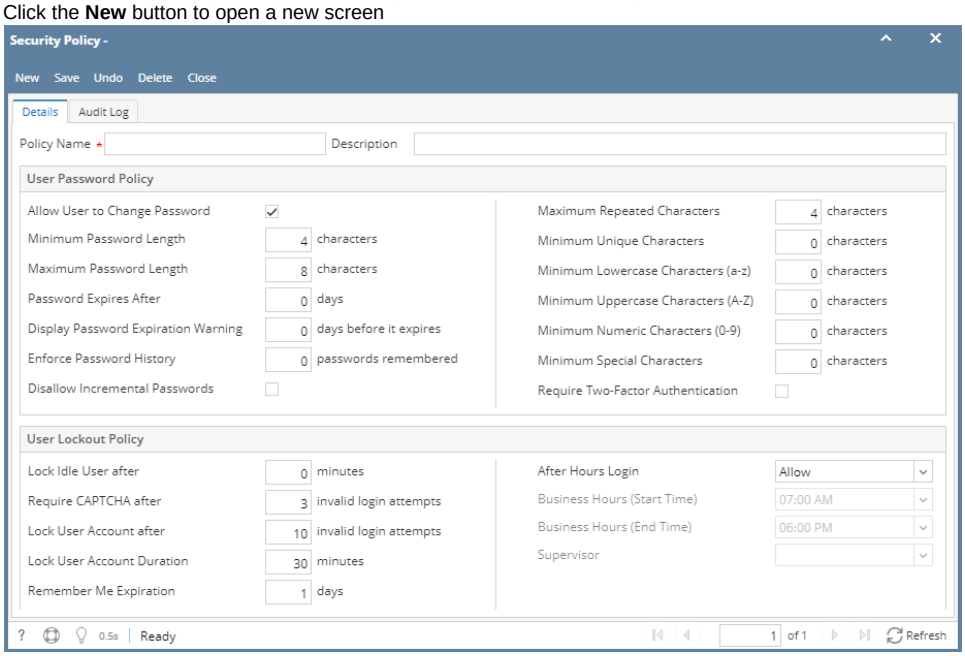
How to Add a Security Policy

1. Log in as **Admin user**
2. On user's menu panel, go to **System Manager** folder then click **Security Policies**
3. Click the **New** button to open a new screen



4. Add a Policy Name and Description
5. Modify the fields that need to be configured. *See field descriptions below*
6. Click the Save button once done.

User Password Policy

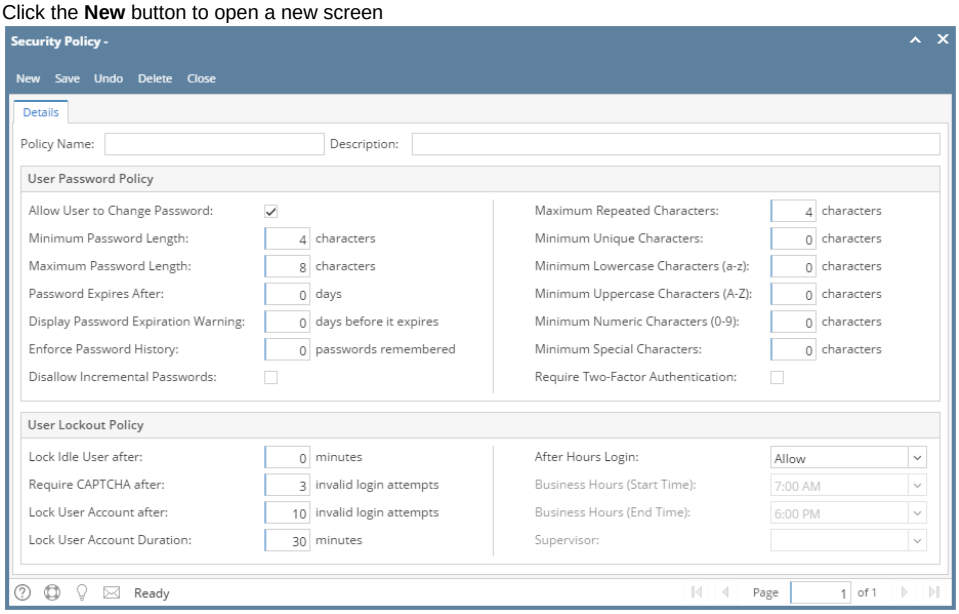
Policy Name	Description
Allow User to Change Password	If this is enabled then the user can change their password. If it's disabled then prevent the user from changing their password
Minimum Password Length	The passwords minimum length
Maximum Password Length	The passwords maximum length
Password Expires After	The password will expire after the set number of days (0 disables this feature)
Display Password Expiration Warning	Display a warning message every time the user logs in xx number of days before the password is set to expire (0 disables this feature) Text for this message: "Your password is going to expire in x days. You will need to change your password on or before the day it expires"
Enforce Password History	This will keep track of the last xx number of passwords the user has created and makesure they cannot reuse the same password in that list. (0 disables this feature)
Disallow Incremental Passwords	Prevent the user from incrementing their password by 1 number or letter. This will only track the last character of the password. Ex: If the password is **My$StrongPassword1** then it should not allow **My$StrongPassword2**
Maximum Repeated Characters	Prevents the number of characters from being repeated more than the number specified and should be case sensitive. If the value for this is 2 then it should never allow any character or number to be used more than 2 times in the password. (0 disables this feature) Ex: This would be an invalid password: **ThisPassword**
Minimum Unique Characters	Verifies that xx number of characters are unique in the password. If this was set to 4 then a password must have at least 4 different characters, numbers of symbols in it. (0 disables this feature)

