PASSWORD SECURITY ADMINISTRATION GUIDE

Descartes Component Framework (DCF)

June 2016

The Descartes Systems Group Inc. | TSX: DSG | NASDAQ: DSGX | 120 Randall Drive, Waterloo, Ontario, N2V 1C6, Canada
Toll Free 800.419.8495 | Int'l 519.746.8110 | info@descartes.com | www.descartes.com

Information in this document is subject to change without notice. Descartes makes no warranties, express or implied, in respect of this document or its contents.

DCF

The Descartes Systems Group Inc.

120 Randall Drive

Waterloo, Ontario Canada, N2V 1C6

Phone: 519-746-8110

Internet: http://www.descartes.com

Customer Support

In North America: 1-877-786-9339

Outside North America: +800 -7866-3390

e-mail: servicedesk@descartes.com

Table of Contents

Introduction

There are six new features designed to make user passwords in LNOS systems more secure:

- Allow blank passwords
- Minimum length for passwords
- Multiple character types required in passwords
- Force password change every X days
- New password may not match the user's last X passwords
- User locked out after X failed login attempts

Setting Up Enhanced Password Security

Each of the above six options may be setup by an administrator by selecting the **Profile Items** option of the **Setup** menu in the DCF user interface. There you will see a list that includes these items in the category 'Password Management'. The value for each item may be set either at the 'Default' level (applies to everything in a database) or at the 'Org' level (only applies to users in that Org).

Allow Blank Passwords

If this option is set to 'True', the user will receive an error message if he or she attempts to change their password to a blank value.

Minimum Length for Passwords

Set this option to the minimum number of characters that will be allowed for new passwords. If the user enters a new password with less than the specified number of characters, the system will return an error message.

Multiple Character Types Required in Passwords

This option should be set to a value in the range 1 – 4. It specifies the number of different types of characters which a user must include in a new password. The character types are:

- Lowercase letters (a – z)
- Uppercase letters (A – Z)
- Numerals (0 – 9)
- Special Characters (`~!@#$%^&*()_-+={}[]|\:;"',.<>?/)

Setting this option to a value greater than 4 will cause all new passwords to be rejected.

Force Password Change Every X Days

Set this option to the number of days a password is valid before a user must choose a new password. If a user logs in and it is determined that his or her password has not been changed in the last X days then he or she will be presented with the

Change Password page instead of the normal home page. Upon entering a new password, the user will be transferred to his or her normal home page. If this option is set to zero, then it will not be applied.

New Password Must Not Match the User's Last X Passwords

If this option is set to a positive number, then the last X passwords the user has used will be maintained and if the user attempts to reuse one of them when entering a new password, he or she will receive and error message. Prior passwords are not retained until this option is turned on, so its affect will not be immediately evident.

User Locked Out after X Failed Login Attempts

If this option is set to a positive number and the user fails to correctly specify his or her password on X consecutive login attempts (not necessarily from the same place), the user's account will be locked out. This functionality only applies to logins via the user interface. It does not apply to logins thru Dataflow, Workflow, a web service or any other non-UI methods.

Resetting a Locked Out User

A User Administrator can unlock a user's account by navigating to the list of active users, right clicking on a user and selecting **Reset Lockout**. This list also contains an additional column indicating if a user is Locked Out.