

FREQUENTLY ASKED QUESTIONS

SATATYA SAMAS

What
When
Which
Where
How
Who
Why



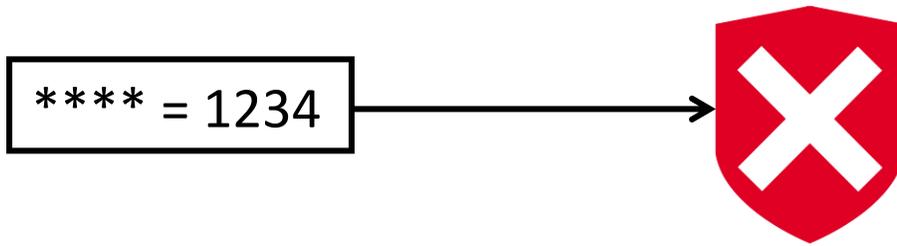
Date: 28th December, 2015

Version: V1R1

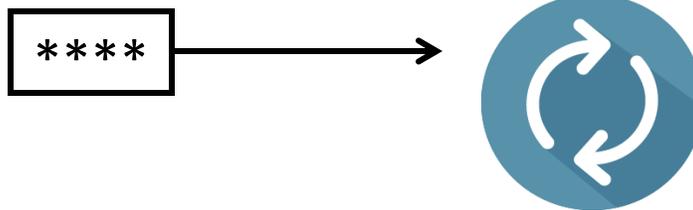
Author: Ashutosh Sharma



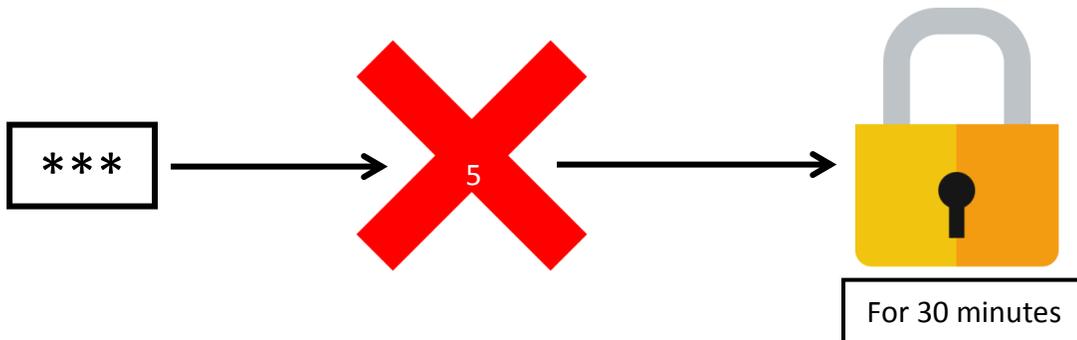
How to Set Password Policy in SATATYA SAMAS?