Minimum Lowercase Characters (a-z)	The password is required to have at least xx number of Lowercase characters. (0 disables this feature)
Minimum Uppercase Characters (A-Z)	The password is required to have at least xx number of Uppercase characters. (0 disables this feature)
Minimum Numeric Characters (0-9)	The password is required to have at least xx number of Numeric characters. (0 disables this feature)
Minimum Special Characters	The password is required to have at least xx number of Special characters. (0 disables this feature)
Require Two-Factor Authentication	Requires the User to Enable Two-Factor Authentication. When the user logs in, it should check to see if 2FA is enabled and if not force the user to enable it. Once enabled the user should not be allowed to disable it unless this option is set to False.

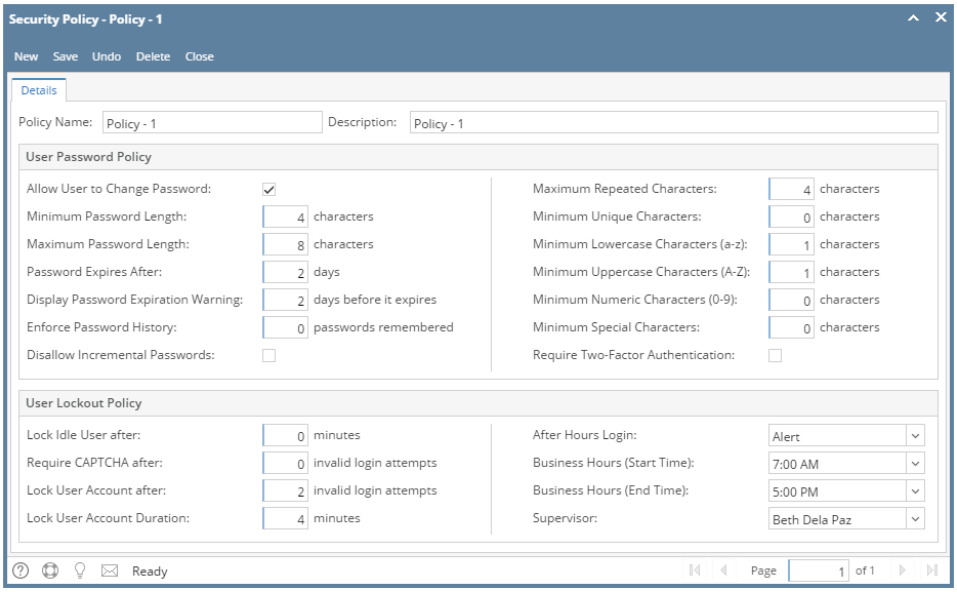
User Lockout Policy

Policy Name	Description
Lock Idle User after	Lock the screen if the user is idle for more than xx number of minutes. (0 disables this feature)
Require CAPTCHA after	Display a CAPTCHA if the user enters the wrong password more than xx number of times. (0 disables this feature)
Lock User Account after	Lock the User from logging in if the user enters the wrong password more than xx number of times. (0 disables this feature)
Lock User Account Duration	If the User Account is locked then keep it locked for xx number of minutes. (0 disables this feature)
Remember Me Expiration days	If the user checked Remember Me on login screen, after the xx number of days set on the policy, the user will be required to login again
After Hours Login	Combo Box with the following options: 1. Allow - Allows the user to login at any time. 2. Prevent - Prevents a user from logging in outside of the defined Business Hours (for example, a secretary would not be allowed in after hours). If a user is already logged in and the time reaches the Business Hours (End Time), display a warning message that their screen will be locked in 5 minutes. This gives the user an extra 5 minutes to finish up what they are working on. If they don't log out within the 5 minutes, then Lock their screen and prevent them from logging in again until after the Business Hours (Start Time). 3. Alert - Sends an email to the supervisor if the user logs in outside of the defined Business Hours
Business Hours (Start Time)	Sets the Start of the Business Hours. Disabled when "After Hour Login" is set to Allow and enabled for any other option. The drop down should display the visual Time selector only (no calendar)
Business Hours (End Time)	Sets the End of the Business Hours. Disabled when "After Hour Login" is set to Allow and enabled for any other option. The drop down should display the visual Time selector only (no calendar)
Supervisor	Combo Box that displays a list of users. The selected user (supervisor) would receive an email when the "After Hours Login" is set to Alert any time the user tries to login outside the defined business hours. Disabled when "After Hour Login" is set to Allow or Prevent. Here is how the email should be formatted. Email Subject: i21 Security Policy Alert - After Hours Login Body: Username logged in at 10:45 PM (EST) from IP address 74.208.161.217. This alert was triggered because it's outside the business hours of 7:00 AM and 6:00 PM.

