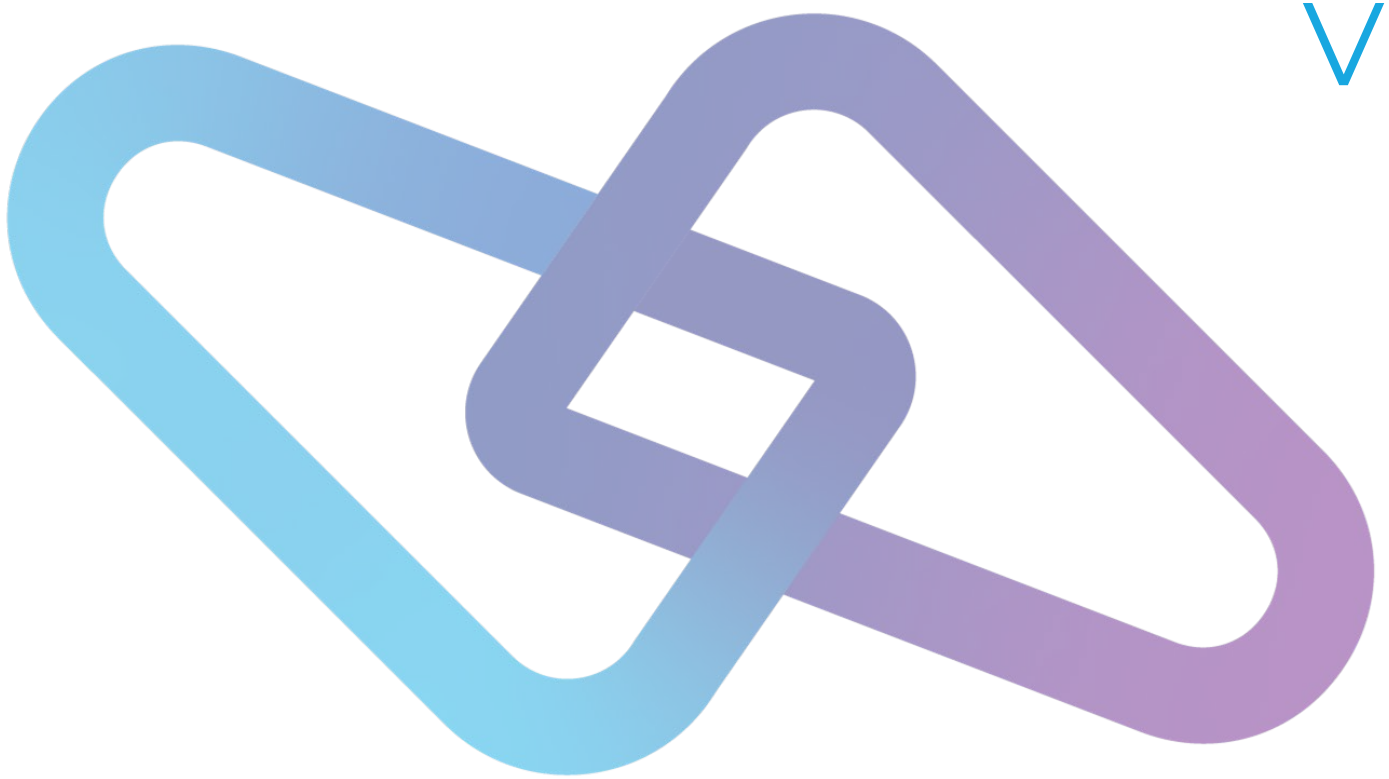
VSEn Secured with MFA

Enhancing Security with LDAP and MFA



Aleksa Medakovic

Software Engineer, 21CS

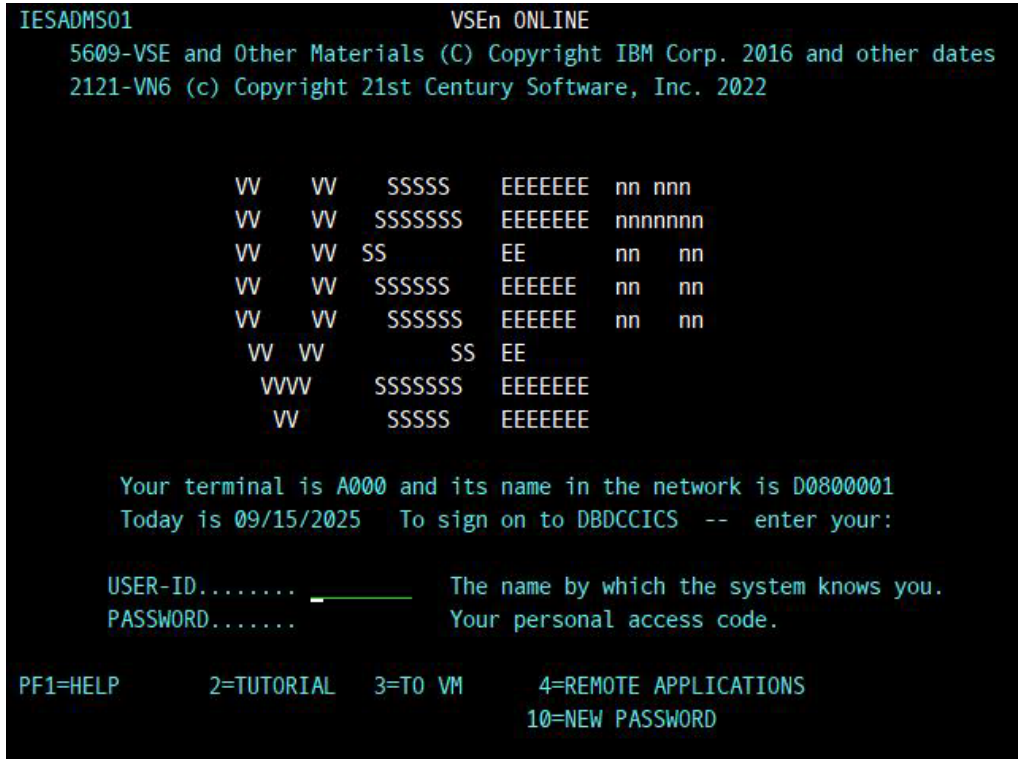
AGENDA

1. VSEn Role in Authentication
2. Introduction to MFA
3. One Way to MFA: The slapo-otp Approach
4. Implementing MFA
5. Considerations & Alternatives
6. Q&A Session

VSEn’s Role in Authentication

The Challenge: Per default, VSEn provides only **single-factor authentication**.

⟶ VSEn can be set up to use LDAP client to connect to an LDAP server (outside of VSEn), in our case, OpenLDAP.



Introduction to LDAP

LDAP (Lightweight Directory Access Protocol) is an open standard for accessing and managing directory information services over an IP network, commonly used for centralized authentication and identity management.

Directory Access

Read and write user, group, and resource entries in a hierarchical tree

Open Standard

Defined by IETF RFCs and supported across virtually every OS and language

Authentication

Centralized login, identity lookup, and access control

Introduction to OpenLDAP

OpenLDAP is open-source implementation of the LDAP protocol

Open Source

slapd Server

Standalone LDAP daemon with replication and scalable backends

Extensible

Overlays and schemas like slapo-otp add features like MFA

Introduction to Multi-Factor Authentication (MFA)

MFA requires two or more verification factors to grant access, creating a critical defense against credential stuffing, and compromised passwords.

Something You Know

Passwords, PINs, security questions

Something You Have

Mobile devices, hardware tokens, smart cards

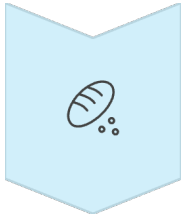
Something You Are

Biometrics like fingerprints, facial recognition

One Way to MFA: OpenLDAP with slapo-otp Approach

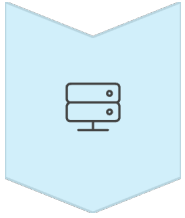
User Initiation

User combines password with current OTP from authenticator app



Application Layer

Application, in our case the sign-on panel, sends combined string to OpenLDAP server via LDAP bind



Server Processing

OpenLDAP server with slapo-otp overlay intercepts and validates both authentication factors

Authentication Result

Success only when both password and OTP validation pass

One Way to MFA: OpenLDAP with slapo-otp Approach

The slapo-otp Configuration

The slapo-otp overlay adds a second authentication layer directly to OpenLDAP, enabling one-time password validation within the directory server itself.

