FREQUENTLY ASKED QUESTIONS

SATATYA NVR/HVR

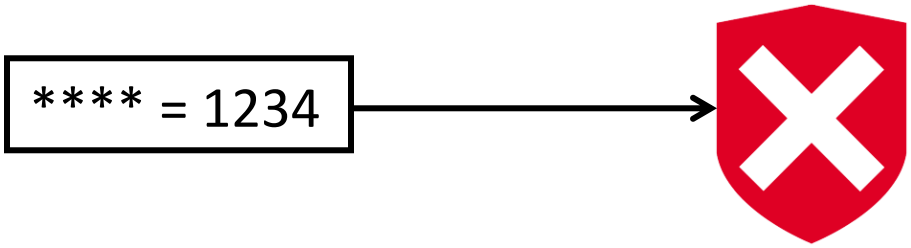
Date: 17th November, 2015

Version: V1R1

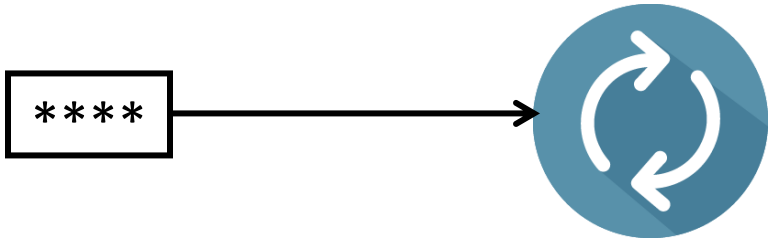
Author: Ashutosh Sharma

MATRIX
TELECOM | SECURITY

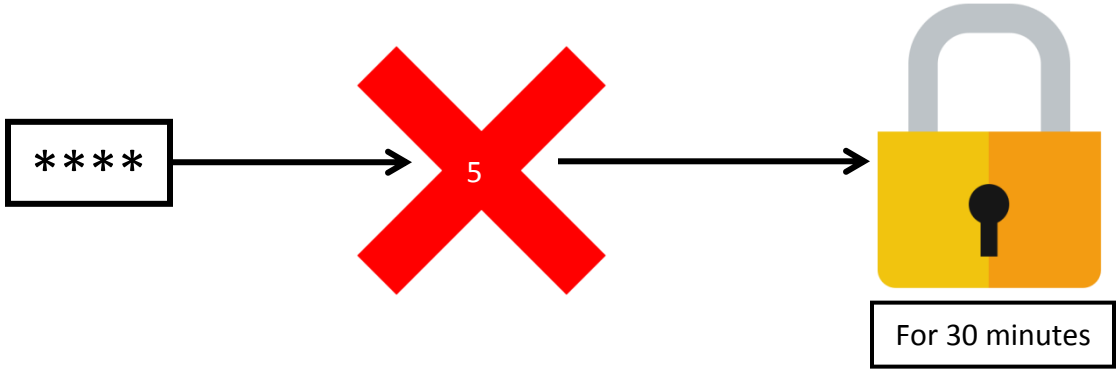
How to Set Password Policy in SATATYA NVR/HVR?



