Google Authenticator Web based Desktop install

For Chrome and Firefox

Installation:

Chrome:

1. For Chrome use this link: https://authenticator.cc/ Click on Add to Chrome button:
2. Click on the button “Add to Chrome”:

![Chrome Web Store](image)

3. Click on the button “Add extension” in the pop-up:

![Add Extension Popup](image)

4. You will see this new extension icon in the upper right hand of side of Chrome:

![Extension Icon](image)
Firefox:

1. For Firefox Use this link: https://addons.mozilla.org/en-US/firefox/addon/auth-helper/

2. Click on the button “Add to Firefox”:

3. Click Add button in the pop-up:

4. You will see this new extension icon in the upper right hand of side of Firefox along with a pop-up that says it has been added Click “OK”:
Setup:

1. Click on the Authenticator icon:

2. Click on settings:
3. Click Security, from the settings menu, to create a password that will be used to secure the application (note this password should not be the same as your password to sign on to your desktop or your Cas login):

![Settings Menu]

This password will be used to encrypt your accounts. No one can help you if you forget the password.

Password

Confirm Password

Ok
Remove
4. After supplying a unique password click Ok and Ok again:

This password will be used to encrypt your accounts. No one can help you if you forget the password.

Password

··········

Success.

Ok

Ok  Remove

5. Click the X in the upper left hand corner to return to the settings menu:

This password will be used to encrypt your accounts. No one can help you if you forget the password.

Password

··········

Confirm Password

··········

Ok  Remove
6. Click “Storage and Backup” from the settings menu, to store your key for the application (note: this will allow you to restore the application should your pc be replaced in the future):
7. Select sync for Storage Location and the click Google Drive (note: you will need to be signed in to your Messiah google account in Chrome):

Choose where your data is stored. Using 'local' stores your data on your PC. Using 'sync' lets your browser sync your data to the cloud if you are signed into a sync account.

Storage Location

Automatically backup your data to 3rd party storage services.

Google Drive

Dropbox

8. Click Allow for Authenticator to be granted additional permissions:
9. Click Sign in (note: this will be your userid@messiah.edu and messiah password):

   ![Sign in](image)

10. You will be presented with a sign-on for Chrome, use your Messiah email as the ID:

   ![Google Sign in to Chrome](image)
11. After clicking next supply your Messiah password and click next again:

Welcome

Enter your password

Forgot password?  Next
12. After authenticating a popup will appear asking which account to connect Authenticator to select the account with the @messiah.edu address:

Choose an account to continue to Authenticator Backup

- Allen Snook
  asnook@messiah.edu

- Use another account
13. You will then see this popup click the Allow button:

Sign in with Google

Authenticator Backup wants to access your Google Account

asnoook@messiah.edu

This will allow Authenticator Backup to:

View and manage Google Drive files and folders that you have opened or created with this app

Make sure you trust Authenticator Backup

You may be sharing sensitive info with this site or app. Learn about how Authenticator Backup will handle your data by reviewing its privacy policies. You can always see or remove access in your Google Account.

Learn about the risks

Cancel   Allow
Add Sites:

**Visa Intellilink:** [https://identity.intellilink.spendmanagement.visa.com/](https://identity.intellilink.spendmanagement.visa.com/)

1. For the Visa website that is requiring 2 factor authentication after logging in you will receive this page click “Use other authentication methods”:
2. Choose the Authenticator App from the Drop Down menu:

Enable two-factor authentication

- Install the authenticator app on your mobile device and scan the QR code from the app to generate an authentication code. [View supported apps]

Unable to scan the QR code?

- Enter the authentication code generated by your authenticator app

[Code] [Verify]

[Use other authentication methods]
3. Now Click on the Authenticator extension icon:
4. Click the scan QR code button:

5. You will need to select the QR as shown:

Enable two-factor authentication

Install the authenticator app on your mobile device and scan the QR code from the app to generate an authentication code. View supported apps.

Unable to scan the QR code?

Enter the authentication code generated by your authenticator app.
6. When selected properly you will receive this pop-up select Ok:

```
identity.intelliink.spendmanagement.visa.com says
asnook@messiah.edu has been added.
```

7. Opening the Authenticator app again you will see something like this:

```
Authenticator

Show all entries

visa
802304
asnook@messiah.edu
```

8. You will need to enter the 6 digit pin number to verify it is working properly:

```
Enter the authentication code generated by your authenticator app

******  Verify
```

9. After successful verification of the pin you will be logged into the Visa IntelliLink website and you should also receive an email saying you successfully setup Two-Factor authentication.
10. In the Authenticator extension click the Lock button each time, to secure the app, you will be required to use the password you supplied during setup to view the pin in the future:

![Authenticator Extension](image)

11. The next time you access the Authenticator extension you will be required to enter your password:

![Password Entry](image)
Troubleshooting / Fixes:

Remove a site:

1. Open the Authenticator app:

2. Click on the pencil icon in the upper right hand corner:
3. After Clicking edit / to remove a site Click the red circle with a line through it in the upper left corner of the site you wish to remove:

![Authenticator](image1)

4. Answer “Yes” to remove:

![Authenticator](image2)
5. It will look similar to this when removed:

![Authenticator](image)

**Visa MFA reset: (remove Email pin)**

1. Call Daisy Anderson or Stephanie Sechrist at X2211, ask them to reset the users’ Multi Factor Authentication option.
2. Have the sure sign-on as normal and then proceed with the site setup as described above.