FREQUENTLY ASKED QUESTIONS

COSEC

Date: 25th August, 2015

Version: V1R1

Author: Monalisa Sahu

MATRIX

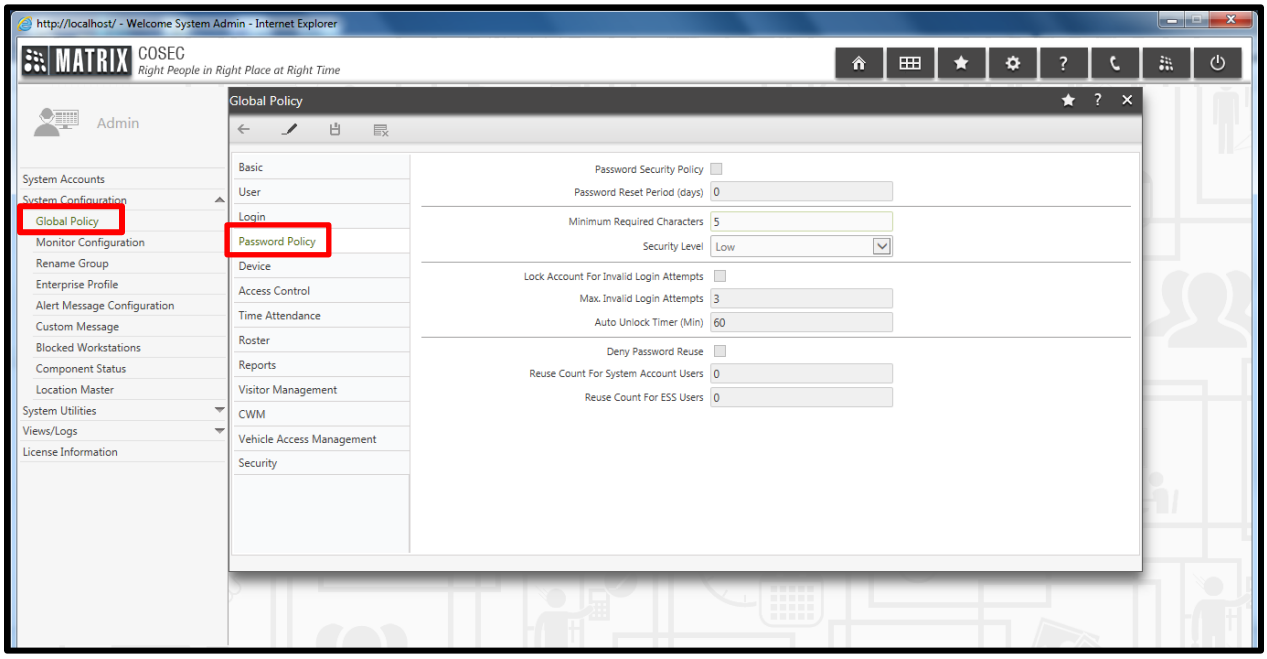
TELECOM | SECURITY

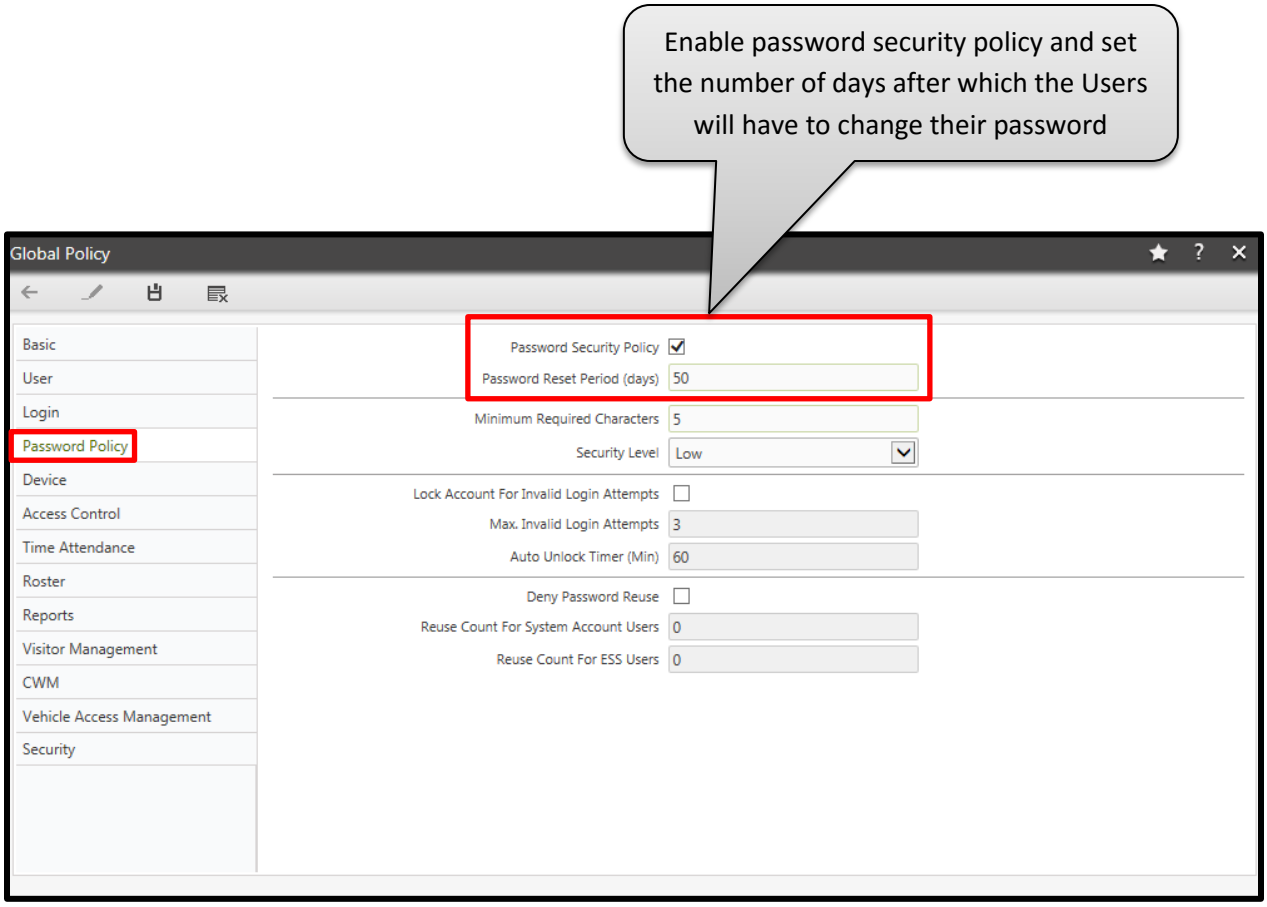
How to configure password Policy?

