DV3401 – System Configuration

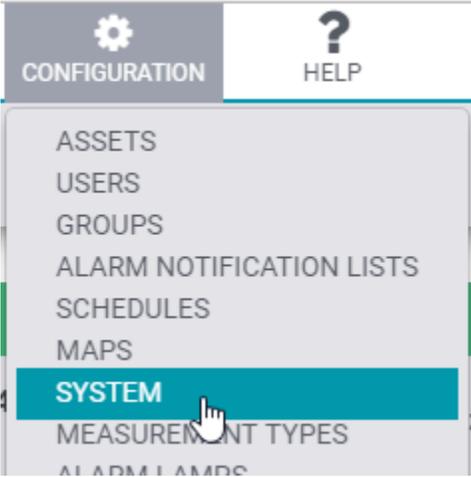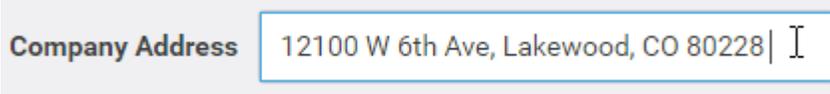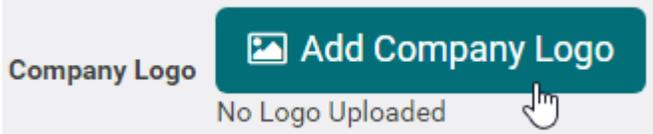|	
Software Version	ViewPoint v1.1.1
Scope	Demonstrate System Configuration options available in the ViewPoint software.
Purpose	Establishing system configurations that hold to organizational needs and communication methods for the software.
Applicable User Groups	Administrator
Requirements	User must be logged in to the ViewPoint software with Administrator privileges.

Process

Step 1	From the ViewPoint home screen, navigate to the **CONFIGURATION** menu and select **SYSTEM**	

Results: This will bring up the System Configuration page. The System Configuration has three sections that are outlined below.

Display Section

Company Name	
Click into the field and type company name.	
Company Address	
Click into the field and type company address.	
Company Logo	
Click the ▢ Add Company Logo button and select an image to upload.	
Results: This is where information is pulled to display on reports.	
Display 4-digit Asset ID	
Results: This is inactive by default. If active, a 4-digit Asset ID will be displayed on the Asset tiles on the home page. This option was implemented for backward compatibility with previous Mesa Systems, and will likely not be active for new installs.	

Security Section

Compliance	
Enable 21 CFR Part 11 Compliance	

Results: This feature requires password verification to make changes in the system. All changes will be noted with the user information in the change log to track which users made what changes

Access

Maximum Login Attempts	Maximum Login Attempts 5

Results: Set per organization standards. This number dictates the acceptable limit for failed login attempts. The next setting outlines how too many attempts is handled.

After too many failed authentication attempts	After too many failed authentication attempts ○ Disable the user (requires an admin to reset) ◉ Lockout the user for 15 minutes

Results: Set per organization standards. In the event a user has too many failed login attempts, either lock a user account for 15 minutes or disable the account until an Admin can reset the account.

Password Expiration Period	○ Never Password Expiration Period ◉ Expires in 180 ▾ days

Results: Set per organization standards. Set to have user passwords expire after either 30, 60, 90, 120, 150, or 180 days.

System will logout after	System will logout after 120 minutes of inactivity

Results: Set per organization standards. Set to have users automatically logged out after the selected number of minutes.

New System PIN and Confirm System PIN	New System PIN 1234 Confirm System PIN 1234

Results: Set a New System PIN and then confirm the new PIN to set.

Communications Section

Notifications	
Security Notification List	
Results: Set the Security Notification Group that will receive email notifications of too many failed login attempts by a user. The list should contain only email addresses, so it is advised to set up a Security Notifications Group specifically for this purpose.	
System Notification List	
Results: Set the System Notification Group that will receive email notifications when a Network Device loses contact or an attempted outbound phone call encounters an error. The list should contain only email addresses, so it is advised to set up a System Notifications Group specifically for this purpose.	
Email	
SMTP Server Information	
Results: Enter organization SMTP server information to send out email notifications. Requires: **SMTP Server, SMTP Port, SMTP Login, SMTP Password**, and **SMTP From**.	

Voice
Voice Alarms
Results: Select **VOIP (text-to-speech)** when Twilio is not activated. Otherwise, to use Twilio select **Cloud-based Call Notification**.

Notes and Comments

None

Related Documents

Document No.	Title	Scope