01

Overlay configuration

slapo-otp integrates seamlessly with existing OpenLDAP infrastructure

02

OTP Integration

Users append their time-based OTP to their regular password

03

Dual Validation

Both password and OTP are verified in a single authentication request

Our PoC

1 OpenLDAP Server

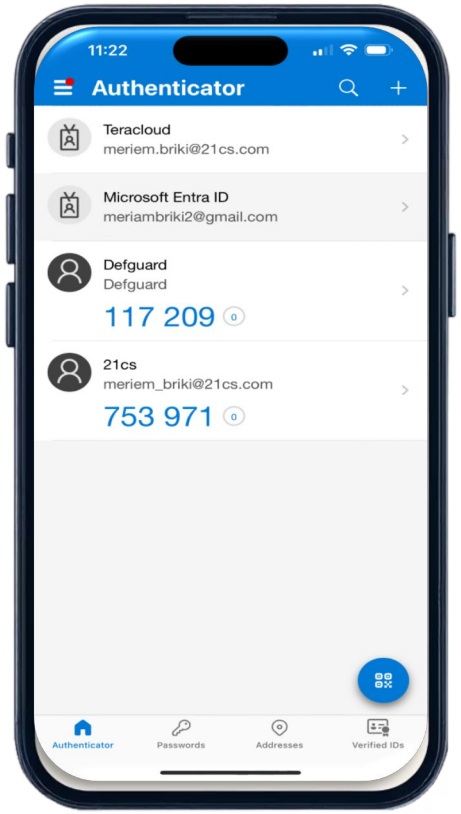
Configured with slapo-otp overlay and test user accounts

2 User Configuration

Test user with otpSecret attribute and standard password

3 Mobile Authenticator

Authenticator or similar TOTP-compatible app



The slapo-otp Configuration

01. Overlay Configuration - Loading the slapo-otp Overlay

Step 1: using otp_ldap.ldif file then modify the slapd config with the command below:

```
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: otp.la
```

Command: `ldapmodify -Y EXTERNAL -H ldapi:// -D cn=config -W -f /appdata/open_ldap/otp_load.ldif`

```
root@pthvlg-vtape-01:/usr/local/bin# ldapmodify -Y EXTERNAL -H ldapi:// -D cn=config -W -f /appdata/open_ldap/otpload.ldif
Enter LDAP Password:
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config"
```

← Output

Step 2: add overlay to LDAP database with this file otp_overlay.ldif

```
dn: olcOverlay=otp,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
```

Command: `ldapadd -Y EXTERNAL -H ldapi:// -D cn=config -W   -f /appdata/open_ldap/otp_overlay.ldif`

```
root@pthvlg-vtape-01:/usr/local/bin# ldapmodify -Y EXTERNAL -H ldapi:// -D cn=config -W -f /appdata/open_ldap/otpload.ldif
Enter LDAP Password:
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config"
```

← Output

Step 3: Configure OTP parameters:

otp_parms.ldif:

```
dn: ou=people,dc=21csw,dc=com,dc=au
changetype: modify
add: objectClass
objectClass: oathTOTPParams
-
add: oathOTPLength
oathOTPLength: 6
-
add: oathHMACAlgorithm
oathHMACAlgorithm: 1.2.840.113549.2.7
-
add: oathTOTPTimeStepPeriod
oathTOTPTimeStepPeriod: 30
-
add: oathTOTPTimeStepWindow
oathTOTPTimeStepWindow: 3
```

Command:

```
ldapmodify -x -D cn=admin,dc=21csw,dc=com,dc=au -W -f
/appdata/open_ldap/otp_parms.ldif
```

Output:

```
root@pthvlg-vtape-01:/usr/local/bin# ldapmodify -x -D cn=admin,dc=21csw,dc=com,dc=au -W -f /appdata/open_ldap/otp_parms.ldif
Enter LDAP Password:
modifying entry "ou=people,dc=21csw,dc=com,dc=au"
```

02. OTP Integration

Step 1: Generate a random key, this will be shared between the server and the user

```
openssl rand 80 > key
```

