MULTIFACTOR AUTHENTICATION WITH INSYNC 170.315(D)(13)

877.246.8484 | info@insynchcs.com | www.insynchcs.com

Table of Contents

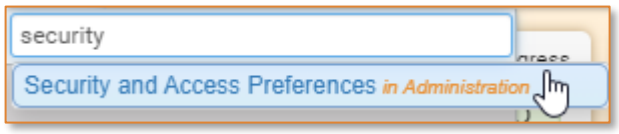
.

OVERVIEW

You can configure a setting to authenticate users when logging on to the InSync software. The authentication can be configured based on various Multifactor Authentication (MFA) Methods such as Email, SMS, and Mobile Authenticator. The OTP (One-Time Password) can be sent to one or all these methods.

ACCESS MULTIFACTOR AUTHENTICATION

In top left smart search box, type **security** and select the **Security and Access Preferences in Administration** option.



On the **Security and Access Preferences** screen, locate the following panels:

- ✓ Access Settings
- ✓ Multifactor Authentication

ACCESS SETTINGS

You can allow or restrict users to access InSync software for the desired date and time or IP address. The users for which the rule is not defined, you can allow or restrict their access using a flag in Customized Preferences.

Configure Access By: Access can be configured one of 3 ways. You can select the single or multiple users, select the users based on their role or resource type. Choose the desired option accordingly from the "User / User Group, Role, Resource Type" switch.

Access Type: There can be 2 types of access. You can set a rule to either allow or restrict access. Choose the desired checkbox accordingly from "Allow" and "Restrict".

Applicable Days: Select the days to allow or restrict access. You can click on the "Applicable Days" link to select or clear the days at once.

IP Address: Select one or more IP addresses to allow or restrict users' access/restrict the system using these IPs.

Date Range: Access can be allowed or restricted either always or during specific date range. Choose the desired option from "Always" or "Custom". When selecting the "Custom" option, you can specify a date range for how long you want to allow or restrict access.

Time Range: Select the time range to allow or restrict the users accessing the system during this time frame. You can select multiple time slots if so desired.

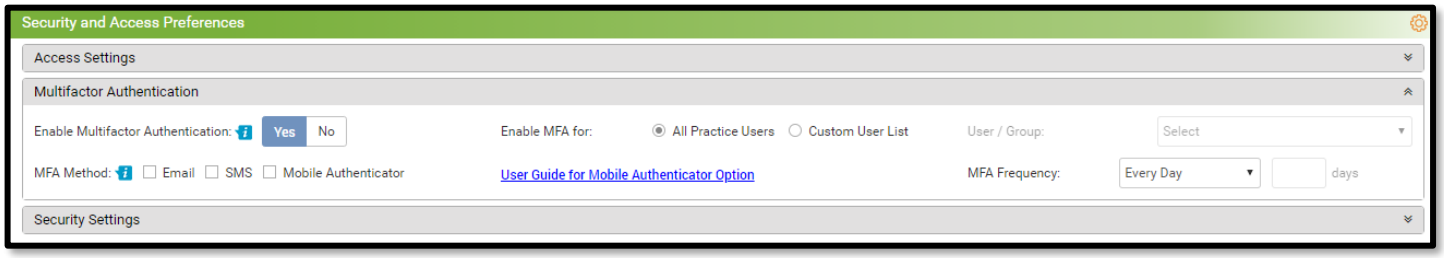
Send To Do on Access Attempt: Select this checkbox to send To Do to the desired users when any action is performed outside the configured rule.

Allow Emergency Access: When the users are restricted to access InSync, you can still allow them to log on with the reason. You can also allow emergency access from all the IPs or from the specific IPs.

- ✓ **No**: Select this checkbox if you do not want to allow users to log on at all.
- ✓ **Yes, with Reason**: Select this checkbox to allow the users to log on by entering the reason.
- ✓ **Allow from All IPs**: Select this checkbox to allow them to log on using all IP Addresses.
- ✓ **Allow from Specific IPs**: Select this checkbox to allow them to log on from the specific IP Addresses. Once you select the checkbox, enter the IPs from which you want to allow.

