

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/prelekcia-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>

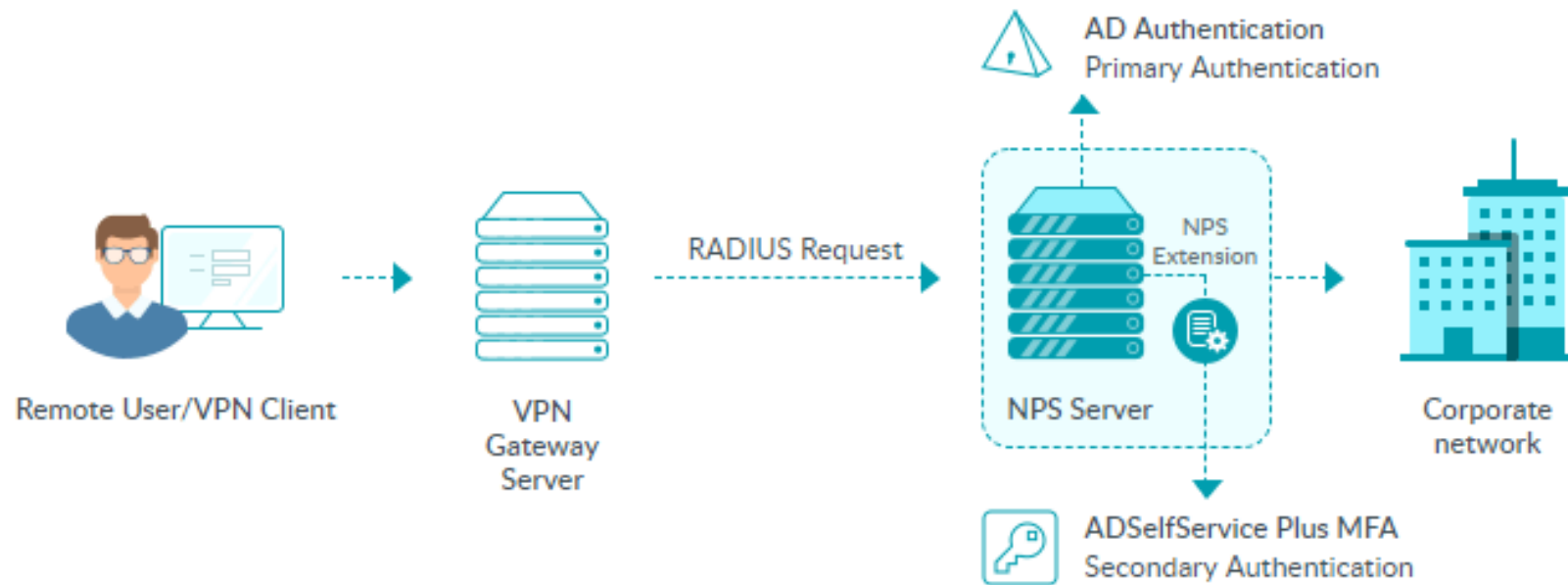
Interesting feature ;)

Supported VPN providers

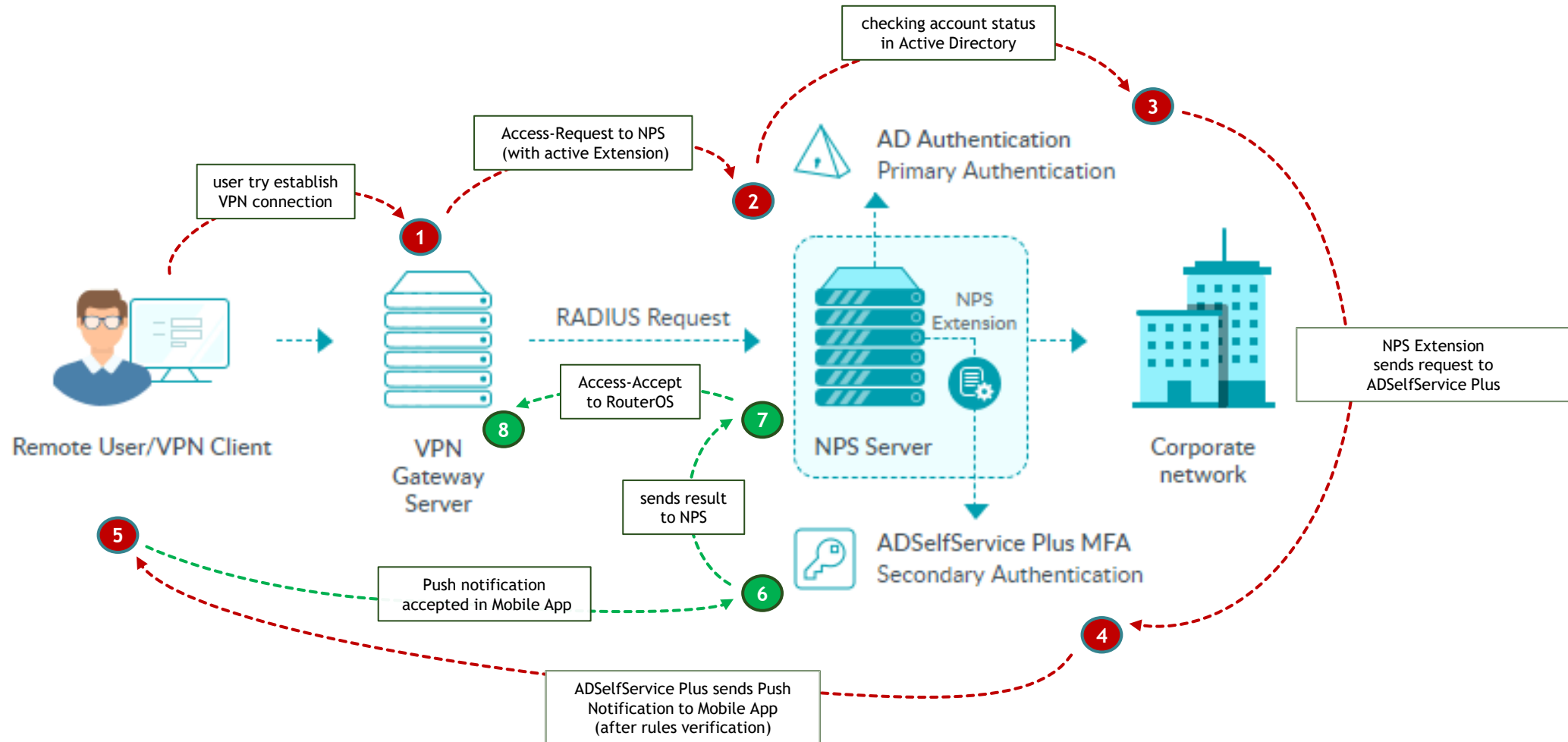
ADSelfService Plus allows admins to secure all RADIUS-supported VPN providers with MFA including:

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

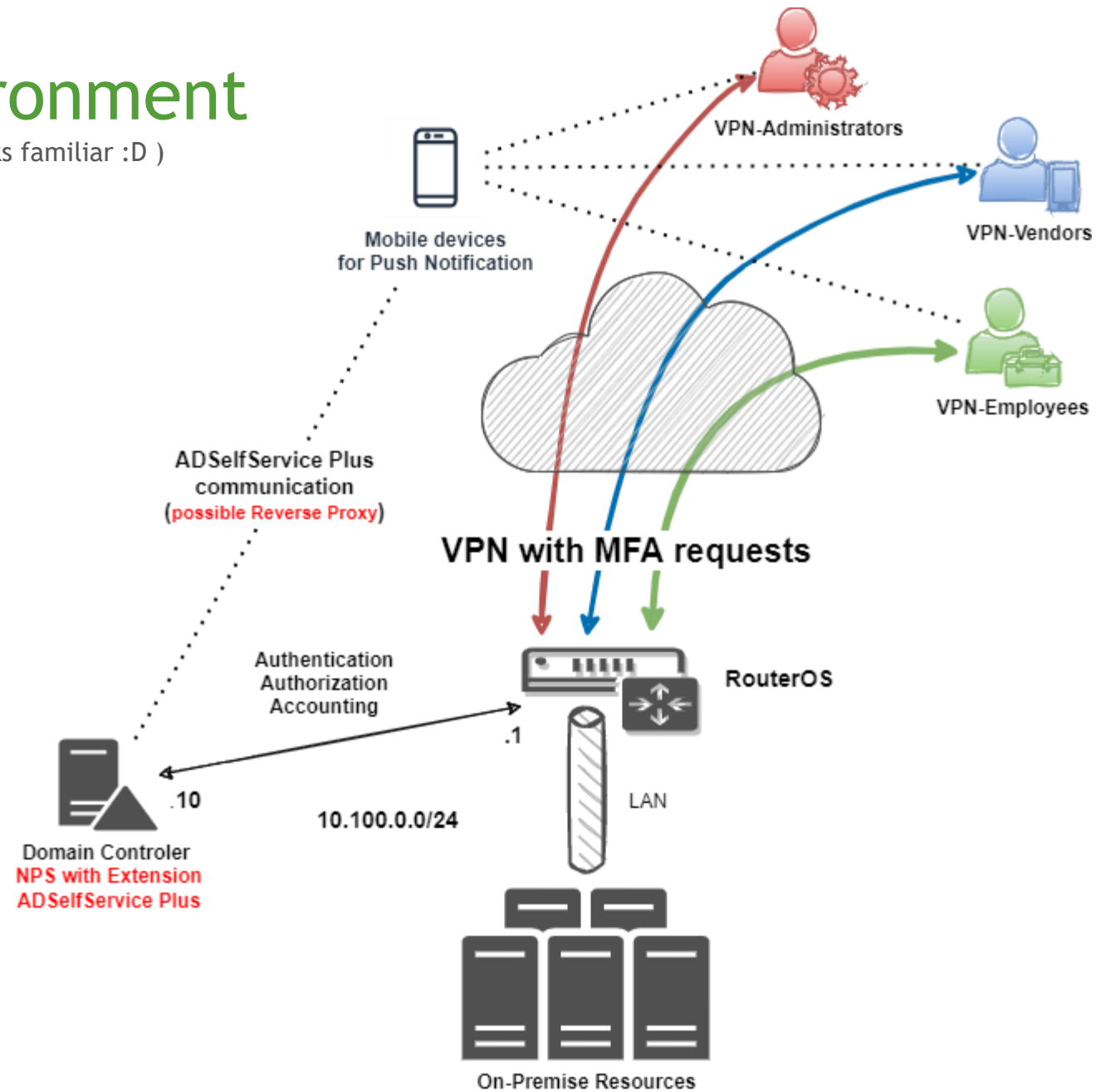


How it works



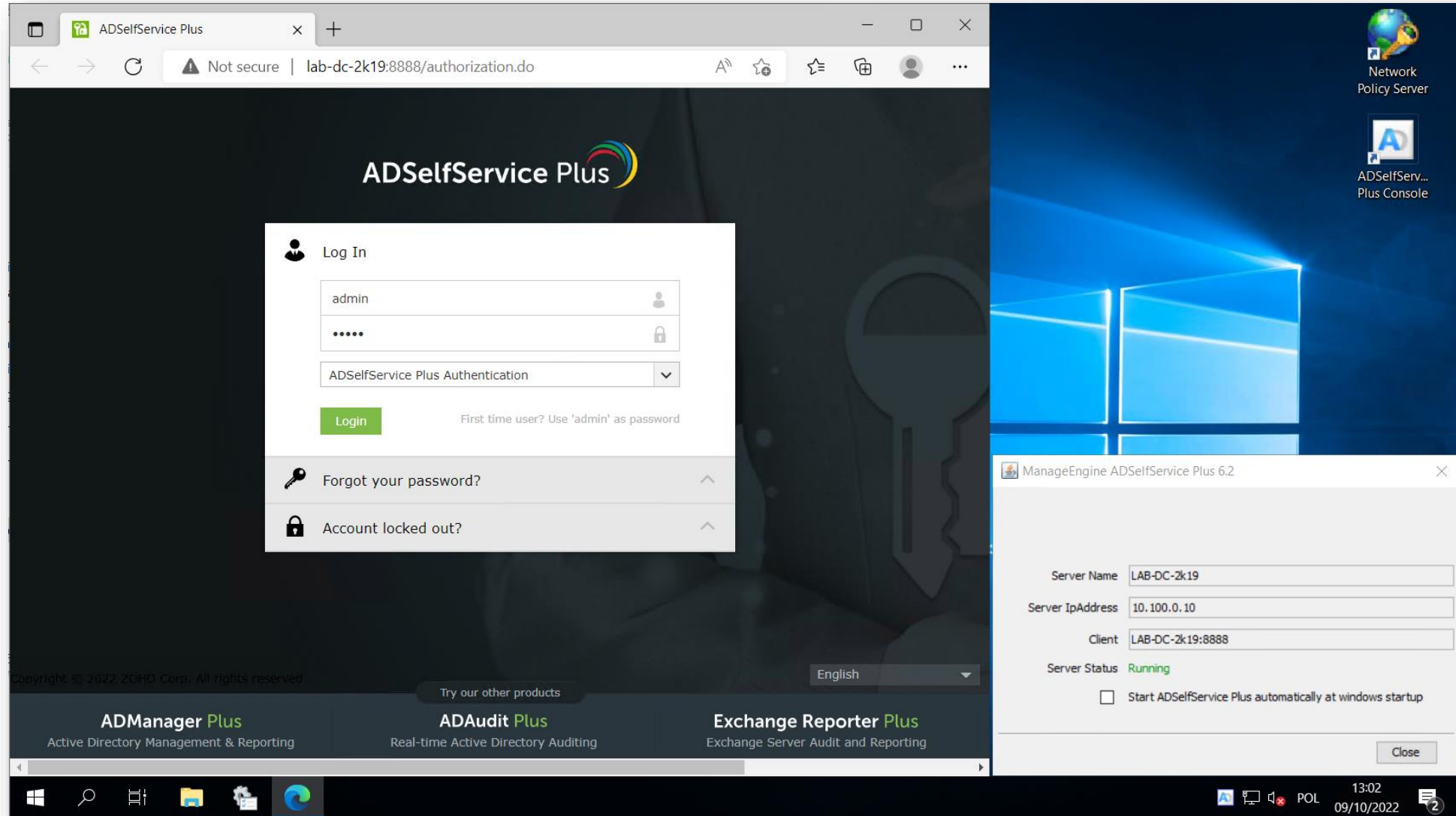
LAB environment

(Hmm, this diagram looks familiar :D)