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

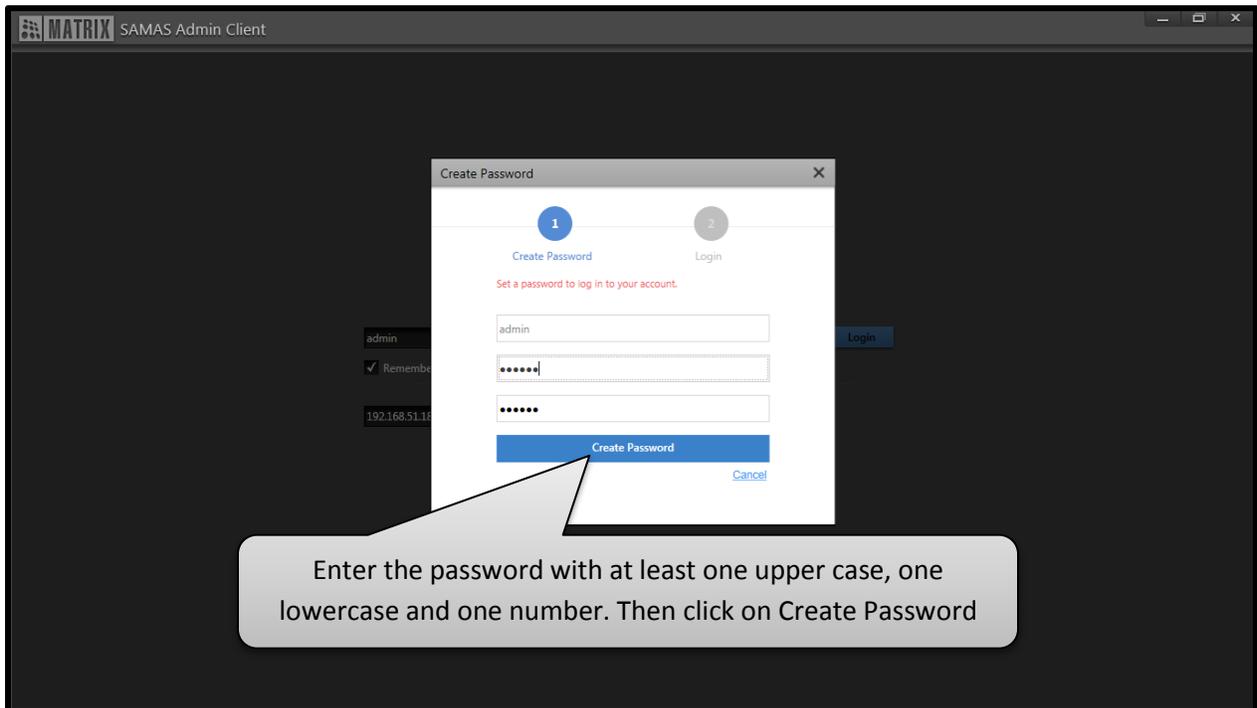
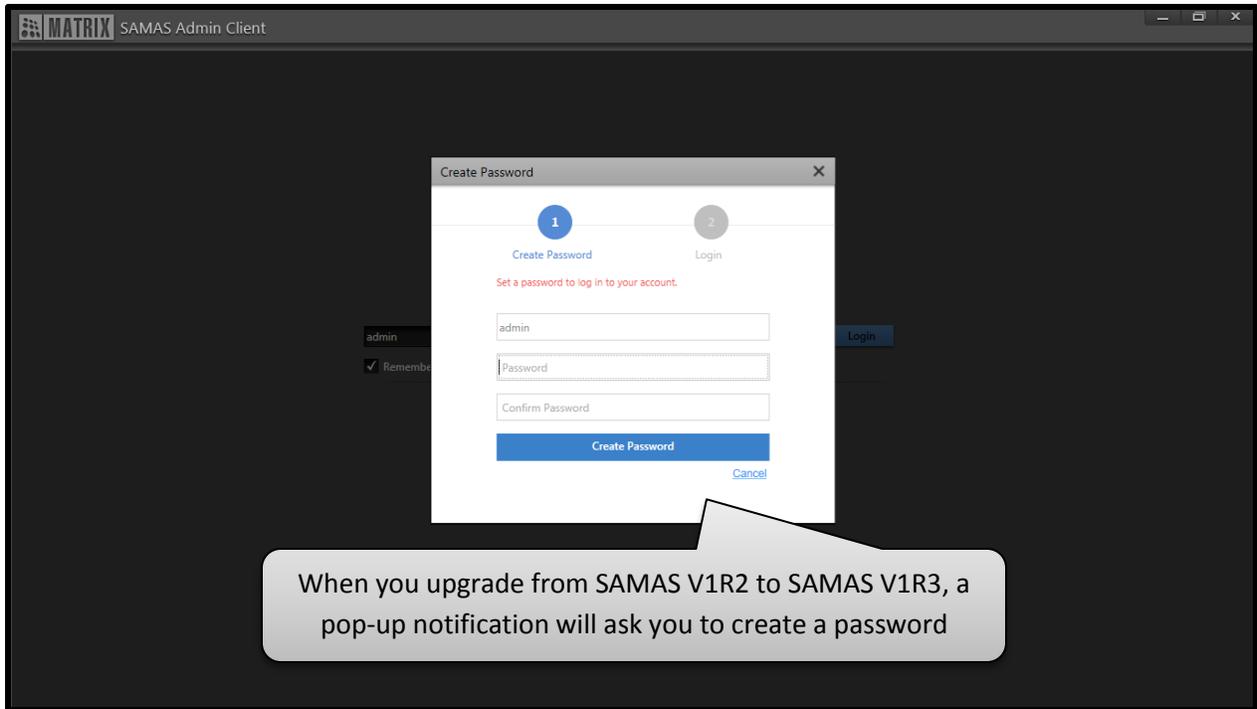


