Secure VPN tunnels with MFA

(using RouterOS platform)

MBUM 2022
Grzegorz Rakuś

Parę słów o mnie

Specjalizuję się w rozwiązaniach VPN (Site-to-Site / Remote Access),
Firewallach L4 / L7 oraz systemach AAA / SSO (RADIUS / MFA / SAML)

- administracja i utrzymanie multi-platformowej infrastruktury sieciowej
- zarządzanie bezpieczeństwem sieci (L2 / L3 / 802.1x / NGFW)

- wsparcie dla środowisk MS (AD / Hyper-V / Microsoft 365 / Azure)

- wdrożenia / konsultacje / doradztwo IT

MTCNA / MTCRE / MTCTCE / MTCSE

CCNA CyberOps / Security / Routing and Switching

grzegorz.rakus@gmail.com

linkedin.com/in/grzegorz-rakus/

The presentation shows how to build two-factor authentication for VPN sessions supported by RouterOS

Requirements:

- RouterOS integrated with Active Directory **using the NPS role** (RADIUS protocol)

  How to configure AD / NPS / CA - **https://mbum.pl/archive/prelekcja-CAPsMAN-WPA2EAP-AD.pdf**

- Configured policies on Network Policy Server (NPS)
- Installed and configured **ADSelfService Plus with NPS extension**

- Certificate for VPN protocols using SSL / TLS (eg. SSTP / IPsec / OpenVPN)
- Configured RouterOS (Profiles / Firewall / Interfaces)

  How to configure VPN settings - **https://mbum.pl/archive/mbum5/Profilowanie%20Sesji%20VPN.pdf**

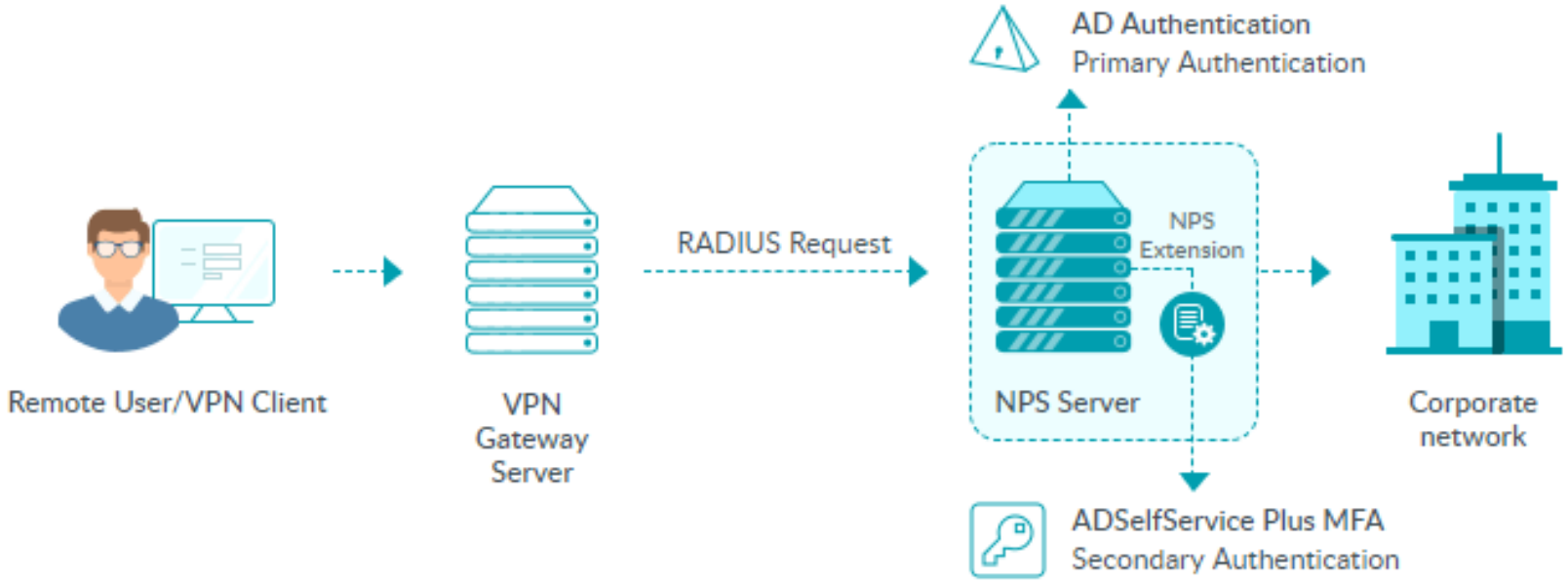
Interesting feature ;)

Supported VPN providers

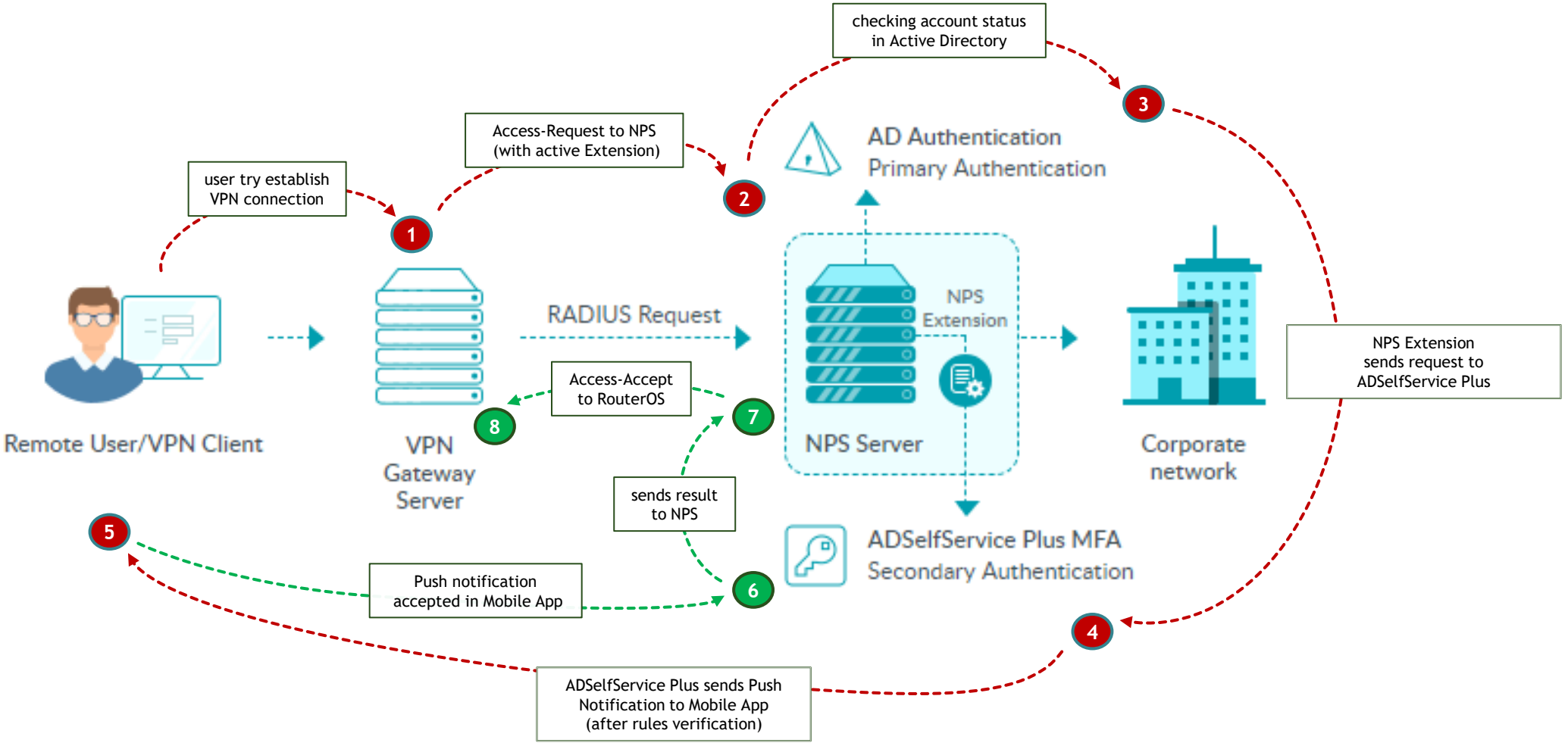
ADSelfService Plus allows admins to secure all RADIUS-supported VPN providers with MFA including:

1. Fortinet
2. Cisco IPSec
3. Cisco AnyConnect
4. Windows native VPN
5. SonicWall NetExtender
6. Pulse
7. Check Point Endpoint Connect
8. SonicWall Global VPN
9. OpenVPN Access Server
10. Palo Alto
11. Juniper