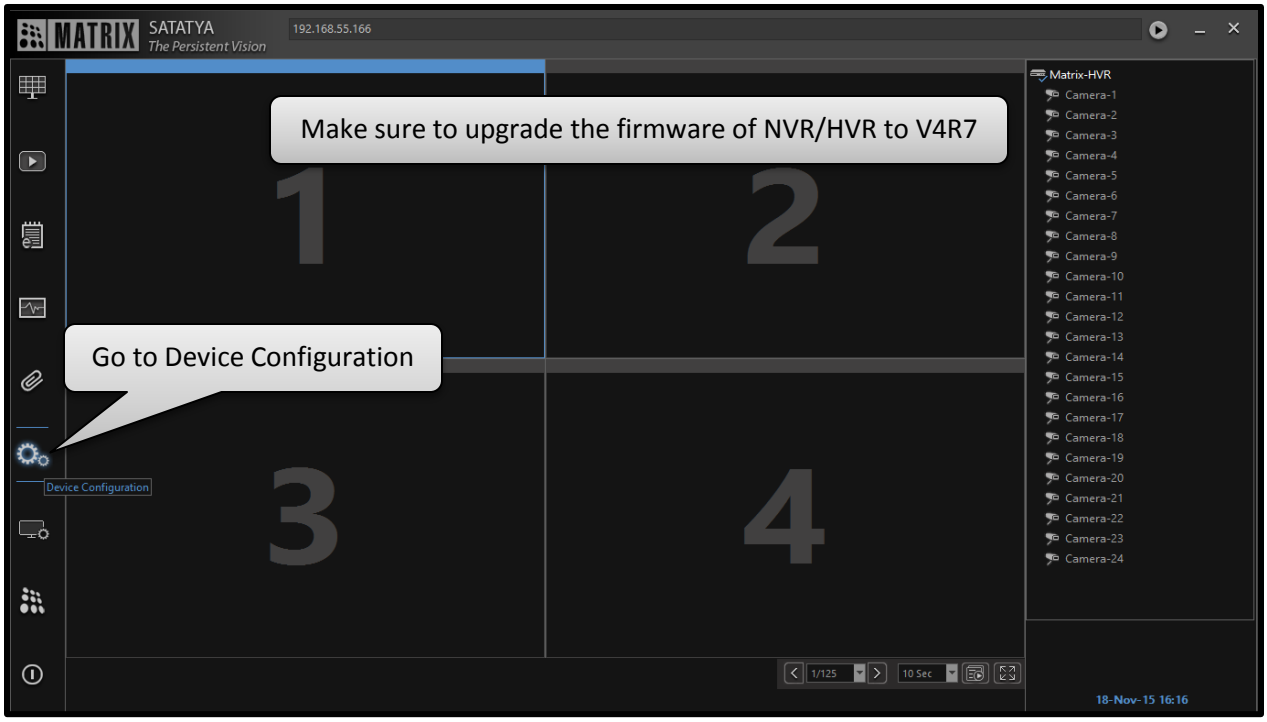
If the password is to be changed, you can set the password strength as either low, medium or high

