Authentication CheckPoint VPN Agent with Microsoft Azure MFA

COMPONENTS:

Check Point:

-Cluster VSX, Appliances 15400, Gaia R80.10 Take:225

-EndPoint Security VPN E82.20 Build 986101311 for windows

-Security Management Server R80.20 Take:103

-SmartConsole R80.20 Build 992000088

Microsoft:

-Windows Server 2016 Datacenter Version 1607 (OS Build 14393.2879)->NPS

-NPS Extension for Azure MFA->Installer

-Windows Server ->Azure AD Connect sync -> side on-premises

-Azure AD Connect sync service-> Side Azure

-Office365

-Laptop ThinkPad Lenovo Windows 10 Pro, Version 1909 (OS Build 18363.720)

DESCRIPTION:

This guide will show you the configuration for configure the 2-factor authentication with Microsoft Azure MFA and Check Point VPN agent. The connections required for configuration is the local domain connection with Azure AD and the NPS extension for Azure MFA, in addition to an NPS server that performs the authentication and authorization of users in the AD. The 2-factor authentication is done through the settings made in each user's Office 365 account. In this case, authentication was performed using an SMS code that receives the configured cell phone number.

CONFIGURATION:

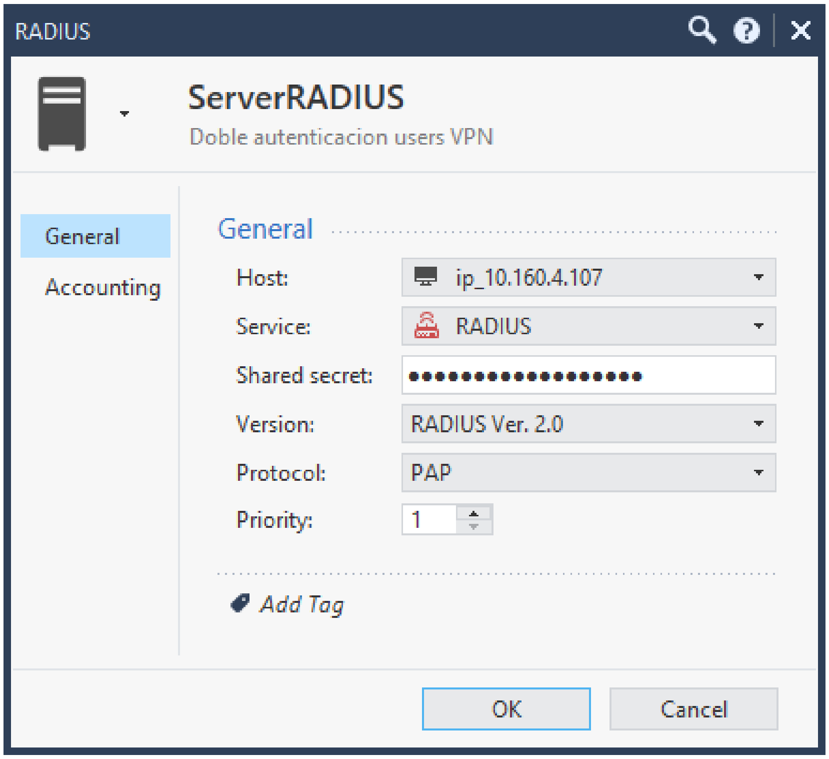
Previous configurations:

1. Synchronization of domain local(on-premise) with Azure AD Connect sync, for this step Azure AD Connect sync must be installed on a Windows server and configured with admin credential (in the references there is a link with the necessary information about the configuration).
2. Users licensed and configure with MFA in Office 365.
3. Licensing for MFA authentication with Azure AD / Office 365 (in the references there is a link with the necessary information about the licenses).
4. Guarantee the communication between the FW or VS and the NPS over service RADIUS UDP/1645 or NEW-RADIUS UDP/1812.
    a. To verify the communication between the FW and the NPS server over service selected run fw monitor or tcpdump to see traffic.

Note: Communication between the FW or VS should not be with NAT.

Configurations Security Management Server:

In Security Management Server (SMS) configure a new RADIUS server type object, these are the only parameters to configure, for example, the NPS object, the RADIUS UDP / 1645 service, the shared secret (this is the same for the RADIUS client on NPS), versión of RADIUS (Ver. 2.0), and protocol PAP (this protocol because support double authentication with SMS code) and priority.



ServerRADIUS

Doble autenticacion users VPN

General

Host: ip_10.160.4.107

Service: RADIUS

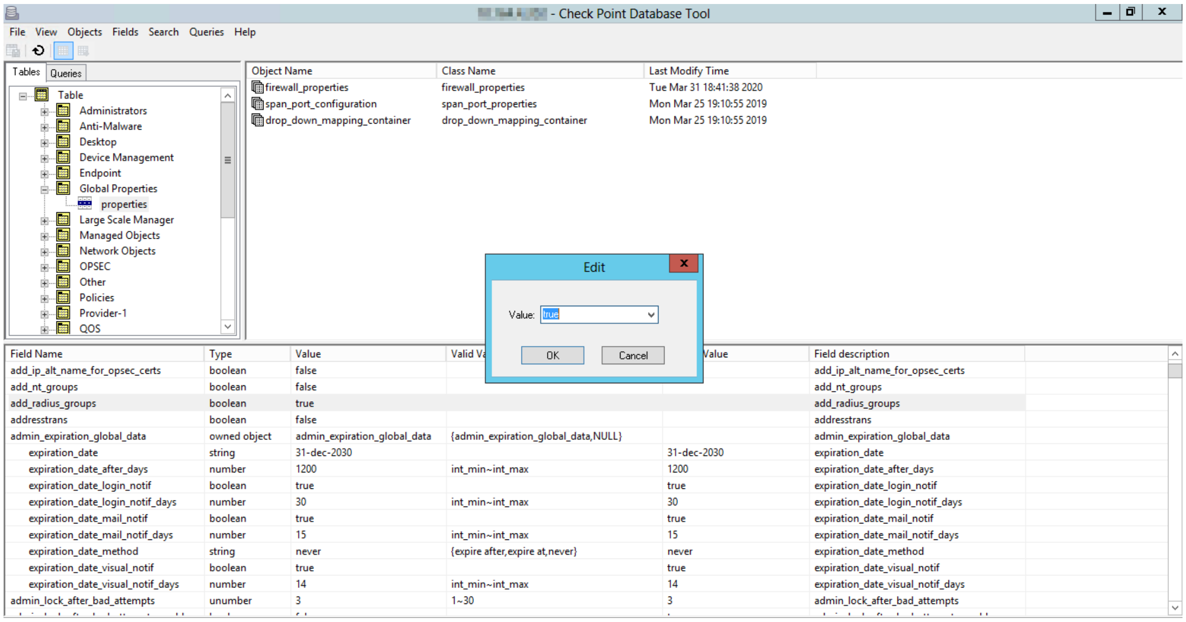
Shared secret: ●●●●●●●●●●●●●●●●●

Version: RADIUS Ver. 2.0

Protocol: PAP

Priority: 1

Open GuiDBedit under Global Properties->Properties->firewall_properties change “add_radius_groups” value to true.

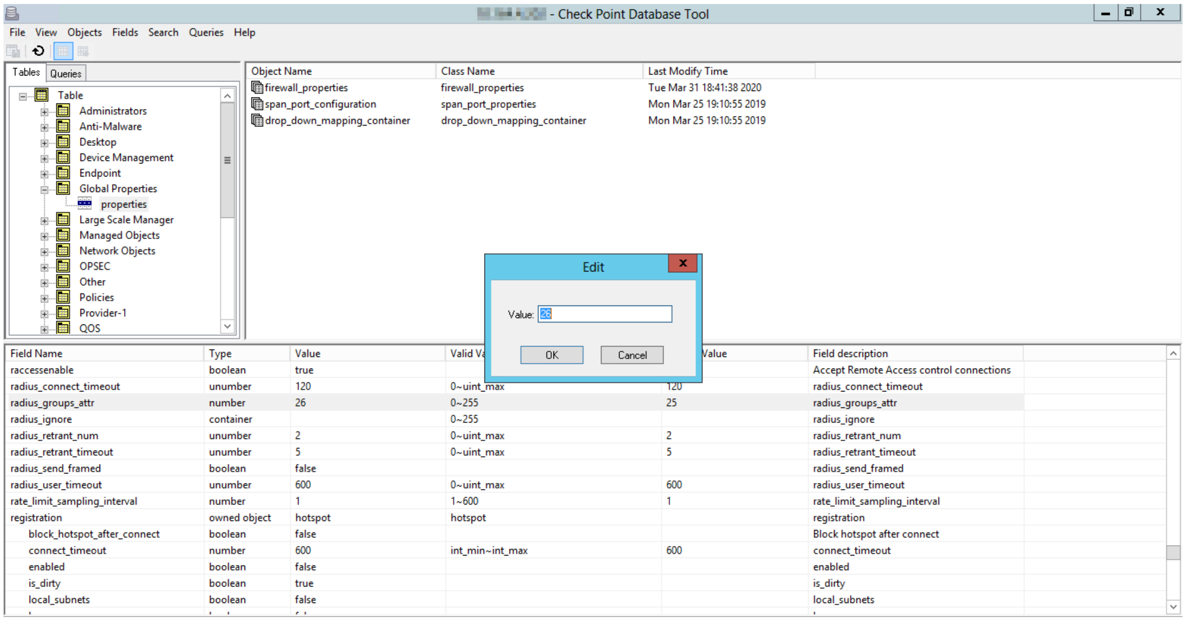


Object Name	Class Name	Last Modify Time
firewall_properties	firewall_properties	Tue Mar 31 18:41:38 2020
span_port_configuration	span_port_properties	Mon Mar 25 19:10:55 2019
drop_down_mapping_container	drop_down_mapping_container	Mon Mar 25 19:10:55 2019

Value: true

Field Name	Type	Value	Valid Va	Value	Field description
add_ip_alt_name_for_opsec_certs	boolean	false			add_ip_alt_name_for_opsec_certs
add_nt_groups	boolean	false			add_nt_groups
add_radius_groups	boolean	true			add_radius_groups
addresstrans	boolean	false			addresstrans
admin_expiration_global_data	owned object	admin_expiration_global_data	{admin_expiration_global_data,NULL}		admin_expiration_global_data
expiration_date	string	31-dec-2030		31-dec-2030	expiration_date
expiration_date_after_days	number	1200	int_min~int_max	1200	expiration_date_after_days
expiration_date_login_notif	boolean	true		true	expiration_date_login_notif
expiration_date_login_notif_days	number	30	int_min~int_max	30	expiration_date_login_notif_days
expiration_date_mail_notif	boolean	true		true	expiration_date_mail_notif
expiration_date_mail_notif_days	number	15	int_min~int_max	15	expiration_date_mail_notif_days
expiration_date_method	string	never	{expire after,expire at,never}	never	expiration_date_method
expiration_date_visual_notif	boolean	true		true	expiration_date_visual_notif
expiration_date_visual_notif_days	number	14	int_min~int_max	14	expiration_date_visual_notif_days
admin_lock_after_bad_attempts	unumber	3	1~30	3	admin_lock_after_bad_attempts

Change “radius_groups_attr” value from 25 to 26. Save your changes and exit GuiDBedit.

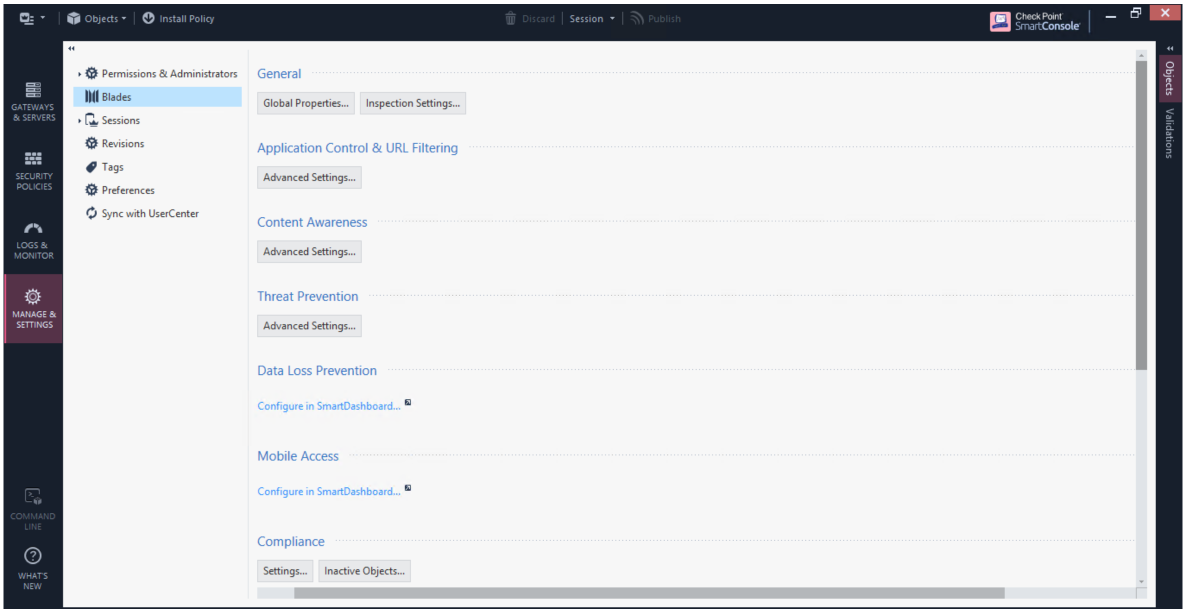


Object Name	Class Name	Last Modify Time
firewall_properties	firewall_properties	Tue Mar 31 18:41:38 2020
span_port_configuration	span_port_properties	Mon Mar 25 19:10:55 2019
drop_down_mapping_container	drop_down_mapping_container	Mon Mar 25 19:10:55 2019

