SUSE Linux Enterprise Server

Hardening SUSE Linux Enterprise with STIG

This document introduces you to auditing and hardening SUSE Linux Enterprise with the Security Technical Implementation Guide (STIG) by the Defense Information Systems Agency (DISA) .

Publication Date: December 12, 2024

Contents

Important: Disclaimer

SUSE seeks to provide customers with quick and easy guides that can assist them in maintaining security compliance. Implementation of the settings contained within this guide without its prior testing in a non-operational environment is highly discouraged. The developers of these profiles and documentation have made reasonable efforts to ensure overall compliance. They assume no responsibility for its use by other parties, and make no guarantee, expressed or implied, about its quality, reliability or any other characteristic.

1 What is STIG?

STIG stands for `Security Technical Implementation Guide`. The Defense Information Systems Agency (DISA) organization, which is a parent agency of the United States Department of Defense (DoD) , approves and publishes `Security Technical Implementation Guides (STIGs)` and updates them every 90 days.

STIGs are a set of rules and best practices for configuring systems to defend against potential threats. Each implementation guide is tailored to a specific product and version, defining a configuration standard with cybersecurity requirements for this product and version.

These requirements must be met when the system connects to a DoD network. But Security Technical Implementation Guides are also used outside of the government sector.

2 Benefits

When a Security Technical Implementation Guide is implemented for a system, the system is hardened. The goals are to minimize attacks and to prevent system access (both physically and via a network) and to define processes for maintenance (applying software updates) and vulnerability patching. Security Technical Implementation Guides can also cover configuration settings, for example, for operating systems, routers, databases, firewall rules, domain name servers and switches.

STIGs are ubiquitous across all systems.

3 Hardening SUSE Linux Enterprise Server with STIG

There are several ways to harden your systems with the STIG.

During installation with YaST or AutoYaST

Starting with SUSE Linux Enterprise 15 SP4, YaST and AutoYaST let you check certain basic aspects of the system at installation time. You can also enable a full scan or scan and remediation, respectively, at first boot of the system.

For details, see *SUSE Linux Enterprise Server Deployment Guide* (https://documentation.suse.com/sles/15/html/SLES-all/cha-install.html#sec-yast-install-proposal-security-profile) ↗.

With OpenSCAP

You can scan or remediate an existing system to bring it to a compliant state. OpenSCAP can be used to check and remediate local systems as well as remote systems.

With STIG Viewer

You can manually review the rules from DISA and apply them to a dedicated system.

4 Applying a STIG profile

The contents delivered with the *SCAP Security Guide* can be used to check or check and remediate systems according to a specific profile.

Regarding STIG, SUSE supports the following *SCAP Security Guide* profiles:

- DISA STIG for SUSE Linux Enterprise 15
- DISA STIG for SUSE Linux Enterprise 12

The following sections give certain examples on how to scan SUSE Linux Enterprise with **`oscap`** for STIG compliance and how to perform a remediation. For more background on OpenSCAP and the *SCAP Security Guide*, see the article *Hardening SUSE Linux Enterprise with OpenSCAP* (https://documentation.suse.com/compliance/all/html/SLES-openscap/article-openscap.html) ↗.

4.1 Scanning a SLE system for STIG compliance

The following example shows how to scan SUSE Linux Enterprise 15 locally with **`oscap`** for vulnerability issues according to the profile `DISA STIG for SUSE Linux Enterprise 15`. You can save the results in XML format and generate an HTML report.

EXAMPLE 1: SCANNING SUSE LINUX ENTERPRISE WITH OSCAP

```
> sudo oscap xccdf eval❶ \
    --profile stig❷ \
    --results /tmp/results.xml❸ \
    --report /tmp/report.html❹ \
    /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❺
```

❶ Calls the **`oscap xccdf`** module and tells it to perform an evaluation (vulnerability scan).

❷ Specifies the profile to use, in this case, `stig`.

❸ Saves the results of the evaluation to *`/tmp/results.xml`*.

❹ Generates an HTML report called *`/tmp/report.html`* in addition to the results in XML.

❺ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: **`ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml`**. For more information about a particular policy, run **`oscap info`** on the file.

The evaluation process usually takes a few minutes, depending on the number of selected rules.

4.2 Making a SLE system STIG-compliant

The following examples show how to scan and remediate SUSE Linux Enterprise locally with **`oscap`** according to the profile `DISA STIG for SUSE Linux Enterprise 15`.

4.2.1 Remediating SUSE Linux Enterprise with oscap (on the fly)

For remediation with **`oscap`** on the fly, use the `--remediate` command-line option.

EXAMPLE 2: REMEDIATING SLE 15 WITH OSCAP (ON THE FLY)

```
> sudo oscap xccdf eval --remediate❶ \
      --profile stig❷ \
      --results /tmp/results.xml❸ \
      /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❹
```

❶ Calls the **`oscap xccdf`** module and tells it to perform an evaluation plus a remediation of the target system in one go.

❷ Specifies the profile to use, in this case, `stig`.

❸ Saves the results of the evaluation to *`/tmp/results.xml`*.

❹ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: **`ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml`**. For more information about a particular policy, run **`oscap info`** on the file.

In the resulting *`/tmp/results.xml`* file, the first `TestResult` element shows the result of the scan *before* the remediation. The second `TestResult` element shows the result of the scan *after* applying the remediation. In the second `TestResult` element, if the result of a rule is `fixed`, this means that the fix was successfully applied, and this rule now passes evaluation. If the result of a rule is `error`, this means that the remediation for this rule was not successful, and the rule still does not pass evaluation.

4.2.2 Remediating SUSE Linux Enterprise with oscap (after scanning)

In this example, we first execute a scan and then run the remediation as next step.

