Hewlett Packard Enterprise

HPE Workload Aware Security for Linux (WASL) 1.0 version User Guide

Abstract

This document describes the user operations available on the version 1.0 of Workload Aware Security for Linux 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.

Acknowledgements

Linux® is a registered Trademark of Linus Torvalds in the U.S. and other countries.

Red Hat® Enterprise Linux® is the registered Trademark of Red Hat® Inc.

SUSE and the SUSE logo are registered trademarks of SUSE LLC in the United States and other countries.

SAP and SAP HANA are registered trademarks of SAP SE in Germany and other countries.

Couchbase® is the registered Trademark of Couchbase, Inc.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

1   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 on the operating system together by a single-click from centralized system (called Security Management Station). WASL can evaluate a workload (just 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 from which details of specific evaluations and remediation can be easily obtained. WASL also offers a feature to rollback any remediation done and get back the workload configuration to a previously known configuration state.

WASL is shipped with basic license offering SLES and RHEL OS hardening policies and advanced licensing offering SAP HANA policies in addition to basic licensing.

WASL uses policies based on the global benchmark standards (XCCDF) and currently provides the following standard policies:

- OS Security for SLES 12 (SP1)
- OS Security for SLES SAP Applications 12 (SP1) (OS Security for SLES 12 SP1 tailored for SAP HANA database)
- OS Security for RHEL 7.2
- SAP HANA 1.0 Database
- SAP HANA 2.0 Database
- OS Security Extras for SAP HANA (SLES 12 SP1) (extra OS protection for securing SAP HANA database)

1.1   WASL Deployment and Architecture

A typical deployment of WASL consists of a Security Management Station (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 workload in the following ways:

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

The Security Management Station (SMS) is a web based application accessible on HTTPS port (default port is 8116). It offers a rich set of GUI that is accessible by a Chrome web browser and supports a varied set of roles for users to login and perform activities.
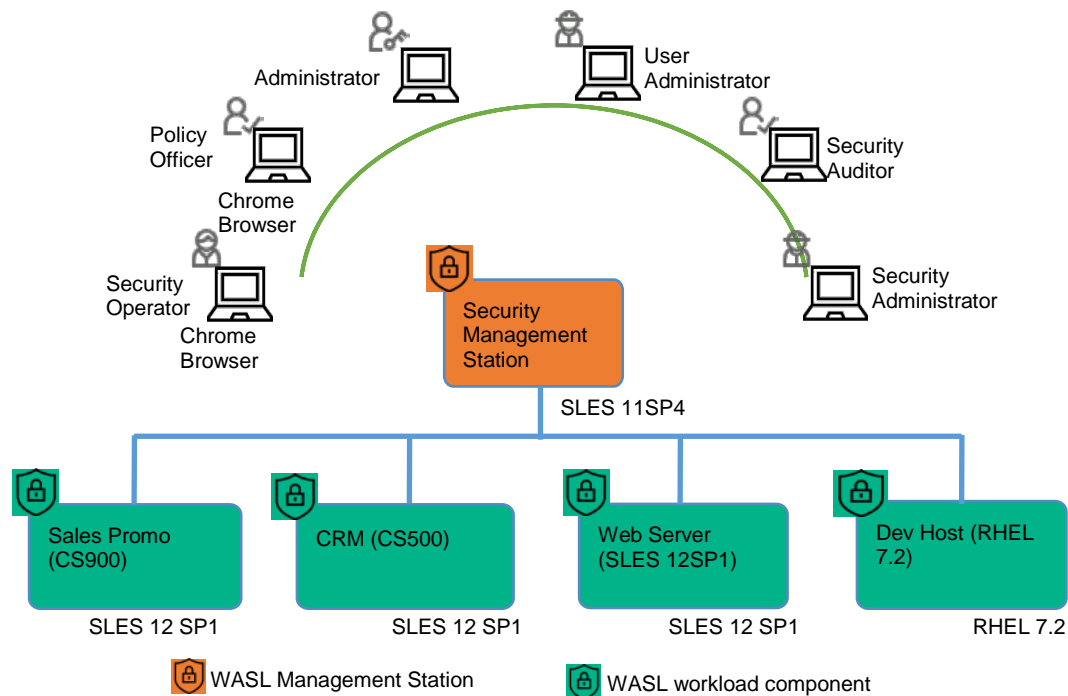

Figure 1: Typical WASL Deployment Scenario

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 also provides an

ability to 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 the application running on the OS.

SMS stores information related to workloads in Couchbase server NOSQL database (accessible via 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 a 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.
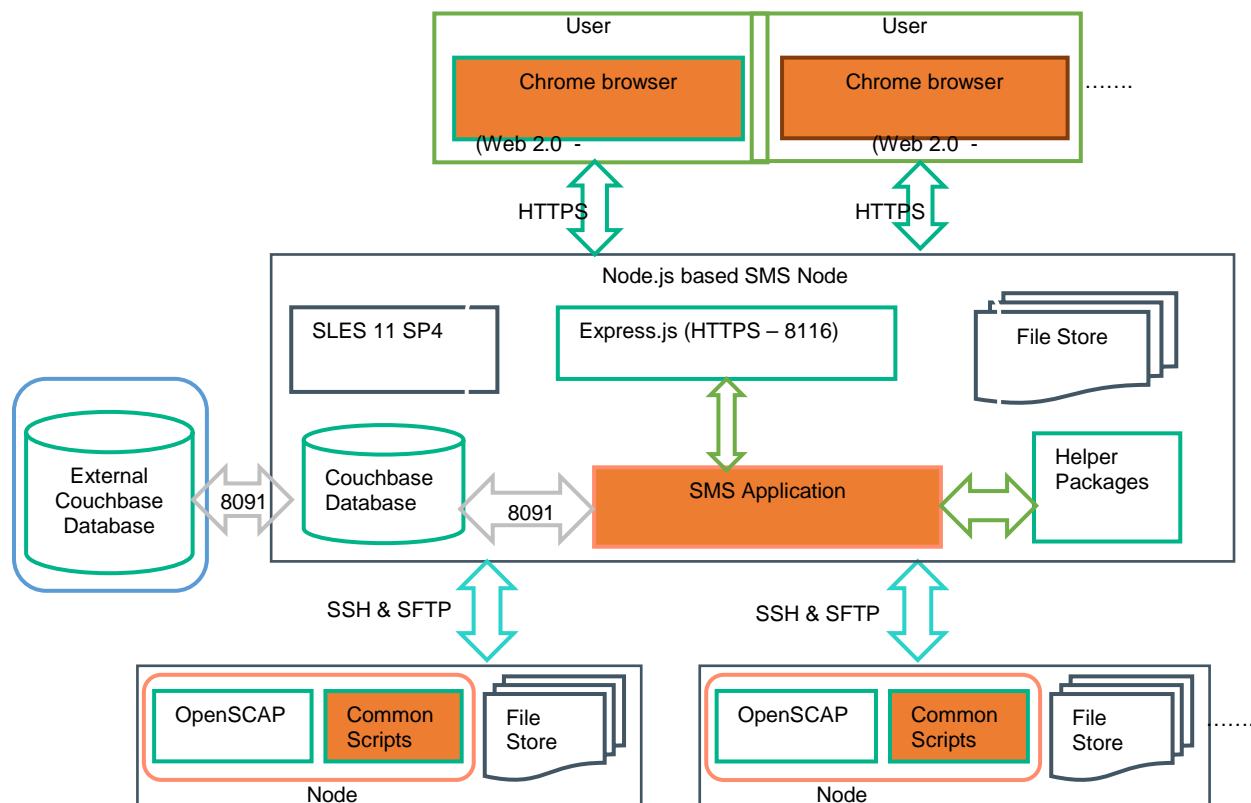
Figure 2: WASL Architecture flow

1.2   SMS Login

Follow the WASL Install and Setup Guide first to install the WASL product. Once the product is installed and running, use Chrome browser to access the SMS at the URL https://<IPAddress of SMS host>:8116 (8116 is the default port used by WASL to expose the web interface). User can authenticate to SMS using the default administrator account username="admin" and password="admin".

You are prompted to change the password on first login. Use this account for admin purposes only. It is recommended to add other SMS user with different roles to perform operations in SMS.

1.3   User Roles

After completing the installation and setup of WASL, it is recommended to create users with appropriate role and access credentials to connect to SMS using a Chrome browser. The type of user role limits the kind of operations that can be performed by the user. The details of these Operations are provided in the "WASL Configuration and Operations" section of this guide. The following table lists the role-based operations allowed for each user role.

Role Name	Operation Name	Operations Permitted
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
		Policy Customization (Copy→Edit→Reload Policy, Import or Delete Policy)
Security Operator	Workload Operations	View, Evaluate, Remediate, Rollback and Search Workload
	View Details	View and Search SMS Activities
		View Dashboard
Security Administrator	Workload Management	Add, Edit, Disable Workload
		Deploy, Undeploy policies on a Workload
	Workload Operations	View, Evaluate, Remediate, Rollback, Reset and Search Workload
	View Details	View and Search SMS Activities
		View Dashboard
Security Auditor	Workload Operations	Only View, Evaluate and Search Workload
	View Details	View and Search SMS Activities
		View Dashboard
Administrator	All Operations	Capability to perform operations related to all roles.
		Additional capability to edit SMS settings
		This role is provided to only "admin" user

2 WASL Configuration and Operations

This section lists the various configurations and operations allowed from SMS.

2.1   Workload Management

Workload Management involves the following:

- Adding or Register a Workload in SMS
  - o   Do automatic Installation of WASL packages on End node during Registration
- Deploy and Undeploy the security policies on the Workload
- Edit Workload
- Disable Workload

2.1.1   Add or Register Workload

This option is visible to users who login as 'Administrator' or 'Security Administrator' role. Register a new workload on clicking the **+** icon on top right once you are in **Workloads** tab.
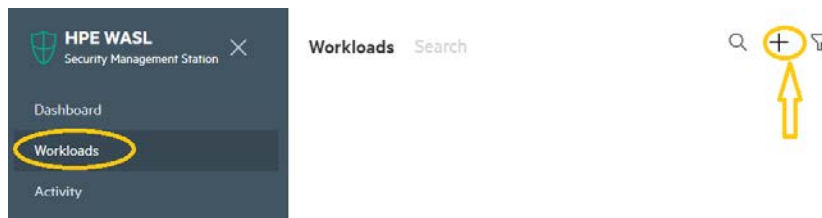
Enter the **Workload Type**. The type can be "**Operating System Only**" or "**SAP HANA Scale-up System**".
Enter the **Workload Name**. The Workload name is used to reference the workload on SMS screen.

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

Incase **Workload Type** is selected as "**Operating System Only**", only a **Node** element is displayed in **Register Workload** screen. If **Workload Type** is selected as "**SAP HANA Scale-up System**", then both **Node** and **SAP HANA System** elements are displayed.

The workload can be re-configured in future using **Edit workload** option after it is registered to SMS.

2.1.1.1   Add Operating System Only Workload

To secure only the Operating system running on the Node, select **Workload Type** as "**Operating System Only**" and enter the Workload Name. Select the **+** sign after the **Node** element. You will be prompted with the **Add Node** screen.

Enter the details of Node. It includes the following:

Host Name: Enter the Host name of the Node here.

IP address: Enter the Node's IP address. (Currently only IPV4 address is supported). WASL uses this IP address to SSH to end Node and perform Node Package installation and Setup (if **Install Package** is turned on in the **Add Node** screen above) and do workload operation like evaluation, remediation, rollback, reset etc on the Node.

Platform: Select the appropriate Operating System version running on the Node. WASL uses this Platform information to display the appropriate security Policies that can be deployed on this workload during Deploy Policy operation.

