Enhanced eHR Security—March 31, 2017

new world ERP – Foundation

Empowering people who serve the public®   tyler technologies

Contents

Enhanced eHR Security—March 31, 2017
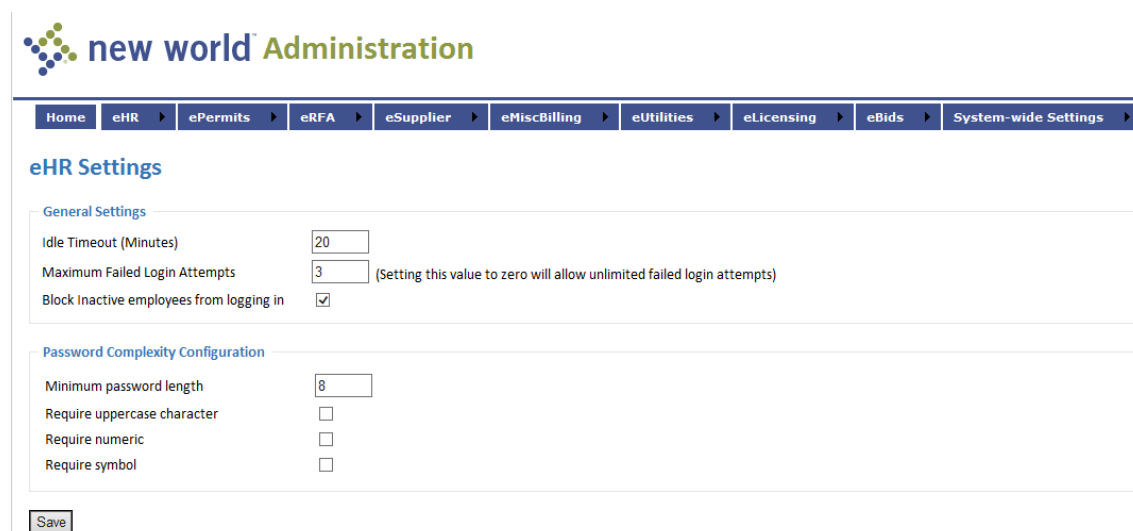
new world ERP – Foundation

INTRODUCTION

This document details the enhancements that are included in the March 31, 2017, patch for eHR Security. The pages affected are eHR Settings, Employee Account Management and Edit Administrator Account.

eHR SETTINGS

eAdministration > eHR > eHR Maintenance > eHR Settings

The eHR Settings page has been enhanced with an expanded **General Settings** section and a **Password Complexity Configuration** section:

GENERAL SETTINGS ADDITIONS

Maximum failed login attempts: Sets the number of times a user may enter incorrect login credentials before being locked out. A value of **0** will allow an unlimited number of failed login attempts. The valid range of entries for this field is **0** to **10**. The default is **3**.

Block inactive employees from logging in: If selected, prohibits employees with an inactive status from logging into the eHR system.

PASSWORD COMPLEXITY CONFIGURATION

Use this section to set the password complexity requirements for eHR users and administrators.

Minimum password length: Must be between 5 and 25 characters. The default entry is **8**.

Require uppercase character: Select if password must contain at least one uppercase letter. Default is checked.

Require numeric: Select if password must contain at least one numeric digit. Default is checked.

Require symbol: Select if password must contain at least one symbol (#, *, %, etc.). Default is checked.
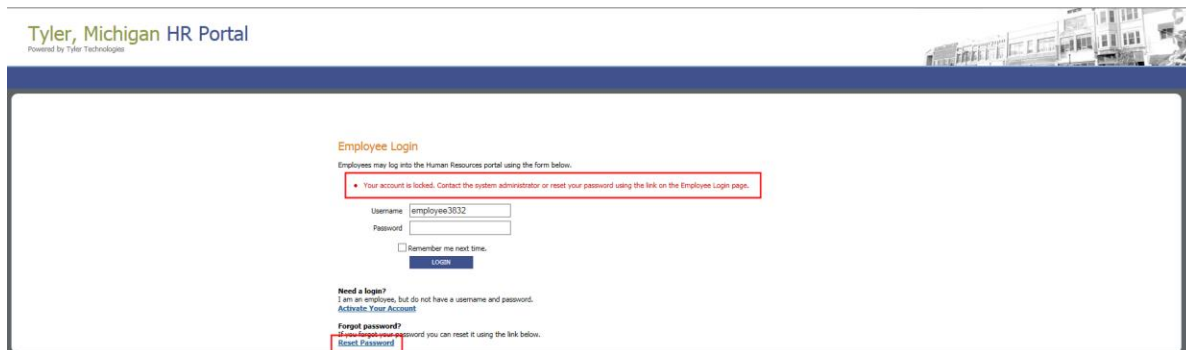
Password complexity requirements are enforced on the following pages:

- Employee Account Management (*eAdministration > eHR > eEmployee > Employee Account Maintenance*)
- Activate Your Account (link from Employee Login page)
- Maintain My Account (link from eHR Welcome page)
- Employee Login
- Password Expired
- Password Reset

Note: These requirements apply to creating and updating passwords, not to logging in with an existing password that may not adhere to the current requirements.

PASSWORD RESET PROCESS

A user whose failed login attempts reach the maximum number of failed attempts identified in eHR Settings will be presented with a locked-out message in red on the Employee Login page:

Clicking the *Reset Password* link will open the Password Reset page, where the user will be asked to type a *Username* and click **CONTINUE**:

Empowering people who serve the public®

A user with a primary email address identified in new world ERP will receive an email at that address with a link to a Password Reset page that will ask for the last four digits of the user's SSN and a new password:
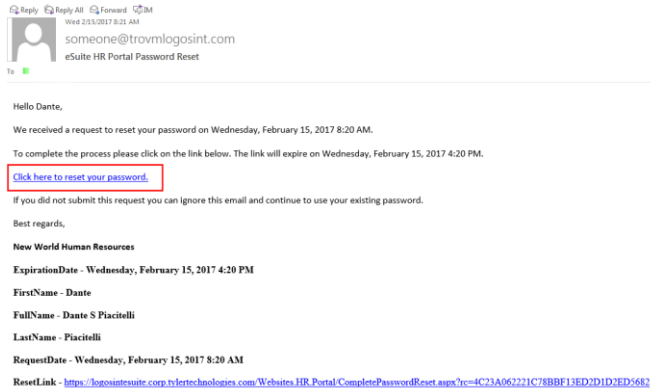
The new password must adhere to the complexity settings in eHR Settings and must be different from the user's current password. After clicking **CONTINUE**, the user will be taken to the Employee Login page:

3

Note: The email link will be valid for eight hours before the user will need to return to the Employee Login page to restart the process of resetting the password.

The content of a "Password Reset" email may be set up in new world ERP at *Maintenance > new world ERP Suite > System > Email Templates*.

EMPLOYEE AND ADMINISTRATOR ACCOUNT MANAGEMENT

UNLOCKING A LOCKED-OUT USER

eAdministration > eHR > eEmployee > Employee Account Maintenance

A *Locked* check box has been added to the Employee Account Management page:

This box will be checked for a user who is locked out of the system after having reached the *Maximum failed login attempts* identified in eHR Settings. If necessary, an administrator may deselect this box and click **Save** to unlock the user. This check box is enabled only when a user is locked out.

A *Locked* check box also has been added to the Edit Administrator Account page (*eAdministration > System-wide Settings > Administrator Accounts > User Name*):

This box will be checked for an administrator who has exceeded the number of allowable invalid logins; a locked-out administrator, however, will not have a password reset option but will need to contact another eSuite administrator.