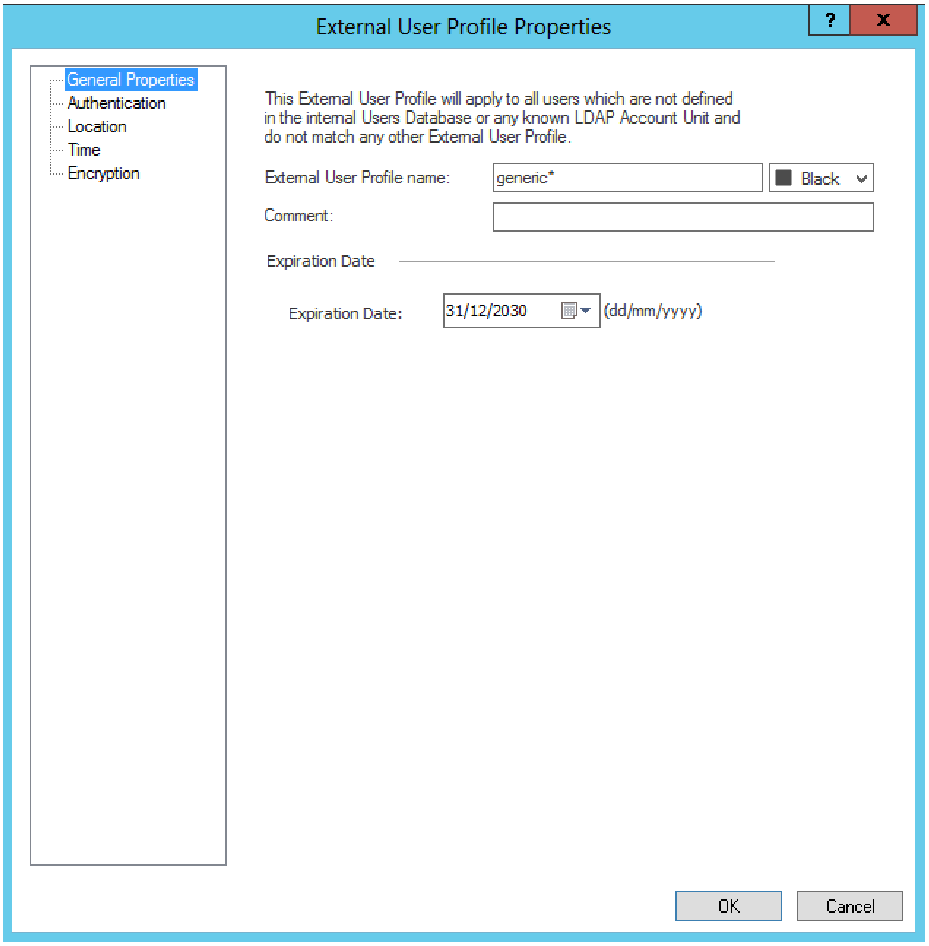
Value: 26

Field Name	Type	Value	Valid Va	Value	Field description
raccessenable	boolean	true			Accept Remote Access control connections
radius_connect_timeout	unumber	120	0~uint_max	120	radius_connect_timeout
radius_groups_attr	number	26	0~255	25	radius_groups_attr
radius_ignore	container		0~255		radius_ignore
radius_retrant_num	unumber	2	0~uint_max	2	radius_retrant_num
radius_retrant_timeout	unumber	5	0~uint_max	5	radius_retrant_timeout
radius_send_framed	boolean	false			radius_send_framed
radius_user_timeout	unumber	600	0~uint_max	600	radius_user_timeout
rate_limit_sampling_interval	number	1	1~600	1	rate_limit_sampling_interval
registration	owned object	hotspot	hotspot		registration
block_hotspot_after_connect	boolean	false			Block hotspot after connect
connect_timeout	number	600	int_min~int_max	600	connect_timeout
enabled	boolean	false			enabled
is_dirty	boolean	true			is_dirty
local_subnets	boolean	false			local_subnets

Open SmartConsole, click on “Manage & Settings”->”Blades”->“Configure in SmartDashboard…”.



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



This External User Profile will apply to all users which are not defined in the internal Users Database or any known LDAP Account Unit and do not match any other External User Profile.

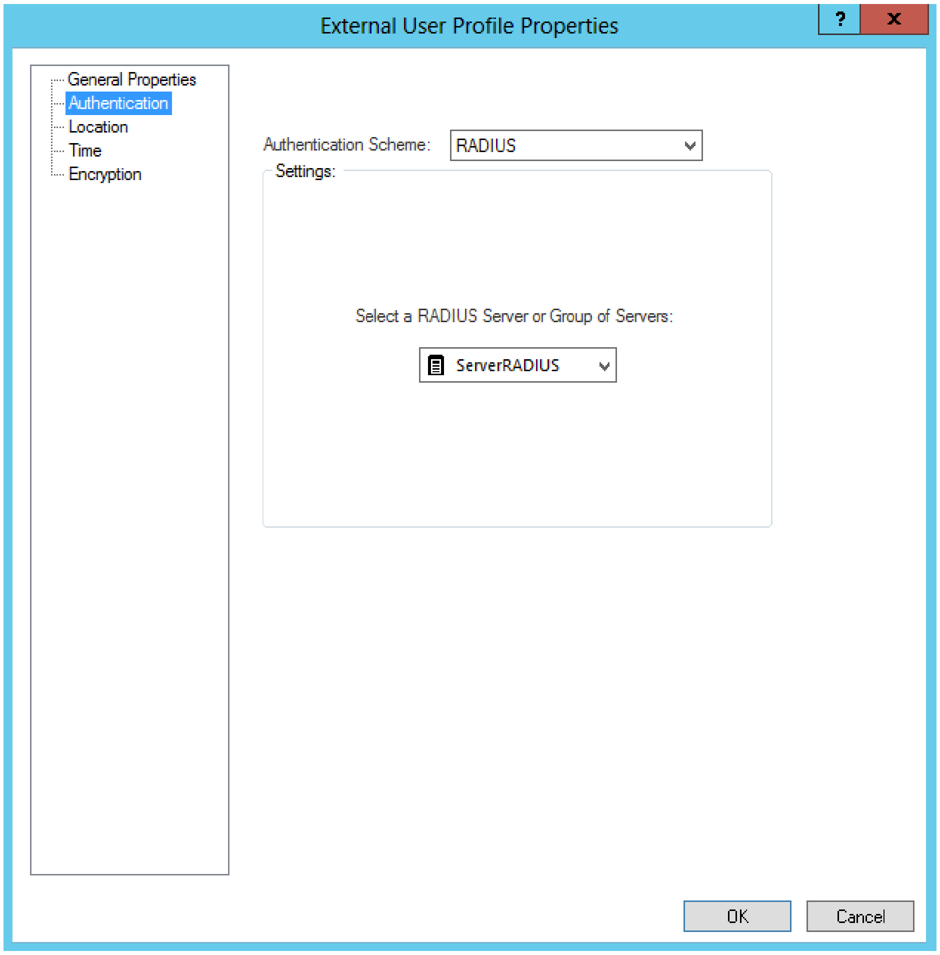
External User Profile name: generic* ■ Black

Comment:

Expiration Date

Expiration Date: 31/12/2030 (dd/mm/yyyy)

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



External User Profile Properties

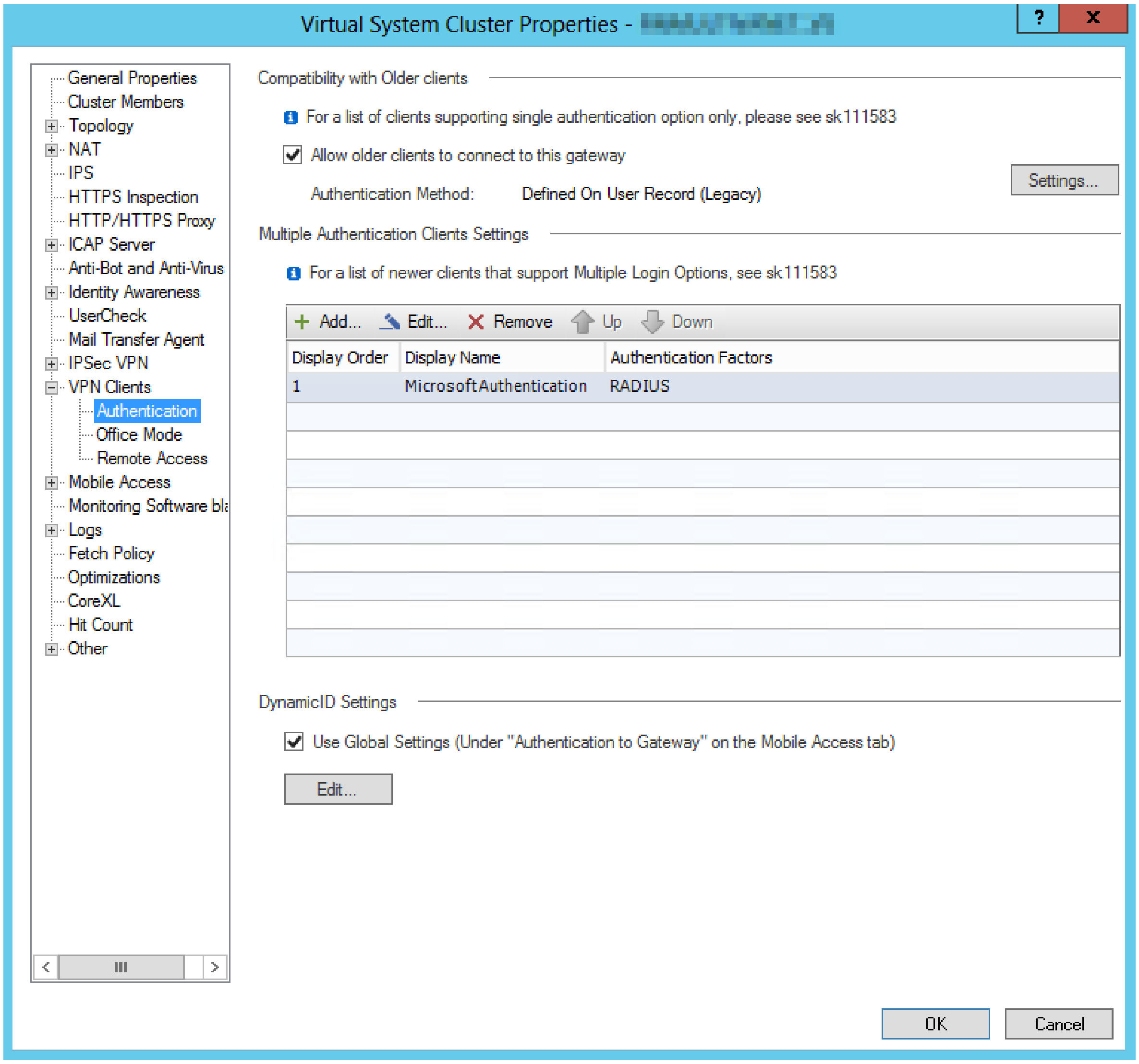
Authentication Scheme: RADIUS

Settings:

Select a RADIUS Server or Group of Servers: ServerRADIUS

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”.



Virtual System Cluster Properties - [redacted]

Compatibility with Older clients

For a list of clients supporting single authentication option only, please see sk111583

☑ Allow older clients to connect to this gateway

Authentication Method: Defined On User Record (Legacy)

Multiple Authentication Clients Settings

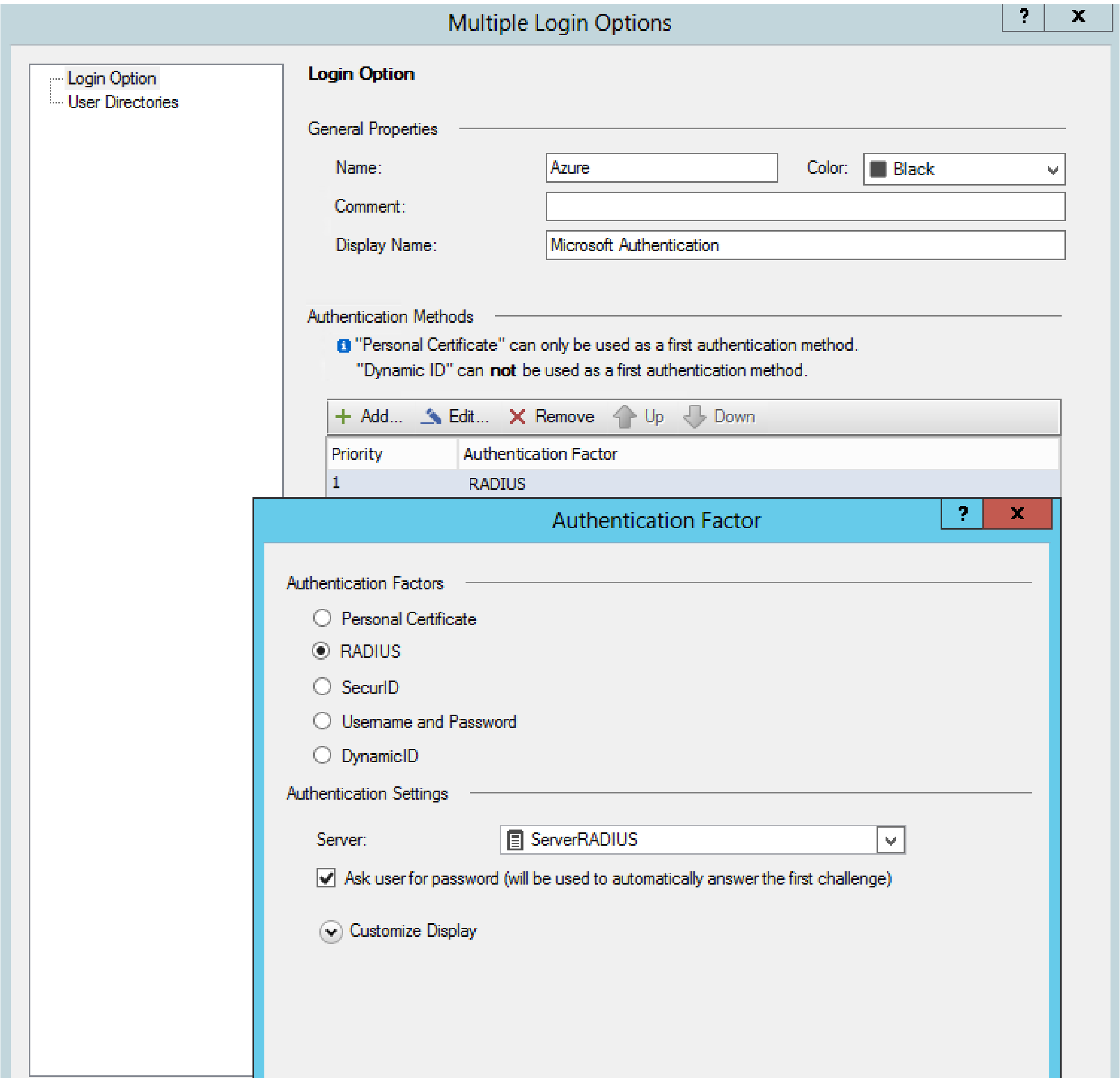
For a list of newer clients that support Multiple Login Options, see sk111583

Display Order	Display Name	Authentication Factors
1	MicrosoftAuthentication	RADIUS

DynamicID Settings

☑ Use Global Settings (Under "Authentication to Gateway" on the Mobile Access tab)

Configure a new “Multiple Authentication Clients Settings”, click “Add”->”New”. Type “Name” and “Display Name” and add a new “Authentication Methods”. Click “Add”, select “RADIUS” and then select the RADIUS server object you created. Select Ok and install policy.