Host Username: Enter the Operating system user name on the Node. The **Host Username** is used by WASL to connect to Node via SSH to perform Node Package installation and Setup (if **Install Package** is turned on in the **Add Node** screen above), and do workload operation like evaluation, remediation, rollback, reset etc. on this Node.

Host Password: The password for the **Host Username**

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

Install Package: If turned on, WASL Node Packages are automatically installed and setup on the Node.

If you have turned on the **Install Package** in the **Add Node** above and **Host Username** is not "root" user, then you need to provide capability to the **Host Username** to sudo as "root" for performing WASL Node package installation and setup command. For steps required 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** in the **Add Node** above, you need to explicitly install and Setup the WASL Node Packages on the Node before doing Workload Register here. You also need to provide capability for **Host Username** to sudo as "root" and perform Workload Operation (Like Evaluate, Remediate, Rollback and Reset) on this Node. Refer to the "Manual Node Package installation and setup from Node" section in WASL Install and Setup guide for details on how this is done.

Click on "**OK**" and register the workload to SMS.

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

- WASL adds a new workload entry (Identified by the **Workload Name**) in the **Workload** page

- WASL also does a SSH to the end node and validate if the details provided in **Add Node** screen is correct
- WASL then tries to Install the Setup the Node Packages if the **Install Package** in the **Add Node** screen is turned on
- You can click on the new workload entry added to know the status
- The status will be updated at the following places
  - o The Taskbar at the top of the workload entry page in case of error
  - o The "Recent Activity" at the bottom of the workload entry page
- The status also gets updated in the "**Activity**" page of WASL.

2.1.1.2   Add SAP HANA Scale-up System Workload

On selecting Workload Type as "**SAP HANA Scale-up System**", along with **Node**, **SAP HANA System** element is also displayed.

Select the **+** sign after the **Node** element. You will be prompted with the **Add Node** screen. Follow the same steps as mentioned in the "Add Operating System Only Workload" section to add the Node details.

Select the **+** sign after the **SAP HANA System** element. You will be prompted with the **Add SAP HANA System** screen.

Enter the details of SAP HANA System Database. It includes the following:

SAP HANA System ID: Specify the SAP HANA system identifier (SID) of SAP HANA database. (Example: HDB, SEQ, etc.)

SAP HANA Instance ID: Specify the Instance Number of the SAP HANA system (example: 00, 01)

