FireLight Design Document

Disconnected Console Security Enhancements

Published: 5/7/2015

Insurance Technologies, LLC
Two South Cascade Avenue
Colorado Springs, CO 80903
USA
Phone: 719.442.6400
FAX: 719.442.0600

Internet E-Mail: info@insurancetechnologies.com
Website: http://www.insurancetechnologies.com

Table of Contents

Console Security Enhancements

Introduction

The existing security features in the FireLight Console can be improved to increase effectiveness. There are also features that can be added to improve security. This document will cover the features to be changed or added.

1. Add more control over password content
2. Limit the number of Active devices a user can have
3. Limit the number of times a password can be changed

Password Content

The current Console authentication uses a numeric PIN to access the device data. It would be significantly more secure to allow alpha numeric characters and symbols when authenticating. In order to allow the additional characters a few more administrative values will be needed. Along with the new values it makes sense to rename some of the existing authentication parameters.

New Value	Old Value	Other Info
Min Password Length	PIN Length	
Min Numbers in Password	N/A	Default DB value: Null, which evaluates to Min Password Length for backwards compatibility
Min Symbols in Password	N/A	Default DB value: Null, which evaluates to 0 for backwards compatibility
Password Expires in	PIN Duration	Days until new password required
Idle Timeout	(same)	No Change
Max Login Attempts	Max Invalid PIN Attempts	
Max Login Attempts window	Authentication Window	
Wipe On Failed Login	(same)	No Change

User Experience

Backwards compatibility will be supported by defaulting the new values above to support the previous PIN style password.

Existing passwords and expirations will be respected. The new password requirements will be enforced when a new password is created. Passwords are created when a device is activated, a password expires, manual password change and a reset password from the App or Admin portal.

When logging into the FireLight Console the numeric keypad will not be displayed. Instead the user will use a standard keyboard to enter the password. Also, any reference to ‘PIN’ in the Console, App portal and Admin portal will be changed to ‘password’ (See figure 1)

User Name/ID in Authentication

FireLight will add an administrative setting to allow an organization to require a username along with the password when logging into the FireLight Console. The new Username setting will consist of 3 options: None, External ID and Custom.

UserName Setting	Notes
None	(Default) Only the password will be required.
External ID	The username must match the External ID provided in the SSO NameIdentifier assertion.
Custom	The user provides a username during the activation process.

To support backwards compatibility the username setting will default to 'None'. As with the password content changes, existing username options will be honored until the password is changed. The new username requirements will be enforced when a new password is created. Passwords are created when a device is activated, a password expires, manual password change and a reset password from the App or Admin portal.