MULTIFACTOR AUTHENTICATION

When this feature is enabled, you can use multiple authentication methods to log on to the InSync software. As per your selected methods, the OTP (One-Time Password) can be sent via email or SMS. You can also use mobile authenticator to enter the OTP.



Enable Multifactor Authentication: Select Yes to enable the Multifactor Authentication.

Enable MFA for: You can configure authentication methods either for all the practice users or only for the desired users. Select the Custom option and then select the desired users from the drop-down list.

MFA Frequency: Select the interval at which you want to allow the user to log on through the authentication method.

- ✓ **Every Day**: Select this option to log on through authentication every day. Once you log on successfully, it will not ask for authentication again during the day.
- ✓ **Every Time**: Select this option to log on through authentication every time. In this case, it will ask for authentication every time the user logs on.
- ✓ **Custom**: Select this option and enter number of days. The system will ask for the authentication until then every day once while logging on for the first time.

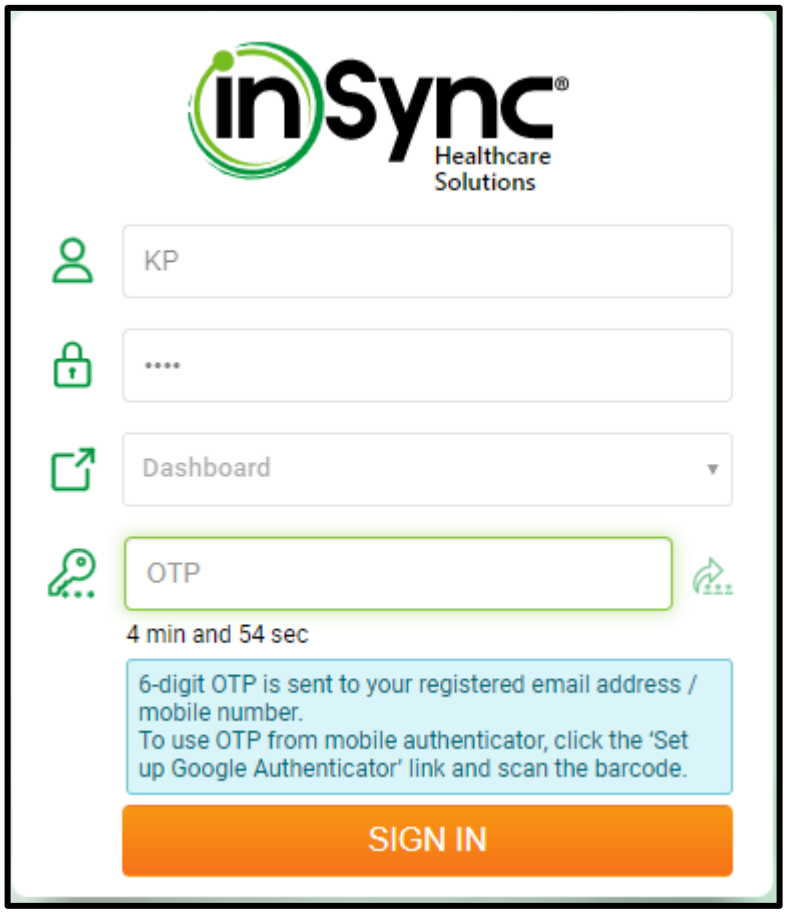
MFA Method: Select the desired method for Multifactor Authentication.

- ✓ **Email**: Select this checkbox to receive the OTP on your email address recorded in Resource Management.
- ✓ **SMS**: Select this checkbox to receive the OTP on your mobile device recorded in Resource Management.
- ✓ **Mobile Authenticator**: Select this checkbox if you have installed the Google Authenticator application in your mobile device and you want to use the OTP from there.