Step 2: Enable TOTP authentication for the user in user_token.ldif

```
dn: uid=userxyz,ou=people,dc=21csw,dc=com,dc=au
changetype: modify
add: objectClass
objectClass: oathTOTPToken
-
add: oathTOTPParams
oathTOTPParams: ou=people,dc=21csw,dc=com,dc=au
-
add: oathSecret
oathSecret:<file:/appdata/open_ldap/key
-
add: objectClass
objectClass: oathTOTPUser
-
add: oathTOTPToken
oathTOTPToken:
uid=userxyz,ou=people,dc=21csw,dc=com,dc=au
```

Command:

```
ldapmodify -x -D cn=admin,dc=21csw,dc=com,dc=au -W
-f /appdata/open_ldap/user_token.ldif
```

Output:

```
root@pthvlg-vtape-01:/usr/local/bin# ldapmodify -x -D cn=admin,dc=21csw,dc=com,dc=au -W -f /appdata/open_ldap/user_token.ldif
Enter LDAP Password:
modifying entry "uid=shahinrk,ou=people,dc=21csw,dc=com,dc=au"
```

Step 3: Generate Base32 Key

```
Base32 key > bkey
```

Step 4: Generate the QR code

Install QR code Generator: `apt install qrencode`

```
echo -n
"otpauth://totp/21cs:userxyz@21csw.com.au?secret=$(</appdata/open_ldap/bkey)&issuer=21cs&period=30&digits=6&a
lgorithm=SHA1" | qrencode -t ansiutf8
```

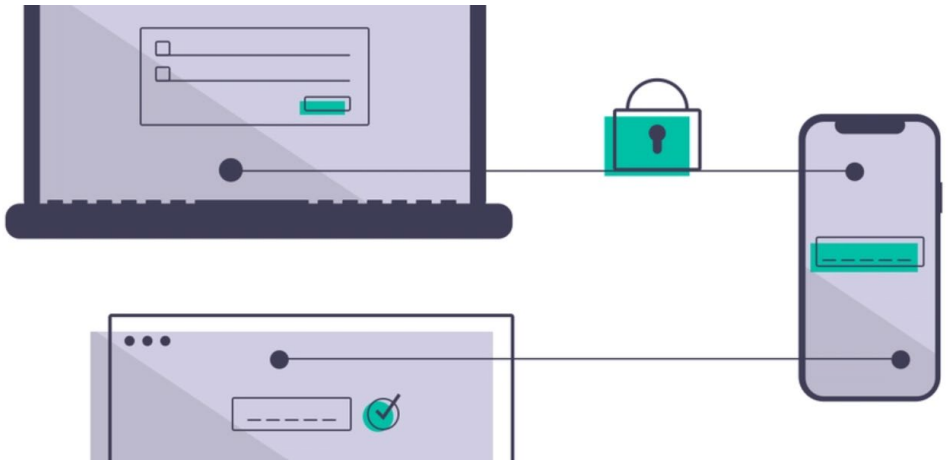
← Output

03. Password verification

Step 1: Open your Authenticator (Microsoft Authenticator) and scan the QR code only once

