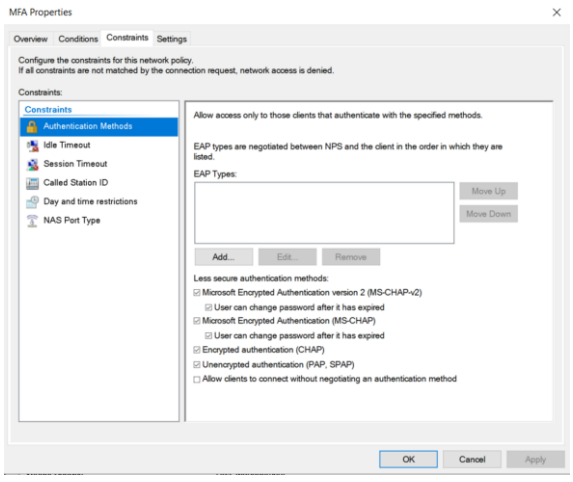


In the "*Conditions*", you can add different conditions, such as Authentication methods, Groups, timeframe, NAS IP addresses, Filters and other.

Into the conditions I configured that only users into AD domain group "DOMAIN\Ras_Management" would be allowed to Authenticate and use the NAS IP address of the Gateway.

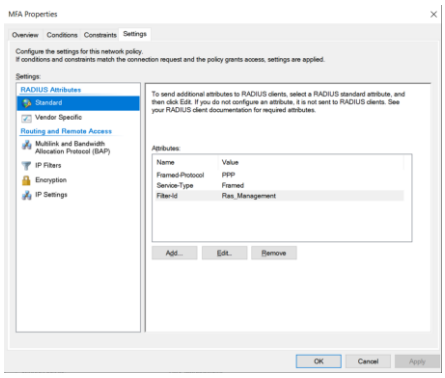


In the "*Constraints*" we will configure the Authentication types, going from PAP, CHAP, MSCHAP or MSCHAPv2.

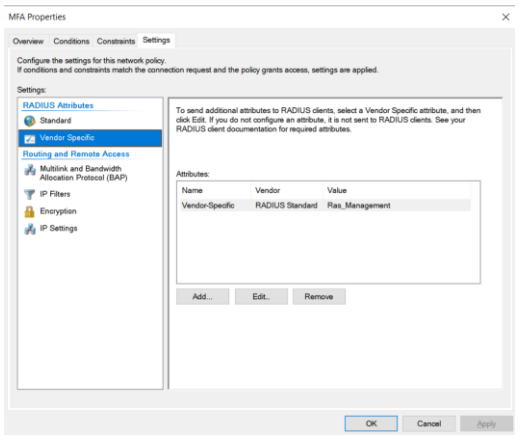


In the “Settings” I added a filter-id in the radius attributes and added the “Vendor Specific” radius attributes for our Check Point IaaS gateways.

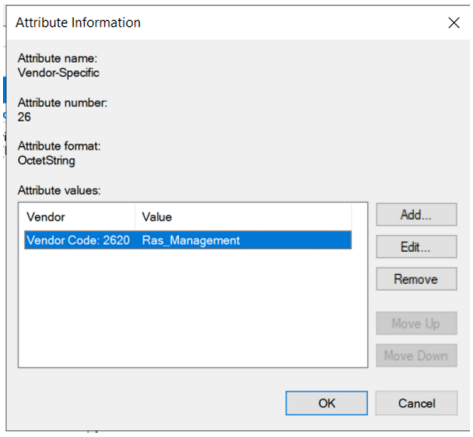
Filter-id = Ras_Management



Vendor Specific



The Vendor code has to set to “2620” with a value “Ras_Management”



For More information see Knowledge Base

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105575

4.3. Registry setting for the NPS

An important setting about MFA is require to add some value into the registry of the NPS server. The authentication method can differ follow the preparation of NPS against MFA.

Prepare NPS for users that aren't enrolled for MFA

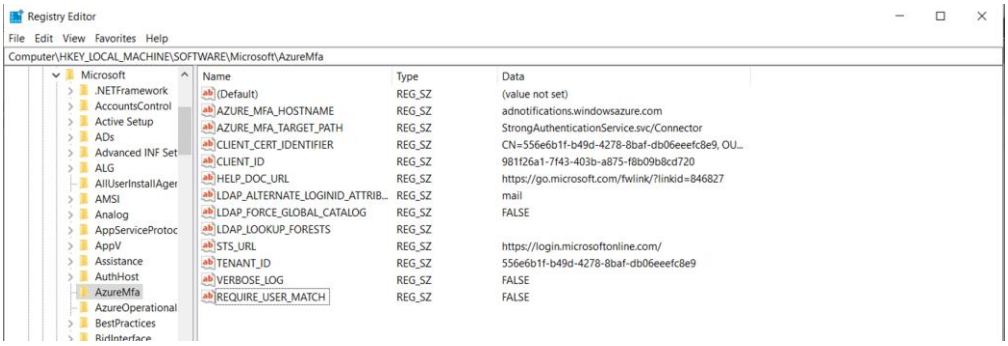
Choose what happens when users that aren't enrolled with MFA try to authenticate. Use the registry setting `REQUIRE_USER_MATCH` in the registry path `HKLM\Software\Microsoft\AzureMFA` to control the feature behavior. This setting has a single configuration option.

Key	Value	Default
`REQUIRE_USER_MATCH`	TRUE / FALSE	Not set (equivalent to TRUE)

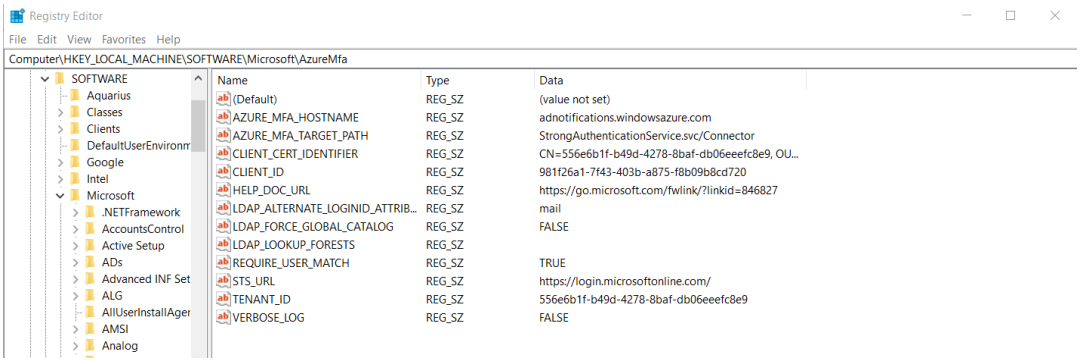
The purpose of this setting is to determine what to do when a user is not enrolled for MFA. The effects of changing this setting are listed in the table below.

