

# FREQUENTLY ASKED QUESTIONS

COSEC

What  
When  
Which  
Where  
How  
Who  
Why



**Date:** 25<sup>th</sup> August, 2015

**Version:** V1R1

**Author:** Monalisa Sahu

## How to configure password Policy?

All the employees have started using Matrix Time-Attendance Devices. They are regularly punching on it. Enable their ESS accounts. Their account safety is a big concern to me. I am handing over this responsibility to you



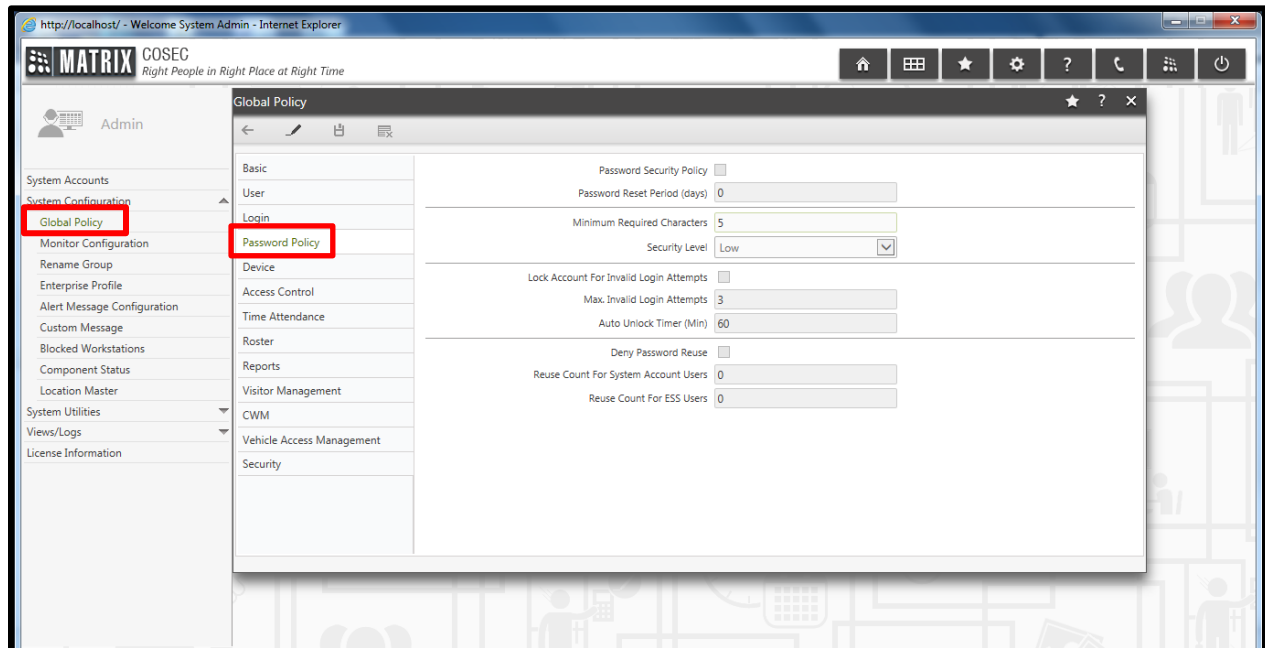
Don't worry sir. In COSEC we can set password policy which can help us in this. Let me study it completely to implement it



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

The screenshot displays the 'Global Policy' configuration window. On the left is a vertical navigation menu with the following items: Basic, User, Login, Password Policy (highlighted with a red box), Device, Access Control, Time Attendance, Roster, Reports, Visitor Management, CWM, Vehicle Access Management, and Security. The main content area shows the configuration for the Password Policy, with a red box highlighting the 'Password Security Policy' checkbox (checked) and the 'Password Reset Period (days)' input field (set to 50). Other visible settings include: Minimum Required Characters (5), Security Level (Low), Lock Account For Invalid Login Attempts (unchecked), Max. Invalid Login Attempts (3), Auto Unlock Timer (Min) (60), Deny Password Reuse (unchecked), Reuse Count For System Account Users (0), and Reuse Count For ESS Users (0).

Basic	Password Security Policy <input checked="" type="checkbox"/>
User	Password Reset Period (days) 50
Login	Minimum Required Characters 5
Password Policy	Security Level Low
Device	Lock Account For Invalid Login Attempts <input type="checkbox"/>
Access Control	Max. Invalid Login Attempts 3
Time Attendance	Auto Unlock Timer (Min) 60
Roster	Deny Password Reuse <input type="checkbox"/>
Reports	Reuse Count For System Account Users 0
Visitor Management	Reuse Count For ESS Users 0
CWM	
Vehicle Access Management	
Security	

Specify the minimum number of characters required in password

The screenshot shows the 'Global Policy' configuration window. On the left is a navigation menu with categories: Basic, User, Login, Password Policy (highlighted in red), Device, Access Control, Time Attendance, Roster, Reports, Visitor Management, CWM, Vehicle Access Management, and Security. The main area displays the 'Password Security Policy' settings. A red box highlights the 'Minimum Required Characters' field, which is set to '7'. Other visible settings include 'Password Security Policy' (checked), 'Password Reset Period (days)' (50), 'Security Level' (High), 'Lock Account For Invalid Login Attempts' (unchecked), 'Max. Invalid Login Attempts' (3), 'Auto Unlock Timer (Min)' (60), 'Deny Password Reuse' (unchecked), 'Reuse Count For System Account Users' (0), and 'Reuse Count For ESS Users' (0).

### Security Levels:

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

The screenshot shows the 'Global Policy' interface with the 'Password Policy' section selected. The 'Lock Account For Invalid Login Attempts' checkbox is checked and highlighted with a red box. A callout box points to this section with the following text:

Specify Max. Login attempts after which User's account will get blocked. Also mention minutes after which account will get unlocked

Setting	Value
Password Security Policy	<input checked="" type="checkbox"/>
Password Reset Period (days)	50
Minimum Required Characters	7
Security Level	High
Lock Account For Invalid Login Attempts	<input checked="" type="checkbox"/>
Max. Invalid Login Attempts	3
Auto Unlock Timer (Min)	60
Deny Password Reuse	<input type="checkbox"/>
Reuse Count For System Account Users	0
Reuse Count For ESS Users	0

The screenshot shows the 'Global Policy' interface with the 'Password Policy' section selected. The 'Deny Password Reuse' checkbox is checked and highlighted with a red box. A callout box points to this section with the following text:

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

Setting	Value
Password Security Policy	<input checked="" type="checkbox"/>
Password Reset Period (days)	50
Minimum Required Characters	7
Security Level	High
Lock Account For Invalid Login Attempts	<input checked="" type="checkbox"/>
Max. Invalid Login Attempts	3
Auto Unlock Timer (Min)	60
Deny Password Reuse	<input checked="" type="checkbox"/>
Reuse Count For System Account Users	3
Reuse Count For ESS Users	2





**Disclaimer:** The information contained in this e-mail and/or attachment may contain confidential or privileged information. Unauthorized use, disclosure or copying is strictly prohibited and may constitute unlawful act and can possibly attract legal action, civil and/or criminal. The contents of this message need not necessarily reflect or endorse the views of Matrix Comsec on any subject matter. Any action taken or omitted on this message is not entirely at your risk and the originator of this message nor does Matrix Comsec take any responsibility or liability towards the same. If you are not the intended recipient, please notify us immediately and permanently delete the message.