EMAIL AND SMS AUTHENTICATION

Based on your selected option (Email or SMS), OTP will be sent to your email address / mobile.

When you log on to the InSync software, the below screen will appear where you will have to enter 6-digit OTP received in your email / SMS. The OTP will expire after 5 minutes.



Upon entering the correct OTP and clicking SIGN IN, you will be able to access the InSync software successfully.

MOBILE AUTHENTICATION

You can use Mobile Authenticator to generate the OTP (One-Time Password) in your mobile through google authentication.

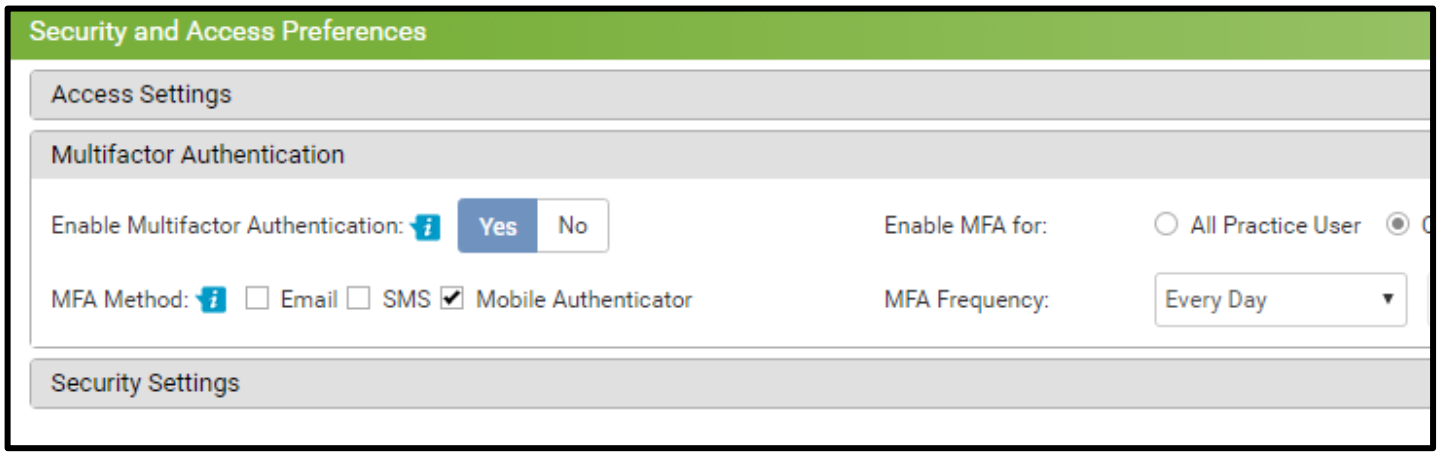
In this process, you will need to download Authenticator app from App Store. Once you download the app, you can scan the QR Code that appears by clicking on the **Set-up Google Authenticator** link on the login screen.

Use Mobile Authenticator for OTP (One-Time Password)