SAP HANA DB Username: Specify the SAP HANA Database username here. WASL uses this user name to connect to SAP HANA Database for doing any Workload Operation on this SAP HANA System Database. The **SAP HANA DB Username** can be the "SYSTEM" database user or any SAP HANA database user who is granted 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 (This
privilege is required in case SAP HANA database version is 2.0 or higher)
```

Replace the <SAP HANA DB Username> above with the actual user name supplied in **SAP HANA DB Username** field**,** if you are planning to use the above SAP HANA SQL command, to grant any user with privileges.

SAP HANA DB Password: The password for the **SAP HANA DB Username.**

Host Username: This can be any non-privileged OS users on the Node where SAP HANA is installed.

WASL does all Workload Operations on the SAP HANA System Database by first logging into the Node using this **Host Username** via SSH (it also uses the IP address provided in the **Add Node** screen) and doing sudo to "waslhanauser" user on the Node. The "waslhanauser" user then connects to the SAP HANA System Database using the **SAP HANA System ID, SAP HANA Instance ID, SAP HANA DB Username** and **SAP HANA DB Password** provided above.

The "waslhanauser" is a non-privileged user created as a part of WASL Node Package installation and Setup (See WASL Install and Setup guide on what happens during Node Package installation and Setup). This installation and Setup is done automatically if **Install Package** option is turned on in the **Add Node** screen above. The installation and Setup of Node Packages does the following:

- Provides the ability for **Host Username** above to sudo to waslhanauser for performing Workload Operation (Like Evaluate, Remediate, Rollback and Reset) on the SAP HANA System Database
- Create certificate for waslhanauser that is signed by the SAP HANA server certificate. This signed certificate is required if SAP HANA database supports only encrypted communication over SSL.
  - o This signed certificate is valid for one year. The certificate gets automatically regenerated, if you Edit the Workload and select **Install Package** option in the **Add Node** screen once again and save the Workload.

The "waslhanauser" requires SAP HANA Client - HDB_CLIENT tool that is provide as a part of SAP HANA database to be installed on the system to connect to the SAP HANA database. You can check if this tool is installed, by checking if the file /usr/sap/hdbclient/hdbcli/dbapi.py is existing on the Node. In case you do not want to install this tool, you can avoid using "waslhanauser" during Workload Operation on SAP HANA database by using the <SID>adm OS user instead ("<SID>adm" OS user is created by SAP HANA for administration operation on SAP HANA database. <SID> is the SAP HANA System ID). You should add **{sidadm=yes}** tag in the **Tags** filed of this **Add System DB** screen to achieve this. In this case all SAP HANA database workload operation is carried out as follows: **Host Username** does a sudo to <SID>adm user which in turn connects to the SAP HANA database using the details provided above. The ability for **Host Username** to do a sudo to <SID>adm is added during the Installation and Setup of WASL Node package. Do not change the **Tags** file to add or remove the **{sidadm=yes}** tag after you have deployed the policies on the workload by editing the Workload, as this might lead to file permission issues on the Node.

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

Tags: You can optionally provide some extra Tag's to for identifying this Node.

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

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

- WASL adds a new workload entry (Identified by the **Workload Name**) in the **Workload** page
- WASL also does a SSH to the end node and validate if the details provided in **Add Node** screen is correct
- WASL then tries to Install the Setup the Node Packages if the **Install Package** in the **Add Node** screen is selected
- WASL also does a SSH to the end node (using the credentials provided in **Add SAP HANA System** screen) and validate 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.
- You can click on the new workload entry added to know the status
- The status will be updated at the following places
  - o The Taskbar at the top of the workload entry page in case of error

-    The status also gets updated in the "**Activity**" page of WASL.

2.1.2 Edit Workload

This option is visible to users who login as 'Administrator' or 'Security Administrator' role. The screens, options and parameters provided are similar to details provided during "Add or Register Workload". All the workload parameters except few parameters like **Workload Name**, **Platform** can be updated.

On clicking "save" after editing a workload, WASL connects to the Node and validating the workload. This operation is similar to what is done during Add or Register Workload. WASL also does Install and Setup of the Node Packages if the **Install Package** is turned on in the **Edit** screen of the **Node**.

There are cases where a Workload is moved to "Unknown" state in WASL, if the Node is not reachable over network or Workload validation fails during any Workload Operations. The Workload can be brought back again into Online state by Editing and saving the workload. If the workload parameters are changed, the parameters can be modified and **Install Package** can be selected in the **Edit** screen of the **Node**, to do an Install and setup once again.

2.1.3 Deploy Security Policy

This option is visible to users who login as 'Administrator' or 'Security Administrator' role. You can deploy security policies on a workload by first clicking on the specific workload, in the **Workload** Page and then selecting the "**Deploy Policy**" Option.

The Deploy Policy screen has 2 options displayed on the screen. **Choose an element** and **Choose a policy.**

The **Choose an element** pull-down shows the Workload elements that are configured on the workload during "Add or Register Workload" operation. It can be the Node (Shown as MasterNode) or SAP HANA System (Shown as SystemDB).
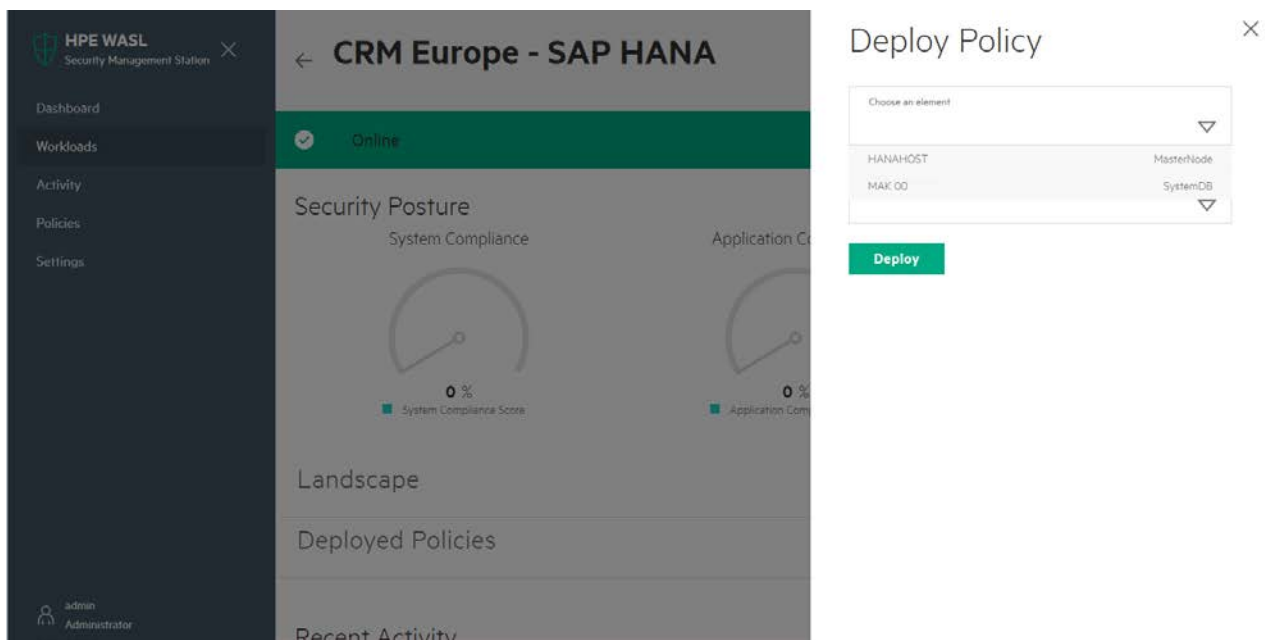
The **Choose a policy** pull-down lists the Policies that are applicable on the Workload element selected via **Choose an element**. (Policies that are already deployed on the Workload elements are not displayed in the pull-down).
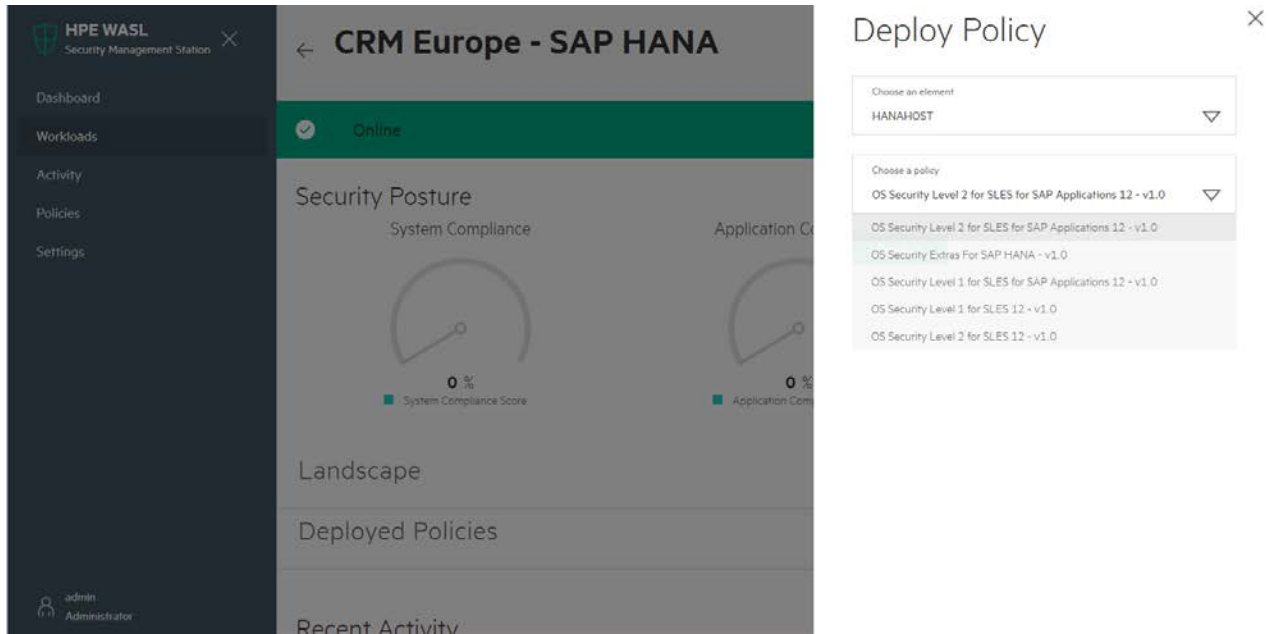
On Clicking "**Deploy**" button in the Deploy Policy page, WASL transfers the policy related files to the Node having the workload and validate the workload settings.

2.1.3.1 Deploy multiple policies on Workload

Follow the same sequence of steps as mentioned in the "Deploy Security Policy" section to deploy additional policies on the workload. A list of all the policies deployed on the workload can be seen from on selecting the workload and clicking the **Deployed Policies** in the central pane.

Click on the workload name from the Workload tab to view the details. Click on the arrow next to **Deployed Policies** option on the screen. A list of all the policies deployed on the workload is shown here.

2.1.4 Undeploy or Remove security policy from workload

This option is visible to users who login as 'Administrator' or 'Security Administrator' role. You can Undeploy security policies that was originally deployed on a workload by first clicking on the specific workload, in the **Workload** Page and then selecting the "**Undeploy Policy**" Option.

The Undeploy Policy screen has 2 options displayed on the screen. **Choose an element** and **Choose a policy.**

The **Choose an element** pull-down shows the Workload elements that are configured on the workload during "Add or Register Workload" operation. It can be the Node (Shown as MasterNode) or SAP HANA System (Shown as SystemDB).

The **Choose a policy** pull-down lists the Policies that are deployed on the Workload element selected via **Choose an element**.
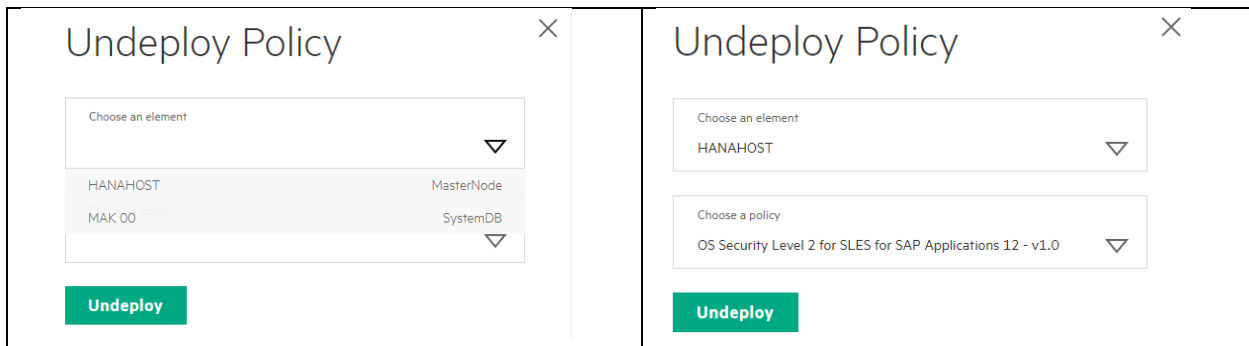
On Clicking "**Undeploy**" button in the Undeploy Policy page, WASL removes the policy related files on the Node.

2.1.5 Disable workload

This option is visible to users who login as 'Administrator' or 'Security Administrator' role. You can disable a workload by first clicking on the specific workload, in the **Workload** Page and then selecting the "**Disable**" Option.

Disable   ✕