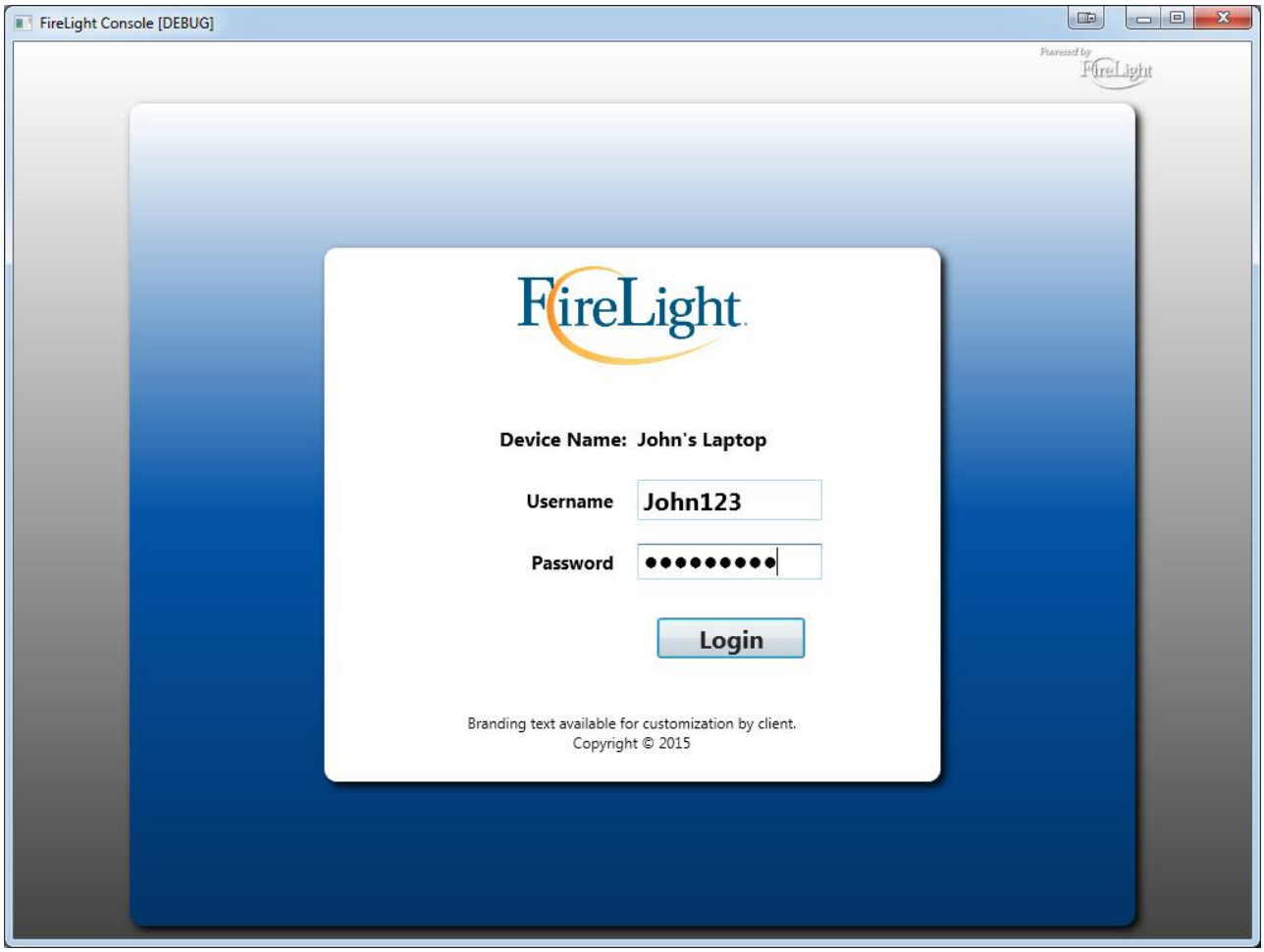

Figure 1

Login Branding

Since the Console knows what client is being accessed when the Login view is displayed it can load client branding and display custom colors, images and text. A new branding text item will be defined to display footer text at the bottom of the login panel. (See Figure 1)

Active Devices

Currently a user can create as many Device profiles as they like. An organization can limit the applications checked out by setting the "Max Checkout out Apps" in the Admin tool. However, the “Max Checked out Apps” value is validated per device, which means a user can create multiple device profiles, and each device doubles the number of allowable checked out applications.

FireLight plans on changing the existing setting name to "Max Checked-Out Apps per Device". And adding a new setting called "Max Devices". Existing validation in the Console does not change. And in the App Portal Preferences page the "Max Devices" setting will be used to determine if a new device can be added.

Password Change Limits

Currently the Console enforces that a PIN cannot match the previous 3 PIN's. However, nothing is preventing a user from circumventing a required password change by changing their password 4 times to return to their original password. The goal is to avoid this scenario.

The FireLight Console will prevent the re-use of any passwords created in the past (3 x Password Expiration) days. This means if the Console is configured to expire a password in 60 days, passwords created in the last 180 days cannot be used.

Revision History

Revision History		
Date	**Name**	**Revision Summary**
5/7/2015	Jayson Bjurstrom	Created