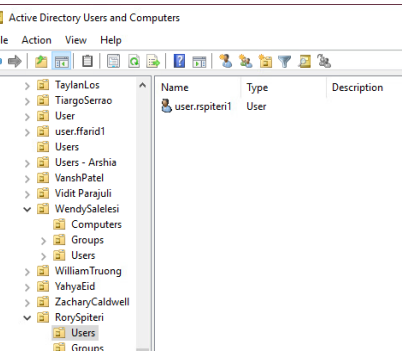
Active Directory Management

Problem: managing thousands of users' computers would be an impossible task, Active directory allows administrators to easily manage group policies from 1 machine. This ensures end users follow safe protocols such as least privilege to minimize the possibilities of compromises by threat actors.

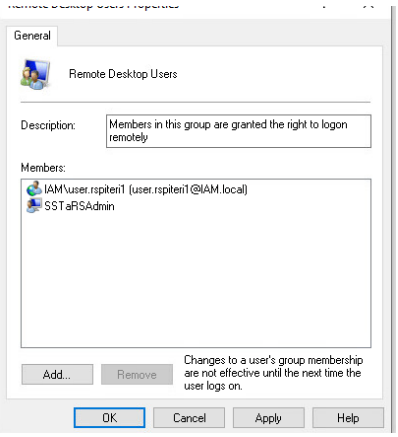
What i learnt: Building and managing a windows domain environment is critical to understanding IT operations and functionality of centralized authentication, policies and user privileges.

Creating a New User

newly acquired individuals will need a standard user account created to allow access to the network.

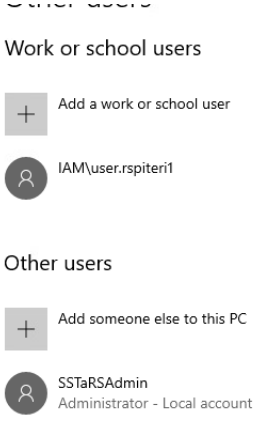


⬅️creating a new user account in users folder



⬅️allowing users to remotely log in

through the admin account setting permissions to work or school user ➡️

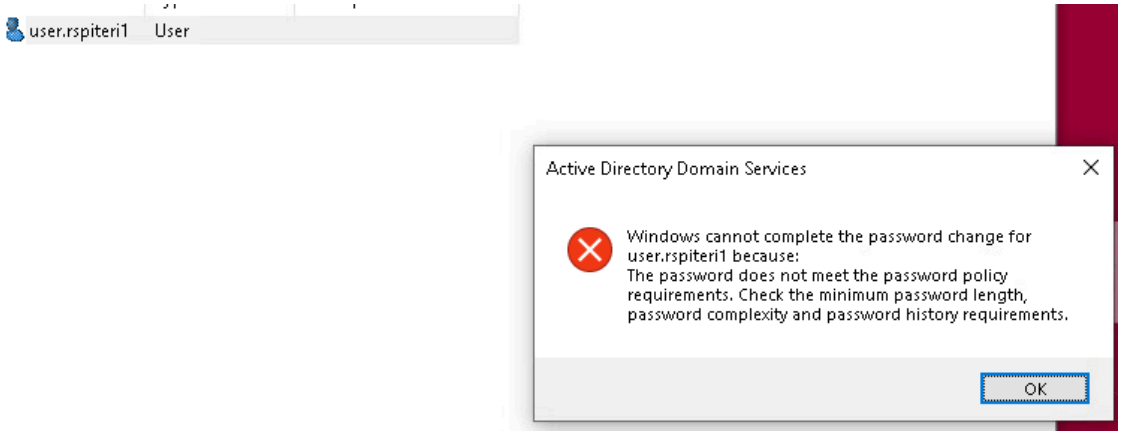


Managing Password Policies for Institution

Creating a secure and complex password is necessary to ensuring that accounts are not compromised through brute force attacks, social engineering and open source intelligence

Policy	Policy Setting
Enforce password history	5 passwords remembered
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	8 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Not Defined

these settings ensure basic password policy to remove the reusing of passwords, standard 8 minimum characters and password complexity requirements (symbols, numbers and capitalized characters)



⬅️(example of user not following password requirements)

Creating Lockout Policies

Lockout policies are critical to preventing nodes being compromised, lockout policies remove the ability for attackers to brute force attack accounts. Adding a timeout policy and threshold for password attempts mitigates such attacks.

Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Allow Administrator account lockout	Enabled
Reset account lockout counter after	30 minutes

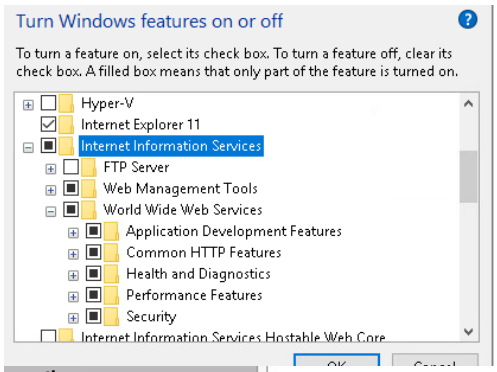
Although lockout policy is a necessity to mitigating brute force attackers. Human nature and memory may accidentally lock themselves out. Active Directory Management allows administrators to unlock accounts.

⬅️(unlocking the account by checking the box)

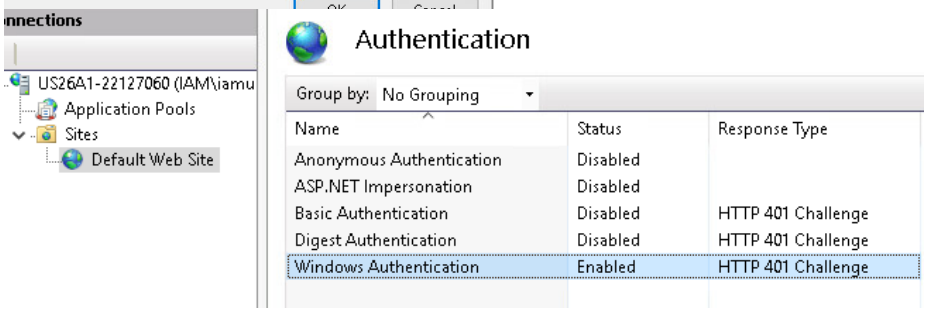
Using HTTP Server Validation for Active Directory

Utilizing HTTP allows company portals and websites to communicate with Active Directory, enabling them to validate a user's identity and permissions before granting or denying access to specific resources.

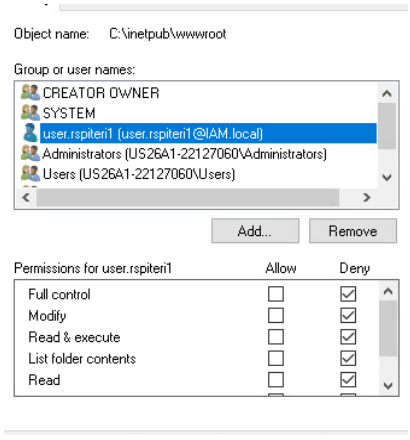
HTTP further allows for a simplified user interface considerably improving efficiency for accessing resources.



⬅️enabling settings for HTTP through Internet Information Services



⬅️Allows users logged into their Windows account to automatically authenticate to the HTTP server through single sign on.



⬅️Edit permissions for end users