z/OS V2.5 IBM Education Assistant

Solution Name: Security Configuration Assistant support external product

Solution Element(s): z/OSMF Security Configuration Assistant

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- Any z/OS components/products (Exploiters) can create security requirement descriptor files in JSON which can be imported into z/OSMF Security Configuration Assistant later by end users
- System programmers (End users) can use Security Configuration Assistant to review and validate security requirements of imported products.
- In V2R5, the first batch of exploiters are DFSMShsm, DFSMSrmm and DFSMSdss.
- Users can also create their own security descriptor files in JSON and import the JSON into SCA.

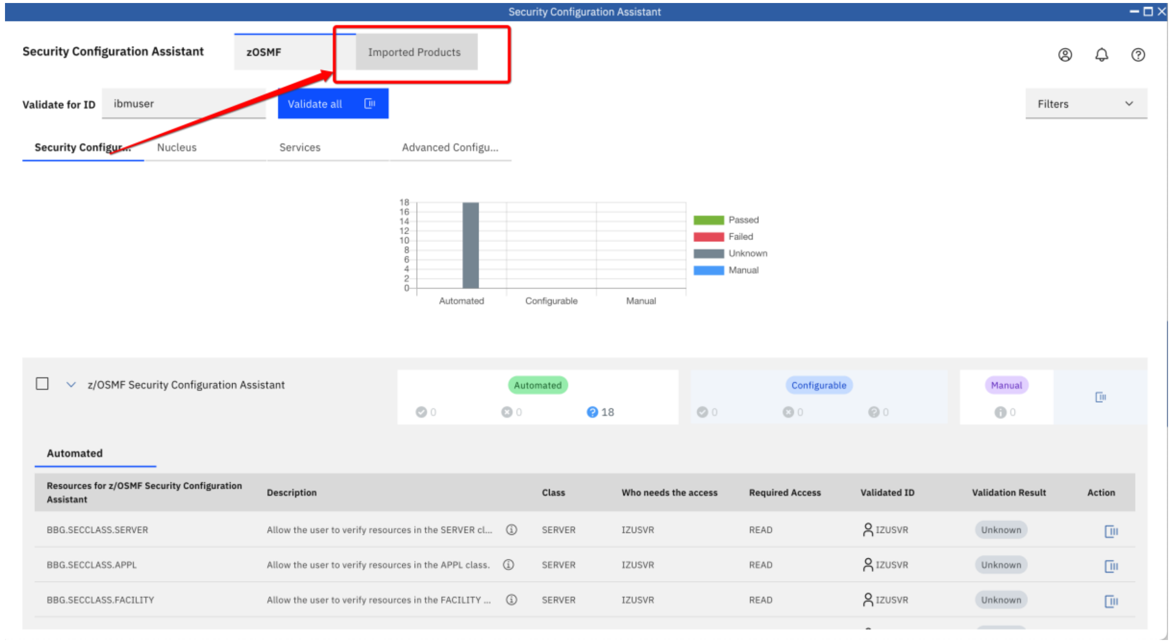
Overview

- Who (Audience)
  - Application Developers
  - System Programmers
- What (Solution)
  - Application developers can describe application security requirements in a JSON file which can be imported into SCA by the end user.
  - End Users can customize a security requirement JSON file which can be imported into SCA.
  - End Users/System Programmers can import multiple JSONs which contains specific security requirements into SCA, and use existing SCA capability to do security validation.
- Wow (Benefit / Value, Need Addressed)
  - Without the need of manual security verification which takes minutes to hours, end users can do security validation in seconds.

Usage & Invocation (1)