Diagram - VPN with ADSelfService Plus MFA

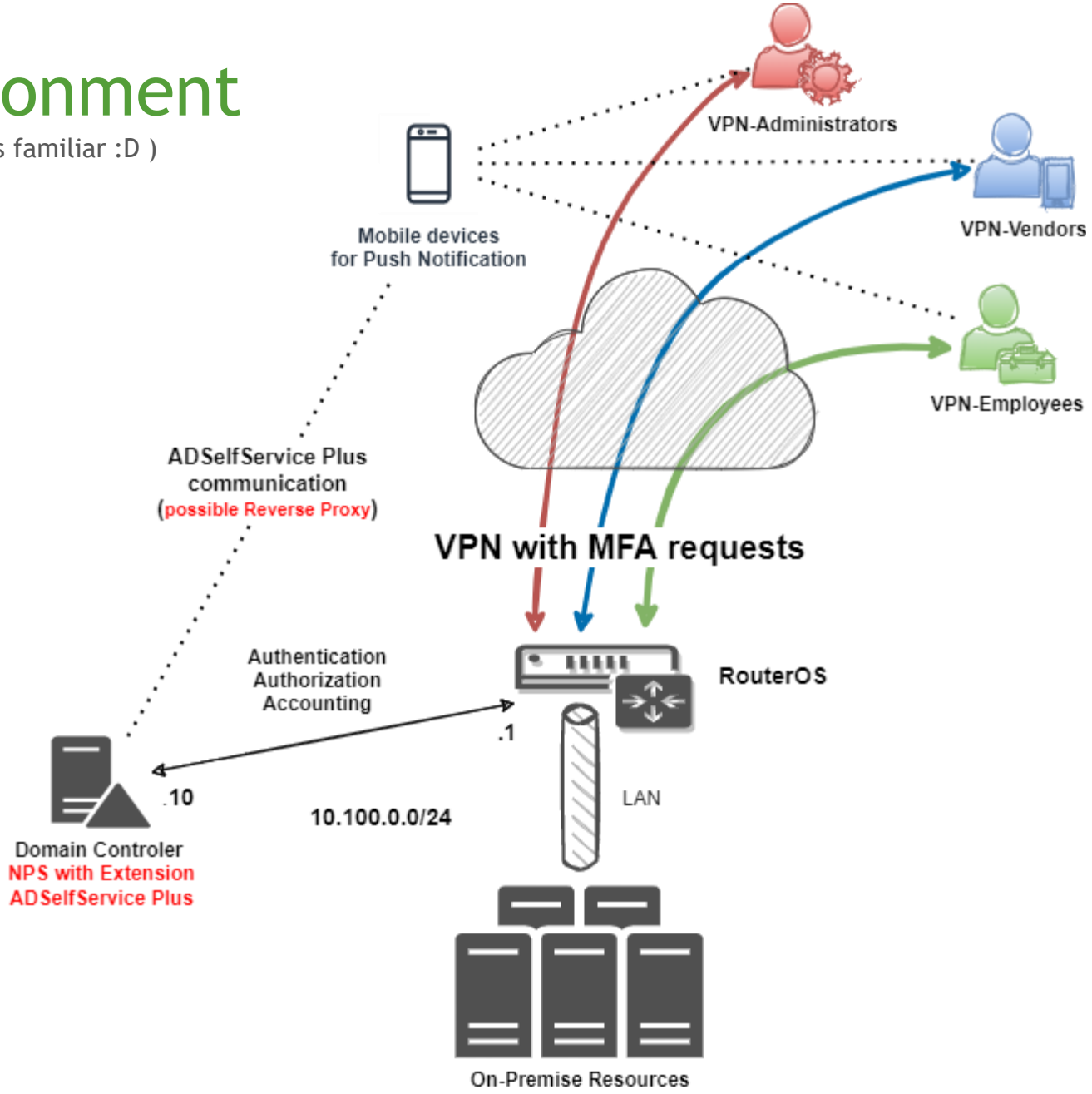


How it works


checking account status in Active Directory
Access-Request to NPS (with active Extension)
user try establish VPN connection
AD Authentication
Primary Authentication
RADIUS Request
NPS Extension
Access-Accept to RouterOS
NPS Extension sends request to ADSelfService Plus
Remote User/VPN Client
VPN Gateway Server
NPS Server
Corporate network
sends result to NPS
ADSelfService Plus MFA
Secondary Authentication
Push notification accepted in Mobile App
ADSelfService Plus sends Push Notification to Mobile App (after rules verification)
1
2
3
4
5
6
7
8

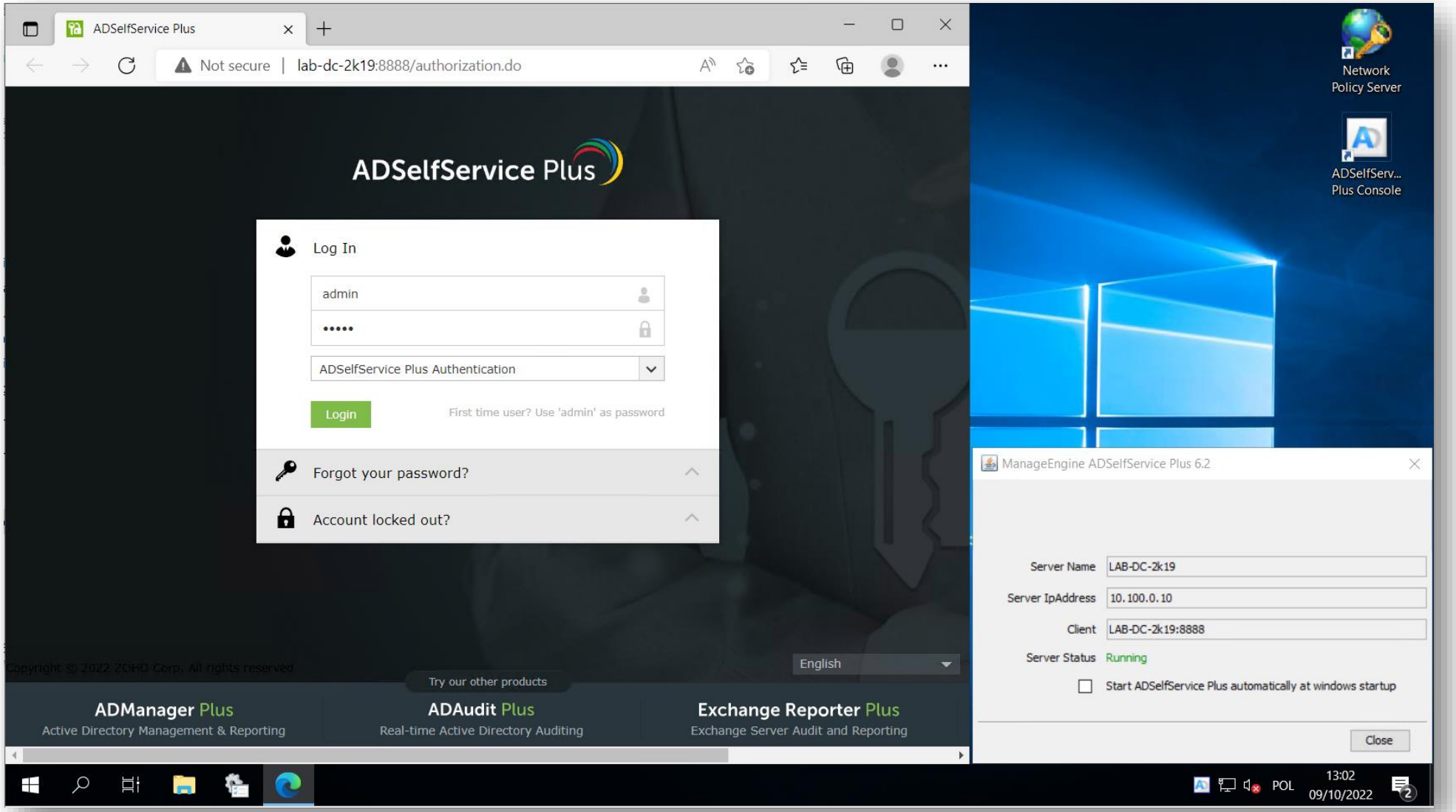
LAB environment

(Hmm, this diagram looks familiar :D)



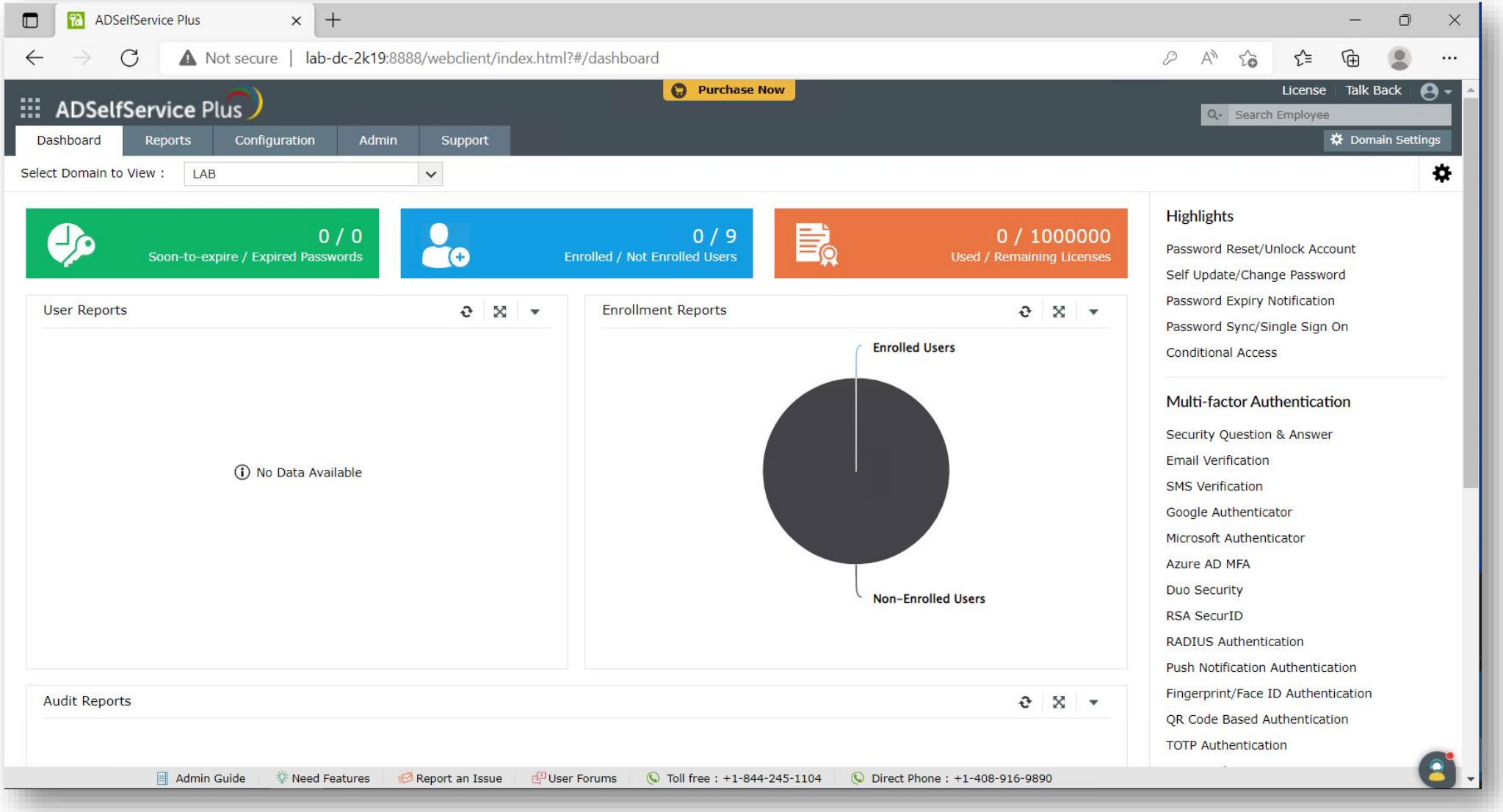
Running ADSelfService Plus

(easy installation from wizard)