Step 2: Logon to your VSEn

⟶ Append the 6-digit code to your user password



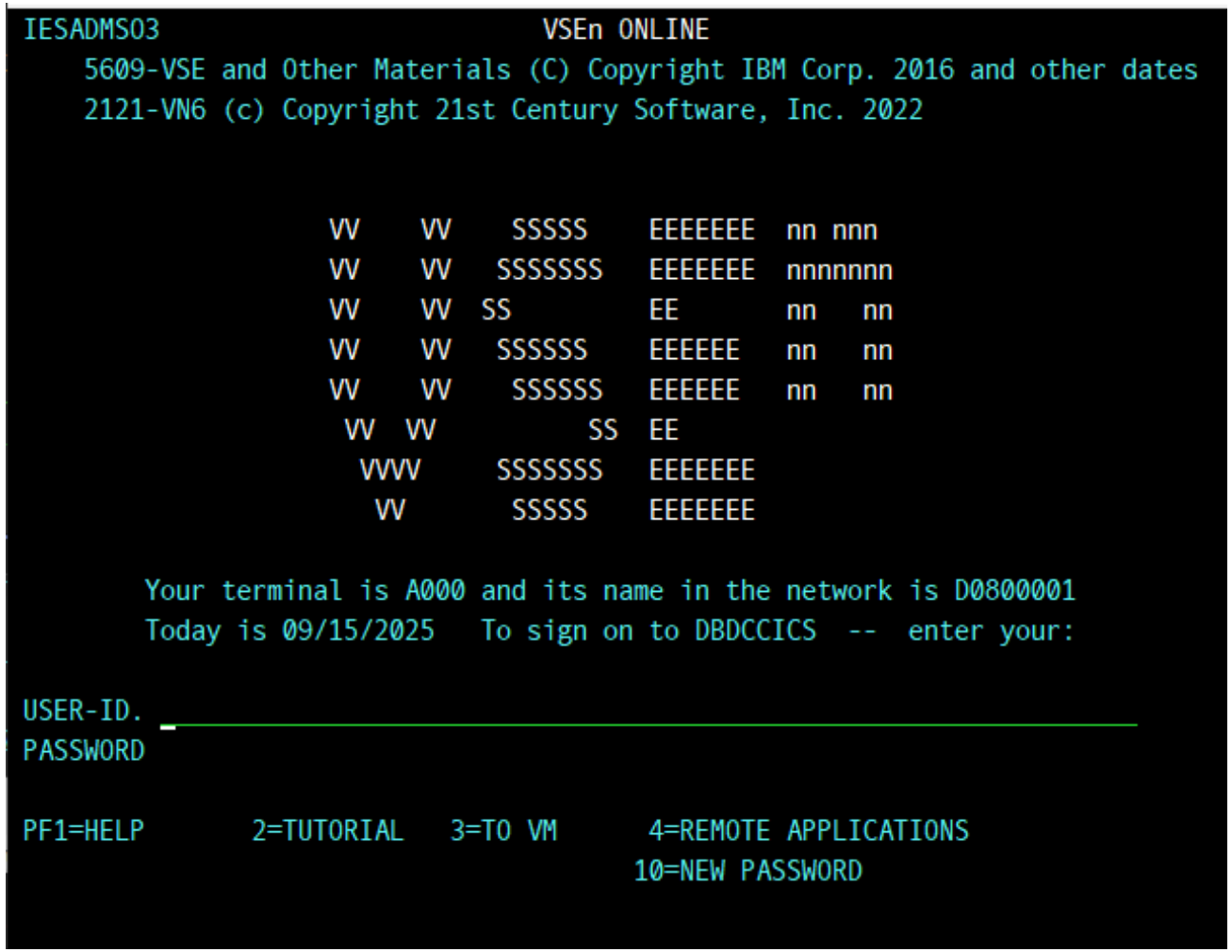
A password that was previously **P@ssw0rd!** will now become **P@ssw0rd!123456**, where P@ssw0rd! remains the static portion and **123456** is the **time-sensitive OTP**.

Configuration from VSEn part

1. Configure and submit your skeleton SKLDCFG.
2. Map LDAP profile to VSEn User.
3. Log off and log in again.

Check the VSEn Administration manual

Output:
New logon Panel



Configure your skeleton SKLDCFG.

```
DN_BIND_PATTERN     DC      CL64'CN=%U,DC=PEOPLE,DC=21CS,DC=COM'
*
* DISTINGUISHED NAME USED FOR BIND WHEN PERFORMING THE SEARCH.
* LEAVE IT BLANK FOR ANONYMOUS BIND
*
BIND_DN             DC      CL64'CN=ADMIN,DC=21CS,DC=COM'
*
* PASSWORD USED FORBIND WHEN PERFORMING THE SEARCH.
* LEAVE IT BLANK FOR ANONYMOUS BIND
*
BIND_PWD            DC      CL64'VMWORKSHOPISGREAT'
*
* USER ID ATTRIBUTE NAME USED WHEN PERFORMING THE SEARCH.
*
USER_ATTRIBUTE      DC      CL64'UID'
*
* BASE DISTINGUISHED NAME USED WHEN PERFORMING THE SEARCH.
*
BASE_DN             DC      CL64'OU=PEOPLE,DC=21CS,DC=COM'
```

Check the VSEn Administration manual

Considerations & Alternatives:

Is Slapo-OTP the right choice for you?