Multiple Login Options

Login Option

General Properties

Name: Azure Color: Black

Comment:

Display Name: Microsoft Authentication

Authentication Methods

"Personal Certificate" can only be used as a first authentication method.
"Dynamic ID" can **not** be used as a first authentication method.

Priority	Authentication Factor
1	RADIUS

Authentication Factor

Authentication Factors

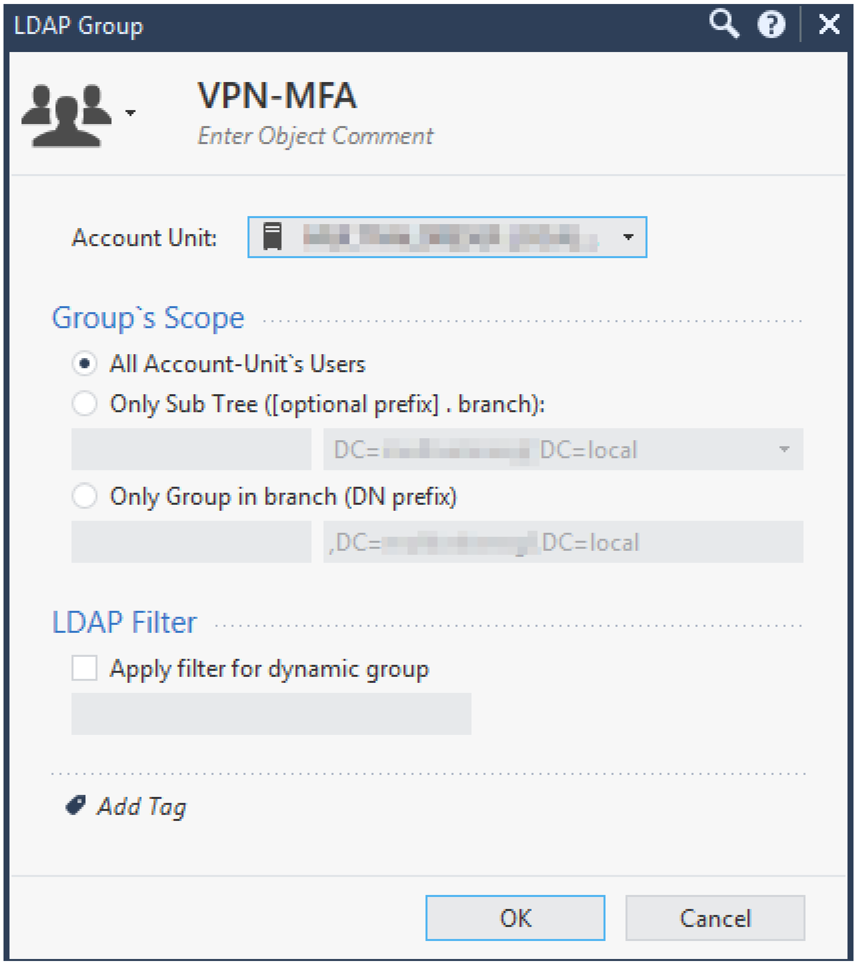
○ Personal Certificate
● RADIUS
○ SecurID
○ Username and Password
○ DynamicID

Authentication Settings

Server: ServerRADIUS

☑ Ask user for password (will be used to automatically answer the first challenge)

Create a new object as LDAP group for the entire domain or access roles for specific users, this to allow access to AD users. Select the account unit and select “All Account-Unit’s Users” option.



LDAP Group

VPN-MFA

Enter Object Comment

Account Unit: [redacted]

Group`s Scope

● All Account-Unit`s Users

○ Only Sub Tree ([optional prefix] . branch):

DC=[redacted] DC=local

○ Only Group in branch (DN prefix)

,DC=[redacted] DC=local

LDAP Filter

□ Apply filter for dynamic group

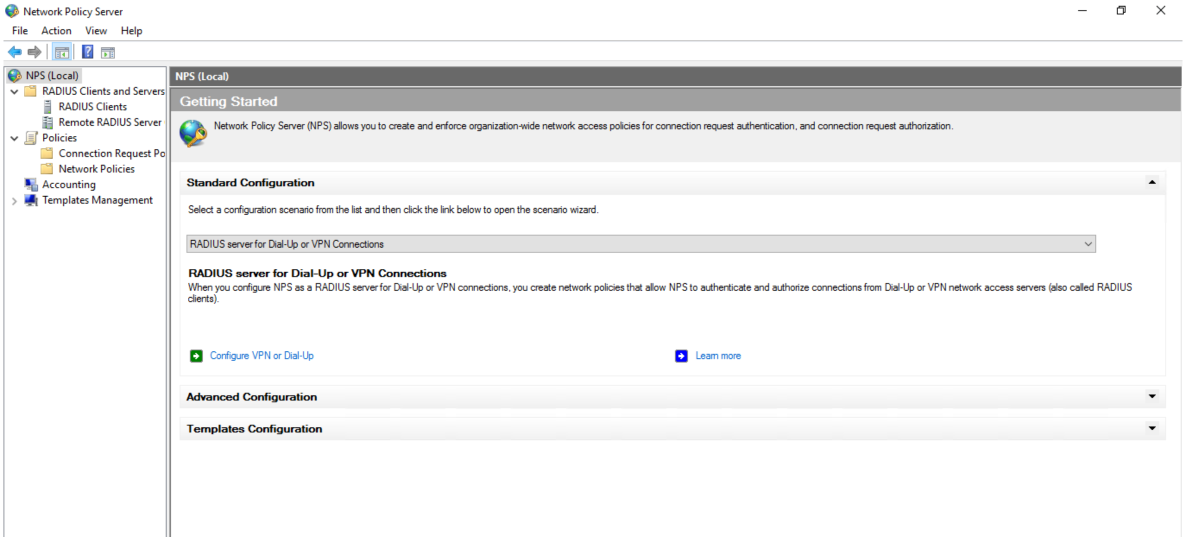
Add Tag

Add the LDAP group to community "Remote Access" how as "Participant User Group" and click ok. So, create a new rule in the FW or VS where the VPN users connect and how source select "Add Legacy User Access..." and select the LDAP group. Now can configure "Destination" and "Services & Applications" especifics.

Configurations Windows Server (NPS):

The Windows server must be 2008 R2 SP1 or above.

The server must be in the local domain, the NPS function is enabled in Server Manager select "Manage" -> "Add Roles and Features" -> "Role-based or feature-based installation" -> Select server-> continue with the installation steps for the Network Policy Server, after install NPS, open again Server Manager and select "Tools"->"Network Policy Server".



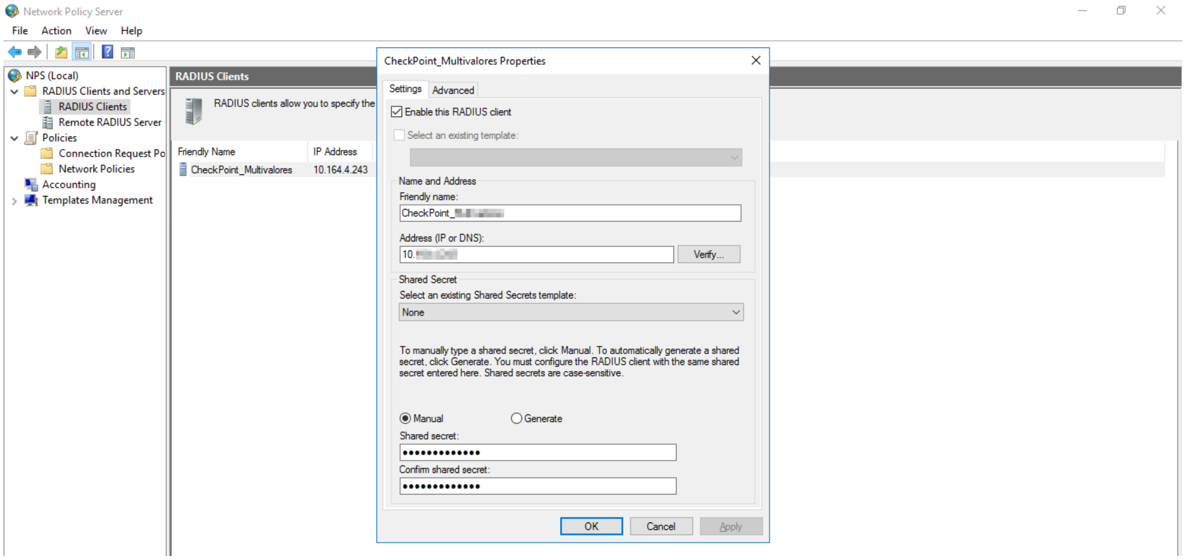
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

RADIUS server for Dial-Up or VPN Connections

RADIUS server for Dial-Up or VPN Connections
When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).

Select "RADIUS Clients", right click and select "New". In this case, the VS is active on member one of the cluster. In other words, that member of the cluster receives requests from VPN users, the internal IP corresponding to the FW will be configured with the VS active.



RADIUS clients allow you to specify the

Friendly Name	IP Address
CheckPoint_Multivalores	10.164.4.243

CheckPoint_Multivalores Properties

☑ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name: CheckPoint_[redacted]

Address (IP or DNS): 10.[redacted]

Shared Secret

Select an existing Shared Secrets template: None

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.

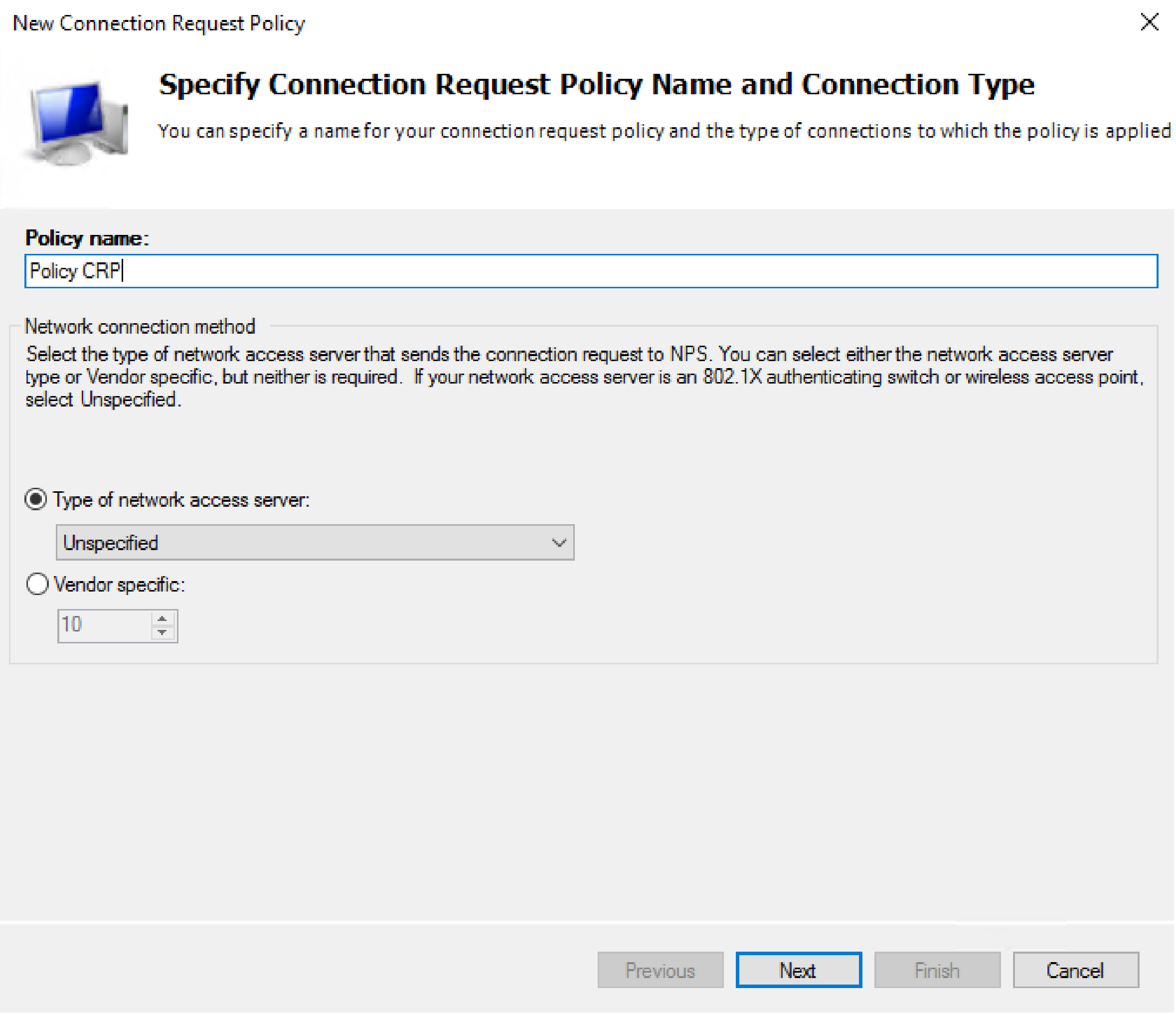
● Manual ○ Generate

Shared secret: •••••••••••••

Confirm shared secret: •••••••••••••

The shared secret is the same as when RADIUS object server is configured in Security Management Server. The vendor name in tab “Advanced” is “RADIUS Standard” and uncheck "Additional Options".