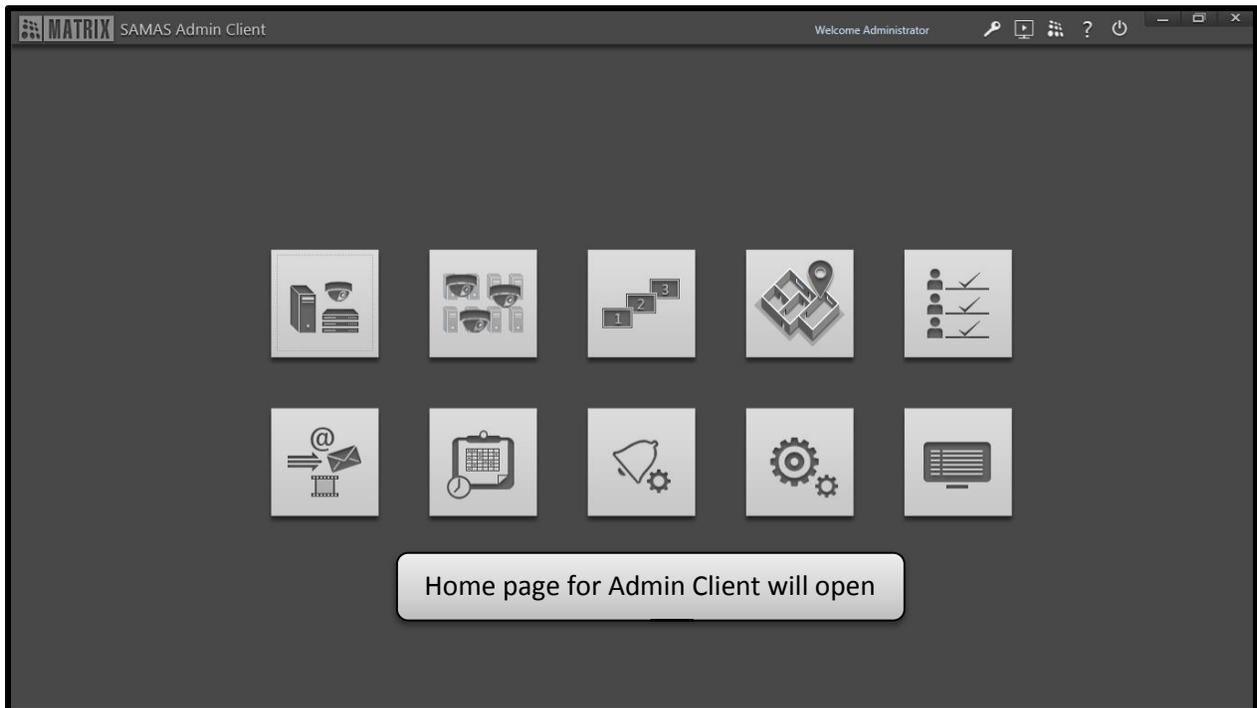
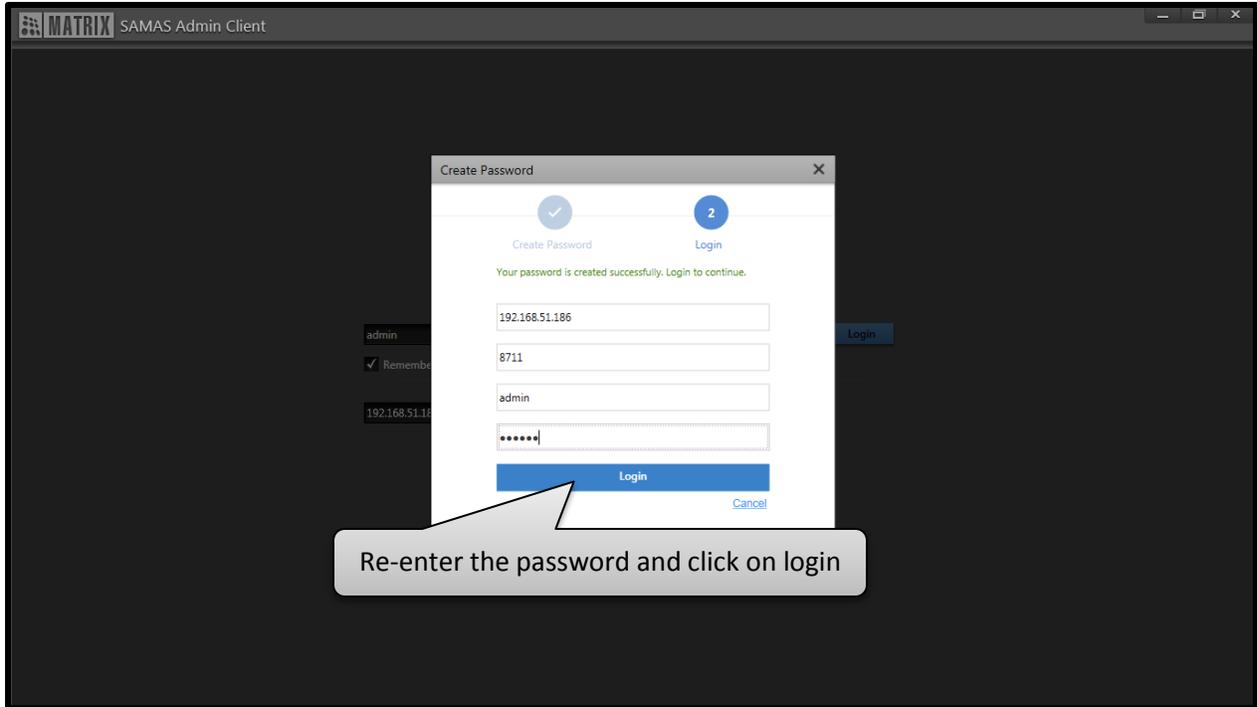
It's a good practice to change password from time to time. You can now set the password reset interval.