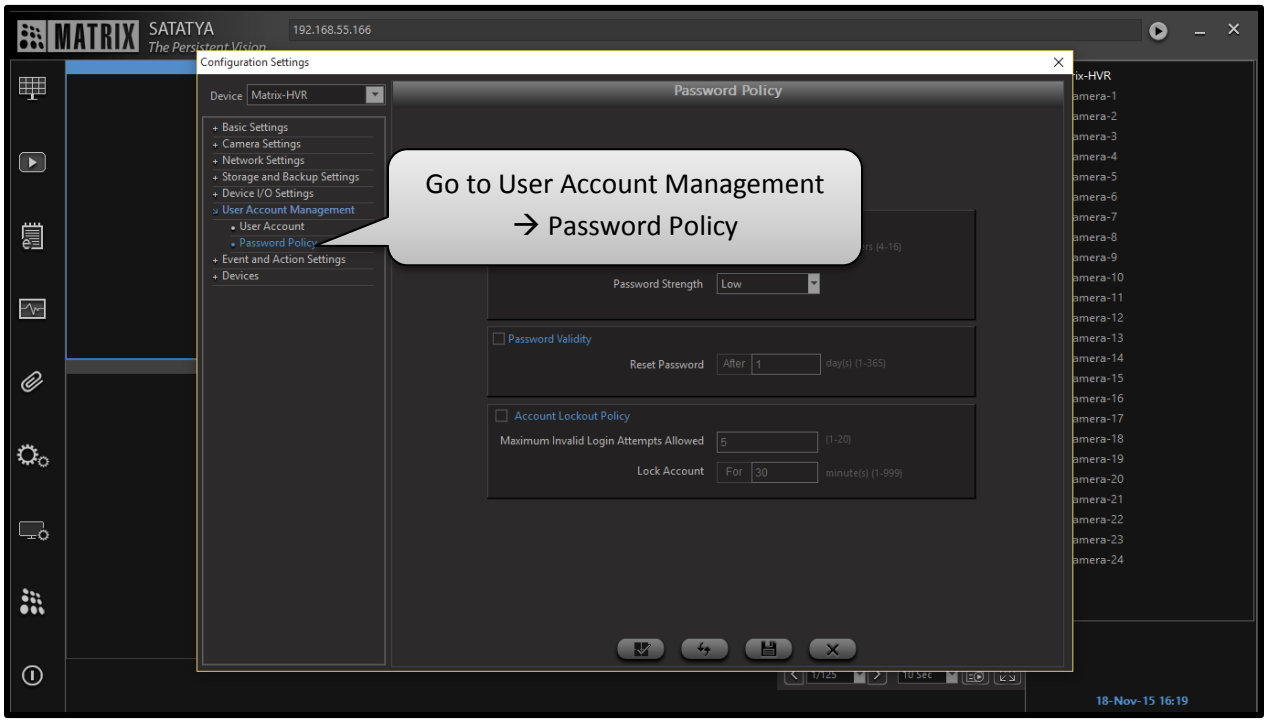


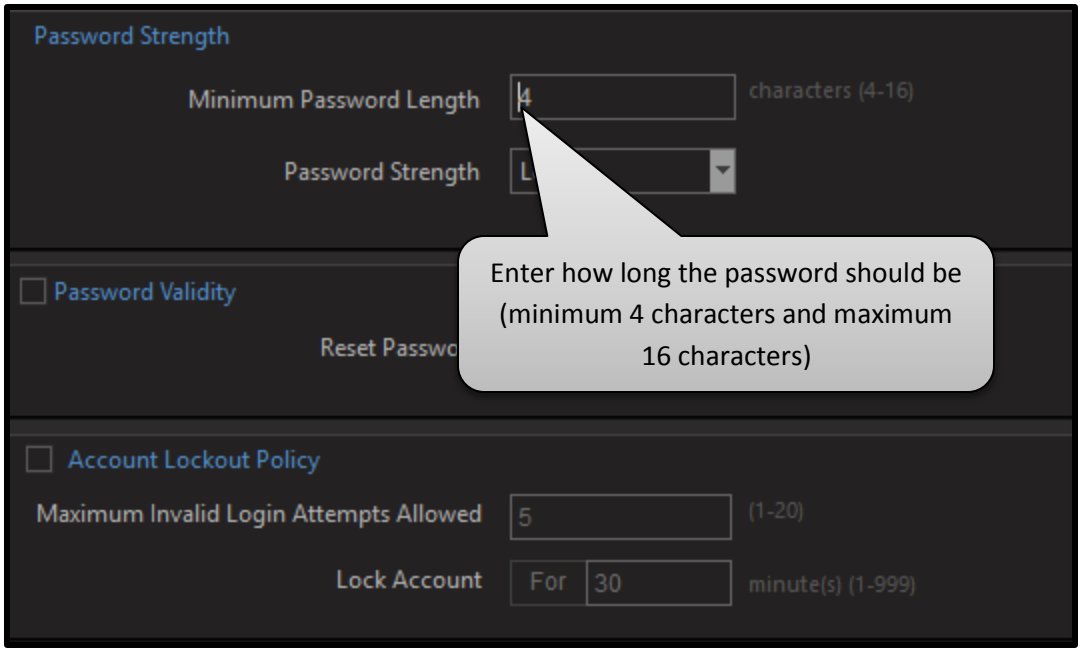
It's a good practice to change password from time to time. You can now set the password reset interval.