Over "Policies", right click in "Connection Request Policies" and click new, specify a name of policy and select "Type of network access server" how "Unspecified", and then next.



New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied

Policy name:

Policy CRP

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

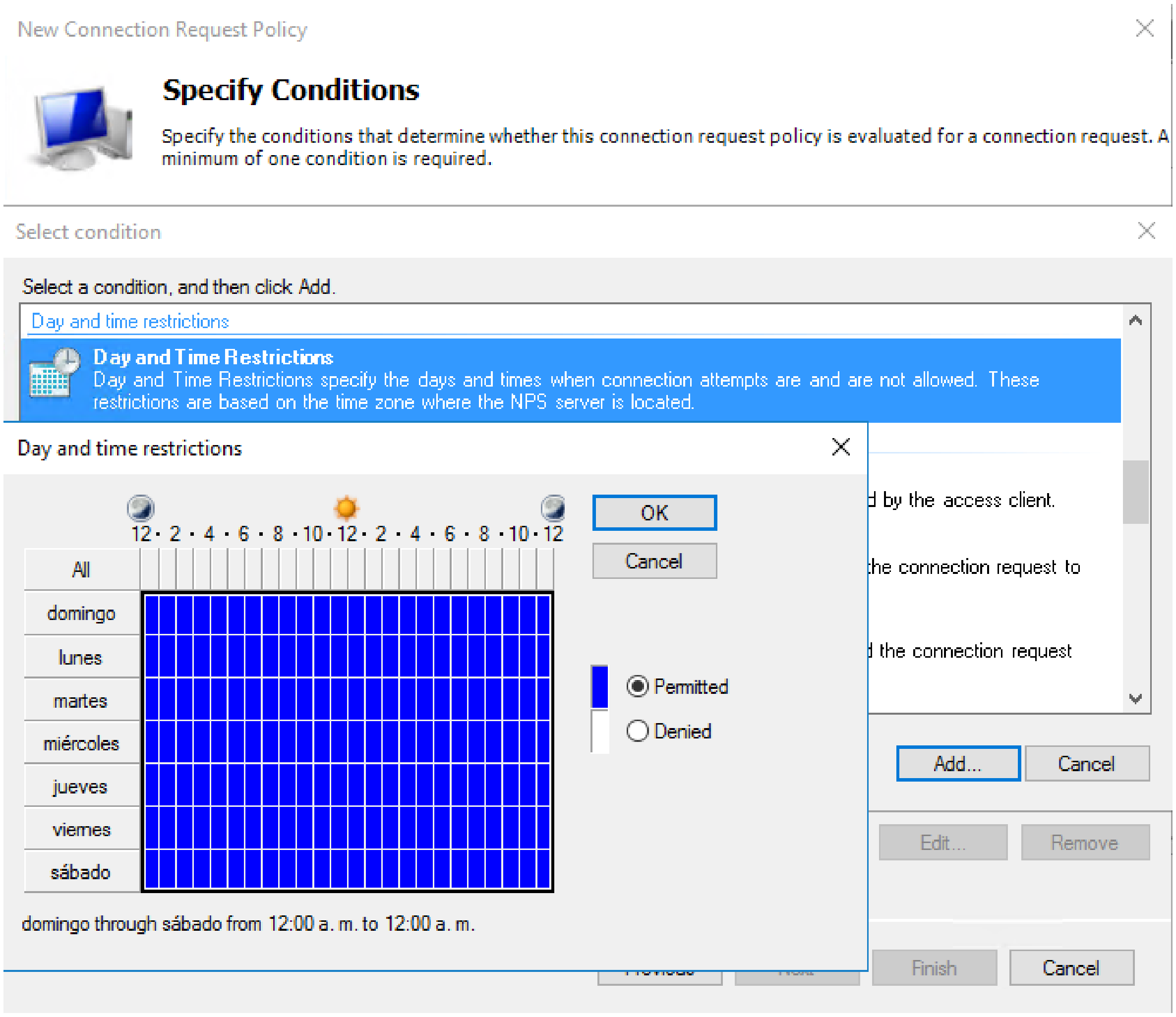
● Type of network access server:

Unspecified

○ Vendor specific:

10

Specify a condition or conditions for connection request, for this environment it was necessary to allow connections all day every day, click next.



New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.

Day and time restrictions

Day and Time Restrictions
Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

d by the access client.

the connection request to

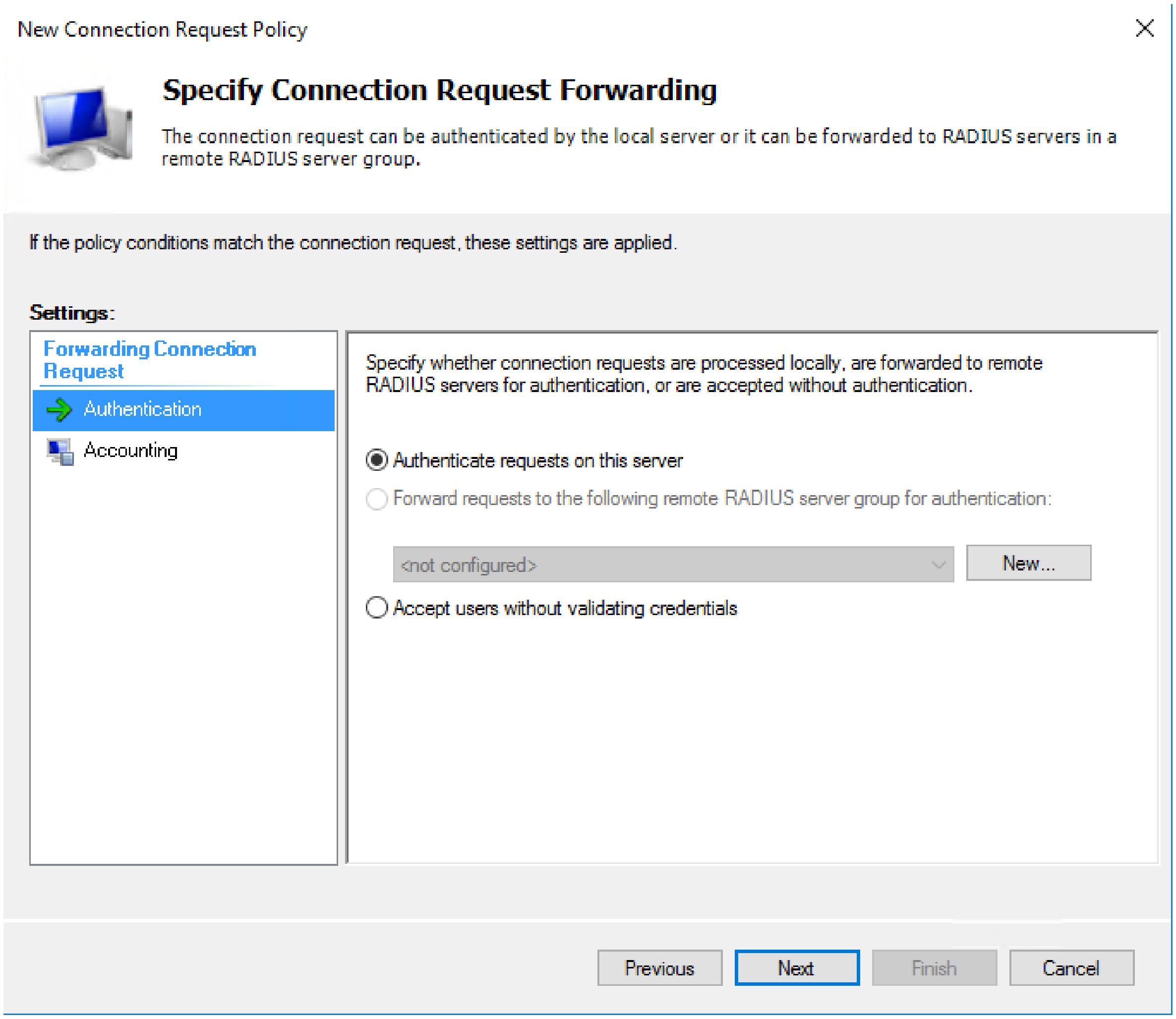
d the connection request

Day and time restrictions

● Permitted
○ Denied

domingo through sábado from 12:00 a. m. to 12:00 a. m.

In “Authentication” select “Authenticate request on this server” and next.



New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

● Authenticate requests on this server

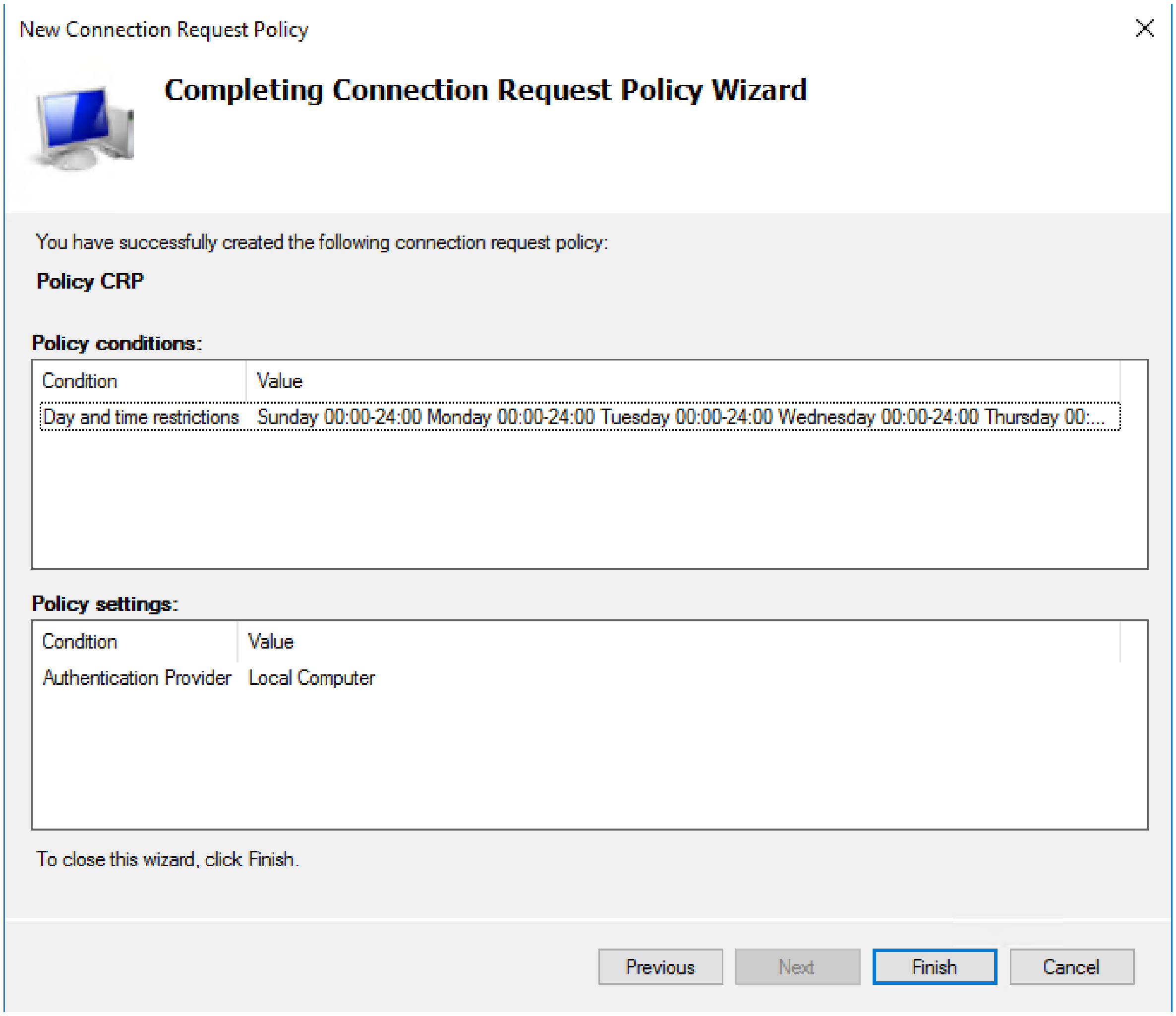
○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials

In “Specify Authentication Methods” and “Configure Settings” not select anything and click next in both windows.

This is the final Windows, click Finish.