Settings	User MFA Status	Effects
Key does not exist	Not enrolled	MFA challenge is unsuccessful
Value set to True / not set	Not enrolled	MFA challenge is unsuccessful
Key set to False	Not enrolled	Authentication without MFA
Key set to False or True	Enrolled	Must authenticate with MFA

If you want to allow users to authenticate against the NPS server that aren't yet enrolled by the MFA, the "REQUIRE_USER_MATCH" = FALSE.



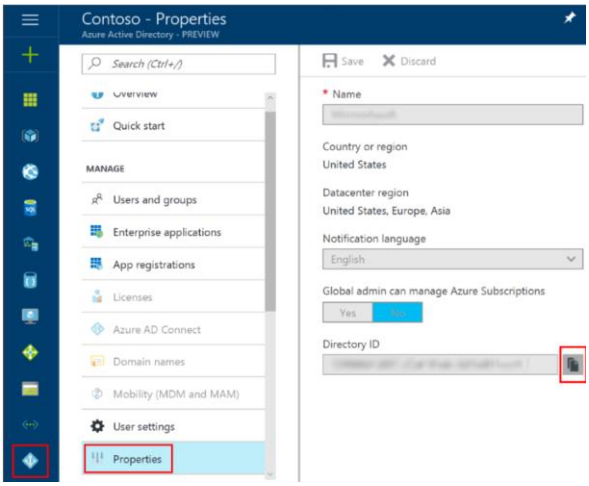
If you lockdown the authentication towards the NPS only for MFA enrolled users then "REQUIRE_USER_MATCH" = TRUE.



5. NPS extension for Azure MFA

When using the NPS extension, this must be synced to Azure Active Directory using Azure AD Connect, and must be registered for MFA.

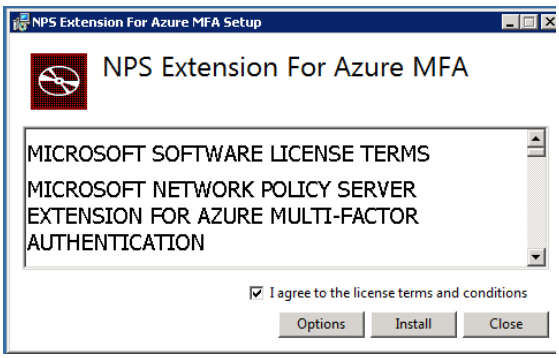
When you install the extension, you need the directory ID and an admin credentials for your Azure AD tenant. You can find your directory ID in the Azure portal. Sign in as an administrator, select the **Azure Active Directory** icon on the left, and then select **Properties**. Copy the GUID in the **Directory ID** box and save it. You use this GUID as the tenant ID when you install the NPS extension.

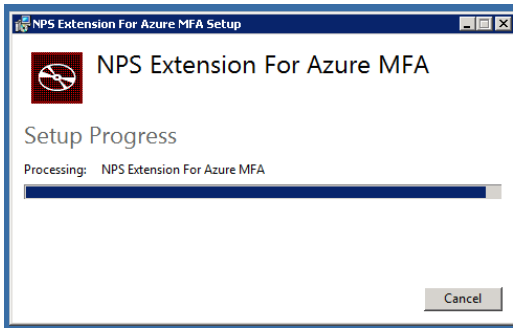


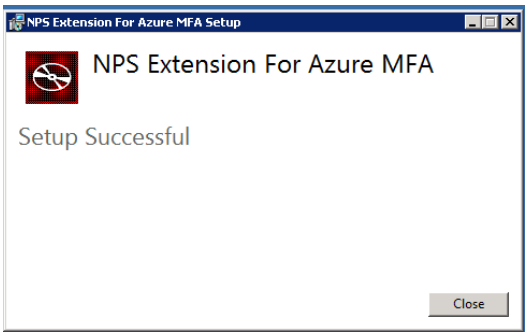
The NPS server needs to be able to communicate with the following URLs over ports 80 and 443.

- https://adnotifications.windowsazure.com
- https://login.microsoftonline.com
- https://login.microsoftonline.com
- https://provisioningapi.microsoftonline.com
- https://aadcdn.msauth.net

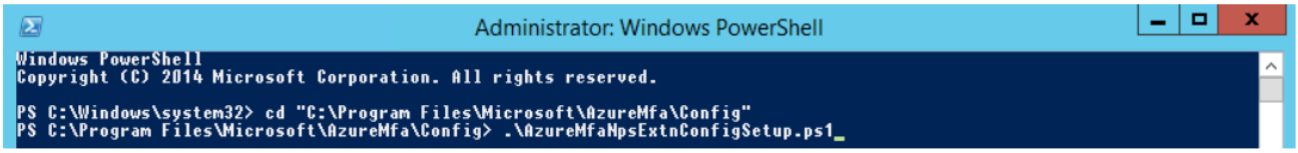
Download the NPS extension from https://aka.ms/npsmfa and launch the “NpsExtnForAzureMfaInstaller.exe”.



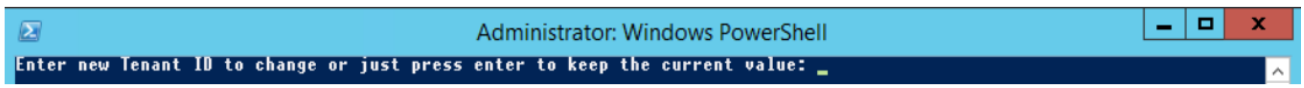




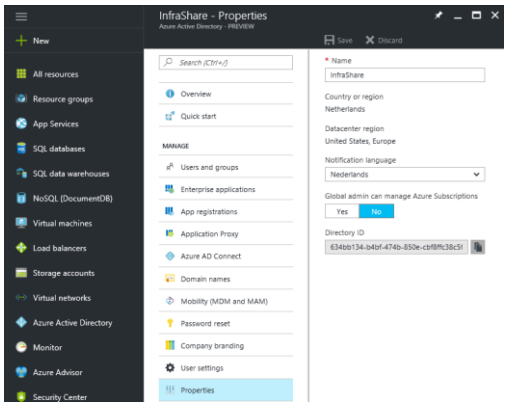
Now we need to **open** a **PowerShell** prompt as administrator – change the default directory location to "*C:\Program Files\Microsoft\AzureMfa\Config*" and **run** the following **script** – AzureMfaNpsExtnConfigSetup.ps1



