



This TechNote describes how to turn on Two-factor Authentication for Agency Integrator.

For increased security of the application and the data it contains, you may want to enable two-factor Authentication, which requires your users to enter a 6-digit token (or second factor) to log into AI, in addition to their already-established password. The token can be sent via email, Microsoft Authenticator app, Authy app, and/or SMS Message, depending on each user's individual preferences. You will also be able to configure how often the system should require that second factor for all users in your agency; whether it be at each login to the system, or perhaps only once every 30 days.

Contents

Enabling Two-factor Authentication.....	2
Two-factor Authentication Methods.....	3
Email Authentication	3
App Authentication	5
SMS Authentication	6
Resetting / Disabling Two-factor Authentication	9
FAQs	11

Enabling Two-factor Authentication

You can enable Two Factor Authentication by going to **System Preferences**.

Click **Administration** from the main navigation bar, select **System** from the sub-menu bar, and then click **Preferences**.

System Preferences		
Preferences		
Preference ↕	Code ↕	Value
Turn on two factor authentication	2FA	select... ▼
Two factor authentication frequency	2FA FREQUENCY	

Two factor authentication is controlled by two **Preferences**:

1. **2FA:** Once set to **ON**, all users will be required to authenticate with a second factor (besides their password) to get logged into Agency Integrator.
2. **2FA FREQUENCY:** If Two-factor authentication is turned on, this is the number of days that can elapse before users will be required to authenticate again with a second factor on each device that they access AI from. If set to 0, users will be required to provide a second factor each time they log into AI on any device. If no value is entered, 30 days is assumed.

Preference ↕	Code ↕	Value
Turn on two factor authentication	2FA	select... ▼
Two factor authentication frequency	2FA FREQUENCY	select...
App Entry - Include Additional Detail	ADDAPPWIZ	Off
App Entry - Check LOB on Appointments	APPTLOBCHECK	On

To turn on **Two-factor authentication**, set the **2FA** Preference to **ON**, then set the **2FA Frequency** Preference as desired.

In the example below, with 2FAFREQUENCY set to “7”, users will be prompted to set up Two-factor authentication at their next login, but won’t be required to enter a token at login again on the

same device for seven days. See below for some additional information regarding how the system uses a combination of IP address, internet browser and operating system to control how often users are prompted to enter a token.

Preference ↕	Code ↕	Value
Turn on two factor authentication	2FA	On ▼
Two factor authentication frequency	2FA FREQUENCY	7

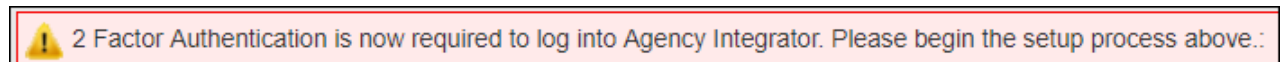
Scenario 1: User BSMITH sets up Two-factor on their laptop at work on the Internet Explorer browser. BSMITH always accesses AI from the same browser, laptop and IP address, so BSMITH won't be required to login with a second factor again for seven days.

Scenario 2: User CBILLS sets up Two-factor on their laptop at work on the Google Chrome browser. Then CBILLS logs into AI on a tablet, also using Chrome, and on the same work IP address. Because a different device is being used, even though the same IP address and browser are being used, CBILLS will be required to enter a token when logging in on their tablet, even though seven days have not elapsed.

Scenario 3: User JJONES sets up Two-factor on their laptop from their home's IP address, using the Google Chrome browser. The next morning, JJONES logs in from that same laptop also on Chrome, but this time from their office IP address. Because the IP address is different, the system will require a second factor, even though seven days have not elapsed.

Two-factor Authentication Methods

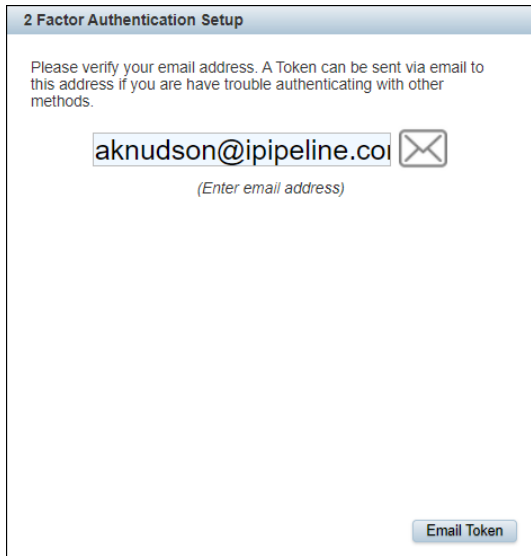
Log out and back in for the new Preference settings to take effect. When logging in, you will see this message at the bottom of the screen:



Email Authentication


You will be prompted to verify your email address first, as having a verified email address is required for all users of Two-factor authentication.