New Connection Request Policy

Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

Policy CRP

Policy conditions:

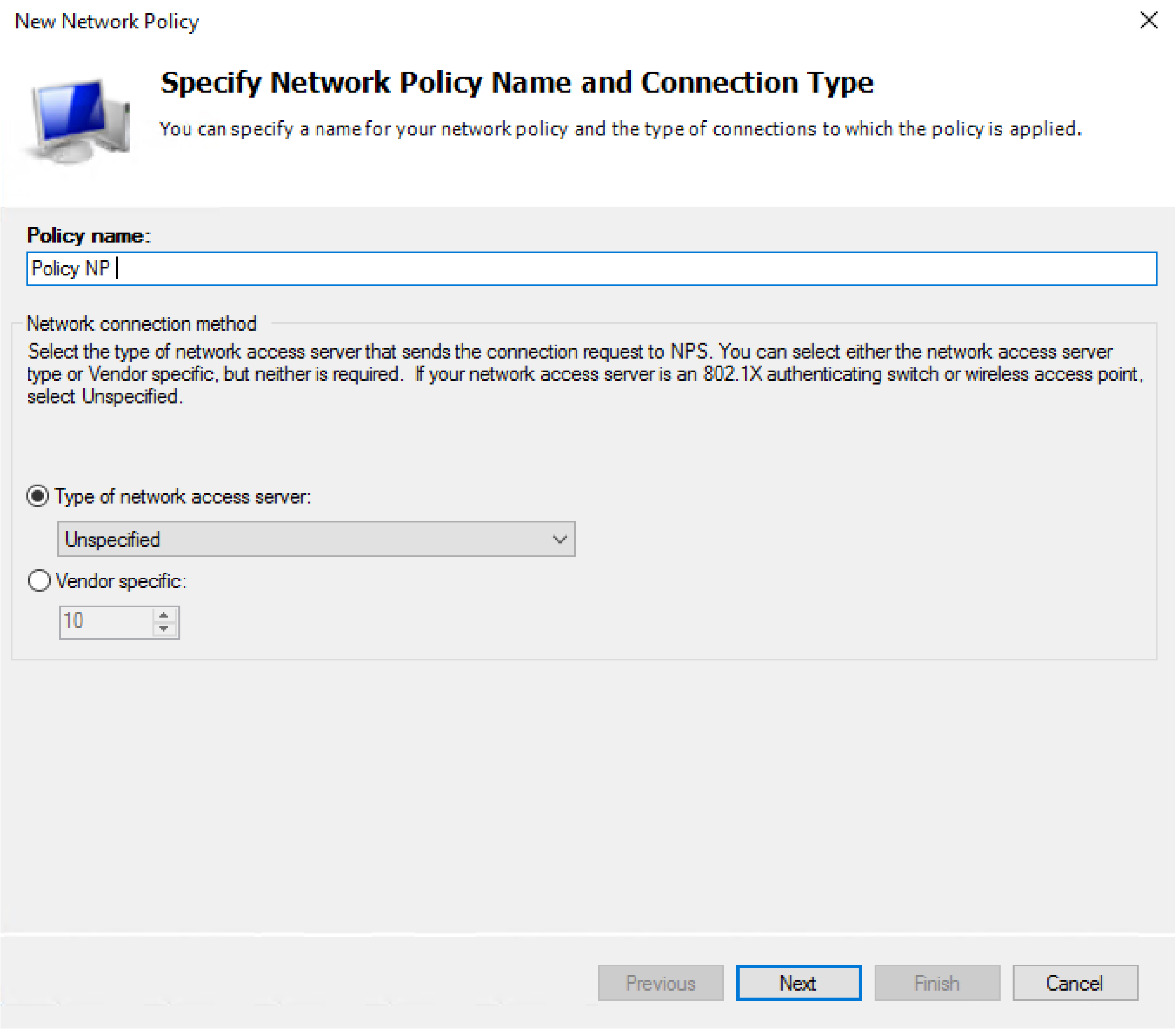
Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:...

Policy settings:

Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

In "Network Policies" right click, select "New", specify a name of policy and select "Type of network access server" how "Unspecified", and then next.



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.

Policy name:

Policy NP

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server:

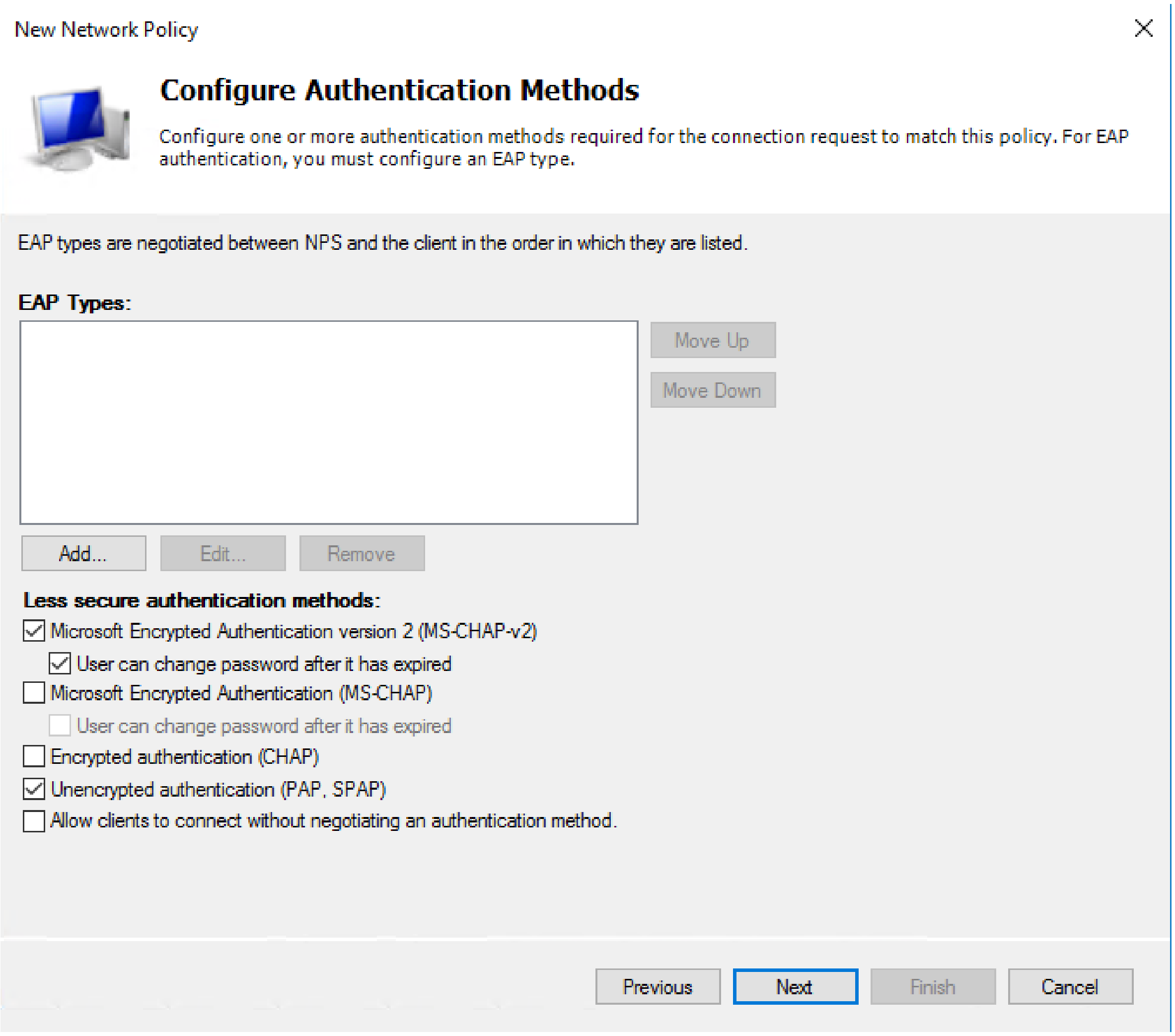
Unspecified

○ Vendor specific:

10

Add a condition or conditions configured in step before. Select “Access granted” and click next.

In window for select Authentication Methods select the protocol to be used for authentication, in this case is with “PAP” for authentication over SMS code.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

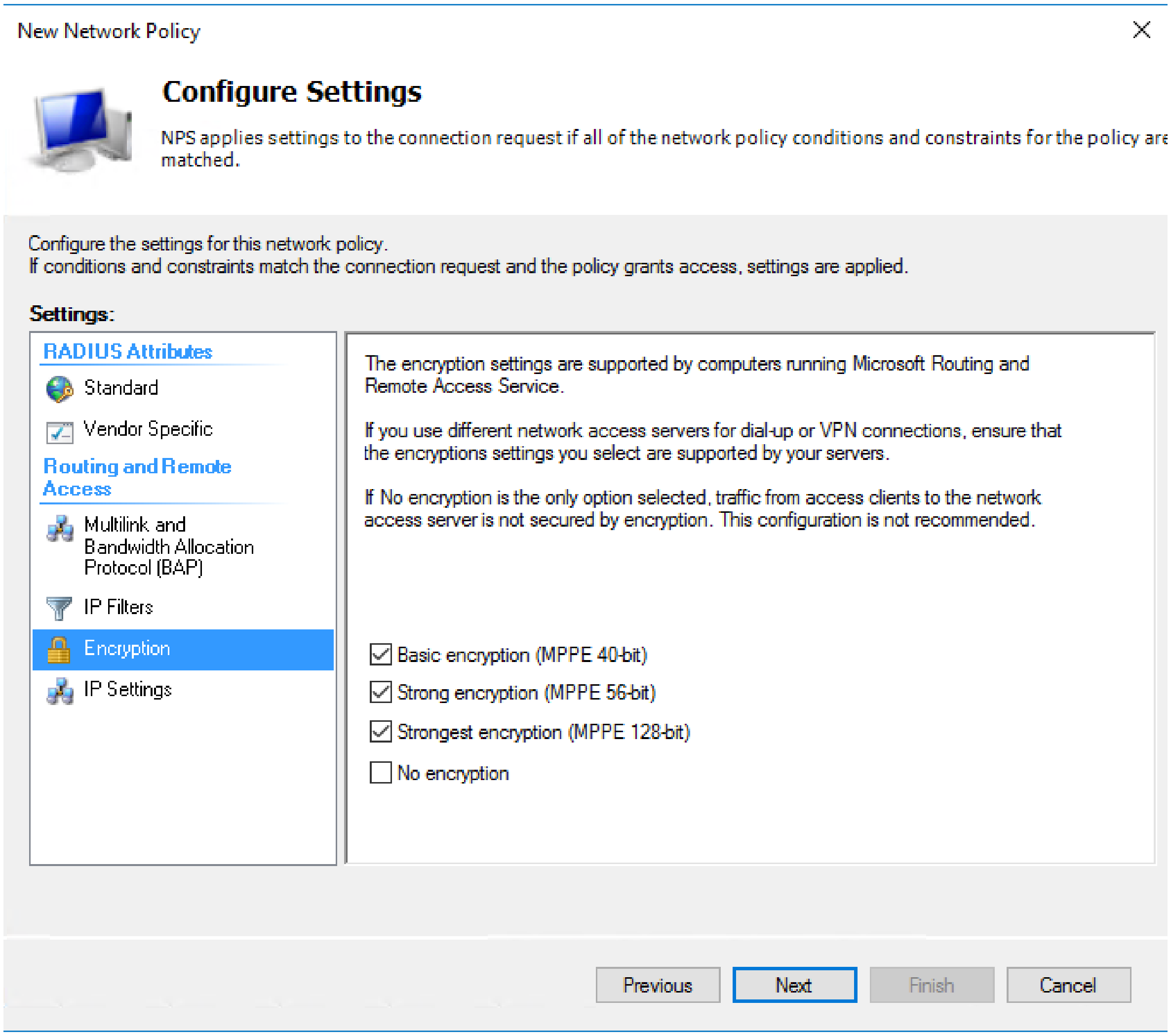
EAP Types:

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☑ User can change password after it has expired
☐ Microsoft Encrypted Authentication (MS-CHAP)
☐ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☑ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.

Click next and change the "Idle Timeout" and "Session Timeout" value to a value considered to the environment.

In Encryption check all options, exception the last option, uncheck “No encryption”.



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings

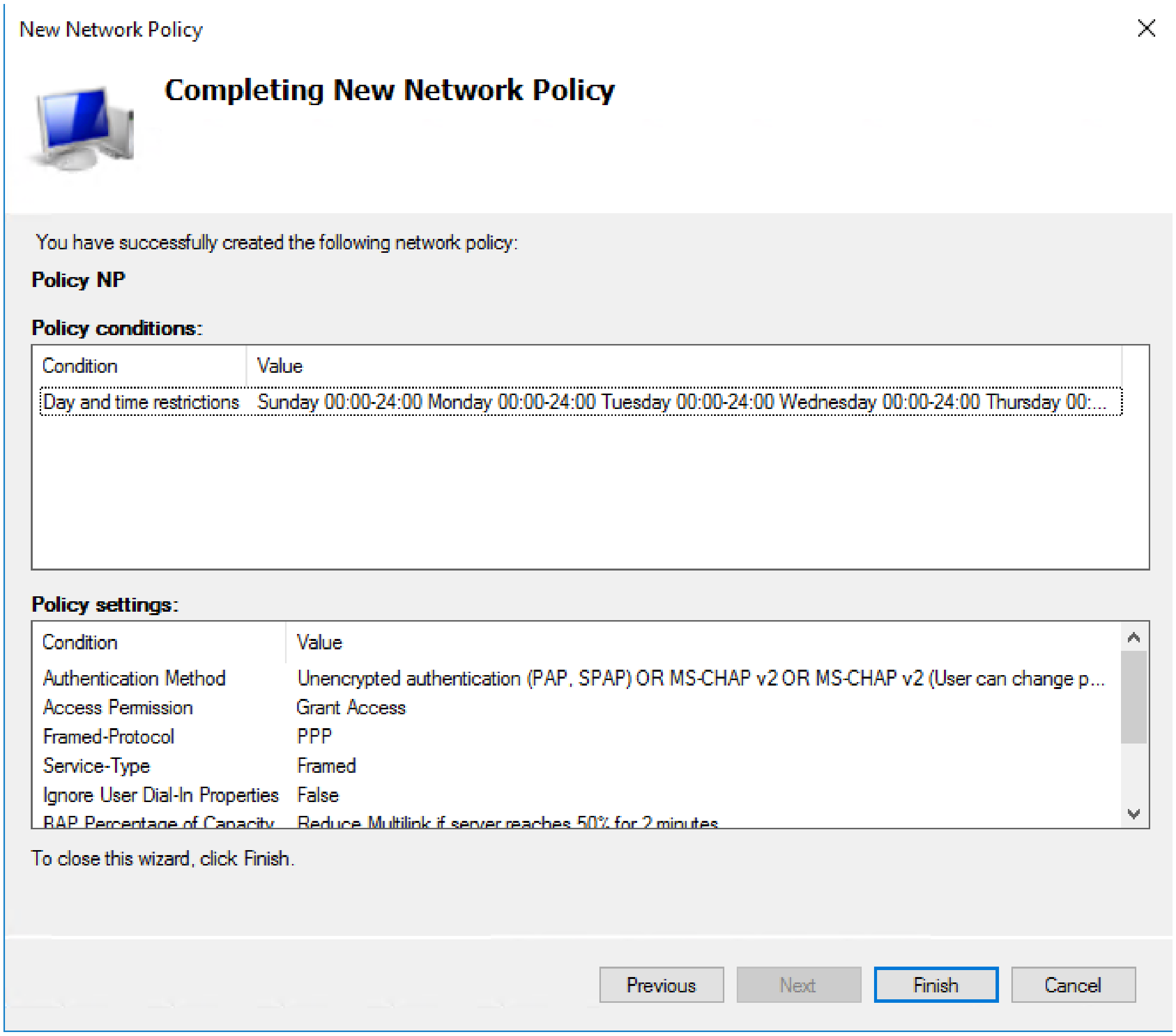
The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryptions settings you select are supported by your servers.