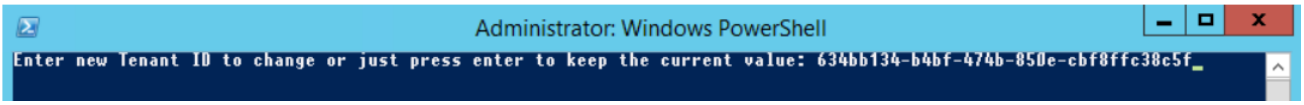
The setup now prompt for the tenant ID of your Azure Active Directory subscription



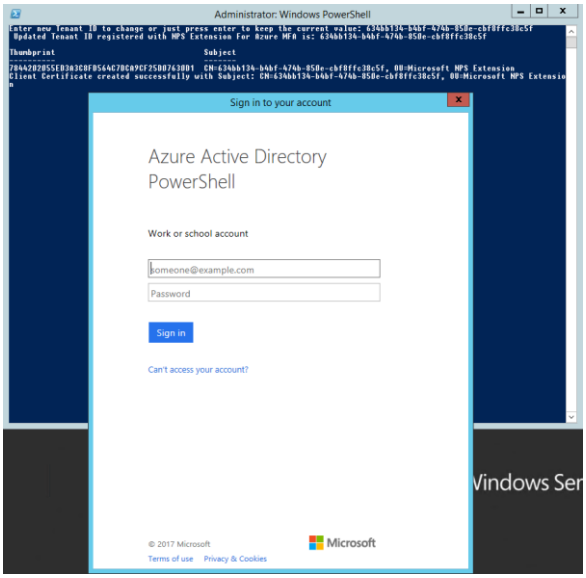
This is not your tenant name, but the **Directory ID** that can be found in the Azure portal under the Properties of your Azure Active Directory Service, **click** on the **copy** button to set it under your clipboard



Paste the **Directory ID** in the PowerShell prompt and click on **Enter**



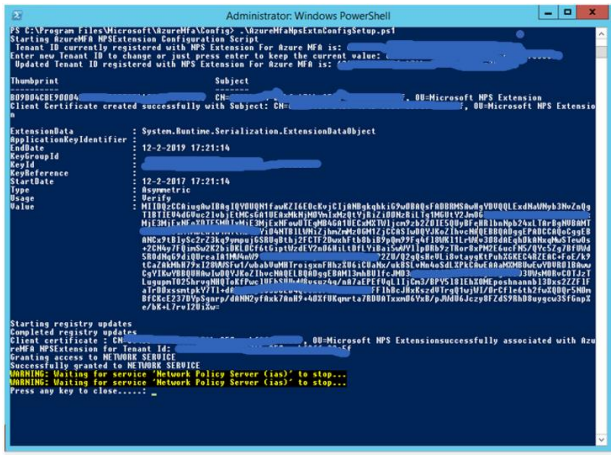
You now need to **sign** in with your Azure AD administrator (global administrator/co-administrator) credentials – **click** on **Sign in** when finished.



The script now starts running, when all the steps proceeded correctly, the screen must be like this – **click** on **random key** afterwards to close the PowerShell prompt

The script performs the following steps:

– Create a self-signed certificate.
– Associate the public key of the certificate to the service principal on Azure AD.
– Store the cert in the local machine cert store.
– Grant access to the certificate's private key to Network User.
– Restart the NPS.



[Protected] Distribution or modification is subject to approval

6. Active Directory

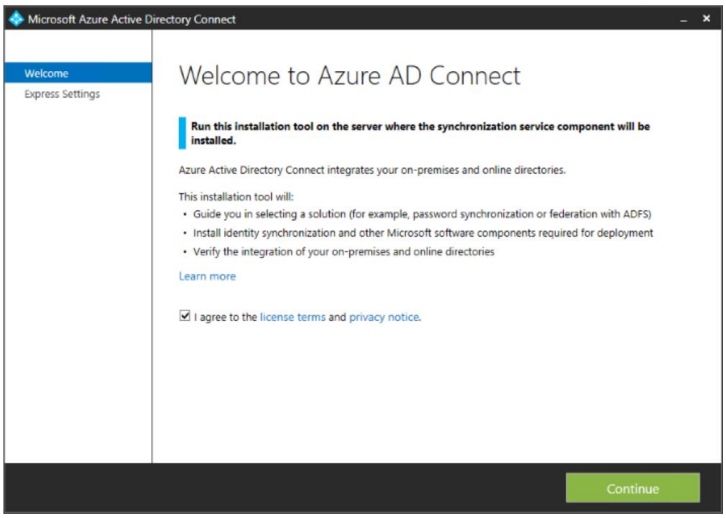
The on-premises Active Directory is a Windows2008R2 server. When installed, run the “DCPromo” to create your domain.

When you Active Directory/domain is ready, download the Azure AD Connect tool.

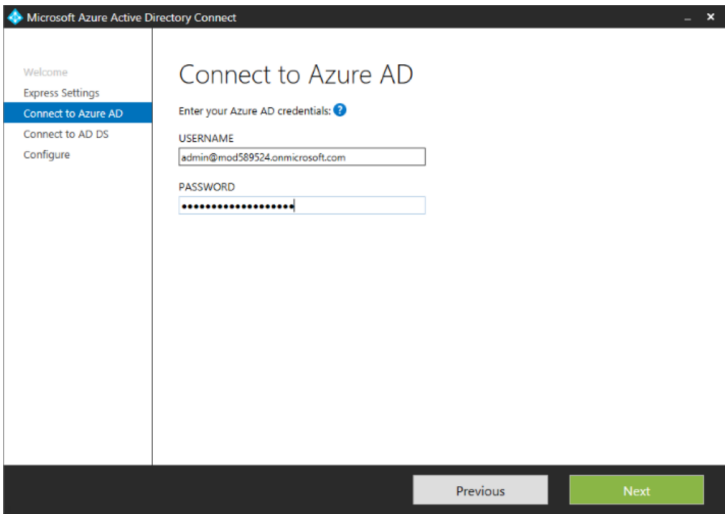
https://www.microsoft.com/en-us/download/details.aspx?id=47594