1. The email address from your user profile will be pre-populated for you. If desired, you can enter a different address to be used specifically for 2FA. Then click **Email Token**.



2 Factor Authentication Setup

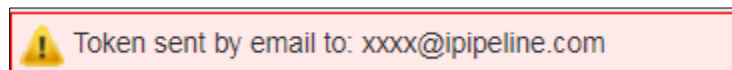
Please verify your email address. A Token can be sent via email to this address if you are have trouble authenticating with other methods.

aknudson@ipipeline.coi 

(Enter email address)

Email Token

2. A message will display:



3. Check your email for a one-time six-digit token.

Important Note: Emails will come from amssupport@ipipeline.com and might go to Clutter / Junk Mail.

Example email:

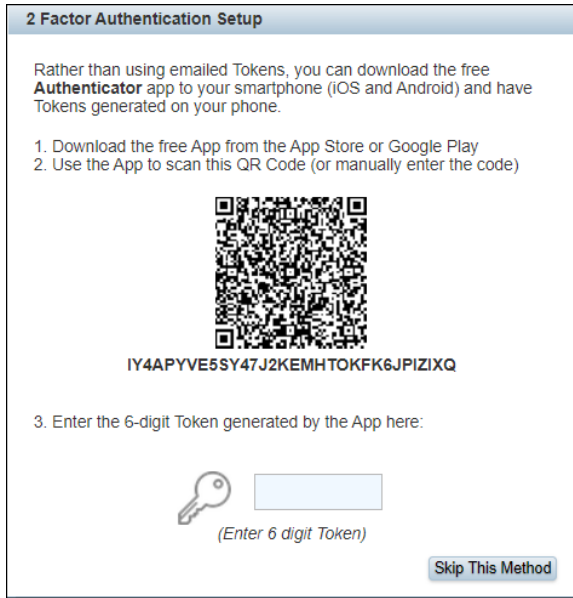
Your Agency Integrator time-based, one-time token is: 344078

This Token will expire in one to two minutes. After expiration, a new Token must be generated from the Agency Integrator login screen.

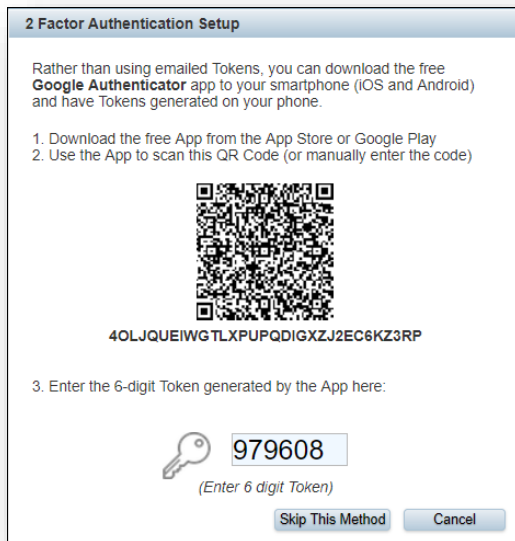
4. Enter the Six-digit token from the email. **Two Factor Authentication** set up is now complete for the Email method. You have the option to add two additional methods (Microsoft Authenticator, Authy, and/or SMS), or skip the additional methods and always receive your token via email.

App Authentication

This authentication method requires a free download from the App Store or Google Play (IOS and Android). There are two apps that work with Agency Integrator: **Microsoft Authenticator** and **Authy**.




1. Search for the **Microsoft Authenticator** or **Authy** app in the App Store or Google Play and download it.
2. After the download, open the **Microsoft Authenticator** or **Authy** app on your device.
3. Click, **Add Account** or select the three dots in the top right and click **Add Account**.
4. Hold your device's camera up to the Agency Integrator screen to scan the **QR Code**.
5. After scanning the QR Code, a token is provided on your device:
6. Enter the six-digit token:



2 Factor Authentication Setup


Rather than using emailed Tokens, you can download the free **Google Authenticator** app to your smartphone (iOS and Android) and have Tokens generated on your phone.