EXAMPLE 3: REMEDIATING SLE WITH OSCAP (AFTER SCANNING)

1.
```
> sudo oscap xccdf eval❶ \
        --profile stig❷ \
        --results /tmp/results.xml❸ \
        /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❹
```

❶ Calls the **`oscap xccdf`** module and tells it to perform an evaluation.

❷ Specifies the profile to use, in this case, `stig`.

❸ Saves the results of the evaluation as an XCCDF file to *`/tmp/results.xml`*.

❹ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15. To list all available policies, run: **`ls -1 /usr/share/xml/scap/ssg/content/ssg-*-ds.xml`**. For more information about a particular policy, run **`oscap info`** on the file.

During this step, the system is only evaluated, and the results are stored in a `TestResult` element in *`/tmp/results.xml`*.

2.

```
> sudo oscap xccdf remediate❶ \
       --results /tmp/results.xml❷ \
       /tmp/results.xml❸
```

❶ Calls the **`oscap xccdf`** module and tells it to perform a remediation.

❷ Saves the results of the remediation to *`/tmp/results.xml`*.

❸ Uses the *`/tmp/results.xml`* XCCDF file from the first step (evaluation) as input file.

During this step, the results file from the first step is used as input for the **`oscap`** command. You can safely store the results from the second step in the same file that you use as input file, *`/tmp/results.xml`*. During this run, **`oscap`** creates a new `xccdf:TestResult` element in the file. The new element is based on the previous one and inherits all the data. The newly created `xccdf:TestResult` element differs only in the `rule-result` elements which failed in the first run. Only for those is the remediation executed.

4.2.3 Remediating a SLE system with Ansible

You can use the Ansible playbooks provided by the `SCAP Security Guide` to remediate a local system.

The `ansible` package is available from `SUSE Package Hub`. Register your SUSE Linux Enterprise system and enable the `SUSE Package Hub` extension. For SUSE Linux Enterprise 12, you additionally need to enable the `Public Cloud` module. Then install the package with **`sudo zypper in ansible`**.

EXAMPLE 4: REMEDIATING SLE 15 WITH ANSIBLE

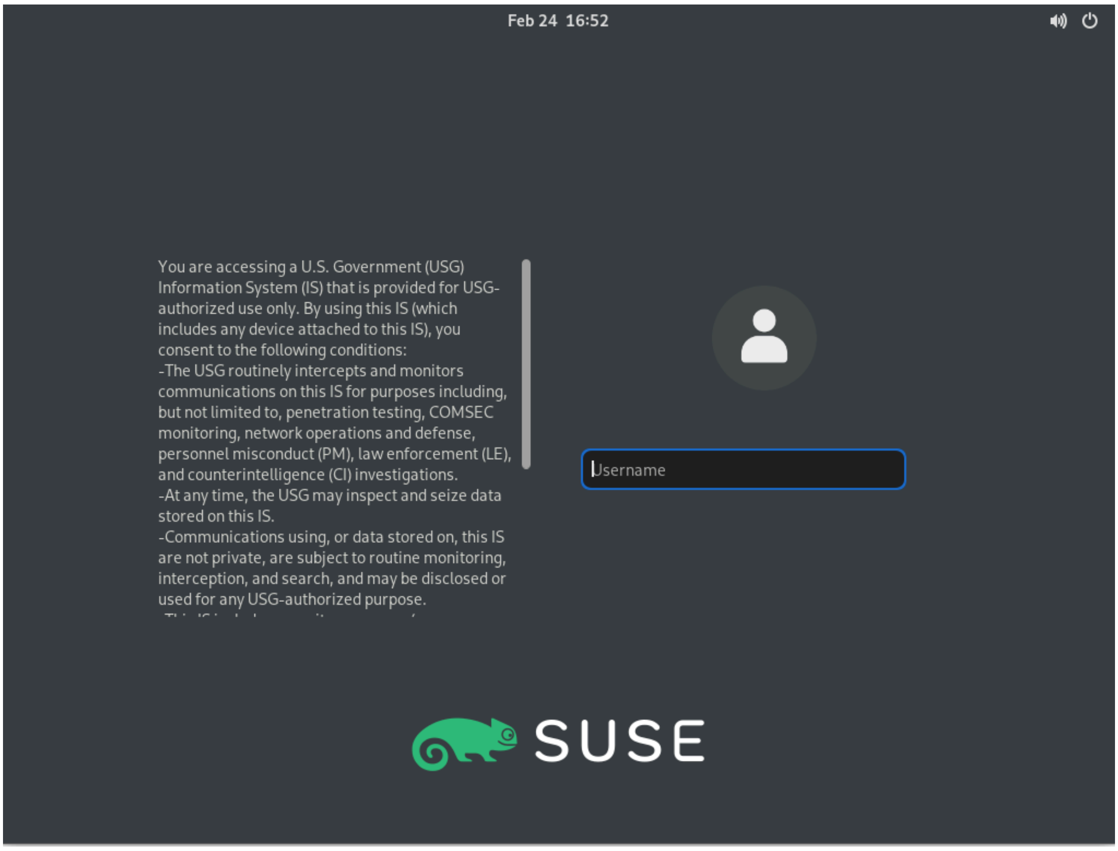
For example, to remediate your system using the STIG Ansible playbook for SUSE Linux Enterprise 15 provided by the `SCAP Security Guide`, use the following command.

Warning: System configuration changes

The following command alters the configuration of your system immediately. Make sure to test this thoroughly in a non-production system first.

```
> sudo ansible-playbook -i "localhost," -c local \
    /usr/share/scap-security-guide/ansible/sle15-playbook-stig.yml
```

After the playbook has finished, you are prompted to log in to your system, which is now compliant to the chosen policy.