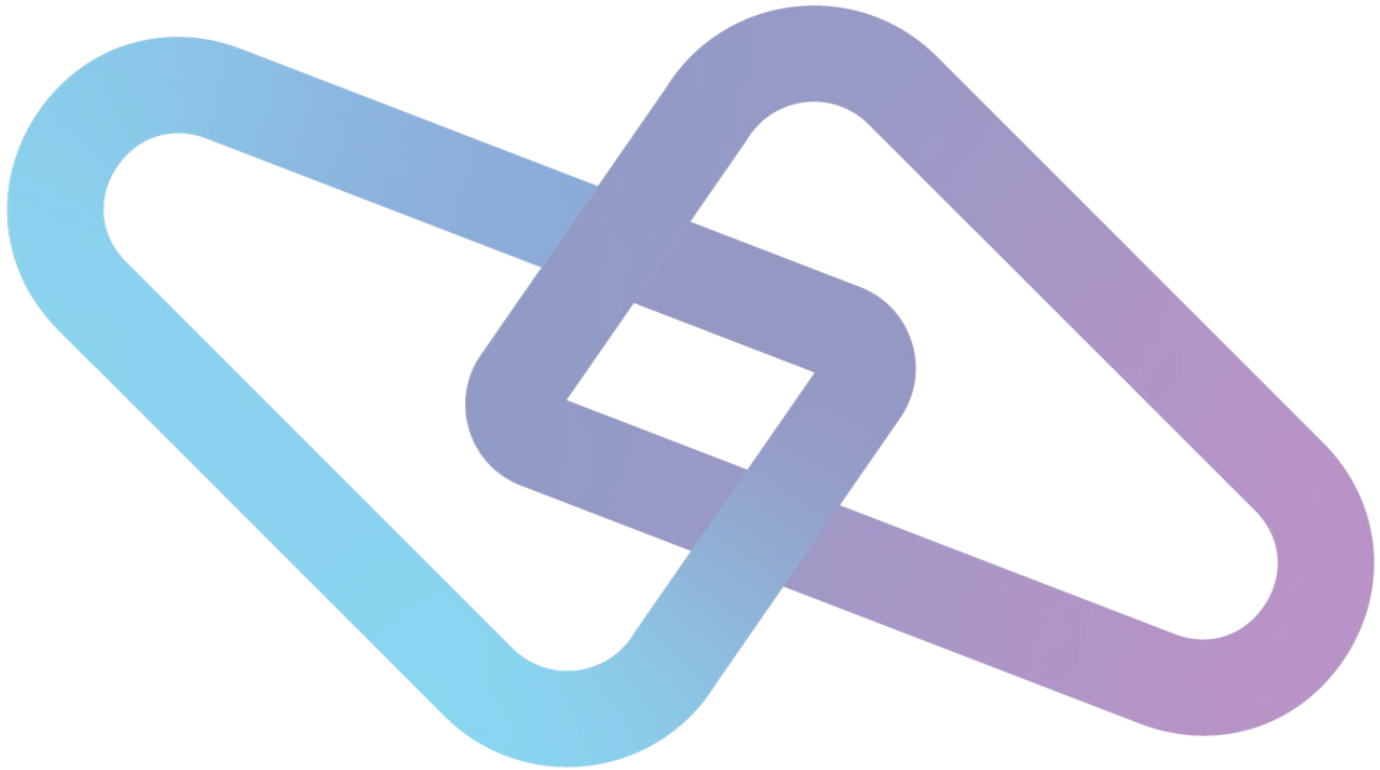
·**The main point:** There is no single "most appropriate" way to implement MFA; it depends on the organization's needs.

·**When slapo-otp may be a good fit:** For environments that are heavily invested in OpenLDAP and want to leverage their existing infrastructure without introducing new services. It's a simple, low-cost solution for adding MFA.

⚠ Check for firewall, network considerations, restrictions on what VSEn can access or not on your enterprise.

·Alternatives:

Other solutions might offer more robust features, like push notifications, biometric integration, or centralized management for a larger range of applications (e.g., RADIUS-based MFA, SAML, or cloud-based identity providers).



Q & A

Thank you!