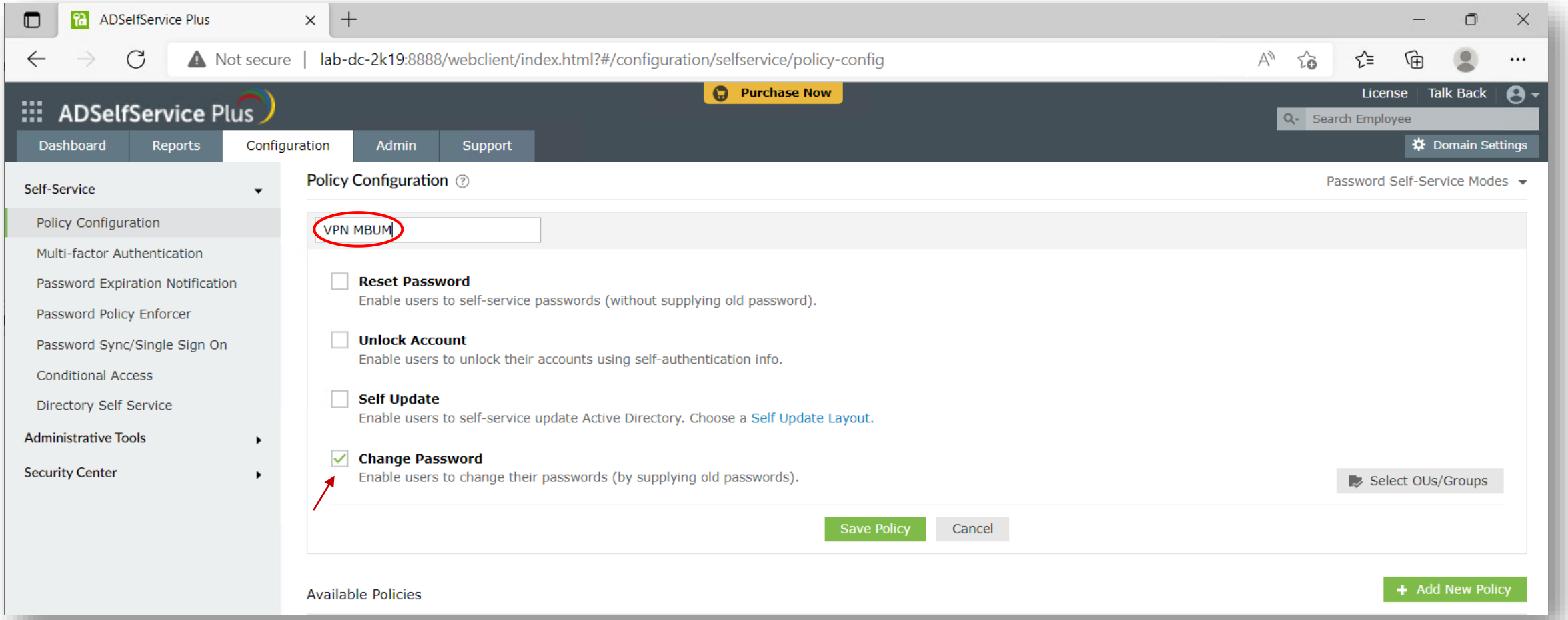
ADSelfService Plus main Dashbord

(first login requires setting up Security Questions for admin account)

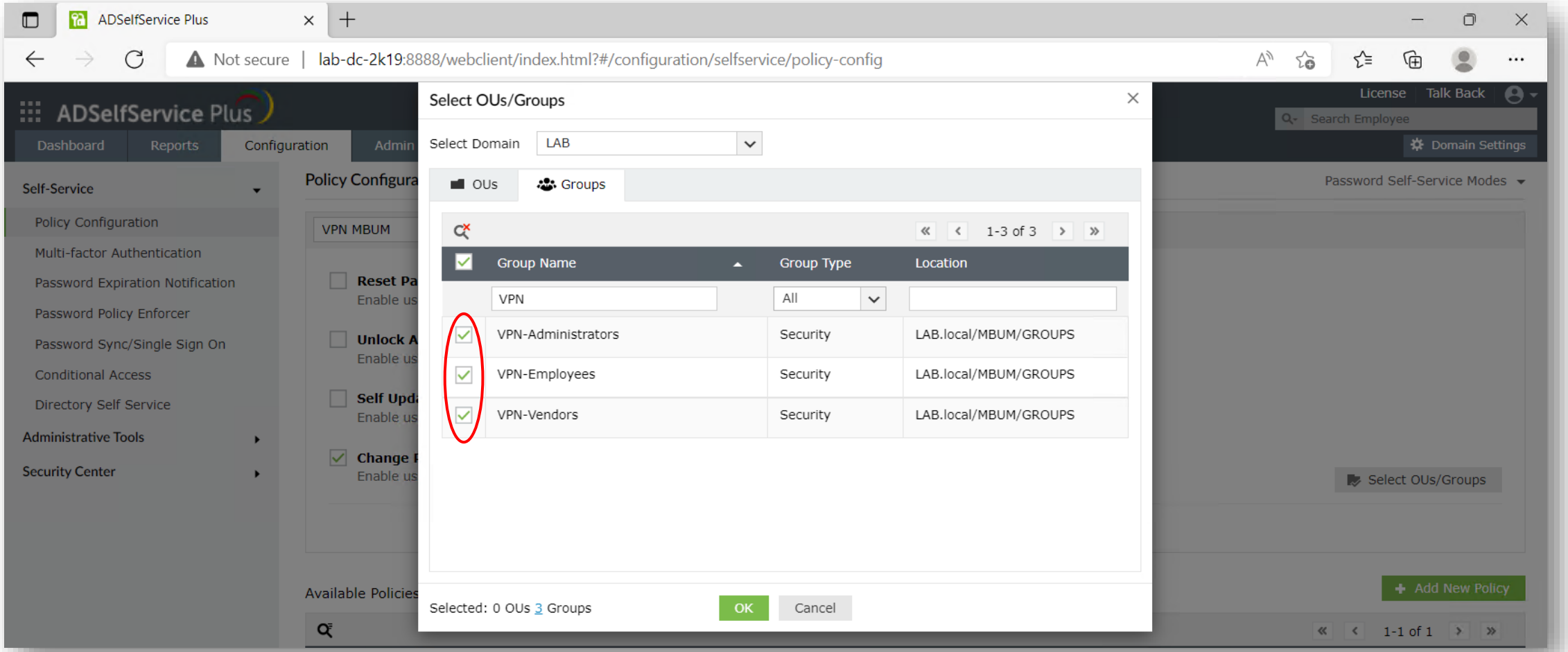


Add New Policy

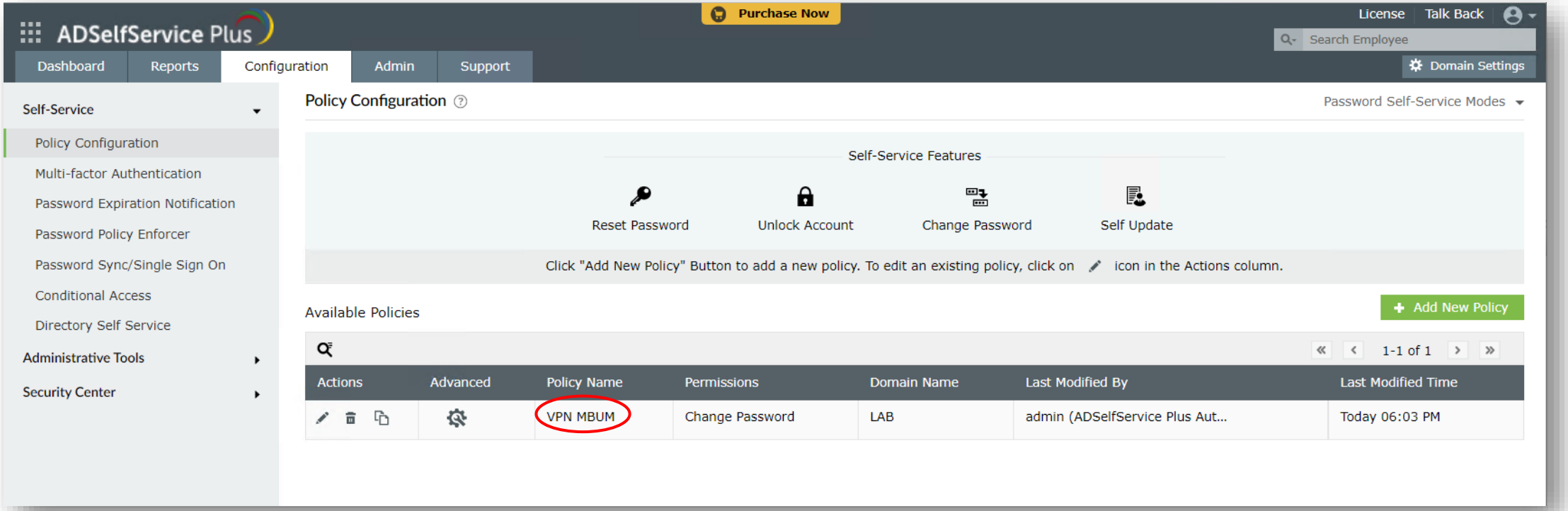
(Configuration / Policy Configuration / Add New Policy – min. of one active feature in the policy is required)



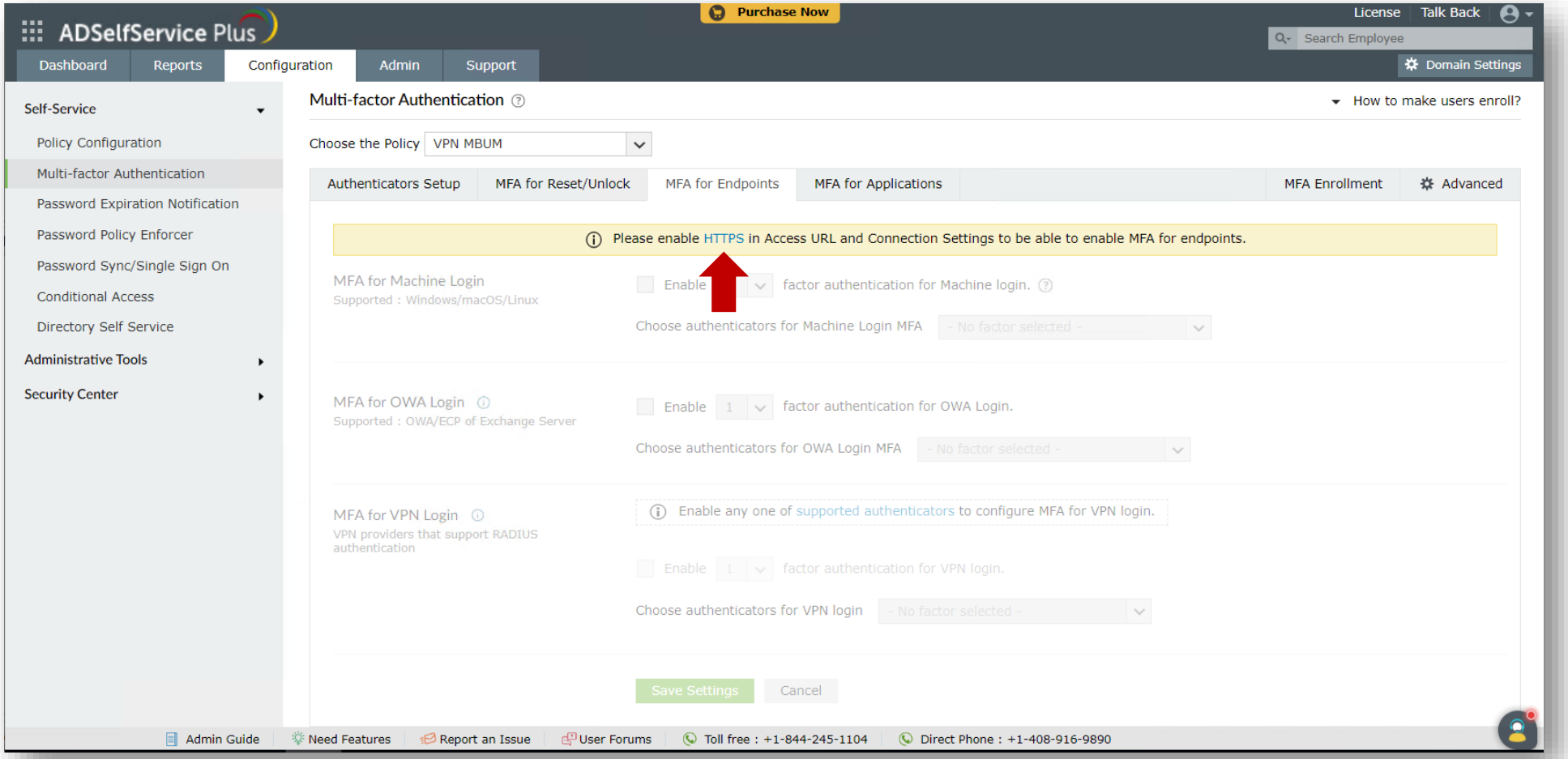
Select OUs/Groups from your Domain in the New Policy