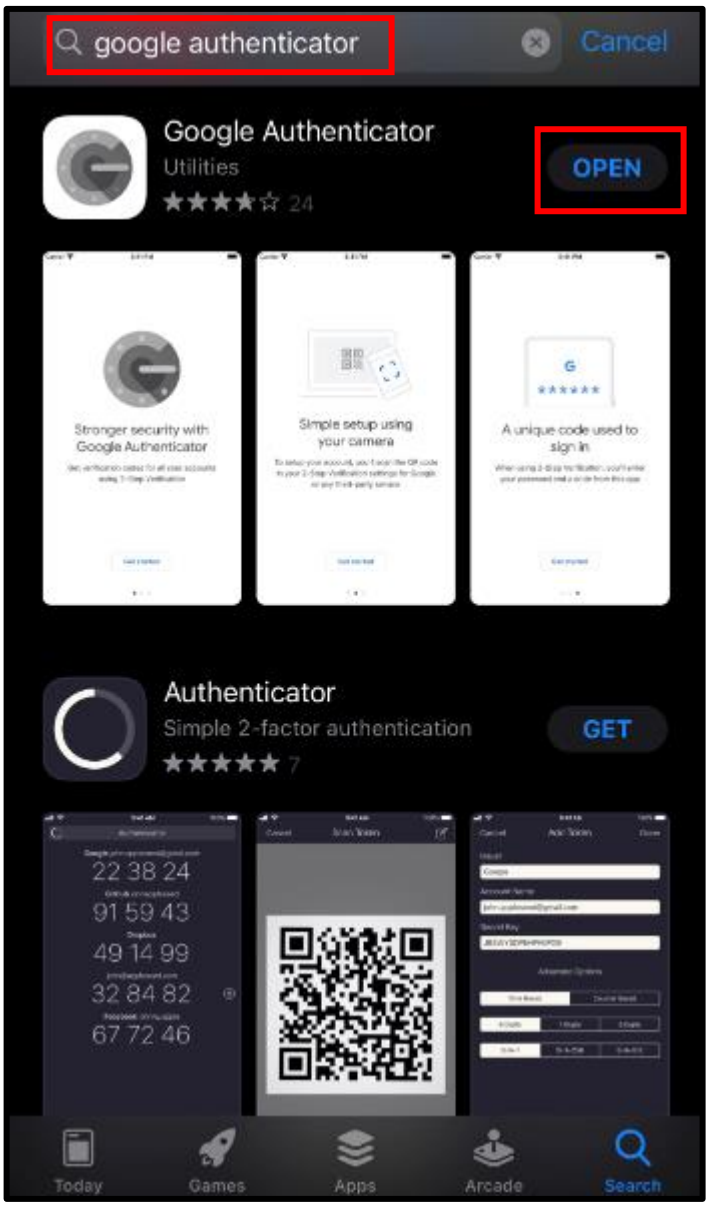
You can perform the following steps to log on to the system through mobile authenticator.

1. On the **Security and Access Preference** screen, expand the **Multifactor Authentication** panel and select the **Mobile Authenticator** check box. Click Save.

