Password Policies for Local Windows Accounts - Demo

Dr. Brahim Ferik

Knowledge Base

Password Policy and Account Lockout Policy

This document provides an overview of managing local Windows accounts, including adding users, setting passwords, and configuring password policies.

Windows User Management

Adding a User without a Password

To add a user without a password:

```
net user username /add
```

Setting a Password

To set a password for a user:

```
net user username password
```

Setting a Password with Confirmation

To set a password with confirmation:

```
net user username *
```

Deleting a Specific User

To delete a specific user:

```
net user username /delete
```

Viewing All Users on the System

To view all users on the system:

```
net user
```

Password Policies for Local Windows Accounts

Enforce Password History

Enforce password history to prevent reuse of previous passwords (e.g., last 5 passwords).

Maximum Password Age

Set the maximum password age between 30 and 90 days.

Minimum Password Length

Set the minimum password length to 8-12 characters.

Password Complexity Requirements

Enable complexity requirements to ensure passwords meet security standards.

Searching Local Security Policy

To open the Local Security Policy:

`Win + R : secpol.msc`

Alternatively, you can use the command:

`secpol.msc`

Computer Management

To manage local users and groups via Computer Management:

`Win + R : lusrmgr.msc`

Or use the command:

`lusrmgr.msc`

Accessing Local Users and Groups

To access local users and groups in Computer Management:

- Navigate to: Computer Management > System Tools > Local Users and Groups.
- Use the following command to open directly:

```
Win + R : lusrmgr.msc
```