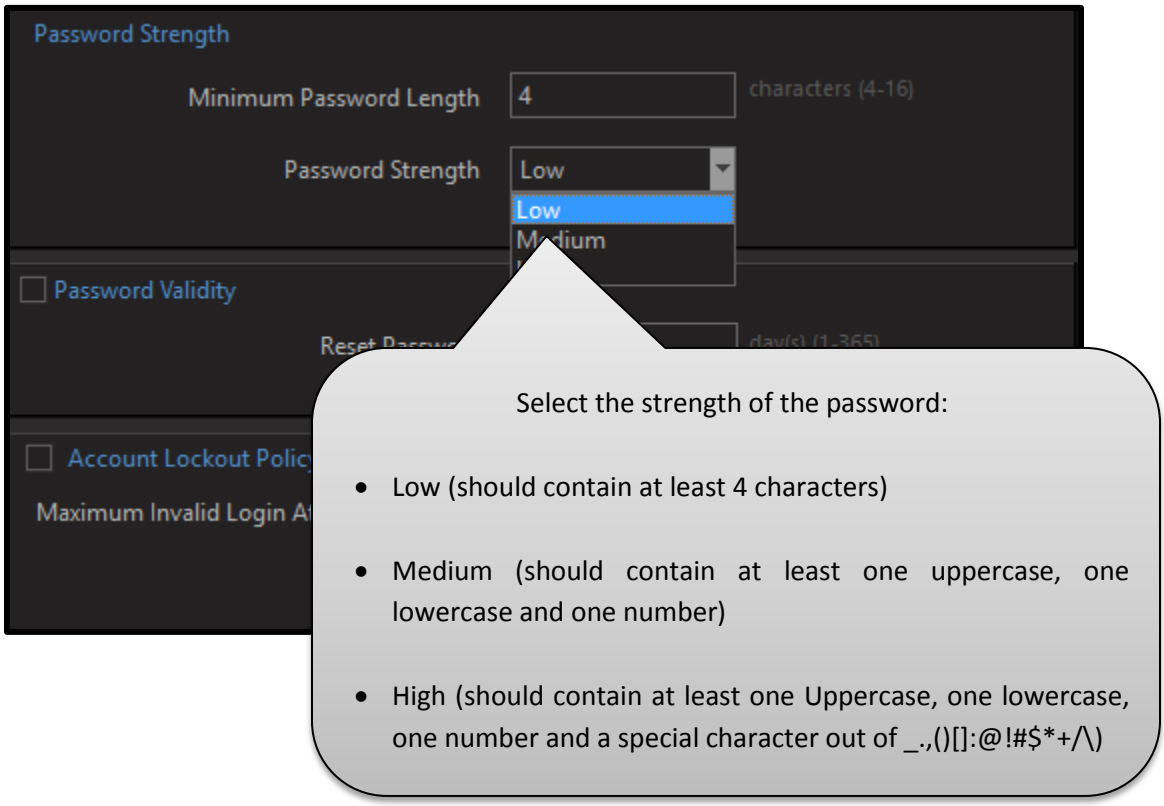


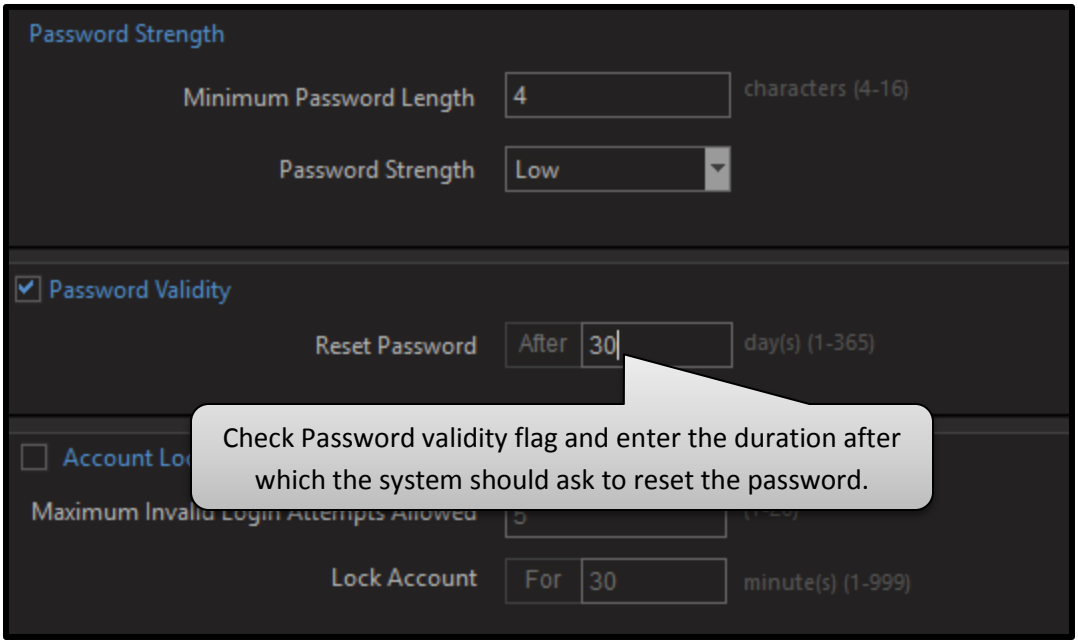
If a user exceeds the number of login attempts allowed, you can lock him for a certain period of time.

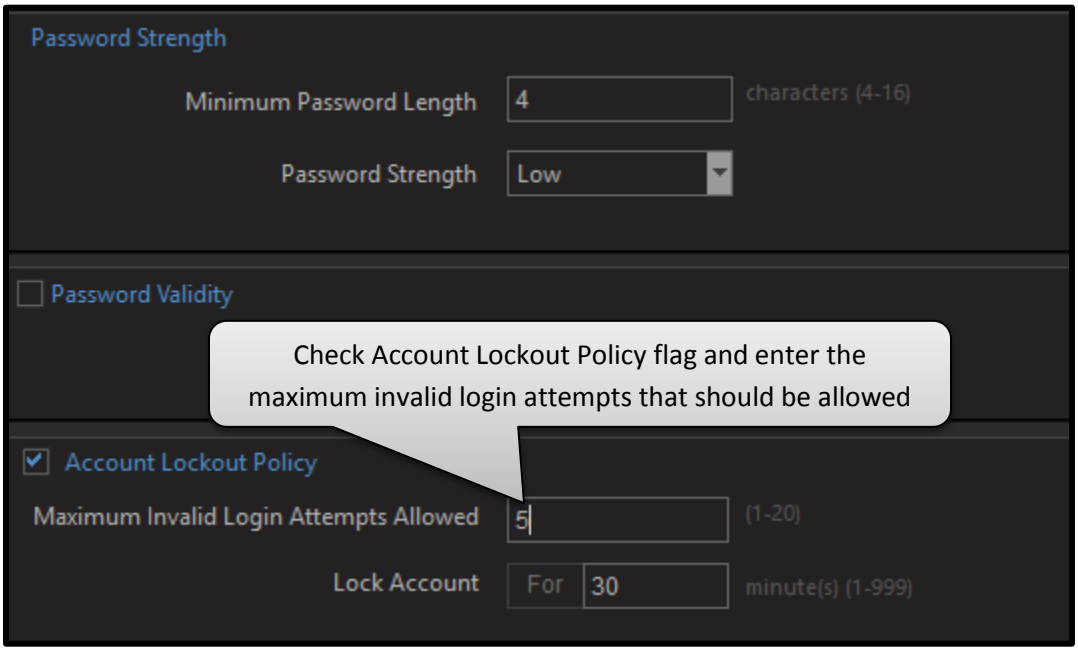

MATRIX
SATATYA
The Persistent Vision
192.168.55.166
Make sure to upgrade the firmware of NVR/HVR to V4R7
Go to Device Configuration
Device Configuration
Matrix-HVR
Camera-1
Camera-2
Camera-3
Camera-4
Camera-5
Camera-6
Camera-7
Camera-8
Camera-9
Camera-10
Camera-11
Camera-12
Camera-13
Camera-14
Camera-15
Camera-16
Camera-17
Camera-18
Camera-19
Camera-20
Camera-21
Camera-22
Camera-23
Camera-24
1
2
3
4
1/125
10 Sec
18-Nov-15 16:16