   *** You can configure this setting either all users of practice or for some specific users.*

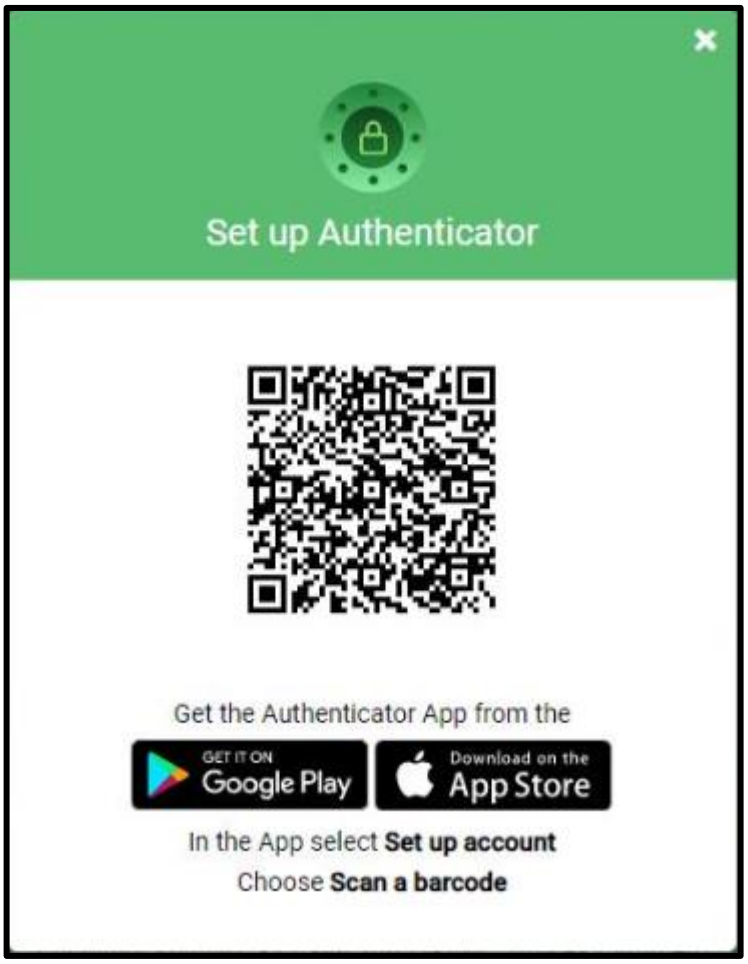


2. From your mobile, go to **App Store / Play Store** and download the Google Authenticator app. Once you download the app, tap on the OPEN button.