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.

5 Using a tailored STIG profile

The standard or default STIG profile is sufficient for most deployments. In addition, you can create, use for evaluation and apply *tailoring files* to tailor SCAP Security Guide content. Using tailoring files, you can change the behavior of a profile without directly modifying its standard configurations.

The following sections provide examples of creating tailoring files using either SCAP Workbench or the `autotailor` command-line utility, and then applying the tailoring file using the `ssg-apply` command-line utility.

Tip: Generalized tailoring

Although the following sections provide examples of tailoring for the STIG profile, you use a similar procedure for tailoring other profiles that are valid for your target system.

5.1 Creating a tailoring file

Tailoring files are XML files containing information about the deviation from the standard SCAP Security Guide content for a profile. You create a tailoring file when you override certain default rules of a standard profile, and save that information along with necessary metadata as an XML file. Once created, you can apply the tailoring file using a suitable program such as the `ssg-apply` utility.

SUSE recommends using any of the following methods of creating a tailoring file:

- Manually, using the SCAP Workbench. This method is best suited when you are unsure of the rules that you want to override in the standard content of a profile, and would prefer the convenience of a graphical software.
- Automatically, using the `autotailor` command-line tool which is bundled with the `openscap-utils` package. This method is best suited when you are sure of all the information that you need to create a tailoring file.

5.1.1 Creating tailoring files using SCAP Workbench

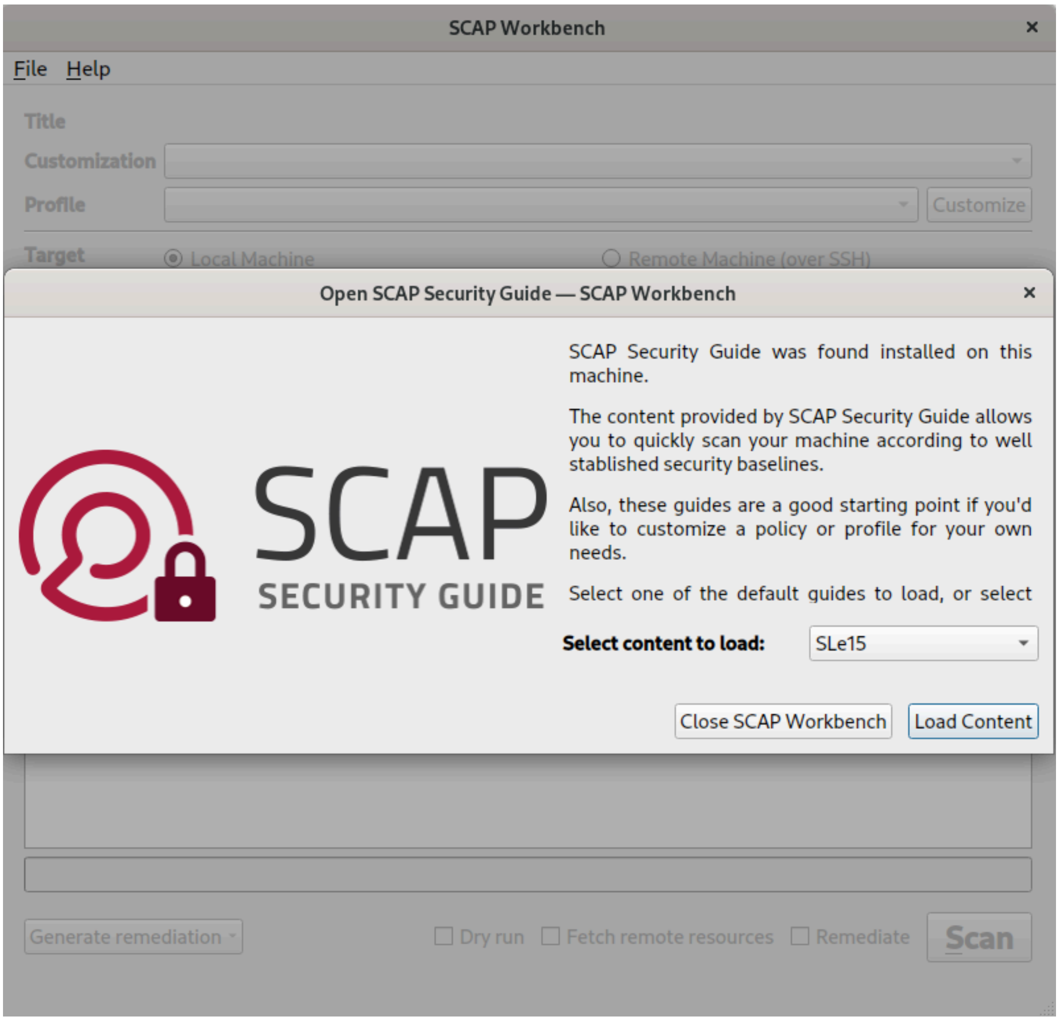
This section provides an example procedure for creating a tailoring file based on the standard STIG profile, using the SCAP Workbench graphical software. You can use a similar procedure to create tailoring files for any other valid profile.

As a prerequisite, ensure that you have installed the necessary packages, as described in the section https://documentation.suse.com/compliance/all/html/SLES-openscap/index.html#openscap-installation ↗.

1. Start SCAP Workbench by invoking it in the terminal:

```
> scap-workbench
```

2. Depending on whether you are using SUSE Linux Enterprise 15 or SUSE Linux Enterprise 12, select either *SLe15* or *SLe12* from the *Select content to load* drop-down list. In this example procedure, we select *SLe15*.



SCAP Security Guide was found installed on this machine.

The content provided by SCAP Security Guide allows you to quickly scan your machine according to well stablished security baselines.