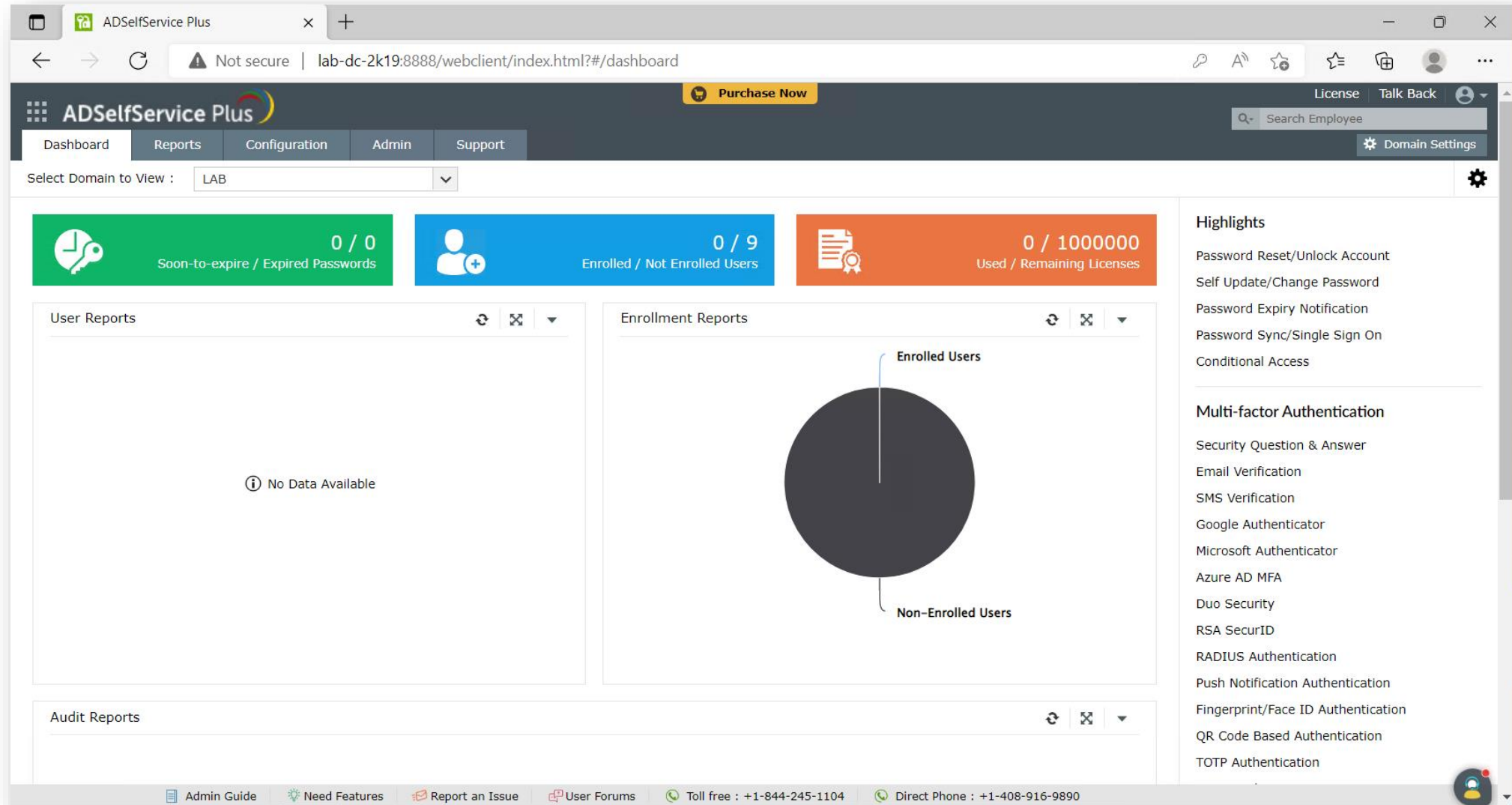
Running ADSelfService Plus

(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)

ADSelfService Plus

Policy Configuration

VPN MBUM

☐ **Reset Password**
Enable users to self-service passwords (without supplying old password).

☐ **Unlock Account**
Enable users to unlock their accounts using self-authentication info.

☐ **Self Update**
Enable users to self-service update Active Directory. Choose a [Self Update Layout](#).

☒ **Change Password**
Enable users to change their passwords (by supplying old passwords).

Select OUs/Groups

Save Policy Cancel

+ Add New Policy

Select OUs/Groups from your Domain in the New Policy

The screenshot displays the ADSelfService Plus web application. A modal dialog titled "Select OUs/Groups" is open, showing a list of groups from the "LAB" domain. The "Groups" tab is active, and three groups are listed: "VPN-Administrators", "VPN-Employees", and "VPN-Vendors". All three groups have their selection checkboxes checked, and these rows are circled in red. The background shows the main interface with a sidebar menu and a "Policy Configuration" section.

Select OUs/Groups Dialog:

- Select Domain: LAB
- Tab: Groups
- Search: [x]
- Page: 1-3 of 3

<input checked="" type="checkbox"/>	Group Name	Group Type	Location
<input checked="" type="checkbox"/>	VPN	All	
<input checked="" type="checkbox"/>	VPN-Administrators	Security	LAB.local/MBUM/GROUPS
<input checked="" type="checkbox"/>	VPN-Employees	Security	LAB.local/MBUM/GROUPS
<input checked="" type="checkbox"/>	VPN-Vendors	Security	LAB.local/MBUM/GROUPS

- Selected: 0 OUs 3 Groups
- Buttons: OK, Cancel

New Policy is ready

The screenshot displays the ADSelfService Plus web interface. The top navigation bar includes the logo, a 'Purchase Now' button, and links for 'License', 'Talk Back', and a user profile. Below this is a secondary navigation bar with tabs for 'Dashboard', 'Reports', 'Configuration', 'Admin', and 'Support'. The 'Configuration' tab is active, and the left sidebar shows a tree view with 'Self-Service' expanded, containing 'Policy Configuration' (selected), 'Multi-factor Authentication', 'Password Expiration Notification', 'Password Policy Enforcer', 'Password