If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

☑ Basic encryption (MPPE 40-bit)
☑ Strong encryption (MPPE 56-bit)
☑ Strongest encryption (MPPE 128-bit)
☐ No encryption

This is the last window, click Finish.



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Policy NP

Policy conditions:

Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:...

Policy settings:

Condition	Value
Authentication Method	Unencrypted authentication (PAP, SPAP) OR MS-CHAP v2 OR MS-CHAP v2 (User can change p...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

To close this wizard, click Finish.

Configurations NPS Extension for Azure MFA:

The following is required for the server NPS:

- Windows Server 2008 R2 SP1 or above
- Directory ID from Azure tenant
- Communication with the next URLs over ports 80 and 443
  - https://adnotifications.windowsazure.com
  - https://login.microsoftonline.com
  - https://credentials.azure.com
  - https://provisioningapi.microsoftonline.com
  - https://aadcdn.msauth.net

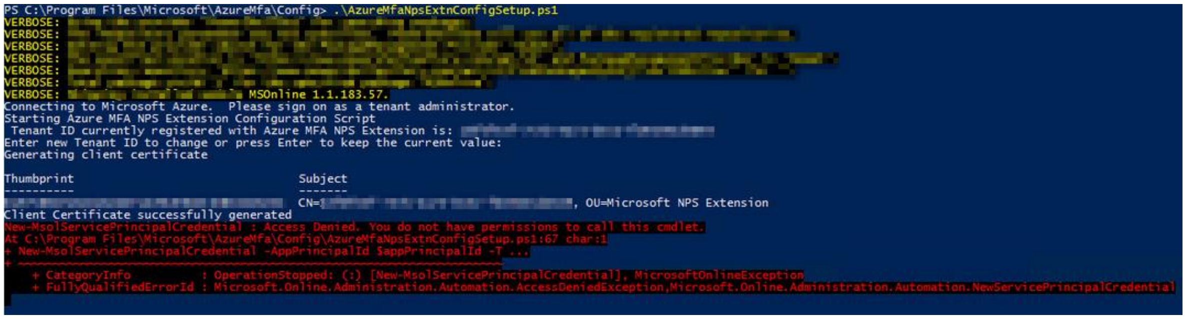
In the same windows server where was installed NPS, download the extension for Azure MFA in the official site from Microsoft and execute the "setup.exe". Run the script “.\AzureMfaNpsExtnConfigSetup.ps1” in "C:\Program Files\Microsoft\AzureMfa\Config", in PowerShell as admin.

This script performs:

- Create a self-signed certificate.
- Associate the public key of the certificate with the service entity in Azure AD.
- Store the certificate in the certificate store on the local computer.
- Grant access to the certificate's private key to the network user.
- Restart NPS.

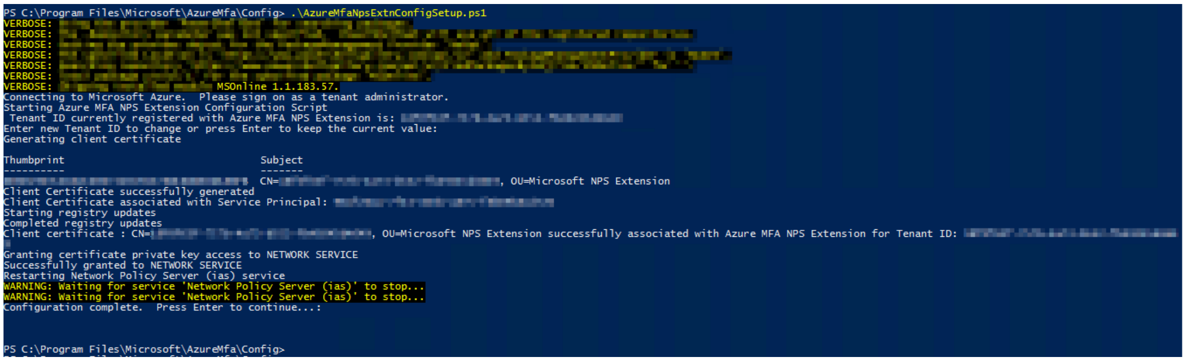
Log into Azure AD as admin, enter Azure Directory ID.

Note: If you do not enter the credentials as administrator, you will get an error like the following:



```
PS C:\Program Files\Microsoft\AzureMfa\Config> .\AzureMfaNpsExtnConfigSetup.ps1
VERBOSE: [redacted]
VERBOSE:
VERBOSE:
VERBOSE:
VERBOSE:
VERBOSE:
VERBOSE: [redacted] MSOnline 1.1.183.57.
Connecting to Microsoft Azure.  Please sign on as a tenant administrator.
Starting Azure MFA NPS Extension Configuration Script
 Tenant ID currently registered with Azure MFA NPS Extension is: [redacted]
Enter new Tenant ID to change or press Enter to keep the current value:
Generating client certificate

Thumbprint                                Subject
----------                                -------
[redacted]                                CN=[redacted], OU=Microsoft NPS Extension
Client Certificate successfully generated
New-MsolServicePrincipalCredential : Access Denied. You do not have permissions to call this cmdlet.
At C:\Program Files\Microsoft\AzureMfa\Config\AzureMfaNpsExtnConfigSetup.ps1:67 char:1
+ New-MsolServicePrincipalCredential -AppPrincipalId $appPrincipalId -T ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationStopped: (:) [New-MsolServicePrincipalCredential], MicrosoftOnlineException
    + FullyQualifiedErrorId : Microsoft.Online.Administration.Automation.AccessDeniedException,Microsoft.Online.Administration.Automation.NewServicePrincipalCredential
```

The successful setup looks like this:

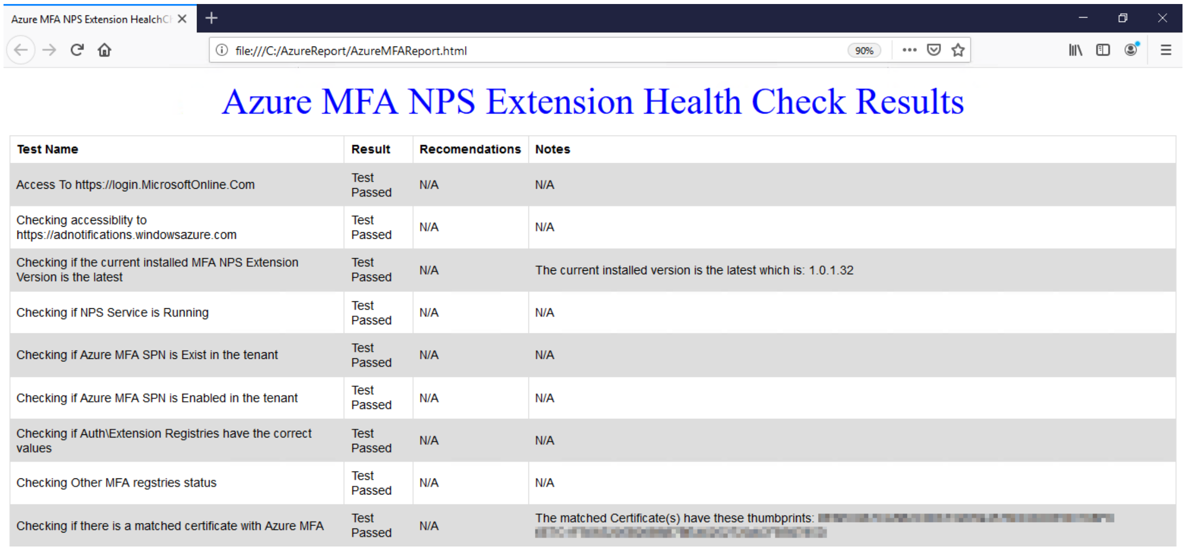


```
PS C:\Program Files\Microsoft\AzureMfa\Config> .\AzureMfaNpsExtnConfigSetup.ps1
VERBOSE: [redacted]
VERBOSE: [redacted]
VERBOSE: [redacted]
VERBOSE: [redacted]
VERBOSE: [redacted]
VERBOSE: [redacted]
VERBOSE: [redacted] MSOnline 1.1.183.57.
Connecting to Microsoft Azure.  Please sign on as a tenant administrator.
Starting Azure MFA NPS Extension Configuration Script
 Tenant ID currently registered with Azure MFA NPS Extension is: [redacted]
Enter new Tenant ID to change or press Enter to keep the current value:
Generating client certificate

Thumbprint                                Subject
----------                                -------
[redacted]                                CN=[redacted], OU=Microsoft NPS Extension
Client Certificate successfully generated
Client Certificate associated with Service Principal: [redacted]
Starting registry updates
Completed registry updates
Client certificate : CN=[redacted], OU=Microsoft NPS Extension successfully associated with Azure MFA NPS Extension for Tenant ID: [redacted]

Granting certificate private key access to NETWORK SERVICE
Successfully granted to NETWORK SERVICE
Restarting Network Policy Server (ias) service
WARNING: Waiting for service 'Network Policy Server (ias)' to stop...
WARNING: Waiting for service 'Network Policy Server (ias)' to stop...
Configuration complete.  Press Enter to continue...:


PS C:\Program Files\Microsoft\AzureMfa\Config>
```

Note: It is recommended to update MSOnline to its latest version 1.1.183.57.

In case the connection is not successful, there is a validation script which indicates where is the problem for which the successful connection was not achieved. This script belongs to Microsoft and will be located in the references, the steps to follow are in the link.

That is the result of Azure MFA NPS extension health check script.



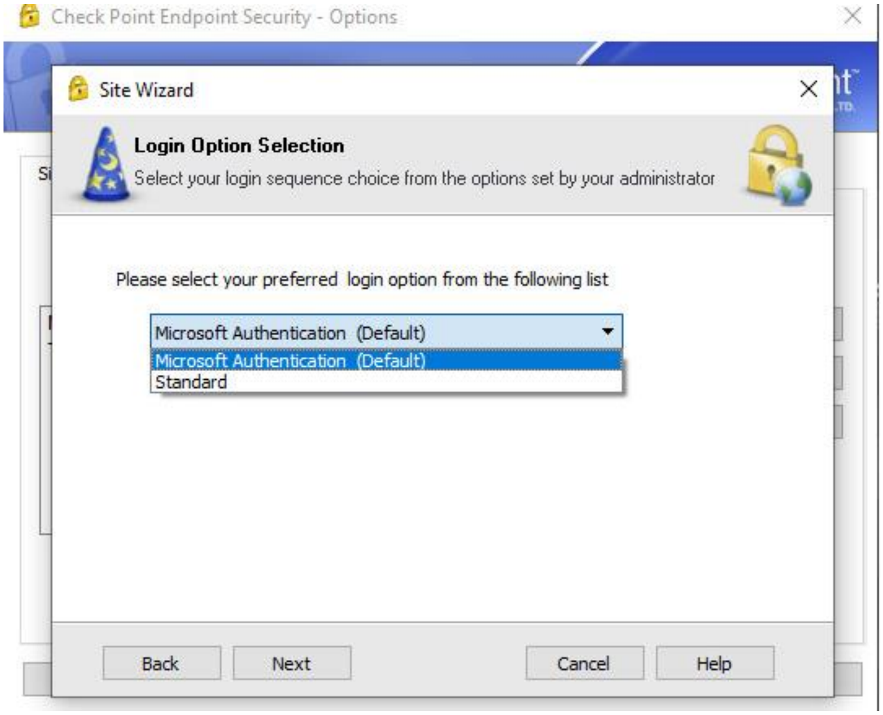
Azure MFA NPS Extension HealthC
file:///C:/AzureReport/AzureMFAReport.html
90%

Azure MFA NPS Extension Health Check Results

Test Name	Result	Recomendations	Notes
Access To https://login.MicrosoftOnline.Com	Test Passed	N/A	N/A
Checking accessiblity to https://adnotifications.windowsazure.com	Test Passed	N/A	N/A
Checking if the current installed MFA NPS Extension Version is the latest	Test Passed	N/A	The current installed version is the latest which is: 1.0.1.32
Checking if NPS Service is Running	Test Passed	N/A	N/A
Checking if Azure MFA SPN is Exist in the tenant	Test Passed	N/A	N/A
Checking if Azure MFA SPN is Enabled in the tenant	Test Passed	N/A	N/A
Checking if Auth\Extension Registries have the correct values	Test Passed	N/A	N/A
Checking Other MFA regstries status	Test Passed	N/A	N/A
Checking if there is a matched certificate with Azure MFA	Test Passed	N/A	The matched Certificate(s) have these thumbprints: [redacted]

Configurations EndPoint Security VPN:

When enabled "Multiple Login Options" in the FW or VS. In the agent appears different manners for configure the agent when crate a new site, in this case appear the option configured before on the VS when create a new site.