Also, these guides are a good starting point if you'd like to customize a policy or profile for your own needs.

Select one of the default guides to load, or select

Select content to load: SLe15

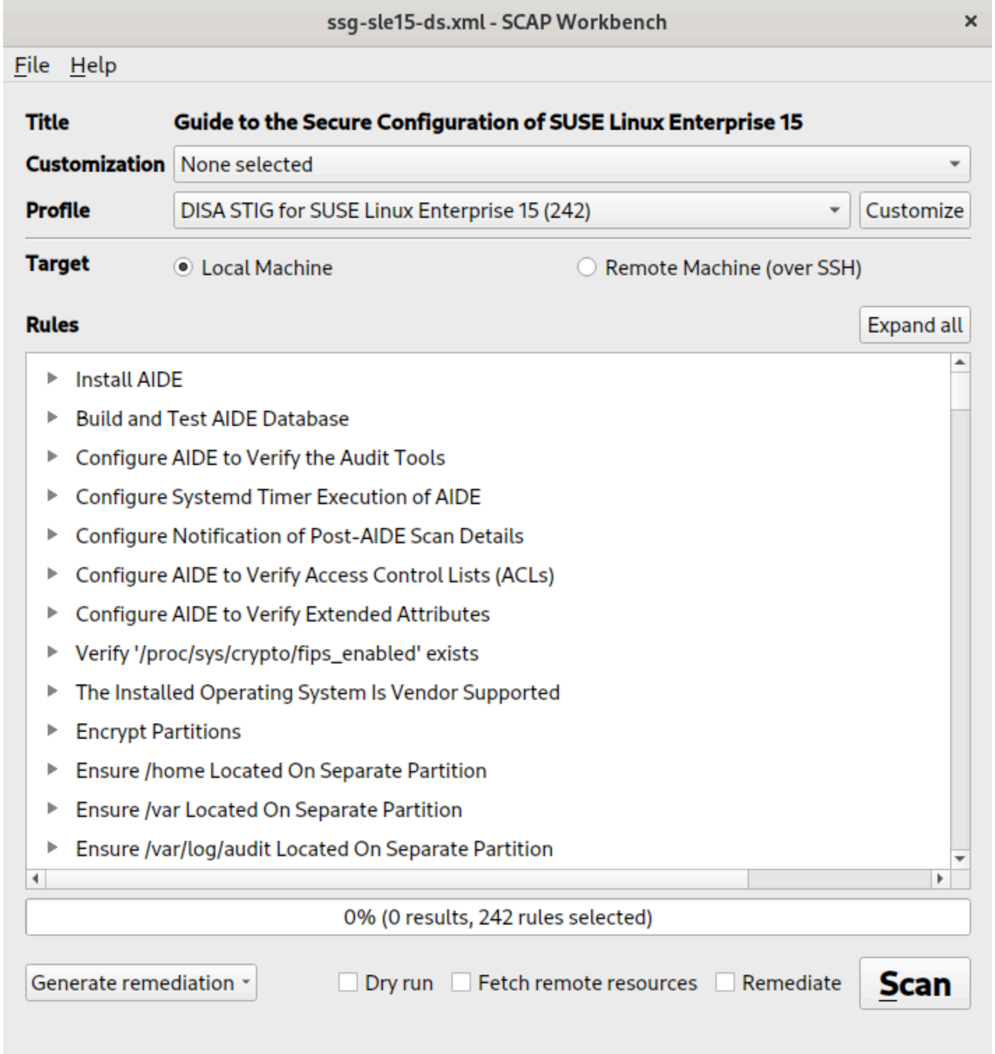
FIGURE 1: SCAP WORKBENCH—SELECT CONTENT TO LOAD

3. Click *Load Content*.

4. In the next window, titled *Guide to the Secure Configuation of SUSE Linux Enterprise 15*, perform the following steps:

   a. From the *Profile* drop-down list, select the profile that you want to customize. In this example, we select *DISA STIG for SUSE Linux Enterprise 15 (242)*. The number within parenthesis at the end of the profile name represents the number of rules that comprise your selected profile. For example, DISA STIG for SUSE Linux Enterprise 15 has 242 rules.

   b. *Optionally*, if your target is a remote system, select the *Remote Machine (over SSH)* and provide necessary information.
      In this example procedure, we assume that the target system is your *Local Machine*.



ssg-sle15-ds.xml - SCAP Workbench

Title Guide to the Secure Configuration of SUSE Linux Enterprise 15

Customization None selected

Profile DISA STIG for SUSE Linux Enterprise 15 (242)

Target ● Local Machine ○ Remote Machine (over SSH)

Rules

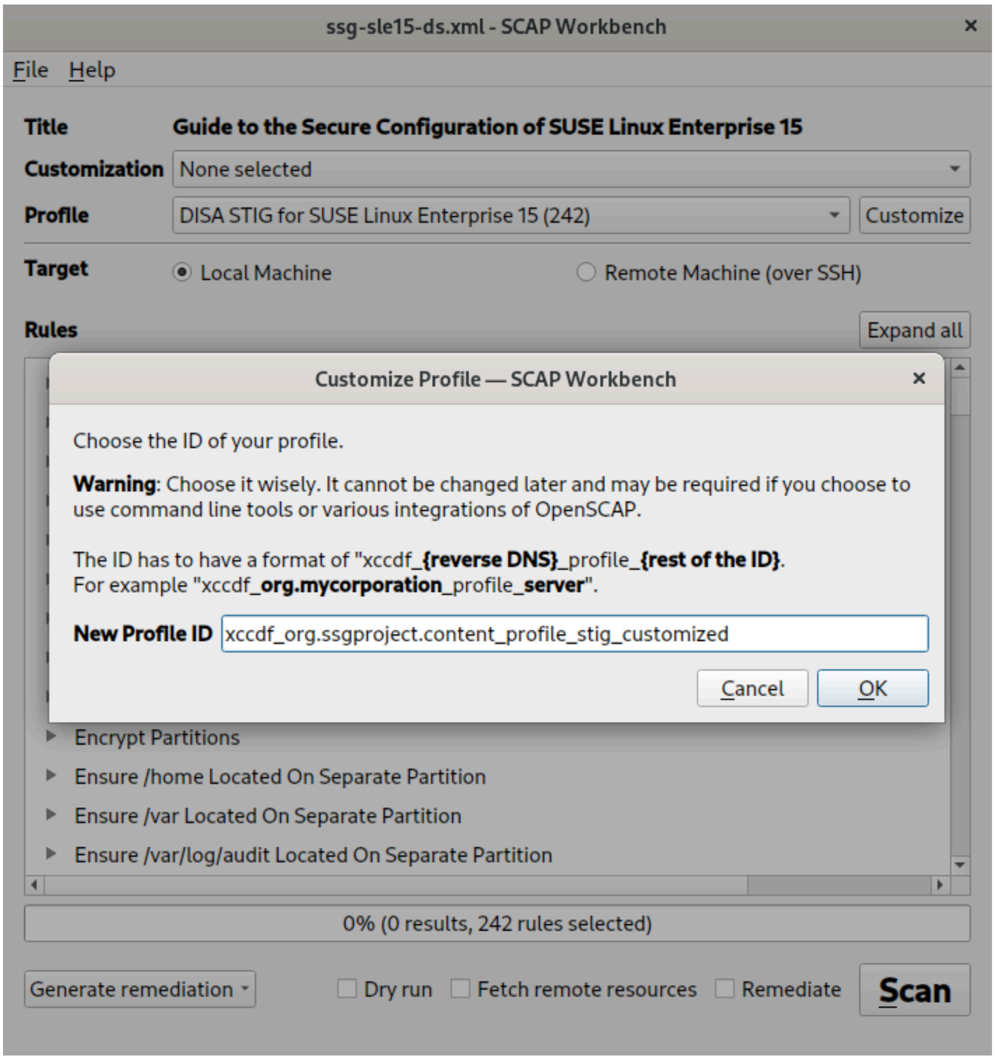
- Install AIDE
- Build and Test AIDE Database
- Configure AIDE to Verify the Audit Tools
- Configure Systemd Timer Execution of AIDE
- Configure Notification of Post-AIDE Scan Details
- Configure AIDE to Verify Access Control Lists (ACLs)
- Configure AIDE to Verify Extended Attributes
- Verify '/proc/sys/crypto/fips_enabled' exists
- The Installed Operating System Is Vendor Supported
- Encrypt Partitions
- Ensure /home Located On Separate Partition
- Ensure /var Located On Separate Partition
- Ensure /var/log/audit Located On Separate Partition

0% (0 results, 242 rules selected)

□ Dry run □ Fetch remote resources □ Remediate

FIGURE 2: SCAP WORKBENCH—DISA STIG PROFILE

c. Click *Customize*, edit the *New Profile ID* field if necessary, and click *OK*. The default *New Profile ID* provided by SCAP Workbench for the selected profile is `xccdf_org.ssgproject.content_profile_stig_customized`.



ssg-sle15-ds.xml - SCAP Workbench

Title: Guide to the Secure Configuration of SUSE Linux Enterprise 15

Customization: None selected

Profile: DISA STIG for SUSE Linux Enterprise 15 (242)

Target: ● Local Machine ○ Remote Machine (over SSH)

Customize Profile — SCAP Workbench

Choose the ID of your profile.

Warning: Choose it wisely. It cannot be changed later and may be required if you choose to use command line tools or various integrations of OpenSCAP.

The ID has to have a format of "xccdf_**{reverse DNS}**_profile_**{rest of the ID}**.
For example "xccdf_**org.mycorporation**_profile_**server**".

New Profile ID: xccdf_org.ssgproject.content_profile_stig_customized

Encrypt Partitions
Ensure /home Located On Separate Partition
Ensure /var Located On Separate Partition
Ensure /var/log/audit Located On Separate Partition

0% (0 results, 242 rules selected)

□ Dry run □ Fetch remote resources □ Remediate

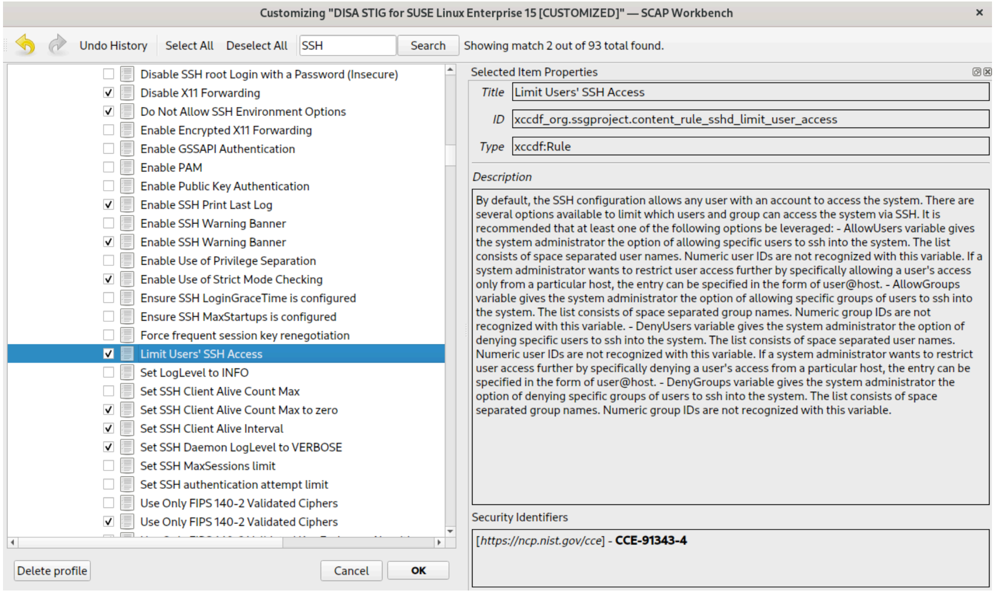
FIGURE 3: SCAP WORKBENCH—CUSTOMIZE STIG PROFILE