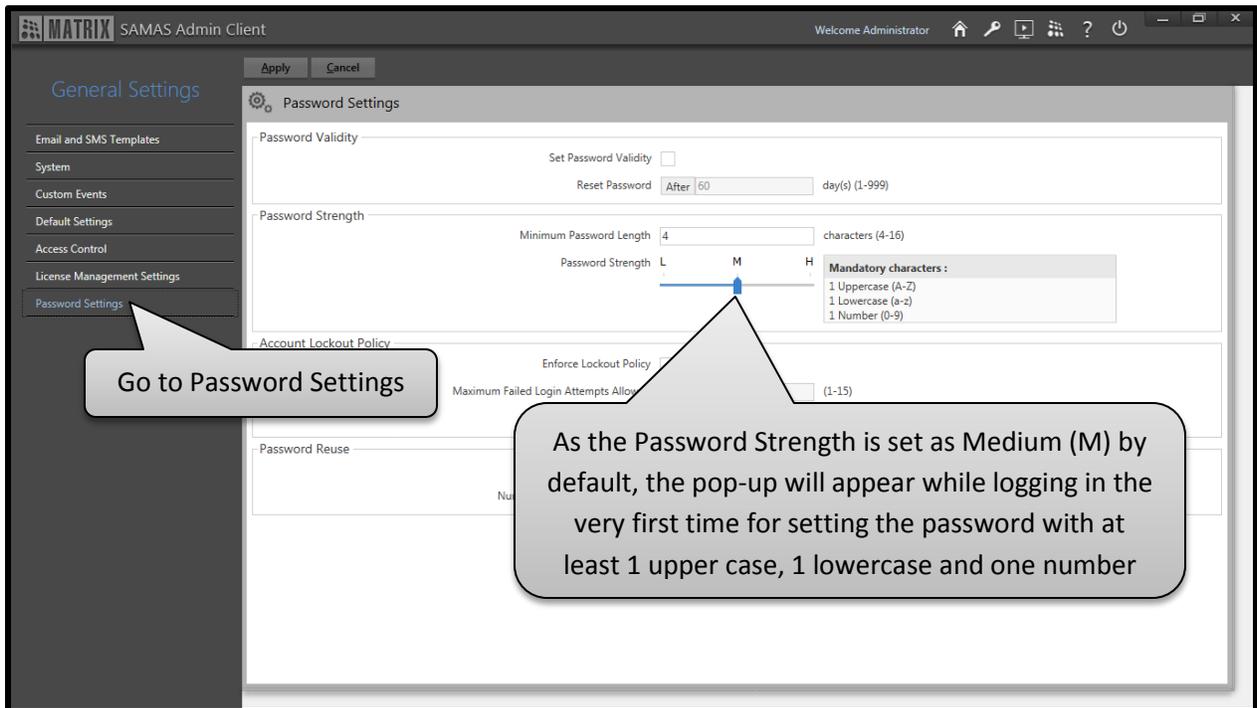
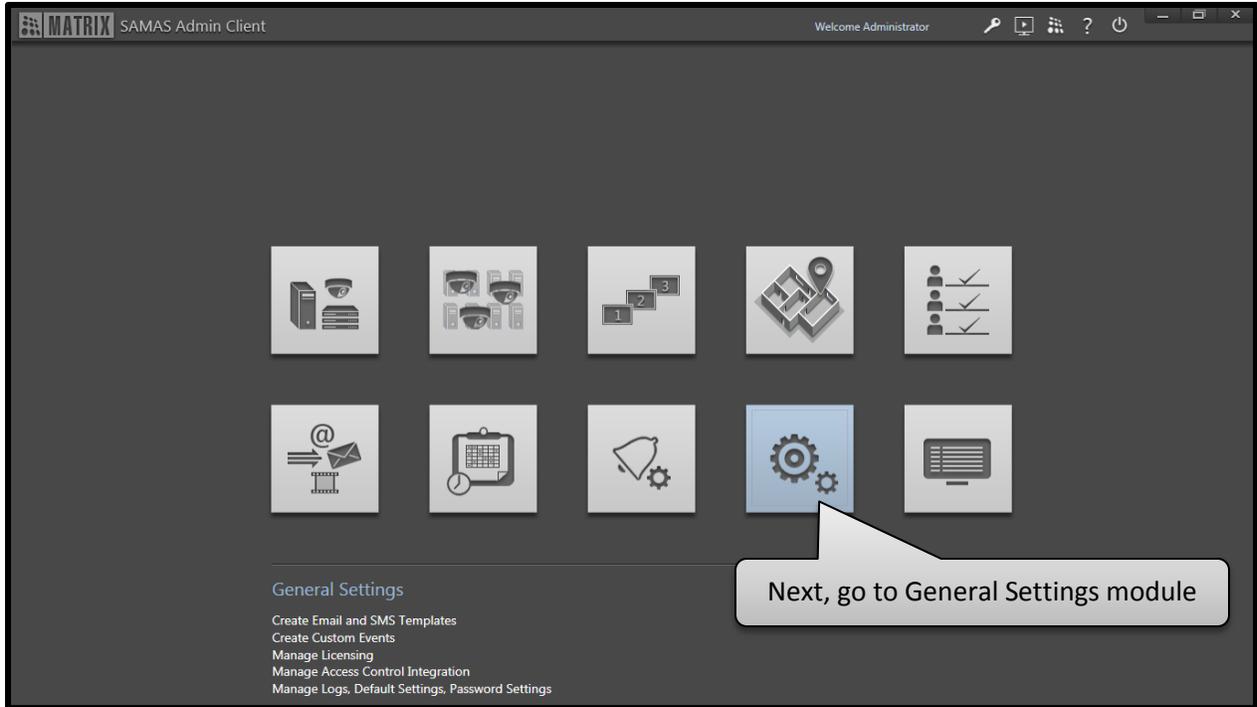