New Policy is ready

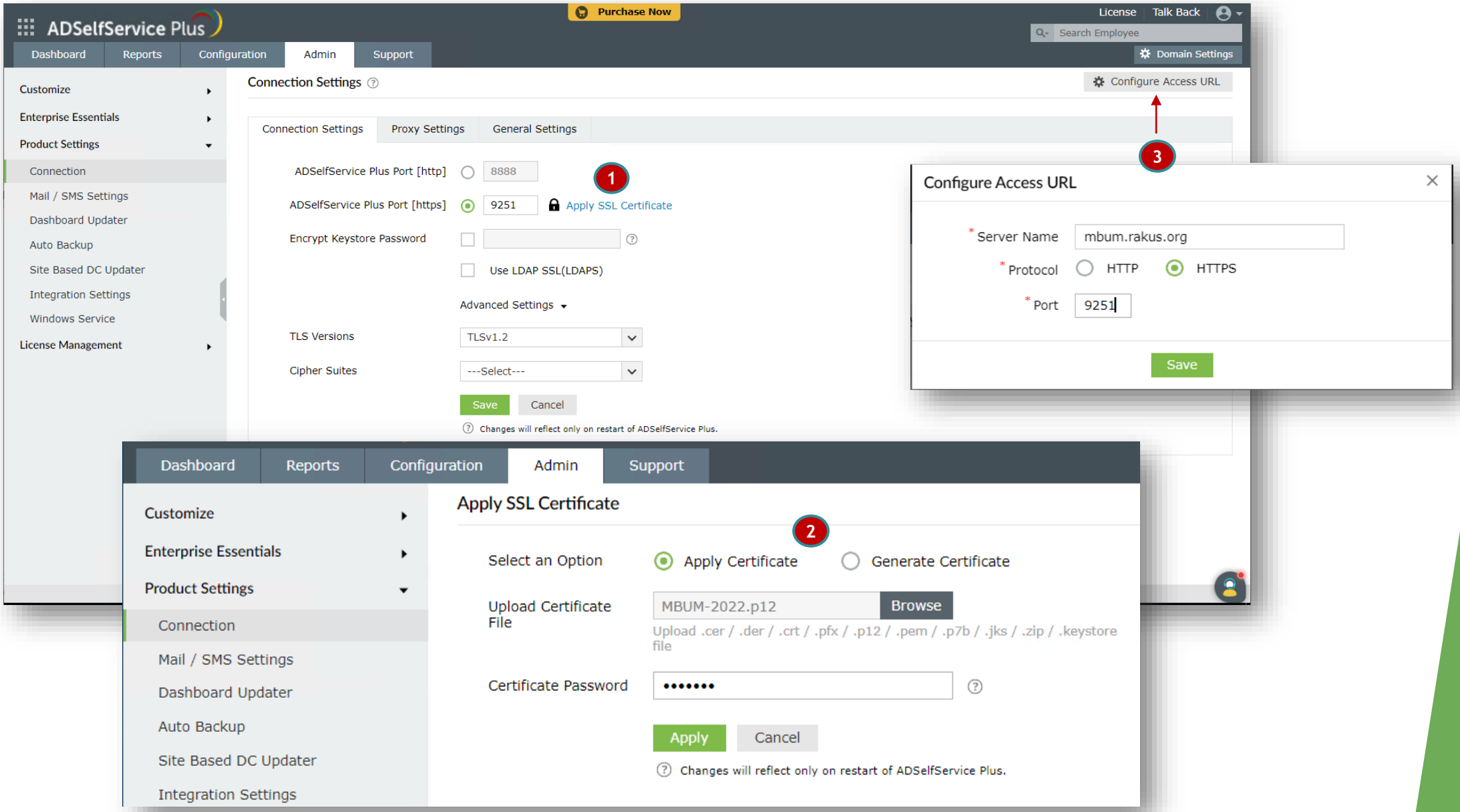


Configure MFA for Endpoints



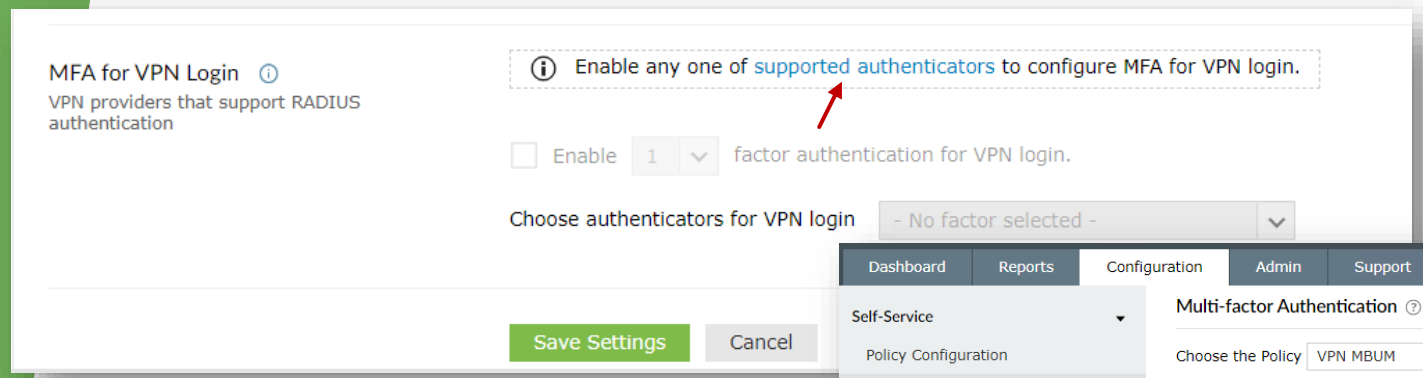
Enable HTTPS and Configure Access URL !!

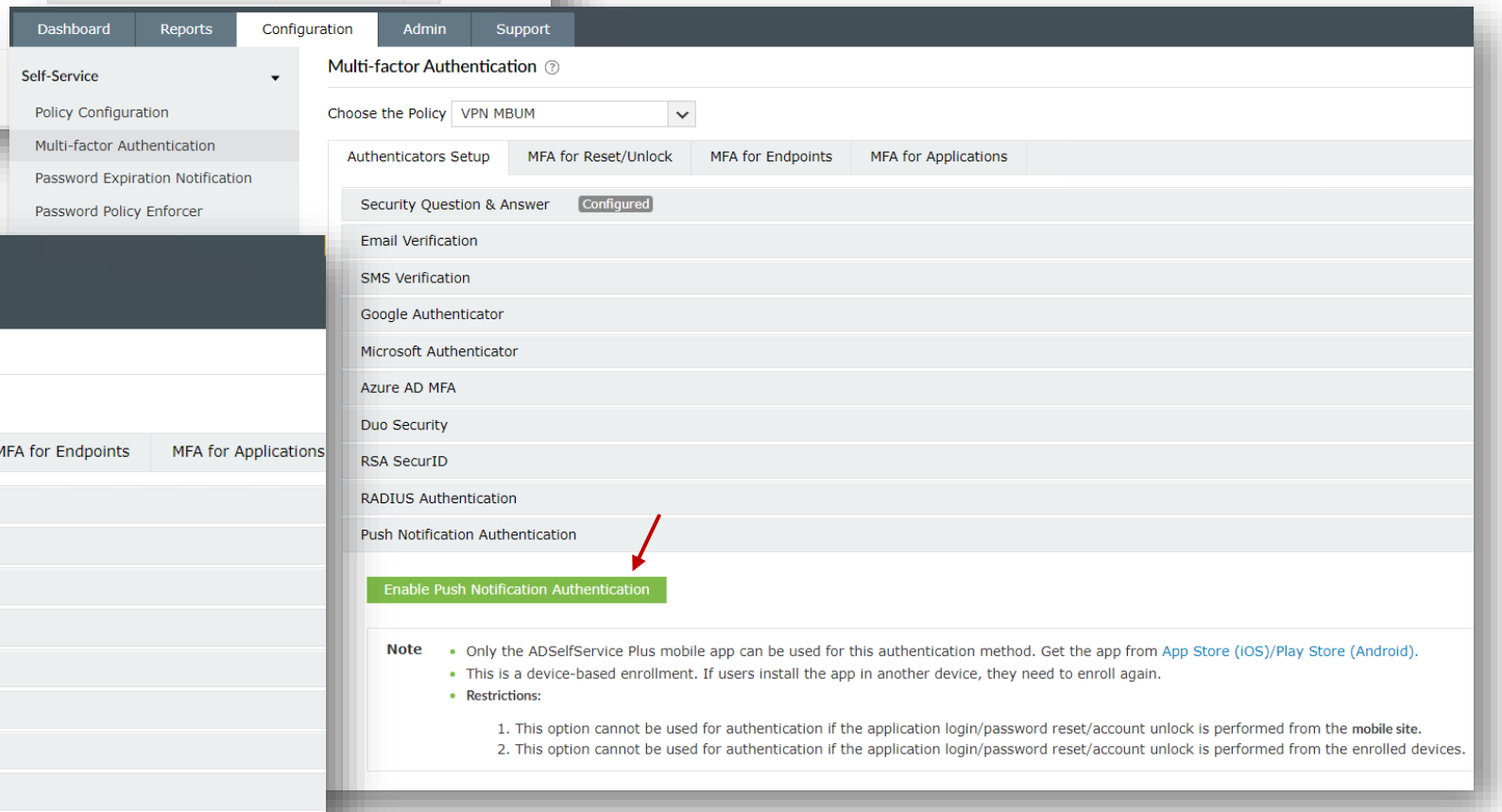
(import or generate self-signed certificate)