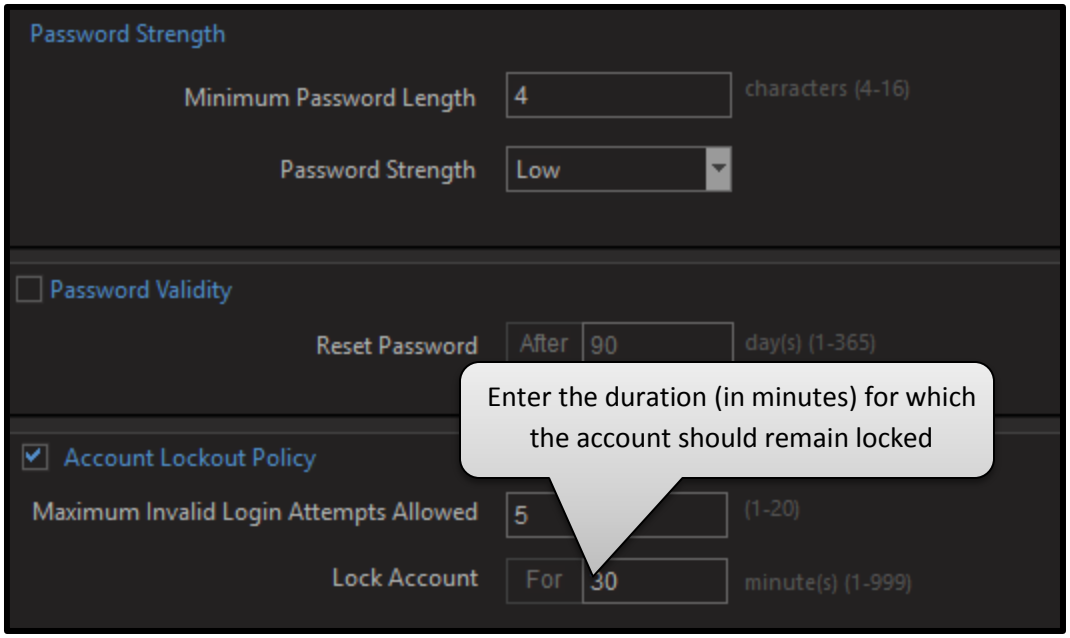

MATRIX
SATATYA
192.168.55.166
Configuration Settings
Device
Matrix-HVR
Password Policy
Basic Settings
Camera Settings
Network Settings
Storage and Backup Settings
Device I/O Settings
User Account Management
User Account
Password Policy
Event and Action Settings
Devices
Go to User Account Management
→ Password Policy
Password Strength
Low
Password Validity
Reset Password
After
1
day(s) (1-365)
Account Lockout Policy
Maximum Invalid Login Attempts Allowed
5
(1-20)
Lock Account
For
30
minute(s) (1-999)
18-Nov-15 16:19