Scenario 1 – Validate security requirement of DFSMS components

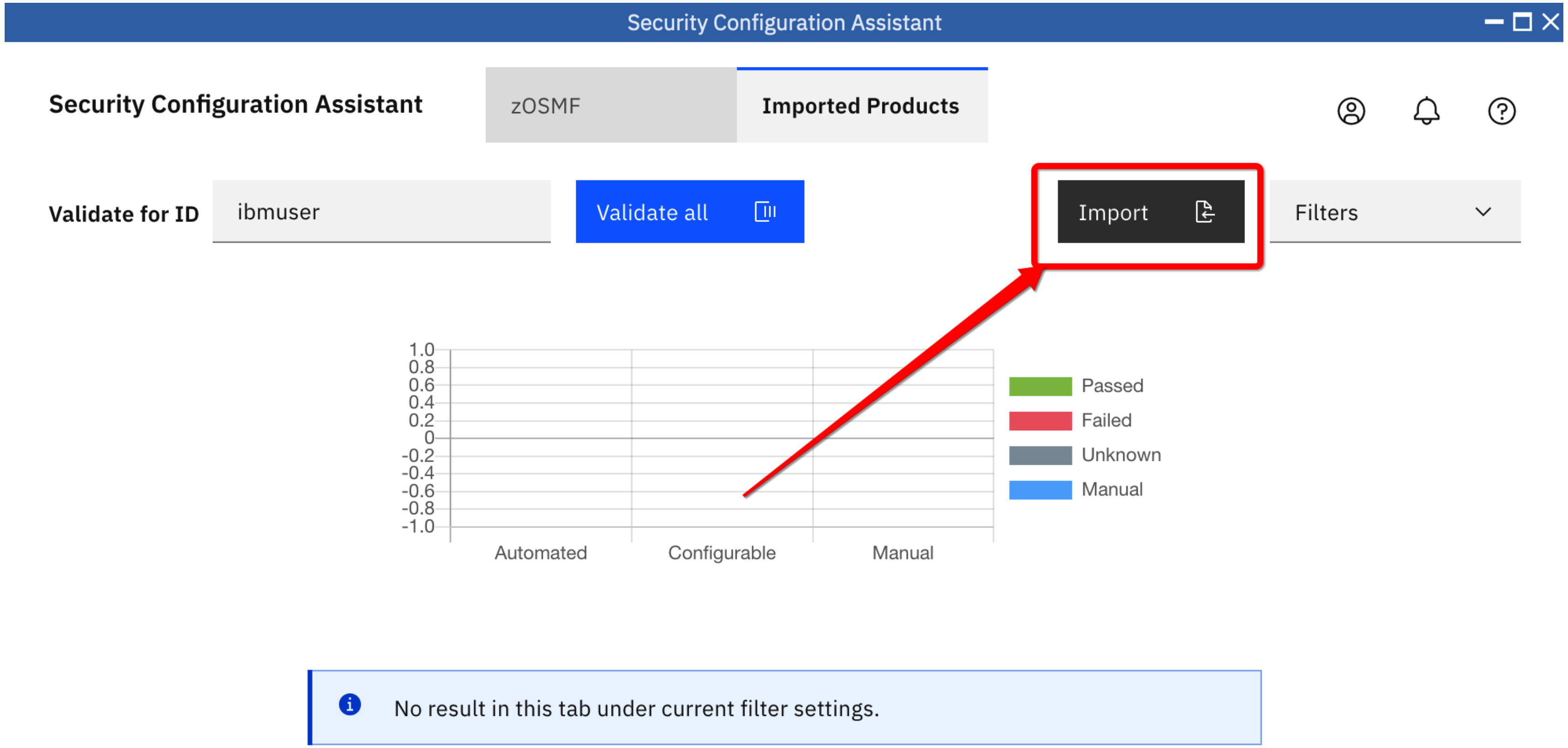
- Step 1.1 – Copy DFSMShsm jsons from '/usr/lpp/dfsms/hsm' to /global/zosmf/configuraiton/security' (replace /global/zosmf with your z/OSMF data directory if there's customization)
- Step 1.2 – Open Security Configuration Assistant, click on the Tab "Imported Products"



Resources for z/OSMF Security Configuration Assistant	Description	Class	Who needs the access	Required Access	Validated ID	Validation Result	Action
BBG.SECCLASS.SERVER	Allow the user to verify resources in the SERVER cl...	SERVER	IZUSVR	READ	IZUSVR	Unknown	
BBG.SECCLASS.APPL	Allow the user to verify resources in the APPL class.	SERVER	IZUSVR	READ	IZUSVR	Unknown	
BBG.SECCLASS.FACILITY	Allow the user to verify resources in the FACILITY ...	SERVER	IZUSVR	READ	IZUSVR	Unknown	

Usage & Invocation (2)

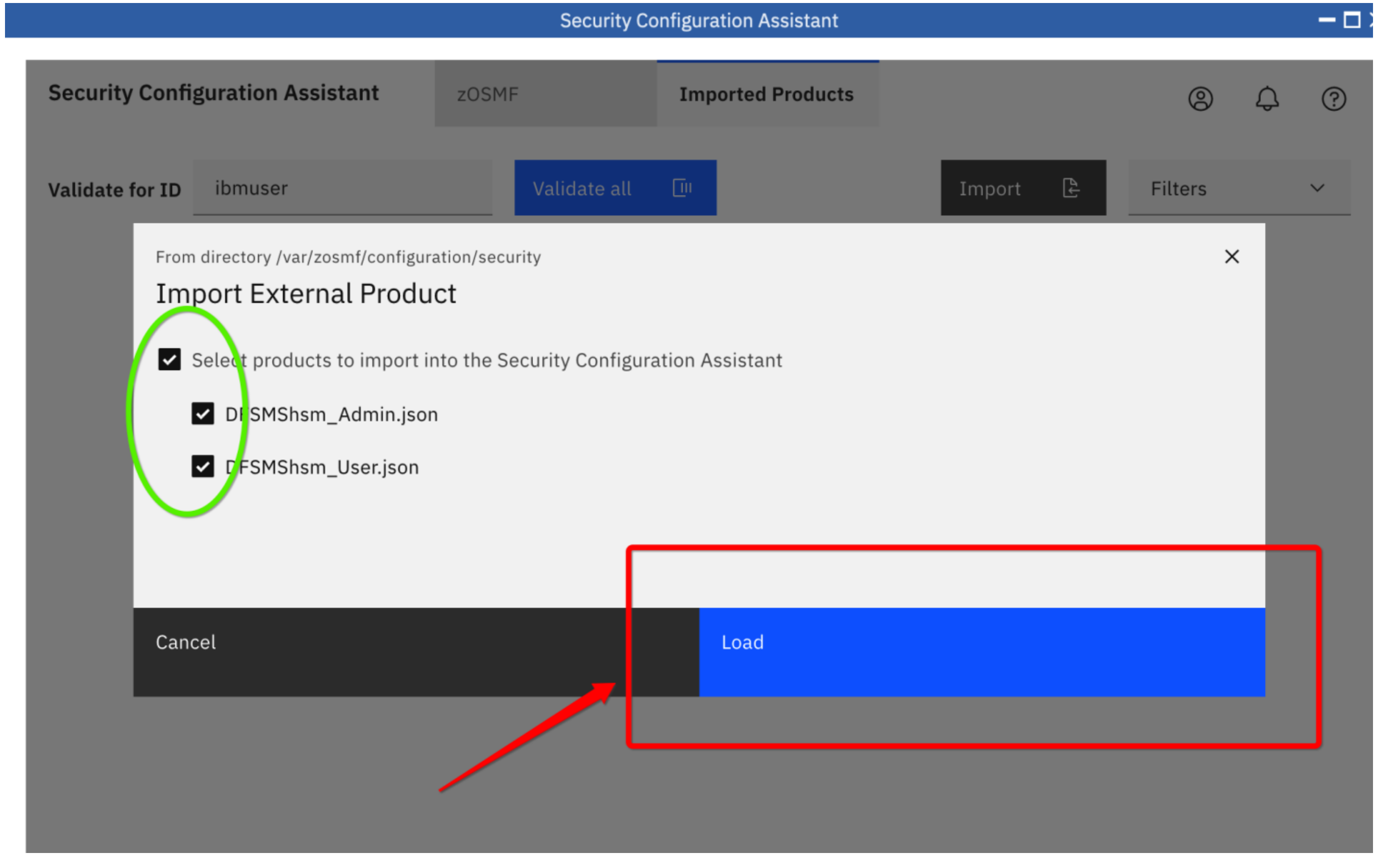
- Step 2 – Click on the "Import" button on "Imported Products" panel