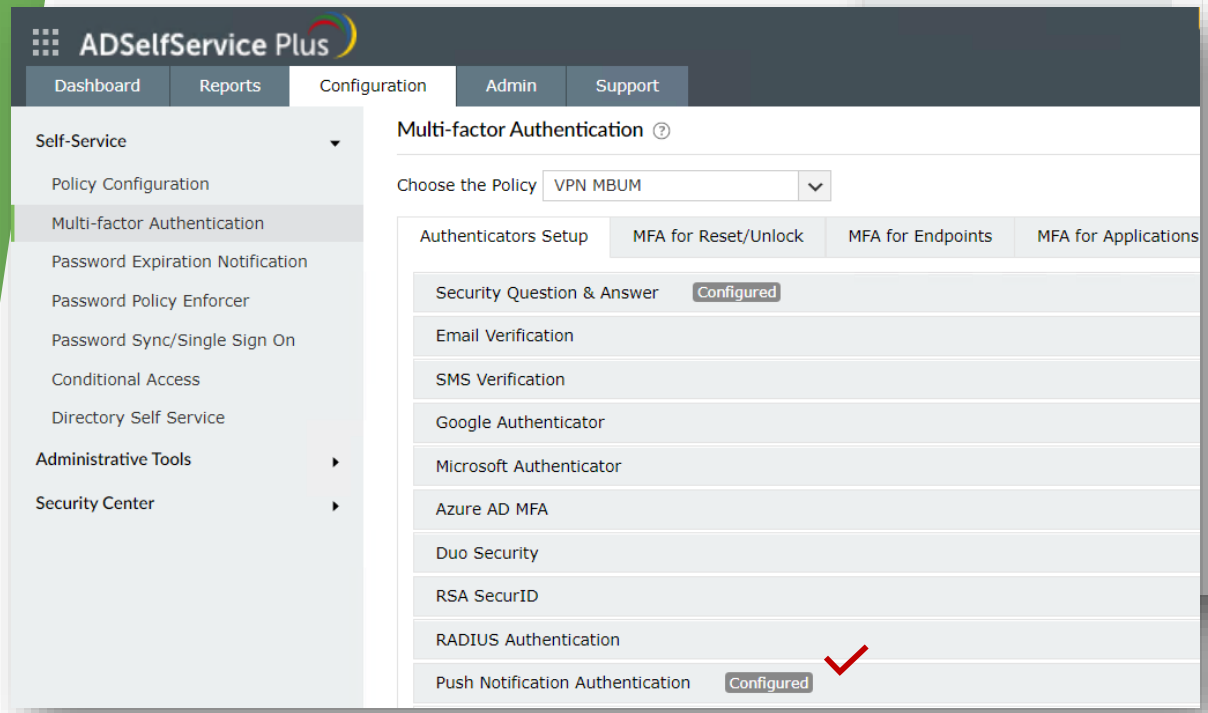


Enable Push Notifiaction Authentication

(it's required to enable **MFA for VPN Login** feature)

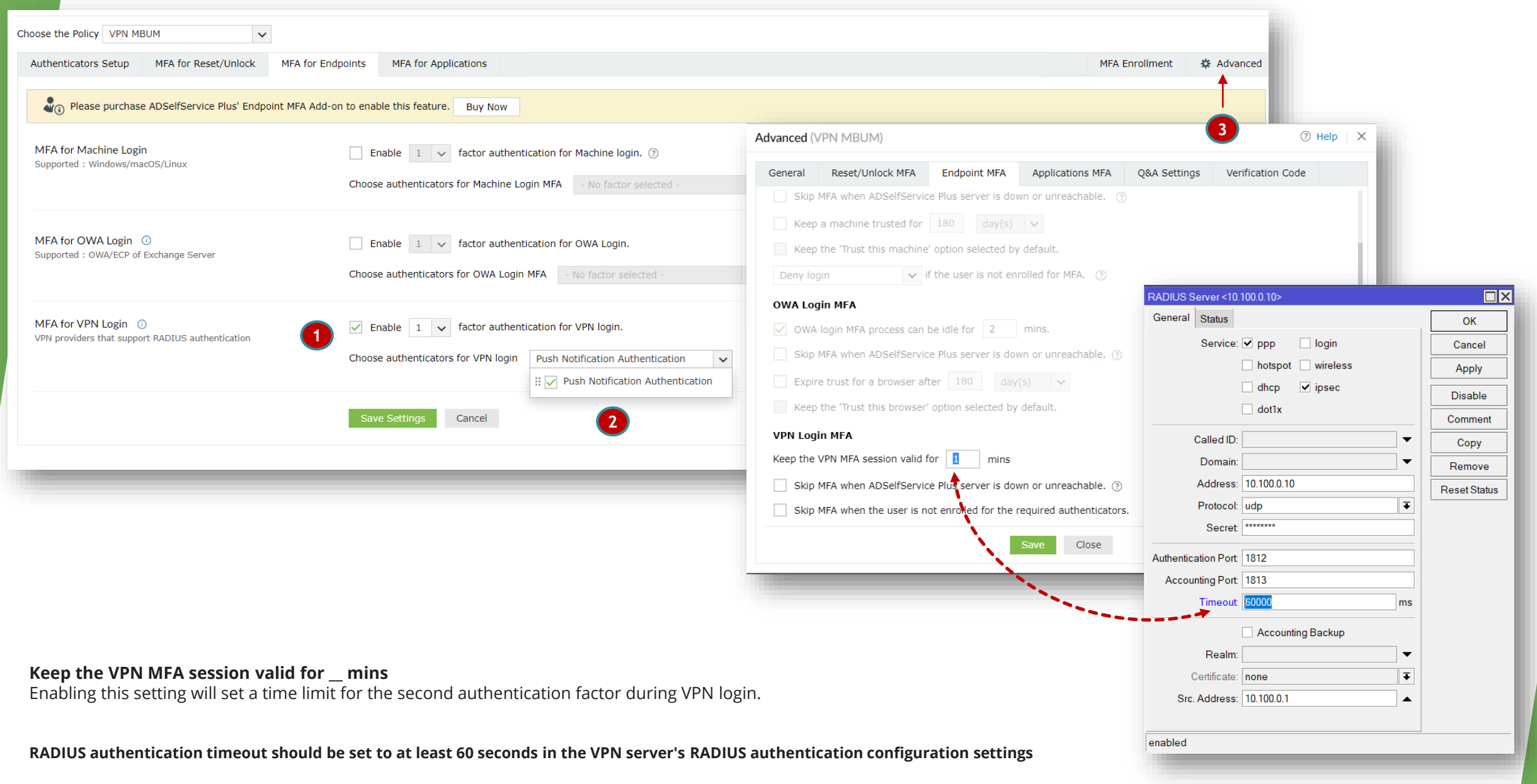






using the 'Time One Time Password' feature with OpenVPN (e.g. in Google Authenticator or MS Authenticator) is not possible because RouterOS doesn't support Challenge/Response (Access-Challenge RADIUS attribute)

'MFA VPN session keep' and 'RADIUS timeout request' together

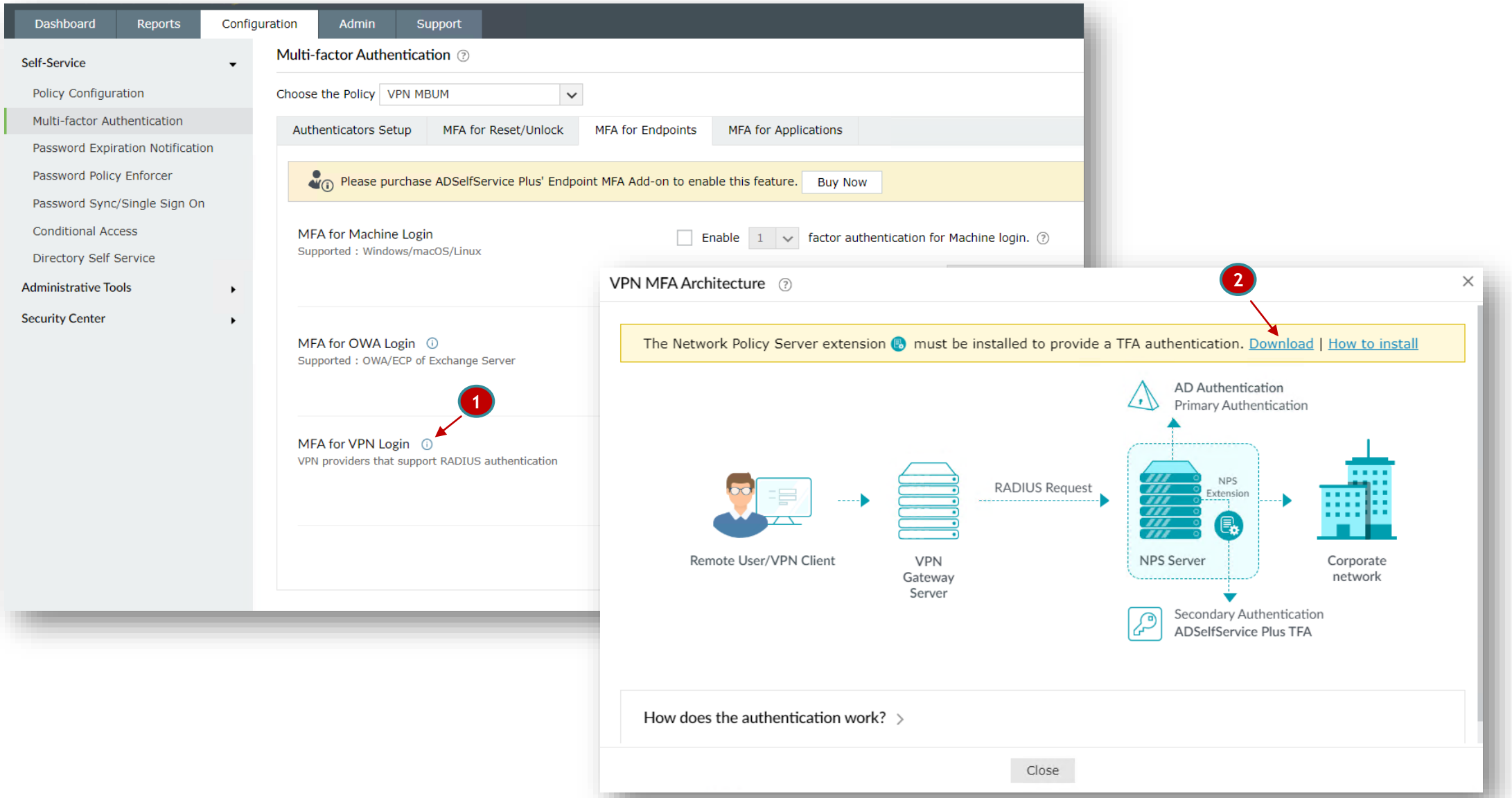


Keep the VPN MFA session valid for __ mins
Enabling this setting will set a time limit for the second authentication factor during VPN login.