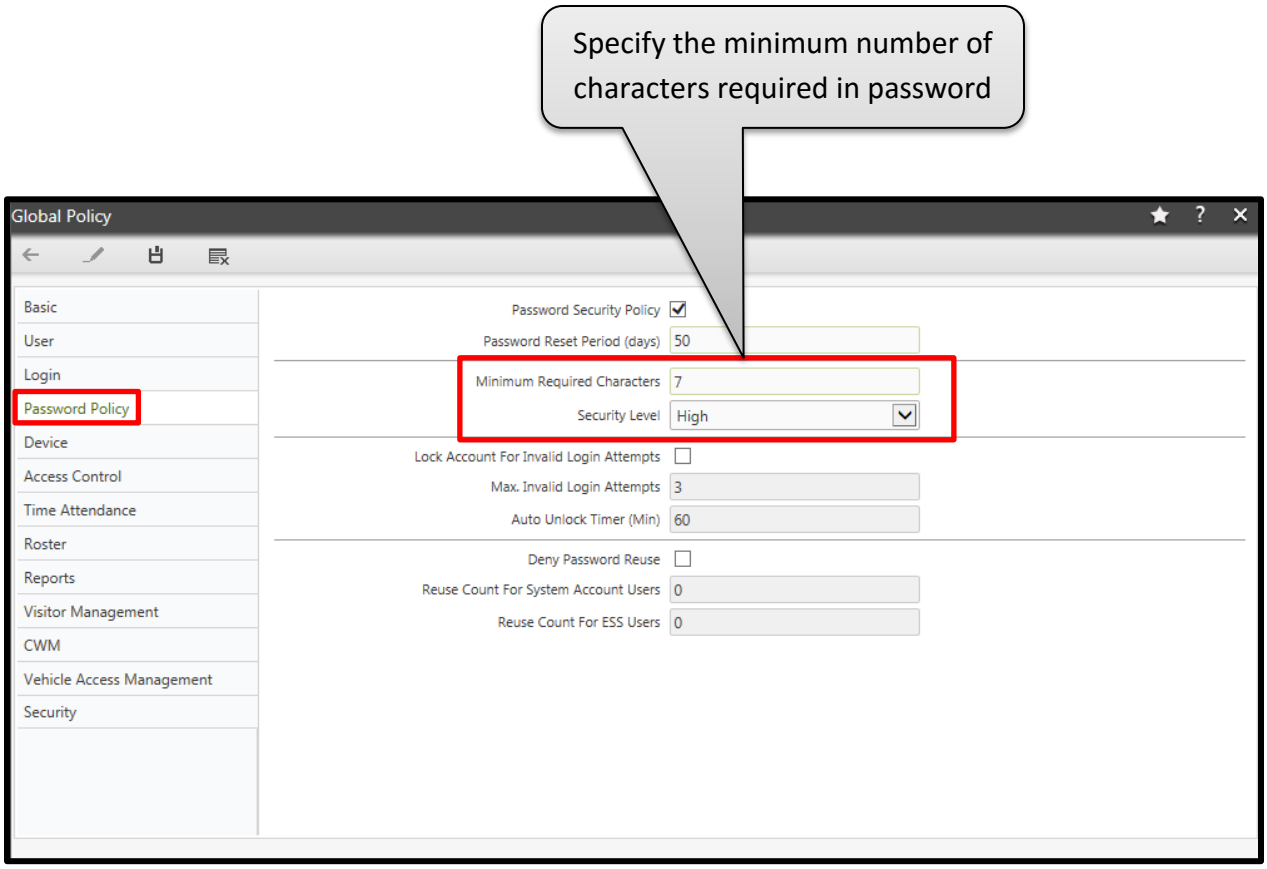

Don’t worry sir. In COSEC we can set password policy which can help us in this. Let me study it completely to implement it


Let me check out password policy so that I can enhance the security of employee's ESS accounts

Password Policy is available from COSEC **V8R1** onwards. It is available in Admin Module → System Configuration → Global Policy → Password Policy.