Login Option Selection

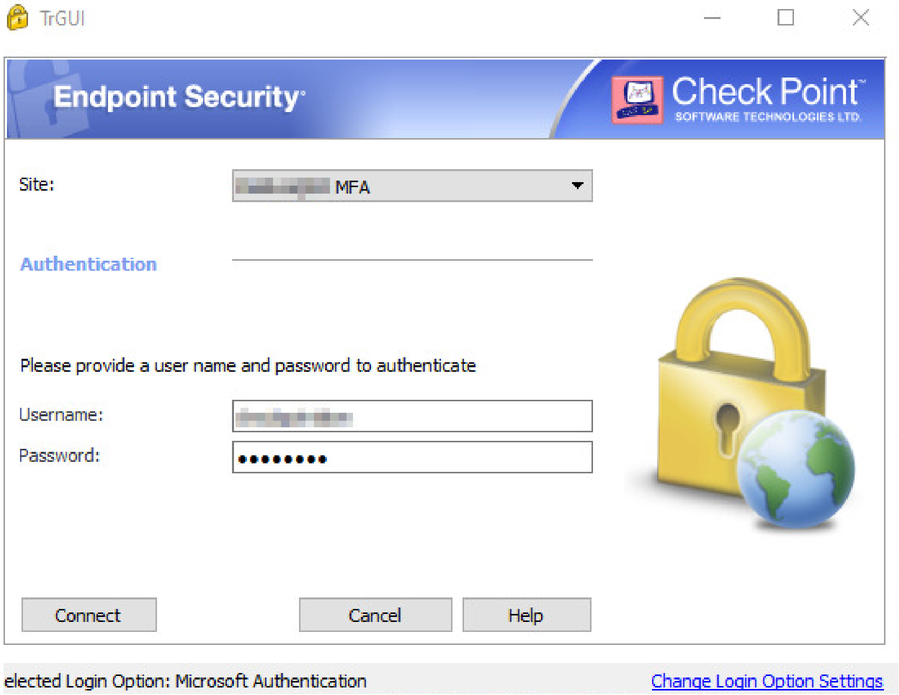
Select your login sequence choice from the options set by your administrator

Please select your preferred login option from the following list

Microsoft Authentication (Default)

Microsoft Authentication (Default)
Standard

Since the site is created with the Microsoft authentication option selected, the local AD user and password are entered.



Site: [redacted] MFA

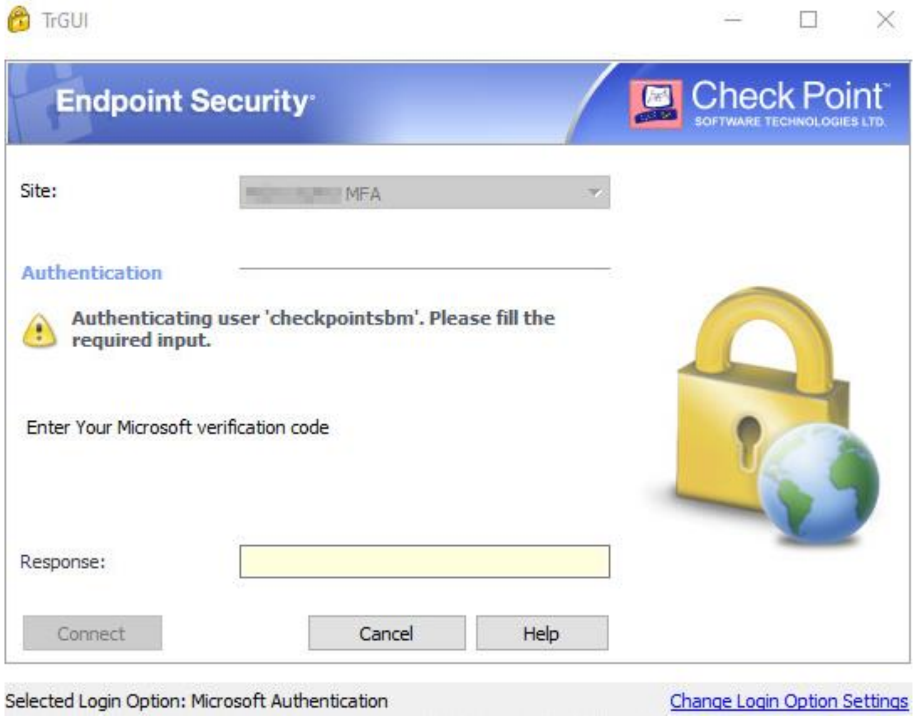
Please provide a user name and password to authenticate

Username: [redacted]

Password: ••••••••

elected Login Option: Microsoft Authentication

A new window appears waiting for the entry of the SMS code sent to the previously configured phone number.



Site: [redacted] MFA

Authentication

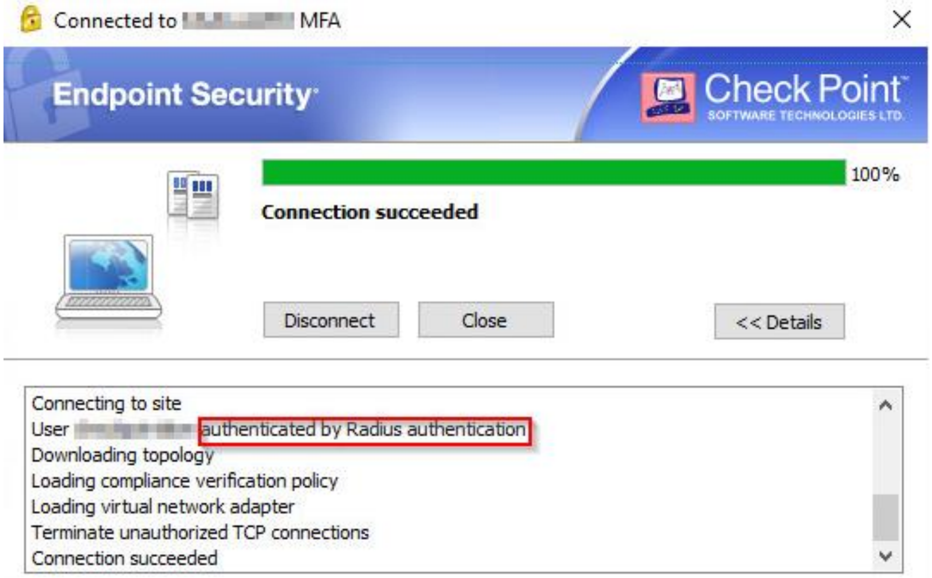
Authenticating user 'checkpointsbm'. Please fill the required input.

Enter Your Microsoft verification code

Response:

Selected Login Option: Microsoft Authentication

When entering the SMS code, the connection is successfull and appears in details that the user authenticated with Radius.



Connected to [redacted] MFA

Connection succeeded

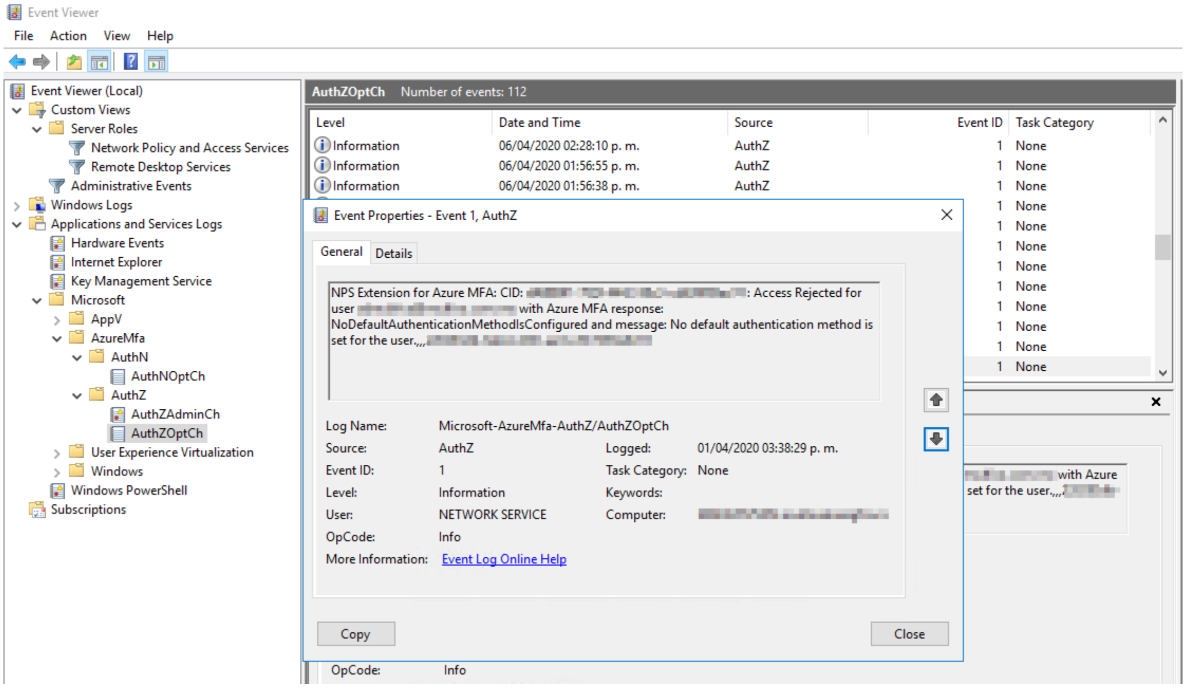
```
Connecting to site
User [redacted] authenticated by Radius authentication
Downloading topology
Loading compliance verification policy
Loading virtual network adapter
Terminate unauthorized TCP connections
Connection succeeded
```

Logs:

NPS logs are seen in "Event Viewer" under "Server Roles" -> "Network Policy and Access Services" and "Applications and Services Logs"->"Microsoft"->"AzureMfa"->"AuthN" and "AuthZ".

These are examples of errors that happened:

This error refers to the fact that there is no double factor authentication method for the user with which to log in. It is solved by verifying that the user is licensed in Azure AD and configuring MFA to the user in office 365.



Level	Date and Time	Source	Event ID	Task Category
Information	06/04/2020 02:28:10 p. m.	AuthZ	1	None
Information	06/04/2020 01:56:55 p. m.	AuthZ	1	None
Information	06/04/2020 01:56:38 p. m.	AuthZ	1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None

Event Properties - Event 1, AuthZ

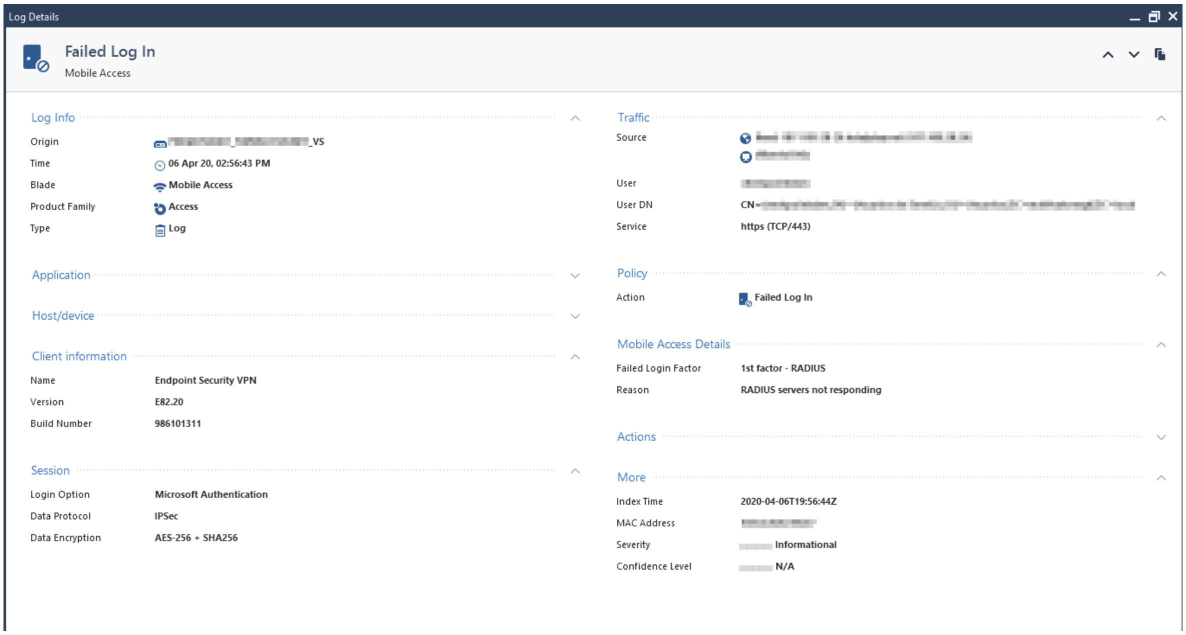
```
NPS Extension for Azure MFA: CID: [redacted]: Access Rejected for
user [redacted] with Azure MFA response:
NoDefaultAuthenticationMethodIsConfigured and message: No default authentication method is
set for the user.,,,[redacted]
```

Log Name:	Microsoft-AzureMfa-AuthZ/AuthZOptCh		
Source:	AuthZ	Logged:	01/04/2020 03:38:29 p. m.
Event ID:	1	Task Category:	None
Level:	Information	Keywords:	
User:	NETWORK SERVICE	Computer:	[redacted]
OpCode:	Info		
More Information:	Event Log Online Help		

[redacted] with Azure
set for the user.,,,[redacted]

OpCode: Info

When the NPS fails to authenticate, it is recommended to review the selected protocol and keep in mind that MS-CHAPv2 only authenticates by phone call and codes through apps, in the FW the log appears as:



Log Info

Origin	[redacted]_VS
Time	06 Apr 20, 02:56:43 PM
Blade	Mobile Access
Product Family	Access
Type	Log

Application

Host/device

Client information

Name	Endpoint Security VPN
Version	E82.20
Build Number	986101311

Session

Login Option	Microsoft Authentication
Data Protocol	IPSec
Data Encryption	AES-256 + SHA256

Traffic

Source	[redacted] [redacted]
User	[redacted]
User DN	CN=[redacted]
Service	https (TCP/443)