RADIUS authentication timeout should be set to at least 60 seconds in the VPN server's RADIUS authentication configuration settings

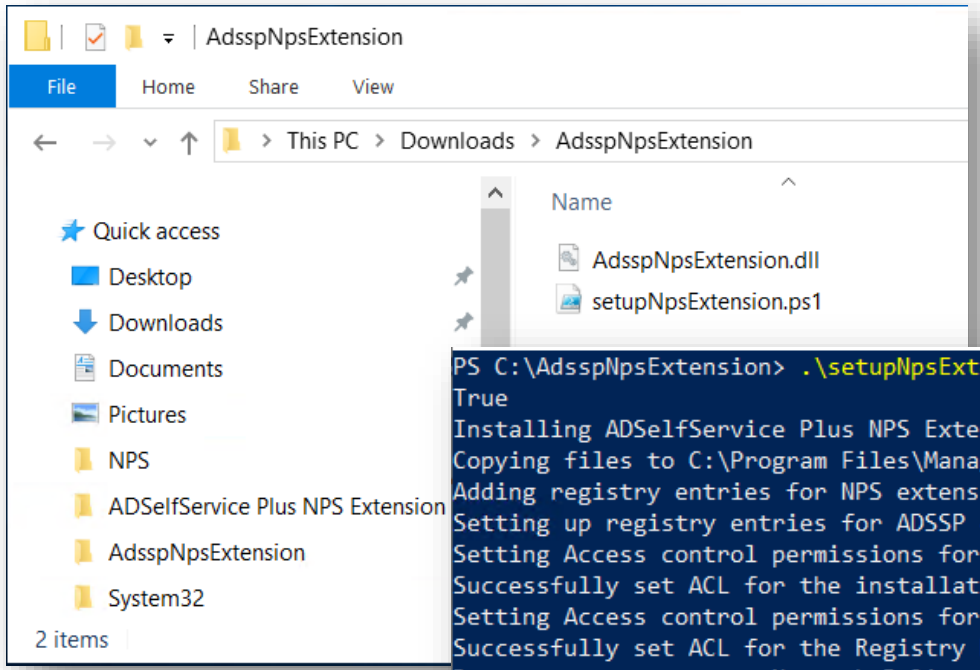
NPS plugin Extension - installation part 1

(the most hidden file location in the world !!)



NPS plugin Extension - installation part 2

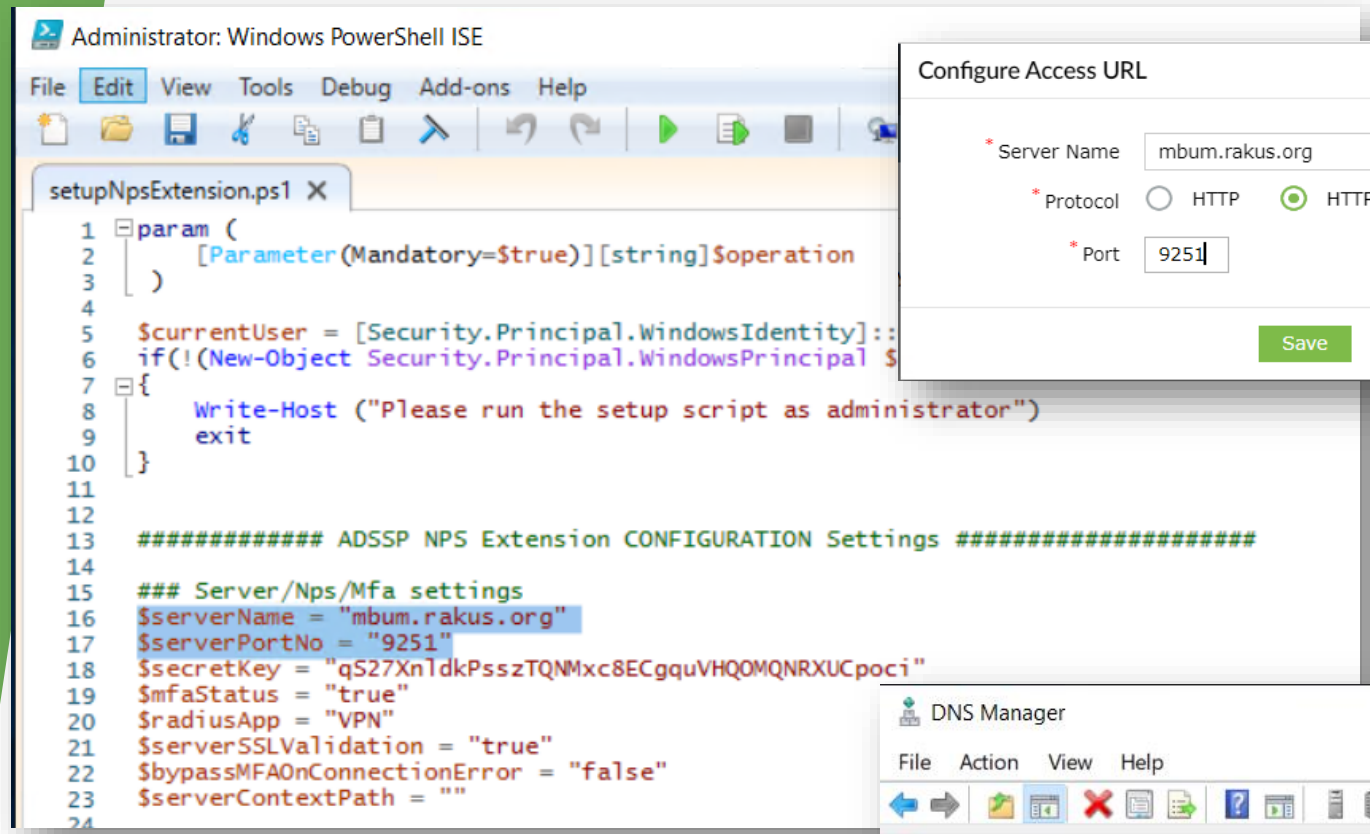
(PowerShell magic ;))

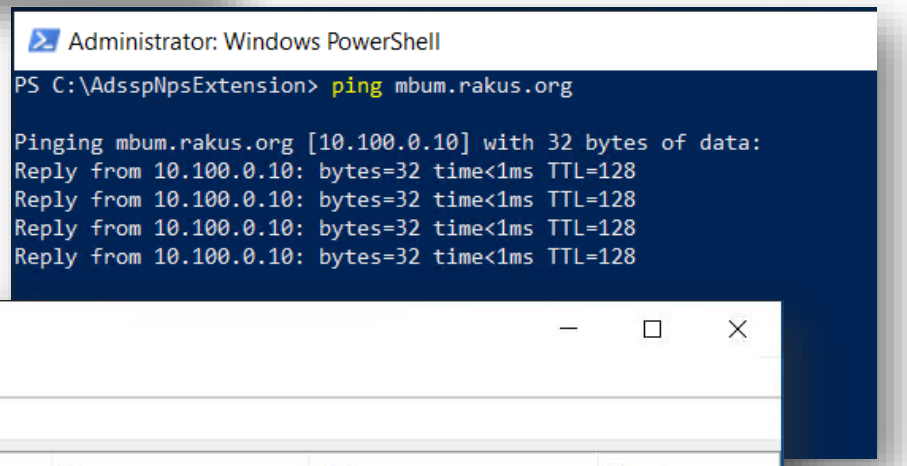


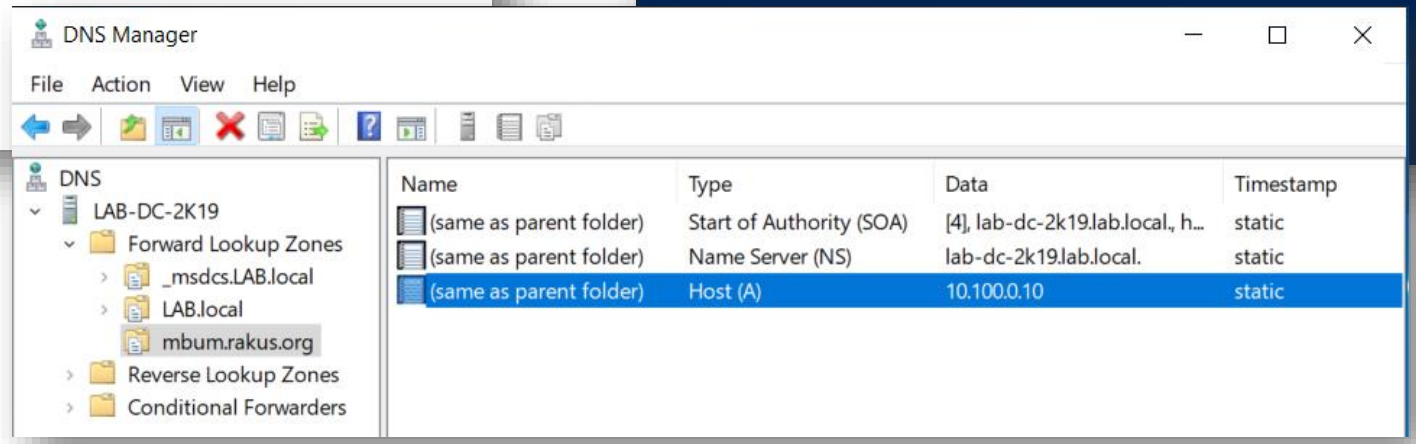

```
PS C:\AdsspNpsExtension> .\setupNpsExtension.ps1 install
True
Installing ADSelfService Plus NPS Extension...
Copying files to C:\Program Files\ManageEngine\ADSelfService Plus NPS Extension
Adding registry entries for NPS extension
Setting up registry entries for ADSSP configuration
Setting Access control permissions for the installation directory
Successfully set ACL for the installation directory
Setting Access control permissions for the Registry key HKLM:\SOFTWARE\ZOHO Corp\ADSelfService Plus NPS Extension
Successfully set ACL for the Registry key
Do you want to restart Network Policy Server(ias) now [y/n] ?: y
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...
Installation completed successfully
Setup complete. Press Enter to continue...:

PS C:\AdsspNpsExtension>
```