No result in this tab under current filter settings.

Usage & Invocation (3)

- Step 3 – On the "Import" dialogue box, the JSON files you just copied are selected by default. Review the list of files you are going to import into SCA. You can unselect the JSON files you don't need later. When the review is done, click on the "Load" button.



Security Configuration Assistant
Security Configuration Assistant
zOSMF
Imported Products
Validate all
Import
Filters
Cancel
Load

Validate for ID ibmuser

From directory /var/zosmf/configuration/security

Import External Product

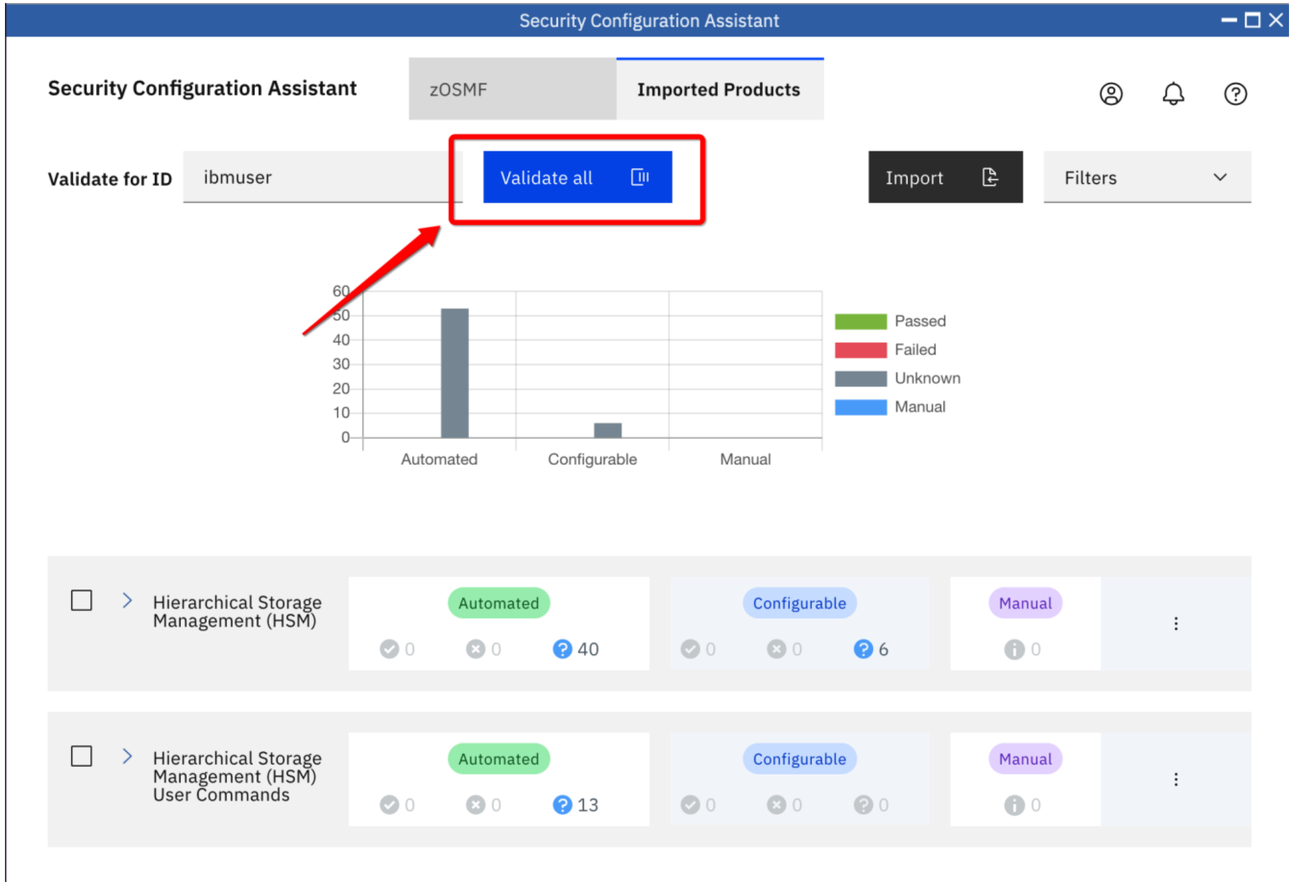
☑ Select products to import into the Security Configuration Assistant

☑ DFSMShsm_Admin.json

☑ DFSMShsm_User.json

Usage & Invocation (4)

- Step 4 – You can review the security requirements just loaded. Click on "Validate All" button to start validating the requirements for your logged on user. Alternatively you change validate the requirements on another user ID.