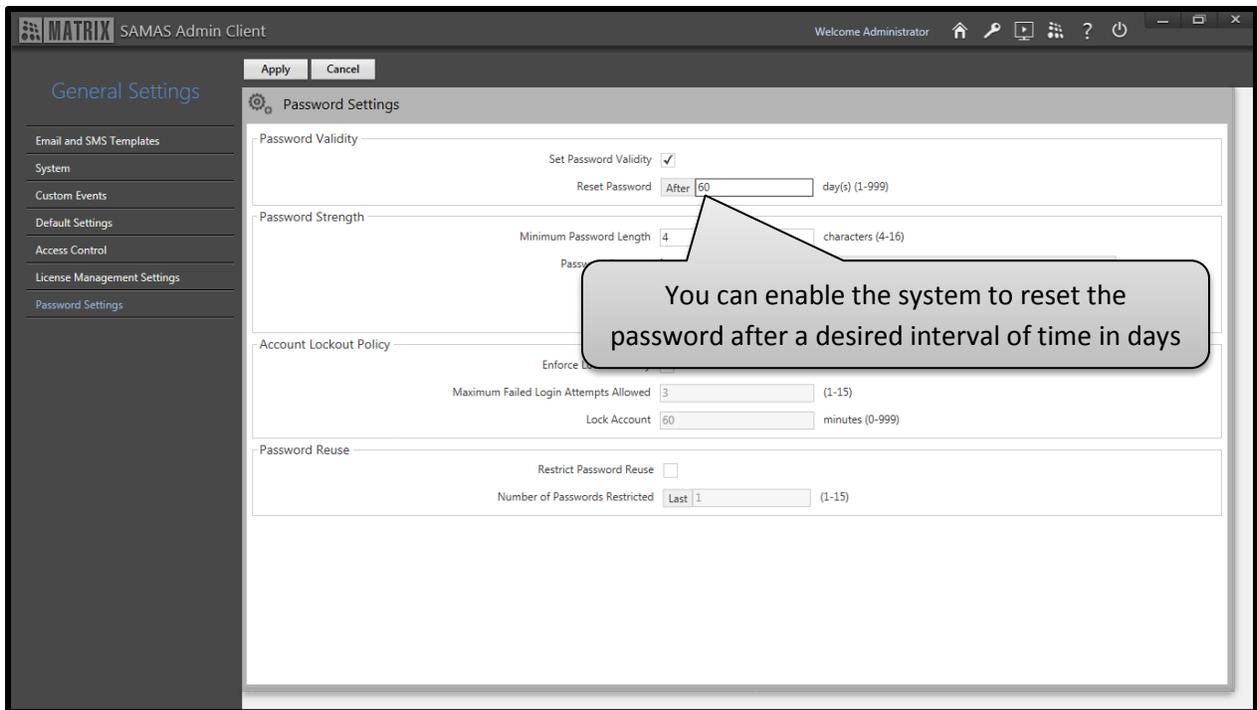
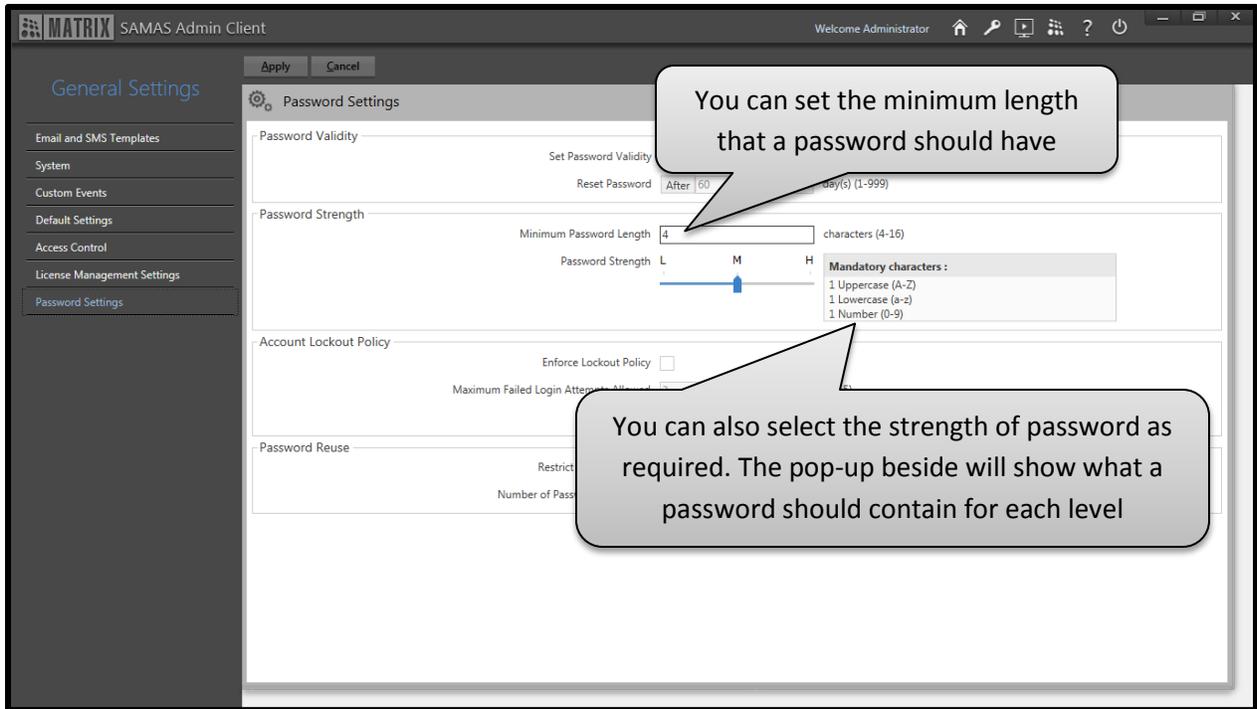
If a user exceeds the number of login attempts allowed with an incorrect password, you can lock him for a certain period of time.