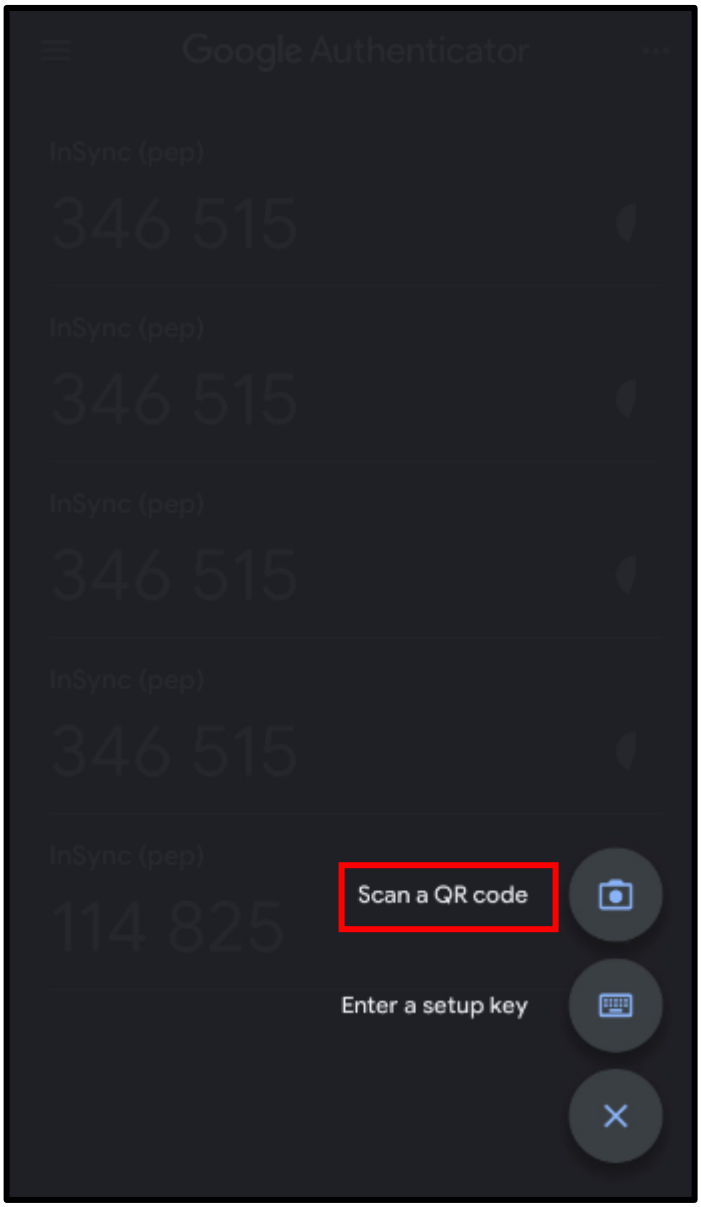


3. On the InSync login page, click on the **Set up Google Authenticator** link as indicated in the screen below.

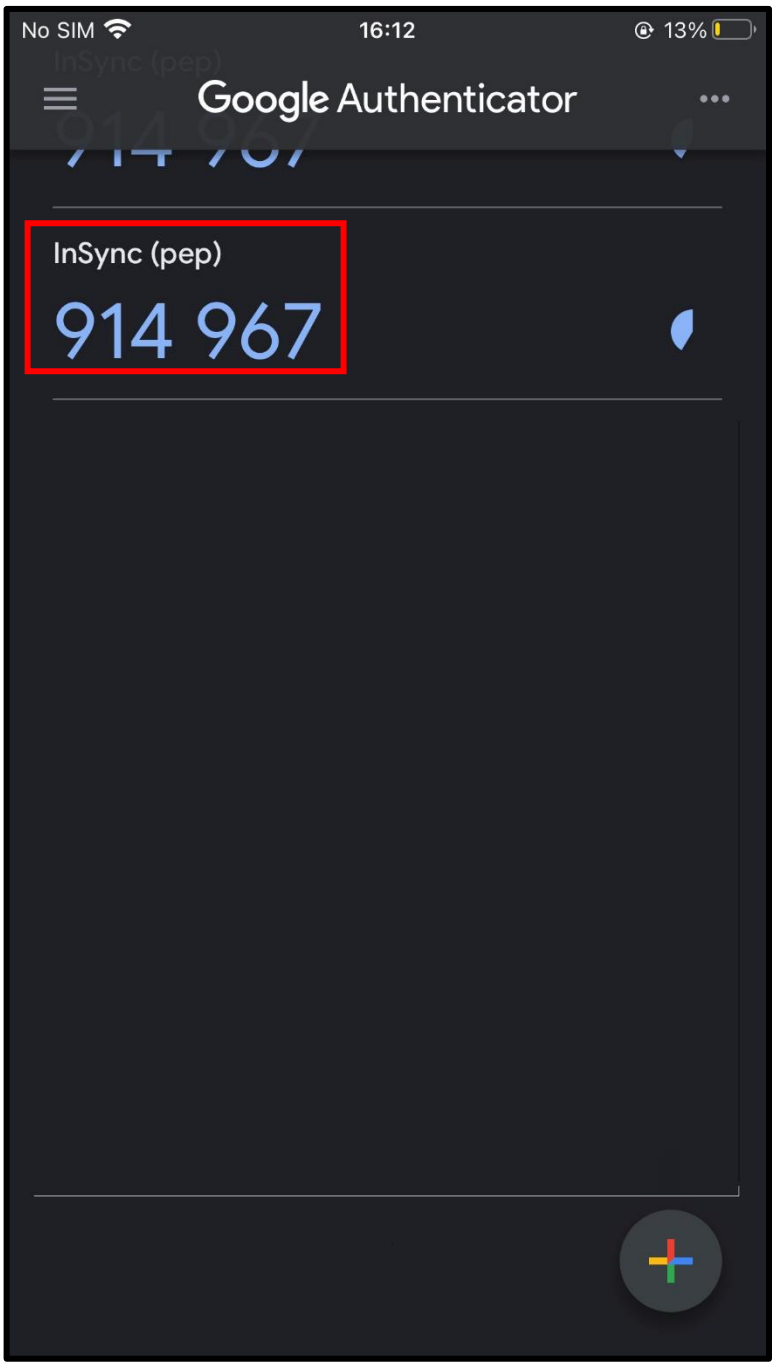
4. Clicking on the link will open the barcode as shown below.



5. Now, open Google Authenticator app from mobile and click on the Scan QR Code option.



6. When you scan the QR Code, you will receive One-Time Password (OTP) on your mobile as shown in the screen below.



7. When you log on to the InSync software, the below screen will appear where you will have to enter 6-digit OTP received in your mobile. The OTP will expire after 5 minutes.

8. Upon entering the correct OTP and clicking SIGN IN, you will be able to access the InSync software successfully.

SUPPORT

For additional assistance, please contact Support at 877-346-7962 or support@insynchcs.com.