1. Log in as **Admin user**
2. On user's menu panel, go to **System Manager** folder then click **Security Policies**
3. Click the **New** button to open a new screen



4. Add a Policy Name and Description
5. Modify the fields that need to be configured



User Password Policy

Policy Name	Description
Allow User to Change Password	If this is enabled then the user can change their password. If it's disabled then prevent the user from changing their password
Minimum Password Length	The passwords minimum length
Maximum Password Length	The passwords maximum length
Password Expires After	The password will expire after the set number of days (0 disables this feature)
Display Password Expiration Warning	Display a warning message every time the user logs in xx number of days before the password is set to expire (0 disables this feature) Text for this message: "Your password is going to expire in x days. You will need to change your password on or before the day it expires"

Enforce Password History	This will keep track of the last xx number of passwords the user has created and makesure they cannot reuse the same password in that list. (0 disables this feature)
Disallow Incremental Passwords	Prevent the user from incrementing their password by 1 number or letter. This will only track the last character of the password. Ex: If the password is **My$StrongPassword1** then it should not allow **My$StrongPassword2**
Maximum Repeated Characters	Prevents the number of characters from being repeated more than the number specified and should be case sensitive. If the value for this is 2 then it should never allow any character or number to be used more than 2 times in the password. (0 disables this feature) Ex: This would be an invalid password: **ThisPassword**
Minimum Unique Characters	Verifies that xx number of characters are unique in the password. If this was set to 4 then a password must have at least 4 different characters, numbers of symbols in it. (0 disables this feature)
Minimum Lowercase Characters (a-z)	The password is required to have at least xx number of Lowercase characters. (0 disables this feature)
Minimum Uppercase Characters (A-Z)	The password is required to have at least xx number of Uppercase characters. (0 disables this feature)
Minimum Numeric Characters (0-9)	The password is required to have at least xx number of Numeric characters. (0 disables this feature)
Minimum Special Characters	The password is required to have at least xx number of Special characters. (0 disables this feature)
Require Two-Factor Authentication	Requires the User to Enable Two-Factor Authentication. When the user logs in, it should check to see if 2FA is enabled and if not force the user to enable it. Once enabled the user should not be allowed to disable it unless this option is set to False.

User Lockout Policy

Policy Name	Description
Lock Idle User after	Lock the screen if the user is idle for more than xx number of minutes. (0 disables this feature)
Require CAPTCHA after	Display a CAPTCHA if the user enters the wrong password more than xx number of times. (0 disables this feature)
Lock User Account after	Lock the User from logging in if the user enters the wrong password more than xx number of times. (0 disables this feature)
Lock User Account Duration	If the User Account is locked then keep it locked for xx number of minutes. (0 disables this feature)
After Hours Login	Combo Box with the following options: 1. Allow - Allows the user to login at any time. 2. Prevent - Prevents a user from logging in outside of the defined Business Hours (for example, a secretary would not be allowed in after hours). If a user is already logged in and the time reaches the Business Hours (End Time), display a warning message that their screen will be locked in 5 minutes. This gives the user an extra 5 minutes to finish up what they are working on. If they don't log out within the 5 minutes, then Lock their screen and prevent them from logging in again until after the Business Hours (Start Time). 3. Alert - Sends an email to the supervisor if the user logs in outside of the defined Business Hours
Business Hours (Start Time)	Sets the Start of the Business Hours. Disabled when "After Hour Login" is set to Allow and enabled for any other option. The drop down should display the visual Time selector only (no calendar)

Business Hours (End Time)	Sets the End of the Business Hours. Disabled when "After Hour Login" is set to Allow and enabled for any other option. The drop down should display the visual Time selector only (no calendar)
Supervisor	Combo Box that displays a list of users. The selected user (supervisor) would receive an email when the "After Hours Login" is set to Alert any time the user tries to login outside the defined business hours. Disabled when "After Hour Login" is set to Allow or Prevent. Here is how the email should be formatted. Email Subject: i21 Security Policy Alert - After Hours Login Body: Username logged in at 10:45 PM (EST) from IP address 74.208.161.217. This alert was triggered because it's outside the business hours of 7:00 AM and 6:00 PM.