2nd Annual

MidPoint Community Meetup

Multi-Factor Authentication

Evolveum

Viliam Repáň

Developer at Evolveum

Agenda

- Introduction
- MFA Configuration & Use
- Limitations
- Demo
- Conclusion
- Q & A

Introduction

- Flexible authentication since 4.1
- Different types of login modules
  - Login form
  - Basic
  - LDAP
  - OIDC
  - SAML 2
  - Oracle Duo
  - etc.

Multi-Factor Authentication

- Before midPoint 4.11 3rd party software needed to setup MFA for authentication
- Now, just update security policy
- Currently supports TOTP
  - Various authenticator apps
  - Multiple secrets per user
- Great for air-tight deployments

```
<totp>
    <identifier>mcm-mfa</identifier>
    <issuer>mcm midpoint</issuer>
    <label>fullName</label>
</totp>
```

```
<module id="8">
    <identifier>mcm-mfa</identifier>
    <order>20</order>
    <necessity>required</necessity>
    <acceptEmpty>true</acceptEmpty>
</module>
```

Configuration & Use

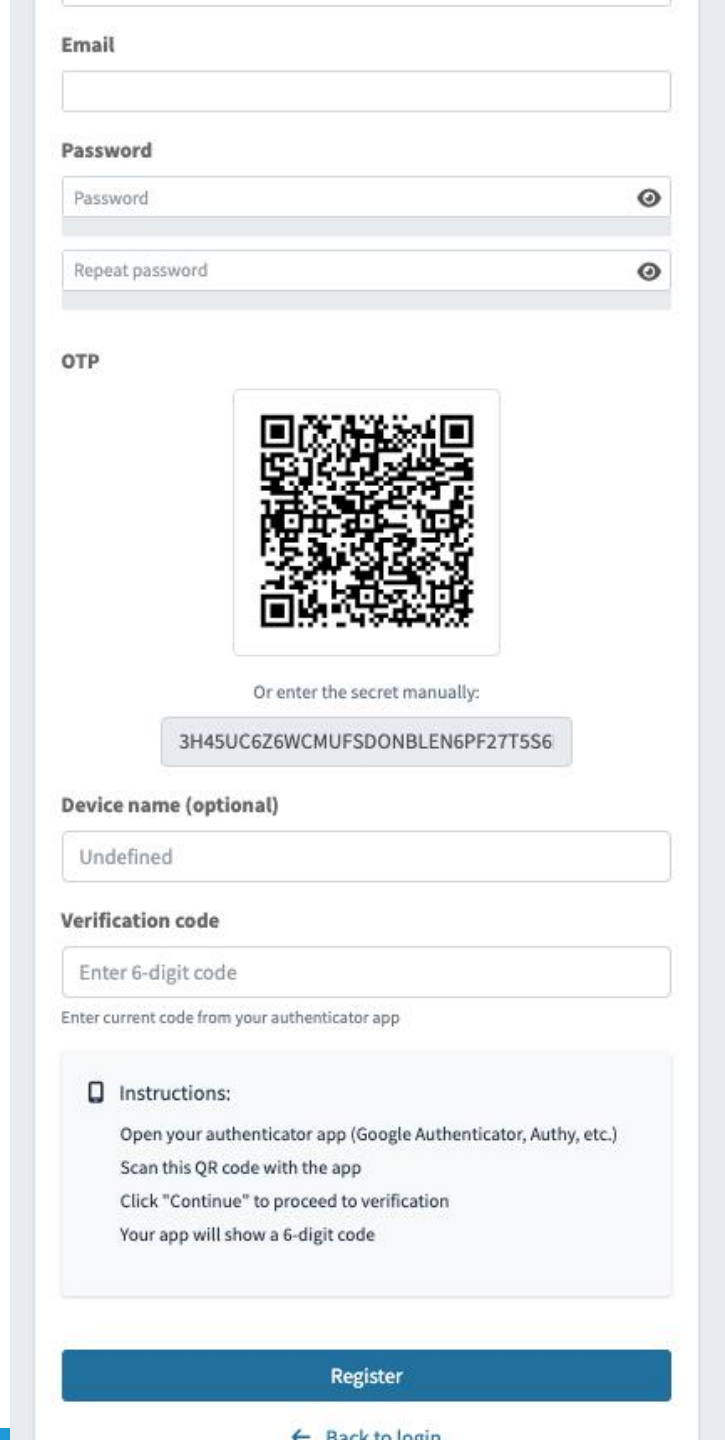
- Security policy configuration
- TOTP module
  - identifier and issuer mandatory, everything else optional (label, algorithm, secretLength, digits)
- Sequence
  - #user (GUI) sequence
  - TOTP module after focus is selected (loginForm, focusIdentification)
  - **acceptEmpty=true** if MFA is not mandatory
- TOTP secrets
  - Stored in credentials container
  - Only **verified=true** validated during authentication

```
<totp>
    <identifier>mcm-mfa</identifier>
    <issuer>mcm midpoint</issuer>
    <label>fullName</label>
</totp>
```

```
<module id="8">
    <identifier>mcm-mfa</identifier>
    <order>20</order>
    <necessity>required</necessity>
    <acceptEmpty>true</acceptEmpty>
</module>
```

Limitations

- Only one TOTP module can be configured in security policy
- TOTP will be available only for GUI authentication (#user channel)
  - admin-gui, emergency
- TOTP setup is not yet supported during user registration, it can be done only later from user profile.



Demo

Conclusion

- No 3rd party software needed to setup MFA
- Simple configuration
- Currently supports TOTP (authenticator apps)


Evolveum
Thank you for your attention
Feel free to ask your questions now!
2nd Annual MidPoint Community Meetup