Two-Factor Authentication for K12Docs

If desired, two-factor authentication for K12Docs (and Host Site Manager) can be enabled for an organization's domain. If two-factor authentication is requested to be enabled for a domain, it is turned on after the initial training is completed.

Note: Two-factor authentication does not apply to GX.

Steps to Enable and Use Two-factor Authentication for K12Docs (and Host Site Manager):

1. A user who is defined as the K12Docs administrator for the organization must log into Host Site Manager and enter an email address for each defined K12Docs user.

   Note: Do not make any changes to the required users: HSMAdmin, HSMNotify, SUIAdmin, SAS, Svcuser, and K12docscloudconnect.
2. Once all the K12Docs users have an email address entered, contact Customer Support at Software Unlimited, Inc. to request two-factor authentication to be enabled for the organization's domain.
3. Inform all K12Docs users at the organization to install the Google Authenticator app on their phone. See below for an image of the Google Authenticator app to be sure the correct one is downloaded.

4. After two-factor authentication has been enabled for the organization's domain, each K12Docs user must complete the following steps the first time logging into K12Docs or Host Site Manager:
   a. On the Signin screen, complete the Domain Name and User Name fields and then click the **Continue** button. See **Diagram A**.
   b. Complete the Password field and then click the **Signin** button. See **Diagram B**.
   c. On the next screen (see **Diagram C**), click the **Google Authenticator Code** link.

Diagram A

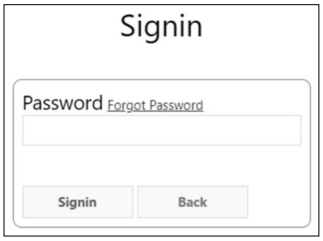

Diagram B

Diagram C

   d. The screen with the QR code (and secret code if needed) will display. See **Diagram D**.

      Note: The QR code is unique for each user (email address).
   e. Scan the QR code using the Google Authenticator app on your phone (or enter the secret code if unable to scan the QR code).
   f. After the QR code has been scanned in the Google Authenticator app (or the secret code entered, if unable to scan the QR code), click the **Return to Signin** link located under the QR code.

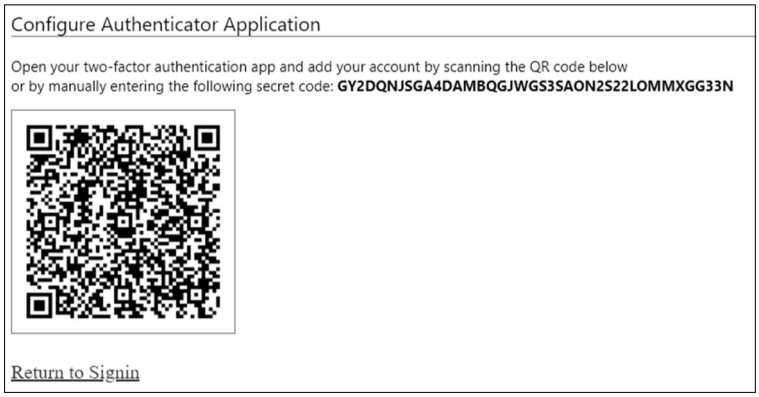

Diagram D

g. When prompted to enter the password token, enter the code from the Google Authenticator app on your phone into the One-Time Password Token field.

h. After the code has been entered, click the **Verify** button to log in.

Note: This is a one-time setup that needs to be done, and it applies for use with both K12Docs and Host Site Manager. After the setup has been completed, the **Google Authenticator Code** link (as shown in **Diagram C**) will no longer display; if the QR code needs to be accessed by the user in the future (for example, if the user has a new phone and needs to set up the Google Authenticator app for use with the new phone), contact Customer Support at Software Unlimited, Inc.

5. In the future, each K12Docs user must complete the following steps for two-factor authentication when logging into K12Docs directly or logging into Host Site Manager:

   a. On the Signin screen, complete the Domain Name and User Name fields and then click the **Continue** button. See **Diagram A**.

   b. Complete the Password field and then click the **Signin** button. See **Diagram B**.

   d. On the next screen (see **Diagram E**), when prompted for the password token, open the Google Authenticator app on your phone to view the token (see **Diagram F**), and then enter the code from the app into the One-Time Password Token field.

   Note: The code within the Google Authenticator app is applicable for 30 seconds and then a new code will automatically display.

   e. After the code has been entered, click the **Verify** button to log in.

Diagram E

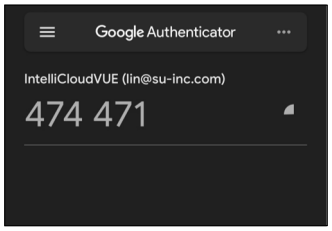

Diagram F