Sync/Single Sign On', 'Conditional Access', and 'Directory Self Service'. The main content area is titled 'Policy Configuration' and features a 'Self-Service Features' section with icons for 'Reset Password', 'Unlock Account', 'Change Password', and 'Self Update'. Below this is a text instruction: 'Click "Add New Policy" Button to add a new policy. To edit an existing policy, click on [edit icon] icon in the Actions column.' The 'Available Policies' section includes a search bar and a table with one policy listed. The 'Policy Name' 'VPN MBUM' is circled in red. A '+ Add New Policy' button is located at the top right of the table.

ADSelfService Plus [Purchase Now](#) [License](#) [Talk Back](#) [Search Employee](#) [Domain Settings](#)

Configuration | Admin | Support

Self-Service

- Policy Configuration
- Multi-factor Authentication
- Password Expiration Notification
- Password Policy Enforcer
- Password Sync/Single Sign On
- Conditional Access
- Directory Self Service

Administrative Tools

Security Center

Policy Configuration

Self-Service Modes

Self-Service Features

- Reset Password
- Unlock Account
- Change Password
- Self Update

Click "Add New Policy" Button to add a new policy. To edit an existing policy, click on [edit icon] icon in the Actions column.

Available Policies [+ Add New Policy](#)

Actions	Advanced	Policy Name	Permissions	Domain Name	Last Modified By	Last Modified Time
[edit] [delete] [clone]	[gear]	VPN MBUM	Change Password	LAB	admin (ADSelfService Plus Aut...	Today 06:03 PM

Configure MFA for Endpoints

ADSelfService Plus [Purchase Now](#) [License](#) [Talk Back](#) [Search Employee](#) [Domain Settings](#)

Configuration | Admin | Support

Self-Service

- Policy Configuration
- Multi-factor Authentication**
- Password Expiration Notification
- Password Policy Enforcer
- Password Sync/Single Sign On
- Conditional Access
- Directory Self Service

Administrative Tools

Security Center

Multi-factor Authentication

Choose the Policy: **VPN MBUM**

Authenticators Setup | **MFA for Reset/Unlock** | **MFA for Endpoints** | MFA for Applications | MFA Enrollment | Advanced

Please enable [HTTPS](#) in Access URL and Connection Settings to be able to enable MFA for endpoints.