6.1. Azure AD connect

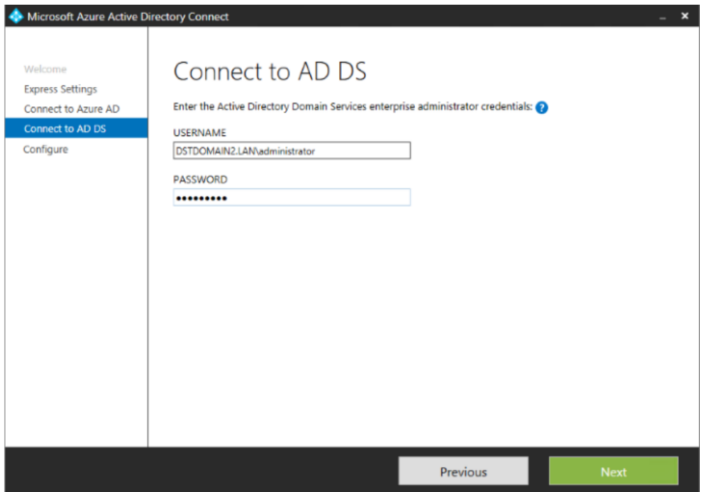
Run the AzureADConnect.msi and follow the steps.



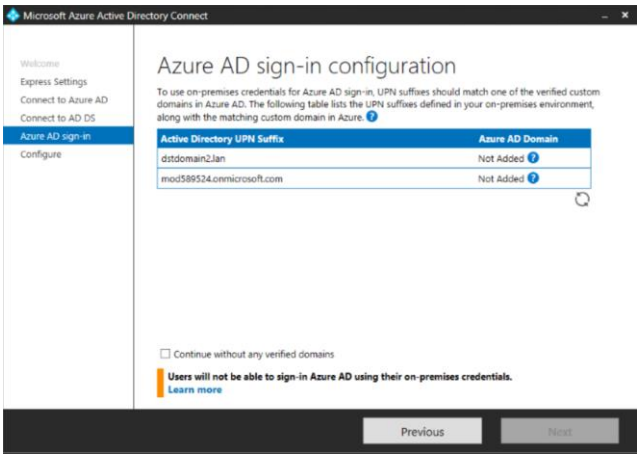
If you have a verified domain, the **Use Express Settings** option will be highlighted to go with. Click on it to start the configuration. If you are using a non-reputable domain, like .local, the wizard will recommend going with the **Customize** option.



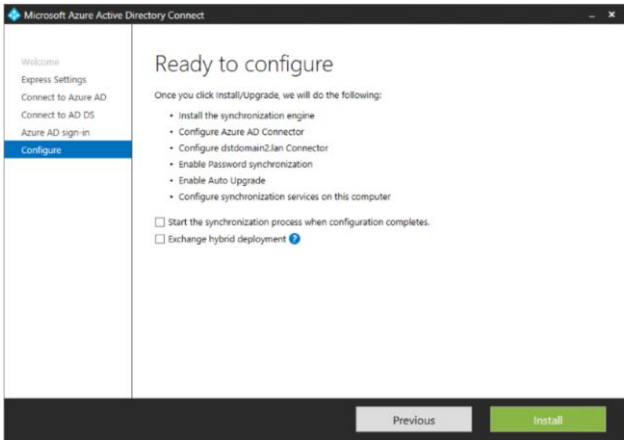
Now, connect to Active Directory DS using your enterprise administration credentials. Click **Next**.



If you didn't add or verify your domain in Azure AD, you will see the **Azure AD sign-in configuration** section in the wizard. Make sure that you followed this instruction to add or verify the domain.

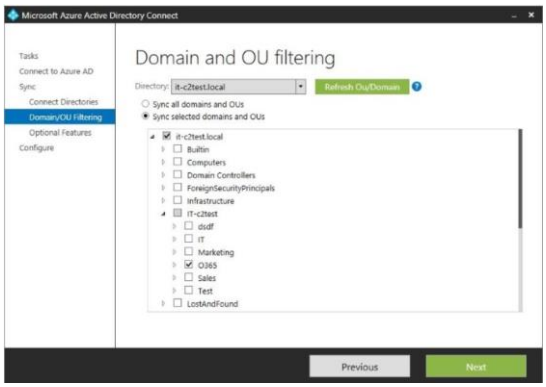


In the **Ready to configure** window, you can put some final touches to the configuration by checking or unchecking available options. In this instruction, I do not want the synchronization to start automatically, so I unchecked the "Start the synchronization process when configuration completes" option.



6.2. To filter Organizational Units

1. Open Azure AD Connect.
2. In the **Domain and OU filtering** section, unselect the OUs you don't want to synchronize (by default all OUs are selected).



[Protected] Distribution or modification is subject to approval

7. Azure Active Directory synchronization with Active Directory.

7.1. Use PowerShell to manage synchronization

If you unchecked the “Start the synchronization process when configuration completes” box in the Configure section in Azure AD Connect, you need to start the synchronization manually. You can do it via PowerShell.

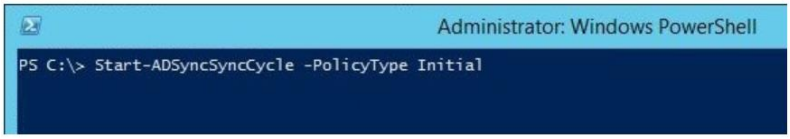
7.2. Check current synchronization settings

To check the current state of the synchronization settings, use this cmdlet:

```
Get-ADSyncScheduler
```

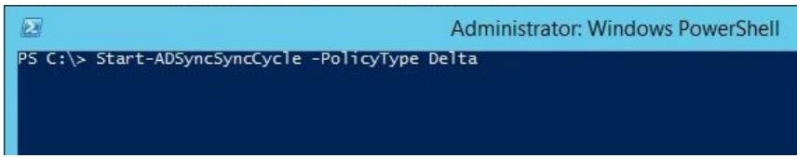
To start the **initial** synchronization run this cmdlet:

```
Start-ADSyncSyncCycle -PolicyType Initial
```



To start the **delta** synchronization use this cmdlet:

```
Start-ADSyncSyncCycle -PolicyType Delta
```



7.3. Alternate login ID

Since the NPS extension **connects to both your on-premises and cloud directories**, you might encounter an issue where your **on-premises user principal names (UPNs)** don't match the names in the cloud. To solve this problem, use alternate login IDs.

Within the NPS extension, you can designate an Active Directory attribute to be used in place of the UPN for Azure Multi-Factor Authentication. This enables you to protect your on-premises resources with two-step verification without modifying your on-premises UPNs.