Note: Edit the workload [✏ **Edit**] to re-enable if needed.

Are you sure you want to disable workload **CRM Europe - SAP HANA**?

Yes, disable

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.

2.2 Workloads Operations

2.2.1 View Workload Details

This option is visible to users who login as 'Administrator', 'Security Administrator', 'Security Operator' or 'Security Auditor' role. You can view the details of a workload by clicking on the specific workload in the **Workload** Page. It displays the following:
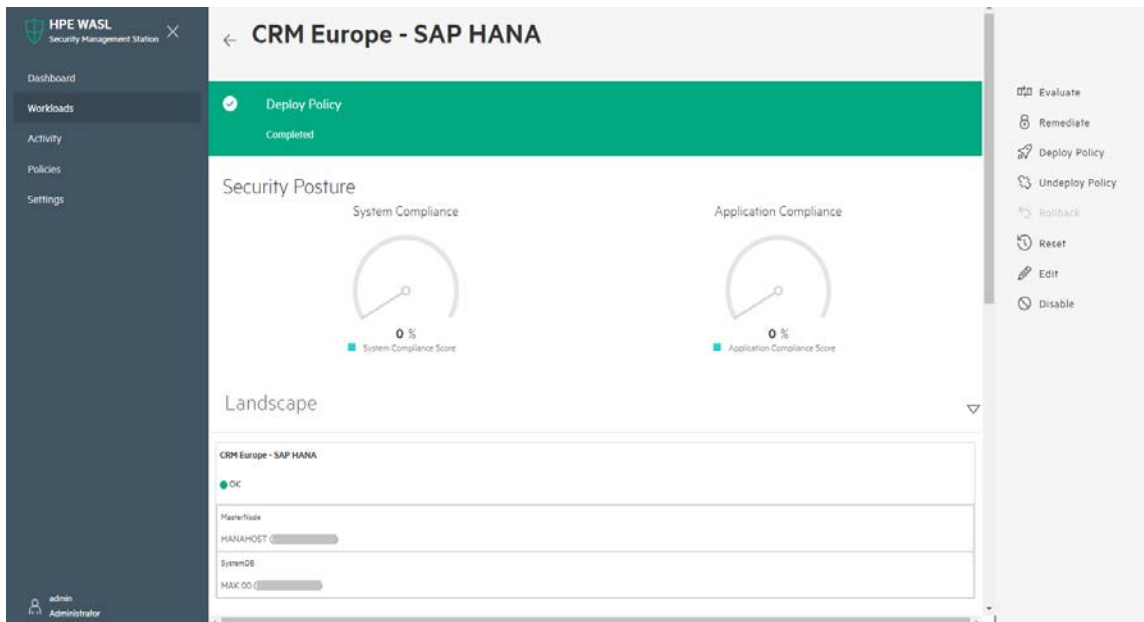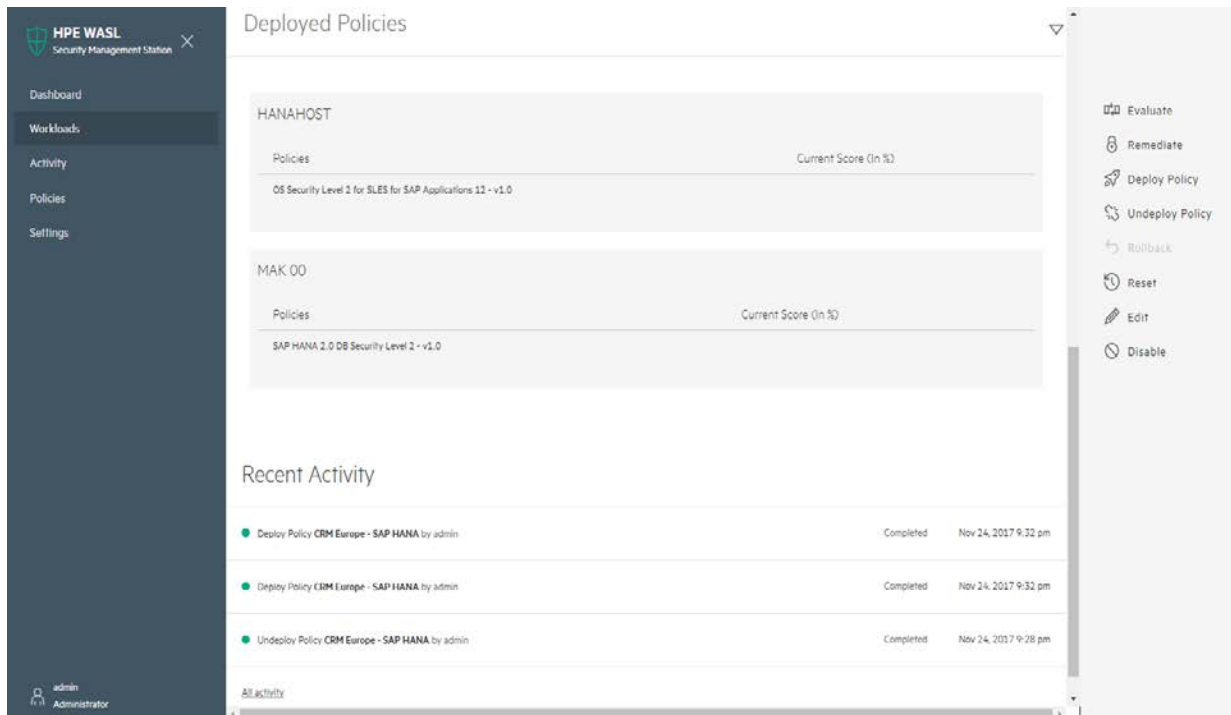
- **Workload Name:** The name of the workload providing during "Add or Register Workload"
- **Status** of the workload
- **Security Posture**: The security posture displays the current system compliance score (i.e. compliance score of the Node element of Workload) and Application compliance score (like compliance score of SAP HANA System element of Workload) from the last evaluation/remediation operation. This score is calculated by cumulative rules evaluated/remediated successfully as defined in all the policies deployed on the workload.
- **Operation:** The right side of the screen shows the various operations like Evaluate, Remediate, Deploy Policy etc. that can be performed on the workload by clicking them. These Operations will vary for different role. For example: A Security Operator will just see an Evaluate, Remediate and Rollback operations.
- **Landscape:** shows the workload synopsis such as the underlying Node and the SAP HANA System details. To see the complete details, use the Edit workload option (Edit Workload option is visible to users with 'Administrator' or 'Security Administrator' roles).
- **Deployed Policies:** Shows a list of all the policies deployed on the workload. It shows all the policies deployed on all the Workload elements that is added during Add or Register Workload operation.
- **Recent Activity:** Shows the most recent activities performed on the workload
- **All activity:** On clicking this link, the screen is redirected to **Activity** Page of WASL and you will see a filtered list of activity that is performed on this workload.
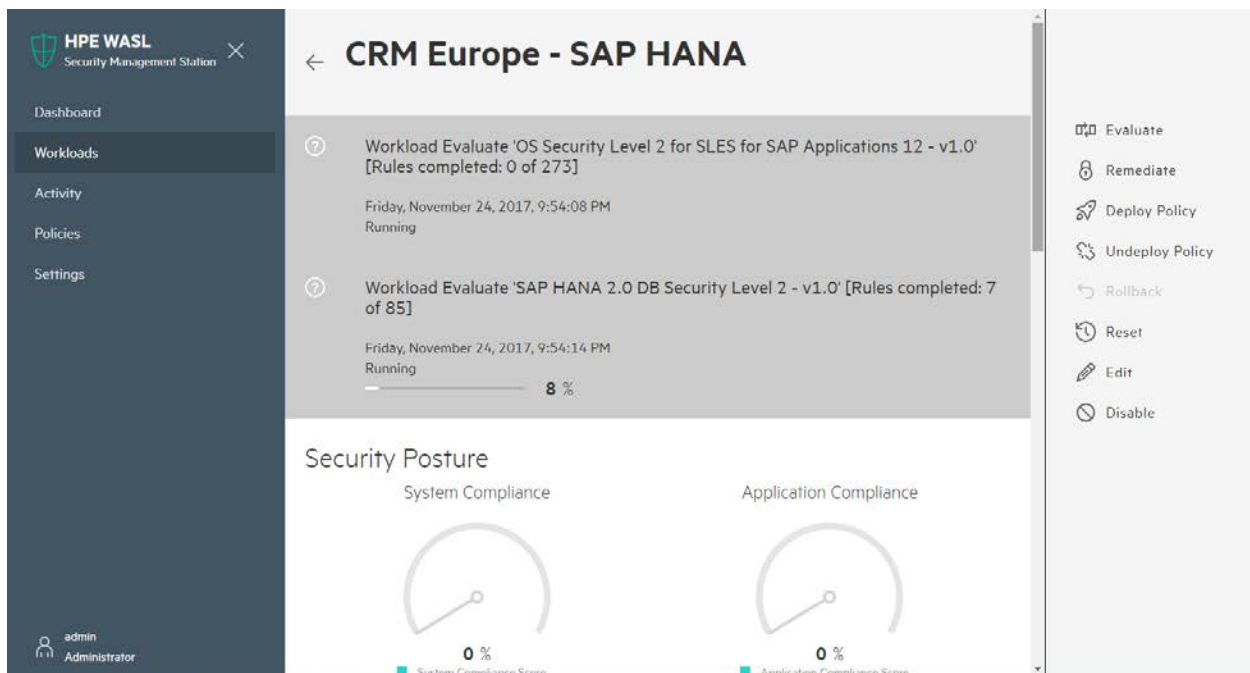
2.2.2 Evaluate Workload

This option is visible to users who login as 'Administrator', 'Security Administrator', 'Security Operator' or 'Security Auditor' role. You can evaluate a workload against policies that are **deployed** on the Workload by clicking on the specific workload in the **Workload** Page and then selecting the "**Evaluate**" Option.
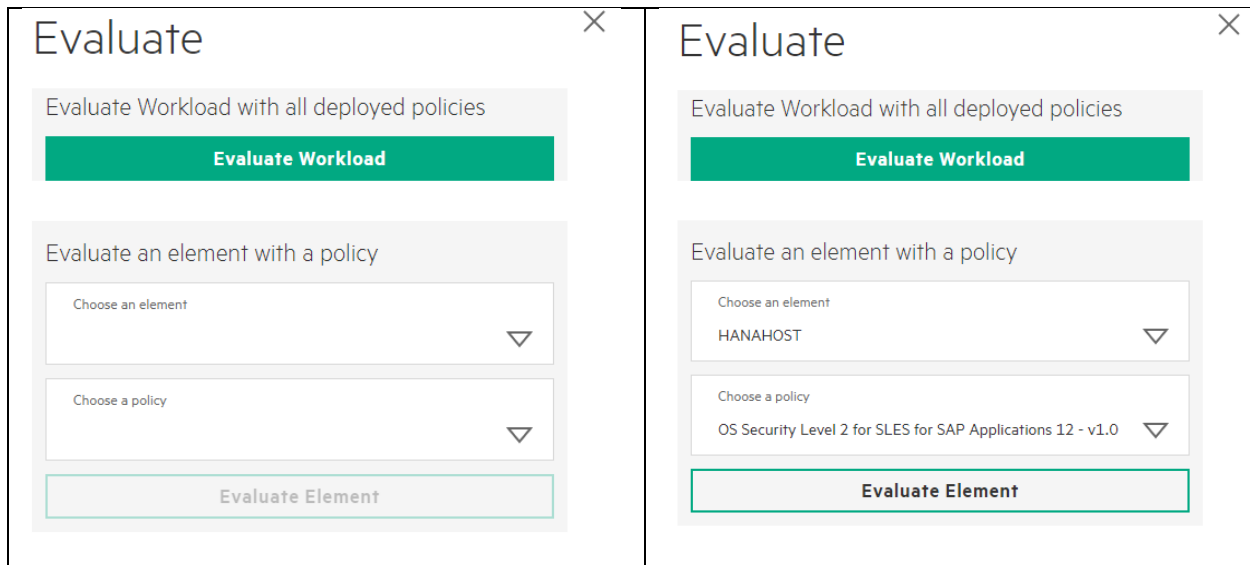
You can evaluate a workload in two ways:

- By Clicking on the "Evaluate Workload" on the top, all the Security Policies that is deployed on the all Workload elements are evaluated on the workload.
- A specific Element of the Workload can be selected via **Choose an element** drop-down, in which case **Choose a policy** displays the applicable policies that are deployed on the workload element. One of these Policy can be selected and Evaluated on the workload.

On starting the Evaluation, the Workload View for this specific Workload shows the different evaluations that are in progress. WASL ensure that only one evaluation (or one Operation generically) will be active at a time on the End Node, as running multiple operations on a Node simultaneously can cause issues.

After the evaluation is complete, the Workload Meters will indicate the current score of the Workload against the policies deployed. The Individual scores of each Policy can be viewed under "Deployed Policies" views and the "Recent Activity" lists all the Policies that are evaluated individually per policy.

Clicking on one Activity, will list more details on the activity, like the number of Passed, Failed rules or Rules with Error in Policy.

You can also see a complete HTML Report by clicking on the "View Full Report" or Download it, by clicking on the ⬇ icon next to "View Full Report". In the "View Full Report" HTML report, you can click on individual Rule and see what the specific rule is doing and the reason for the rule to Fail or give Error.

Verify Integrity with RPM `2x fail`		
Verify and Correct File Permissions with RPM	high	**pass**
Verify and Correct File Ownership with RPM	high	**fail**
Verify and Correct File group owner with RPM	high	**fail**
Uninstall prelink Package	low	**pass**
File Permissions and Masks `16x fail`		
Restrict Partition Mount Options `5x fail`		
Add nodev Option to /home	low	**fail**
Add nodev Option to Removable Media Partitions	low	**pass**
Add nodev Option to /tmp	low	**fail**
Add noexec Option to /tmp	low	**fail**
Add nosuid Option to /tmp	low	**fail**
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**
Disable Mounting of cramfs	low	**pass**
Disable Mounting of freevxfs	low	**pass**
Disable Mounting of jffs2	low	**pass**
Disable Mounting of hfs	low	**pass**
Disable Mounting of hfsplus	low	**pass**

2.2.3 Remediate Workload

This option is visible to users who login as 'Administrator', 'Security Administrator' or 'Security Operator' role. You can Remediate or Harden a workload against policies that are **deployed** on the Workload by clicking on the specific workload in the **Workload** Page and then selecting the "**Remediate**" Option.

Note: Care must be taken during workload Remediation, as it changes the configuration of the Workload element on the end Node. It is advised to test this on a non-production Node first.

You can remediate a workload in two ways:

- By Clicking on the "Remediate Workload" on the top, all the Security Policies that is deployed on the all Workload elements are remediated on the end Node.

- A specific Element of the Workload can be selected via **Choose an element** drop-down, in which case **Choose a policy** displays the applicable policies that are deployed on the workload element. One of these Policy can be selected and remediated on the end Node.

On starting the Remediation, the Workload View for this specific Workload shows the different remediation that are in progress. WASL ensure that only one remediation (or one Operation generically) will be active at a time on the End Node, as running multiple operations on a Node simultaneously can cause issues.
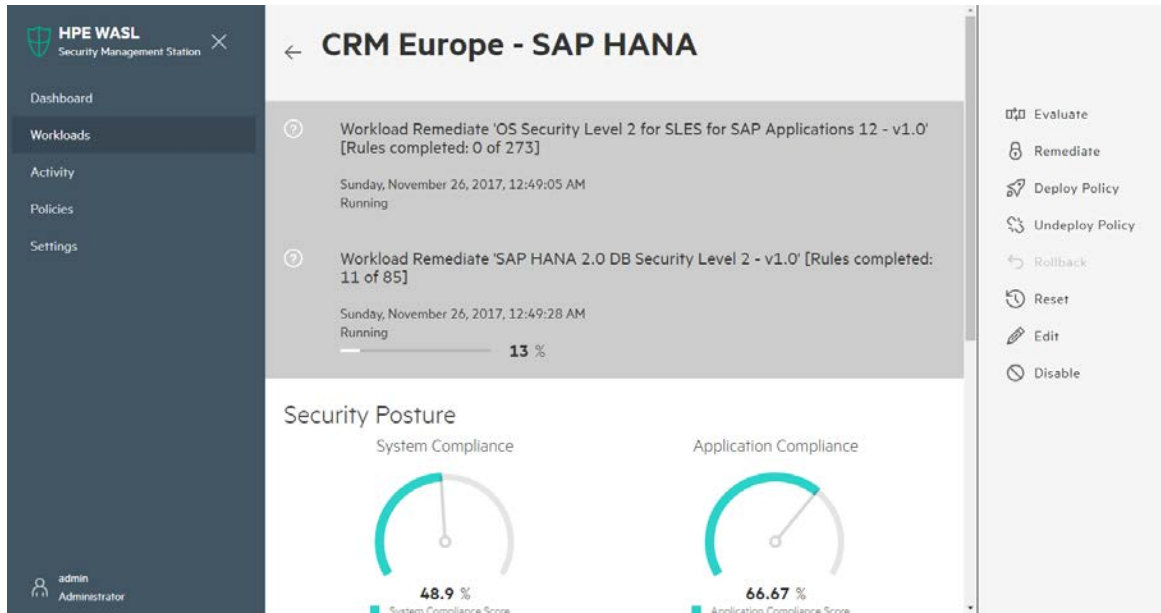
After the remediation is complete, the Workload Meters will indicate the current score of the Workload against the policies deployed. The Individual scores of each Policy can be viewed under "Deployed Policies" views. The "Recent Activity" lists all the Policies that are remediated individually per policy.
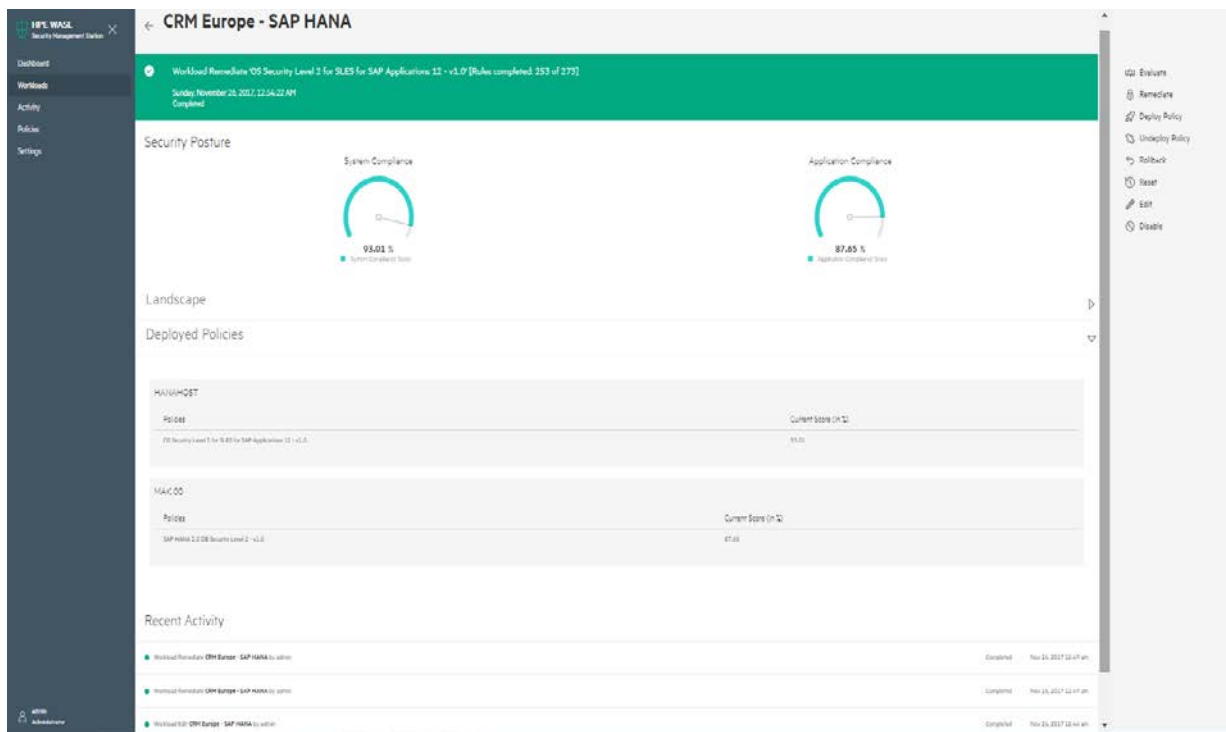
Clicking on one Activity, will list more details on the activity, like the number of Passed, Failed rules or Rules with Error in Policy.

Workload Remediate

By User : 'admin'   Nov 26, 2017 12:49 am

Remediation Report for

Workload: CRM Europe - SAP HANA

Policy: OS Security Level 2 for SLES for SAP Applications 12 - v1.0

Compliance Score   Rule Summary

273
Total

93.01 %
■ Compliance Score

■ Passed   133
■ Fixed   120
■ Failed   10
■ Error   10

Total   273
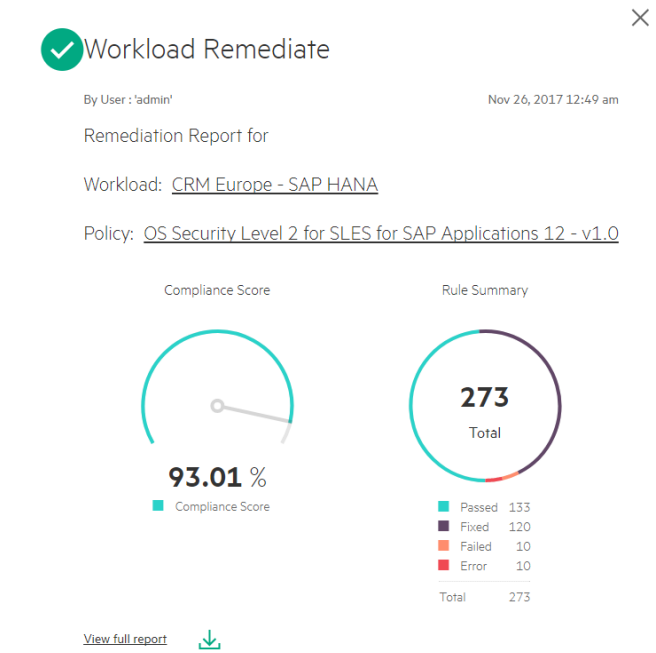
View full report

You can also see a complete HTML Report by clicking on the "View Full Report" or Download it, by clicking on the ⤓ icon next to "View Full Report". In the "View Full Report" HTML report, you can click on individual Rule and see what the specific rule is doing and the reason for the rule to Fail or give Error.

There are chances that the Default Policies shows "Error" for some rules during remediation. The Error happen as remediation script is present for the rules in the policies but they are not run.

-   These rules are sometimes intentionally not remediated, as they might disrupt the environment on the workload. You can look at the rule description and enable remediation on them if required, by tailoring the Security Policy (For more information, see Policy customization).
-   Some of the preconditions for the rules to remediate might not present. For example: A rule to add node to /home partition might not remediate and give error, as /home might not be a separate partition on the Node.

The details of each rule can be obtained by clicking on the individual rule.

Verify Integrity with RPM		
Verify and Correct File Permissions with RPM	high	pass
Verify and Correct File Ownership with RPM	high	fixed
Verify and Correct File group owner with RPM	high	fixed
Uninstall prelink Package	low	pass
File Permissions and Masks 3x fail 3x error		
Restrict Partition Mount Options 1x error		
Add nodev Option to /home	low	error
Add nodev Option to Removable Media Partitions	low	pass
Add nodev Option to /tmp	low	fixed
Add noexec Option to /tmp	low	fixed
Add nosuid Option to /tmp	low	fixed
Add nodev Option to /dev/shm	low	pass
Add noexec Option to /dev/shm	low	fixed
Add nosuid Option to /dev/shm	low	pass
Restrict Dynamic Mounting and Unmounting of Filesystems		
Disable the Automounter	medium	pass
Disable Mounting of cramfs	low	pass
Disable Mounting of freevxfs	low	pass
Disable Mounting of jffs2	low	pass
Disable Mounting of hfs	low	pass

Add nosuid Option to /tmp

Rule ID	mount_option_tmp_nosuid
Result	fixed
Time	2017-11-25T19:30:59
Severity	low
Identifiers and References	Identifiers: CCE-80151-4 References: CM-7, MP-2, 1.1.3
Description	The `nosuid` mount option can be used to prevent execution of setuid programs in `/tmp`. The SUID and SGID permissions should not be required in these world-writable directories. This rule evaluates if `/tmp` is currently mounted and with `nosuid` option in the system. To manually check if `/tmp` is mounted with `nosuid`, check the mount output from the command: `$ mount	grep /tmp	grep nosuid`  If `/tmp` is not mounted with `nosuid` option, as part of remediation, this rule does the following: If there is no entry in `/etc/fstab` for `/tmp`, but `/tmp` is currently mounted on the system, remediation adds the entry for `/tmp` from `/etc/mtab` (or mount command output) to `/etc/fstab` along with `nosuid` as the new mount option. It also removes any `suid` or `default` mount options if present. If there is entry in `/etc/fstab` for `/tmp`, this entry is modified by adding `nosuid` mount option and removing any `suid` or `default` mount options if present. The device `/tmp` is remounted as part of remediation for the change to take effect.
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.

Evaluation messages

info
```
Fix execution completed and returned: 0
```

info
```
Modifying the entry in /etc/fstab
Current entry in /etc/fstab: UUID=3381eb41-0b38-470b-8bc1-7fd9d661f768 /tmp btrfs subvol=@/tmp,nodev,noexec 0 0
Modified entry in /etc/fstab: UUID=3381eb41-0b38-470b-8bc1-7fd9d661f768 /tmp btrfs subvol=@/tmp,nodev,noexec,nosuid 0 0
/dev/sda3 on /tmp type btrfs (rw,nodev,noexec,relatime,space_cache,subvolid=264,subvol=/@/tmp)
```

Add nodev Option to /home

Rule ID	mount_option_home_nodev
Result	error
Time	2017-11-25T19:30:57
Severity	low
Identifiers and References	**Identifiers:** CCE-80149-8 **References:** CM-7, MP-2, 1.1.2
Description	The nodev mount option can be used to prevent device files from being created in /home . Legitimate character and block devices should not exist within /home . This rule evaluates if /home is currently mounted and with nodev option in the system. To manually check if /home is mounted with nodev , check the mount output from the command: `$ mount	grep /home	grep nodev` If /home is not mounted with nodev option, as part of remediation, this rule does the following: If there is no entry in /etc/fstab for /home , but /home is currently mounted on the system, remediation adds the entry for /home from /etc/mtab (or mount command output) to /etc/fstab along with nodev as the new mount option. It also removes any dev or default mount options if present. If there is entry in /etc/fstab for /home , this entry is modified by adding nodev mount option and removing any dev or default mount options if present. The device /home is remounted as part of remediation for the change to take effect.
Rationale	The only legitimate location for device files is the /dev directory located on the root partition. The only exception to this is chroot jails.

Evaluation messages

info
Fix execution completed and returned: 1

info
There is no entry for /home in /etc/mtab and /etc/fstab. Remediation cannot proceed further. Returning failure

info
Failed to verify applied fix: Checking engine returns: fail

2.2.4 Rollback last Remediation operation on Workload

This option is visible to users who login as 'Administrator', 'Security Administrator' or 'Security Operator' role. You can rollback a remediation that is previously done on a workload by clicking on the specific workload in the **Workload** Page and then selecting the "**Rollback**" Option. Rollback moves the configuration of the workload to a stage that was present before the remediation.

You can use Advanced Rollback Options, to select the Workload element (That is added during "Add or Register Workload" operation) that needs to be rolled back.

Contrary to Remediation, rollback is allowed only on one policy that has been recently remediated on the Workload. Remediation on the other hand can be done on all the policies that are deployed on a workload by just clicking one button. If you want to rollback all the policies that were remediation by the previous remediation operation, you need to see the **Activity** page of WASL to identify the number of remediation that was done on the different workload elements. You need to then run the rollback operation on those

workload elements that much number of times. For example, say "OS security Level 2 for SLES 12" and "OS Security Extras for SAP HANA" policies are deployed on the Node Workload element and "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, rollback has to be done two time on the Node workload element and one time on SAP HANA system workload element, to move the Workload configuration to the state that was present before remediation.

Rollback works by taking snapshot of the workload element before remediation operation. These snapshot of workload configuration gets stored on the end node getting remediated. This snapshot can contain 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 configuration related to the default Policy as well as other related Policy. For example, during remediation of "OS security Level 1 for SLES 12", a snapshot is taken for both "OS security Level 1 for SLES 12" and "OS security Level 2 for SLES 12" policies, since both these policies are derived from the same XCCDF sources. This can result in extra snapshot being taken though a specific policy might not be deployed on the workload. Thus rollback might revert back more changes than expected on the workload element based on the snapshot.

Note2: Snapshot will take entire file backup in some cases, like say the /etc/ssh/sshd_config file is completely backed up during snapshot stage of secure shell configuration. During rollback any other user specific changes on these files will be lost.

Note 3: 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 more information, see Policy customization). It is recommended to test the tailoring done for Policy rollback operation from SMS.

Note 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 regarding this.

2.2.5 Reset Workload

This option is visible to users who login as 'Administrator' or 'Security Administrator' role. Reset Workload allows to reset 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. To reset a workload click on the specific workload, in the **Workload** Page and then selecting the "**Reset**" Option.

A reset operation is used in situations when customers wants to eliminate the operating system or application hardening as a potential cause towards an application downtime. Reset option should be used cautiously, as multiple Remediates could have got performed on a workload over a period of time. It is recommended to use rollback of workload recursively instead of reset.


2.3 User Management

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

2.3.1 View Users

This option is visible to users who login as 'Administrator' or 'User Administrator' role. Select the **Settings->User Management** option from the left pane. A list of users on SMS is displayed. In case the icon before the user is grey in color then the user is in "De-activate" state. Such users are not allowed to login to SMS. A user with green icon is in "Activated" state and can login to SMS. On the Right side of each user, we can see the role assigned to the user.
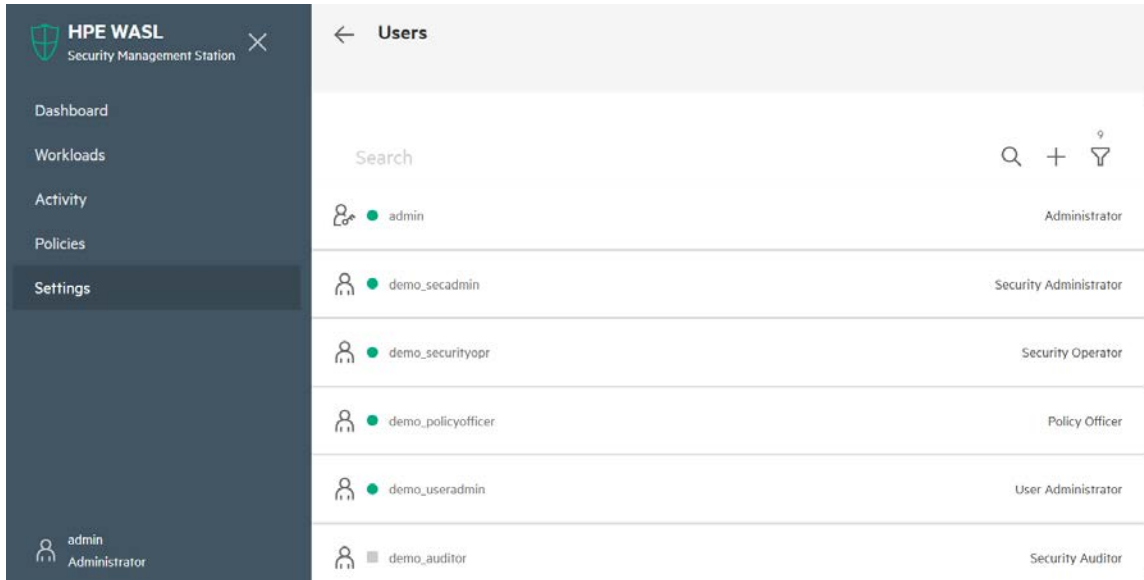
Click on a user to see more details on the user and perform operation on the user account.
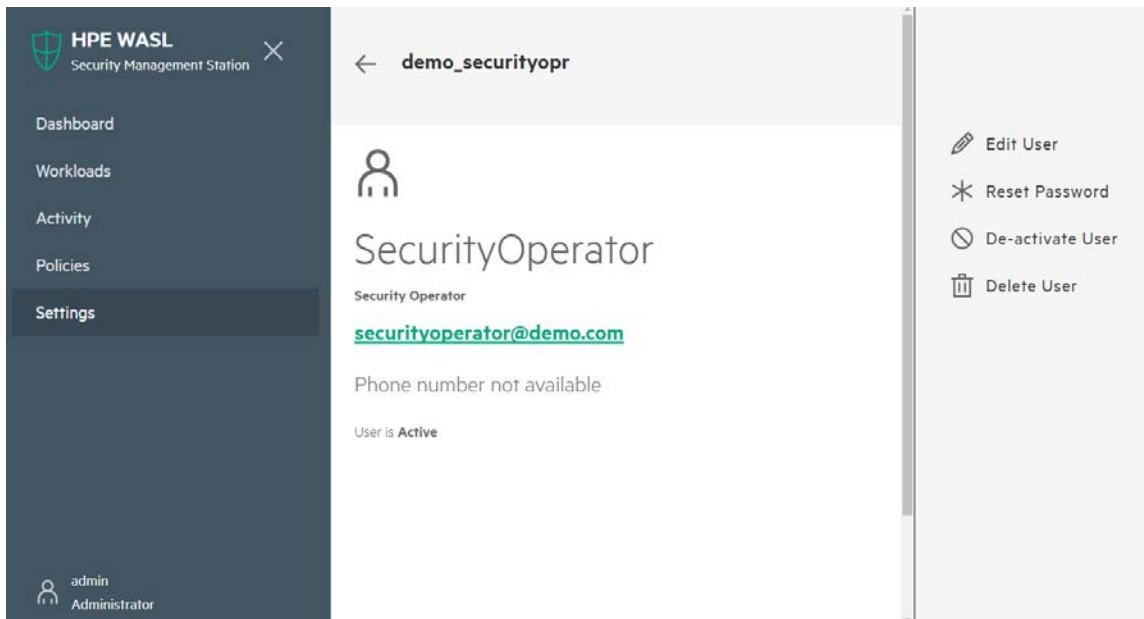
2.3.2 Add User

This option is visible to users who login as 'Administrator' or 'User Administrator' role. It allows to enter new user credentials.

From **Settings->User Management** click on "**+**" symbol on top right hand screen to create a window to enter the user credentials such as **User ID**, **Full Name**, **Password**, **Email** and **Office Phone**. Select the role to assign the user.
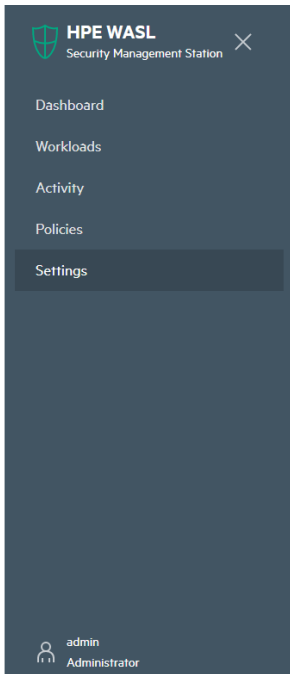
For different user roles and operations that are allowed for each role, see **User Roles**.

The new user will be asked to change the password during first time login.

2.3.2.1 Delete User

The new user created in SMS can be deleted until a login is done by the user. Deleting a user is possible only until the user first does a login to SMS. Once a user login to SMS, the user record cannot be deleted and is maintained for auditing purposes. Such users can only be De-Activated.

From **Settings->User Management** click on the specific user you want to delete. The "**Delete User**" option will be visible only this user has not logged in earlier any time to SMS. Click on the "**Delete User**" option to delete this user.
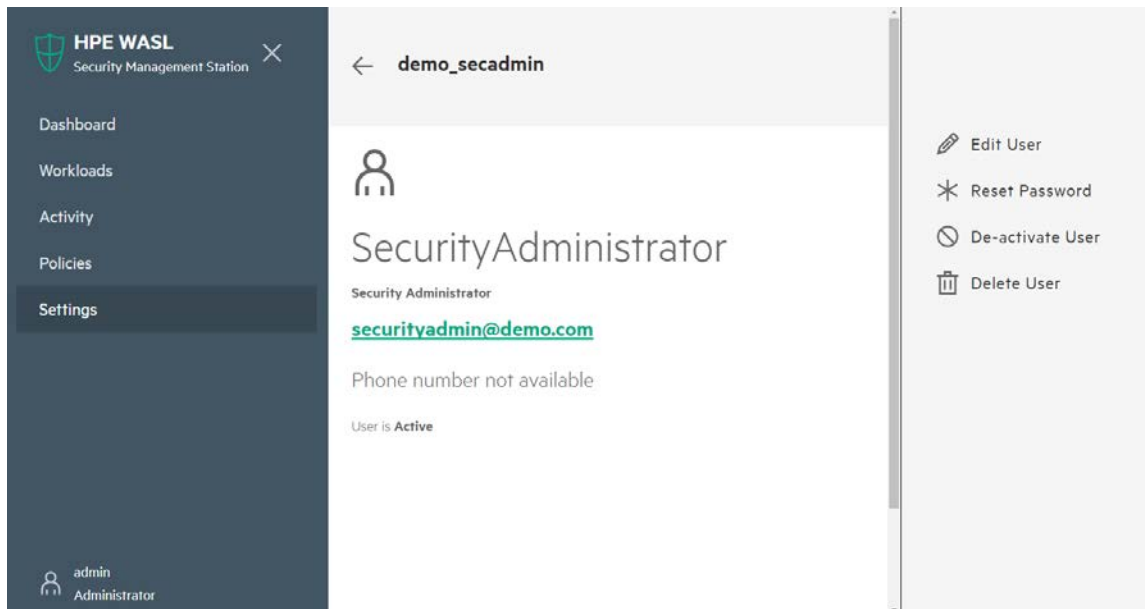
2.3.3 Edit User

This option is visible to users who login as 'Administrator' or 'User Administrator' role. It allows to edit a user account.

From **Settings->User Management** click on the specific user you want to edit. Then click on the "**Edit User**" Option to edit the user details or change the user role and save.
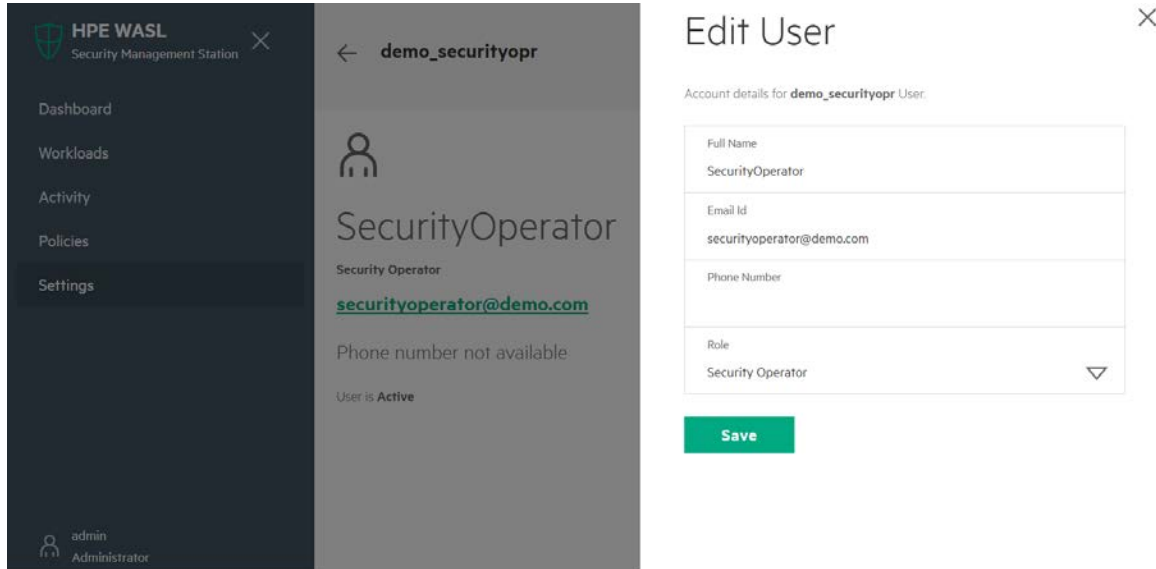
2.3.4 Reset User Password

This option is visible to users who login as 'Administrator' or 'User Administrator' role. It allows to reset the user password incase the user forgets his password.

From **Settings->User Management** click on the specific user you want to reset the password. Then click on the "**Reset Password**" Option to reset the user password.

The user will be asked to change the password during next login.

2.3.5 Activate/De-activate Users

This option is available to users who login as 'Administrator' or 'User Administrator' role. In case the administrator needs to perform a maintenance operation or suspect a suspicious operation being performed from a user-account or the user has left the organization, the user can be de-activated from the user management screen. This user is prevented from login to SMS once the account is de-activated.

The user account can be activated to enable login to SMS once again if required.

From **Settings->User Management** click on the specific user you want to De-activate or activate. Select the "**De-activate User**" or "**Activate User**" option.
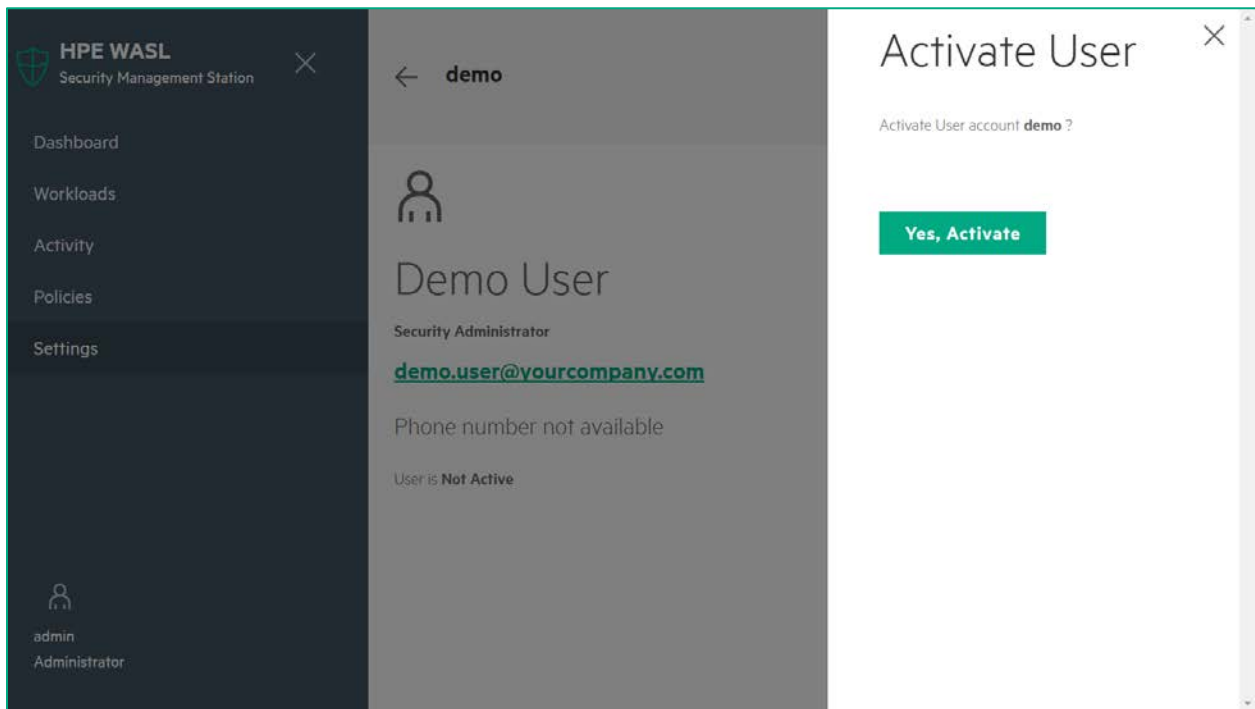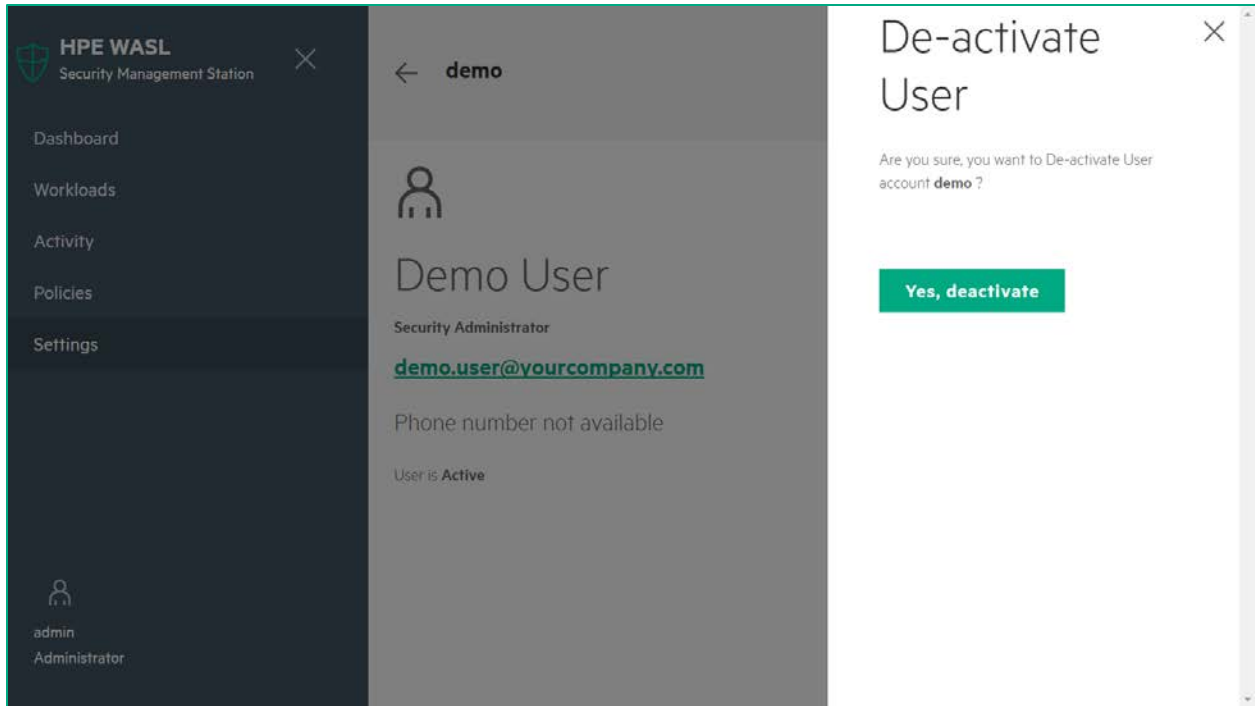
2.4 Policy Operations

2.4.1 View security policies on workload

This option is visible to users who login as 'Administrator' or 'Policy Officer' role. Select the **Policies** option from the left pane. A list of policies available on SMS are displayed. In case the icon before the policy is grey in color then the policy is in "disable" state. Such policies are not available for deployment on SMS workload element. A policy with green icon is in "enable" state and are available to deployment on the workload element. (Refer Disable/Enable security policy section for more details on policy state.)

On the Right side of each Policy, Policy type "**Default**" or "**User defined**" is displayed. The **Default** Policy is shipped along with the WASL product. A **User defined** Policy is a policy created by Policy customization (For more information, see Policy customization).

Click on a specific policy to get more information on the Policy. The policy details shows:

Policy Name: At the Top of the page

Status Task Bar: Green color Indicates policy is enabled and can be deployed on a workload. Grey color indicates 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.

Type: Type **"System"**, indicates that the Policy can be deployed on Node elements of the workload (Operating system Only workload). Type **"Application"** indicates that the policy can be deployed on an application (like SAP HANA database) that is running on the Node.

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.

Compliance: Indicates if the Policy addresses some compliances.

Workloads: If the Policy type is Application, then the Workload entry indicates the type of application which this policy secures.

Policy Directory: The directory on WASL SMS system where all the policy related files are stored.

XCCDF File: This is the main XML file based on XCCDF standards that has entry point for all the rules in the policy and what actions are 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.

Tailoring File: This is a file created per policy by WASL during the first time XCCDF file is loaded into WASL product. Each WASL Policy has a unique tailoring file. Each tailoring file contains a XCCDF profile (List of rules or List of group of rules) that is picked from the XCCDF file during first time load of the XCCDF file by WASL.

Rule Count: The number of rules (or group of rules) inside the policy.

2.4.2 Disable/Enable security policy

This option is visible to users who login as 'Administrator' or 'Policy Officer' role. Select the Policy option from the left side menu of WASL and click on a policy. Click on "**Disable**" option from the right side operations menu to disable the policy. 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. The Disable Policy option is exercised by the policy officer if a new version of policy is available. The new version of policy can be enabled and current version of policy disabled from further deployments.

Click on the "**Enable**" option to enable the policy for deployment to workload. Only enabled policies can be deployed on a workload.

2.4.3 Policy customization

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

This operation is allowed from an 'Administrator' or 'Policy Office' role. 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.

Note 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 first to create and test this tailored policy first. If there are issues in a tailored policy, it can

- o   Cause issues on the workload
- o   There are chances that you might create multiple tailored policy to get the final desired policy. Once a tailored policy is loaded and deployed on a Workload, it will not be allowed to be deleted (Policy already deployed once, can only be disabled). This can leave too many unwanted intermediate tailored policies on the SMS.

Select the Policy option from the left side menu of WASL and click on a policy to tailor. Click on "Copy" option to copy the policy to a new Policy.

Copy   ✕

Create a copy of **OS Security Level 1 for SLES 12 - v1.0**

Title

Custom OS Security Level 1 for SLES 12 - v1.0

Description

Custom policy for organization

Copy

To see the copied policy, Click on the Task (Activity) which indicates the successful policy copy operation and then click on the new policy that is copied. Alternatively, you can search for the new policy in the **Policies** page of WASL.

HPE WASL
Security Management Station ✕

- Dashboard
- Workloads
- Activity
- Policies
- Settings

← **OS Security Level 1 for SLES 12 - v1.0**

📄 Copy
🚫 Disable

✓ Policy Copy: Successful.

Saturday, November 25, 2017, 5:19:34 PM
Completed

This policy contains rules to ensure OS security Level 1 baseline of SUSE Linux Enterprise Server 12 SP1 system. These rules provide basic security that is required to protect the Operating System instance.

Type	System
Platforms	SUSE Linux Enterprise Server 12 SP1 SUSE Linux Enterprise Server for SAP Applications 12 SP1
Compliance	System security
Workloads	None
Rule Count	213

File Information ▷

admin
Administrator

✕

✔ Policy Copy

By User : 'admin'   Nov 25, 2017 5:19 pm

Policy **OS Security Level 1 for SLES 12 - v1.0** copied into a new policy **Custom OS Security Level 1 for SLES 12 - v1.0** by 'admin'.

The details of the new policies are displayed in the center window. Click on the arrow next to **File Information** option to see the policy details such as location of policy files on SMS node. Edit only the tailoring file to tailor the new policy on the SMS system by using a text editor like vim etc (Note that the tailoring file should be owned by waslsms user and group)

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_-_v1.0.xml
-rw-rw---- 1 waslsms waslsms 30683 Nov 25 17:01
tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12_-_v1.0.xml
Sms-node: # vi
tailoring_xccdf_hpe.wasl_profile_Custom_OS_Security_Level_1_for_SLES_12_-_v1.0.xml
```

