

Real-World Scenario 11-3: Configuring Password Policies and User Account Restrictions

Scenario: As the network security administrator of a company with 5000 users, you are required to enforce complex passwords and make sure that user access to the network is restricted to specific times. More importantly, you *must* employ a certain level of automation. Let's face it, even the fastest computer operator wouldn't be able to keep up with all the password requests and timeframe configurations for users on an individual basis in an enterprise environment such as this. Your organization has a Windows domain with three domain controllers.

In your own words, describe how you would enforce complex passwords and user account restrictions. Explain how you would automate the process, utilize templates, and work with organizational units.

Real-World Scenario 11-3 Solution

A network security administrator will have far too much work to do to have to worry about individual password requests or deal with configuring users one at a time. So the smart admin will utilize password policies that are based on individual organizational units (OUs) in Windows or other similar grouping structures in other operating systems. These policies will default to a self-reset mode, where the users change the passwords themselves, when prompted by the system. And the policy will make sure that the user meets the complexity requirements.

User account restrictions can be configured through policies and by creating a basic user template, off of which other user accounts are based, effectively copying any restrictions from the template to the new user.

By automating as much as possible, the admin reduces the amount of time required for basic configurations and can spend more time researching the latest CVEs and installing required updates.

Video Solution: Watch the video solution "11-3: Configuring Password Policies and User Account Restrictions."

Simulation: Complete the simulation "11-3: Configuring Logon Hours."