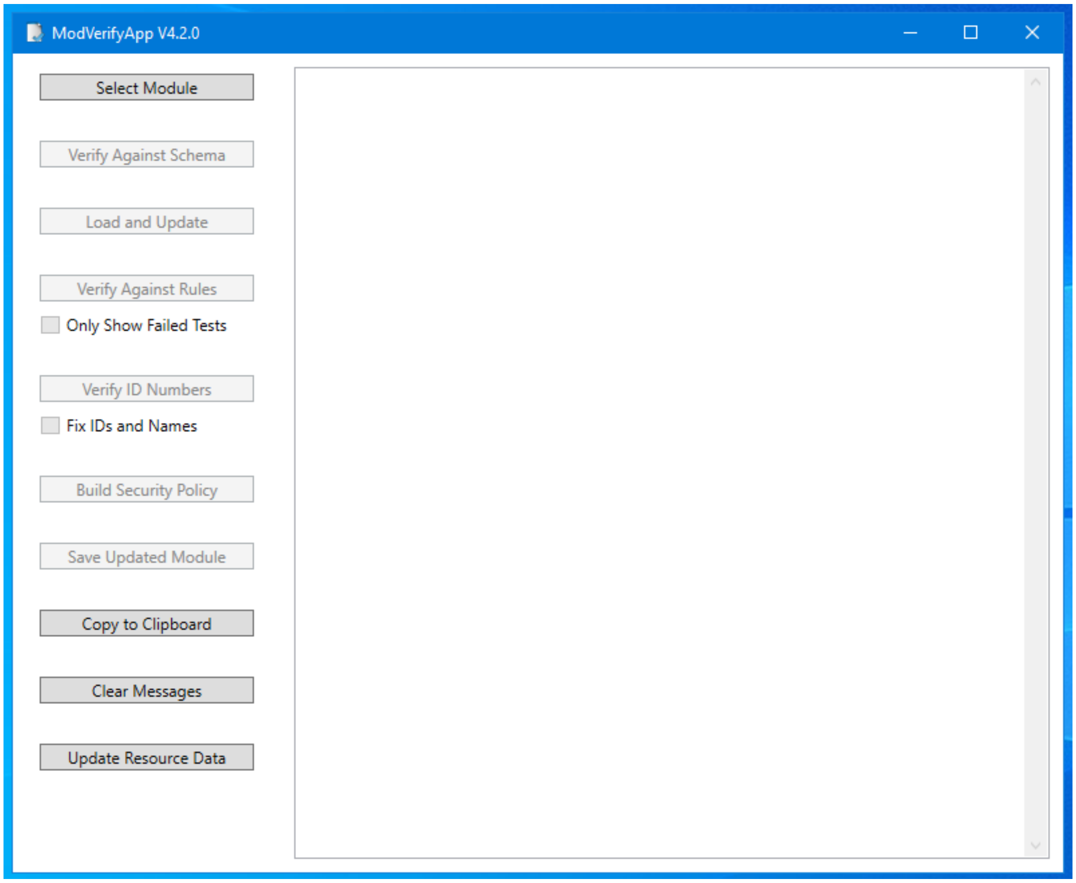
ModVerifyApp Use Instructions

(3/22/2024)

Description: ModVerifyApp is a Windows desktop application, dependent on .net Version 6, that is used to work with the _module.json file that contains the module related information entered in Web Cryptik Br1. There are functions that this program performs that are not yet available within Web Cryptik Br1.

Installation:

1. Download the ModVerifyApp zip file from the CMVP SP800-140B webpage: https://csrc.nist.gov/projects/cmvp/sp800-140b
2. Create a directory (the name is not required to match any defined name or format but it would be helpful to name it ModVerifyApp) and unzip the contents of the zip file into that directory.
3. To run the program, run the ModVerifyApp.exe executable file.
4. The following window should appear:



Load Resource Data: If this is the first time the program has been run, you will see the message "Unable to find ResourceDataGroup.json" displayed. This indicates that the latest set of resource files need to be loaded into the program. These are combined into a ResourceFiles.zip file that is included in the program zip file and should be available in the directory the program is located. Click on the "Update Resource Data" button and select the "ResourceFiles.zip" file. The files will be loaded and the "Select Module" button will become active.

There will be occasions in the future when the resource files will be updated. A new ResourceFiles.zip file will be available on the 140B webpage. Download that file and repeat the above procedure to update the resources. The CMVP will send out a notice when there are updates available to download and update.

Select Module: Click this button and select the appropriate _module.json file. The file is opened and the text of the json is loaded into the program. This enables the “Verify Against Schema” button. Once a module is selected, the “Verify Against Schema” button will become active.

Verify Against Schema: This button compares the selected _module.json against the latest MisSchema file and displays the schema errors. Often these errors exist as a result of having created the _module.json file with an earlier version of Web Cryptik Br1. Whether or not there are errors, the next step is to click the “Load and Update” button.

Load and Update: This button evaluates the loaded json and upgrades the information and structure to match the current schema version. Where possible, data existing in the selected module will be converted to match the structure of the current schema. At times, the schema is invalid and the program reports that the module cannot be successfully upgraded. Is successfully loaded and upgraded, the module should report that there are no schema errors.

Verify Against Rules: The resource files contain a set of validation rules to be run against the module to determine is the data contained passes those rules. Clicking on the button runs the rules against the loaded module and reports the results, grouped by table/category. The results will show both successes and failures. To see only the rule failures, select the “Only Show Failed Tests” option.

Verify ID Numbers: Within the _module.json, there are instances where the text representing an item has an associated ID number that is internal to the NIST systems. When the _module.json is built from Web Cryptik Br1, all of these ID numbers should be included. When these particularly elements within the _module.json are edited directly, the ID numbers can be missing. Clicking the button display a list where there is a missing or mis-matched entry. Selecting the “Fix IDs and Names” checkbox before clicking the button instructs the program to attempt to fill in missing and to correct inaccurate values. Typically this option would only be necessary in very limited cases when _module.json has been directly edited.

Build Security Policy: Previously in the SP800-140Br1 process, there was a separate program (SPBuilderApp) available to merge the information in _module.json with the completed SP template. That program has been eliminated and the function combined into ModVerifyApp.

After clicking this button, select the completed SPTemplate word document and the loaded module will be merged with the template and a new document, with “-new” added to the selected filename will be created in the same directory as the selected template.

Save Updated Module: Because there are ways this program updates the _module.json, this button provides the option to save the module in a json file with the updated content and matching the current schema. Though possible, it is recommended that the saved module file doesn’t overwrite the originally selected file.

Copy to Clipboard: Copies the text of the messages in the window to the clipboard.

Clear Messages: Clicking this button clears all the messages in the window.

Important Note: Because of the potential of changes in the _module.json schema related to different versions of Web Cryptik Br1, it is important to Select, Load and Update, and Save previously generated _module.json files before importing them into Web Cryptik Br1. Web Cryptik is not able to upgrade schema and even with editing and saving, will perpetuate schema errors into newer versions.