MFA for Machine Login
Supported : Windows/macOS/Linux

☐ Enable **1** factor authentication for Machine login.

Choose authenticators for Machine Login MFA: - No factor selected -

MFA for OWA Login
Supported : OWA/ECP of Exchange Server

☐ Enable **1** factor authentication for OWA Login.

Choose authenticators for OWA Login MFA: - No factor selected -

MFA for VPN Login
VPN providers that support RADIUS authentication

☐ Enable **1** factor authentication for VPN login.

Choose authenticators for VPN login: - No factor selected -

Save Settings **Cancel**

[Admin Guide](#) [Need Features](#) [Report an Issue](#) [User Forums](#) [Toll free : +1-844-245-1104](#) [Direct Phone : +1-408-916-9890](#)

Enable HTTPS and Configure Access URL !!

(import or generate self-signed certificate)

The image shows the ADSelfService Plus configuration interface with three numbered steps:

- Step 1:** In the **Connection Settings** tab, the **ADSelfService Plus Port [https]** is set to **9251**. The **Apply SSL Certificate** link is visible next to the port field.
- Step 2:** The **Apply SSL Certificate** dialog is open. Under **Select an Option**, **Apply Certificate** is selected. The **Upload Certificate File** field shows **MBUM-2022.p12** with a **Browse** button. The **Certificate Password** field is masked with dots.
- Step 3:** The **Configure Access URL** dialog is open. The **Server Name** is **mbum.rakus.org**, the **Protocol** is **HTTPS**, and the **Port** is **9251**. A **Save** button is at the bottom.

Changes will reflect only on restart of ADSelfService Plus.

Enable Push Notification Authentication

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

MFA for VPN Login ⓘ

VPN providers that support RADIUS authentication

ⓘ Enable any one of [supported authenticators](#) to configure MFA for VPN login.

☐ Enable 1 factor authentication for VPN login.

Choose authenticators for VPN login - No factor selected -

Save Settings

Cancel

Dashboard Reports Configuration Admin Support

Self-Service
Policy Configuration
Multi-factor Authentication
Password Expiration Notification
Password Policy Enforcer

Multi-factor Authentication ⓘ

Choose the Policy VPN MBUM

Authenticators Setup MFA for Reset/Unlock MFA for Endpoints MFA for Applications

Security Question & Answer Configured

Email Verification

SMS Verification

Google Authenticator

Microsoft Authenticator

Azure AD MFA

Duo Security

RSA SecurID

RADIUS Authentication

Push Notification Authentication

Enable Push Notification Authentication

Note

- Only the ADSelfService Plus mobile app can be used for this authentication method. Get the app from [App Store \(iOS\)](#)/[Play Store \(Android\)](#).
- This is a device-based enrollment. If users install the app in another device, they need to enroll again.
- Restrictions:
 - This option cannot be used for authentication if the application login/password reset/account unlock is performed from the mobile site.
 - This option cannot be used for authentication if the application login/password reset/account unlock is performed from the enrolled devices.

ADSelfService Plus

Dashboard Reports Configuration Admin Support

Self-Service

Policy Configuration
Multi-factor Authentication
Password Expiration Notification
Password Policy Enforcer
Password Sync/Single Sign On
Conditional Access
Directory Self Service

Administrative Tools

Security Center

Multi-factor Authentication ⓘ

Choose the Policy VPN MBUM

Authenticators Setup MFA for Reset/Unlock MFA for Endpoints MFA for Applications

Security Question & Answer Configured

Email Verification

SMS Verification

Google Authenticator

Microsoft Authenticator

Azure AD MFA

Duo Security

RSA SecurID

RADIUS Authentication

Push Notification Authentication Configured

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

The image shows a composite of three screenshots illustrating the configuration of MFA VPN session keep and RADIUS timeout request.

Left Screenshot (Main MFA Settings): Shows the 'VPN MBUM' policy configuration. The 'MFA for VPN Login' section is highlighted with a red circle '1'. It shows 'Enable' checked, '1' factor authentication for VPN login, and 'Push Notification Authentication' selected as the authenticator. A red circle '2' is placed over the 'Save Settings' button.

Middle Screenshot (Advanced Settings): Shows the 'Advanced (VPN MBUM)' settings. The 'VPN Login MFA' section is highlighted with a red circle '3'. It shows 'Keep the VPN MFA session valid for' set to '1' mins. A red dashed arrow points from this setting to the RADIUS server configuration.

Right Screenshot (RADIUS Server Configuration): Shows the 'RADIUS Server <10.100.0.10>' configuration. The 'General' tab is selected. The 'Service' section shows 'ppp' checked. The 'Called ID' is empty, 'Domain' is empty, 'Address' is '10.100.0.10', 'Protocol' is 'udp', and 'Secret' is '*****'. The 'Authentication Port' is '1812' and 'Accounting Port' is '1813'. The 'Timeout' is set to '60000' ms. The 'Accounting Backup' checkbox is unchecked. The 'Realm' is empty, 'Certificate' is 'none', and 'Src. Address' is '10.100.0.1'. The status at the bottom is 'enabled'.

