Performance DNA Administrator Guide

Password Settings

5/10/2025

Password Settings

For added security, you can set few parameters for the password. Navigate to `System Settings -> General Settings` tab and go to the **Password Settings** section. The table below explains the Password Settings parameters.

> **Important**
>
> After configuring these settings, Performance DNA or OrgData will check against these password rules whenever a password is created or edited.

Password Setting	Description
Minimum Password Length	This has a minimum value of 7. By default, passwords are set to require `10` characters. Any value entered must be a whole number.
Require an Uppercase, Lowercase, and Numeric character	This setting can be toggled on and off and requires at least one of each uppercase, lowercase, and numeric character. For example: • Valid: **Myvalidpassword1** • Invalid: **myvalidpassword1** and **Myvalidpassword**
Includes a Special Character	This setting can be toggled on and off and enforces the use of at least one special character in the password. These include the following: !"#$%&'()+,-./:;<=>?@[]^_`{|}~* Note that the first character is a space.
Maximum Consecutive Repeated Characters	This limits the number of characters that can be repeated consecutively. It defaults to 3 and must be a whole number. If using the default, the password **aaabcd** would be invalid.
Prevent Repeated Characters Making Up More Than Half of a Password	This setting can be toggled on and off and ensures that a single character does not make up more than half the password. For example, **abacadaeafa** would be invalid because the password is 11 characters long and includes 6 a's
Disallowed Passwords (; separated)	This setting contains a list of disallowed passwords, separated by semicolons. The defaults are as follows: • password - displays as `password` • p455w0rd - displays as `p455w0rd` • p@ssw0rd - displays as `p@ssw0rd`

Password Setting	Description
	Note: You should not enter a password with a ; in the disallowed list; if you do, it will be treated as a separator.
After reset, user must change password on first login	By default, this option is enabled. Users who log in for the first time will be redirected to the Change Password screen. If a user logs in and does not provide a new password (for example the user cancels or closes the browser), the user can log back in and attempt to change the password again. There is no limit to the number of times a user can cancel.
Lockout Users After X Failed Attempts	The number of failed login attempts that triggers a locked account. For example, if the value is set to 6 and the user has failed to log in 5 times, on the 6th failed attempt, the account is automatically locked for the duration of time specified in the **Lockout Time Duration (Mins)** option (below). After a successful login, the failed login attempts counter is set back to 0. For example, if a user fails to log in 5 times but then successfully logs in on the 6th attempt, the failed login attempts counter returns to 0 and the user successfully logs in.
Lockout Time Duration (Mins)	The duration, in minutes, that an account is locked after the user has exceeded the number of login attempts specified in the **Lockout Users After X Failed Attempts** field. If a user tries to log in during this time period, a message appears onscreen, indicating that the account is locked.
Password Expiry Duration (Days)	The period of time (in days) that a password can be used before the system requires the user to change it.
User Cannot use the Same Password for X Number of Days	The period of time (in days) before an old password can be used again. If a user attempts to re-use an old password before the time specified in this field has lapsed, the user will be prompted to choose a different password.