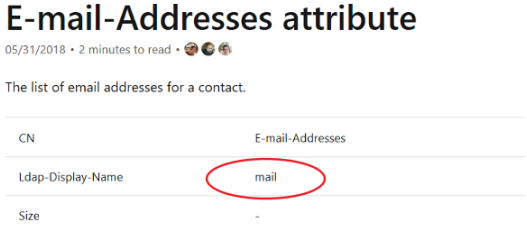
[Protected] Distribution or modification is subject to approval

To configure alternate login IDs, go to ***HKLM\SOFTWARE\Microsoft\AzureMfa*** and edit the following registry values:

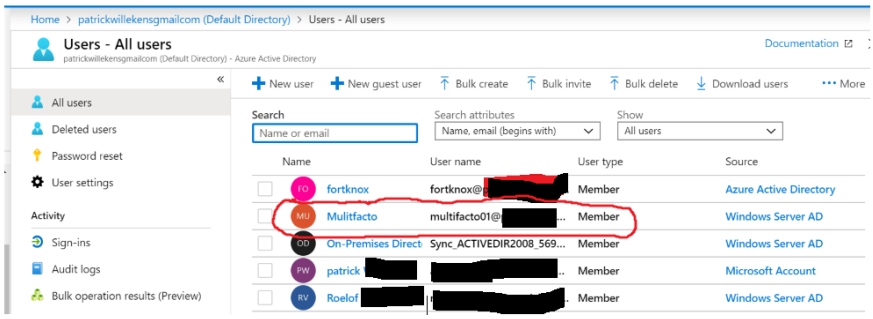
Name	Type	Default value	Description
LDAP_ALTERNATE_LOGINID_ATTRIBUTE	string	Empty	**Designate the name of Active Directory attribute that you want to use instead of the UPN. This attribute is used as the AlternateLoginId attribute. If this registry value is set to a valid Active Directory attribute (for example, mail or displayName), then the attribute's value is used in place of the user's UPN for authentication. If this registry value is empty or not configured, then AlternateLoginId is disabled and the user's UPN is used for authentication.**
LDAP_FORCE_GLOBAL_CATALOG	boolean	False	Use this flag to force the use of Global Catalog for LDAP searches when looking up AlternateLoginId. Configure a domain controller as a Global Catalog, add the AlternateLoginId attribute to the Global Catalog, and then enable this flag. If LDAP_LOOKUP_FORESTS is configured (not empty), **this flag is enforced as true**, regardless of the value of the registry setting. In this case, the NPS extension requires the Global Catalog to be configured with the AlternateLoginId attribute for each forest.
LDAP_LOOKUP_FORESTS	string	Empty	Provide a semi-colon separated list of forests to search. For example, *contoso.com;foobar.com*. If this registry value is configured, the NPS extension iteratively searches all the forests in the order in which they were listed, and returns the first successful AlternateLoginId value. If this registry value is not configured, the AlternateLoginId lookup is confined to the current domain.

https://docs.microsoft.com/en-us/windows/win32/adschema/attributes-all?redirectedfrom=MSDN

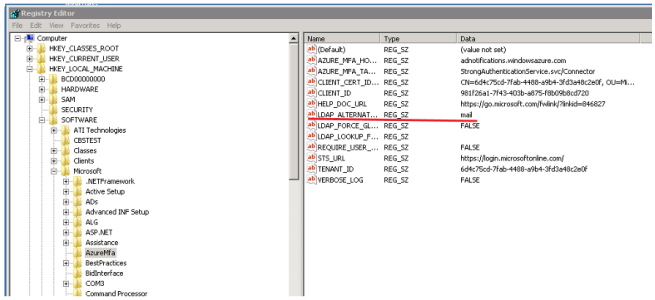
We did choose as attribute “mail” in order to verify against the Azure Active Directory user name.



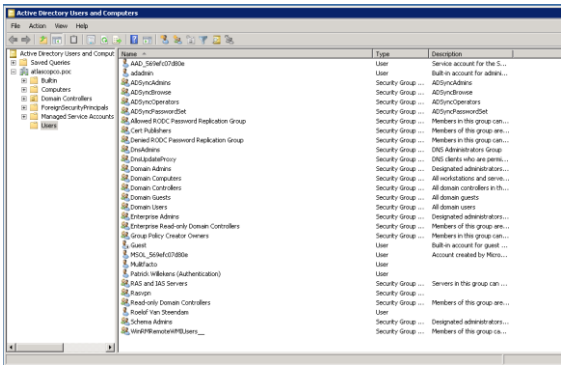
In Azure Active Directory we have the users, f.e. “Multifacto – multifacto@domain.com”



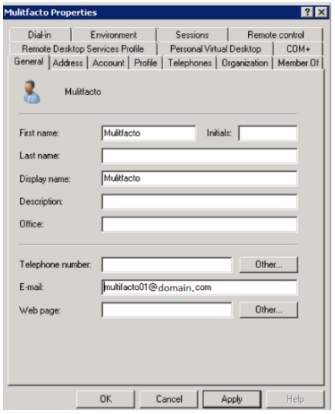
On the NPS server, we did modify the Registry entry “***LDAP_ALTERNATE_LOGINID_ATTRIBUTE***” and added “***mail***”.



7.4. Active Directory on premise

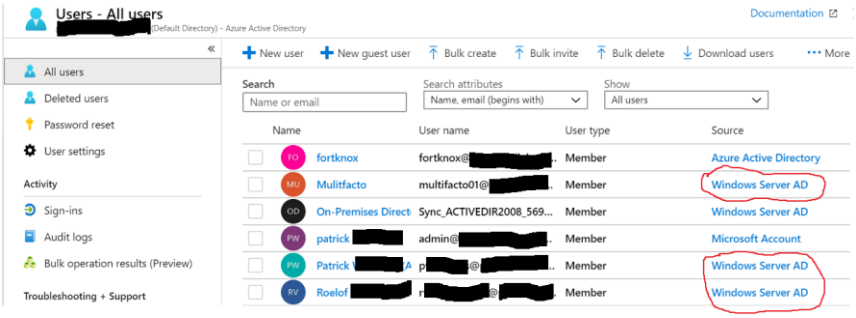


Into the Active Directory on premise, we did add the user mail address multifacto01@domain.com.