 ... This feature is available from SATATYA SAMAS firmware version V1R3.









You can also impose a Lockout Policy for any account created in SAMAS

MATRIX SAMAS Admin Client

Welcome Administrator

General Settings

Apply Cancel

Password Settings

Set Password Validity

Reset Password After 60 day(s) (1-999)

Minimum Password Length 4 characters (4-16)

Password Strength L M H

Mandatory characters :
1 Uppercase (A-Z)
1 Lowercase (a-z)
1 Number (0-9)

Enforce Lockout Policy

Maximum Failed Login Attempts Allowed 3 (1-15)

Lock Account 60 minutes (0-999)

Restrict Password Reuse

Number of Passwords Restricted L

Enter the Maximum Failed Login Attempts Allowed and Lock Account time in minutes

So, if any user enters an invalid password for 3 times, his account will be locked for 60 minutes

MATRIX SAMAS Admin Client

Welcome Administrator

General Settings

Apply Cancel

Password Settings

Set Password Validity

Reset Password After 60 day(s) (1-999)

Minimum Password Length 4 characters (4-16)

Password Strength L M H

Mandatory characters :
1 Uppercase (A-Z)
1 Lowercase (a-z)
1 Number (0-9)

Enforce Lockout Policy

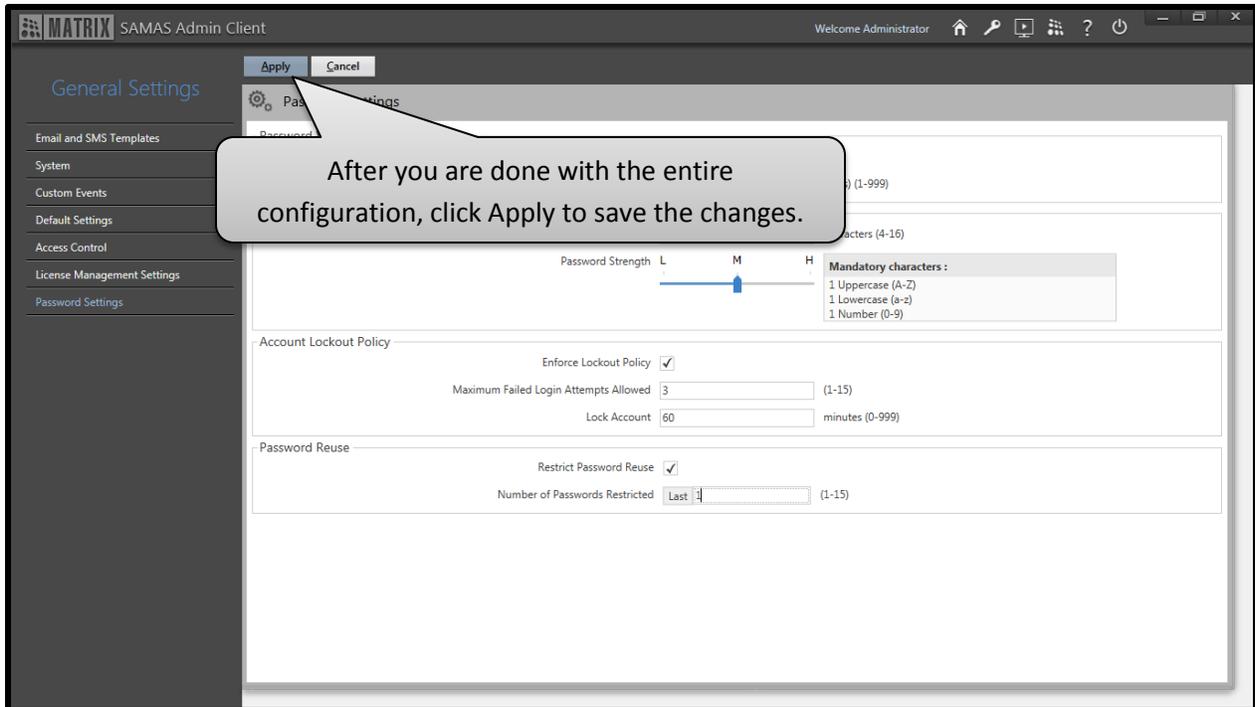
Maximum Failed Login Attempts Allowed 3 (1-15)

Lock Account 60 minutes (0-999)

Restrict Password Reuse

Number of Passwords Restricted Last 1 (1-15)

You can enable Restrict Password Re-use to prevent a user from using an old password again. Enter the number of passwords that should be restricted



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, possibly leading to 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 on or omitted in this message will be at the owner's risk and the originator of this message or Matrix ComSec does not take any responsibility or liability towards the same. If you are not the intended recipient, please notify us immediately and permanently delete the message.