Why 'Configure Access URL' is so important

(don’t forget verify / add DNS record for internal NPS extension requests)

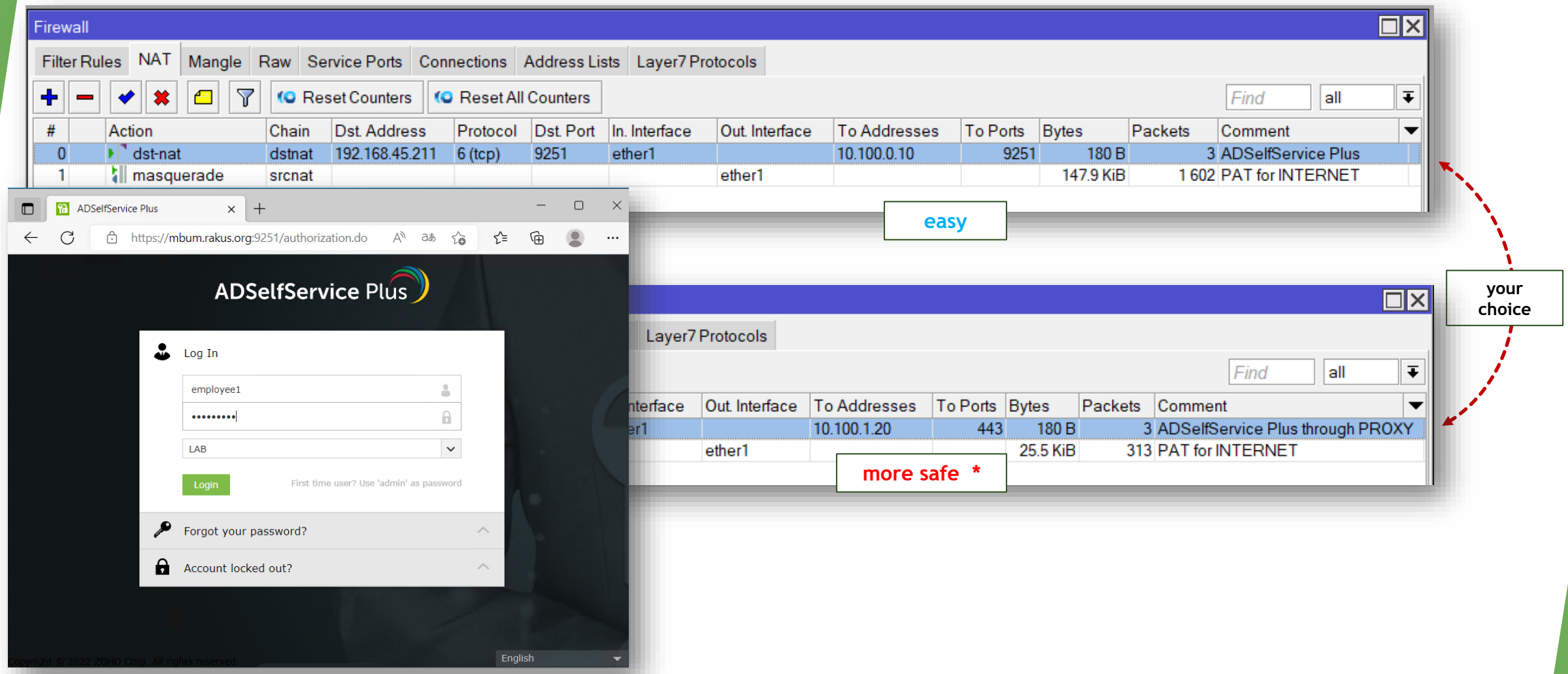






add DST-NAT rule for ADSelfService Plus publication **and… secure it using Reverse Proxy ***

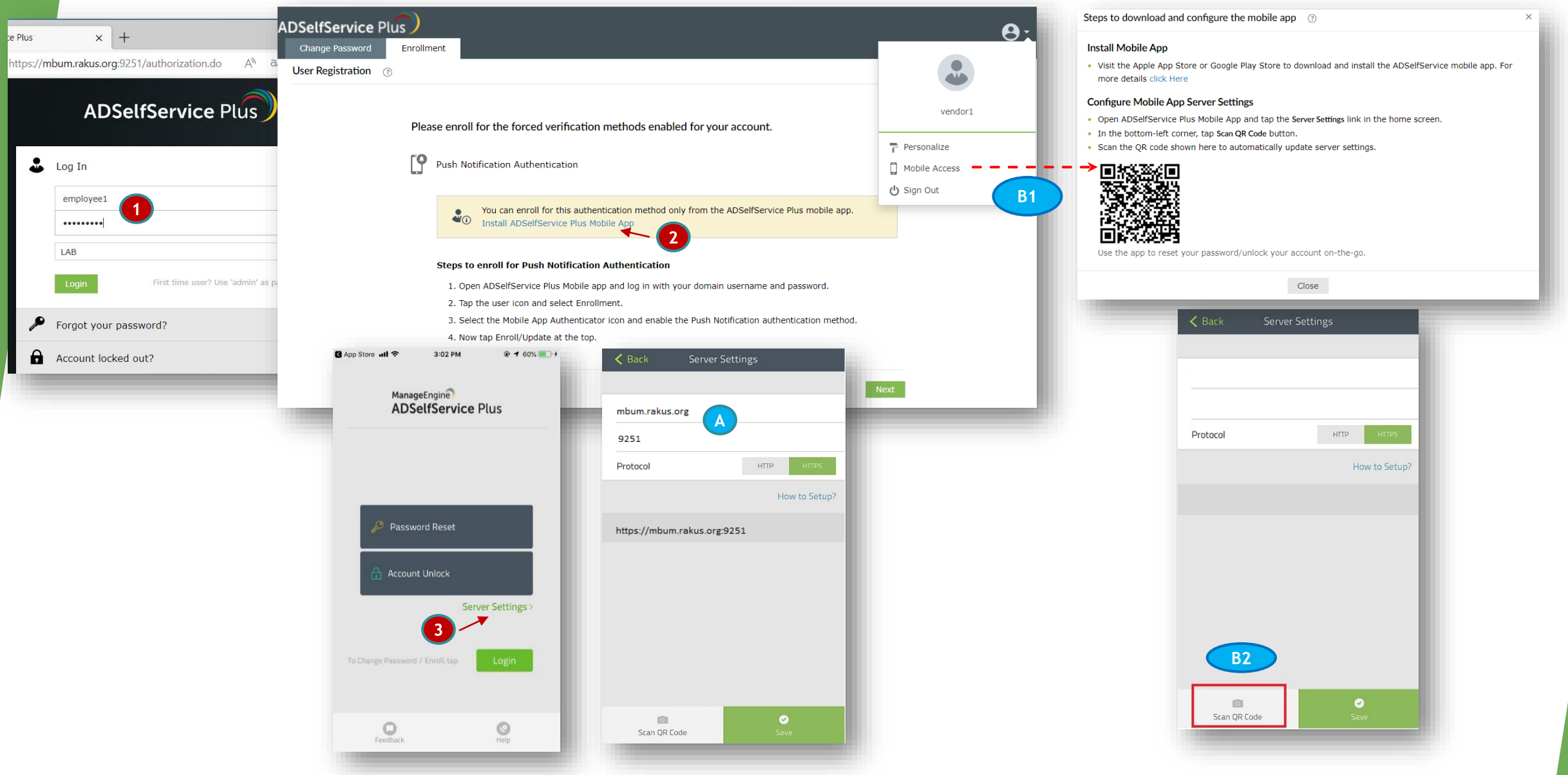
(required for communication from Internet – eg. Push Notification / Enrollment)



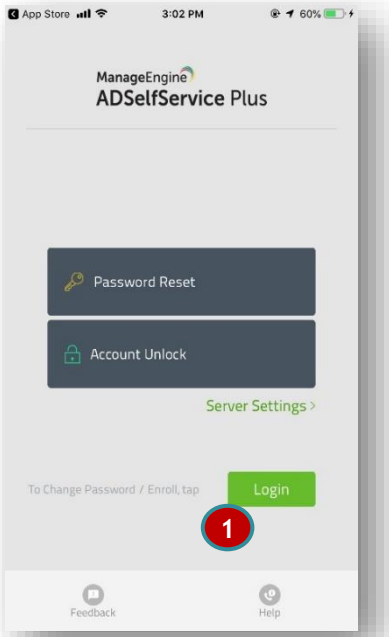
* example reverse proxy using IIS - https://download.manageengine.com/products/self-service-password/adselfservice-plus-reverse-proxy-using-iis.pdf

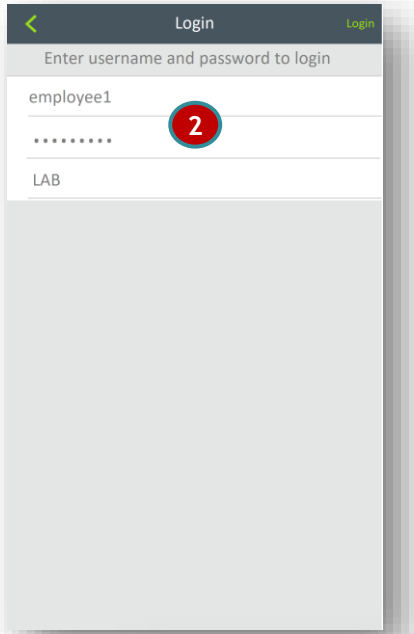
Configure Server Settings in Mobile App

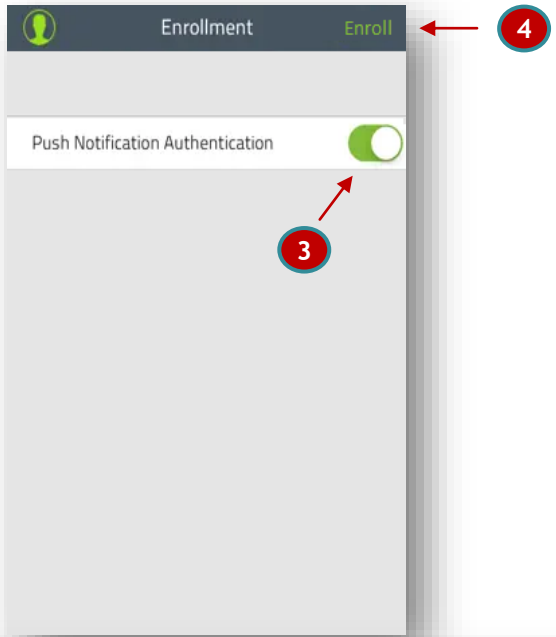
configuration example - manually **(A)** or by QR code **(B)**