Keep the VPN MFA session valid for __ mins

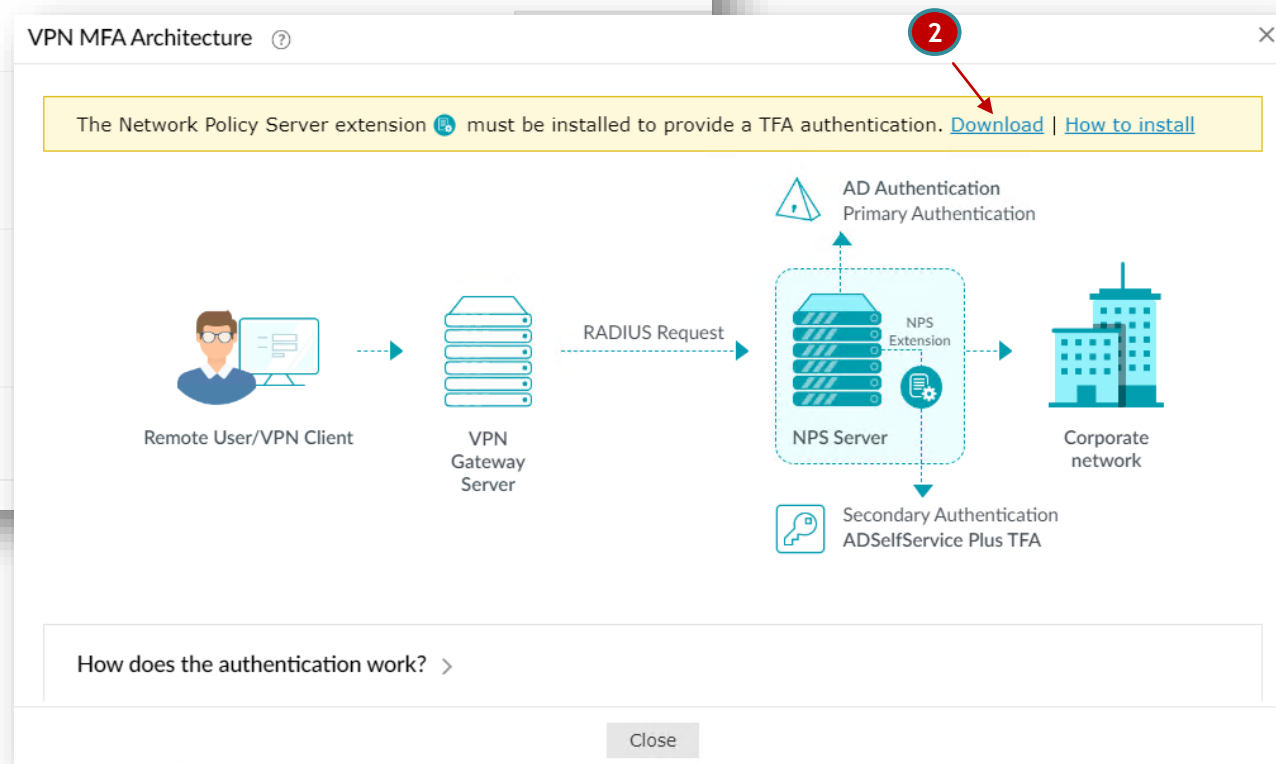
Enabling this setting will set a time limit for the second authentication factor during VPN login.

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

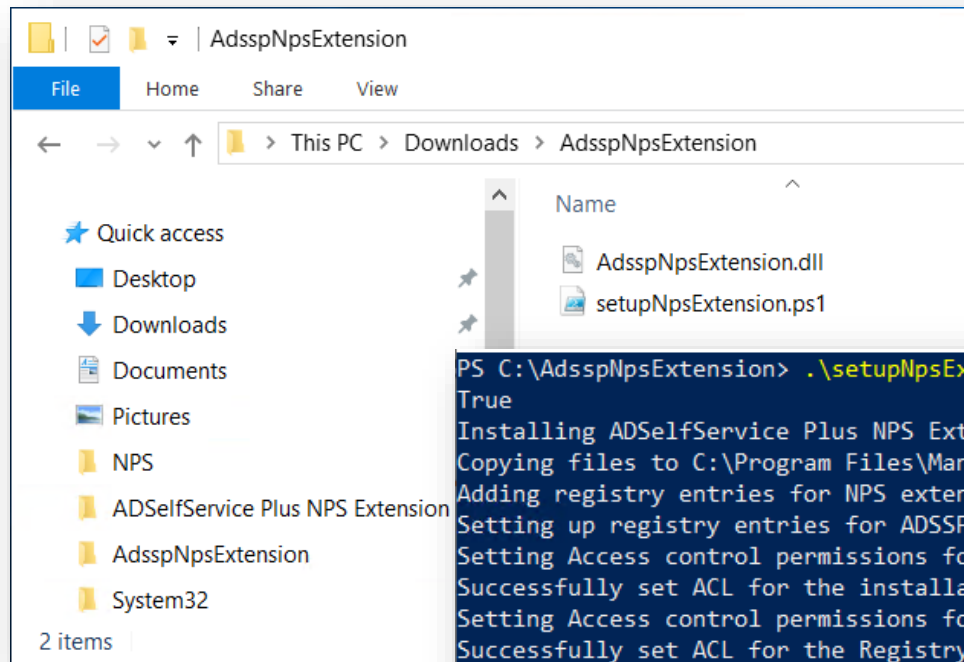
(the most hidden file location in the world !!)

The screenshot shows the NPS configuration interface. The left sidebar has a menu with 'Self-Service' expanded, showing 'Policy Configuration', 'Multi-factor Authentication', 'Password Expiration Notification', 'Password Policy Enforcer', 'Password Sync/Single Sign On', 'Conditional Access', and 'Directory Self Service'. The 'Multi-factor Authentication' section is selected. The main area is titled 'Multi-factor Authentication' and shows a 'Choose the Policy' dropdown set to 'VPN MBUM'. Below this are tabs for 'Authenticators Setup', 'MFA for Reset/Unlock', 'MFA for Endpoints', and 'MFA for Applications'. A yellow banner states: 'Please purchase ADSelfService Plus' Endpoint MFA Add-on to enable this feature. Buy Now'. Below this, there are sections for 'MFA for Machine Login' (with an 'Enable' checkbox and a dropdown set to '1'), 'MFA for OWA Login', and 'MFA for VPN Login'. A red circle with the number '1' is placed over the 'MFA for VPN Login' section, which is described as 'VPN providers that support RADIUS authentication'.