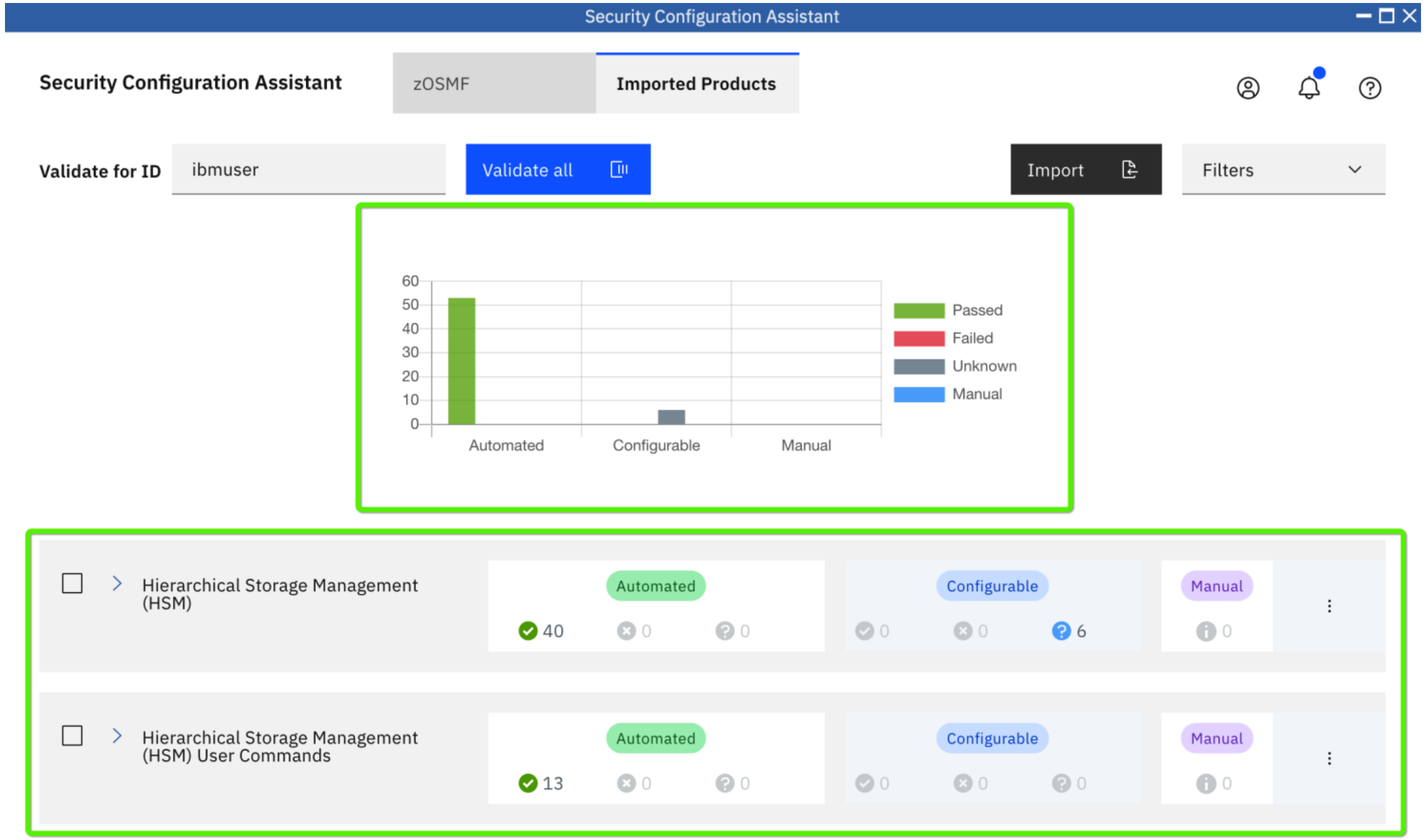


Validate for ID: ibmuser

	Automated	Configurable	Manual
□ Hierarchical Storage Management (HSM)	✓ 0 ✗ 0 ? 40	✓ 0 ✗ 0 ? 6	i 0
□ Hierarchical Storage Management (HSM) User Commands	✓ 0 ✗ 0 ? 13	✓ 0 ✗ 0 ? 0	i 0

Usage & Invocation (5)

- Step 5 – Review validation report once the validation is completed

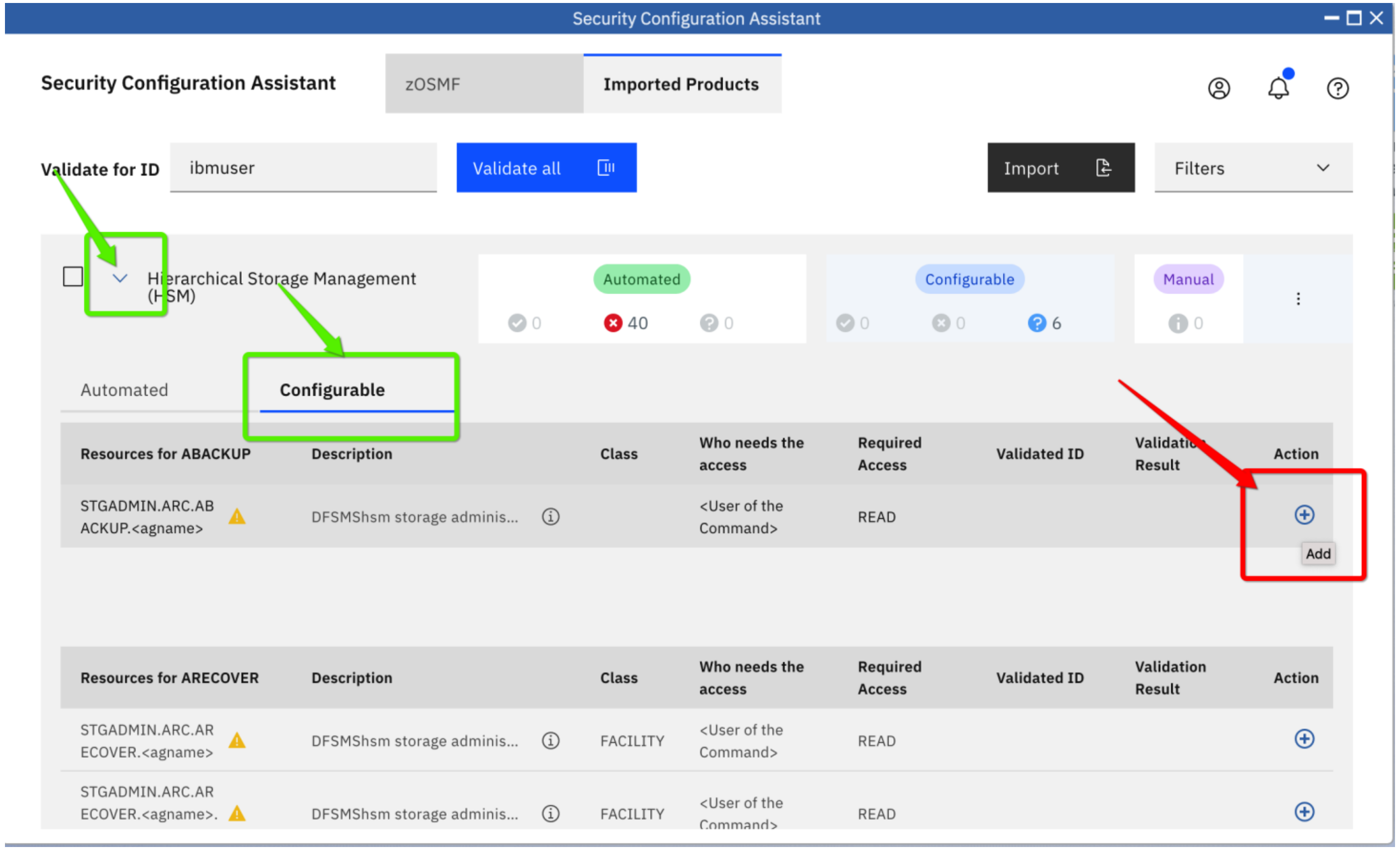


Validate for ID: ibmuser

	Product	Automated			Configurable			Manual
□	Hierarchical Storage Management (HSM)	✓ 40	✗ 0	? 0	✓ 0	✗ 0	? 6	ⓘ 0
□	Hierarchical Storage Management (HSM) User Commands	✓ 13	✗ 0	? 0	✓ 0	✗ 0	? 0	ⓘ 0

Usage & Invocation (6)

- Step 6 – To validate resources in "Configurable" column, you must provide your security customization by adding one or more values on the variables.



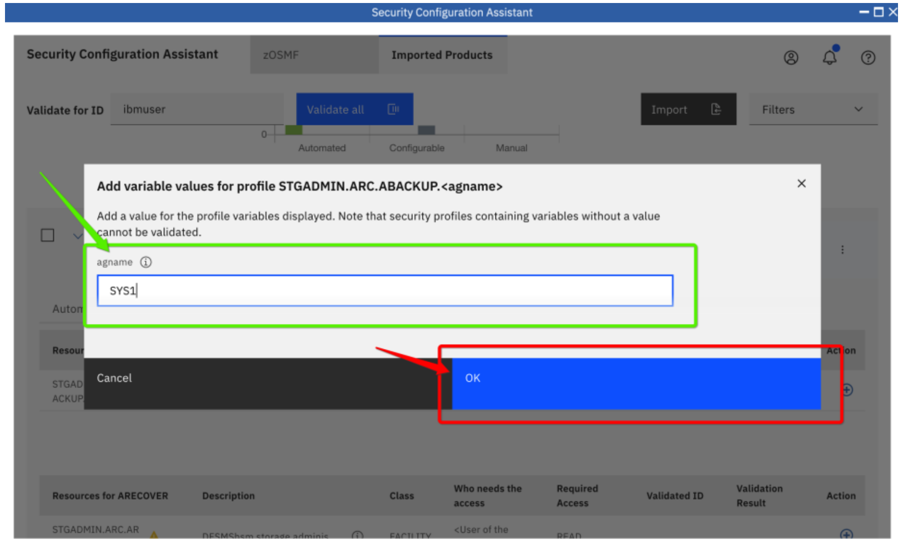
Validate for ID: ibmuser

□ Hierarchical Storage Management (HSM)

Automated			Configurable			Manual
✓ 0	✕ 40	? 0	✓ 0	✕ 0	? 6	i 0

Resources for ABACKUP	Description	Class	Who needs the access	Required Access	Validated ID	Validation Result	Action
STGADMIN.ARC.ABACKUP.<agname> ⚠	DFSMShsm storage adminis... ⓘ		<User of the Command>	READ			⊕