[Protected] Distribution or modification is subject to approval

7.5. Azure Active Directory



[Protected] Distribution or modification is subject to approval

8. Plan authentication methods

Administrators can choose the authentication methods that they want to make available for users. It is important to allow more than a single authentication method so that users have a backup method available in case their primary method is unavailable. The following methods are available for administrators to enable:

- **Notification through mobile app**

A push notification is sent to the Microsoft Authenticator app on your mobile device. The user views the notification and selects **Approve** to complete verification. Push notifications through a mobile app provide the least intrusive option for users. They are also the most reliable and secure option because they use a data connection rather than telephony.

- **Verification code from mobile app**

A mobile app like the Microsoft Authenticator app generates a new OATH verification code every 30 seconds. The user enters the verification code into the sign-in interface. The mobile app option can be used whether or not the phone has a data or cellular signal.

- **Call to phone**

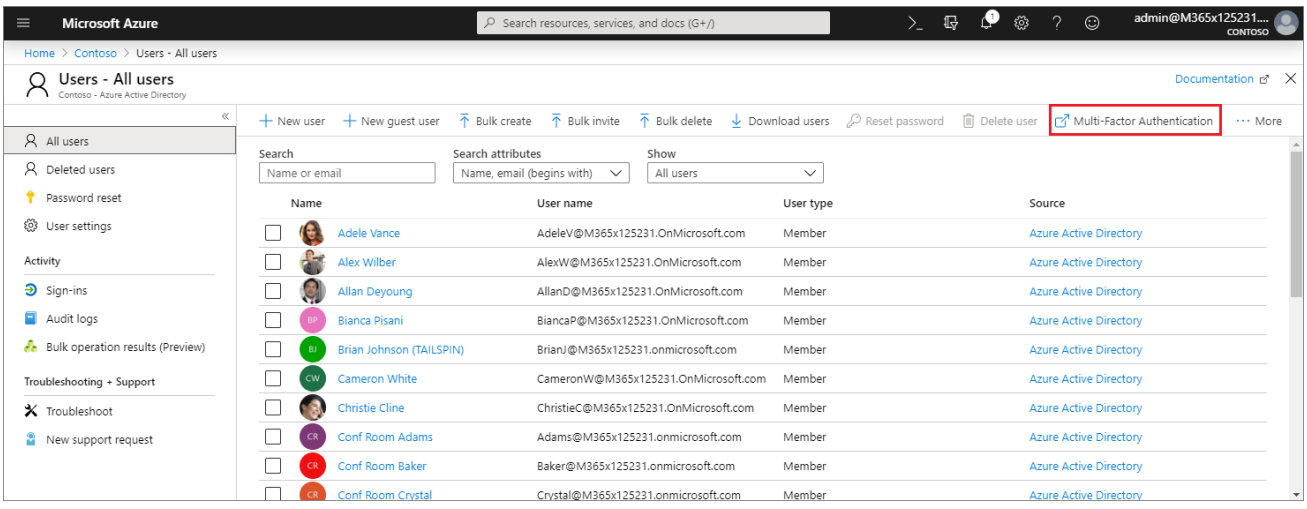
An automated voice call is placed to the user. The user answers the call and presses **#** on the phone keypad to approve their authentication. Call to phone is a great backup method for notification or verification code from a mobile app.

- **Text message to phone**

A text message that contains a verification code is sent to the user, the user is prompted to enter the verification code into the sign-in interface.

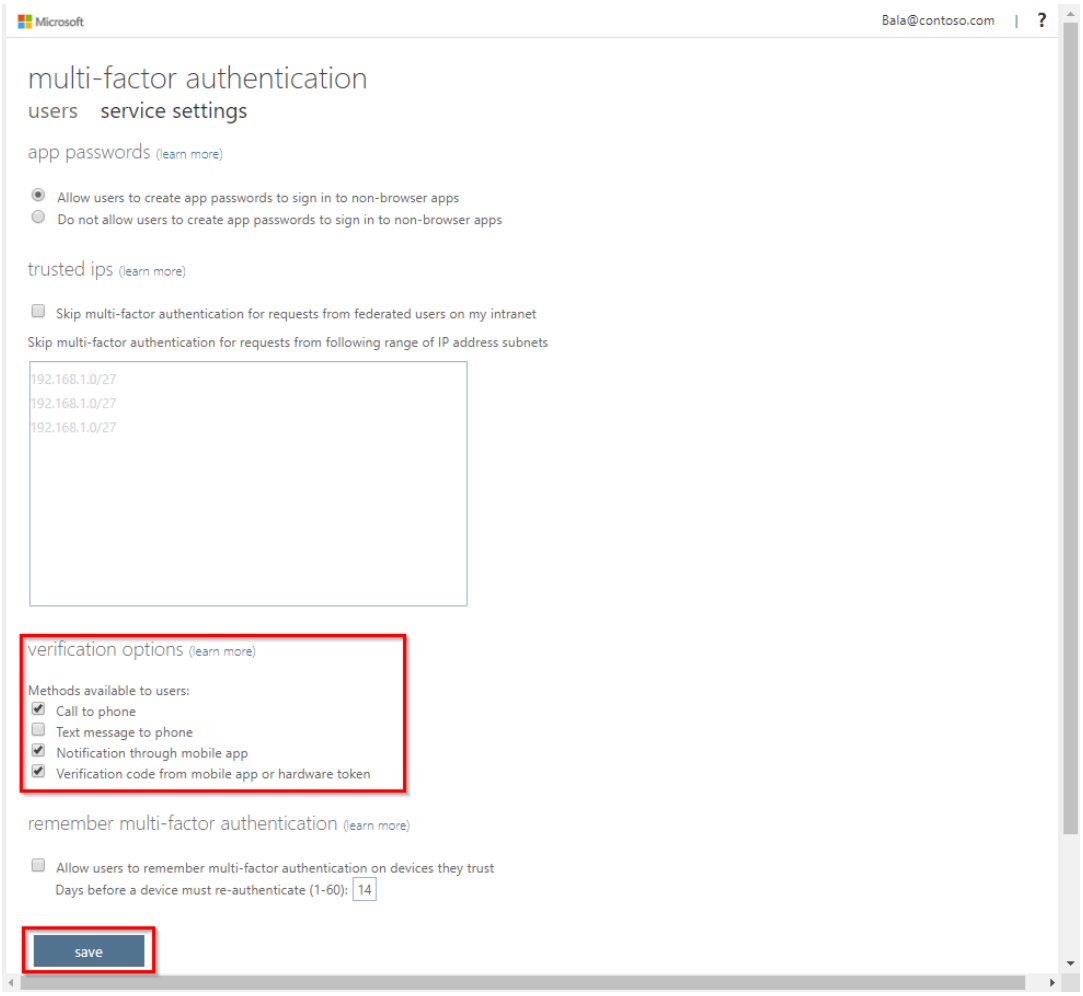
- **Choose verification options**

Browse to **Azure Active Directory**, **Users**, **Multi-Factor Authentication**.