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\ZOH0 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)

Administrator: Windows PowerShell ISE

```
File Edit View Tools Debug Add-ons Help

setupNpsExtension.ps1 X
1 param (
2     [Parameter(Mandatory=$true)][string]$operation
3 )
4
5 $currentUser = [Security.Principal.WindowsIdentity]::GetCurrent()
6 if(!(New-Object Security.Principal.WindowsPrincipal $currentUser.IsAuthenticated))
7 {
8     Write-Host ("Please run the setup script as administrator")
9     exit
10 }
11
12 ##### ADSSP NPS Extension CONFIGURATION Settings #####
13
14 ### Server/Nps/Mfa settings
15 $serverName = "mbum.rakus.org"
16 $serverPortNo = "9251"
17 $secretKey = "qS27XnldkPsszTQNMxc8ECgquVHQOMQNRXUCpoci"
18 $mfaStatus = "true"
19 $radiusApp = "VPN"
20 $serverSSLValidation = "true"
21 $bypassMFAOnConnectionError = "false"
22 $serverContextPath = ""
23
24
```

Configure Access URL

* Server Name

* Protocol ☐ HTTP ☒ HTTPS

* Port

Save

Administrator: Windows PowerShell

```
PS C:\AdsspNpsExtension> ping mbum.rakus.org

Pinging mbum.rakus.org [10.100.0.10] with 32 bytes of data:
Reply from 10.100.0.10: bytes=32 time<1ms TTL=128
Reply from 10.100.0.10: bytes=32 time<1ms TTL=128
Reply from 10.100.0.10: bytes=32 time<1ms TTL=128
Reply from 10.100.0.10: bytes=32 time<1ms TTL=128
```

DNS Manager

File Action View Help

DNS	
LAB-DC-2K19	
Forward Lookup Zones	
_msdcs.LAB.local	
LAB.local	
mbum.rakus.org	
Reverse Lookup Zones	
Conditional Forwarders	

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[4], lab-dc-2k19.lab.local, h...	static
(same as parent folder)	Name Server (NS)	lab-dc-2k19.lab.local.	static
(same as parent folder)	Host (A)	10.100.0.10	static

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

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

The image shows two overlapping screenshots. The top screenshot is the Mikrotik WinBox Firewall NAT configuration window. It displays a table of NAT rules. Rule 0 is a 'dst-nat' rule that maps traffic from 10.100.0.10 to 192.168.45.211 on port 9251. Rule 1 is a 'masquerade' rule for the 'srcnat' chain. The bottom screenshot is the ADSelfService Plus login page, showing a 'Log In' form with fields for username, password, and a 'LAB' dropdown. A 'Login' button is present, along with links for 'Forgot your password?' and 'Account locked out?'. A red dashed arrow points from the 'your choice' box to the 'ADSelfService Plus through PROXY' rule in the bottom screenshot.

Firewall NAT Configuration Table:

#	Action	Chain	Dst. Address	Protocol	Dst. Port	In. Interface	Out. Interface	To Addresses	To Ports	Bytes	Packets	Comment
0	dst-nat	dstnat	192.168.45.211	6 (tcp)	9251	ether1		10.100.0.10	9251	180 B	3	ADSelfService Plus
1	masquerade	srcnat					ether1			147.9 KiB	1 602	PAT for INTERNET

ADSelfService Plus Login Page:

Log In

employee1

.....

LAB

Login

First time user? Use 'admin' as password

Forgot your password?

Account locked out?

English

Layer7 Protocols Configuration Table:

Interface	Out. Interface	To Addresses	To Ports	Bytes	Packets	Comment
ether1		10.100.1.20	443	180 B	3	ADSelfService Plus through PROXY
	ether1			25.5 KiB	313	PAT for INTERNET

* 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)

ADSelfService Plus

Change Password | Enrollment

User Registration

Please enroll for the forced verification methods enabled for your account.

Push Notification Authentication

You can enroll for this authentication method only from the ADSelfService Plus mobile app.
[Install ADSelfService Plus Mobile App](#)

Steps to enroll for Push Notification Authentication

1. Open ADSelfService Plus Mobile app and log in with your domain username and password.
2. Tap the user icon and select Enrollment.
3. Select the Mobile App Authenticator icon and enable the Push Notification authentication method.
4. Now tap Enroll/Update at the top.

Steps to download and configure the mobile app

Install Mobile App

- Visit the Apple App Store or Google Play Store to download and install the ADSelfService mobile app. For more details [click Here](#)

Configure Mobile App Server Settings

- Open ADSelfService Plus Mobile App and tap the **Server Settings** link in the home screen.
- In the bottom-left corner, tap **Scan QR Code** button.
- Scan the QR code shown here to automatically update server settings.

Use the app to reset your password/unlock your account on-the-go.