Policy

Action	Failed Log In

Mobile Access Details

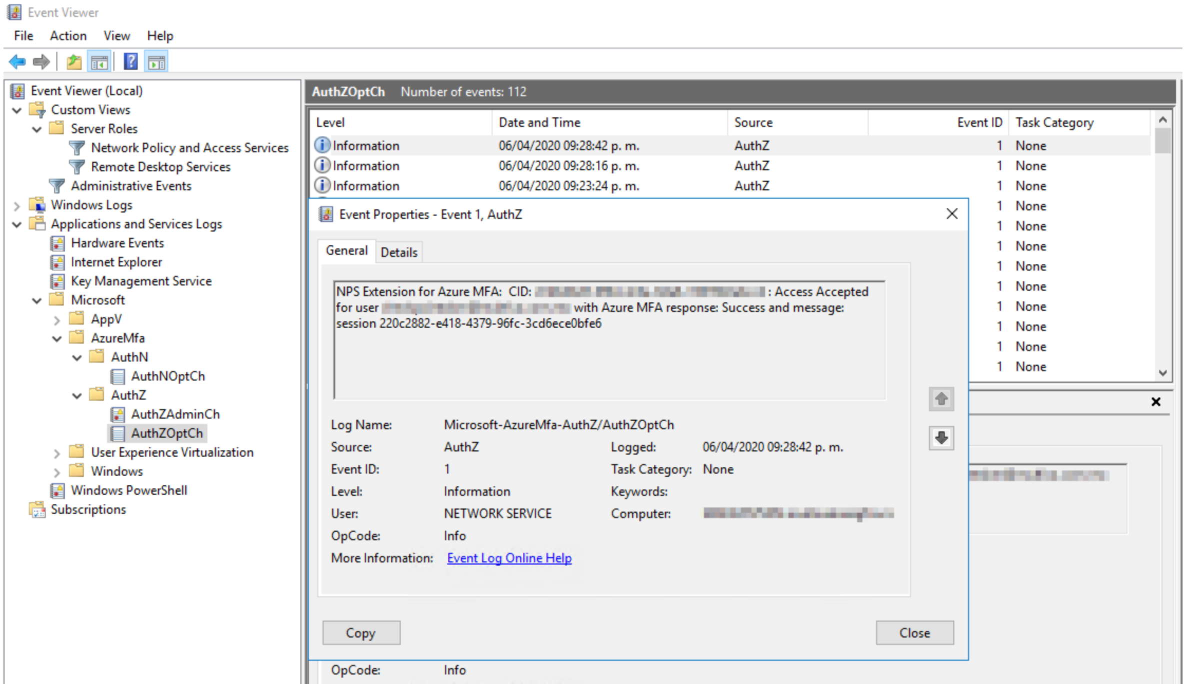
Failed Login Factor	1st factor - RADIUS
Reason	RADIUS servers not responding

Actions

More

Index Time	2020-04-06T19:56:44Z
MAC Address	[redacted]
Severity	Informational
Confidence Level	N/A

The log indicating that the authentication was successful in NPS is as follows:



AuthZOptCh Number of events: 112

Level	Date and Time	Source	Event ID	Task Category
Information	06/04/2020 09:28:42 p. m.	AuthZ	1	None
Information	06/04/2020 09:28:16 p. m.	AuthZ	1	None
Information	06/04/2020 09:23:24 p. m.	AuthZ	1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None
			1	None

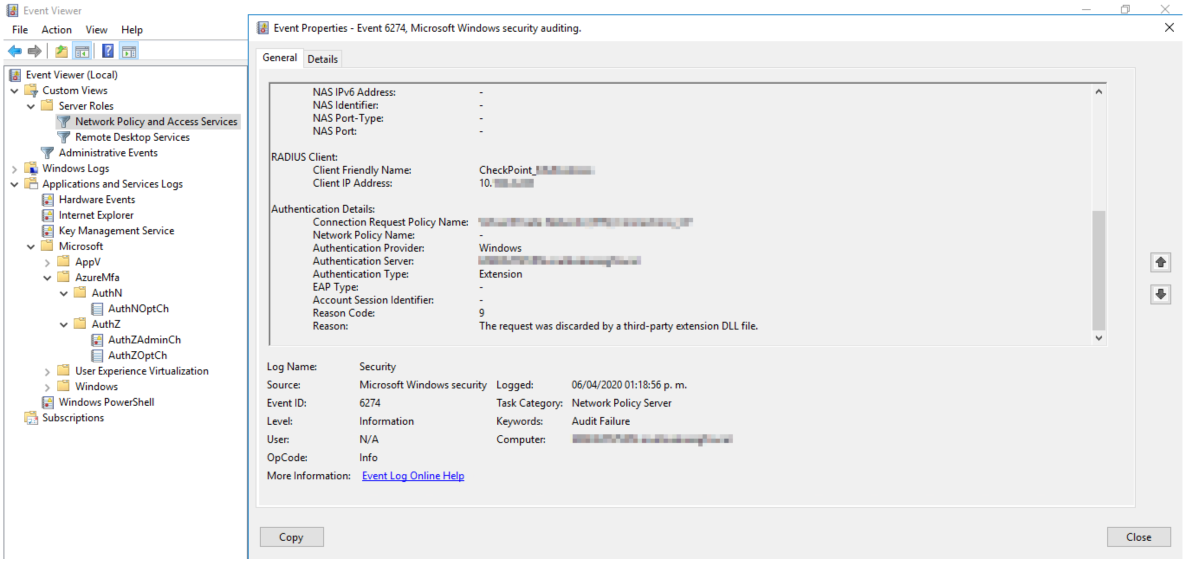
Event Properties - Event 1, AuthZ

NPS Extension for Azure MFA: CID: [redacted] : Access Accepted for user [redacted] with Azure MFA response: Success and message: session 220c2882-e418-4379-96fc-3cd6ece0bfe6

Log Name:	Microsoft-AzureMfa-AuthZ/AuthZOptCh		
Source:	AuthZ	Logged:	06/04/2020 09:28:42 p. m.
Event ID:	1	Task Category:	None
Level:	Information	Keywords:	
User:	NETWORK SERVICE	Computer:	[redacted]
OpCode:	Info		
More Information:	Event Log Online Help		

OpCode: Info

When you don't create the rule in the FW to allow access to users belonging to the AD, the following log in the NPS appears "Network Policy Server discarded the request for a user"...

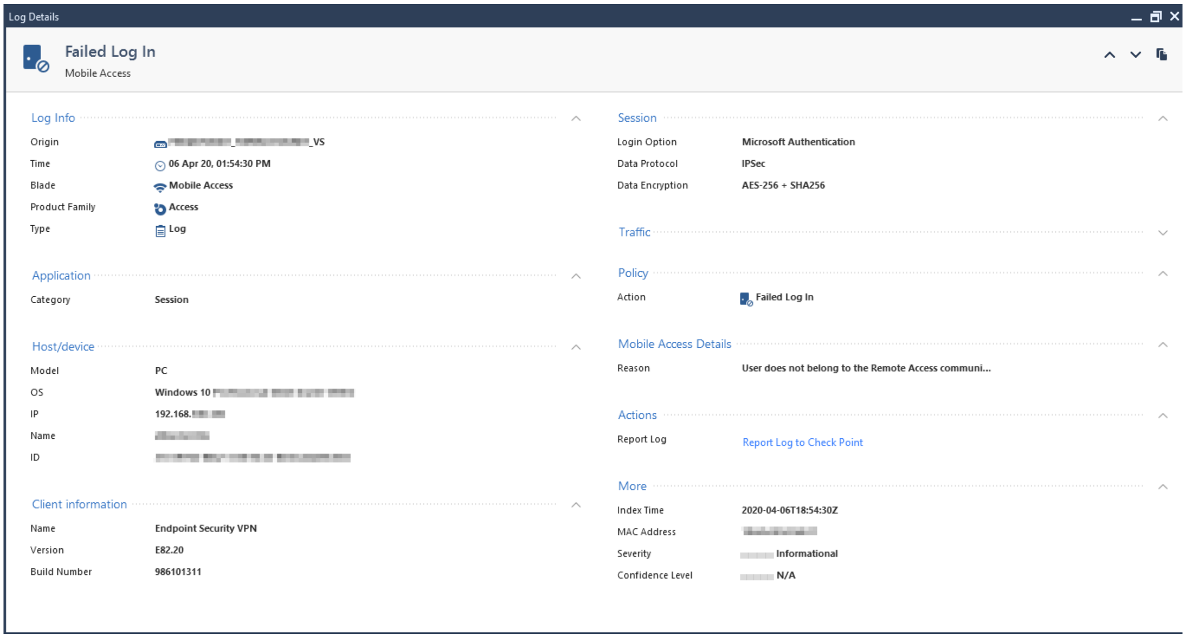


Event Properties - Event 6274, Microsoft Windows security auditing.

```
        NAS IPv6 Address:               -
        NAS Identifier:                 -
        NAS Port-Type:                  -
        NAS Port:                       -

RADIUS Client:
        Client Friendly Name:           CheckPoint_[redacted]
        Client IP Address:              10.[redacted]

Authentication Details:
        Connection Request Policy Name: [redacted]
        Network Policy Name:            -
        Authentication Provider:        Windows
        Authentication Server:          [redacted]
        Authentication Type:            Extension
        EAP Type:                       -
        Account Session Identifier:     -
        Reason Code:                    9
        Reason:                         The request was discarded by a third-party extension DLL file.
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	06/04/2020 01:18:56 p. m.
Event ID:	6274	Task Category:	Network Policy Server
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	[redacted]
OpCode:	Info		
More Information:	Event Log Online Help		

And the log that appears in the FW is as follows:



Failed Log In
Mobile Access

Log Info

Origin	[redacted]_VS
Time	06 Apr 20, 01:54:30 PM
Blade	Mobile Access
Product Family	Access
Type	Log

Application

Category	Session

Host/device

Model	PC
OS	Windows 10 [redacted]
IP	192.168.[redacted]
Name	[redacted]
ID	[redacted]

Client information

Name	Endpoint Security VPN
Version	E82.20
Build Number	986101311

Session

Login Option	Microsoft Authentication
Data Protocol	IPSec
Data Encryption	AES-256 + SHA256

Traffic

Policy

Action	Failed Log In

Mobile Access Details

Reason	User does not belong to the Remote Access communi...

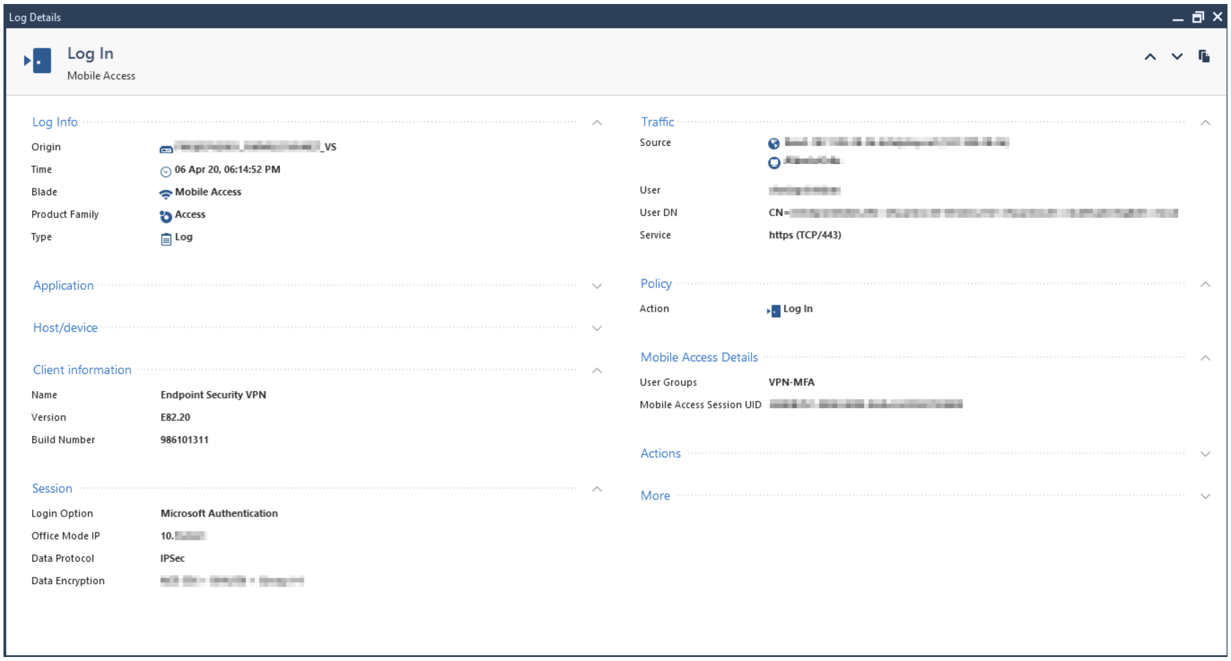
Actions

Report Log	Report Log to Check Point

More

Index Time	2020-04-06T18:54:30Z
MAC Address	[redacted]
Severity	Informational
Confidence Level	N/A

When authentication is successful, the log appears as the following:



Log In
Mobile Access

Log Info

Origin	[redacted]_VS
Time	06 Apr 20, 06:14:52 PM
Blade	Mobile Access
Product Family	Access
Type	Log

Application

Host/device

Client information

Name	Endpoint Security VPN
Version	E82.20
Build Number	986101311

Session

Login Option	Microsoft Authentication
Office Mode IP	10.[redacted]
Data Protocol	IPSec
Data Encryption	[redacted]

Traffic

Source	[redacted] [redacted]
User	[redacted]
User DN	CN=[redacted]
Service	https (TCP/443)

Policy

Action	Log In

Mobile Access Details

User Groups	VPN-MFA
Mobile Access Session UID	[redacted]

Actions

More

REFERENCES:

Remote Access VPN R80.20 Administration Guide

https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_RemoteAccessVPN_AdminGuide/html_frameset.htm

Azure AD Connect sync: Understand and customize synchronization

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis

Integrate your existing NPS infrastructure with Azure Multifactor Authentication

https://docs.microsoft.com/pt-br/azure/active-directory/authentication/howto-mfa-nps-extension

Resolve error messages from the NPS extension for Azure Multi-Factor Authentication

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-errors

MSOnline

https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0#msonline

Azure MFA NPS extensión health check script

https://docs.microsoft.com/es-es/samples/azure-samples/azure-mfa-nps-extension-health-check/azure-mfa-nps-extension-health-check/

NPS Extension for Azure MFA

https://www.microsoft.com/en-us/download/details.aspx?id=54688

Features and licenses for Azure Multi-Factor Authentication

https://dos.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing