



**Hewlett Packard  
Enterprise**

# **HPE Workload Aware Security for Linux 1.2 version User Guide**

## **Abstract**

This document describes the user operations available on the version 1.2 of Workload Aware Security for Linux (WASL) product. This document is targeted for IT administrator, Users and Support personnel who provide security service. It provides steps on how to work with WASL product.

Part Number: P12139-001  
Published: December 2018  
Edition: 1.2

## Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

## Acknowledgments

Intel<sup>®</sup>, Itanium<sup>®</sup>, Pentium<sup>®</sup>, Xeon<sup>®</sup>, Intel Inside<sup>®</sup>, and the Intel Inside logo are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft<sup>®</sup> and Windows<sup>®</sup> are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe<sup>®</sup> and Acrobat<sup>®</sup> are trademarks of Adobe Systems Incorporated.

Java<sup>®</sup> and Oracle<sup>®</sup> are registered trademarks of Oracle and/or its affiliates.

UNIX<sup>®</sup> is a registered trademark of The Open Group.

VMware vSphere<sup>®</sup> is a registered trademark of VMware, Inc. in the United States and/or other jurisdictions.

## Revision history

| Part number | Publication date | Edition |
|-------------|------------------|---------|
| P12139-001  | December 2018    | 1.2.0   |
| P03766-001  | April 2018       | 1.1.0   |

# Contents

- Workload Aware Security for Linux Overview.....5**
  - Deployment and architecture..... 5
  - SMS Login.....7
  - User Roles..... 7
  
- WASL Configuration and Operations.....9**
  - Workload Management..... 9
    - Add or Register Workload..... 9
    - Edit Workload..... 15
    - Deploy Security Policy..... 16
    - Undeploy or Remove security policy from workload..... 17
    - Disable workload..... 17
  - Workloads Operations..... 18
    - View Workload Details..... 18
    - Evaluate Workload..... 21
    - Remediate Workload..... 24
    - Rollback last Remediation operation on Workload..... 31
    - Reset Workload..... 32
  - User Management..... 33
    - View Users..... 33
    - Add User..... 34
    - Edit User..... 36
    - Reset Password..... 36
    - Activate/De-activate Users..... 37
    - Delete User..... 37
  - Policy Operations..... 38
    - View policies..... 38
    - Disable/Enable security policy..... 40
    - Policy customization..... 40
    - Policy update..... 49
  
- Session operation and Help..... 55**
  
- Websites..... 56**
  
- Support and other resources..... 57**
  - Accessing Hewlett Packard Enterprise Support..... 57
  - Accessing updates..... 57
  - Customer self repair..... 58
  - Remote support..... 58
  - Warranty information..... 58
  - Regulatory information..... 59
  - Documentation feedback..... 59

**Sample JSON file used to import policy..... 60**

**Sample profile\_apis.py optionally used in importing policy..... 61**

**Acronyms.....66**

# Workload Aware Security for Linux Overview

Workload Aware Security for Linux (WASL) provides a way to secure the operating system instance and the associated application running together by a single-click from centralized system (called Security Management Station). WASL can evaluate a workload (operating system or operating system with associated application) to access the current security level, do remediation to increase the security level of the workload. It also offers rich reports and shows the details of specific evaluations and remediations. WASL also offers a feature to roll back any remediation done and gets back the workload configuration to a previously known configuration state.

WASL is shipped with basic and advanced licensing. Basic license offers SUSE Linux Enterprise Server (SLES) and Red Hat Enterprise Linux (RHEL) OS hardening profiles whereas advanced licensing offers SAP HANA profiles and basic licensing.

WASL uses a profile based on the global benchmark standards Extensible Configuration Checklist Description Format (XCCDF) and currently provides the following standard profiles:

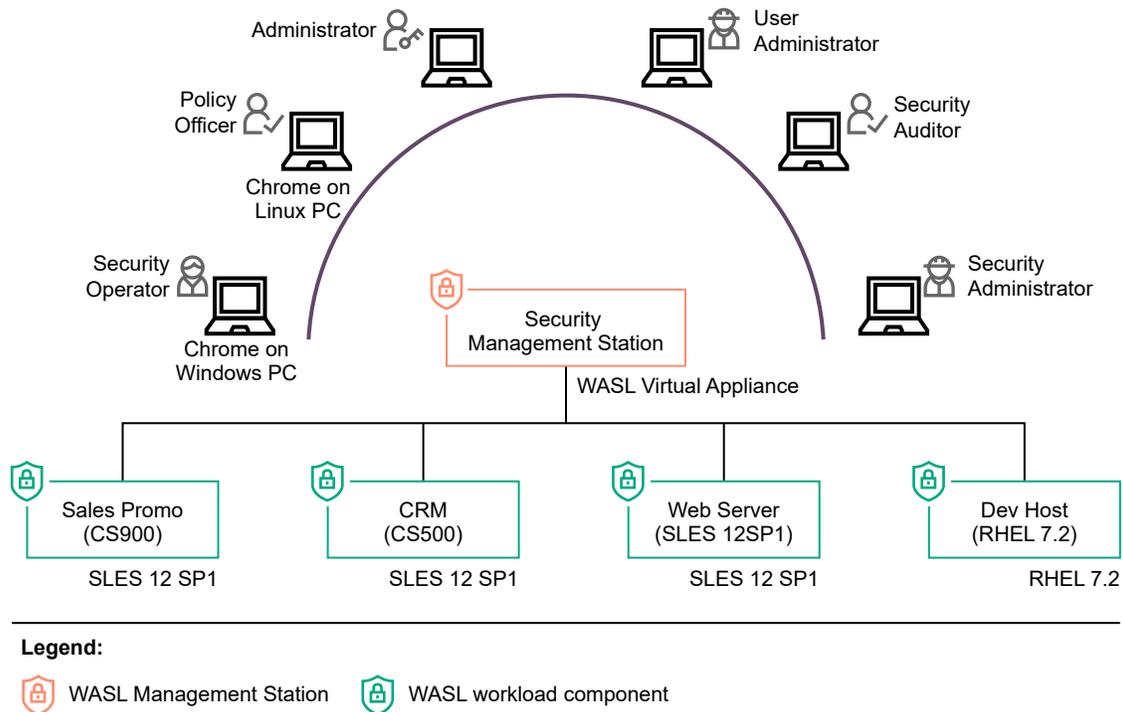
- OS Security for SLES 12 (SP1, SP2, and SP3)
- OS Security for SLES SAP HANA 12 (SP1, SP2, and SP3) (OS Security tailored for SAP HANA database)
- OS Security for RHEL 7 (7.2, 7.3, 7.4, and 7.5)
- SAP HANA 1.0 Database
- SAP HANA 2.0 Database
- OS extended profile for SLES 12 SAP HANA (SP1, SP2, and SP3) (extra OS protection for securing SAP HANA database)

## Deployment and architecture

A typical deployment of WASL consists of a SMS and a set of workloads. A workload can be just an instance of operating system or it can be an instance of operating system with associated application installed on it. WASL can secure the following workloads:

- Operating System only
- Operating System and associated application
- Associated application only

The SMS is a web-based application accessible on HTTPS default port (443). It offers a rich set of GUI that is accessible through Chrome and supports a varied set of roles for users to log in and perform activities.



**Figure 1: WASL Deployment Scenario**

Users can register multiple workloads in SMS. It captures the workload access credentials as a part of registration process. SMS interacts with these workloads establishing a secure shell session between the SMS node and the target node. It can also automatically push the Node packages to target node and install remotely. It invokes the security tool to secure the workload element. A workload element can either be an OS or OS and the application running on the OS or only the application.

SMS stores information related to workloads in Couchbase Server NoSQL database (accessible through default port 8091). Critical data like user passwords, workload credentials is encrypted and stored in the Couchbase Server database using public/private keys protected by a master password. This master password is to be supplied during SMS startup. Some of the data like the reports of a workload evaluation/remediation, logs are stored as flat files.

SMS exposes an HTTPS-based web interface using Express.js and Node.js based technologies and Grommet UX framework.

On the Node, WASL uses OpenSCAP product to perform evaluation and remediation of workload using security policies that are based on XCCDF specification. This specification is provided as a part of Security Content Automation Protocol (SCAP) standard maintained by National Institute of Standards and Technology (NIST). The use of this format allows WASL to import and work with many policies that are based on these standards.

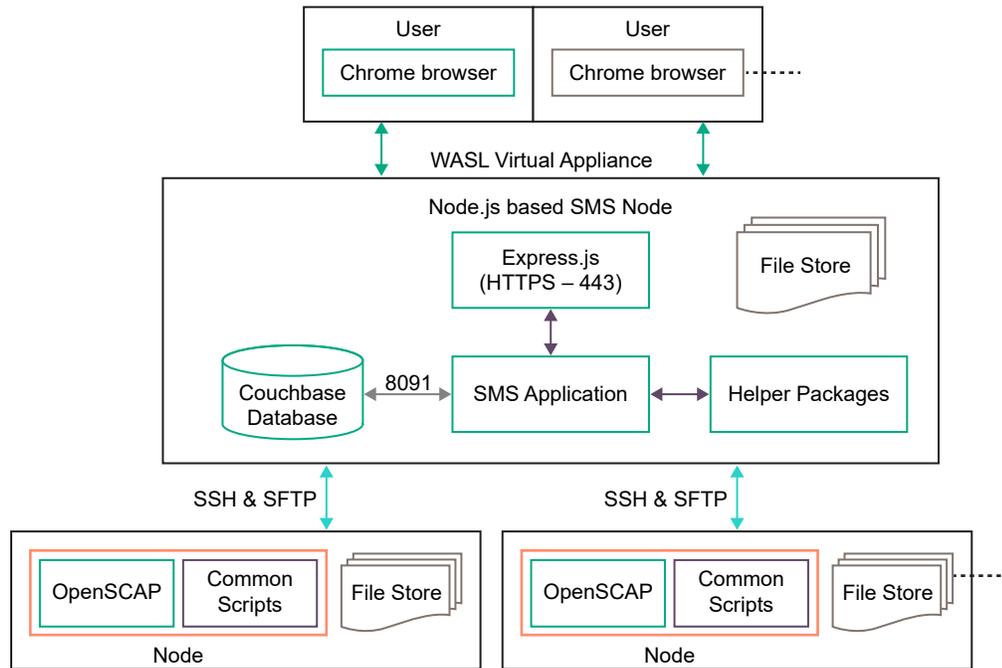


Figure 2: WASL Architecture flow

## SMS Login

### Prerequisites

Install the WASL product. For more information, see the *WASL Install and Setup guide*.

### Procedure

1. Access SMS using Chrome browser.
2. Enter the URL `https://<IPAddress of SMS host>`.  
443 is the default port used by WASL to expose the web interface.
3. Authenticate to SMS using the default administrator account username="admin" and password="admin".
4. You are prompted to change the password on first login.
5. Use this account for admin purposes only.

To perform operations in SMS, add other SMS user with different roles.

## User Roles

To connect to SMS, create users with appropriate role and access credentials.

The type of user role limits the kind of operations that can be performed by the user.

For information on different operations that is possible in WASL, see [WASL Configuration and Operations](#).

The following table lists the role-based operations allowed to each user role:

**Table 1: Role-based operations**

| <b>Role Name</b>       | <b>Operation Name</b> | <b>Operations Permitted</b>   |
|------------------------|-----------------------|---|
| User Administrator     | User Management       | View, Create, Edit, Delete, Activate, De-activate, and Search users   |
|                        |                       | Reset Password of user  |
|                        |                       | Assign role to user.  |
| Policy Officer         | Policy Management     | View, Enable, Disable, Search Policies<br>Policy Customization (Add, Copy, Edit, Reload Policy, Import, or Delete Policy) and Policy Update   |
| Security Operator      | Workload Operations   | View, Evaluate, Remediate, Rollback, and Search Workload  |
|                        | View Details          | View and Search SMS Activities<br>View Dashboard  |
|                        |                       |   |
| Security Administrator | Workload Management   | Add, Edit, Disable Workload.<br>Deploy, Undeploy policies on a Workload.  |
|                        | Workload Operations   | View, Evaluate, Remediate, Rollback, Reset, and Search Workload   |
|                        | View Details          | View and Search SMS Activities<br>View Dashboard  |
|                        |                       |   |
| Security Auditor       | Workload Operations   | Only View, Evaluate, and Search Workload  |
|                        | View Details          | View and Search SMS Activities<br>View Dashboard  |
|                        |                       |   |
| Administrator          | All Operations        | Capability to perform operations related to all roles.<br>More capability to edit SMS settings.<br>This role is provided to only "admin" user |

# WASL Configuration and Operations

## Workload Management

Workload Management involves the following:

- Add or register a Workload in SMS
  - automatic Installation of WASL packages on end node during registration
- Deploy and Undeploy the security policies on the Workload
- Edit Workload
- Disable Workload

## Add or Register Workload

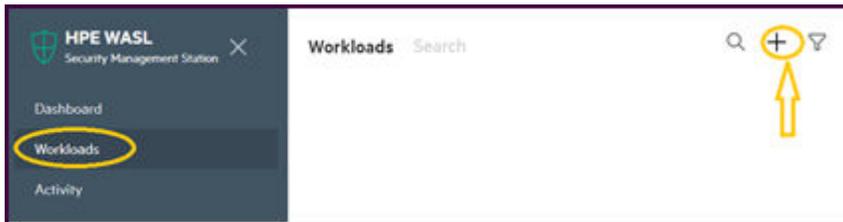
### Prerequisites

This option is visible to users with 'Administrator' or 'Security Administrator' roles.

### Procedure

To add or register a workload from the Workloads tab:

1. Click + icon.



2. Enter the **Workload Name**.

The Workload name is used to reference the workload on SMS screen and should be unique for different workload.

3. Enter the **Workload Type**.

The **Workload Type** can be **Operating System Only** or **SAP HANA Scale-up System**.

- a. If you select **Operating System Only** type, then only **Add Node** element is displayed.

## Register Workload ✕

Workload Type

Operating System Only ▾

Workload Name

Enter Workload name

Node +

**Register**

- b. If you select **SAP HANA Scale-up System** type, then both **Add Node** and **SAP HANA System** elements are displayed.

## Register Workload ✕

Workload Type

SAP HANA Scale-up System ▾

Workload Name

Enter Workload name

Node +

SAP HANA System +

**Register**

4. Click the **Register** button to register a new workload on SMS.

Workload once added cannot be deleted. The Workload record is maintained for auditing purposes. It can only be disabled.

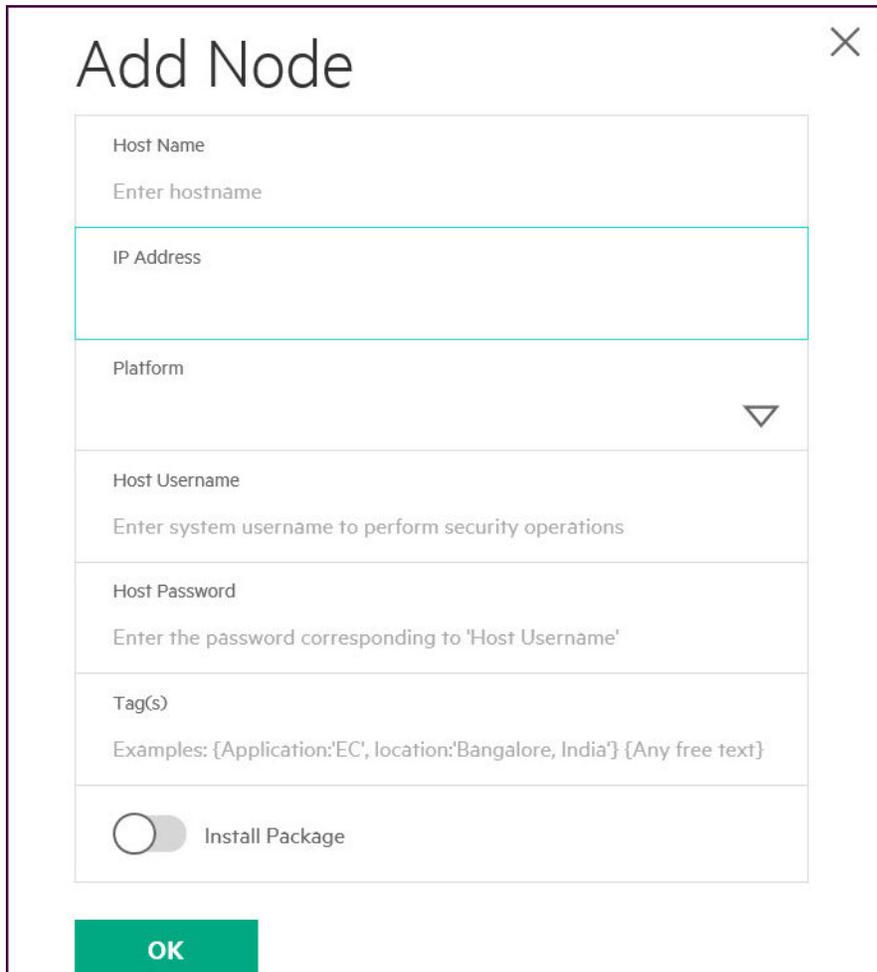
---

**NOTE:** The workload can be reconfigured in future using **Edit** workload option after it is registered to SMS.

---

## Add Node.

To register the node associated with the workload, enter the following details:



The screenshot shows a dialog box titled "Add Node" with a close button in the top right corner. The dialog contains the following fields and controls:

- Host Name:** A text input field with the placeholder text "Enter hostname".
- IP Address:** A text input field, currently highlighted with a red border.
- Platform:** A dropdown menu with a downward-pointing triangle icon.
- Host Username:** A text input field with the placeholder text "Enter system username to perform security operations".
- Host Password:** A text input field with the placeholder text "Enter the password corresponding to 'Host Username'".
- Tag(s):** A text input field with the placeholder text "Examples: {Application:'EC', location:'Bangalore, India'} {Any free text}".
- Install Package:** A toggle switch that is currently turned off.
- OK:** A green button at the bottom left of the dialog.

### Procedure

- 1. Host Name** Enter the Host name of the Node.
- 2. IP address:** Enter the IP address of the Node. Only IPV4 address is supported. WASL uses this IP address to SSH to install and set up Node Package.
- 3. Platform:** Select the Operating System version running on the Node. WASL uses the Platform information to display the security policies that can be deployed on the workload during Deploy Policy operation.
- 4. Host Username:** Enter the Operating system user name on the Node.  
The **Host Username** is used by WASL to connect to Node through SSH for the following:
  - Install and set up Node Package if **Install Package** option is turned on.
  - Perform workload operations like evaluation, remediation, rollback, reset on this node element.

If **Install Package** is turned on, then you can perform the workload operations like evaluation, remediation, rollback, reset on this node.

5. **Host Password:** The password for the **Host Username**.
6. **Tag(s):** You can optionally provide some extra Tag's to for identifying this Node.
7. **Install Package:** If turned on, the WASL Node Packages are automatically installed and setup on the Node.  
If you have turned on the **Install Package** and **Host Username** is not "root" user, then you must provide capability to the **Host Username** to sudo as "root" for performing WASL Node package installation and setup command. For the steps to update sudo user information in `/etc/sudoers.d/waslcore_install` file on Node, see the *Automatic Node Package installation and setup from SMS* section in *WASL Install and Setup guide*. The installation and setup of WASL Node Packages automatically adds the capability for **Host Username** to sudo as "root" and perform Workload Operation (like Evaluate, Remediate, Rollback, and Reset) on this Node.

If you have not turned on the **Install Package**, you must explicitly install and Set up the WASL Node Packages on the Node before registering the Workload. You also must provide capability for **Host Username** to sudo as "root" and perform Workload Operation (like Evaluate, Remediate, Rollback, and Reset) on this Node. For more information, see the *Manual Node Package installation and setup from Node* section in *WASL Install and Setup guide*.

8. Click **OK** and register the workload to SMS.

On Clicking **OK** in the **Register Workload** page:

- a. WASL adds workload entry (Identified by the **Workload Name**) in the **Workload** page.
- b. If the **Install Package** in the **Add Node** screen is turned on, then WASL tries to Install and Set up the Node Packages.
- c. WASL also does an SSH to the end node and validate if the details provided in **Add Node** screen are correct.

Click on the new workload entry in Workload page to know the status of editing this workload. The status is updated at following places:

- The Taskbar at the top of the workload entry page if there is error.
- The **Recent Activity** at the bottom of the workload entry page.
- The **Activity** page of WASL.

## Add SAP HANA System

Enter the following details of SAP HANA System Database:

## Add SAP HANA System ✕

|   |
|---|
| SAP HANA System ID  |
| Enter SAP HANA System ID  |
| SAP HANA Instance ID  |
| Enter SAP HANA Instance ID  |
| SAP HANA DB Username  |
| Enter SAP HANA DB Username  |
| SAP HANA DB Password  |
| Enter SAP HANA DB Password  |
| Host Username   |
| Enter system username to perform security operations                  |
| Host Password   |
| Enter the password corresponding to 'Host Username'                   |
| Tag(s)  |
| Examples:[Application:'BW',type:standby] {sidadm:yes} {Any free text} |

OK

### Procedure

1. **SAP HANA System ID:** Enter the **SAP HANA System ID** (SID) of SAP HANA database.  
Example: HDB, SEQ, etc.
2. **SAP HANA Instance ID:** Enter the **SAP HANA Instance ID** of the SAP HANA system.  
Example: 00, 01
3. **SAP HANA DB Username:** Enter the **SAP HANA DB Username**. WASL uses this user name to connect to SAP HANA Database for Workload Operation on SAP HANA System Database. The **SAP HANA DB Username** can be the database user "SYSTEM" or any SAP HANA database user who is granted the following privileges:

```
GRANT DATA ADMIN TO <SAP HANA DB Username> WITH ADMIN OPTION
GRANT RESOURCE ADMIN TO <SAP HANA DB Username> WITH ADMIN OPTION
GRANT INIFILE ADMIN TO <SAP HANA DB Username> WITH ADMIN OPTION
GRANT SERVICE ADMIN TO <SAP HANA DB Username> WITH ADMIN OPTION
GRANT AUDIT ADMIN TO <SAP HANA DB Username> WITH ADMIN OPTION
GRANT SELECT,INSERT,DELETE ON "_SYS_SECURITY" . "_SYS_PASSWORD_BLACKLIST" TO <SAP HANA DB Username>
GRANT ENCRYPTION ROOT KEY ADMIN TO <SAP HANA DB Username> WITH ADMIN OPTION
(The ENCRYPTION ROOT KEY ADMIN privilege is required in case SAP HANA database version is 2.0 or higher)
```

Use SAP HANA SQL command to grant these privileges. Replace the **<SAP HANA DB Username>** with the user name provided in **SAP HANA DB Username** field.

4. **SAP HANA DB Password:** The password for the **SAP HANA DB Username**.
5. **Host Username:** This can be any non-privileged OS users on the Node where SAP HANA is installed.

WASL performs all Workload Operations on the SAP HANA System Database by logging into the Node using this Host Username via SSH. It then does a sudo to **waslhanauser** user on the Node. The **waslhanauser** in turn connects to the SAP HANA System Database or runs specific scripts with higher privileges (using sudo) to perform operation like deploy, evaluation, remediation, rollback and reset.

WASL product uses **SAP HANA Client - HDB\_CLIENT** tool provided along with SAP HANA database to connect with the SAP HANA database. The default path looked by WASL for this tool is either `/usr/sap/hdbclient` or `/home/waslhanauser/sap/hdbclient`.

If HDB\_CLIENT tool is not installed in these locations, then **Host Username** provided here can be made to sudo to **<SID>adm** OS user instead of **waslhanauser** user and run all the WASL operations. Running the WASL operations as **<SID>adm** OS user allows WASL to lookup more paths like `/usr/sap/<SID>/HDB<INSTANCE_NUMBER>/exe/python_support/hdbcli` or `/usr/sap/<SID>/home/sap/hdbclient/` for locating and using **HDB\_CLIENT** tool. To use **<SID>adm** OS user instead of **waslhanauser** add `{sidadm=yes}` tag in the Tags field of this Add System DB screen.

---

**NOTE:**

- a. **<SID>adm** OS user is created by SAP HANA for administration operation on SAP HANA database. **<SID>** is the SAP HANA System ID.
- b. The **waslhanauser** is a non-privileged user created as a part of WASL Node Package installation.
- c. Specific setup like creating SAP HANA client certificates, enabling to run some scripts with higher privileges is required for **waslhanauser** or **<sid>adm** user.

This setup is automatically done if Install Package option is turned on in the Add Node screen.

For more information or if you are doing manual Node package installation and setup, see WASL Install and Setup guide.

The SAP HANA client certificates setup during this phase is valid for one year. The certificate gets automatically regenerated, if you Edit Workload and select Install Package option in the Add Node screen once again and save the Workload.

- d. Do not change the Tags file to add or remove the `{sidadm=yes}` tag from time to time as this might lead to file permission issues on end Node.

---

**6. Host Password:** The password for **Host Username**.

**7. Tag(s):** You can optionally provide extra Tag's to for identifying this Node.

**8.** Click **OK** and register the workload to SMS after updating all entries.

**9.** On Clicking **OK** in the **Register Workload** page:

- a. WASL adds a new workload entry (Identified by the **Workload Name**) in the **Workload** page.
- b. WASL also does a SSH to the end node and validate if the details provided in **Add Node** screen is correct.
- c. If the **Install Package** in the **Add Node** screen is turned on, then WASL tries to Install and Setup the Node Packages.
- d. WASL also does a SSH to the end node (using the credentials provided in **Add SAP HANA System** screen). It validates if the details provided in **Add SAP HANA System** screen is correct. Details like database connectivity, privileges provided to **SAP HANA DB Username** is checked.
- e. You can click on the new workload entry added to know the status

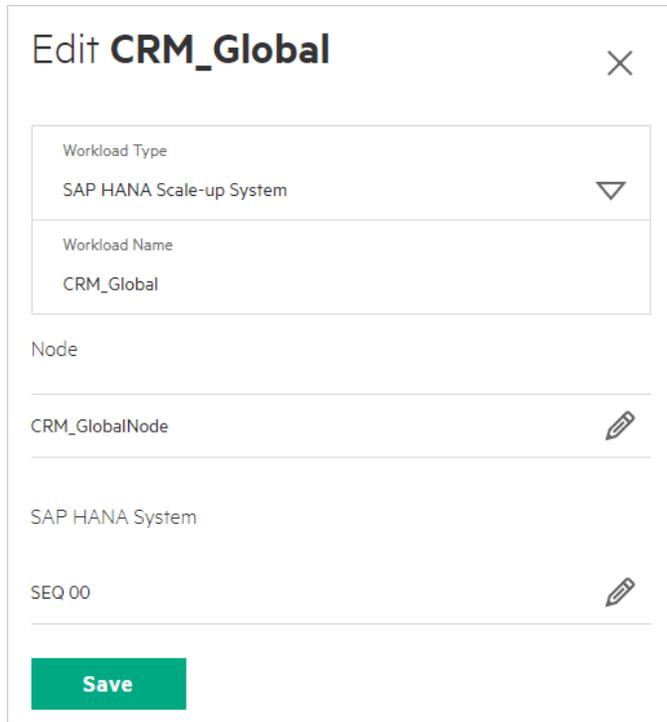
The status is updated at the following:

- The Taskbar at the top of the workload entry page in case of error.
- The **Recent Activity** at the bottom of the workload entry page.
- The status also gets updated in the **Activity** page of WASL.

## Edit Workload.

### Prerequisites

This option is visible to users with "Administrator" or 'Security Administrator' roles.



The screenshot shows a dialog box titled "Edit CRM\_Global" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Workload Type:** A dropdown menu currently showing "SAP HANA Scale-up System".
- Workload Name:** A text field containing "CRM\_Global".
- Node:** A section header.
- CRM\_GlobalNode:** A text field containing "CRM\_GlobalNode" with an edit icon (pencil) to its right.
- SAP HANA System:** A section header.
- SEQ 00:** A text field containing "SEQ 00" with an edit icon (pencil) to its right.
- Save:** A green button at the bottom left.

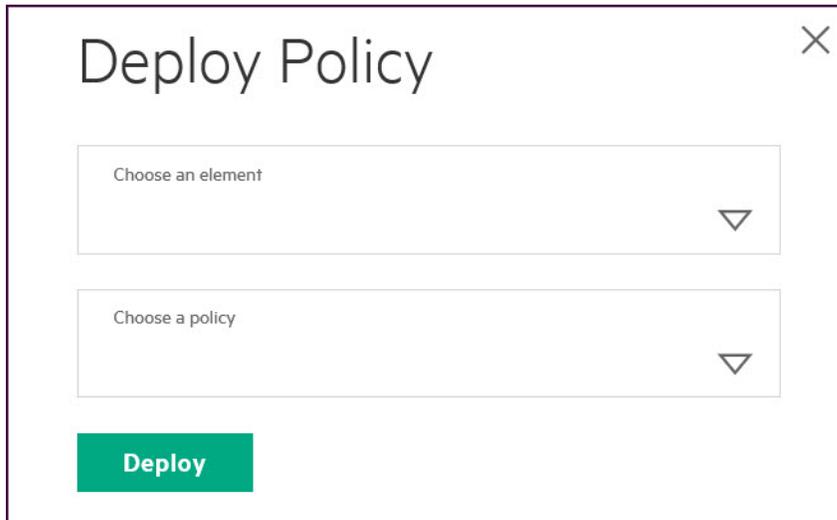
### Procedure

1. Click the workload in the **Workload** page.
2. Select the **Edit** button.
3. The screens, options, and parameters provided are similar to details provided in the **Add or Register Workload**. All the workload parameters except few parameters like **Workload Name**, **Platform** can be updated.
4. If the **Install Package** in the **Edit Node** screen is turned on, then WASL tries to Install and Set up the Node Packages.
5. WASL connects to the Node and validates the workload as done during **Add or Register Workload**

## Deploy Security Policy

### Prerequisites

This option is visible to users with "Administrator" or 'Security Administrator' roles.



The screenshot shows a dialog box titled "Deploy Policy" with a close button (X) in the top right corner. Inside the dialog, there are two dropdown menus. The first dropdown is labeled "Choose an element" and the second is labeled "Choose a policy". Below these dropdowns is a green button labeled "Deploy".

### Procedure

To deploy security policies on a workload,

1. Click the workload in the **Workload** page.
2. Select the **Deploy Policy** button.
3. Select from the drop-down of **Choose an element** option.  
This option displays the Workload elements that are configured during *Add or Register Workload* operation. The drop-down options can be one of the following:
  - a. Node (Shown as MasterNode)  
Or
  - b. SAP HANA System (Shown as SystemDB)
4. Select from the drop-down of **Choose a policy** option.  
This option lists the Policies that are applicable on the Workload element selected through **Choose an element**.  
Policies that are already deployed on the Workload elements are not displayed in the drop-down.
5. Click the **Deploy** button.  
WASL transfers the policy-related files to the Node having the workload and validate the workload settings.

### Deploy multiple policies on Workload.

To deploy multiple policies on workload, follow the same process defined in [Deploy Security Policy](#)

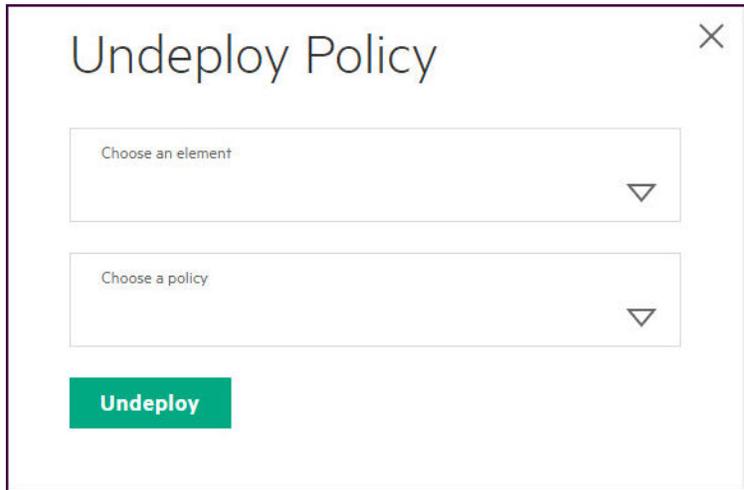
## Procedure

1. To view the details, click the workload name from the Workload tab.
2. Click the arrow next to **Deployed Policies** option on the screen.
3. A list of all the policies deployed on the workload is displayed.

## Undeploy or Remove security policy from workload.

### Prerequisites

This option is visible to users with "Administrator" or 'Security Administrator' roles.



The screenshot shows a dialog box titled "Undeploy Policy". It features two dropdown menus. The first dropdown is labeled "Choose an element" and the second is labeled "Choose a policy". Below these dropdowns is a prominent green button labeled "Undeploy".

## Procedure

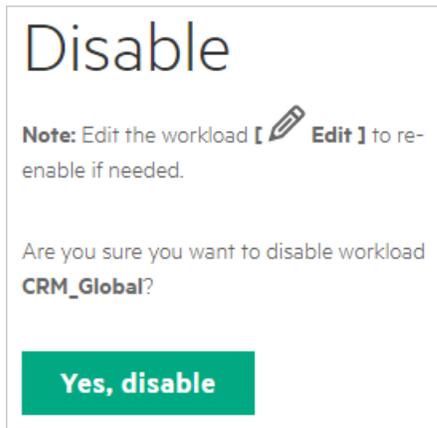
To Undeploy security policy that is deployed on a workload:

1. Click the workload in the **Workload** page.
2. Select the **Undeploy Policy** button.
3. Select from the drop-down of **Choose an element** option.  
This option displays the Workload elements that are configured during *Add or Register Workload* operation. The drop-down options can be one of the following:
  - a. Node (Shown as MasterNode)  
Or
  - b. SAP HANA System (Shown as SystemDB)
4. Select from the drop-down of **Choose a policy** option.  
This option lists the Policies that are applicable on the Workload element selected through **Choose an element**.
5. Click the **Undeploy** button.
6. WASL removes the policy-related files on the Node.

## Disable workload.

### Prerequisites

This option is visible to users with "Administrator" or 'Security Administrator' roles.



### Procedure

To disable a workload,

1. Click the workload in the **Workload** page.
2. Click the **Disable** button.

Once a Workload is disabled, no other operation apart from **Edit Workload** is allowed on this workload.

The workload gets re-enabled on editing the workload.

Edit of the workload tries to validate the workload before re-enabling it.

## Workloads Operations

### View Workload Details

#### Prerequisites

This option is visible to users with "Administrator", "Security Administrator", "Security Operator" and "Security Auditor" roles.

←
CRM\_Global

✓
Online

Security Posture

System Compliance



64 %

■ System Compliance Score

Application Compliance



57 %

■ Application Compliance Score

Landscape ▷

---

Deployed Policies ▷

---

Recent Activity

|   |           |                      |
|---|-----------|----------------------|
| <span style="color: green;">●</span> Workload Evaluate <b>CRM_Global</b> by Admin | Completed | 10 Dec 2018 11:27 am |
|---|-----------|----------------------|

[All activity](#)

- ⇄ Evaluate
- 🔒 Remediate
- 📄 Deploy Policy
- 🗑️ Undeploy Policy
- ↶ Rollback
- 🔄 Reset
- ✎ Edit
- 🚫 Disable

## Procedure

To view details of the Workloads.

1. Click the Workload entry in the **Workload** page. Following details are visible:
  - a. **Workload Name:** The name of the workload entered during "Add or Register Workload".
  - b. **Status** of the workload.
  - c. **Security Posture:** It displays the current system and application compliance score from the last evaluation/remediation operation.  
 The current system compliance score is the score of the Node element of Workload.  
 The application compliance score is the score of SAP HANA System element of Workload.  
 This score is calculated by cumulative rules evaluated/remediated successfully as defined in all the policies deployed on the workload.
  - d. **Operation:** The right side of the screen displays various operations like Evaluate, Remediate, Deploy Policy and more. These operations can be performed on the workload by clicking them. The Operations will vary for different role.  
 For example: A Security Operator will see an Evaluate, Remediate, and Rollback operations.
  - e. **Landscape:** Displays the workload synopsis such as the underlying Node and the SAP HANA System details. To see the complete details, use the Edit operation in this screen.

## Landscape

**CRM\_Global**

● OK

---

MasterNode

CRM\_GlobalNode  

---

SystemDB

SEQ 00

Edit operation is visible only to users with 'Administrator' or 'Security Administrator' roles.

- f. Deployed Policies:** Displays a list of all the policies deployed on the workload.

## Deployed Policies

CRM\_GlobalNode

| Policy   | Deployed Version | Current Score (In %) | Update Available |
|--|------------------|----------------------|------------------|
| OS Security Level 1 for SLES for SAP Applications 12 | v1.2.0           | 64.25                | <b>No</b>        |

---

SEQ 00

| Policy                           | Deployed Version | Current Score (In %) | Update Available |
|----------------------------------|------------------|----------------------|------------------|
| SAP HANA 1.0 DB Security Level 1 | 1.2.0            | 65.28                | <b>No</b>        |
| SAP HANA 1.0 DB Security Level 2 | 1.2.0            | 58.02                | <b>No</b>        |

- g. Recent Activity:** Displays the most recent activities performed on the workload.

## Recent Activity

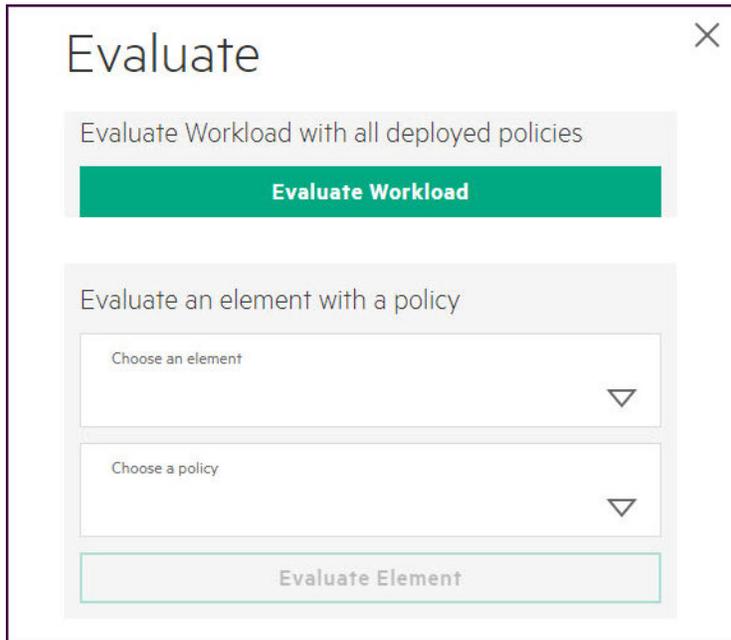
- Workload Evaluate **CRM\_Global** by admin Completed 10 Dec 2018 6:09 pm
- Workload Evaluate **CRM\_Global** by admin Completed 10 Dec 2018 5:39 pm
- Workload Evaluate **CRM\_Global** by admin Completed 10 Dec 2018 5:39 pm

- h. All activity:** The screen is redirected to Activity Page of WASL and you will see a filtered list of activity performed on this workload.

## Evaluate Workload.

### Prerequisites

This option is visible to users with "Administrator", "Security Administrator", "Security Operator" and "Security Auditor" roles.



The screenshot shows a dialog box titled "Evaluate" with a close button (X) in the top right corner. It contains two main sections. The first section is titled "Evaluate Workload with all deployed policies" and features a prominent green button labeled "Evaluate Workload". The second section is titled "Evaluate an element with a policy" and contains two dropdown menus: "Choose an element" and "Choose a policy", both with downward-pointing triangles. Below these dropdowns is a button labeled "Evaluate Element".

### Procedure

You can evaluate a workload against policies that are deployed on the Workload.

1. Click the workload in the **Workload** page.
2. You can evaluate a workload in the following two ways:
  - a. Click the **Evaluate** button.  
All the Security Policies that are deployed on the all Workload elements are evaluated on the workload.
  - b. Select from the drop-down of **Choose an element** option. The **Choose a policy** displays the applicable policies that are deployed on the workload element. Select one of the policies. Click **Evaluate Element**.

- When the evaluation starts, the Workload View displays different evaluations that are in progress.

CRM\_Global

Workload Evaluate 'OS Security Level 1 for SLES for SAP Applications 12'  
[Rules completed: 96 of 194]  
  
Monday, 10 December, 2018, 11:35:21 AM  
Running  

10 %

### Security Posture

System Compliance



64 %

System Compliance Score

Application Compliance



57 %

Application Compliance Score

Landscape ▶

Deployed Policies ▶

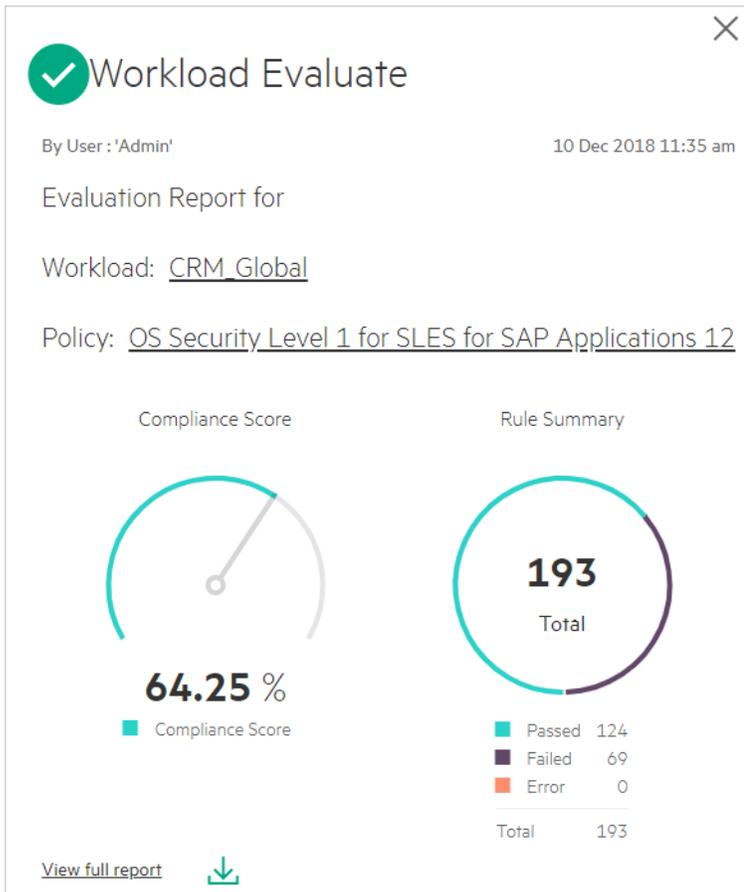
### Recent Activity

|  |  |                     |
|--|--|---------------------|
| <input type="radio"/> Workload Evaluate CRM_Global by admin            | <div style="width: 100px; height: 5px; background: linear-gradient(to right, #00a090 10%, #ccc 10%);"></div> | <b>10 %</b>         |
| <input type="radio"/> Workload Evaluate CRM_Global by admin            | Completed  | 10 Dec 2018 6:20 am |
| <input checked="" type="radio"/> Workload Evaluate CRM_Global by admin | Completed  | 10 Dec 2018 6:02 am |

[All activity](#)

WASL ensures that only one evaluation or operation is active on the End Node.

- After the evaluation is complete, the Workload Meters indicates the current score of the Workload against the policies deployed.  
The Individual scores of each Policy can be viewed under "Deployed Policies" views.
- The "Recent Activity" lists all the Policies that are evaluated individually per policy.
- To view more details on Evaluate Workload activity like the number of Passed, Failed rules or Rules with Error in Policy, click each activity.



- In the **Workload Evaluated** window, click the **View Full Report** to see a complete HTML Report. You can also download it by clicking the download icon.

**Rule results**

124 passed 69 failed

**Severity of failed rules**

24 low 44 medium 1

**Score**

| Scoring system         | Score      | Maximum    | Percent |
|------------------------|------------|------------|---------|
| urn:xccdf:scoring:flat | 124.000000 | 193.000000 | 64.25%  |

**Rule Overview**

pass     fail     notchecked  
 fixed     error     notapplicable  
 informational     unknown

Search through XCCDF rules

Group rules by:

| Title   | Severity | Result |
|---|----------|--------|
| ▼ Guide to the Secure Configuration of SUSE Linux Enterprise 12 <b>69x fail 1x notchecked</b> |          |        |
| ▼ System Settings <b>61x fail 1x notchecked</b>   |          |        |
| ▶ Installing and Maintaining Software   |          |        |
| ▼ File Permissions and Masks <b>11x fail</b>  |          |        |
| ▼ Restrict Partition Mount Options <b>1x fail</b>   |          |        |
| Add nodev Option to Removable Media Partitions  | low      | pass   |
| Add nodev Option to /dev/shm  | low      | pass   |
| Add noexec Option to /dev/shm   | low      | fail   |
| Add nosuid Option to /dev/shm   | low      | pass   |
| ▼ Restrict Dynamic Mounting and Unmounting of Filesystems                                     |          |        |
| Disable the Automounter   | medium   | pass   |
| ▼ Verify Permissions on Important Files and Directories <b>6x fail</b>                        |          |        |
| ▼ Verify Permissions of the cron Files and Directories <b>3x fail</b>                         |          |        |

You can click the individual rule and view the **Rule Summary**.

Add nosuid Option to /dev/shm ✕

|                            |  |
|----------------------------|--|
| Rule ID                    | mount_option_dev_shm_nosuid  |
| Result                     | <b>pass</b>  |
| Time                       | 2018-12-11T16:54:48  |
| Severity                   | low  |
| Identifiers and References | <b>Identifiers:</b> CCE-80154-8<br><b>References:</b> CM-7, MP-2, 1.1.14   |
| Description                | <p>The <code>nosuid</code> mount option can be used to prevent execution of setuid programs in <code>/dev/shm</code>. The SUID and SGID permissions should not be required in these world-writable directories.</p> <p>This rule evaluates if <code>/dev/shm</code> is currently mounted and with <code>nosuid</code> option in the system.</p> <p>To manually check if <code>/dev/shm</code> is mounted with <code>nosuid</code>, check the mount output from the command:</p> <pre>\$ mount   grep /dev/shm   grep nosuid</pre> <p>If <code>/dev/shm</code> is not mounted with <code>nosuid</code> option, as part of remediation, this rule does the following:</p> <p>If there is no entry in <code>/etc/fstab</code> for <code>/dev/shm</code>, but <code>/dev/shm</code> is currently mounted on the system, remediation adds the entry for <code>/dev/shm</code> from <code>/etc/mtab</code> (or mount command output) to <code>/etc/fstab</code> along with <code>nosuid</code> as the new mount option. It also removes any <code>suid</code> or <code>default</code> mount options if present.</p> <p>If there is entry in <code>/etc/fstab</code> for <code>/dev/shm</code>, this entry is modified by adding <code>nosuid</code> mount option and removing any <code>suid</code> or <code>default</code> mount options if present.</p> <p>The device <code>/dev/shm</code> is remounted as part of remediation for the change to take effect.</p> |
| Rationale                  | The presence of SUID and SGID executables should be tightly controlled. Users should not be able to execute SUID or SGID binaries from temporary storage partitions.   |

## Remediate Workload

### Prerequisites

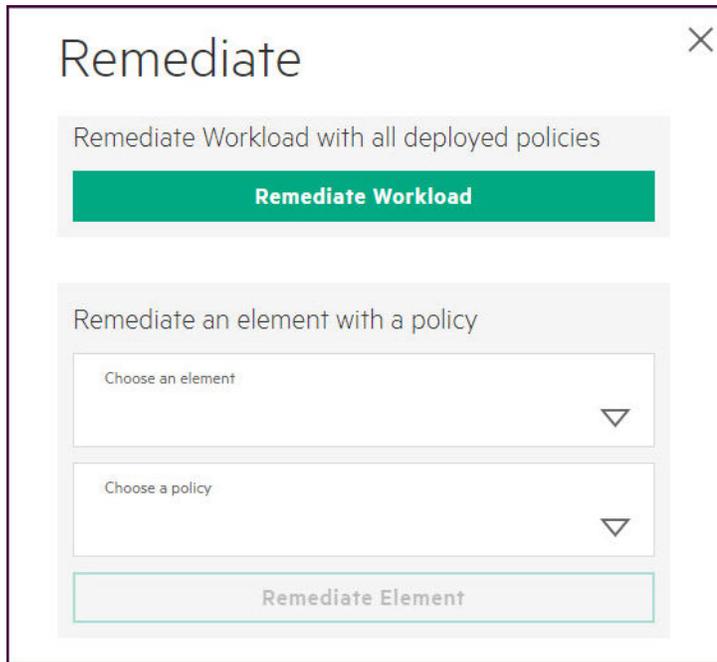
This option is visible to users with 'Administrator', 'Security Administrator', and 'Security Operator' roles.

### Procedure

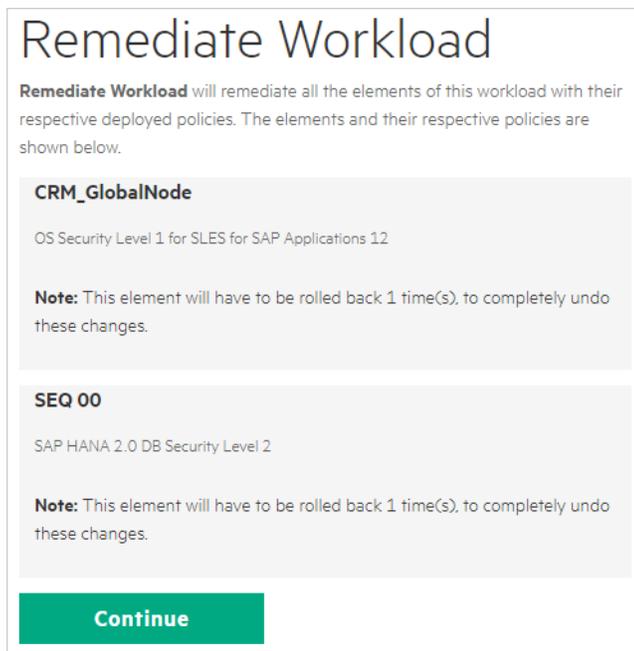
You can remediate a workload against policies that are deployed on the Workload.

1. Click the workload in the **Workload** page.
2. You can remediate a workload in the following two ways:

- a. Click the **Remediate Workload** button.



All the Security Policies that are deployed on the all Workload elements are remediated on the end node.

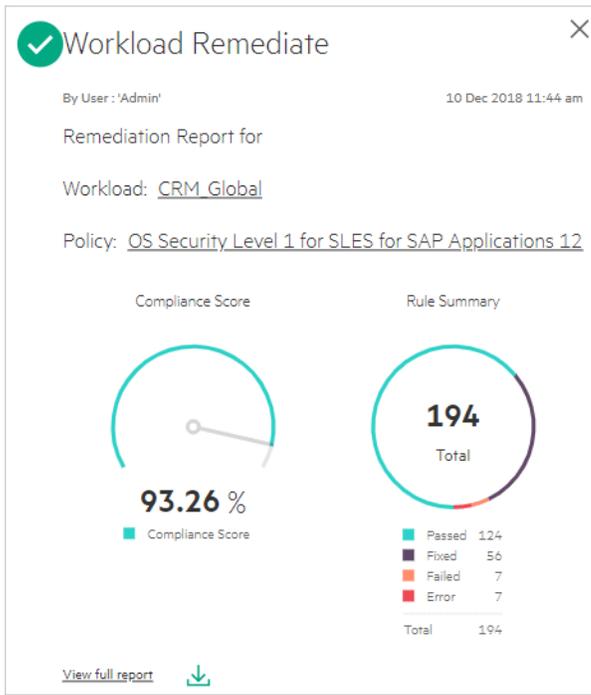


- b. Select from the drop-down of **Choose an element** option. The **Choose a policy** displays the applicable policies that are deployed on the workload element. Select one of the policies. Click **Remediate Workload**.
3. When the remediation starts, the Workload View displays different remediation that are in progress.

WASL ensures that only one remediation or operation is active on the End Node.

The screenshot displays the CRM\_Global dashboard. At the top, there is a navigation bar with a back arrow and the title 'CRM\_Global'. Below this, there are two workload evaluation tasks listed in a grey box. The first task is 'Workload Evaluate 'OS Security Level 1 for SLES for SAP Applications 12'' with 96 of 194 rules completed, running since Monday, 10 December, 2018, 11:35:21 AM, and is 10% complete. The second task is 'Workload Evaluate ...' running since Monday, 10 December, 2018, 11:35:15 AM. Below the grey box, the 'Security Posture' section features two gauge charts: 'System Compliance' at 64% and 'Application Compliance' at 57%. Further down, there are three expandable sections: 'Landscape', 'Deployed Policies', and 'Recent Activity'. The 'Recent Activity' section shows a 'Workload Remediate CRM\_Global by admin' task that is 9% complete.

4. After the remediation is complete, the Workload Meters indicates the current score of the Workload against the policies deployed.  
The Individual scores of each Policy can be viewed under "Deployed Policies" views.
5. The "Recent Activity" lists all the Policies that are Remediated individually per policy.
6. To view more details on Workload Remediate activity like the number of Fixed, Passed, Failed rules or Rules with Error in Policy, click each activity.



7. In the **Workload Remediate** window, click the **View Full Report** to see a complete HTML Report. You can also download it by clicking the download icon. You can click the individual rule and view the **Rule**

## Summary.

Rule results

180 passed 6 8 other

Severity of failed rules

3 low 3 medium

Score

| Scoring system        | Score      | Maximum    | Percent |
|-----------------------|------------|------------|---------|
| um:xccdf:scoring:flat | 180.000000 | 193.000000 | 93.26%  |

Rule Overview

pass  fail  notchecked  
 fixed  error  notapplicable  
 informational  unknown

Search through XCCDF rules  Search

Group rules by:

| Title  | Severity | Result |
|--|----------|--------|
| ▼ Guide to the Secure Configuration of SUSE Linux Enterprise 12 6x fail 7x error 1x notchecked |          |        |
| ▼ System Settings 3x fail 7x error 1x notchecked   |          |        |
| ▶ Installing and Maintaining Software  |          |        |
| ▼ File Permissions and Masks 2x fail 3x error  |          |        |
| ▶ Restrict Partition Mount Options   |          |        |
| ▶ Restrict Dynamic Mounting and Unmounting of Filesystems                                      |          |        |
| ▼ Verify Permissions on Important Files and Directories 2x fail 3x error                       |          |        |
| ▼ Verify Permissions of the cron Files and Directories 2x fail                                 |          |        |
| Verify User Who Owns Crontab Directories   | medium   | pass   |
| Verify Group Who Owns Crontab Directories  | medium   | pass   |
| Verify Permissions on Crontab Directories  | medium   | fixed  |
| Verify permissions of the /etc/crontab file  | medium   | pass   |
| Verify permissions of the /etc/cron.allow file   | medium   | pass   |

8. The Default Policies displays "Error" for some rules during remediation. The Error occurs when remediation script is present for the rules in the policies but not run due to the following reasons:

## Rule Summary

Verify Permissions on Crontab Directories

|                            |   |
|----------------------------|---|
| Rule ID                    | file_permissions_crontab_dirs   |
| Result                     | fixed   |
| Time                       | 2018-12-10T11:50:34   |
| Severity                   | medium  |
| Identifiers and References | Identifier: <a href="#">GEN003100</a><br>Reference: <a href="#">ECLP-1, 225</a>   |
| Description                | Crontab directories should be protected from unwanted permissions. To properly set the group permissions of <code>/etc/cron.d, /etc/cron.hourly, /etc/cron.daily, /etc/cron.weekly, /etc/cron.monthly</code> directories, run the command:<br><pre>chmod og-rwx /etc/cron.d /etc/cron.hourly /etc/cron.daily /etc/cron.weekly /etc/cron.monthly</pre> |
| Rationale                  | Read access to these directories allows users to have insight on system jobs, which can create security risk. Similarly, write access will enable user to run any program with higher privileges.   |
| Evaluation message         | <p>Info</p> <pre>Fix execution completed and returned: 0</pre>  |

- a. These rules are sometimes intentionally not remediated, as they might disrupt the environment on the workload. If required, you can look at the rule description and enable remediation on them, by tailoring the Security Policy. For more information, see **Policy customization**.  
For example: WASL can check for `/etc/issues` banner file for specific banner messages, But will not do remediation of this rule automatically as banner messages might differ from one organization to another.

The Policy can be however customized to allow remediation to happen and change the banner to an appropriate text.

X
Modify the System Login Banner (/etc/issue)

|                            |  |
|----------------------------|--|
| Rule ID                    | banner_etc_issue   |
| Result                     | <b>error</b>   |
| Time                       | 2018-12-10T19:36:59  |
| Severity                   | medium   |
| Identifiers and References | <p><b>Identifiers:</b> <a href="#">CCE-27303-7</a></p> <p><b>References:</b> <a href="#">AC-8(a)</a>, <a href="#">AC-8(b)</a>, <a href="#">AC-8(c)(1)</a>, <a href="#">AC-8(c)(2)</a>, <a href="#">AC-8(c)(3)</a>, <a href="#">48</a>, <a href="#">SRG-OS-000023-GPOS-00006</a>, <a href="#">SRG-OS-000024-GPOS-00007</a>, <a href="#">SLES-12-030120</a></p>  |
| Description                | <p>To configure the system login banner edit <code>/etc/issue</code>. Replace the default text with a message compliant with the local site policy or a legal disclaimer.</p> <p>This rule checks the contents of <code>/etc/issue</code> with the pattern provided in <code>login_banner_text</code> xccdf variable. The <code>login_banner_text</code> xccdf variable is pre populated with a set of standard login banners. Edit the <code>login_banner_text</code> xccdf variable in the profile, with any specific changes required to the login banner.</p> <p>The remediation is not done automatically and will happen only if the <code>remediate_banner_etc_issue</code> xccdf variable is set to true (Default is false). The remediation, will use the banner in <code>login_banner_text</code> xccdf variable, formats it and write the contents to <code>/etc/issue</code>.</p> <p>Sample DoD required text is either:</p> <pre style="font-family: monospace; font-size: 0.9em;"> You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. </pre> <p>OR:</p> <pre style="font-family: monospace; font-size: 0.9em;"> I've read &amp; consent to terms in IS user agreem't. </pre> |
| Rationale                  | <p>Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.</p>  |

**Evaluation messages**

**info**

Fix execution completed and returned: 1

**info**

This rules is not enabled for automatic remediation. To enable automatic remediation, set the xccdf profile variable "remediate\_banner\_etc\_issue" to true. Ensure that the remediation will not cause any undesired effects on the system

**info**

Failed to verify applied fix: Checking engine returns: fail

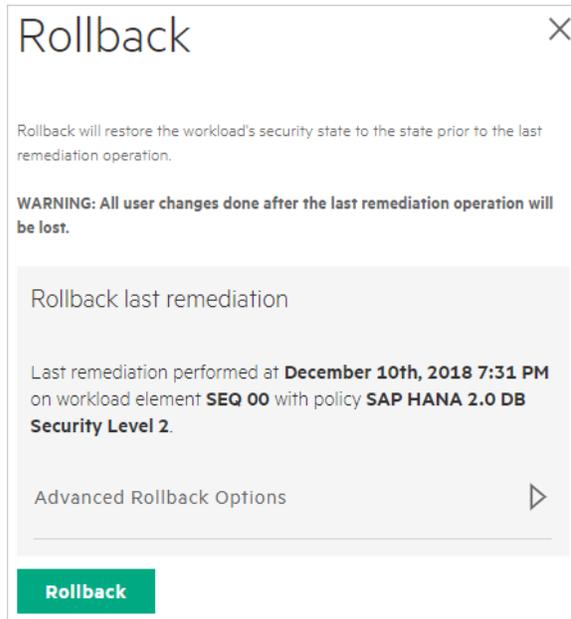
**Remediation Shell script:** [\(show\)](#)

- b. Some of the preconditions for the rules to remediate might not present. For example: A rule to add node to `/tmp` partition might not remediate and give error, as `/tmp` might not be a separate partition on the Node.

# Rollback last Remediation operation on Workload

## Prerequisites

This option is visible to users with "Administrator", "Security Administrator", and "Security Operator" roles.



## Procedure

You can roll back a remediation that is previously done on a workload.

1. Click the workload in the **Workload** page.
2. Click the **Rollback** button.  
Rollback moves the configuration of the workload to a stage that was present before the remediation.
3. By Default Rollback is done on the last Policy remediated on any of the elements in the Workload. If required, you can select the Workload element on which rollback is performed by selecting "Advanced Rollback Options". Rollback will then happen on the last Policy remediation on that Workload element.

Contrary to Remediation, rollback is allowed only on one policy that has been recently remediated on the Workload. Whereas remediation can be done on all the policies that are deployed on a workload by just clicking one button. If you want to roll back all the policies, then see the **Activity** page of WASL to identify the number of remediations done on different workload elements. Then run the rollback operation on those workload elements that many numbers of times.

## Example

The **OS security Level 2 for SLES 12** and **OS Security Extras for SAP HANA** policies are deployed on the Node Workload element. The SAP HANA 2.0 DB Security Level 2 policy is deployed on SAP HANA System workload element for a specific workload. The remediation can be done on all these policies in one go. However, to move the Workload configuration to the state present before remediation, rollback has to be done twice on the Node workload element and once on SAP HANA system workload element.

Rollback works by taking snapshot of the workload element before remediation operation. The snapshot of workload configuration gets stored on the end node getting remediated. This snapshot contains configuration files, service settings, RPM package status, audit file, password policy settings, PAM settings, SAP HANA configuration settings and much more. It is based on the workload element. On doing rollback, the configuration snapshot that is stored is applied back.

---

**NOTE:**

1. During snapshot of default Policies, WASL takes a backup of multiple configurations related to the default Policy and other related Policy. For example, during remediation of "SAP HANA 2.0 DB Security Level 1", a snapshot is taken for both "SAP HANA 2.0 DB Security Level 1" and "SAP HANA 2.0 DB Security Level 2" policies, since both these policies are derived from the same XCCDF sources. It can result in extra snapshot being taken though a specific policy might not be deployed on the workload. Thus rollback might revert more changes than expected on the workload element based on the snapshot.
  2. Snapshot will take entire file backup. For example, the `/etc/ssh/sshd_config` file is backed up during snapshot stage of secure shell configuration. During rollback any other user-specific changes on these files will be lost.
  3. Policy tailoring, specifically if you are changing the content of any of the XCCDF Value/variable using `<set-value>` tag might leave gaps while taking snapshot. For more information, see [Policy customization](#). It is recommended to test the tailoring done for Policy rollback operation from SMS.
  4. Rollback of newly imported policy is possible only if snapshot and rollback options are supported with the policy. You will have to check with the provider of the policy to be imported.
- 

## Reset Workload

### Prerequisites

This option is visible to users with "Administrator" or "Security Administrator" roles.

# Reset

Reset will restore the workload's security state to the state prior to the first remediation operation.

**WARNING: All user changes done after the first remediation operation will be lost.**

Are you sure you want to reset `CRM_Global`?

**Yes, reset**

### Procedure

Reset Workload resets all the security operations performed on the workload to the original state.

The Reset of the workload runs Rollback on all the remediation done so far on the workload elements in the reverse order.

1. Click the workload in the **Workload** page.
2. Click the **Reset** button.  
A reset operation is used in situations when you want to eliminate the operating system or application hardening as a potential cause towards an application downtime.

**NOTE:** Cautiously, use the Reset option as multiple Remediate could have got performed on a workload over a period. Use the rollback of workload recursively instead of reset.

# User Management

This section describes the various operations that are supported for managing the users of SMS.

## View Users

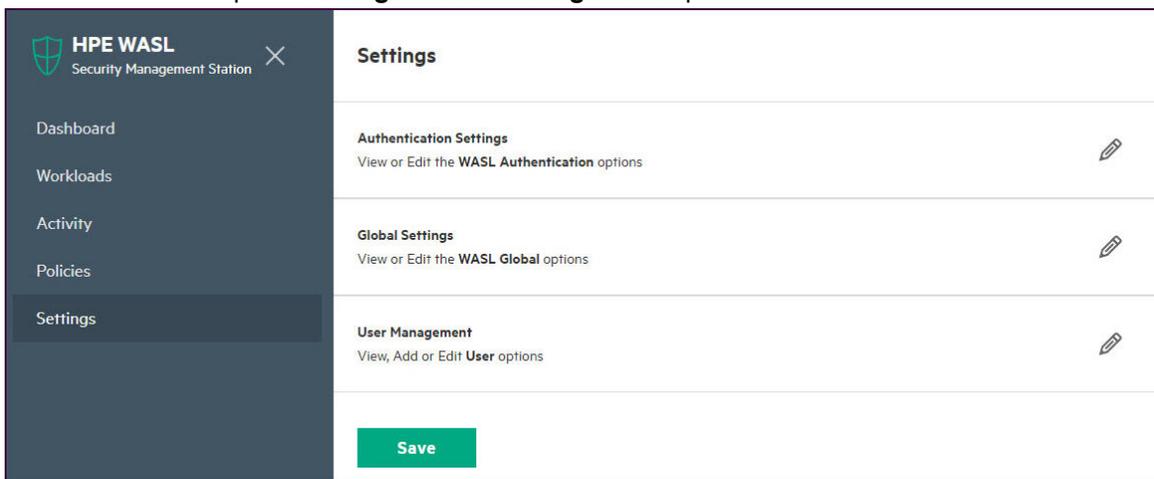
### Prerequisites

This option is visible to users with "Administrator" or "User Administrator" roles.

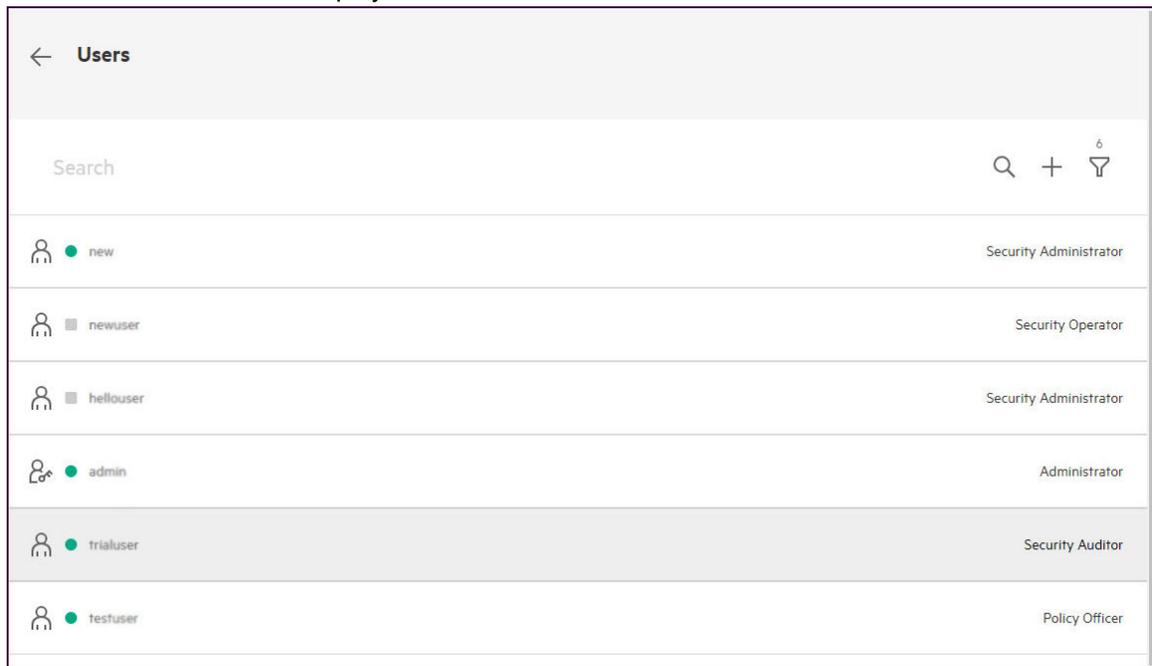
### Procedure

To view users,

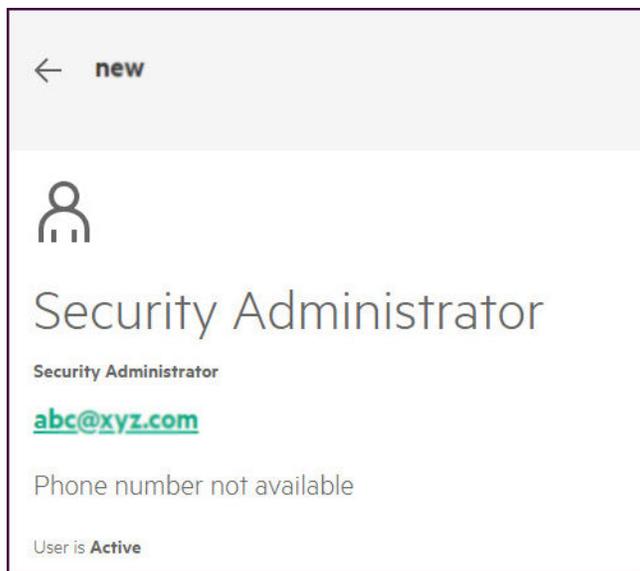
1. Select from the left pane **Settings > User Management** option.



A list of users on SMS is displayed.



- If the icon before the user is gray in color, then the user is in "De-activate" state. The users in De-activate state are not allowed to log in to SMS.
  - A user with green icon is in "Activated" state and can log in to SMS.
2. On the Right side of each user, you can view the role assigned to the user.
  3. To view more details on the user and perform operation on the user, click any of the users account.



## Add User

### Prerequisites

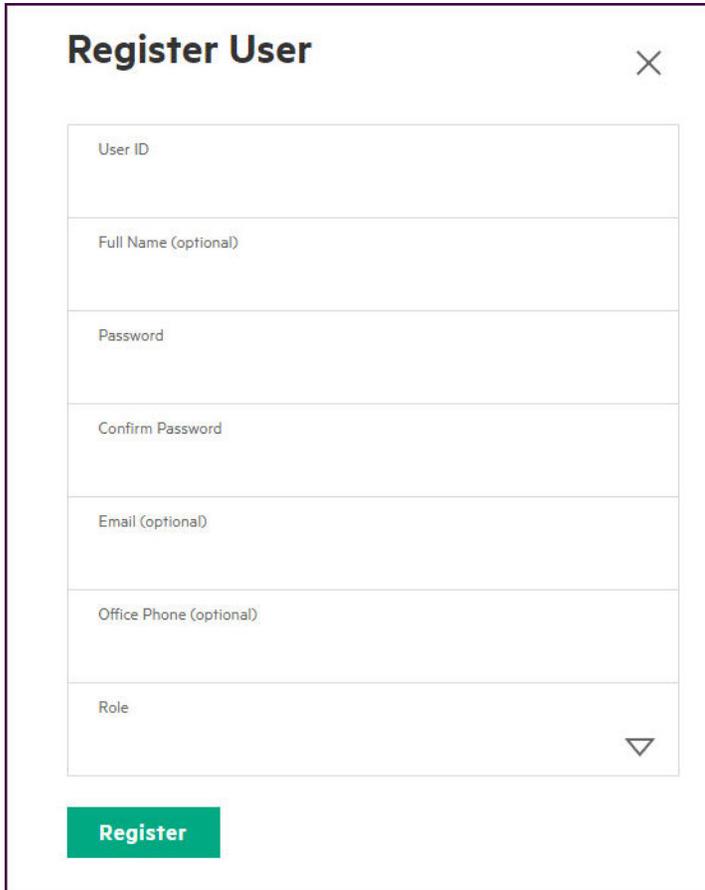
This option is visible to users with "Administrator" or "User Administrator" roles. You can enter new user credentials.

## Procedure

To add user,

1. Select the **Settings > User Management** option from the left pane.
2. Click **+** symbol.

Enter the following details on the **Register User** window.



The screenshot shows a window titled "Register User" with a close button (X) in the top right corner. The window contains several input fields stacked vertically: "User ID", "Full Name (optional)", "Password", "Confirm Password", "Email (optional)", "Office Phone (optional)", and "Role" (which is a dropdown menu with a downward arrow). At the bottom left of the window is a green button labeled "Register".

- a. **User ID**
  - b. **Full Name (Optional)**
  - c. **Password**
  - d. **Confirm Password**
  - e. **Email (Optional)**
  - f. **Office Phone (Optional)**
3. To assign the user, select from the list of **Role**. For different user roles and operations that are allowed for each role, see **User Roles**.
  4. Click **Register** button.

The new user will require to change the password during first-time login.

## Edit User

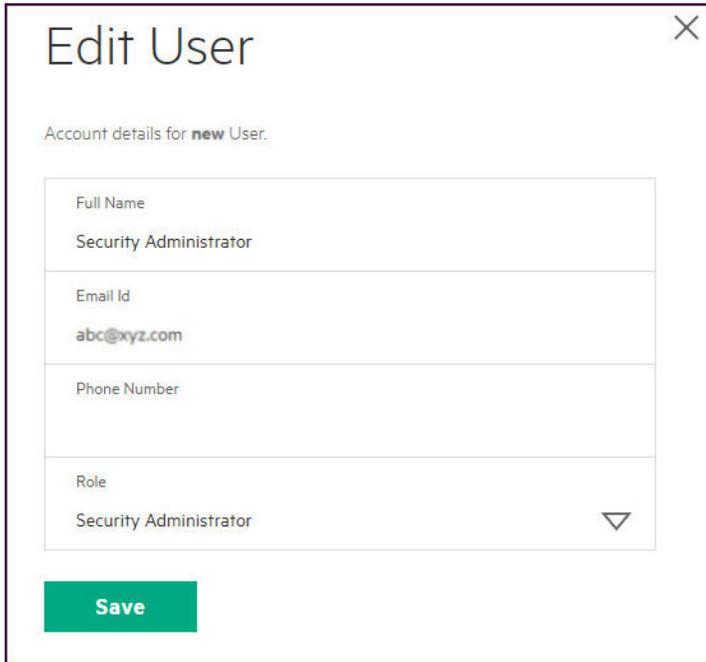
### Prerequisites

This option is visible to users with "Administrator" or "User Administrator" roles.

### Procedure

To edit user,

1. Select the **Settings > User Management** option from the left pane.
2. Click the specific user you want to edit.



3. To edit the user details or change the user role and save, click the **Edit User** option.

## Reset Password

### Prerequisites

This option is visible to users with "Administrator" or "User Administrator" roles. If the user forgets the password, the password can be reset.

### Procedure

To reset user password,

1. Select the **Settings > User Management** option from the left pane.
2. Click the specific user you want to edit.

Reset Password

Reset password for **new** account.

New Password

Confirm New Password

Reset

3. To reset the user password, click the **Reset Password** option.

The user will require to change the password during next login.

## Activate/De-activate Users

The user account apart from 'admin' user can be activated or de-activated at any time.

### Prerequisites

This option is visible to users with 'Administrator' or 'User Administrator' roles.

### Procedure

1. Select the **Settings > User Management** option from the left pane.
2. Click the specific user you want to activate or de-activate.
3. Select **Activate** or **De-activate** option.

### Example

The user can be deactivated for multiple reasons like:

- The administrator is performing a maintenance operation.
- There is a suspicious operation being performed from a user-account.
- The user has left the organization.

## Delete User.

### Prerequisites

This option is visible to users with 'Administrator' or 'User Administrator' roles.

### Procedure

To delete user,

1. Select the **Settings > User Management** option from the left pane.

2. Click the specific user you want to delete.

3. Click **Delete User** option.

A user can be deleted only when no operations are performed using this user credentials. All operations performed by the users are logged and retained for security audit and forensic analysis.

## Policy Operations

### View policies

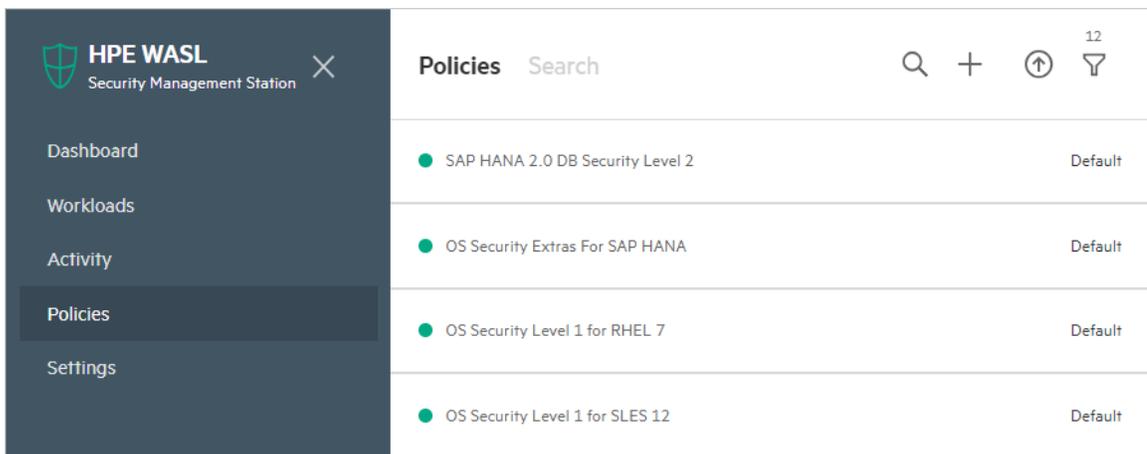
#### Prerequisites

This option is visible to users with 'Administrator' or 'Policy Officer' roles.

#### Procedure

To View the list of security policies provided in WASL:

1. Select the **Policies** option from the left pane.



The screenshot shows the HPE WASL Security Management Station interface. On the left is a dark sidebar with navigation options: Dashboard, Workloads, Activity, Policies (highlighted), and Settings. The main content area is titled 'Policies' and includes a search bar and icons for search, add, refresh, and filter. Below this is a table of policies:

| Policy Name                      | Status  |
|----------------------------------|---------|
| SAP HANA 2.0 DB Security Level 2 | Default |
| OS Security Extras For SAP HANA  | Default |
| OS Security Level 1 for RHEL 7   | Default |
| OS Security Level 1 for SLES 12  | Default |

A list of policies available on SMS is displayed.

- If the icon before the policy is gray in color, then the policy is in "Disable" state. The policies in disable state are not available for deployment on SMS workload element.
  - A policy with green icon is in "enable" state and available for deployment on the workload element.
  - Policies highlighted as **Default** are provided with WASL product.
  - Policies highlighted as **User Defined** are created by Policy customization. For more information, see [Policy customization](#).
2. To get more information on the Policy, click a specific policy. The policy details display the following fields:

←

## OS Security Level 1 for SLES 12

✓ Deployed on 1 element
📄 Copy

🔌 Disable

This policy contains rules to ensure OS security Level 1 baseline of SUSE Linux Enterprise Server 12 system. These rules provide basic security that is required to protect the Operating System instance.

|                   |   |
|-------------------|---|
| <b>Type</b>       | System  |
| <b>Version</b>    | v1.2.0  |
| <b>Platforms</b>  | SUSE Linux Enterprise Server 12<br>SUSE Linux Enterprise Server for SAP Applications 12 |
| <b>Compliance</b> | System security   |
| <b>Workloads</b>  |   |
| <b>Rule Count</b> | 214   |

**File Information** ▽

|   |
|---|
| Policy Directory                                  |
| /opt/hpe/wasl/sms/server/policies/ssg-sle12-xccdf |
| XCCDF File  |
| ssg-sle12-xccdf.xml                               |
| Tailoring File                                    |
| tailoring_xccdf_sles12-c4sl1_profile_default.xml  |

3. **Policy Name:** Name of the policy is displayed on the top of the page.
4. **Status task bar:** Green color Indicates policy is enabled and can be deployed on a workload. Grey color indicates that policy is disabled and cannot be deployed on workloads any more. The status task bar also indicates the number of Workload elements on which the policy is already deployed.
5. **Type:**
  - a. The type **System** indicates that the Policy can be deployed on Node elements of the workload (Operating system Only workload).
  - b. The type **Application** indicates that the policy can be deployed on an application like SAP HANA database that is running on the Node.
6. **Platforms:** The Operating System versions on which the policy can be deployed. This version maps to “PRETTY\_NAME” filed in /etc/os-release file on the end Node.
7. **Compliance:** Indicates if the Policy addresses some compliance.
8. **Workloads:** If the Policy type is Application, then the Workload entry indicates the type of application which this policy secures.
9. **Rule Count:** The number of rules (or group of rules) inside the policy.
10. **File Information:** Click to view the following details:

- a. **Policy Directory:** The directory on WASL SMS system where all the policy-related files are stored.
- b. **XCCDF File:** XCCDF is the main XML file based on XCCDF standards. It has entry point for all the rules in the policy and actions to be taken during evaluation and remediation of the policy. The XCCDF file also has profiles (List of rules or List of group of rules), which is used by WASL to create policies.
- c. **Tailoring File:** Tailoring file is created by WASL when the XCCDF file is loaded into WASL product for the first time. There will be one unique tailoring file per policy. Each tailoring file contains an XCCDF profile (List of rules or List of group of rules). The XCCDF profile is picked from the XCCDF file during first-time load of the XCCDF file by WASL.

## Disable/Enable security policy

### Prerequisites

This option is visible to users with 'Administrator' or 'Policy Officer' roles.

### Procedure

To enable/disable security policy.

1. Select the **Policies** option from the left pane.
2. To get more information on the Policy, click a specific policy.
3. To disable the policy, click **Disable** option from the right side operations menu.
  - Once a policy is disabled, it is not available to deploy on any workload.
  - If the policy is already deployed on a workload, those deployments will not be affected.
4. To enable the policy for deployment to workload, click **Enable** option. Only enabled policies can be deployed on a workload.

## Policy customization

### Tailoring an existing Policy (Copy and Edit security policy)

**Prerequisites:** This option is visible to users with 'Administrator' or 'Policy Officer' roles.

This option provides a way to copy an existing policy and tailor it to the organization-specific policy.

---

### NOTE:

1. Tailoring can only be done on a newly copied policy before the policy is enabled.
  2. If you are planning major changes to a policy by tailoring it, then it is recommended to use a test SMS node with test Workloads. Create and test this tailored policy first. If there are issues in a tailored policy, it can.
    - Cause issues on the workload.
    - There are chances that you might create multiple tailored policies to get the final desired policy. You cannot delete a tailored policy loaded and deployed on a Workload, Policy already deployed once, can only be disabled. It can leave too many unwanted intermediate tailored policies on the SMS.
-

1. Select the **Policies** option from the left pane.
2. Click on the policy you want to create a copy.
3. To copy the policy to a new Policy, click **Copy** option.

4. Provide a new unique Policy Name under **Title** and also provide the **Description** of this new policy.
5. To see the copied policy, click **Task (Activity)** which indicates the successful policy copy operation. Alternatively, you can search for the new policy in the **Policies** page of WASL.

6. Click the new policy that is copied. The details of the new policies are displayed in the center window.

|                   |   |
|-------------------|---|
| <b>Type</b>       | System  |
| <b>Version</b>    | v1.2.0  |
| <b>Platforms</b>  | SUSE Linux Enterprise Server 12<br>SUSE Linux Enterprise Server for SAP Applications 12 |
| <b>Compliance</b> | System security   |
| <b>Workloads</b>  |   |
| <b>Rule Count</b> | 214   |

- To see the policy details such as location of policy files on WASL Virtual Appliance, click the arrow next to **File Information** option.

← Custom OS Security Level 1 for SLES 12

- Not deployed on any element

Custom policy

|                   |   |
|-------------------|---|
| <b>Type</b>       | System  |
| <b>Version</b>    | v1.2.0  |
| <b>Platforms</b>  | SUSE Linux Enterprise Server 12<br>SUSE Linux Enterprise Server for SAP Applications 12 |
| <b>Compliance</b> | System security   |
| <b>Workloads</b>  |   |
| <b>Rule Count</b> | 214   |

**File Information** ▽

|   |
|---|
| Policy Directory  |
| /opt/hpe/wasl/sms/server/policies/ssg-sle12-xccdf                           |
| XCCDF File  |
| ssg-sle12-xccdf.xml   |
| Tailoring File  |
| tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12.xml |

- To tailor the new policy on the SMS system by using a text editor like vim, edit only the tailoring file.

**Example:**

```
Sms-node: # cd /opt/hpe/wasl/sms/server/policies/ssg-sle12-xccdf
Sms-node: # ll tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12.xml
-rw-rw---- 1 waslsms waslsms 30696 Apr 23 15:29
tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12.xml
Sms-node: # vi tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12.xml
```

---

**NOTE:**

- a. The tailoring file must be owned by **waslsms** user and group.
- b. There are chances that remnant files (like the vim editor swap file) will be created sometimes in the policy directory. Ensure that such files are deleted before you reload the policy to SMS.
- c. You can run the following command to check if any files have user and group other than **waslsms**:  

```
# find . \! -user waslsms  
# find . \! -group waslsms
```

Take appropriate action of either deleting these files or changing the user/group ownership.
- d. Policy tailoring, specifically if you are changing the content of the any of the XCCDF Value/variable using `<set-value>` tag might leave gaps while taking snapshot. For information on snapshot, see **Rollback last Remediation operation on Workload**. It is recommended to test the tailoring done for Policy rollback operation from SMS.

---

**9.** A sample edit of a copied profile is as follows:

- a. Copy the **OS Security Level 1 For SLES 12** security policy to **Custom OS Security Level 1 For SLES 12** security policy.
- b. We will try changing the rules in **Custom OS Security Level 1 For SLES 12** to **change the terminal banner messages and enable remediation (in /etc/issues and /etc/issues.net)**, and also **disable the gnome login banner rules**.

Following is the set of rules related to this:

- `banner_etc_issue` - Check and Modify the System Login Banner (/etc/issue)
- `banner_etc_issue_net` - Check and Modify the System Login Banner (/etc/issue.net)
- `dconf_gnome_banner_enabled` - Checks and Enable gnome login banner
- `dconf_gnome_login_banner_text` - Check and Modify the gnome login banner text

If we do evaluation or remediation of an **OS Security Level 1 For SLES 12** policy, the rule description in the evaluation or remediation reports has details on these rules and the XCCDF variables used by them. Details on these rules and XCCDF variables are also available in the XCCDF file (in this case `ssgs1e12-xccdf.xml` ).

| Modify the System Login Banner (/etc/issue) |  |
|---|--|
| Rule ID                                     | banner_etc_issue   |
| Result                                      | error  |
| Time  | 2017-11-03T08:41:17  |
| Severity                                    | medium   |
| Identifiers and References                  | <p><b>Identifiers:</b> <a href="#">CVE-2017-1000002</a></p> <p><b>References:</b> <a href="#">AC-6(a)</a>, <a href="#">AC-6(b)</a>, <a href="#">AC-6(c)(1)</a>, <a href="#">AC-6(c)(2)</a>, <a href="#">AC-6(c)(3)</a>, 48, <a href="#">SRG-OS-000023-GPOS-00006</a>, <a href="#">SRG-OS-00024-GPOS-00007</a>, <a href="#">C10040</a></p>  |
| Description                                 | <p>To configure the system login banner edit <code>/etc/issue</code>. Replace the default text with a message compliant with the local site policy or a legal disclaimer.</p> <p>This rule checks the contents of <code>/etc/issue</code> with the pattern provided in <code>login_banner_text</code> xccdf variable. The <code>login_banner_text</code> xccdf variable is pre populated with a set of standard login banners. Edit the <code>login_banner_text</code> xccdf variable in the profile, with any specific changes required to the login banner.</p> <p>The remediation is not done automatically and will happen only if the <code>remediate_banner_etc_issue</code> xccdf variable is set to true (Default is false). The remediation will use the banner in <code>login_banner_text</code> xccdf variable, format it and write the contents to <code>etc/issue</code>.</p> <p>Sample DoD required text is either:</p> <p>You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:</p> <ul style="list-style-type: none"> <li>-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMINT monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.</li> <li>-At any time, the USG may inspect and seize data stored on this IS.</li> <li>-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.</li> <li>-This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy.</li> <li>-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.</li> </ul> <p>OR:</p> <p>I've read &amp; consent to terms in IS user agreement.</p> |
| Rationale                                   | Display of a standardized and approved use notification before granting access to the operating system ensures privacy and security notification language used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance. System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.  |
| Remediation/Recovery                        | <p><b>Info</b></p> <p>Fix execution completed and returned: 1</p> <p><b>Info</b></p> <p>This rule is not enabled for automatic remediation. To enable automatic remediation, set the xccdf profile variable "remediate_banner_etc_issue" to true. Ensure that the remediation will not cause any undesired effects on the system.</p> <p><b>Info</b></p> <p>Failed to verify applied fix: Checking engine returns: fail</p> <p><b>Remediation Shell script:</b> <a href="#">(show)</a></p>   |

Only edit the Tailoring file `/opt/hpe/wasl/sms/server/policies/ssg-sle12-xccdf/tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12.xml` in the WASL Virtual Appliance to make all the necessary changes.

- c. The `dconf_gnome_banner_enabled` and `dconf_gnome_login_banner_text` can be disabled by setting the `selected="true"` to `selected="false"` for the following rules:

#### Change from:

```

--
<refine-rule idref="dconf_gnome_login_banner_text" weight="0" />
<select idref="dconf_gnome_login_banner_text" selected="true"></select>
--
<refine-rule idref="dconf_gnome_banner_enabled" weight="0" />
<select idref="dconf_gnome_banner_enabled" selected="true" />
--

```

#### Change to:

```

--
<refine-rule idref="dconf_gnome_login_banner_text" weight="0" />
<select idref="dconf_gnome_login_banner_text" selected="false"></select>
--
<refine-rule idref="dconf_gnome_banner_enabled" weight="0" />
<select idref="dconf_gnome_banner_enabled" selected="false" />
--

```

d. The `banner_etc_issue` and `banner_etc_issue_net` rule depends on the following XCCDF variables:

- **login\_banner\_text:** This variable has the banner text against which evaluation and remediation is done. The default value is set to a banner as prescribed by United States Government Configuration Baseline and identified by "usgcb\_default" idref (ID reference) in the XCCDF file. There are also options to set this to DOD default (identified by "dod\_default" idref) or short (identified by "dod\_short" idref) or DOD Office of Designated Approving Authority DDA (identified by "dod\_odda\_default" idref) login banners.

To use any of the alternative idref ("usgcb\_default", "dod\_default", "dod\_short", "dod\_odda\_default") already available, use `<refine-value>` tag in the tailoring file. However, in this sample we can use `<set-value>` tag, and set the login banner to a different text as follows:

```
<set-value idref="login_banner_text">
This system belongs to Demo corp.
Only authorized users are allowed to Login.
I've read &amp; consent to terms in IS user agreem't.
</set-value>
```

- **remediate\_banner\_etc\_issue:** This variable needs to be set to true to enable remediation on `banner_etc_issue` rule. The default value is "false". The other possible value supported in the XCCDF is "true". In this sample, we can use `<refine-value>` tag in the tailoring file and enable remediation as:

```
<refine-value idref="remediate_banner_etc_issue" selector="true" />
```

- **remediate\_banner\_etc\_issue\_net:** This variable needs to be set to true to enable remediation on `banner_etc_issue_net` rule. The default value is "false". The other possible value supported in the XCCDF is "true". In this sample, we can use `<refine-value>` tag in the tailoring file and enable remediation as:

```
<refine-value idref="remediate_banner_etc_issue_net"
selector="true" />
```

e. The `tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12.xml` after editing will be as follows:

```
<?xml version='1.0' encoding='utf-8'?>
<Tailoring id="xccdf_org.open-scap_tailoring_example"
xmlns="http://checklists.nist.gov/xccdf/1.2">
  <status>incomplete</status>
  <version time="2013-01-15T16:00:00.000+02:00">1.0</version>
  <Profile id="xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12">
    <title>Custom OS Security Level 1 for SLES 12</title>
    <description>Custom policy for organization</description>
    <set-value idref="login_banner_text">
This system belongs to Demo corp.
Only authorized users are allowed to Login.
I've read &amp; consent to terms in IS user agreem't.
</set-value>
    <refine-value idref="remediate_banner_etc_issue" selector="true" />
    <refine-value idref="remediate_banner_etc_issue_net" selector="true" />
    -
    <refine-rule idref="dconf_gnome_login_banner_text" weight="0" />
    <select idref="dconf_gnome_login_banner_text" selected="false"></select> <!-- marked the rule selected to false -->
    -
    <refine-rule idref="dconf_gnome_banner_enabled" weight="0" />
    <select idref="dconf_gnome_banner_enabled" selected="false" /> <!-- marked the rule selected to false -->
    -
  </Profile>
</Tailoring>
```

f. To summarize, the following actions are taken in the tailoring file:

- Set **selected=false** on rules `dconf_gnome_banner_enabled` and `dconf_gnome_login_banner_text`.
- Set the Login banner to be evaluated and remediated to:  

```
This system belongs to Demo corp.
Only authorized users are allowed to Login.
I've read & consent to terms in IS user agreem't
```
- Enabled remediation on "banner\_etc\_issue" and "banner\_etc\_issue\_net" by setting `idref="remediate_banner_etc_issue"` and `idref="remediate_banner_etc_issue_net"` to "true".

← **Custom OS Security Level 1 for SLES 12**

Not deployed on any element

Custom policy

|                   |   |
|-------------------|---|
| <b>Type</b>       | System  |
| <b>Version</b>    | v1.2.0  |
| <b>Platforms</b>  | SUSE Linux Enterprise Server 12<br>SUSE Linux Enterprise Server for SAP Applications 12 |
| <b>Compliance</b> | System security   |
| <b>Workloads</b>  |   |
| <b>Rule Count</b> | 214   |

Copy  
**Reload**  
 Enable  
 Delete

10. Once the tailoring file is edited and saved on WASL Virtual Appliance, the Policy can be reloaded, by clicking on the "Reload" option in the Policy screen. You can note any changes in **Rule Count** if any rules are disabled.

← **Custom OS Security Level 1 for SLES 12**

✓ **Policy Reload**

Monday, 10 December, 2018, 12:07:30 PM  
Completed

Custom policy

|                   |   |
|-------------------|---|
| <b>Type</b>       | System  |
| <b>Version</b>    | v1.2.0  |
| <b>Platforms</b>  | SUSE Linux Enterprise Server 12<br>SUSE Linux Enterprise Server for SAP Applications 12 |
| <b>Compliance</b> | System security   |
| <b>Workloads</b>  |   |
| <b>Rule Count</b> | 212   |

11. This Policy needs to be finally enabled, so that it can be deployed on different workloads.

## Import new policy

### Prerequisites

This option is visible to users with "Administrator" or "Policy Officer" roles.

### Import Security Policies

Do consider the following points before uploading new profiles:

1. The names of archived directory, XCCDF file, JSON file and the resultant archive file should be same.
2. The naming conventions of the profiles inside the XCCDF file should comply with `xccdf_1^_1+profile.+` syntax as per XCCDF 1.2 Specification.
3. JSON file follows the guidelines mentioned in the documentation.
4. Upload file should be less than **100MB** and must be a **.TAR.GZ** or **.ZIP** file.

For detailed information about archive import, please refer policy customization section of the user manual.

Upload .TAR.GZ or .ZIP file

Choose File No file chosen

**Import**

## Procedure

To import new policy.

1. Select the **Policies** option from the left pane.
2. Click **+** symbol.  
A window is displayed to specify the details of security policy to import into Security Management Station (SMS).
3. To import the file into SMS, click **Choose file** option.
4. Read the instructions displayed on the screen carefully.
5. A policy is a ZIP or TAR.GZ file. It consists of four different types of files in a directory:
  - a. XCCDF file, which has the various rules and the profile.
    - I. Profiles are list of rules or list of group of rules present in the XCCDF file. The list is created to achieve specific security protection together.
    - II. For each Profile in the XCCDF, a tailoring file is created by SMS that maps to an SMS Policy. The Name of the profiles must match the pattern as `xccdf_[^#]_profile.+`. For example, `xccdf_sample_profile_1`.
  - b. OVAL and/or Script file that has the implementation for evaluation and remediation of the rules. The OpenSCAP product shipped with WASL on the node to be secured is enabled with Script Check Engine <https://www.open-scap.org/features/other-standards/sce/>. It allows Evaluation of a rule to happen using scripts (like python and shell scripts) along with the OVAL XML files based evaluations.
  - c. JSON file required by SMS to identify the policy name, applicable OS version for the policy and the compliance fulfillment of the policy, Type of Application (Workload). See the Sample JSON file with details at [Sample JSON file used to import policy](#).
  - d. Optional `profile_apis.py` (Python file), primarily to enable snapshot (taken during remediation) and rollback features on a workload for the policy. APIs should be exported from `profile_apis.py` for doing snapshot and rollback. Other APIs also can be exposed from `profile_apis.py`. The APIs get called during Workload Operation for the set of Policies that is getting imported. See the Sample `profile_apis.py` file at [Sample profile\\_apis.py optionally used in importing policy](#).
6. Ensure that the following files have same names with different extensions:
  - a. Names of directory holding the files
  - b. The XCCDF file name
  - c. The JSON file name
  - d. The resultant archive `.tar.gz` or `.zip` file

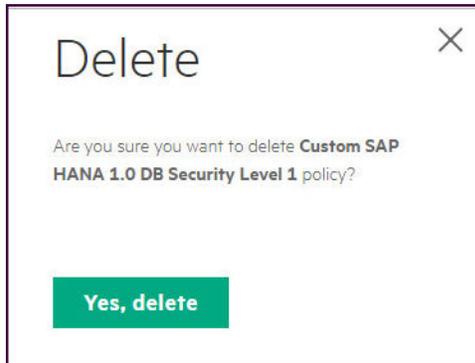
SMS uses this name to identify the different files.
7. On successful completion of **Import** operation, a new policy is registered to SMS. If the policy is not in compliance with XCCDF standards, the import operation is unsuccessful. The respective activity errors logs can be referenced for further actions.
8. The imported policy is displayed in SMS as a **User defined** policy. By default the policy is in disable status. Enable the policy to make it available to deploy on the workload element.

## Delete Policy.

### Prerequisites

This option is visible to users with "Administrator" or "Policy Officer" roles.

Delete Option is not provided to policies that are already deployed once. Even if the policy is undeployed from all workload elements for auditing reasons.



### Procedure

To Delete the policy,

1. Select the **Policies** option from the left pane.  
A list of policies available on SMS is displayed.
2. Select the **User defined** policy that has to be deleted.
3. To delete the policy from SMS, use the **Delete** option.

## Policy update

### Prerequisites

This option is visible to users with 'Administrator' or 'Policy Officer' roles.

| Policies |  | Search | + | ↑ | 11 | ↓       |
|----------|--|--------|---|---|----|---------|
| ●        | OS Security Extras For SAP HANA                      |        |   |   |    | Default |
| ●        | OS Security Level 1 for RHEL 7                       |        |   |   |    | Default |
| ●        | OS Security Level 1 for SLES 12                      |        |   |   |    | Default |
| ●        | OS Security Level 1 for SLES for SAP Applications 12 |        |   |   |    | Default |
| ●        | OS security Level 2 For RHEL 7                       |        |   |   |    | Default |
| ●        | OS Security Level 2 for SLES 12                      |        |   |   |    | Default |
| ●        | OS Security Level 2 for SLES for SAP Applications 12 |        |   |   |    | Default |
| ●        | SAP HANA 1.0 DB Security Level 1                     |        |   |   |    | Default |
| ●        | SAP HANA 1.0 DB Security Level 2                     |        |   |   |    | Default |

## Procedure

To perform Policy update,

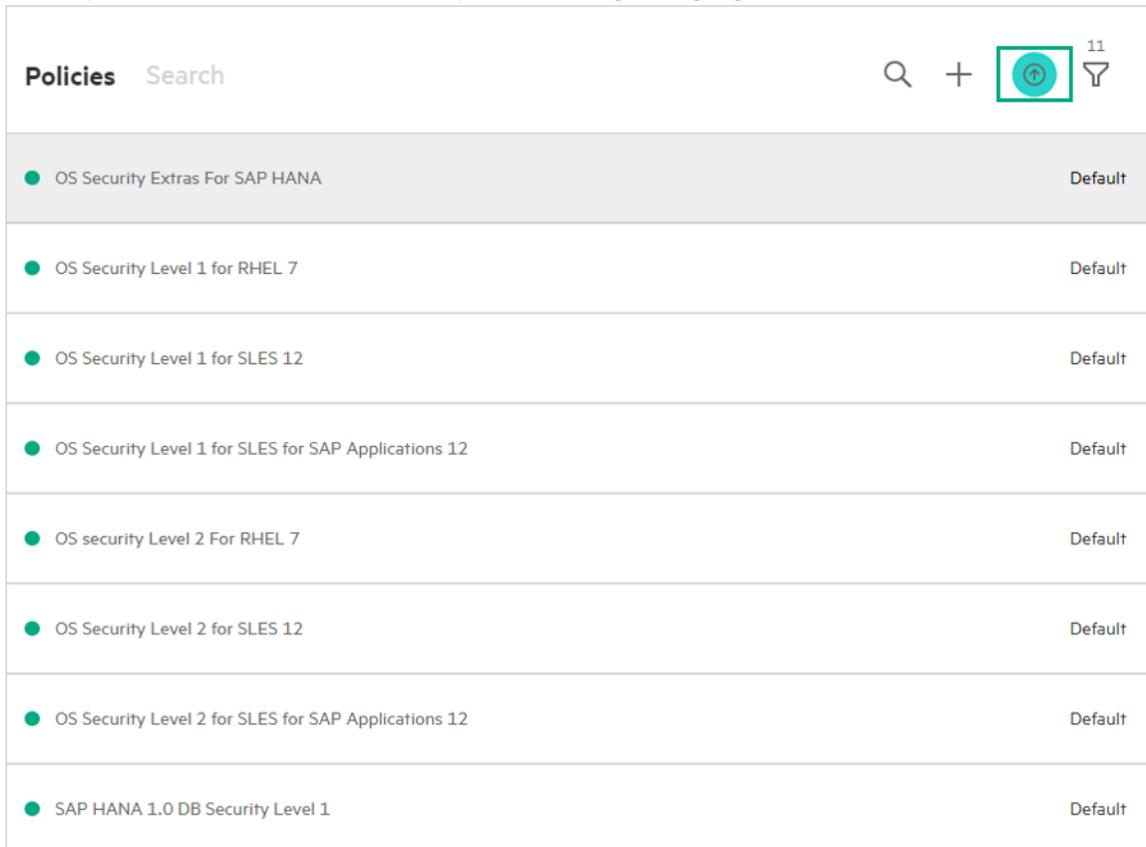
1. Transfer any new policy rpm packages provided to the WASL Virtual Appliance using **wasladmin** user access.
2. Log in to the WASL Virtual Appliance through secure shell or console access as **wasladmin** user.
3. Unlock the **root** user account for a period until you install the new rpm packages:

```
# sudo /opt/hpe/wasl/sms/tools/lockunlock_root.sh -unlock
[sudo] password for wasladmin: <<<<< Enter the password of wasladmin here
Enter the root user Password : <<<<< Enter a new password for root user
Confirm the root user Password : <<<<< Re-Enter the new password once again
root user is enabled with the given password. Please lock the root user after
usage.
```

4. Once the **root** user is unlocked, login to the WASL Virtual Appliance as **root** user using the password set in **Step 3**. Install the policy rpm packages using `yum install <rpm_package>` command.
5. Once the packages are installed, logout of the **root** session.
6. Log in to the WASL Virtual Appliance through secure shell or console access as **wasladmin** user. Lock the **root** user account using the following command:

```
# sudo /opt/hpe/wasl/sms/tools/lockunlock_root.sh -lock
```

7. Wait for around 15 seconds and then check the update button by logging into the SMS.
8. If the updates are available, then the update button gets highlighted.



| Policies Search  |         | 11 |
|--|---------|----|
| ● OS Security Extras For SAP HANA                      | Default |    |
| ● OS Security Level 1 for RHEL 7                       | Default |    |
| ● OS Security Level 1 for SLES 12                      | Default |    |
| ● OS Security Level 1 for SLES for SAP Applications 12 | Default |    |
| ● OS security Level 2 For RHEL 7                       | Default |    |
| ● OS Security Level 2 for SLES 12                      | Default |    |
| ● OS Security Level 2 for SLES for SAP Applications 12 | Default |    |
| ● SAP HANA 1.0 DB Security Level 1                     | Default |    |

9. If the update button is not highlighted, you can make WASL SMS to recheck for updates by logging into WASL Virtual Appliance through Secure Shell/Console as `wasladmin` user and running the following command:

```
# sudo /opt/hpe/wasl/sms/tools/wasl_sms.sh -check_policy_updates
```

10. To see the details of policies to be updated as well as new policies if any, click the update button in SMS GUI.

### Update Security Policies ✕

Update the WASL security policies using the following steps:

1. Install the policy update RPM(s) by logging into the WASL appliance.
2. Any new policies and updates to existing policies will be displayed below. Click on the UPDATE button to load these policies into WASL SMS.
3. For new policies, start deploying them on the workloads.
4. For updated policies, un-deploy them if already deployed on any workload and then deploy the updated policies.

**For more details refer to the user manual.**

| New Policies                               |  | Version |
|--|--|---------|
| OS Security Level 1 for RHEL 7 - sample v2 |  | v1.1    |

| Policies to be Updated         | Current Version | New Version |
|--------------------------------|-----------------|-------------|
| OS Security Level 1 for RHEL 7 | v1.2.1          | v1.2.2      |
| OS security Level 2 For RHEL 7 | v1.2.1          | v1.2.2      |

**Update**

11. To consume the policy update, click the update button

12. Once the policy update is consumed, the final status is displayed.

### Update Security Policies ✕

Update the WASL security policies using the following steps:

1. Install the policy update RPM(s) by logging into the WASL appliance.
2. Any new policies and updates to existing policies will be displayed below. Click on the UPDATE button to load these policies into WASL SMS.
3. For new policies, start deploying them on the workloads.
4. For updated policies, un-deploy them if already deployed on any workload and then deploy the updated policies.

**For more details refer to the user manual.**

| New Policies                               | Version | Status |
|--|---------|--------|
| OS Security Level 1 for RHEL 7 – sample v2 | v1.1    | ✔      |

| Updated Policies               | From Version | To Version | Status |
|--------------------------------|--------------|------------|--------|
| OS Security Level 1 for RHEL 7 | v1.2.1       | v1.2.2     | ✔      |
| OS security Level 2 For RHEL 7 | v1.2.1       | v1.2.2     | ✔      |

✔
Policy Update Successful

Close

13. Check the activity page as well for Policy Update status. For any issues during the update, the Policy Update status on activity page will show "Additional Information".

✔

### Policy Update ✕

By User : 'admin' Dec 4, 2018 10:40 am

Policy Update Successful

| New Policies                               | Version | Status |
|--|---------|--------|
| OS Security Level 1 for RHEL 7 – sample v2 | v1.1    | ✔      |

| Updated Policies               | From Version | To Version | Status |
|--------------------------------|--------------|------------|--------|
| OS Security Level 1 for RHEL 7 | v1.2.1       | v1.2.2     | ✔      |
| OS security Level 2 For RHEL 7 | v1.2.1       | v1.2.2     | ✔      |

14. Click the policy page to see the new policy **OS security Level 1 for RHEL 7 - sample v2** added to the existing policy list.

| Policies <input type="text" value="Search"/>  |  | 12      |
|---|--|---------|
| <span style="color: green;">●</span> OS Security Extras For SAP HANA                      |  | Default |
| <span style="color: green;">●</span> OS Security Level 1 for RHEL 7                       |  | Default |
| <span style="color: green;">●</span> OS Security Level 1 for RHEL 7 - sample v2           |  | Default |
| <span style="color: green;">●</span> OS Security Level 1 for SLES 12                      |  | Default |
| <span style="color: green;">●</span> OS Security Level 1 for SLES for SAP Applications 12 |  | Default |
| <span style="color: green;">●</span> SAP HANA 1.0 DB Security Level 1                     |  | Default |

15. The above steps ensures that SMS has the recent updated policies or new policies loaded. You can start deploying this new or updated policies on any new workloads.
16. On workload having an older version of the updated policy, Un-Deploy the older version and start using the latest version of the Policy. Following are the steps:
  - a. Click workloads where the old policies were deployed. A banner message is displayed as *Policy updates are available. Please check "Deployed Policies."*

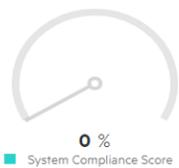
←
RHEL 7.5

✓
Online

Policy updates are available, please check "Deployed Policies."

Security Posture

System Compliance



0 %

■ System Compliance Score

Landscape ▷

Deployed Policies ▷

Recent Activity

- b. Scroll down on the same page and click deployed policies to check policy details. In the example here, two policies by name **OS security Level 1 for RHEL 7** and **OS security Level 2 for RHEL**

7 are deployed with version number 1.2.1 and an updated version of 1.2.2 is available.

Landscape 

---

Deployed Policies 

---

rhel 7.5

| Policy                         | Deployed Version | Current Score (In %) | Update Available |
|--------------------------------|------------------|----------------------|------------------|
| OS Security Level 1 for RHEL 7 | v1.2.1           | Not yet evaluated.   | <b>v1.2.2</b>    |
| OS security Level 2 For RHEL 7 | v1.2.1           | Not yet evaluated.   | <b>v1.2.2</b>    |

Please un-deploy and then deploy the policies to start using the updates.

Recent Activity

- c. Un-deploy these policies and redeploy them to use the latest version of policies.

---

**NOTE:** It is possible that the updated policies might require the latest WASL Node packages to be installed on the Workload. It is recommended to first install the latest Node packages on the Workload before deploying the latest policies.

To install the Node packages automatically, edit the Workload, click on Node element and select "Install Packages". For more information on Installing the Node packages, see the WASL Install and Setup Guide.

---

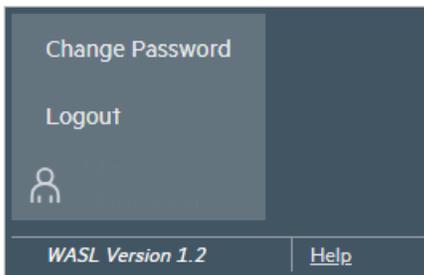
# Session operation and Help

All users who log in to WASL SMS can see the user name and the role that they have logged in. To view user name and role:

1. Click the LeftHand bottom corner screen after the user icon.



2. The following options are displayed:



- **Change Password:** Change the password of the current logged in user. The newly updated password gets applied from next login.
- **Logout:** To log out from SMS.
- **WASL Version:** To identify the version of WASL.
- **Help:** Opens the WASL Help, to view information about each of the WASL screens in SMS.

# Websites

## **General websites**

**Hewlett Packard Enterprise Information Library**

**[www.hpe.com/info/EIL](http://www.hpe.com/info/EIL)**

**Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix**

**[www.hpe.com/storage/spock](http://www.hpe.com/storage/spock)**

**Storage white papers and analyst reports**

**[www.hpe.com/storage/whitepapers](http://www.hpe.com/storage/whitepapers)**

For additional websites, see **[Support and other resources](#)**.

# Support and other resources

## Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:  
<http://www.hpe.com/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:  
<http://www.hpe.com/support/hpesc>

### Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

## Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:  
**Hewlett Packard Enterprise Support Center**  
[www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)  
**Hewlett Packard Enterprise Support Center: Software downloads**  
[www.hpe.com/support/downloads](http://www.hpe.com/support/downloads)  
**Software Depot**  
[www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)
- To subscribe to eNewsletters and alerts:  
[www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:  
[www.hpe.com/support/AccessToSupportMaterials](http://www.hpe.com/support/AccessToSupportMaterials)

---

**!** **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

---

## Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

<http://www.hpe.com/support/selfrepair>

## Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

### Remote support and Proactive Care information

#### HPE Get Connected

[www.hpe.com/services/getconnected](http://www.hpe.com/services/getconnected)

#### HPE Proactive Care services

[www.hpe.com/services/proactivecare](http://www.hpe.com/services/proactivecare)

#### HPE Proactive Care service: Supported products list

[www.hpe.com/services/proactivecaresupportedproducts](http://www.hpe.com/services/proactivecaresupportedproducts)

#### HPE Proactive Care advanced service: Supported products list

[www.hpe.com/services/proactivecareadvancedsupportedproducts](http://www.hpe.com/services/proactivecareadvancedsupportedproducts)

#### Proactive Care customer information

##### Proactive Care central

[www.hpe.com/services/proactivecarecentral](http://www.hpe.com/services/proactivecarecentral)

##### Proactive Care service activation

[www.hpe.com/services/proactivecarecentralgetstarted](http://www.hpe.com/services/proactivecarecentralgetstarted)

## Warranty information

To view the warranty information for your product, see the links provided below:

#### HPE ProLiant and IA-32 Servers and Options

[www.hpe.com/support/ProLiantServers-Warranties](http://www.hpe.com/support/ProLiantServers-Warranties)

#### HPE Enterprise and Cloudline Servers

[www.hpe.com/support/EnterpriseServers-Warranties](http://www.hpe.com/support/EnterpriseServers-Warranties)

#### HPE Storage Products

[www.hpe.com/support/Storage-Warranties](http://www.hpe.com/support/Storage-Warranties)

#### HPE Networking Products

[www.hpe.com/support/Networking-Warranties](http://www.hpe.com/support/Networking-Warranties)

# Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

[www.hpe.com/support/Safety-Compliance-EnterpriseProducts](http://www.hpe.com/support/Safety-Compliance-EnterpriseProducts)

## Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

[www.hpe.com/info/reach](http://www.hpe.com/info/reach)

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

[www.hpe.com/info/ecodata](http://www.hpe.com/info/ecodata)

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

[www.hpe.com/info/environment](http://www.hpe.com/info/environment)

# Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hpe.com](mailto:docsfeedback@hpe.com)). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

# Sample JSON file used to import policy

Following is a sample JSON file used during policy import:

```
[
{
  "id": "xccdf_sles12-c4s11_profile_default",
  "info": {
    "version": "v1.1",
    "xccdf_file": "ssg-sle12-xccdf.xml",
    "applicable_platforms": ["SUSE Linux Enterprise Server
12", "SUSE Linux Enterprise Server for SAP Applications 12"],
    "applicable_compliance": ["System security"],
    "type": "System" }
},
{
  "id": "xccdf_sles12-c4s12_profile_default",
  "info": {
    "version": "v1.1",
    "xccdf_file": "ssg-sle12-xccdf.xml",
    "applicable_platforms": ["SUSE Linux Enterprise Server
12", "SUSE Linux Enterprise Server for SAP Applications 12"],
    "applicable_compliance": ["System security"],
    "type": "System" }
}
]
```

Here:

**id:** Should point to one of the profile defined in the XCCDF file. I.e. In the above example, the corresponding XCCDF file should have the following entry:

```
<Profile id="xccdf_sles12-c4s11_profile_default">
-
-
</Profile>
```

SMS looks up in the XCCDF file for this profile, validate, and load it as a policy in SMS. The **<title>** in the XCCDF file is used to identify the Policy. This profile title should be unique across all profiles in the XCCDF file. Multiple profiles presented in the XCCDF file is specified as multiple blocks of the JSON file separated by curly braces `{}` (displayed in the example).

- **Version:** Version of the Policy
- **xccdf\_file:** Name of the XCCDF file for corresponding policy
- **applicable\_platforms:** The Operating System versions on which the policy can be deployed. This version maps to "PRETTY\_NAME" filed in /etc/os-release file on the end Node.
- **applicable\_workloads:** If the Policy type is Application, then the Workload entry indicates the type of application which this policy secures. Example: "SAP HANA".
- **applicable\_compliance:** Indicates if the Policy addresses some compliances.
- **type:** Type "System" indicates that the Policy is for system compliance (that is. compliance of the Node element of Workload). Type "Application" indicates that the Policy is for Application compliance (like compliance of SAP HANA System element of Workload).

# Sample profile\_apis.py optionally used in importing policy

```
# (c)Copyright 2017 Hewlett Packard Enterprise Development LP
import sys,os,pwd,json,importlib

import common.helper
import common.workload_helper
from common.workload_helper import raise_error

import common.text_logger
from common.text_logger import get_logger

from config.core_config import SS_POLICY,LIB_PATH

from config.core_config import SNAPSHOT_LOCATION,SS_POLICY,LOGGER_NAME,SS_LOG_PATH,TMP_PATH

logger = get_logger(LOGGER_NAME)

policy_type = "hana"    # can be either hana or system currently

'''
Define generic entry points
'''
#
# This API gets called before multiple operations to get a
# descriptive name of the workload
#
def workload_descriptive_name():
    return "Sample Workload"

#
# This API gets called before multiple operations of SMS like
# policy evaluation, remediation, rollback.
#
# This API can implement different validation logic
# to check if the system or application that needs to
# to be secured is running properly.
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
#
# For SAP HANA workload type, provide following API:
# def validate_hana():
# For SYSTEM workload type, provide following API:
# def validate_system():
def validate_hana():
    try:
        logger.debug("Perform Validation here")
    except Exception,e:
        raise_error("Error occurred during validation:"+str(e))

#
#
# This API gets called after the policy is deployed.
#
# This API can implement checks to perform post deployment
# activity.
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS.
# On calling a raise_error(), the deploy operation is indicated
# as a failure and the policy will be removed from the
# target deployed directory.
#
def validate_deploy(profile_name, target_profile_dir_deployed):
    try:
```

```

        logger.debug("Perform post deploy check here")
    except Exception,e:
        raise_error("Error occurred during deploy:"+str(e))

#
# This API gets called during the SMS evaluation operation, before
# the evaluation operation is performed on a policy
#
# Following are the different arguments passed:
# 1) profile_name - Name of the Profile
# 2) xccdf_file - XCCDF file name
# 3) tailor_file - Name of the tailoring file
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def pre_evaluate(profile_name,xccdf_file=None,tailor_file=None):
    base_policy_path=SS_POLICY+"/"+policy_type+"/"+profile_name
    try:
        logger.debug("Perform pre evaluation here")
    except Exception,e:
        raise_error("Error occurred during pre evaluation:"+str(e))

#
# This API gets called during the SMS evaluation operation, after
# the evaluation operation is performed on a policy
#
# Following are the different arguments passed:
# 1) primary_status - The status of the evaluate operation. zero
# indicates a success. Any other status apart from zero is an error.
# See /opt/hpe/wasl/core/common/error.py on an end Node to see the list
# of status.
# 2) secondary_status - The secondary status of the evaluate operation.
# zero indicates a success. Any other status apart from zero is an
# error.
# 3) profile_name - Name of the Profile
# 4) xccdf_file - XCCDF file name
# 5) tailor_file - Name of the tailoring file
# 6) report_file - The HTML report file that is generated and having the
# evaluation report (output of OpenSCAP evaluation)
# 7) result_file - The XML XCCDF evaluation result (output of OpenSCAP
# evaluation)
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
#
def post_evaluate(primary_status,secondary_status,profile_name,
    xccdf_file=None,tailor_file=None,report_file=None,result_file=None):
    base_policy_path=SS_POLICY+"/"+policy_type+"/"+profile_name
    try:
        logger.debug("Perform post evaluation here")
    except Exception,e:
        raise_error("Error occurred during post evaluation:"+str(e))

#
# This API gets called during the SMS remediation operation, before
# the remediation operation is performed on a policy
#
# Following are the different arguments passed:
# 1) profile_name - Name of the Profile
# 2) xccdf_file - XCCDF file name
# 3) tailor_file - Name of the tailoring file
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def pre_remediate(profile_name,xccdf_file=None,tailor_file=None):
    base_policy_path=SS_POLICY+"/"+policy_type+"/"+profile_name
    try:
        logger.debug("Perform pre remediation here")
    except Exception,e:

```

```

        raise_error("Error occurred during pre remediation:"+str(e))

#
# This API gets called during the SMS remediation operation, before
# the remediation operation and after pre_remediate() API is called.
#
# The Snapshot i.e. the configuration state of the different files,
# sysctl parameters, other configuration which the policy is expected
# to remediate, should be collected and stored in snapshot_dir in
# snapshot() API.
# The rollback() API should be able to revert this collect configuration
# state back on the system.
#
# Following are the different arguments passed:
# 1) snapshot_dir - The directory to which snapshot should be taken
# (With path). This is same as:
#     SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id
# 2) snapshot_id - The final snapshot directory
# 3) reports - not used currently
#
# The Policy XCCDF, OVAL, Scripts, including this profile_apis.py will be
# stored in SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy"
# directory while before snapshot() API.
#
# Before calling this API, the details of the Policy, like profile name
# gets stored in file:
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy/profile.dat"
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def snapshot(snapshot_dir,snapshot_id=None,reports=None):
    try:
        logger.debug("Perform configuration snapshot here")
    except Exception,e:
        raise_error("Error occurred during snapshot:"+str(e))

#
# This API gets called during the SMS remediation operation, after
# the remediation operation is performed on a policy
#
# Following are the different arguments passed:
# 1) primary_status - The status of the remediate operation. zero
# indicates a success. Any other status apart from zero is an error.
# See /opt/hpe/wasl/core/common/error.py on an end Node to see the list
# of status.
# 2) secondary_status - The secondary status of the remediate operation.
# zero indicates a success. Any other status apart from zero is an
# error.
# 3) profile_name - Name of the Profile
# 4) xccdf_file - XCCDF file name
# 5) tailor_file - Name of the tailoring file
# 6) report_file - The HTML report file that is generated and having the
# remediation report (output of OpenSCAP remediation)
# 7) result_file - The XML XCCDF remediation result (output of OpenSCAP
# remediation)
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def post_remediate(primary_status,secondary_status,profile_name,
    xccdf_file=None,tailor_file=None,report_file=None,result_file=None,
    snapshot_id=None):
    base_policy_path=SS_POLICY+"/"+policy_type+"/"+profile_name
    try:
        logger.debug("Perform post remediation here")
    except Exception,e:
        raise_error("Error occurred during post remediation:"+str(e))

#
# This API gets called during the SMS rollback operation, before
# the rollback operation is performed on a policy.

```

```

#
# Following are the different arguments passed:
# 1) snapshot_id - The final snapshot directory.
#
# The complete snapshot directory having the snapshot of configuration
# stored in snapshot() API will be present here:
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id
#
# The Policy XCCDF, OVAL, Scripts, including this profile_apis.py will be
# stored in SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy"
# directory while before snapshot() API.
# This current API will be invoked from profile_apis.py stored in
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy" directory.
#
# Before calling this API, the details of the Policy, like profile name
# gets stored in file:
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy/profile.dat"
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def pre_rollback(snapshot_id):
    try:
        logger.debug("Perform pre rollback here")
    except Exception,e:
        raise_error("Error occurred during pre rollback:"+str(e))

#
# This API gets called during the SMS rollback operation, after
# the rollback operation is performed on a policy.
#
# Following are the different arguments passed:
# 1) primary_status - The status of the rollback operation. zero
# indicates a success. Any other status apart from zero is an error.
# See /opt/hpe/wasl/core/common/error.py on an end Node to see the list
# of status.
# 2) secondary_status - The secondary status of the rollback operation.
# zero indicates a success. Any other status apart from zero is an
# error.
# 3) snapshot_id - The final snapshot directory.
#
#
# The complete snapshot directory having the snapshot of configuration
# stored in snapshot() API will be present here:
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id
#
# The Policy XCCDF, OVAL, Scripts, including this profile_apis.py will be
# stored in SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy"
# directory while before snapshot() API.
# This current API will be invoked from profile_apis.py stored in
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy" directory.
#
# Before calling this API, the details of the Policy, like profile name
# gets stored in file:
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy/profile.dat"
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def post_rollback(primary_status,secondary_status,snapshot_id):
    try:
        logger.debug("Perform post rollback here")
    except Exception,e:
        raise_error("Error occurred during post rollback:"+str(e))

#
# This API gets called during the SMS rollback operation.
#
# The Snapshot i.e. the configuration state of the different files,
# sysctl parameters, other configuration which the policy is expected
# to remediate, should be collected and stored in snapshot_dir in

```

```

# snapshot() API.
# The rollback() API should be able to revert this collect configuration
# state back on the system.
#
# Following are the different arguments passed:
# 1) snapshot_dir - The directory to which snapshot was taken
#    (With path) that should be reverted back. This is same as:
#    SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id
# 2) snapshot_id - The final snapshot directory
# 3) reports - not used currently
#
# The Policy XCCDF, OVAL, Scripts, including this profile_apis.py will be
# stored in SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy"
# directory while before snapshot() API.
# This current API will be invoked from profile_apis.py stored in
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy" directory.
#
# Before calling this API, the details of the Policy, like profile name
# gets stored in file:
# SNAPSHOT_LOCATION+"/"+policy_type+"/"+snapshot_id+"/policy/profile.dat"
#
# call raise_error(<string_message>), in order to indicate a
# failure of this API. The <string_message> will be displayed to
# end users of SMS
#
def rollback(snapshot_path,snapshot_id=None,reports=None):
    try:
        logger.debug("Perform rollback of configuration here")
    except Exception,e:
        raise_error("Error occurred during rollback:"+str(e))

```

# Acronyms

| <b>Acronym</b> | <b>Definition</b>                                     |
|----------------|---|
| WASL           | Workload Aware Security for Linux                     |
| SMS            | Security Management Station                           |
| RHEL           | Red Hat Enterprise Linux                              |
| SLES           | SUSE Linux Enterprise Server                          |
| SAP HANA       | SAP High Performance Analytic Appliance               |
| TDI            | Tailored Data Center Integration                      |
| SP1, SP2, SP3  | Service Pack 1, Service Pack 2, Service Pack 3        |
| CS 500 / 900   | ConvergedSystem 500 / 900                             |
| XCCDF          | Extensible Configuration Checklist Description Format |
| GUI            | Graphical User Interface                              |
| OpenSCAP       | Open Security Containment and Automation Protocol     |
| OVAL           | Open Vulnerability and Assessment Language            |
| FTP            | File Transfer Protocol                                |
| DB             | Database  |
| SSH            | Secure Shell  |
| REST           | Representational State Transfer                       |
| SFTP           | Secure File Transfer Protocol                         |