In the new tab that opens browse to **service settings**.

Under **verification options**, check all of the boxes for methods available to users.



Click on **Save**.

Close the **service settings** tab.

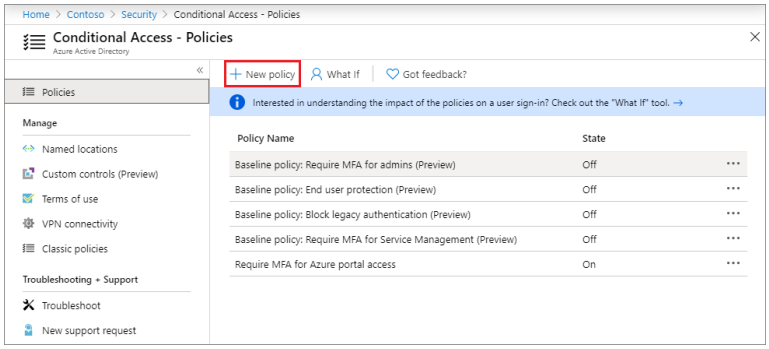
[Protected] Distribution or modification is subject to approval

9. Plan Conditional Access policies

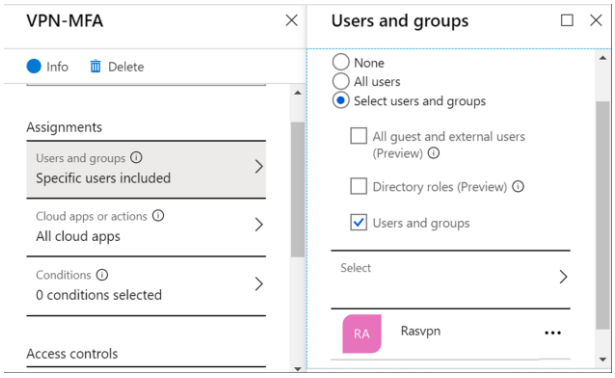
To plan your Conditional Access policy strategy, which will determine when MFA and other controls are required.

Create Conditional Access policy

1. Sign in to the Azure portal using a global administrator account.
2. Browse to **Azure Active Directory**, **Conditional Access**.
3. Select **New policy**.



1. Under **users and groups**:
   - On the **Include** tab, select the **Select users and groups** radio button
   - Check the box for **Users and groups** and choose your emergency access accounts(in our case Rasvpn group).
   - Click **Done**.



Under **Cloud apps**, select the **All cloud apps** radio button.

- OPTIONALLY: On the **Exclude** tab, choose cloud apps that your organization does not require MFA for.
- Click **Done**.

Under **Conditions** section:

- OPTIONALLY: If you have enabled Azure Identity Protection, you can choose to evaluate sign-in risk as part of the policy.
- OPTIONALLY: If you have configured trusted locations or named locations, you can specify to include or exclude those locations from the policy.

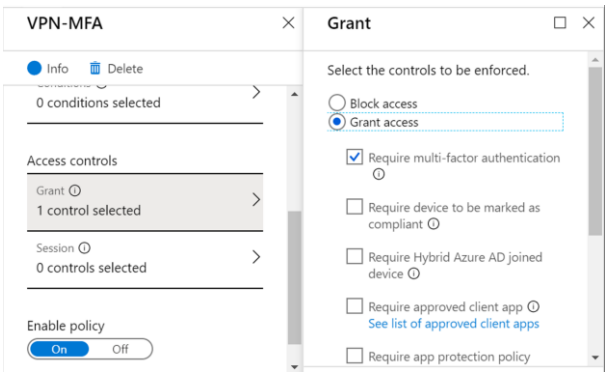
Under **Grant**, make sure the **Grant access** radio button is selected.

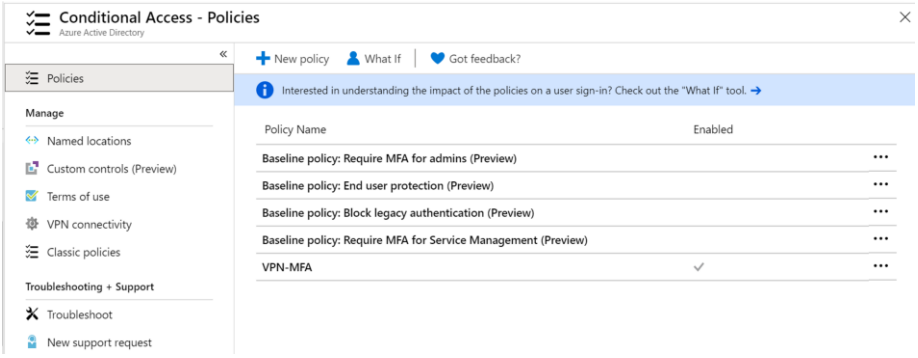
- Check the box for **Require multi-factor authentication**.
- Click **Select**.

Skip the **Session** section.

Set the **Enable policy** toggle to **On**.

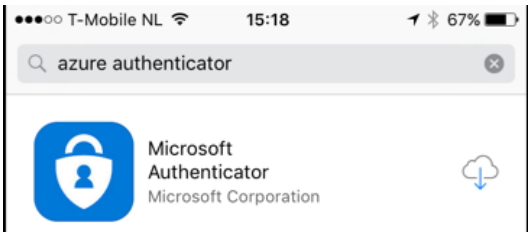
Click **Create**.