A sample to edit the SLES 12 OS security policy to have only two rules related to login banners in /etc/issues and /etc/issues.net is as follows. There are two rules related to this in OS security policy:

- banner_etc_issue - Modify the System Login Banner (/etc/issue)
- banner_etc_issue_net - Modify the System Login Banner (/etc/issue.net)

If we look at the reports of evaluation or remediation, the rule description indicates that these rule depends on following XCCDF variables. Details on these variables are also present in the XCCDF file (ssg-sle12-xccdf.xml in this case).

- login_banner_text – This variable contains the actual login banner text against which the evaluation or remediation is done. (Evaluation checks if /etc/issue and /etc/issue.net has this login banner text. Remediation if enabled, set the file to this login banner text)
    - login_banner_text is set to a banner as prescribed by United States Government Configuration Baseline and identified by "usgcb_default" idref (ID rereference) 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 in the XCCDF.
        - To use any of the alternative idref already available, <refine-value> tag can be used in the tailoring file. However in this sample we are using <set-value> tag, and setting the login banner to a different text.
- 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 are using <refine-value> tag in the tailoring file and setting the value to "true" so that remediation is enabled.

- 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 are using <refine-value> tag in the tailoring file and setting the value to "true" so that remediation is enabled.

Modify the System Login Banner (/etc/issue)

Rule ID	banner_etc_issue
Result	error
Time	2017-11-03T06:41:17
Severity	medium
Identifiers and References	**Identifiers:** CCE-27303-7 **References:** AC-8(a), AC-8(b), AC-8(c)(1), AC-8(c)(2), AC-8(c)(3), 48, SRG-OS-000023-GPOS-00006, SRG-OS-000024-GPOS-00007, 010040
Description	To configure the system login banner edit /etc/issue . Replace the default text with a message compliant with the local site policy or a legal disclaimer. This rule checks the contents of /etc/issue with the pattern provided in login_banner_text xccdf variable. The login_banner_text xccdf variable is pre populated with a set of standard login banners. Edit the login_banner_text xccdf variable in the profile, with any specific changes required to the login banner. The remediation is not done automatically and will happen only if the remediate_banner_etc_issue xccdf variable is set to true (Default is false). The remediation, will use the banner in login_banner_text xccdf variable, formats it and write the contents to /etc/issue. Sample DoD required text is either: 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. OR: I've read & consent to terms in IS user agreem't.
Rationale	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.