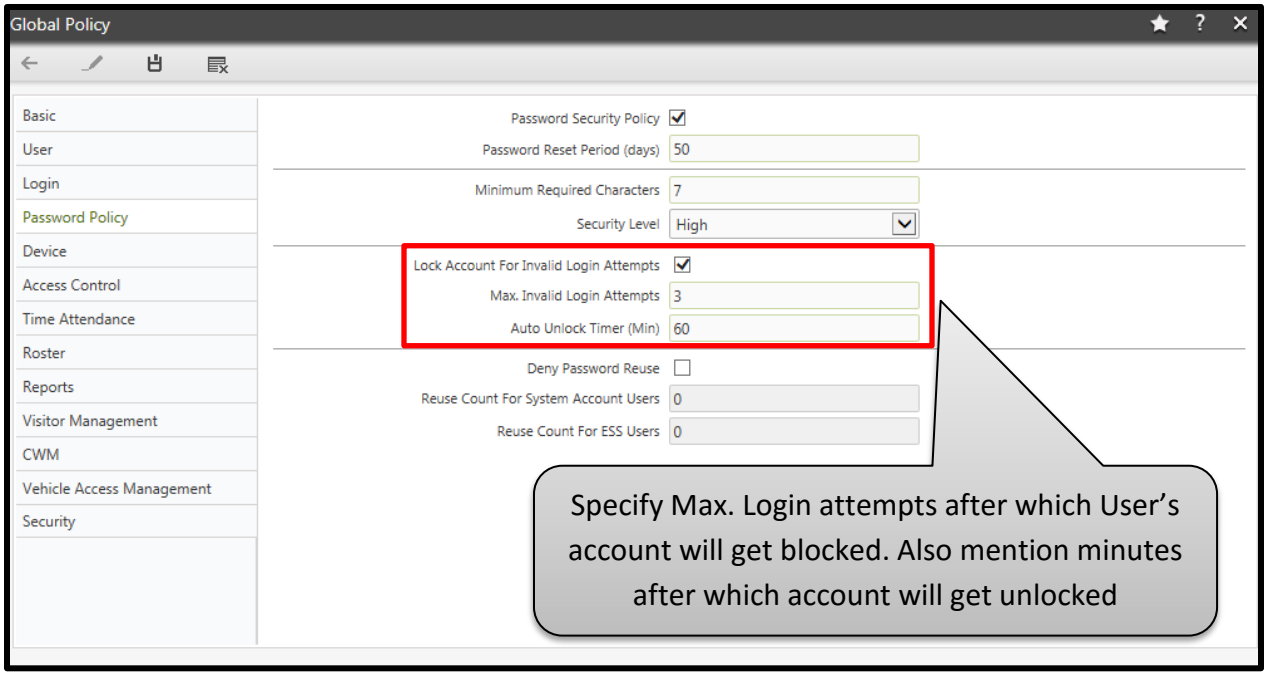


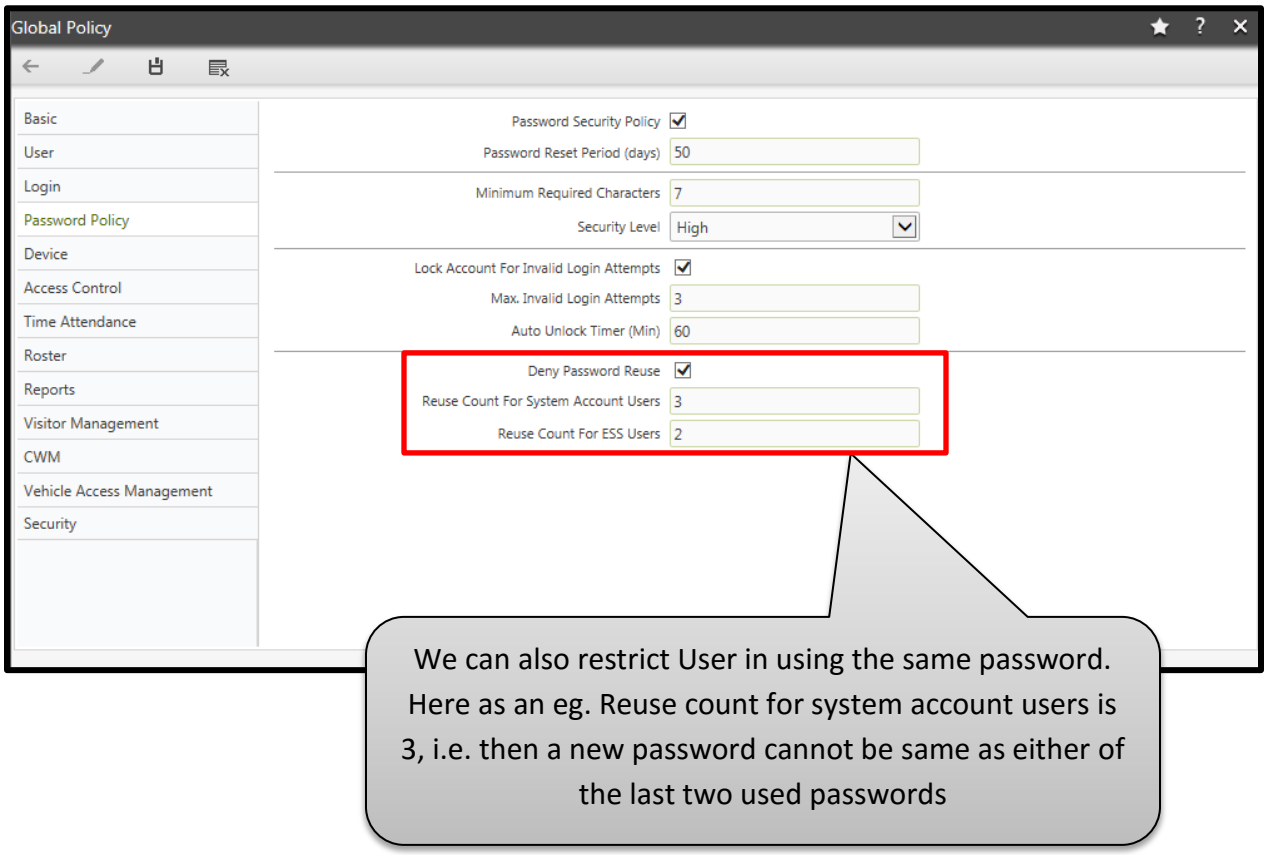

Enable password security policy and set the number of days after which the Users will have to change their password
Global Policy
Basic
User
Login
Password Policy
Device
Access Control
Time Attendance
Roster
Reports
Visitor Management
CWM
Vehicle Access Management
Security
Password Security Policy
Password Reset Period (days)
50
Minimum Required Characters
5
Security Level
Low
Lock Account For Invalid Login Attempts
Max. Invalid Login Attempts
3
Auto Unlock Timer (Min)
60
Deny Password Reuse
Reuse Count For System Account Users
0
Reuse Count For ESS Users
0



Security Levels:

Low	No restriction. All characters allowed in password
Medium	1 lowercase (a-z) character and 1 number (0-9) mandatory in password
High	Here 1 uppercase (A-Z) character, 1 lowercase (a-z) character, 1 number (0-9) and 1 special character (`~!@#$%^&*()- =_+[]\{}|;':",./<>?) mandatory


Global Policy
Basic
User
Login
Password Policy
Device
Access Control
Time Attendance
Roster
Reports
Visitor Management
CWM
Vehicle Access Management
Security
Password Security Policy
Password Reset Period (days) 50
Minimum Required Characters 7
Security Level High
Lock Account For Invalid Login Attempts
Max. Invalid Login Attempts 3
Auto Unlock Timer (Min) 60
Deny Password Reuse
Reuse Count For System Account Users 0
Reuse Count For ESS Users 0
Specify Max. Login attempts after which User's account will get blocked. Also mention minutes after which account will get unlocked


Global Policy
Basic
User
Login
Password Policy
Device
Access Control
Time Attendance
Roster
Reports
Visitor Management
CWM
Vehicle Access Management
Security
Password Security Policy
Password Reset Period (days) 50
Minimum Required Characters 7
Security Level High
Lock Account For Invalid Login Attempts
Max. Invalid Login Attempts 3
Auto Unlock Timer (Min) 60
Deny Password Reuse
Reuse Count For System Account Users 3
Reuse Count For ESS Users 2
We can also restrict User in using the same password. Here as an eg. Reuse count for system account users is 3, i.e. then a new password cannot be same as either of the last two used passwords