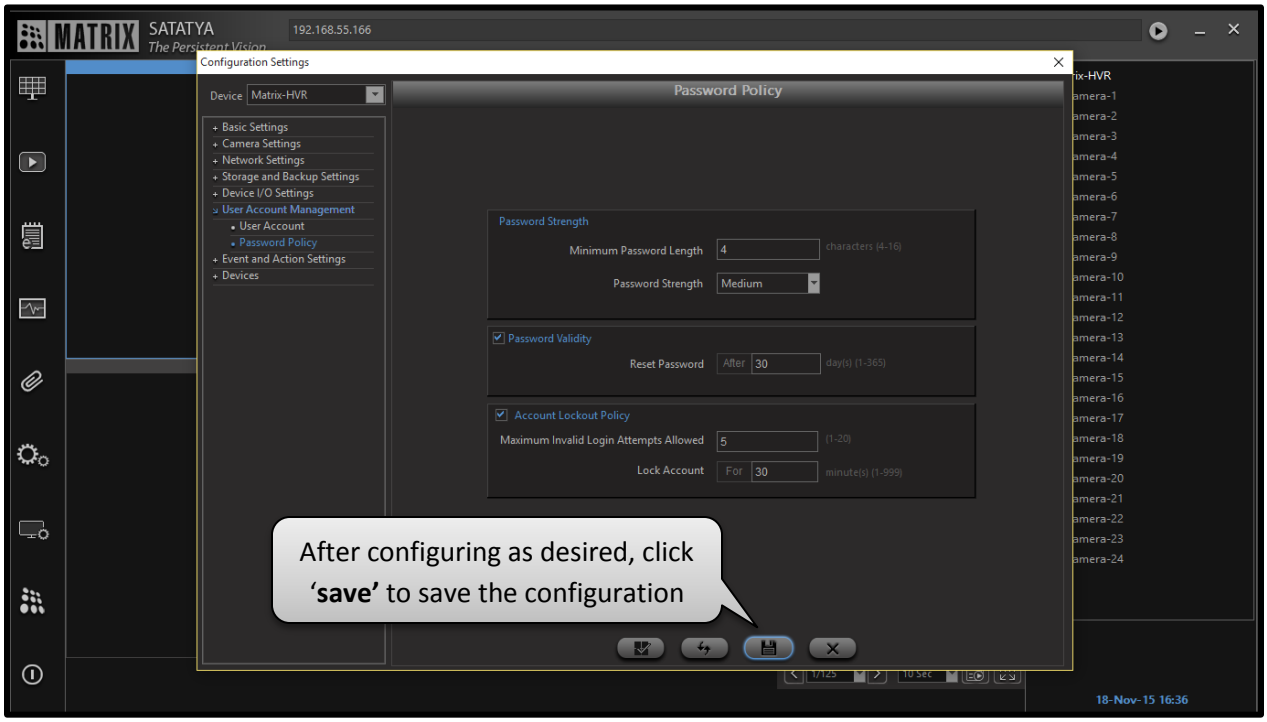

Password Strength
Minimum Password Length
4
characters (4-16)
Password Strength
Password Validity
Reset Passwo
Enter how long the password should be (minimum 4 characters and maximum 16 characters)
Account Lockout Policy
Maximum Invalid Login Attempts Allowed
5
(1-20)
Lock Account
For
30
minute(s) (1-999)


Password Strength
Minimum Password Length
4
characters (4-16)
Password Strength
Low
Low
Password Validity
Account Lockout Polic
Maximum Invalid Login A
Select the strength of the password:
• Low (should contain at least 4 characters)
• Medium (should contain at least one uppercase, one lowercase and one number)
• High (should contain at least one Uppercase, one lowercase, one number and a special character out of _.,()[]:@!#$*+/\)


Password Strength
Minimum Password Length
4
characters (4-16)
Password Strength
Low
Password Validity
Reset Password
After
30
day(s) (1-365)
Check Password validity flag and enter the duration after which the system should ask to reset the password.
Lock Account
For
30
minute(s) (1-999)


Password Strength
Minimum Password Length
4
characters (4-16)
Password Strength
Low
Password Validity
Check Account Lockout Policy flag and enter the maximum invalid login attempts that should be allowed
Account Lockout Policy
Maximum Invalid Login Attempts Allowed
5
(1-20)
Lock Account
For
30
minute(s) (1-999)





Please note the Password Policy is applied to any and every user created in SATATYA Device Client.