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)

Edit the tailoring file on the SMS node to have the following contents:

```
<?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_-_v1.0">
    <title>Custom OS Security Level 1 for SLES 12 - v1.0</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="banner_etc_issue" weight="1.000000" />
    <select idref="banner_etc_issue" selected="true" />
    <refine-rule idref="banner_etc_issue_net" weight="1.000000" />
    <select idref="banner_etc_issue_net" selected="true" />
  </Profile>
</Tailoring>
```

To summarize, we have done the following in the tailoring file:

- Retained only two rules "banner_etc_issue" and "banner_etc_issue_net"

- 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".

Note: 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.

Once the tailoring file is edited and saved on SMS Node, the Policy can be reloaded, by clicking on the "Reload" option in the Policy screen:
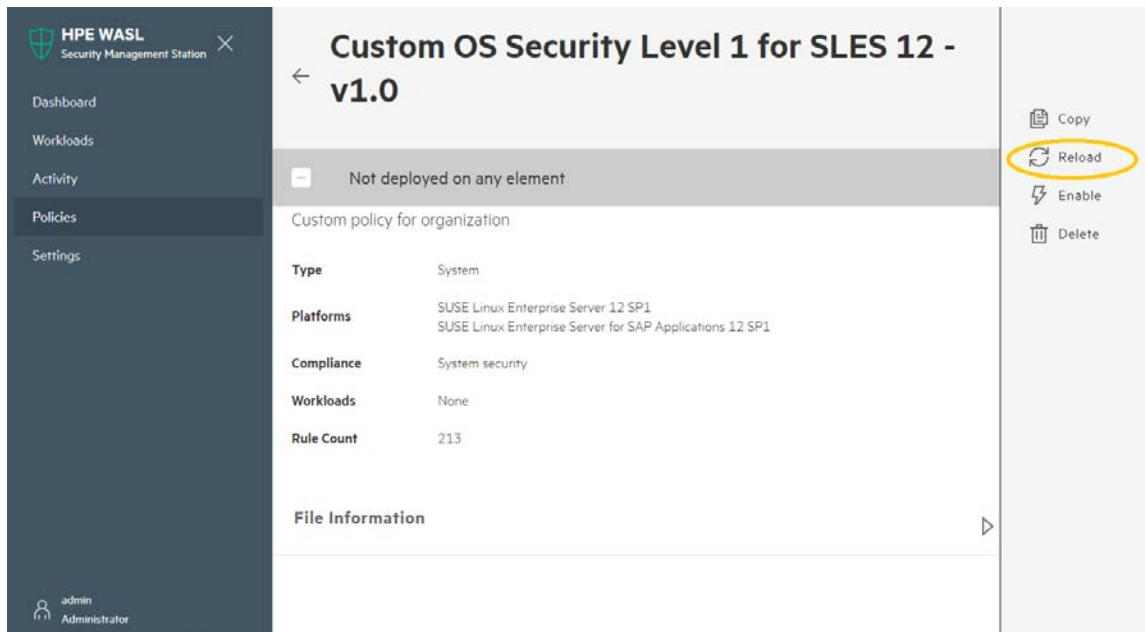
Once the reload is complete, the Rule Count entry of the Policy is updated:
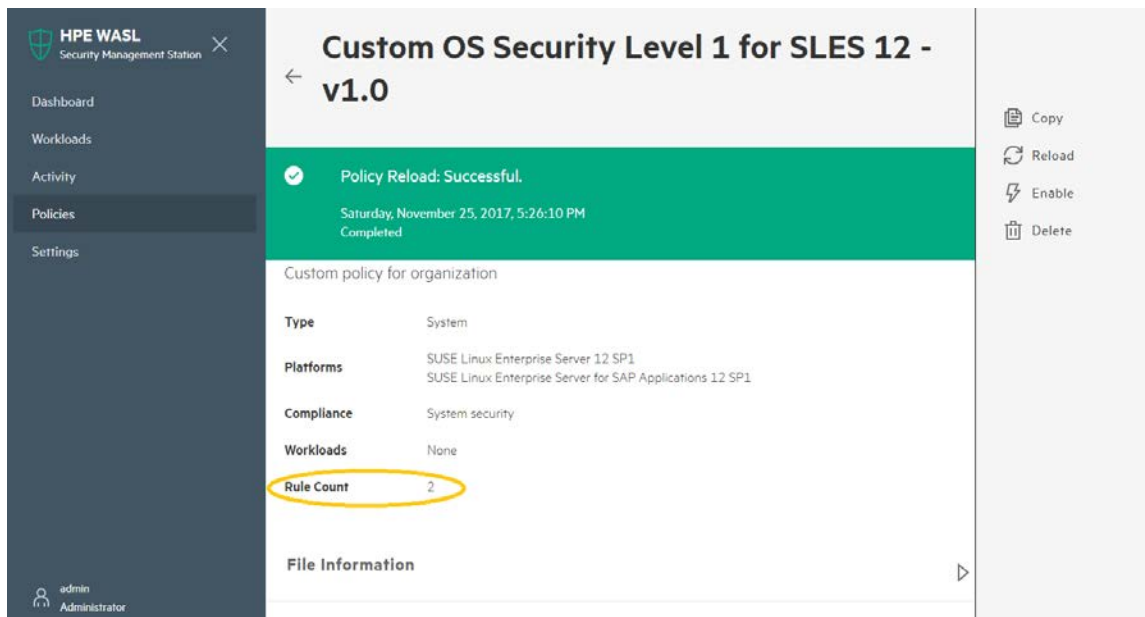
This Policy needs to be finally enabled, so that it can be deployed on different workloads.

2.4.3.2   Import new policy

This operation is allowed from an 'Administrator' or 'Policy Office' role. Select the Policy option from the left side menu of WASL and clicking the + icon on top right. A window is displayed to specify the details of security policy to import into Security Management Station (SMS).

The **Choose file** option allows the user to import the file into SMS. Read the instructions displayed on the screen carefully. A policy is a ZIP or TAR.GZ file. It consists of 4 different type of files in a directory:

1.   XCCDF file, which has the various rules and the Profile.
     a.   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.

      b.   For each Profile in the XCCDF a tailoring file is created by SMS that maps to a SMS Policy. The Name of the profiles should match the pattern: "Xccdf_[^#]_profile.+". Example: xccdf_sample_profile_1

2. 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/). This allows Evaluation of a rule to happen using scripts (like python and shell scripts) along with the OVAL XML files based evaluations.

3. 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). Sample JSON file with details is provided Appendix section – "Sample JSON file used to import policy".

4. Optional profile_apis.py (Python file), to mainly to enable snapshot (Taken during remediation) and rollback features on a workload for the policy. API's needs to be exported from profile_apis.py for doing this snapshot and rollback. Other API's also can be exposed from profile_apis.py. These API's gets called during Workload Operation for the set of Policies that are getting imported. Sample profile_apis.py is provided in Appendix section – "Sample profile_apis.py optionally used in importing policy".

Ensure that the names of directory holding these files, the XCCDF file name, the JSON file name and the resultant archive .tar.gz or .zip file should be having the same names with different extensions. SMS, uses this name to identify the different files.

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 and respective activity errors logs can be referenced for further actions.

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.

2.4.3.3   Delete Policy

This operation is allowed from an 'Administrator' or 'Policy Office' role. The Option is also allowed only for user defined Policies (i.e. Policies that are copied for Customization or imported policies) and only if the policy is not deployed even once. Delete Option is not provided to policies that are already deployed once (even if the policy is currently un-deployed from all workload elements) for auditing reasons.

Select the **Policies** option from the left pane of WASL. A list of policies available on SMS is displayed. Select the **User defined** that needs to be deleted and use the delete option to delete the policy from SMS.

3 Session Information and Operations

All users who login to WASL SMS can see the user name and the role they have logged in on the left hand bottom corner screen after the user icon. On clicking the user icon, following options are provided:

- **Help**: Opens the WASL Help, to view information about each of the WASL screens in SMS.
- **Change Password**: Change the password of the current logged in user. The newly updated password gets applied from next login.
- **Logout**: logout from SMS.
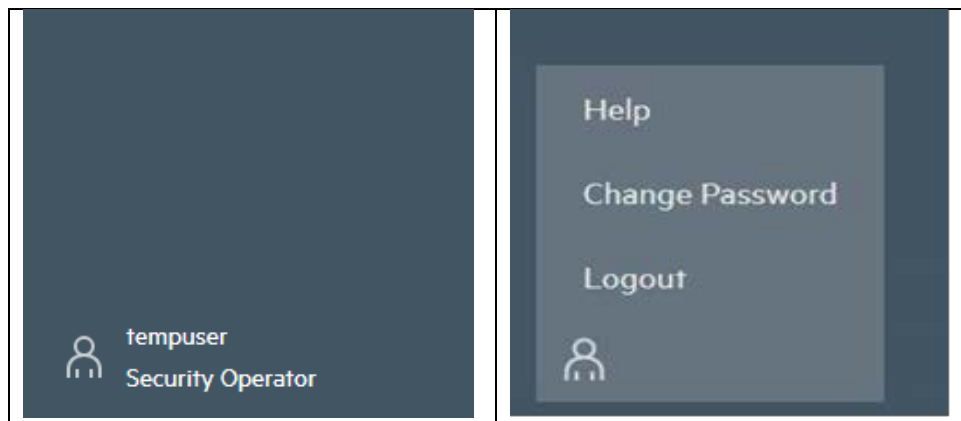
4 Appendix

4.1 Sample JSON file used to import policy

Following is a sample JSON file used during policy import:

```
[
{
 "id": "xccdf_com.hpe.wasl.content_profile_SAP_HANA_1_SINGLE_HOST_LEVEL_1_V1.00",
 "info": {
         "applicable_platforms": ["SUSE Linux Enterprise Server 12 SP1","SUSE Linux Enterprise
Server for SAP Applications 12 SP1"],
         "applicable_workloads": ["SAP HANA"],
         "applicable_compliance": ["SAP HANA Security Guide"],
         "type":"Application" }
},
{
 "id": "xccdf_com.hpe.wasl.content_profile_SAP_HANA_2_SINGLE_HOST_LEVEL_1_V1.00",
 "info": {
         "applicable_platforms": ["SUSE Linux Enterprise Server 12 SP1","SUSE Linux Enterprise
Server for SAP Applications 12 SP1"],
         "applicable_workloads": ["SAP HANA"],
```

```
        "applicable_compliance": ["SAP HANA Security Guide"],
        "type":"Application" }
}
]
```

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_com.hpe.wasl.content_profile_SAP_HANA_1_SINGLE_HOST_LEVEL_1_V1.00">
<title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">SAP HANA 1.0 Security Policies
for Single Host installation - Level 1 V1.00</title>
-
-
</Profile>
```

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

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 (i.e. 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).

4.2   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
#
def validate_hana():
    try:
        logger.debug("Perform Validation here")
    except Exception,e:
        raise_error("Error occurred during validation:"+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))
```

4.3 Acronyms

Commonly used acronyms are described for reference.

Acronym	Abbreviation
WASL	Workload Aware Security for Linux
SMS	Security Management Station
RHEL	RedHat Enterprise Linux
SLES	SUSE Linux Enterprise Server
SAP HANA	SAP High Performance Analytic Appliance
TDI	Tailored Data Center Integration
SP1	Service Pack 1
CS 500 / 900	ConvergedSystem 500 / 900
XCCDF	Extensible Configuration Checklist Description Format. More details are available here: https://scap.nist.gov/specifications/xccdf/
GUI	Graphical User Interface
OpenSCAP	Open Security Containment and Automation Protocol
OVAL	Open Vulnerability and Assessment Language. More details are available here: https://scap.nist.gov/specifications/xccdf/
FTP	File Transfer Protocol
DB	Database
SSH	Secure Shell
REST	Representational State Transfer
SFTP	Secure File Transfer Protocol