Resources for ARECOVER	Description	Class	Who needs the access	Required Access	Validated ID	Validation Result	Action
STGADMIN.ARC.ARECOVER.<agname> ⚠	DFSMShsm storage adminis... ⓘ	FACILITY	<User of the Command>	READ			⊕
STGADMIN.ARC.ARECOVER.<agname>. ⚠	DFSMShsm storage adminis... ⓘ	FACILITY	<User of the Command>	READ			⊕



Validate for ID: ibmuser

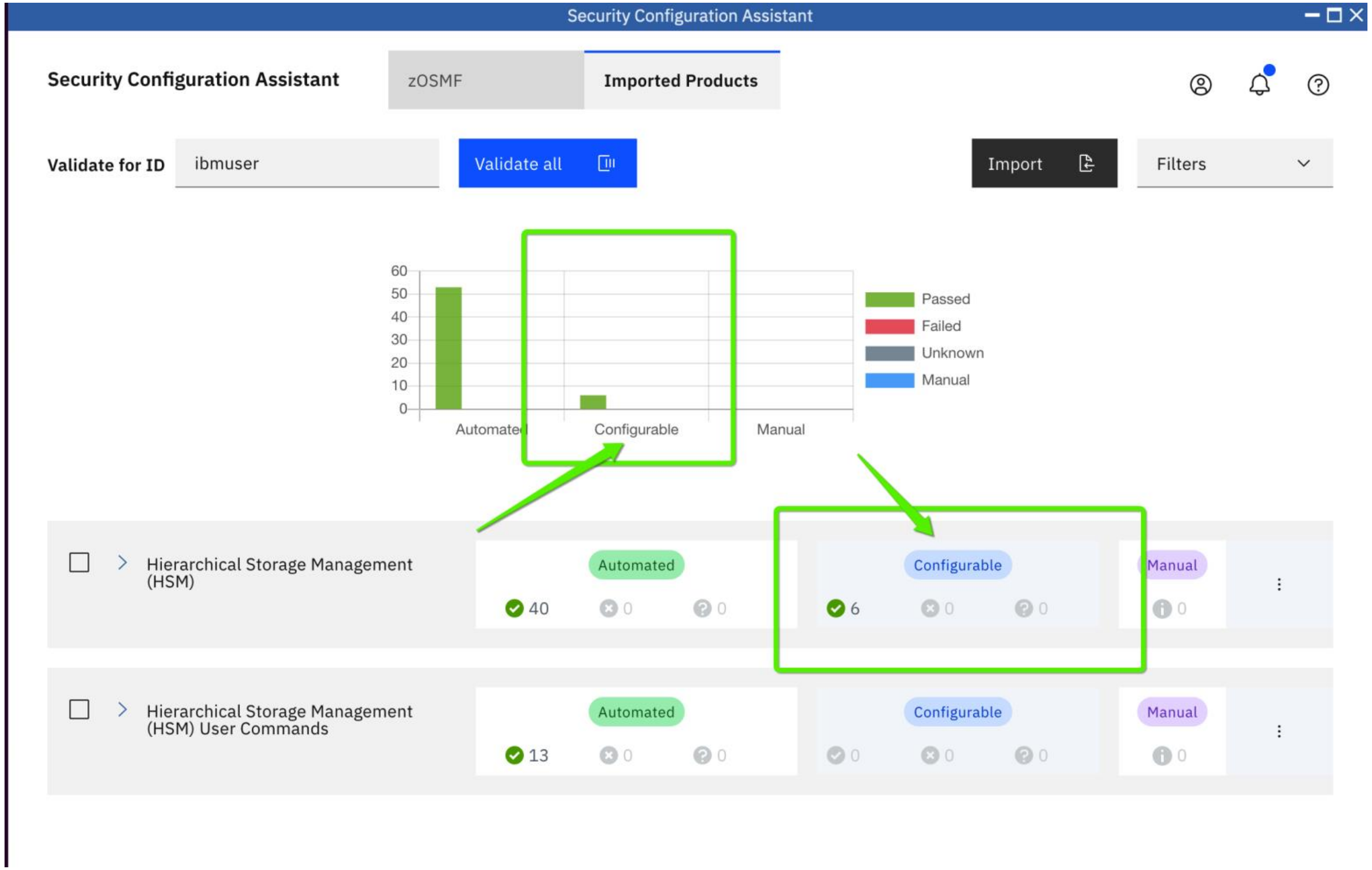
Add variable values for profile STGADMIN.ARC.ABACKUP.<agname>

Add a value for the profile variables displayed. Note that security profiles containing variables without a value cannot be validated.

agname ⓘ: SYS1

Usage & Invocation (8)

- Step 7 – When all variables are set, there should be no more "unknown" results in the "Configurable" column. The validation results should be either PASSED or FAILED.