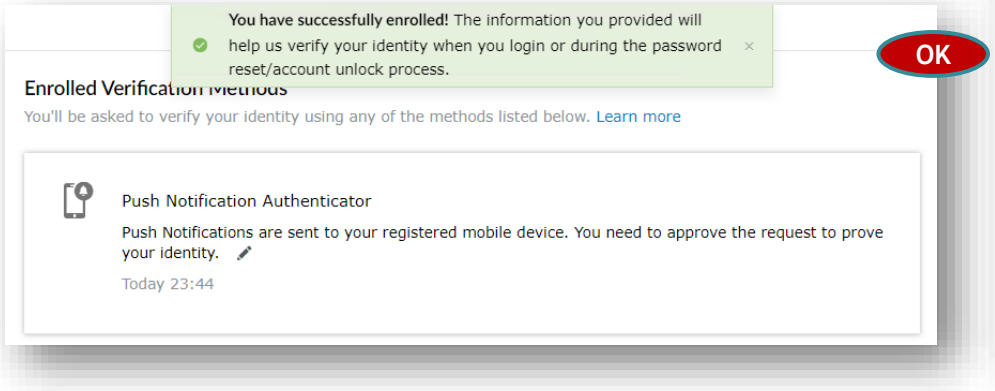


User enrollment and Push activation

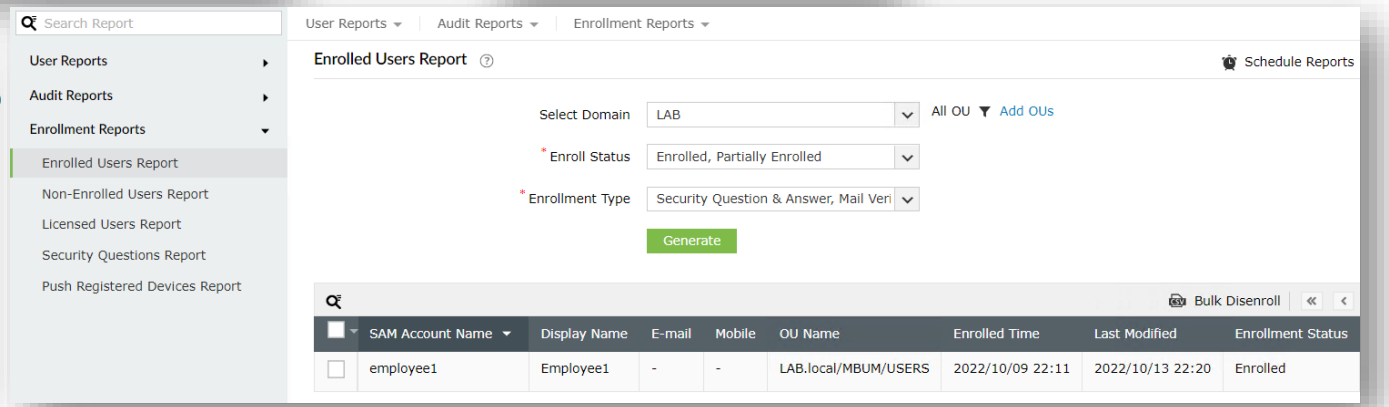








OK



Summary tests – checking VPN connections

User not enrolled

```
User-Name = "vendor1"
Calling-Station-Id = "192.168.45.165"
Called-Station-Id = "0.0.0.0"
Acct-Session-Id = "81d00001"
MS-CHAP-Challenge = 0xa4f6cbf3e11d884df6acca5945f6025a
MS-CHAP2-Response = 0x0100bee8cfe54ed68cdc5f77860b3f85
 50050000000000000000033d9e96501d3
 5e642a4f084d46a7473331355f56c40f
 804f
NAS-Identifier = "LAB - MT CHRv7"
NAS-IP-Address = 10.100.0.1
received Access-Reject with id 5 from 10.100.0.10:1812
Signature = 0x90fb43b165c12abc7e6a9de35ad7f8e6
Reply-Message = "You need to enroll in the required authentication factors to proceed."
MS-CHAP-Error = 0x00453d36393120523d3020563d33
received reply for 1b:02
: user vendor1 authentication failed
```

Event 6273, Microsoft Windows security auditing.

General | Details

Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:

Security ID:	LAB\vendor1
Account Name:	vendor1
Account Domain:	LAB
Fully Qualified Account Name:	LAB.local/MBUM/USERS/Vendor1

Event 6273, Microsoft Windows security auditing.

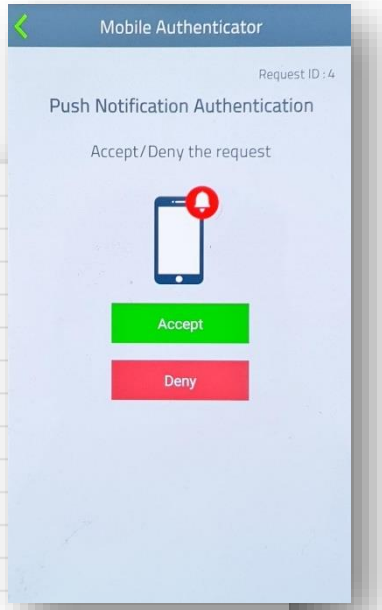
General | Details

Authentication Details:

Connection Request Policy Name:	Use Windows authentication for all users
Network Policy Name:	VPN-Vendors
Authentication Provider:	Windows
Authentication Server:	LAB-DC-2k19.LAB.local
Authentication Type:	Extension
EAP Type:	-
Account Session Identifier:	3831643030303031
Logging Results:	Accounting information was written to the local log file.
Reason Code:	21
Reason:	An NPS extension dynamic link library (DLL) that is installed on the NPS server rejected the connection request.

User enrolled

```
User-Name = "employee1"
Calling-Station-Id = "192.168.45.165"
Called-Station-Id = "0.0.0.0"
Acct-Session-Id = "81d00002"
MS-CHAP-Challenge = 0xcea5461d353909b84834e8f6616fae01
MS-CHAP2-Response = 0x0100aee46a72b94cc9718566efe07787
 17f50000000000000000018da6dedbaee
 3fd4a98e2b1232b2bd658538bff7bba7
 b9e7
NAS-Identifier = "LAB - MT CHRv7"
NAS-IP-Address = 10.100.0.1
received Access-Accept with id 6 from 10.100.0.10:1812
Signature = 0xb3436807d32d10e7760743d438bd4858
Framed-Protocol = 1
Service-Type = 2
Reply-Message = "Identity verified successfully."
```



sstp, ppp, info	<sstp-employee1>: authenticated
sstp, ppp, info	<sstp-employee1>: connected ✓

Event 6272, Microsoft Windows security auditing.

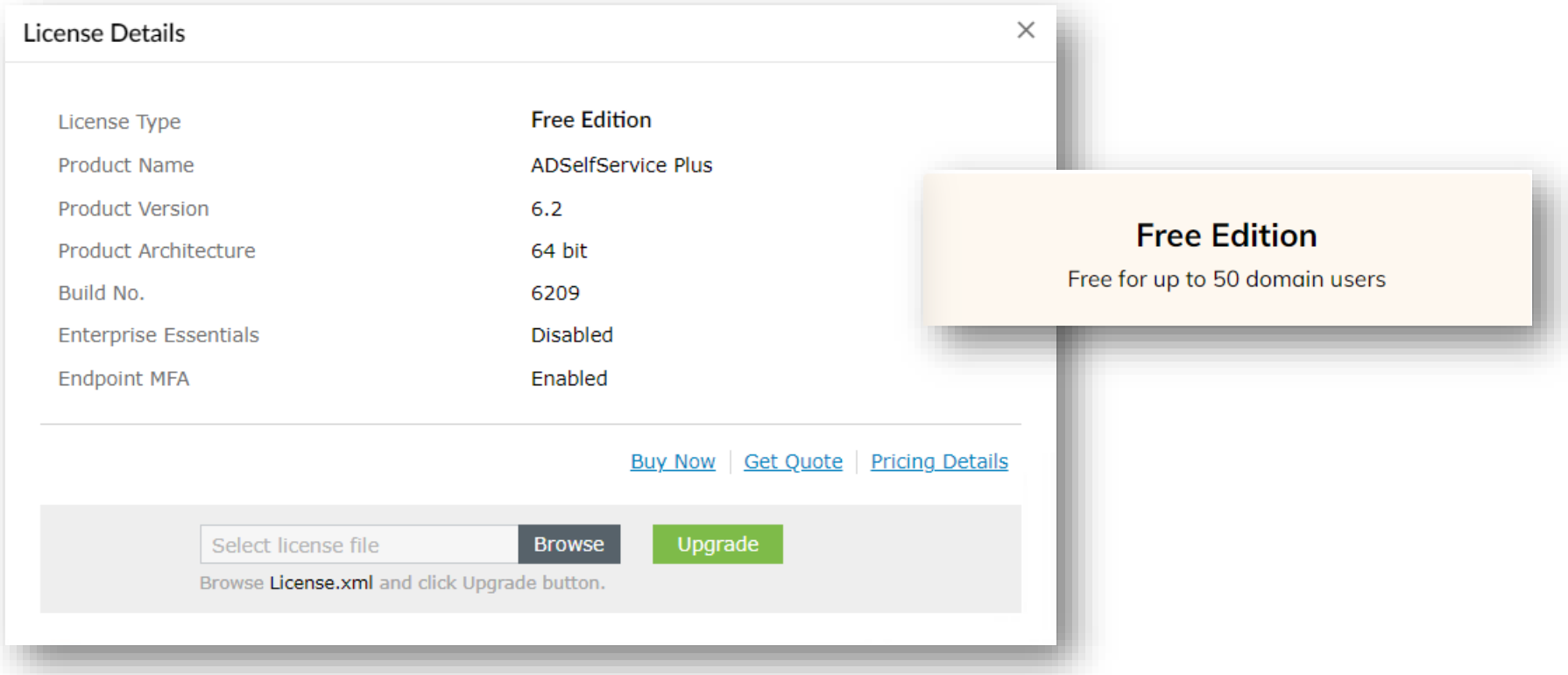
General | Details

Network Policy Server granted access to a user.

User:

Security ID:	LAB\employee1
Account Name:	employee1
Account Domain:	LAB
Fully Qualified Account Name:	LAB.local/MBUM/USERS/Employee1

Small Bonus ;)


License Details
License Type
Free Edition
Product Name
ADSelfService Plus
Product Version
6.2
Product Architecture
64 bit
Build No.
6209
Enterprise Essentials
Disabled
Endpoint MFA
Enabled
Buy Now
Get Quote
Pricing Details
Select license file
Browse
Upgrade
Browse License.xml and click Upgrade button.
Free Edition
Free for up to 50 domain users