5. In the next window titled *Customizing "DISA STIG for SUSE Linux Enterprise 15 [CUSTOMIZED]"—SCAP Workbench*, perform the following steps:

a. Override the default rules by selecting or deselecting them. For example, we select the checkbox next to the rule *Limit Users' SSH Access* to further harden the target system's access over SSH. You can select or deselect multiple rules.

Tip: When unsure, read the rule's description

Before selecting or deselecting the checkbox next to the rule, you can click the rule and read the *Description* provide at the right pane of the window.



Customizing "DISA STIG for SUSE Linux Enterprise 15 [CUSTOMIZED]" — SCAP Workbench
×
Undo History
Select All
Deselect All
SSH
Search

Showing match 2 out of 93 total found.

- ☐ Disable SSH root Login with a Password (Insecure)
- ☑ Disable X11 Forwarding
- ☑ Do Not Allow SSH Environment Options
- ☐ Enable Encrypted X11 Forwarding
- ☐ Enable GSSAPI Authentication
- ☐ Enable PAM
- ☐ Enable Public Key Authentication
- ☑ Enable SSH Print Last Log
- ☐ Enable SSH Warning Banner
- ☑ Enable SSH Warning Banner
- ☐ Enable Use of Privilege Separation
- ☑ Enable Use of Strict Mode Checking
- ☐ Ensure SSH LoginGraceTime is configured
- ☐ Ensure SSH MaxStartups is configured
- ☐ Force frequent session key renegotiation
- ☑ Limit Users' SSH Access
- ☐ Set LogLevel to INFO
- ☐ Set SSH Client Alive Count Max
- ☑ Set SSH Client Alive Count Max to zero
- ☑ Set SSH Client Alive Interval
- ☑ Set SSH Daemon LogLevel to VERBOSE
- ☐ Set SSH MaxSessions limit
- ☐ Set SSH authentication attempt limit
- ☐ Use Only FIPS 140-2 Validated Ciphers
- ☑ Use Only FIPS 140-2 Validated Ciphers

Selected Item Properties

Title Limit Users' SSH Access

ID xccdf_org.ssgproject.content_rule_sshd_limit_user_access

Type xccdf:Rule

Description

By default, the SSH configuration allows any user with an account to access the system. There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged: - AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically allowing a user's access only from a particular host, the entry can be specified in the form of user@host. - AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. - DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host. - DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