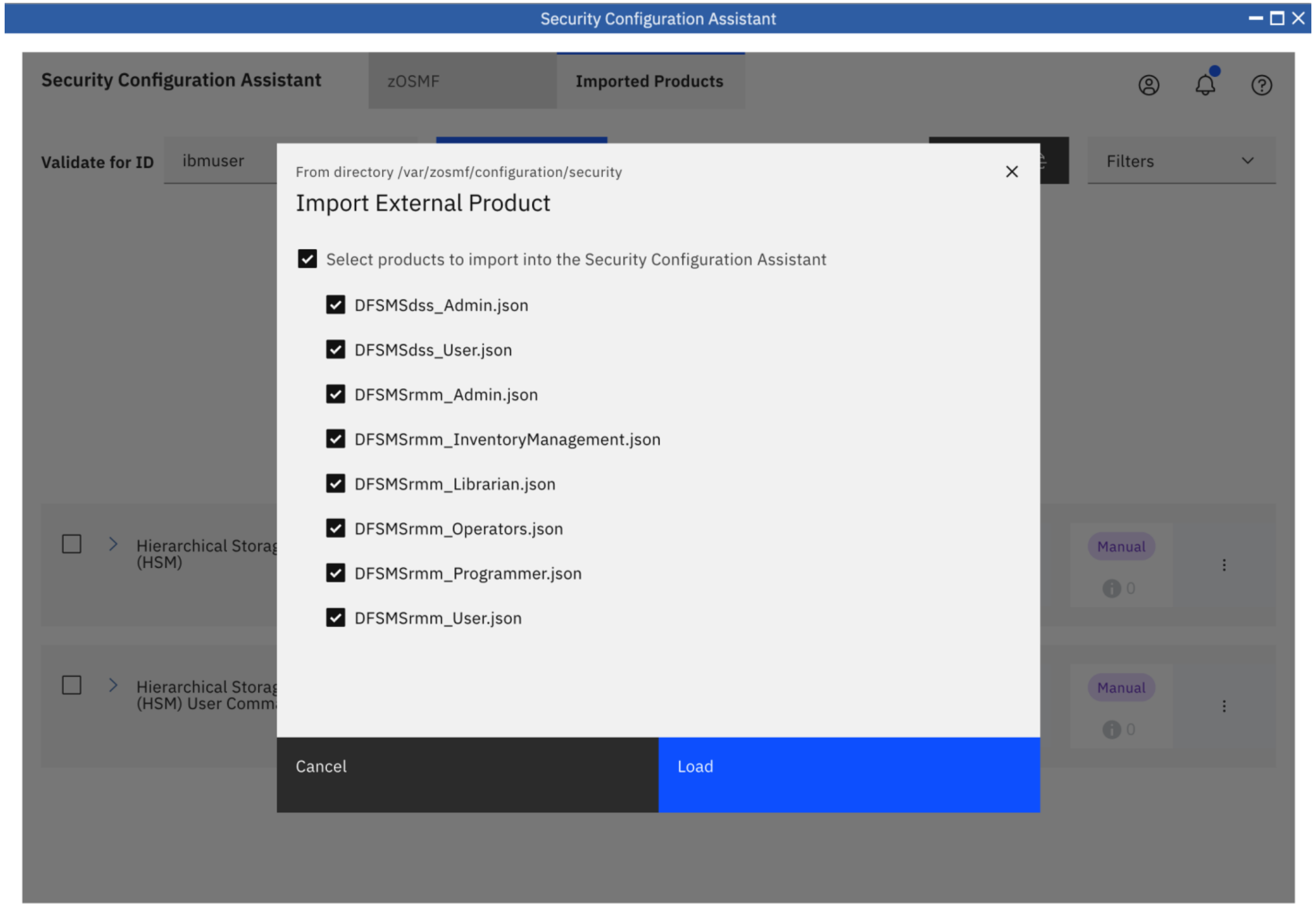
Validate for ID: ibmuser

Hierarchical Storage Management (HSM) — Automated: ✓ 40, ☒ 0, ? 0; Configurable: ✓ 6, ☒ 0, ? 0; Manual: ⓘ 0

Hierarchical Storage Management (HSM) User Commands — Automated: ✓ 13, ☒ 0, ? 0; Configurable: ✓ 0, ☒ 0, ? 0; Manual: ⓘ 0

Usage & Invocation (9)

- Step 9 – You can repeat above steps to validate security requirements on other DFSMS components.