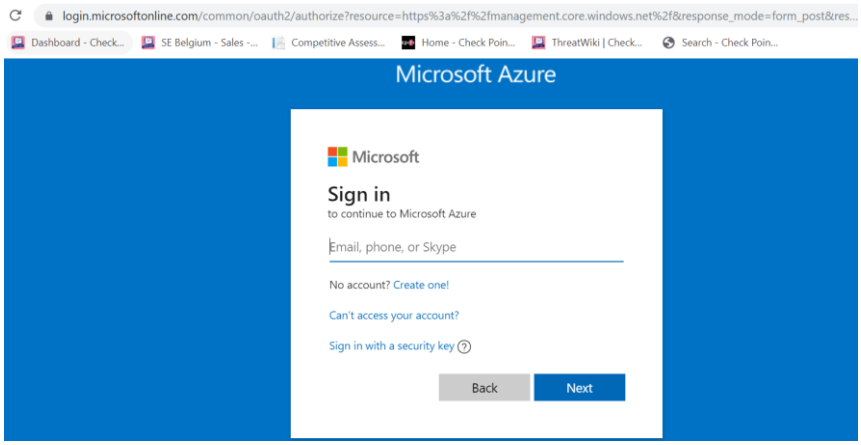


10. User registration for Microsoft Authenticator.

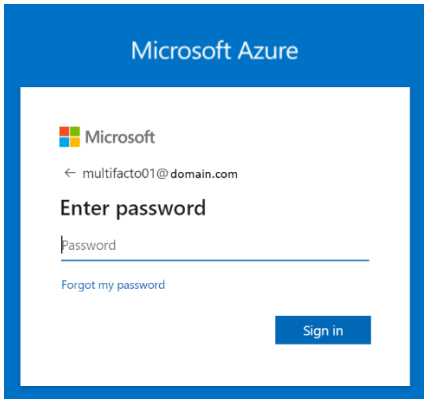
Download the Microsoft Authenticator **App** on your mobile device and setup your work account, these steps are straight forward.



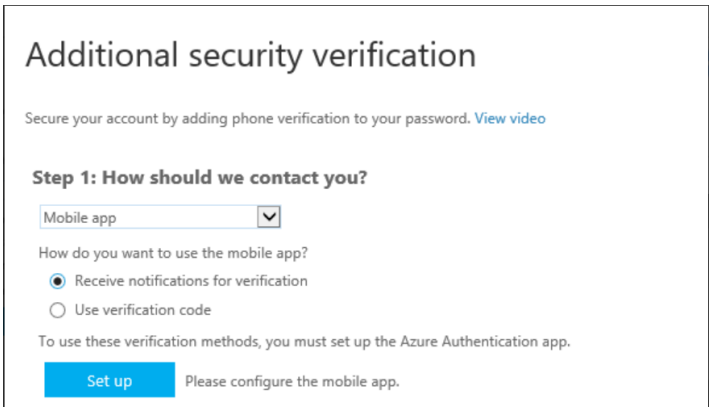
Logon to Azure (portal.office.com / portal.azure.com), with the MFA pre-activated account, you will be prompt to proceed how you want to authentication second (phone or App), **click** on the – Set it up now – **button** to proceed these steps



Fill in your Active Directory user Credentials, f.e. = multifacto01@domain.com

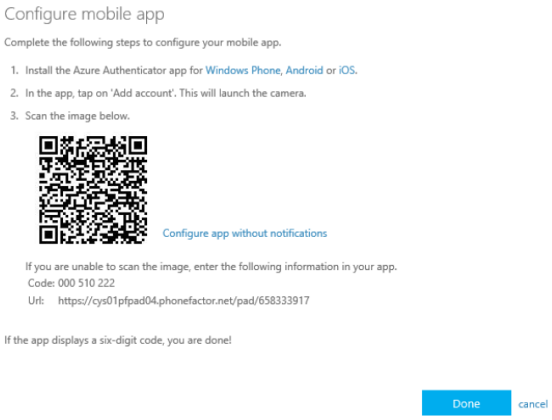


You will able to choose between two authentication methods, choose “Receive notifications for verification”.

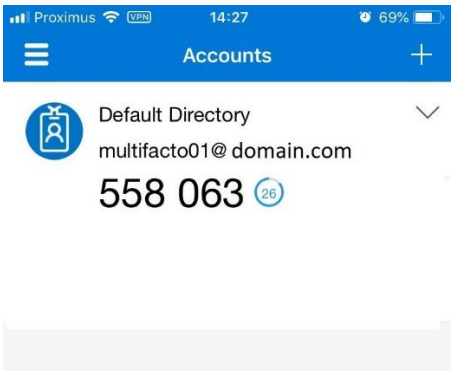


You can now scan through your Mobile app the QR code in order to create your account.

The camera needs to be activated.



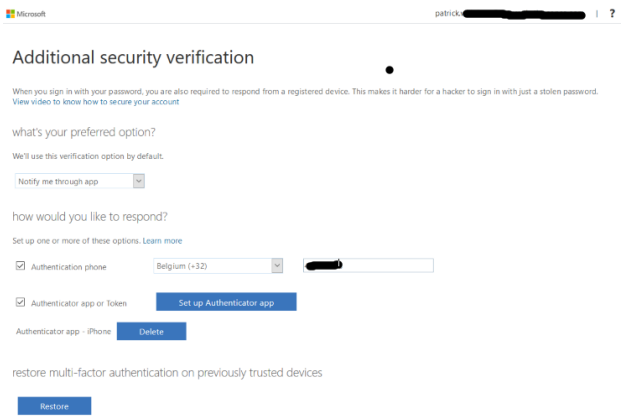
Your Microsoft Authenticator should now display your account.



11. Authentication methods.

11.1. PUSH authentication via the Microsoft Authenticator.

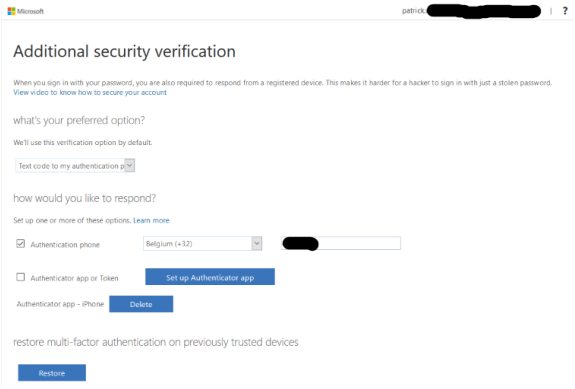
Choose “Notify me through app” from the drop down box. Please check “Authentication phone and fill you country code and number.



To verify your authentication method, the MFA will send a PUSH via your Microsoft Authenticator.

11.2. SMS authentication.

If you prefer to send a SMS for the Multi factor authentication, please select “Text code to my authentication phone” and check also “Authentication phone” and fill you country code and number.



It would send you a SMS with a code in order to verify your number.

- For the VPN connectivity, please follow the first part of the procedure is similar, your AD credentials username@domain.com and password,

    - For Microsoft Authenticator, you will receive a PUSH “Approve” or “Refuse”.
    - For SMS code, you will prompted to enter a challenge “Response” from the VPN client where you fill in your code you received.