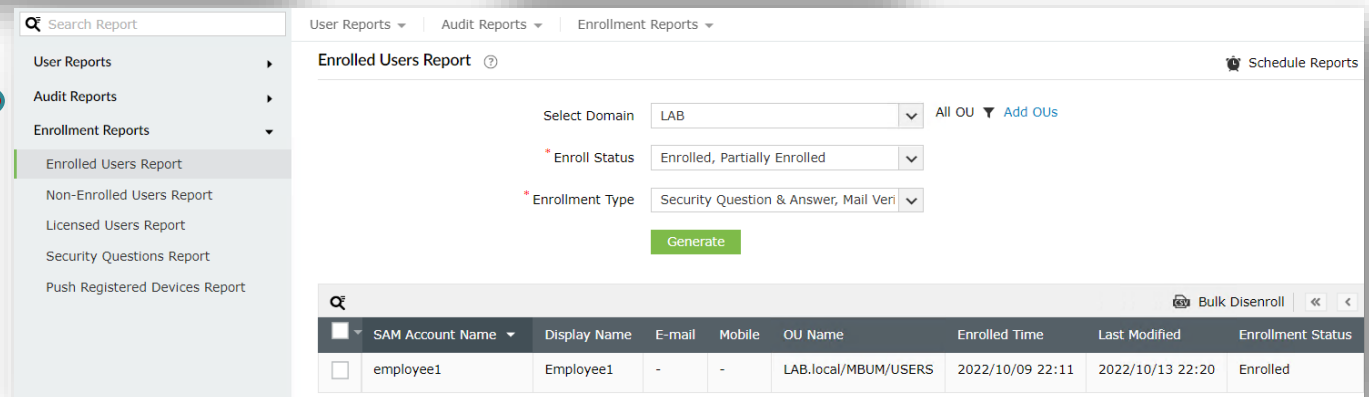
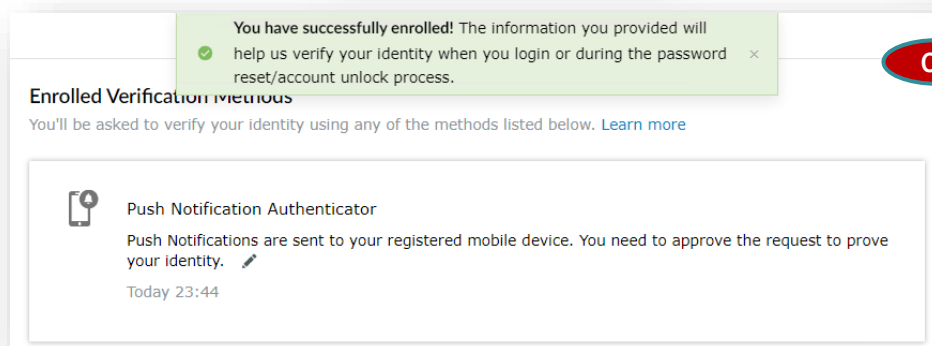
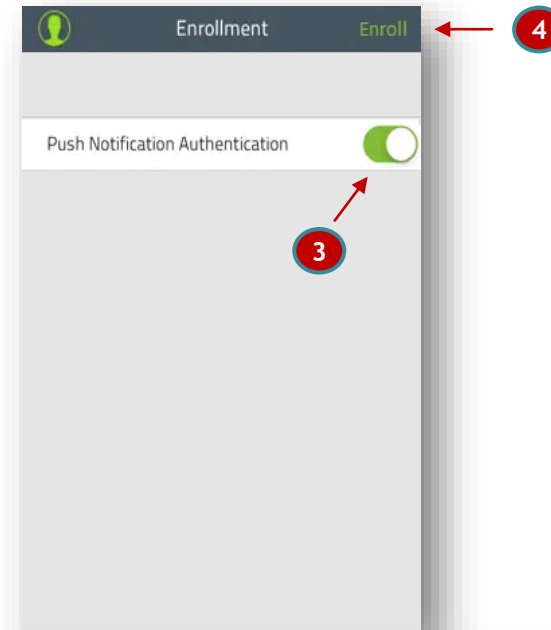
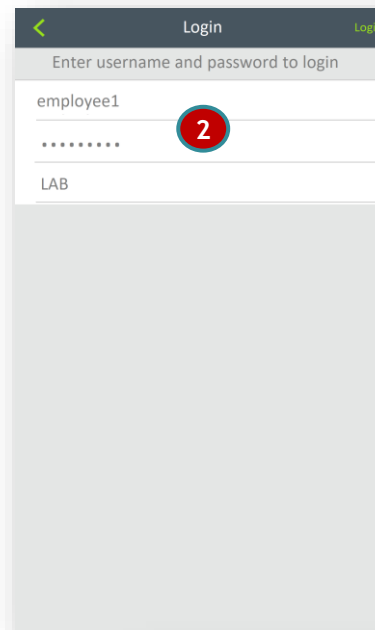
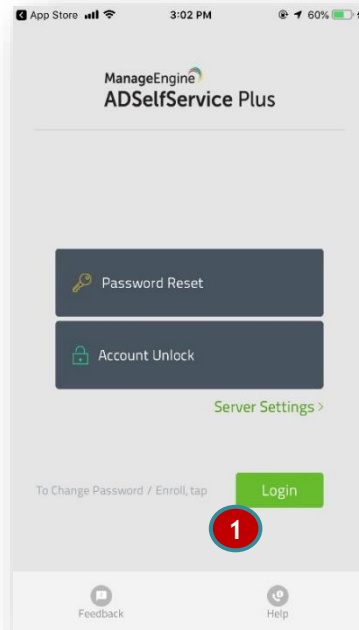
Server Settings

mbum.rakus.org
9251
Protocol: HTTP | HTTPS
https://mbum.rakus.org:9251

How to Setup?

Scan QR Code | Save

User enrollment and Push activation



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"
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
```

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 instal

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
17f5000000000000000018da6dedbaee
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."
```

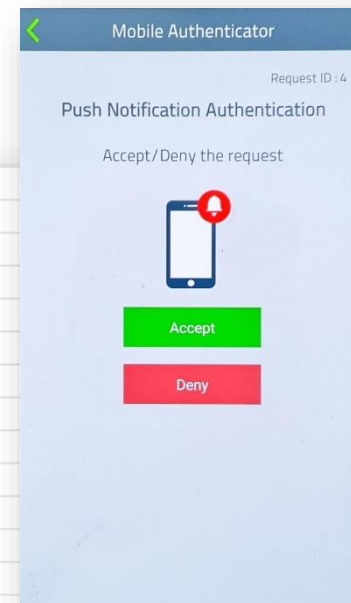
sstp, ppp, info	<ssstp-employee1>: authenticated
sstp, ppp, info	<ssstp-employee1>: connected

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