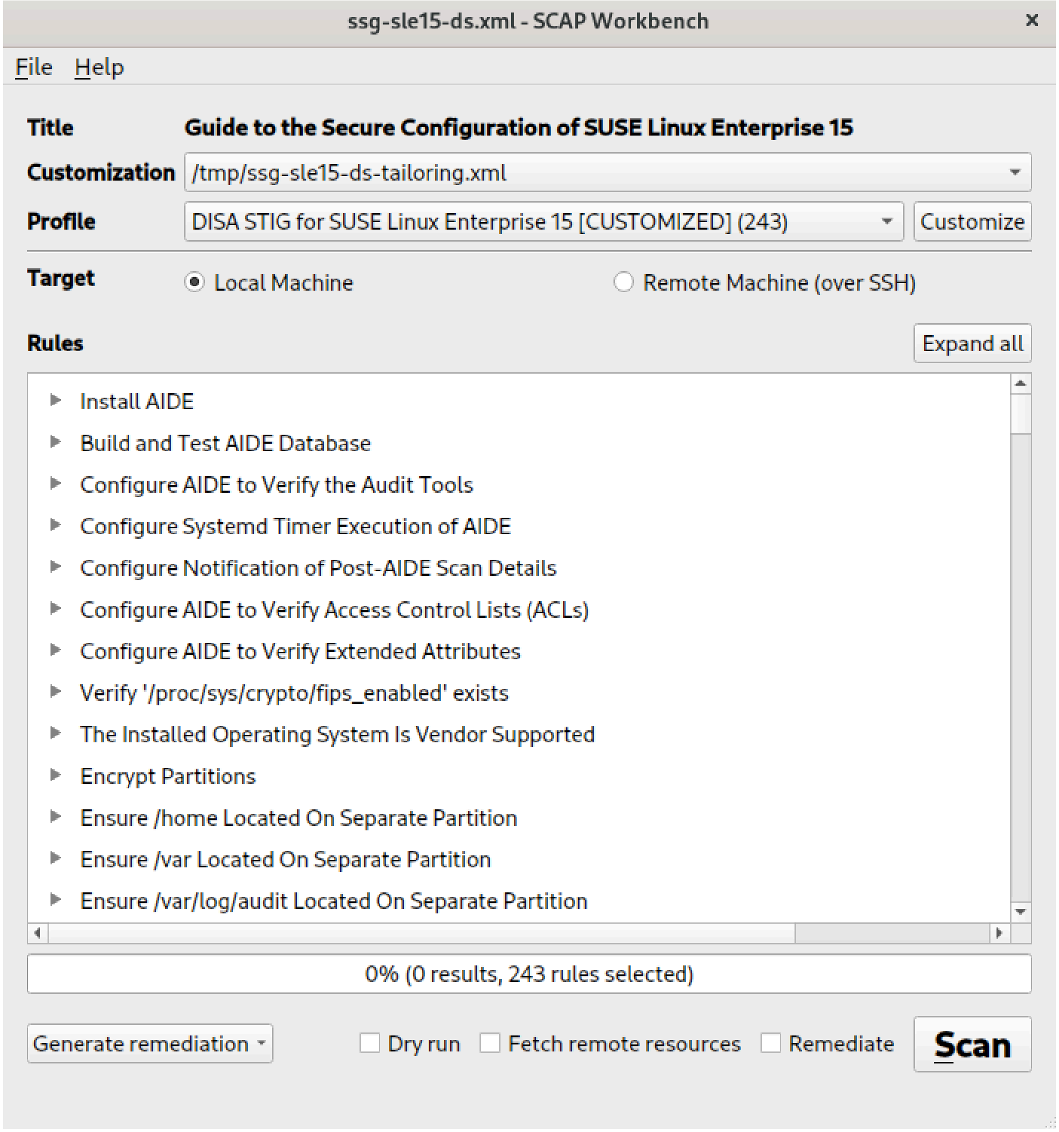
Security Identifiers

[*https://ncp.nist.gov/cce*] - **CCE-91343-4**

FIGURE 4: SCAP WORKBENCH—SELECT RULE

b. When you are sure about the override of rules, click *OK*.

6. On returning to the *home* window of SCAP Workbench, notice that the *Customization* field has changed to *(unsaved changes)*.
   Using the menu at the top left of the window, save the customization by clicking *File* › *Save Customization Only* and choosing the path of the tailoring file as `/tmp/ssg-sle15-ds-tailoring.xml`.
   When saved, the *Customization* field displays the path to the tailoring file. In addition, the name of the new *Profile* contains the suffix `(243)`, which indicates that an additional rule has been selected, as compared to the default of 242 rules.



ssg-sle15-ds.xml - SCAP Workbench

Title: Guide to the Secure Configuration of SUSE Linux Enterprise 15

Customization: /tmp/ssg-sle15-ds-tailoring.xml

Profile: DISA STIG for SUSE Linux Enterprise 15 [CUSTOMIZED] (243)

Target: ● Local Machine ○ Remote Machine (over SSH)

Rules

- Install AIDE
- Build and Test AIDE Database
- Configure AIDE to Verify the Audit Tools
- Configure Systemd Timer Execution of AIDE
- Configure Notification of Post-AIDE Scan Details
- Configure AIDE to Verify Access Control Lists (ACLs)
- Configure AIDE to Verify Extended Attributes
- Verify '/proc/sys/crypto/fips_enabled' exists
- The Installed Operating System Is Vendor Supported
- Encrypt Partitions
- Ensure /home Located On Separate Partition
- Ensure /var Located On Separate Partition
- Ensure /var/log/audit Located On Separate Partition

0% (0 results, 243 rules selected)

□ Dry run □ Fetch remote resources □ Remediate

FIGURE 5: SCAP WORKBENCH—SAVE TAILORING FILE

7. *Optionally*, inspect the tailoring file by opening it with a text editor of your choice. Based on the example override of rules, the tailoring file contains the following information.

```
<?xml version="1.0" encoding="UTF-8"?>
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2" id="xccdf_scap-
workbench_tailoring_default">
  <xccdf:benchmark href="/tmp/scap-workbench-sbgnfq/ssg-sle15-ds.xml"/>
  <xccdf:version time="2024-01-25T07:21:34">1</xccdf:version>
  <xccdf:Profile id="xccdf_org.ssgproject.content_profile_stig_customized"
 extends="xccdf_org.ssgproject.content_profile_stig">
    <xccdf:title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US"
 override="true">DISA STIG for SUSE Linux Enterprise 15 [CUSTOMIZED]</xccdf:title>
```

```
    <xccdf:description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US"
 override="true">This profile contains configuration checks that align to the
DISA STIG for SUSE Linux Enterprise 15 V1R4.</xccdf:description>
    <xccdf:select idref="xccdf_org.ssgproject.content_rule_sshd_limit_user_access"
 selected="true"/>
  </xccdf:Profile>
</xccdf:Tailoring>
```

5.1.2 Creating tailoring files using **autotailor**

There might be deployments where installing a graphical software such as SCAP Workbench is not suitable. In even more sensitive deployments, the customization of a remote target machine over SSH from a client machine running SCAP Workbench might also not be an option.

In such situations, the **`autotailor`** command-line tool that comes bundled with the `openscap-utils` is a suitable choice. However, you must be sure of all the information necessary for creating the tailoring file.

To create a tailoring file with **`autotailor`**, use the following syntax:

```
> autotailor \
  --select RULE_ID ❶ \
  --unselect RULE_ID ❷ \
  --var-value VAR=VALUE ❸ \
  --output TAILORING_FILE ❹ \
  --new-profile-id NEW_PROFILE_ID ❺ \
  DS_FILENAME ❻ \
  BASE_PROFILE_ID ❼
```

❶ `--select RULE_ID` adds a rule with `RULE_ID`. To select multiple rules, you can use this argument multiple times.

❷ `--unselect RULE_ID` discards a rule with `RULE_ID`. To discard multiple rules, you can use this argument multiple times.

❸ `--var-value VAR=VALUE` specifies modification of the XCCDF value in the form `VARIABLE=VALUE`.

❹ `TAILORING_FILE` specifies the path of the tailoring file, which is the final *output* of the **`autotailor`** tool.

❺ Specifies the ID of the new customized profile that you want to create.

❻ Specifies the path to the SCAP source data stream that is tailored.