1. Download the free App from the App Store or Google Play
2. Use the App to scan this QR Code (or manually enter the code)



4OLJQUEIWGTLXPUPQDIGXZJ2EC6KZ3RP

3. Enter the 6-digit Token generated by the App here:

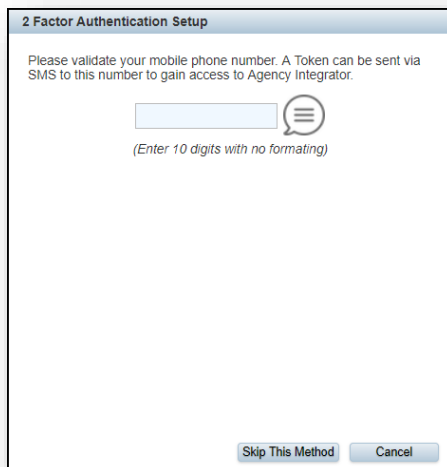


(Enter 6 digit Token)

Two Factor Authentication set up is now complete for the app method. You have the option to add one additional methods (SMS), or skip the additional method and always receive your token via Email or Authenticator.


SMS Authentication

This authentication method will send the six-digit token to you via text message. Standard messaging rates apply.



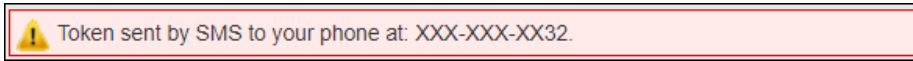
2 Factor Authentication Setup

Please validate your mobile phone number. A Token can be sent via SMS to this number to gain access to Agency Integrator.

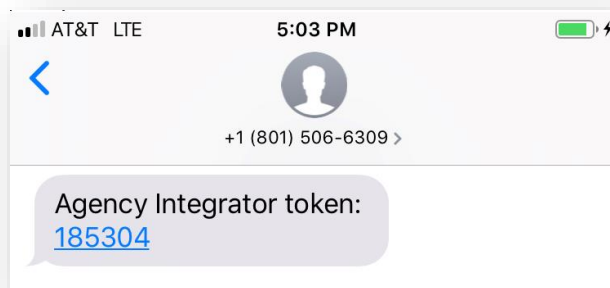


(Enter 10 digits with no formatting)

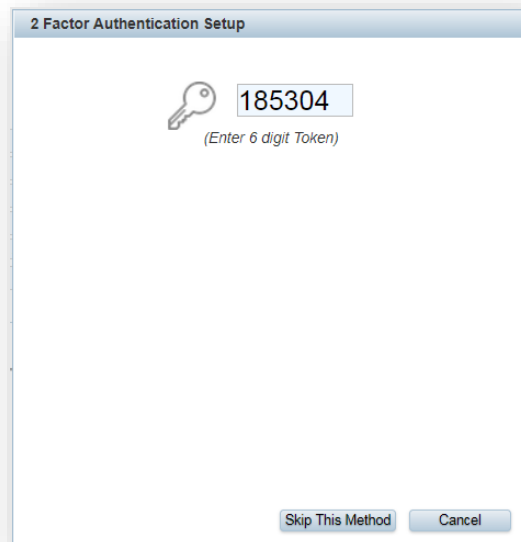
1. Enter the mobile phone number you wish to receive your tokens to. The token will automatically be sent without clicking anything. A message is displayed:



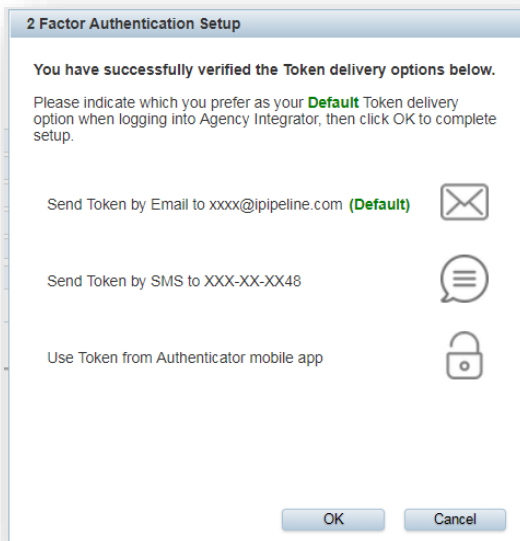
Example SMS:



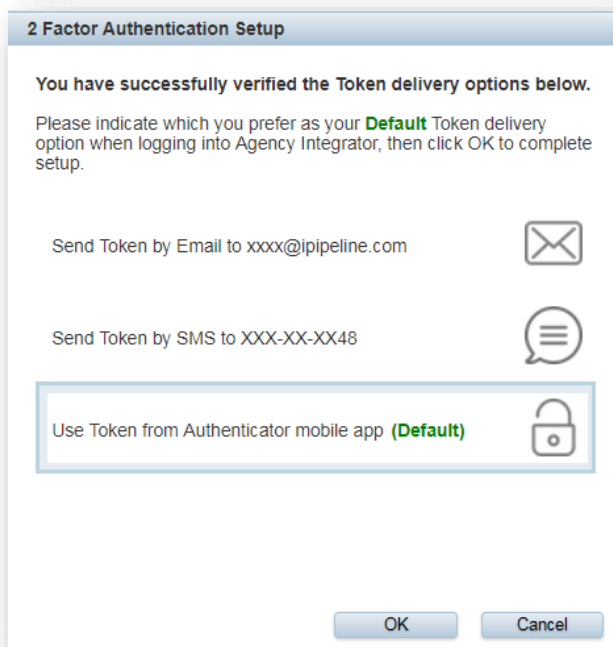
2. Enter the six-digit token from the SMS:



3. Once complete, you will be prompted to select a **Default** authentication method. Whichever method is chosen here will determine how the system delivers your tokens going forward. Note that you won't be given an option at your next login, the system will simply use whatever is set here as the Default.

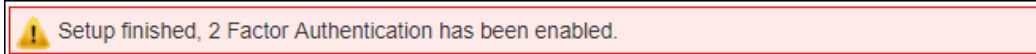


Email has been chosen for you, but you can click on **SMS** or **Authenticator** if you prefer. Your choice will be outlined in blue and the green **(Default)** text will be displayed next to it:



4. Click **OK** after selecting your desired **Default** method.

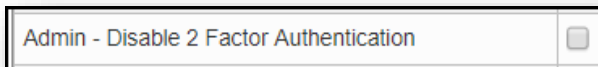
5. A message displays indicating that setup is complete:



Resetting / Disabling Two-factor Authentication

After setup is complete, each user will have the ability to temporarily turn off 2FA for their own user ID if needed, without adding any additional UserRights.

A User Right (**Admin-Disable 2 Factor Authentication**) can also be assigned to authorized Administrators who should be able to Reset/Disable 2FA for other users in the agency.



Scenarios where this option might be helpful:

- Users with SMS or App as their Default delivery method who leave their phone at home for the day or have lost their phone
- Users with SMS or App as their Default delivery method who get a new phone number
- Users with Email as their Default delivery method who get a new email address
- Users who wish to switch their Default delivery method to a different one

Each user will see two new buttons on their User Profile: **Setup 2 Factor Authentication** and **Reset/Disable 2 Factor Authentication**

Clicking on the **Reset/Disable 2 Factor Authentication** button (either for your own User ID or another User ID) will temporarily disable the two factor requirement, allowing the user to login once with only their password. Then, after login, they will be prompted to set up 2FA again.

If an administrative user has the appropriate User Right assigned, they will also see these two buttons when accessing other Users' Profiles.

1. Click **Administration**
2. Select **Users**, then click **User Administration**.
3. Select the name of the user to work with:

FAQs

Q: By selecting 0 (zero) as the frequency, will two factor authentication be required at every log in on every device?

- Yes.

Q: Do I have to set up all three methods of authentication?

- No. You can choose to set up one, two, or all three available methods. You will be given an option to pick a default method prompt before set-up completion.

Q: How many times can I try the six-digit token before it's no longer valid?

- After three failed attempts, the user will need to log in again.

Q: What if I log in to AI with a different IP address or device?

- You will be required to enter a token each time you log in on a different device. An email will also be sent to you, indicating that there was a sign on to AI from a new connection:

