



## Hands-On Lab

# z/OSMF Security Configuration Assistant

### Abstract:

The z/OS Management Facility (z/OSMF) provides a web-based graphical interface for system programmers on z/OS. This hand on lab will give an opportunity to learn about the functions and features in z/OSMF first hand. Attendees can use a centralized UI to manage and validate security requirements by product or function.

This session will be useful to systems programmers and security administrator who needs to work with security configuration for scenarios like security validation, security trouble shooting, etc.

## Introduction to z/OSMF Security Configuration Assistant task:

When configure a z/OSMF server or enable a z/OSMF service, security setup is usually involved. The administrator might need execute a set of commands or script to figure out what security requirements they lack. This is usually time-consuming and needs much communication efforts.

The Security Configuration Assistant (SCA) task provides a centralized visual framework for examining [the security requirements of z/OSMF and other z/OS components](#). Specifically, SCA task lists the required resources and access requirements by z/OSMF services. You can also import security descriptor file (in human-readable JSON format) of other z/OS components, or import the security descriptor files you created by your own, into z/OSMF. Authorized administrator can validate those security requirements automatically. This could mitigate the repeated communication between z/OS system programmer, who configures z/OSMF or other z/OS components, and z/OS security administrator. SCA task consists of tabbed sections and tabular reports that can be expanded or collapsed, as needed. This framework provides a comprehensive perspective on your z/OS security setup.

## Key features of the z/OSMF Security Configuration Assistant (SCA) task

With the SCA task, you can:

- Review z/OSMF security requirements by Nucleus, Services and Advanced Configurations.
- Automatically validate z/OSMF security requirements on a flexible scope, regardless of what your security product is.

With Import function of SCA task, you can

- Create a JSON file (a.k.a. Security Descriptor file) to organize and describe security requirement based on your need.
- Import Security Descriptor files into SCA and review their security requirements in SCA.
- Specify runtime values to variables in security resource profile.
- Perform security validation against user id or group id for a flexible scope.
- Review validation result in graphic chart
- Filter validation results so that you can quickly narrow down to security requirements with specific type of validation result.

---

# SCA Lab

This lab consists of 10 tasks:

1. Log on to z/OSMF
2. Launch the Security Configuration Assistant task.
3. Check the result of Validation all
4. View the details of each tab
5. Check the statistics of validation
6. Filter out the failed validation
7. Validate another user
8. Validate Configurable security requirements
9. Import external Security Descriptor files
10. SCA RESTful API

It is recommended that you execute these tasks in the order listed above. As you get familiar with the SCA, you will be able to work directly with the task you need to accomplish.

## 1. Logon to z/OSMF

- Launch browser from your workstation
- Point browser to z/OSMF – enter the following URL  
<https://share.centers.ihost.com/zosmf/>
- Login with SHARE userid/pw as provided by the lab instructor
  - Each workstation has been assigned a unique z/OS user id

Note: All screen captures in the handout show the ID SHARA01, your browser will be slightly different to reflect the User ID that you were given.

IBM z/OS Management Facility

LEARN MORE NEED HELP?

## Welcome to z/OS

The highly secure, scalable and resilient enterprise operating system for the IBM z Systems mainframe.

z/OS USER ID

SHARA01

z/OS PASSWORD

.....

LOG IN

Shopz  
IBM Support

z Systems Redbooks  
z/OSMF home Page

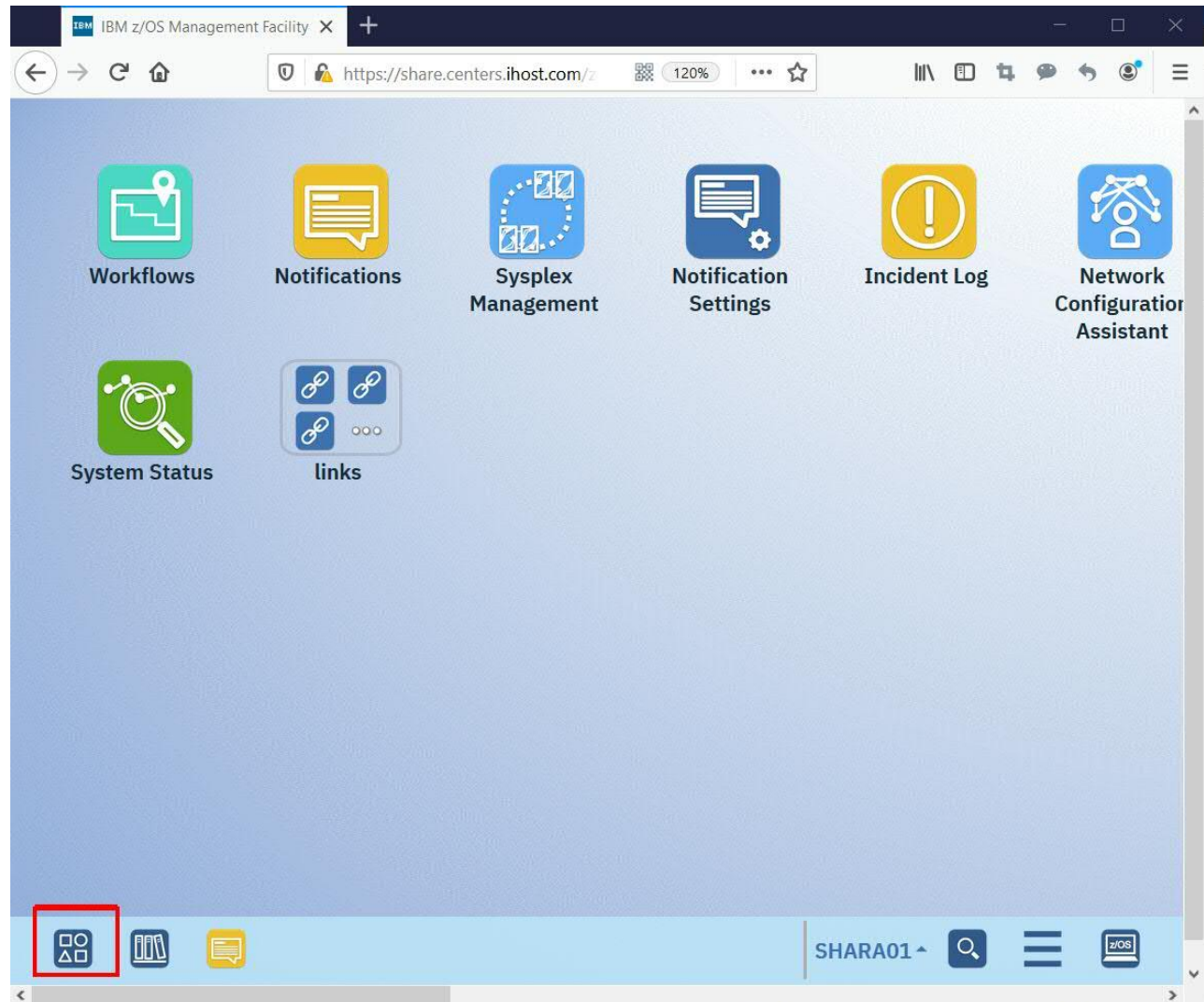
WCS Flashes and Techdocs  
z/OS home Page

z/OS Knowledge Center

## 2. Launch the Security Configuration Assistant task.

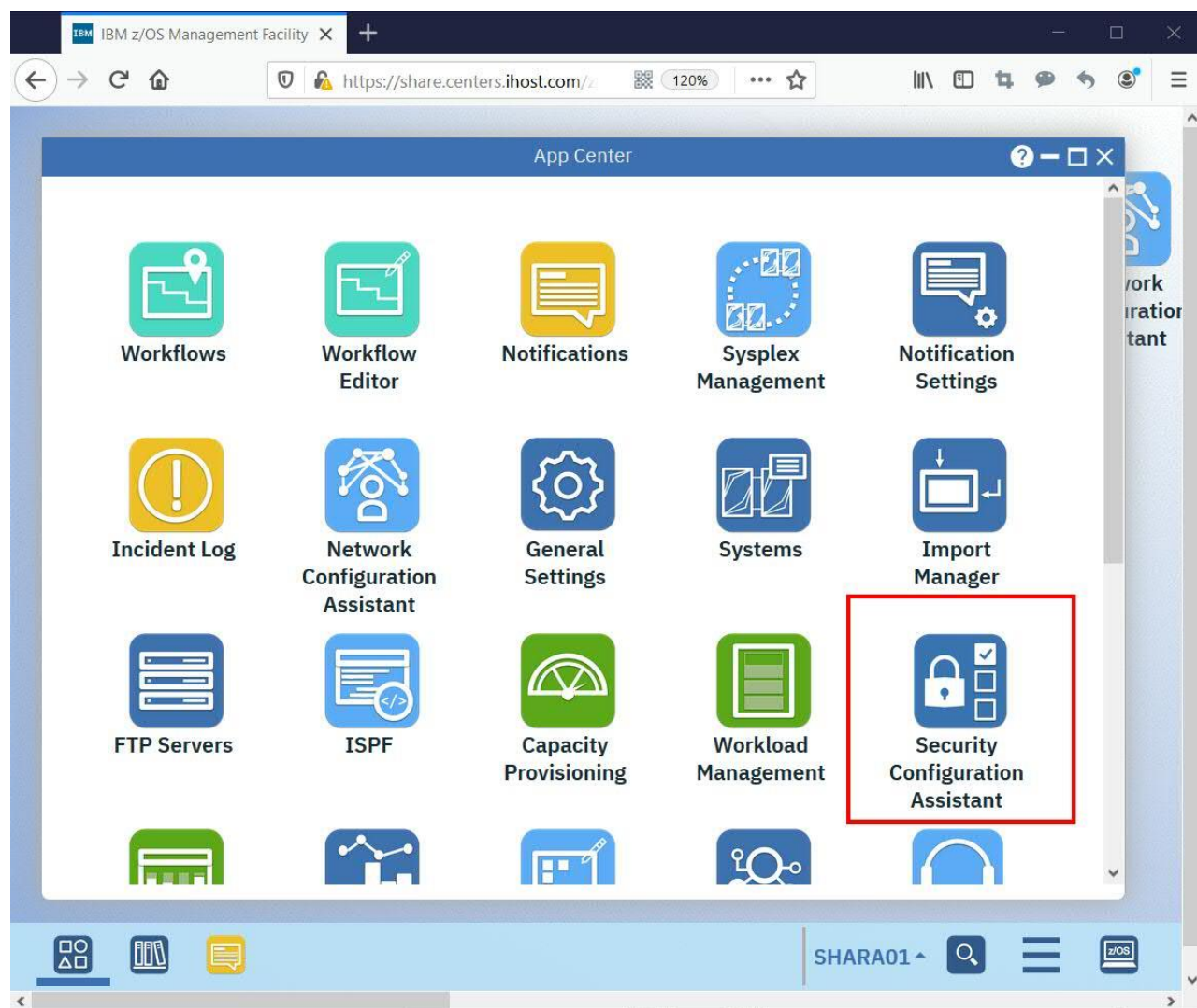
Step 2a: Open z/OSMF App Center

Click on the icon of App Center on the bottom left of z/OSMF desktop



Step 2b: Open Security Configuration Assistant task

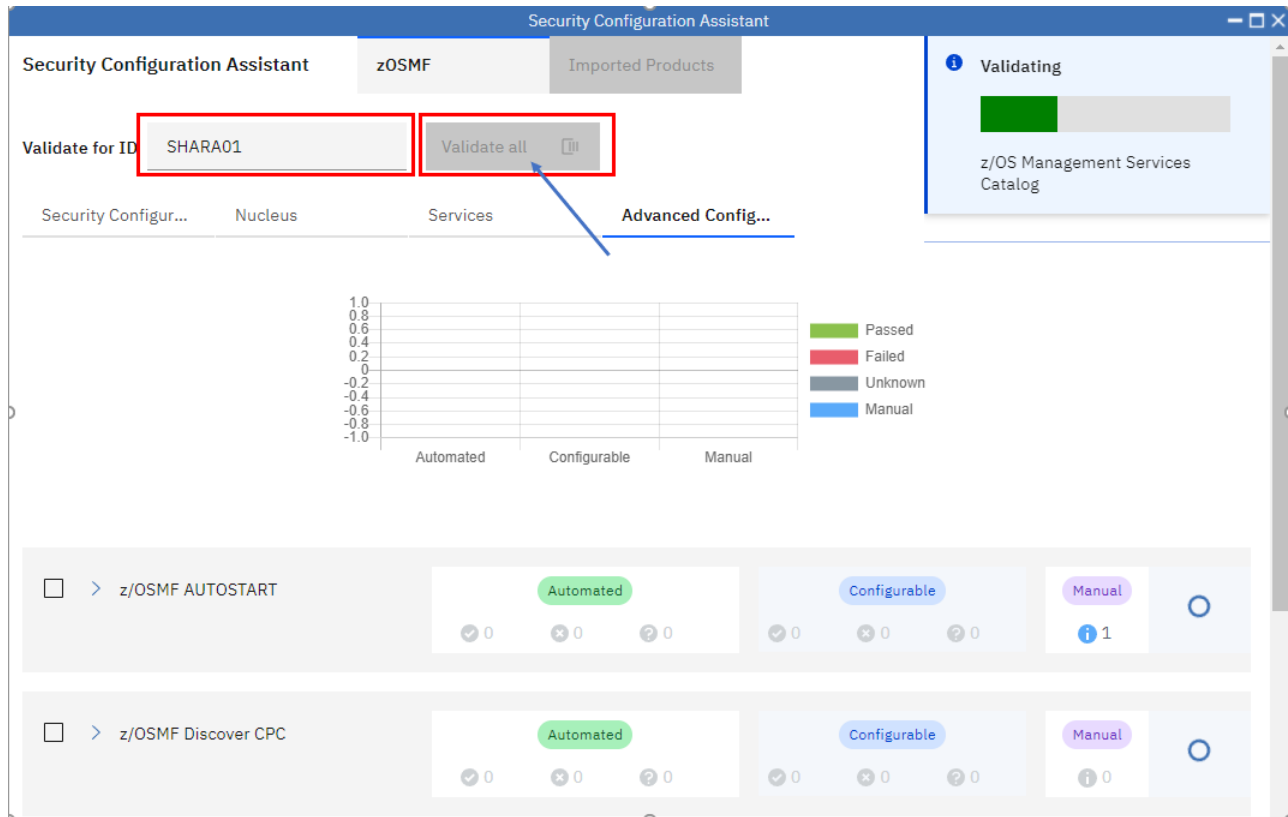
Double click on the icon of “Security Configuration Assistant”. You can enter character S to quickly locate the icon of “Security Configuration Assistant”.



### 3. Check the result of Validation all.

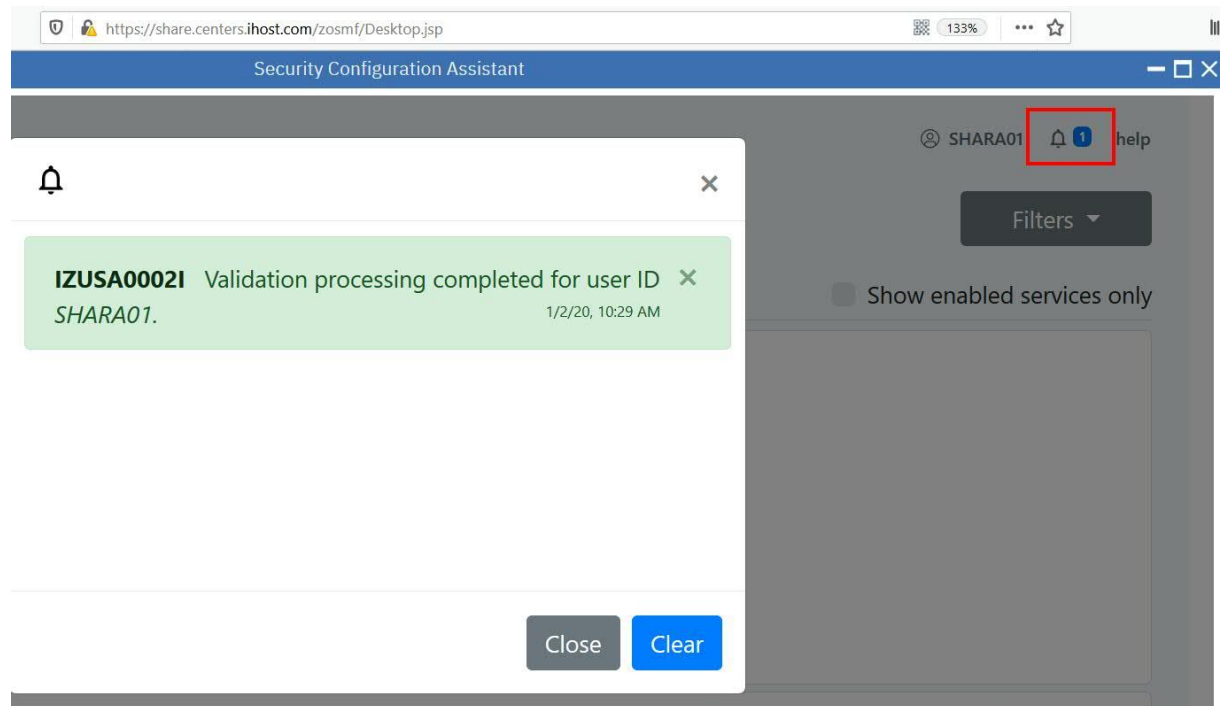
#### Step 3a: Validate all security requirements managed by SCA

Click **Validate all**, you may wait for a few seconds for the validation process to be completed.



### Step 3b: Check the message of SCA Task

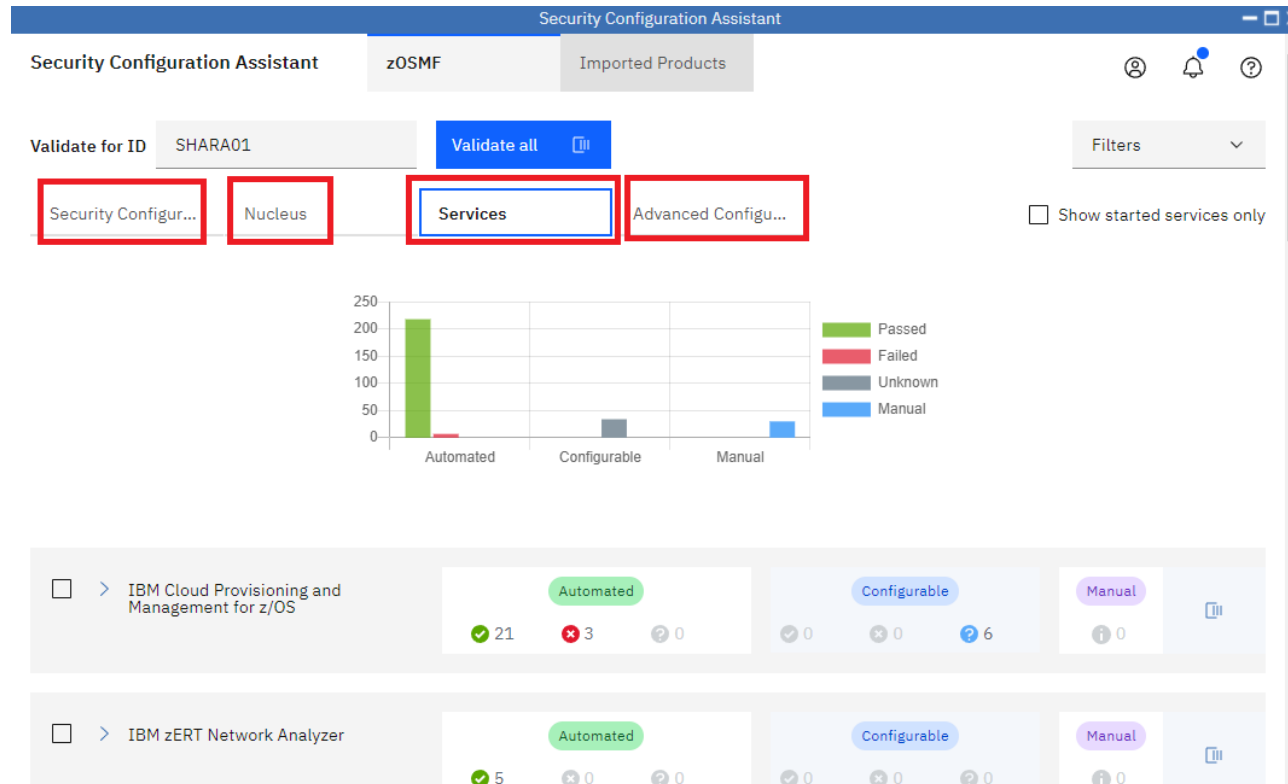
When the **Validation all** is completed, messages will be popped up to indicate the validation status. You can also check the messages by clicking on the bell icon on the top right.





### Step 3c: Check different tabs of SCA task

You can see there are 4 tabs for security requirements of z/OSMF itself in SCA task. Each tab contains security requirements and result for different group of z/OSMF functions.



## 4. View the details of each tab

Now let's check out details in each tab.

### Step 4a: Check the tab of Security Configuration Assistant

Extend the category of “z/OSMF Security Configuration Assistant”. The list in this tab includes all security requirements that are required to run the SCA task itself. If those security requirements are not satisfied, the later validations done by SCA task automatically may show the ‘Unknown’ status. Each line in the table indicates one specific security requirement which include:

- SAF resource name and explains why the authorization is needed.
- SAF resource class, Who needs access, access level
- User ID of the currently validated user.
- Validation result, which indicate if the authorities has been granted
- Action. If the corresponding security setup is changed later, you can rerun the validation for specific item to verify if the change was successful. To do so, click the refresh icon in this **Action** column. The Security Configuration Assistant task runs validation again to determine whether the user has the required level of access to the selected resource name

Security Configuration Assistant

Validate for user ID: SHARA01 [Validate all]

Security Configuration Assistant Nucleus Services 23 Advanced Configuration 24

z/OSMF Security Configuration Assistant

Automated Checks: Passed 18, Failed 0, Unknown 0

Resources for z/OSMF Security Configuration Assistant	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
BBG.SECC.LASS.SERVER	Allow the user to verify resources in the SERVER class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.APPL	Allow the user to verify resources in the APPL class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.FACILITY	Allow the user to verify resources in the FACILITY class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.EJBROLE	Allow the user to verify resources in the EJBROLE class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.SERVAUTH	Allow the user to verify resources in the SERVAUTH class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.STARTED	Allow the user to verify resources in the STARTED class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.ZMFCLD	Allow the user to verify resources in the ZMFCLD class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.ACCTNUM	Allow the user to verify resources in the ACCTNUM class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.TSOPROC	Allow the user to verify resources in the TSOPROC class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.TSOAUTH	Allow the user to verify resources in the TSOAUTH class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.OPERCMDS	Allow the user to verify resources in the OPERCMDS class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.CSFSESV	Allow the user to verify resources in the CSFSESV class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.JESSPOOL	Allow the user to verify resources in the JESSPOOL class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.LOGSTRM	Allow the user to verify resources in the LOGSTRM class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.UNDXPRIV	Allow the user to verify resources in the UNDXPRIV class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
BBG.SECC.LASS.RDATALIB	Allow the user to verify resources in the RDATALIB class.	SERVER	IZUSVR	READ	IZUSVR	Passed	Refresh
IZUDFLT.ZOSMF.CONFIGURATION.SECURITY_ASSISTANT	Allow the user to access to Security Configuration Assistant.	ZMFAPLA	IZUADMIN	READ	SHARA01	Passed	Refresh
IZUDFLT.IzuManagementFacilitySecurityConfigurationAssistant.IzuUsers	Allow the user to connect to the Security Configuration Assistant task.	EJBROLE	<User of the Service>	READ	SHARA01	Passed	Refresh

## Step 4b: Check the tab of Nucleus

Extend the category of “z/OSMF Nucleus” and scroll down a little bit. The items in this tab includes all security requirement required for z/OSMF nucleus.

Security Configuration Assistant

Validate for user ID: SHARA01 [Validate all](#)

Security Configuration Assistant | **Nucleus** | Services 23 | Advanced Configuration 24

☐ z/OSMF Nucleus

Automated: 19 Passed, 0 Failed, 0 Unknown | Manual: 6

Resources for z/OSMF Liberty Server	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
BBG.ANGEL.IZUANG1	Allow the z/OSMF server to access the angel process.	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.AUTHMOD.BBGZSAFM	Enable the z/OSMF server to use the z/OS Authorized services.	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.AUTHMOD.BBGZSAFM.SAFCRED	To enable the SAF authorized user registry services and SAF authorization services(SAFCRED).	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.AUTHMOD.BBGZSAFM.ZOSWLM	To enable the WLM services(ZOSWLM).	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.AUTHMOD.BBGZSAFM.TXRRS	To enable the RRS transaction services(TXRRS).	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.AUTHMOD.BBGZSAFM.ZOSDUMP	To enable the SVC DUMP services(ZOSDUMP).	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.SECFPX.IZUOFLT	Allow the z/OSMF server to make authentication calls against the APPL-ID.	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.SECCLASS.ZMFAPLA	Allow the z/OSMF server to authorize checks for the ZMFAPLA class.	SERVER	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BBG.SYNC.IZUOFLT	Allow the z/OSMF server to authorize checks for the ZMFACLOUD class.	FACILITY	IZUSVR	CONTROL	IZUSVR	Passed	<a href="#">Refresh</a>
BPX.WLMSEVER	Allows the z/OSMF server to use WLM functions to create and manage work requests.	FACILITY	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
BPX.CONSOLE	Allow the user to filter z/OS UNIX messages. Specifically, this setting suppresses the BPXM023I message prefix from any write-to-operator (WTO) messages that z/OSMF writes to the console.	FACILITY	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>
IZUOFLT	Allow access to the z/OSMF application domain. If there is no matching profile in the APPL class, RACF allows the user to access the application.	APPL	IZUGUEST	READ	IZUGUEST	Passed	<a href="#">Refresh</a>

Resources for Keyring and Certificate	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
JRR.DIGTCERT.LISTRING	Allow the started task user ID to list and get the certificate kevrnt.	FACILITY	IZUSVR	READ	IZUSVR	Passed	<a href="#">Refresh</a>

## Step 4c: Check the tab of Services

This tab includes security requirements for all z/OSMF services. They are grouped by service. You can extend each category to see the details of each z/OSMF service.

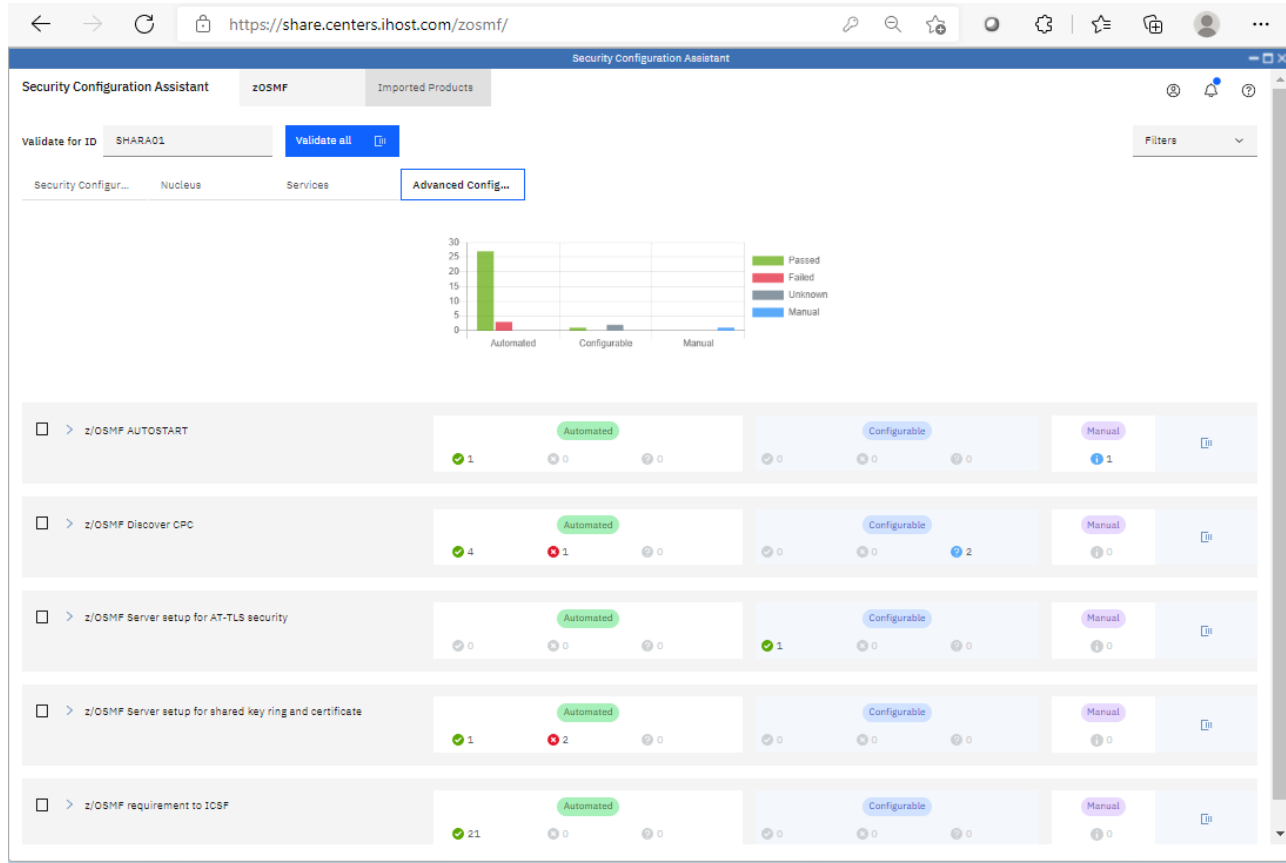
Administrator can leverage this tab to check if the security requirements of a specific z/OSMF service are satisfied or not.

The screenshot displays the 'Security Configuration Assistant' interface within the IBM z/OS Management Facility. The 'Services' tab is active, showing a list of services and their associated security checks. The interface includes a search bar, a 'Validate all' button, and a 'Filters' dropdown. The services are listed in a table with columns for 'Passed', 'Automated Checks', 'Unknown', and 'Manual Checks'. Each row represents a service category, and the counts indicate the status of the security checks.

Service	Passed	Automated Checks	Unknown	Manual Checks
> z/OSMF Sysplex Management	28	1	0	10
> z/OSMF Settings	3	0	0	0
> z/OSMF Notifications	4	0	0	0
> z/OSMF Support Swagger Document	0	2	0	0
> Network Configuration Assistant	6	2	0	7
> z/OSMF Administration	5	1	0	0
> TSO/E Address Space Services	2	0	0	3
> z/OS Jobs REST Interface	1	0	0	2
> z/OS Operator Consoles	15	0	0	7
> IBM Cloud Provisioning and Management for z/OS	15	9	0	6

## Step 4d: Check the tab of Advanced Configuration

The items in this tab include security requirements for z/OSMF advanced configurations.



## 5. Check the statistics of validation

Now let's continuously focus on "Advanced Configuration" tab and check out the statistics of validation result.

### Step 5a: Count the number of "Passed" and "Failed"

Extend "z/OSMF Discover CPC" category and count the number of "Passed" and "Failed".

Security Configuration Assistant   Nucleus   Services **23**   Advanced Configuration **24**

☐ **z/OSMF Discover CPC**   Automated Checks: Passed 4, Failed 1, Unknown 0   Manual Checks: 2

Automated   Manual

Resources for Discover CPC service	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
HWI.APPLNAME.HWISERV	Allows the administrator groups access to the BCPII services.	FACILITY	IZUADMIN	READ	SHARA01	Failed	

Resources for z/OS data set and file REST interface	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
CEA.CEATSO.TSOREQUEST	Allows CEA to invoke a TSO session.	SERVAUTH	IZUUSER IZUADMIN IZUSVR	READ	SHARA01	Passed	
IZUACCT	Allows access to the Account Number resource profile.	ACCTNUM	IZUUSER IZUADMIN	READ	SHARA01	Passed	
IZUFPROC	Allows access to the TSO Procedure resource profile.	TSOPROC	IZUUSER IZUADMIN	READ	SHARA01	Passed	
IZUDFLT.IzuManagementFacilityRestFiles.izuUsers	Allows access to z/OS data set and file REST interface	EJBROLE	<User of the Services>	READ	SHARA01	Passed	

## Step 5b: Review the summarized numbers for a category

There is a summary area for each category in the same row of the category name. It shows the summarized numbers of validation result for the specific category. It should be consistent with the number you counted in step 5a.

The Manual Checks indicates how many security requirements can not be automatically validated and require user's manual check. You can click on the sub tab of "Manual" to see the details

The screenshot shows the Security Configuration Assistant interface. At the top, there are tabs for "Security Configuration Assistant", "Nucleus", "Services 23", and "Advanced Configuration 24". Below these, there is a section for "z/OSMF Discover CPC". This section has a summary bar with "Automated Checks" (Passed: 4, Failed: 1, Unknown: 0) and "Manual Checks" (2). Below the summary bar, there are two tabs: "Automated" and "Manual". The "Automated" tab is selected, showing a table of resources for the Discover CPC service. The table has columns: Resources for Discover CPC service, Description, Class, Who needs the access, Required Access, Validated User ID, Validation Result, and Action. The first row shows a resource "HWI.APPLNAME.HWISERV" with a "Failed" validation result. Below this, there is a section for "Resources for z/OS data set and file REST interface" with a table of resources. The table has columns: Resources for z/OS data set and file REST interface, Description, Class, Who needs the access, Required Access, Validated User ID, Validation Result, and Action. The resources listed are "CEA.CEATSO.TSOREQUEST", "IZUACCT", "IZUFPROC", and "IZUDFLT.IzuManagementFacilityRestFiles.IzuUsers". All of these resources have a "Passed" validation result.

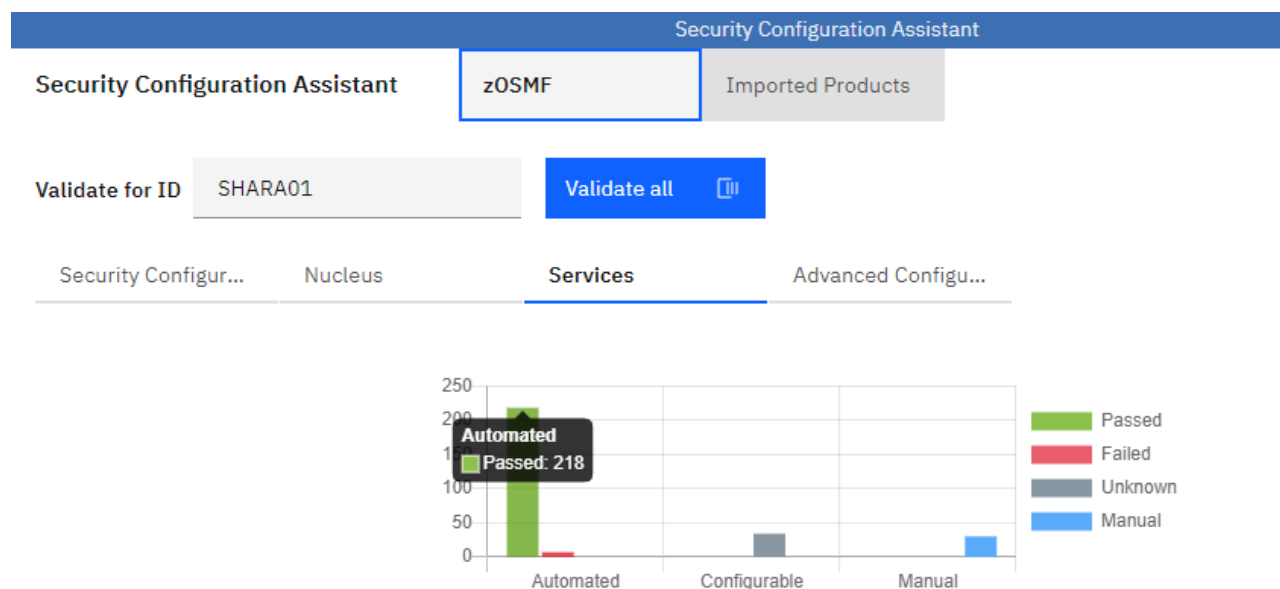
Resources for Discover CPC service	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
HWI.APPLNAME.HWISERV	Allows the administrator groups access to the BCPII services.	FACILITY	IZUADMIN	READ	SHARA01	Failed	<a href="#">Refresh</a>

Resources for z/OS data set and file REST interface	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
CEA.CEATSO.TSOREQUEST	Allows CEA to invoke a TSO session.	SERVAUTH	IZUUSER IZUADMIN IZUSVR	READ	SHARA01	Passed	<a href="#">Refresh</a>
IZUACCT	Allows access to the Account Number resource profile.	ACCTNUM	IZUUSER IZUADMIN	READ	SHARA01	Passed	<a href="#">Refresh</a>
IZUFPROC	Allows access to the TSO Procedure resource profile.	TSOPROC	IZUUSER IZUADMIN	READ	SHARA01	Passed	<a href="#">Refresh</a>
IZUDFLT.IzuManagementFacilityRestFiles.IzuUsers	Allows access to z/OS data set and file REST interface.	EJBROLE	<User of the Service>	READ	SHARA01	Passed	<a href="#">Refresh</a>

## Step 5c: Check the overall summary via chart

On the top of each tab, there is a chart summarizes the validation result for the specific tab.



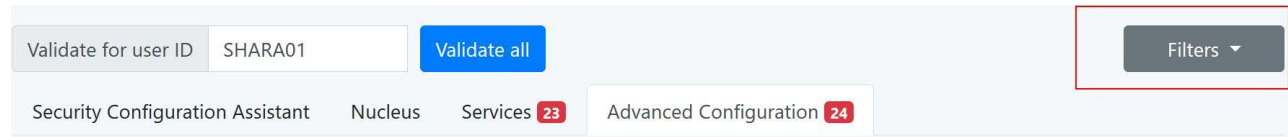


---

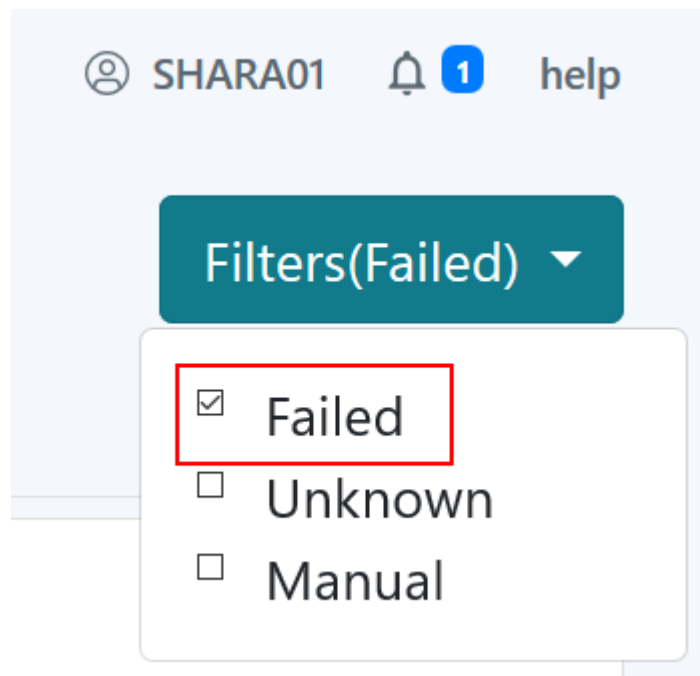
## 6. Filter out the failed validation

Sometimes, you may only care about the failed validations, the Filter function can help you with that.

Click on the button 'Filters' on the top right corner.



Then select 'Failed' option



Then extend some categories and only failed validations are displayed so that you can quickly find out what security requirements have not been satisfied.

Unselect the 'Failed' check box in the Filter drop down menu so that we can continue with next step.

## 7. Validate another user

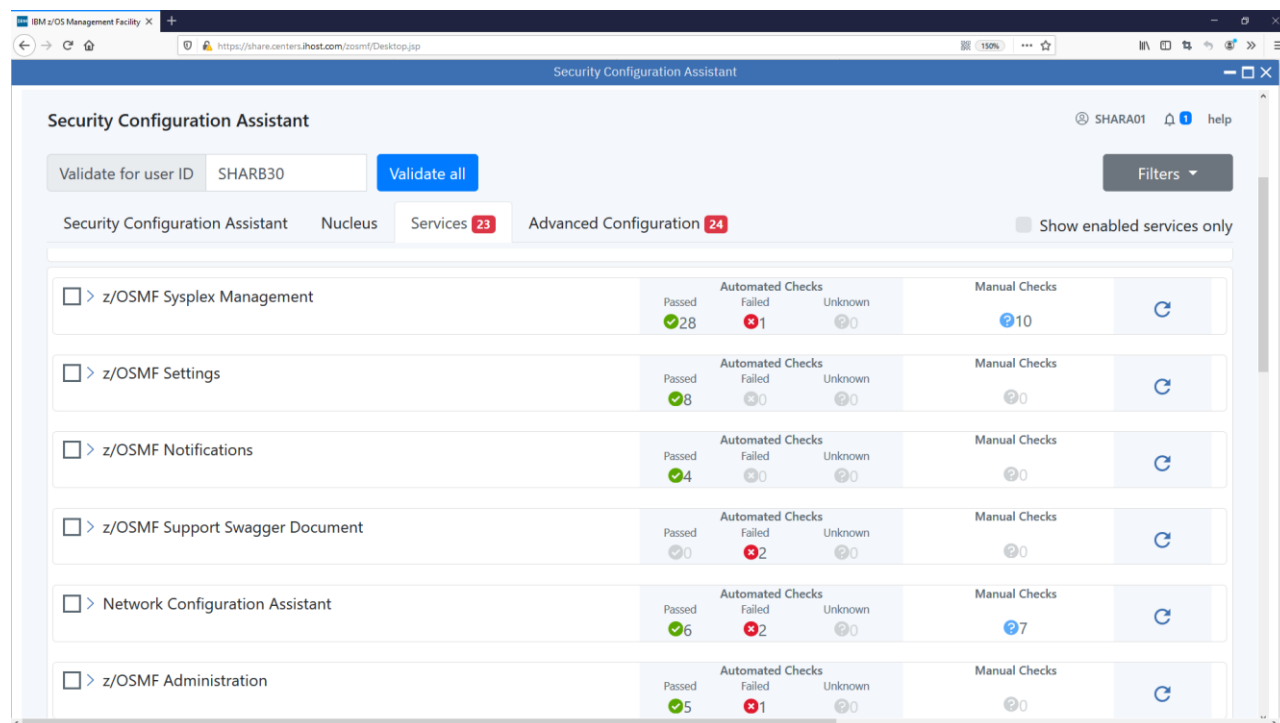
As an authorized administrator, you can validate z/OSMF security requirements for specified user id or group id.

### Step 7a: Specify a different user to be validated

Specify the user id in the input box on the top



Then click on the “Services” tab to list all the services and plugins. Here we will use the tab of Services for hands-on,



## Step 7b: Validate a specific security requirement for the specified user

Extend z/OSMF Sysplex Management category, click on the refresh button in the first row. The validation will be started to check if “SHARB30” has the “READ” access to z/OSMF Sysplex Management service which is protected by SAF profile IZUDFLT.ZOSMF.SYSPLEX.

The screenshot shows the 'Security Configuration Assistant' interface. At the top, there is a search bar with 'Validate for user ID' set to 'SHARB30' and a 'Validate all' button. Below this, there are tabs for 'Security Configuration Assistant', 'Nucleus', 'Services' (with a red '23' badge), and 'Advanced Configuration' (with a red '24' badge). A 'Filters' dropdown is on the right. The main content area shows a tree view with 'z/OSMF Sysplex Management' expanded. It displays a summary of checks: Automated Checks (Passed: 28, Failed: 1, Unknown: 0) and Manual Checks (10). Below this is a table with columns: Resources for z/OSMF Sysplex Management service, Description, Class, Who needs the access, Required Access, Validated User ID, Validation Result, and Action. The table has two rows. The first row is highlighted, and its 'Action' column contains a refresh icon, which is highlighted with a red box. The second row also has a refresh icon.

Resources for z/OSMF Sysplex Management service	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUDFLT.ZOSMF.SYSPLEX	Allows the user to view sysplex resources.	ZMFAPLA	IZUUSER IZUADMIN	READ	SHARA01	Passed	
IZUDFLT.ZOSMF.SYSPLEX.MODIFY	Allows the user to modify sysplex resources.	ZMFAPLA	IZUADMIN	READ	SHARA01	Passed	

When the validation is completed, a message will be popped up to display the result of validation. The user id “SHARB30” is also displayed in the column of “Validated User ID”. Another column right after it shows the status of “Passed” which means the validation is successful.

The screenshot shows the 'Security Configuration Assistant' interface after validation. A green message box is displayed, stating: 'IZUSA0014I Validation processing completed for user ID SHARB30 for resource IZUDFLT.ZOSMF.SYSPLEX.' Below the message box, the 'Validate for user ID' field now shows 'SHARB30'. The table below has the same structure as the previous screenshot, but the 'Validated User ID' for the first row is now 'SHARB30' and the 'Validation Result' is 'Passed', both highlighted with red boxes. The 'Action' column still contains the refresh icon.

Resources for z/OSMF Sysplex Management service	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUDFLT.ZOSMF.SYSPLEX	Allows the user to view sysplex resources.	ZMFAPLA	IZUUSER IZUADMIN	READ	SHARB30	Passed	
IZUDFLT.ZOSMF.SYSPLEX.MODIFY	Allows the user to modify sysplex resources.	ZMFAPLA	IZUADMIN	READ	SHARA01	Passed	

## Step 7c: Run validation for a specific z/OSMF service

Click on the refresh icon on the same row with the category title “z/OSMF Sysplex Management”. This triggers an validation for all the security requirements required by the service “z/OSMF Sysplex Management”.

Security Configuration Assistant SHARA01 help

Validate for user ID SHARB30 Validate all Filters

Security Configuration Assistant Nucleus Services 21 Advanced Configuration 24 Show enabled services only

☐ **z/OSMF Sysplex Management** Passed 28 Automated Checks Failed 1 Unknown 0 Manual Checks 10 Refresh

Automated Manual

Resources for z/OSMF Sysplex Management service	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUDFLT.ZOSMF.SYSplex	Allows the user to view sysplex resources.	ZMFAPLA	IZUUSER IZUADMIN	READ	SHARB30	Passed	Refresh
IZUDFLT.ZOSMF.SYSplex.MODIFY	Allows the user to modify sysplex resources.	ZMFAPLA	IZUADMIN	READ	SHARA01	Passed	Refresh
IZUDFLT.ZOSMF.SYSplex.LOG	Allows the user to clean up the sysplex command log table and edit the clean-up settings.	ZMFAPLA	<User of the Service>	READ	SHARA01	Passed	Refresh
CEA.XCF.CF	Allows the user to access CEA for the Sysplex CF resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARA01	Passed	Refresh
CEA.XCF.CDS	Allows the user to access CEA for the Sysplex CDS resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARA01	Passed	Refresh
CEA.XCF.SYSplex	Allows the user to access CEA for the Sysplex system resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARA01	Passed	Refresh
CEA.XCF.STRUCTURE	Allows the user to access CEA for the Sysplex structure resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARA01	Passed	Refresh
IZUDFLT.IzuManagementFacilitySysplexManagement.IzuUsers	Allows the user to start z/OSMF Sysplex Management service.	EJBROLE	<User of the Service>	READ	SHARA01	Passed	Refresh

When the validation is completed, a message pops up and displays the result of validation. This operation is usually used to verify if a user can access a specific z/OSMF service. Depends on the different user you specified on the top, the validation result may vary.

Security Configuration Assistant IZUSAD00151 Validation processing completed for the z/OSMF service z/OSMF Sysplex Management.

Validate for user ID SHARB30 Validate all Show enabled services only

Security Configuration Assistant Nucleus Services 27 Advanced Configuration 24

☐ **z/OSMF Sysplex Management** Passed 24 Automated Checks Failed 5 Unknown 0 Manual Checks 10 Refresh

Automated Manual

Resources for z/OSMF Sysplex Management service	Description	Class	Who needs the access	Required Access	Validated User ID	Validation Result	Action
IZUDFLT.ZOSMF.SYSplex	Allows the user to view sysplex resources.	ZMFAPLA	IZUUSER IZUADMIN	READ	SHARB30	Passed	Refresh
IZUDFLT.ZOSMF.SYSplex.MODIFY	Allows the user to modify sysplex resources.	ZMFAPLA	IZUADMIN	READ	SHARB30	Passed	Refresh
IZUDFLT.ZOSMF.SYSplex.LOG	Allows the user to clean up the sysplex command log table and edit the clean-up settings.	ZMFAPLA	<User of the Service>	READ	SHARB30	Passed	Refresh
CEA.XCF.CF	Allows the user to access CEA for the Sysplex CF resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARB30	Passed	Refresh
CEA.XCF.CDS	Allows the user to access CEA for the Sysplex CDS resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARB30	Passed	Refresh
CEA.XCF.SYSplex	Allows the user to access CEA for the Sysplex system resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARB30	Passed	Refresh
CEA.XCF.STRUCTURE	Allows the user to access CEA for the Sysplex structure resource.	SERVAUTH	IZUUSER IZUADMIN	READ	SHARB30	Passed	Refresh
IZUDFLT.IzuManagementFacilitySysplexManagement.IzuUsers	Allows the user to start z/OSMF Sysplex Management service.	EJBROLE	<User of the Service>	READ	SHARB30	Passed	Refresh

## 8. Validate Configurable security requirements

Each component may have the **Configurable** items, in this tab, security resource name contains variables.

Extend “Network Configuration Assistant”, then click on “Configurable” tab. Click the + icon in **Action** column to add variable value for configurable requirements.




Validate for ID: SHARA01 Validate all Filters

Security Configur... Nucleus **Services** Advanced Configu... ☐ Show started services only

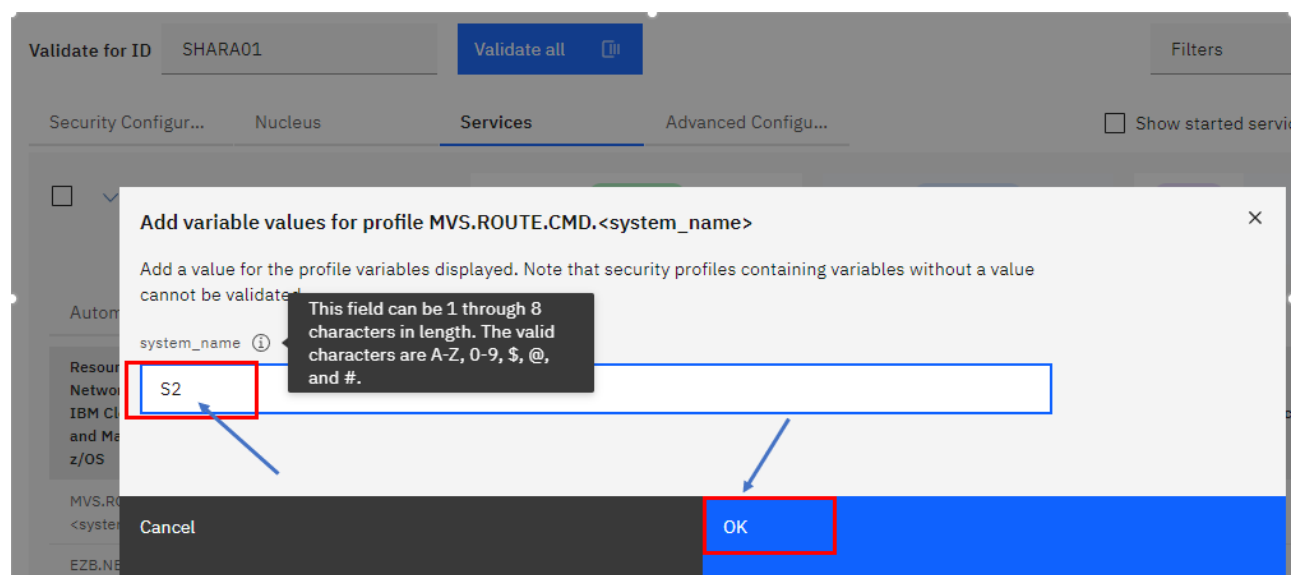
☐ Network Configuration Assistant

Automated **Configurable** Manual

Automated: 7 (green), 1 (red), 0 (grey) | Configurable: 0 (green), 0 (red), 3 (blue) | Manual: 4 (blue)

Resources for Networking support for IBM Cloud Provisioning and Management for z/OS	Description	Class	Who needs the access	Required Access	Validated ID	Validation Result	Action
MVS.ROUTE.CMD.<system_name>	Allows the Network Confi...	OPERCMD5	IZUSVR	READ			
EZB.NETSTAT.<system_name>.<tcp_procedure_name>.CONFIG	Allows the Network Confi...	SERVAUTH	IZUSVR	READ			
EZB.NETSTAT.<system_name>.<tcp_procedure_name>.VIPADCFG	Allows the Network Confi...	SERVAUTH	IZUSVR	READ			

Input value **S2** for the variable name <system\_name>, and click **OK**.

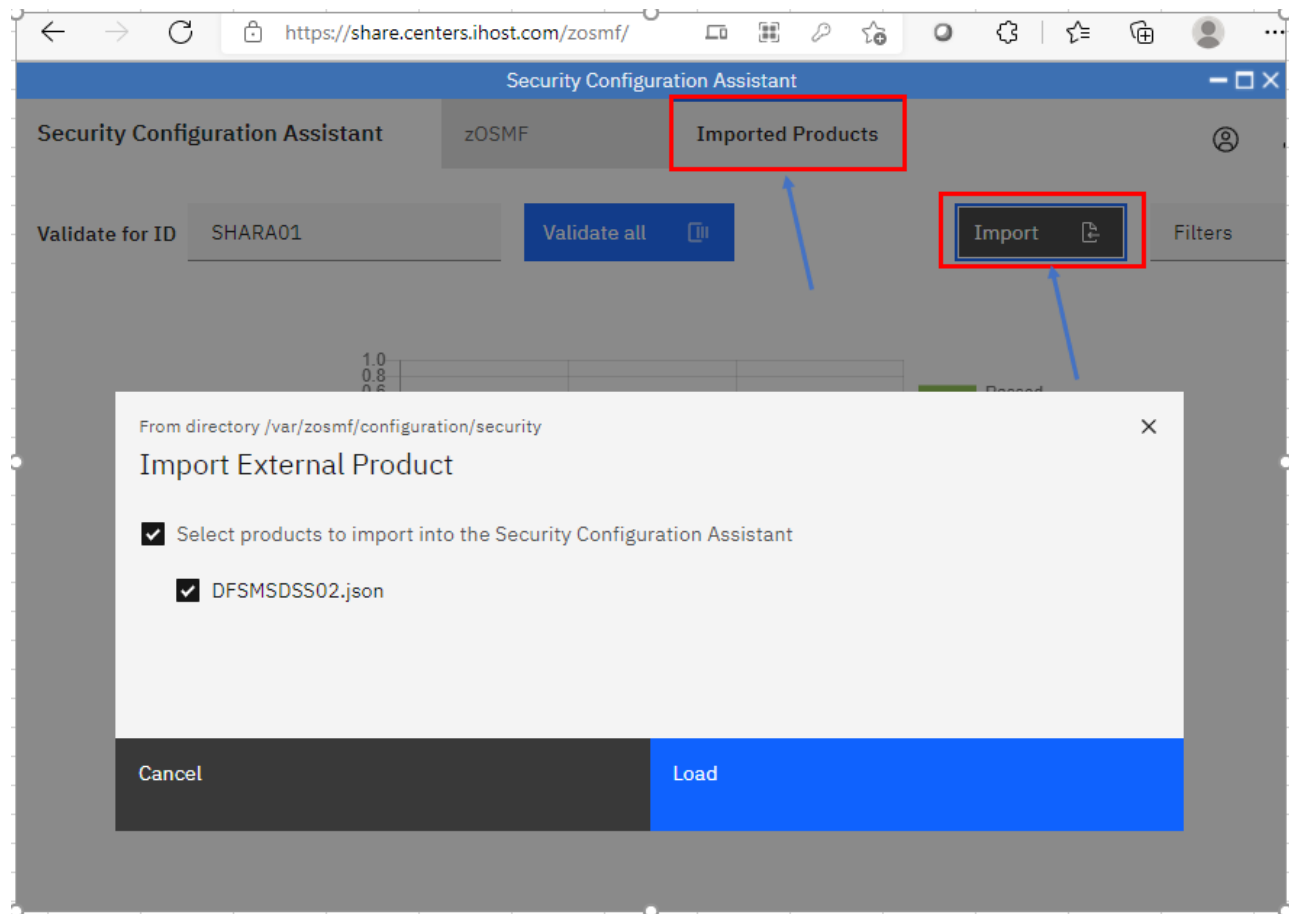


The added resource will be validated automatically.

## 9. Import external security descriptor file

SCA can support other external products. Once you have a security descriptor file, upload it to <z/OSMF data directory>/configuration/security directory. Then SCA will be able to discover it and allows administrator to import it to SCA.

To import a Security Descriptor file, click **Imported Products** tab, and then click **Import** button. All Security Descriptor files under <z/OSMF data directory>/configuration/security directory will be listed. For this lab, we won't do the real "Load" action, please just click on the "Cancel" button to cancel the Import action. In fact, once the Security Descriptor file is imported into SCA, the functions you explored above for z/OSMF security requirements also work for security requirements described in the Security Descriptor file.



## 10. SCA RESTful API

This step does not require your actions. It's only for your awareness.

With APAR PH41248, SCA now exposes its capability of automatic security validation via REST API. Since REST API is easy to be consumed by many programming languages either locally or remotely, it's now easy to consume SCA capability without having to open SCA UI.

Here is an example of SCA REST API which specifies the security requirements directly in REST API request body:

Request:

```
Post
'https://share.centers.ihost.com/zosmf/config/security/v1/validate?userid=ibm
user'

{
  "resourceItems": [
    {
      "resourceProfile": "IZUDFLT.ZOSMF.CONFIGURATION.SECURITY_ASSISTANT",
      "resourceClass": "ZMFAPLA",
      "access": "READ"
    }
  ]
}
```

Response:

```
{
  "resourceItems": [
    {
      "resourceProfile": "IZUDFLT.ZOSMF.CONFIGURATION.SECURITY_ASSISTANT",
      "resourceClass": "ZMFAPLA",
      "access": "READ",
      "action": "validate",
      "validatedId": "ibmuser",
      "status": "Passed"
    }
  ]
}
```



```
}
```

Here is another example of REST API which accepts the path of the Security Descriptor file:

**Request:**

```
Post
'https://share.centers.ihost.com/zosmf/config/security/v1/validate/descriptor?userid=ibmuser'
{
  "path": "/usr/lpp/zosmf/configuration/izu5655S28SM01.json"
}
```

**Response:**

```
{
  "serviceId": "5655S28SM01",
  "serviceName": "z/OSMF Security Configuration Assistant",
  "version": "1.0",
  "vendor": "IBM",
  "resourceItems": [
    {
      "itemId": "5655S28SM01I00001000",
      "itemType": "PROGRAMMABLE",
      "itemCategory": "z/OSMF Security Configuration Assistant",
      "itemDescription": "Allow the user to verify resources in the SERVER class.",
      "resourceProfile": "BBG.SECCLASS.SERVER",
      "resourceClass": "SERVER",
      "whoNeedsAccess": "<IZU_STARTED_TASK_USERID_NAME>",
      "access": "READ",
      "action": "validate",
      "validatedId": "ibmuser",
      "status": "Passed"
    }
  ]
}
```

**End of exercise**