From directory /var/zosmf/configuration/security

Import External Product

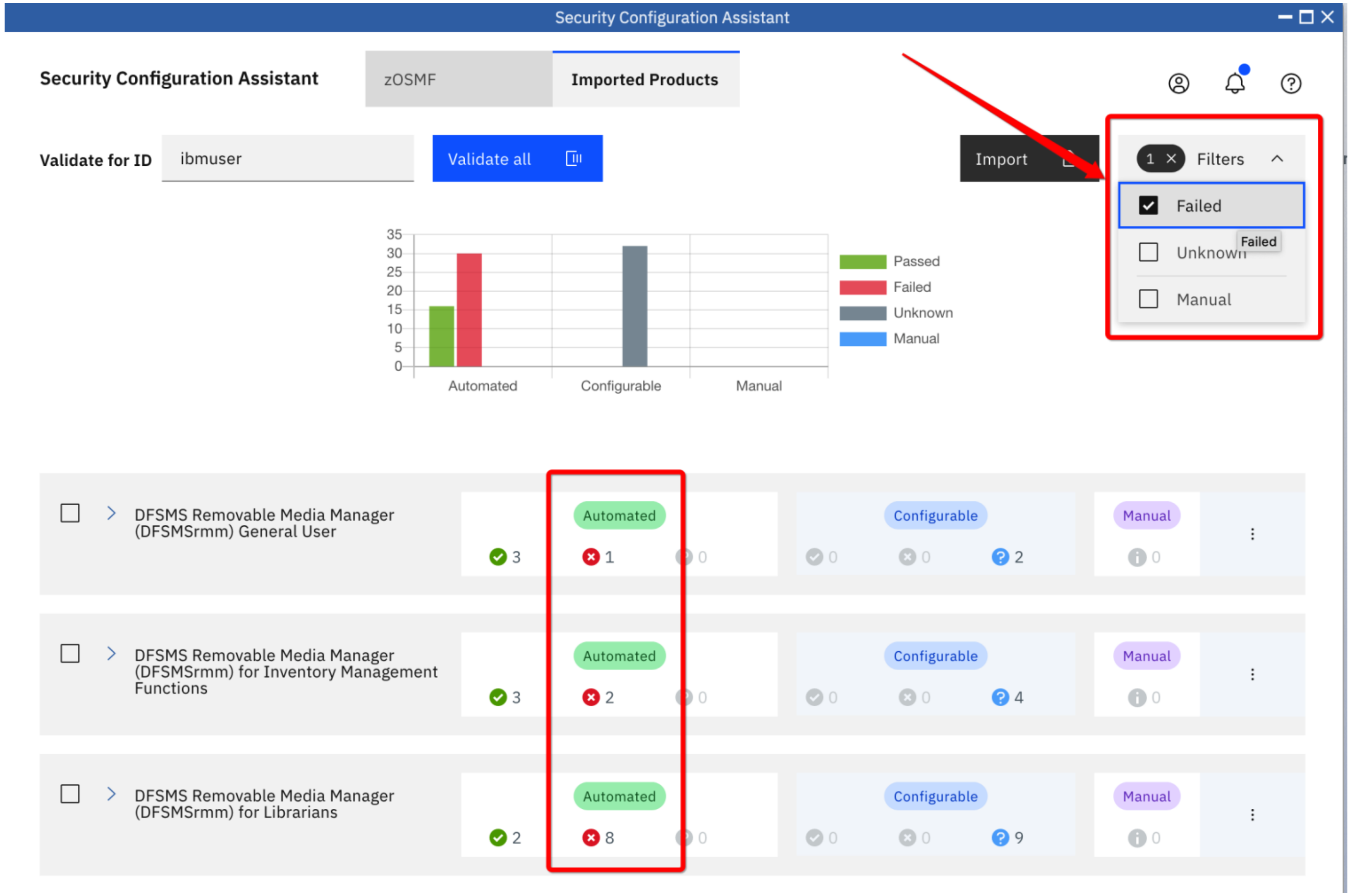
☑ Select products to import into the Security Configuration Assistant

- ☑ DFSMSdss_Admin.json
- ☑ DFSMSdss_User.json
- ☑ DFSMSrmm_Admin.json
- ☑ DFSMSrmm_InventoryManagement.json
- ☑ DFSMSrmm_Librarian.json
- ☑ DFSMSrmm_Operators.json
- ☑ DFSMSrmm_Programmer.json
- ☑ DFSMSrmm_User.json

Cancel | Load

Usage & Invocation (10)

- Step 10 – There will be more than 100 validation results once you imported all DFSMS jsons. To quick locate "Failed" or "Unknown" results, you can use the Filters on the panel.



Validate for ID: ibmuser

Filters:
☑ Failed
☐ Unknown
☐ Manual

		Automated			Configurable			Manual
☐	DFSMS Removable Media Manager (DFSMSrmm) General User	✓ 3	✖ 1	0	0	0	? 2	0
☐	DFSMS Removable Media Manager (DFSMSrmm) for Inventory Management Functions	✓ 3	✖ 2	0	0	0	? 4	0
☐	DFSMS Removable Media Manager (DFSMSrmm) for Librarians	✓ 2	✖ 8	0	0	0	? 9	0

Interactions & Dependencies

- Software Dependencies
  - N/A (SCA supports all External Security Manager products)
  - This function doesn't require other APARs to run. However, to validate security requirements for DFSMS components, you must install DFSMS support to get DFSMS security descriptor JSON files.
- Hardware Dependencies
  - N/A
- Exploiters
  - DFSMShsm
  - DFSMSrmm
  - DFSMSdss

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: {No}
- List any toleration/coexistence APARs/PTFs.
  N/A
- List anything that doesn't work the same anymore.
  When opening Security Configuration Assistant, z/OSMF won't start validating all z/OSMF resources automatically. User can click on the "Validate All" button to start the validation. This change intends to improve the startup performance of Security Configuration Assistant task.
- Upgrade involves only those actions required to make the new system behave as the old one did.
  User must check "Validate All" button manually to review z/OSMF security report.
- Coexistence applies to lower level systems which coexist (share resources) with latest z/OS systems.
  N/A

Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these:
  - Are any APARs or PTFs needed for enablement?
    No additional APARs needed on V2R5. This function will be rolled back to V2R3 and V2R4 through APAR PH29907
  - What jobs need to be run?
    If this is the first time you use z/OSMF SCA, you must run IZUSASEC firstly. This item doesn't introduce new security requirement if you have SCA enabled before.
  - What hardware configuration is required? N/A
  - What PARMLIB statements or members are needed? N/A
  - Are any other system programmer procedures required? N/A
  - Are there any planning considerations? N/A
  - Are any special web deliverables needed? N/A
  - Does installation change any system defaults? N/A

Summary

- The following z/OS V2R5 Security Configuration Assistant item has been explained:
  - Security Configuration Assistant support external product

Appendix

- To reference how to program your own security descriptor in a json file, please refer to z/OSMF Configuration Guide https://www.ibm.com/support/knowledgecenter/SSLTBW_2.4.0/com.ibm.zos.v2r4.izua300/V2R4/zosmf/izua300/izuconfig_SecurityDescriptorFile.htm