❼ Specifies the original or base profile ID that you want to customize.

- As an **example**, run the following command to generate a tailoring file that is similar to the one created by using SCAP Workbench in the previous section:

```
> autotailor \
  --select sshd_limit_user_access❶ \
  --output /tmp/ssg-sle15-ds-tailoring.xml❷ \
  --new-profile-id stig_customized❸ \
  /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❹ \
  stig❺
```

❶ The ID of the *Limit Users' SSH Access* rule.

❷ The path to the tailoring file, which is the output.

❸ The ID of the new customized profile.

❹ The path to the SCAP Security Guide content of the original STIG profile.

❺ The name of the original STIG profile.

For more information about the `autotailor` tool, read its help information by running `autotailor -h` or refer to its man page by running `man autotailor`.

5.2 Scanning using a tailoring file

You can use a tailoring file and the `oscap` command-line tool to scan and evaluate your target system based on a customized data stream.

To evaluate your target system using a tailoring file created earlier, perform the following steps:

1. List the profiles in the tailoring file by running the following command:

```
> oscap info /tmp/ssg-sle15-ds-tailoring.xml❶
Document type: XCCDF Tailoring
Imported: TIMESTAMP
Benchmark Hint: /tmp/scap-workbench-VIdbAj/ssg-sle15-ds.xml
Profiles:
 Title: DISA STIG for SUSE Linux Enterprise 15 [CUSTOMIZED]
  Id: xccdf_org.ssgproject.content_profile_stig_customized
```

❶ The path to the tailoring file created earlier, using either SCAP Workbench or `autotailor`.

2. Evaluate the target system based on the tailoring file by running the following command:

```
> oscap xccdf eval \
--profile xccdf_org.ssgproject.content_profile_stig_customized❶ \
--tailoring-file /tmp/ssg-sle15-ds-tailoring.xml❷ \
--results /tmp/results.xml❸ \
/usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❹
```

❶ The ID reference of the new customized profile.

❷ The path to the tailoring file created earlier.

❸ The path to store the results of the evaluation in a machine-readable XML format.

❹ The path to the SCAP Security Guide content for the standard STIG profile.

Note: Redirection of results

Apart from storing the results of the scan in an XML file, **`oscap`** displays the results of the evaluation in a human-readable format on the screen. If you redirect the stream of human-readable results to a file, the debug logs are displayed on the screen.

5.3 Applying a tailoring file

After you create a tailoring file either using SCAP Workbench or **`autotailor`**, you must apply the custom profile to harden your target system. SUSE recommends using the **`ssg-apply`** command-line tool.

5.3.1 Applying tailoring file using **`ssg-apply`**

`ssg-apply` is a command-line tool maintained by SUSE and is part of the `ssg-apply` package. You can install it by running the following command:

```
> sudo zypper install -y ssg-apply
```

For detailed information on `ssg-apply`, refer to `/usr/share/doc/packages/ssg-apply/README`.

To apply the tailoring file that you have already created using SCAP Workbench or **`autotailor`**, perform the following steps:

1. As a best practice, create a copy of `/etc/ssg-apply/default.conf` with the name `/etc/ssg-apply/override.conf`. The new file must contain information pointing to the overridden or customized configuration.

   ```
   > sudo cp /etc/ssg-apply/default.conf /etc/ssg-apply/override.conf
   ```

2. Edit the `/etc/ssg-apply/override.conf` file to make its content similar to the following:

   ```
   #
   # This is the configuration file for the ssg-apply executable.
   #

   #
   # content-file - scap-security-guide content to be used for eval/remediation
   #
   content-file=/usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml

   #
   # profile - profile as specified in content-file
   #
   profile=stig

   #
   # remediation setting - Take care before changing this setting to "yes",
   # as enabling remediation will likely make changes to the system.
   #
   remediate=no

   #
   # tailoring-file - tailoring file to disable specific rules
   #
   tailoring-file=/tmp/ssg-sle15-ds-tailoring.xml❶
   ```

   ❶ The path to the tailoring file created using SCAP Workbench or **`autotailor`**.

3. Apply the tailoring file by running the following command:

   ```
   > ssg-apply
   ```

4. *Optionally*, after running **`ssg-apply`**, you can observe the following:

   a. The output of OpenSCAP in the `/var/log/ssg-apply/ssg-apply-TIMESTAMP.out` files.
   For example, you can find the line number containing the mention of the *Limit Users' SSH Access* rule using the following command:

   ```
   > cat /var/log/ssg-apply/ssg-apply-TIMESTAMP.out | grep -n
    sshd_limit_user_access
   1180:xccdf_org.ssgproject.content_rule_sshd_limit_user_access
   ```

   Then you can locate the lines containing the status of the *Limit Users' SSH Access* rule in the `/var/log/ssg-apply/ssg-apply-TIMESTAMP.out` file:

   ```
   1179 Limit Users' SSH Access
   1180 xccdf_org.ssgproject.content_rule_sshd_limit_user_access
   1181 CCE-91343-4
   1182 faillt
   ```

   b. The debug logs in the `/var/log/ssg-apply/ssg-apply-TIMESTAMP.log` files.

6 Working with checklists in DISA STIG Viewer

DISA STIG Viewer is a Java-based graphical user interface to open content and create checklists for managing the STIG security settings on your system or network.

6.1 Installing DISA STIG Viewer

The *DISA STIG Viewer* application is available as a ZIP archive from https://public.cyber.mil/stigs/stig-viewing-tools/. Download the Linux version of the *DISA STIG Viewer*.

To install *DISA STIG Viewer*, unpack the ZIP archive. In the directory with the extracted files, start the *DISA STIG Viewer* with **`./STIGViewer`**.

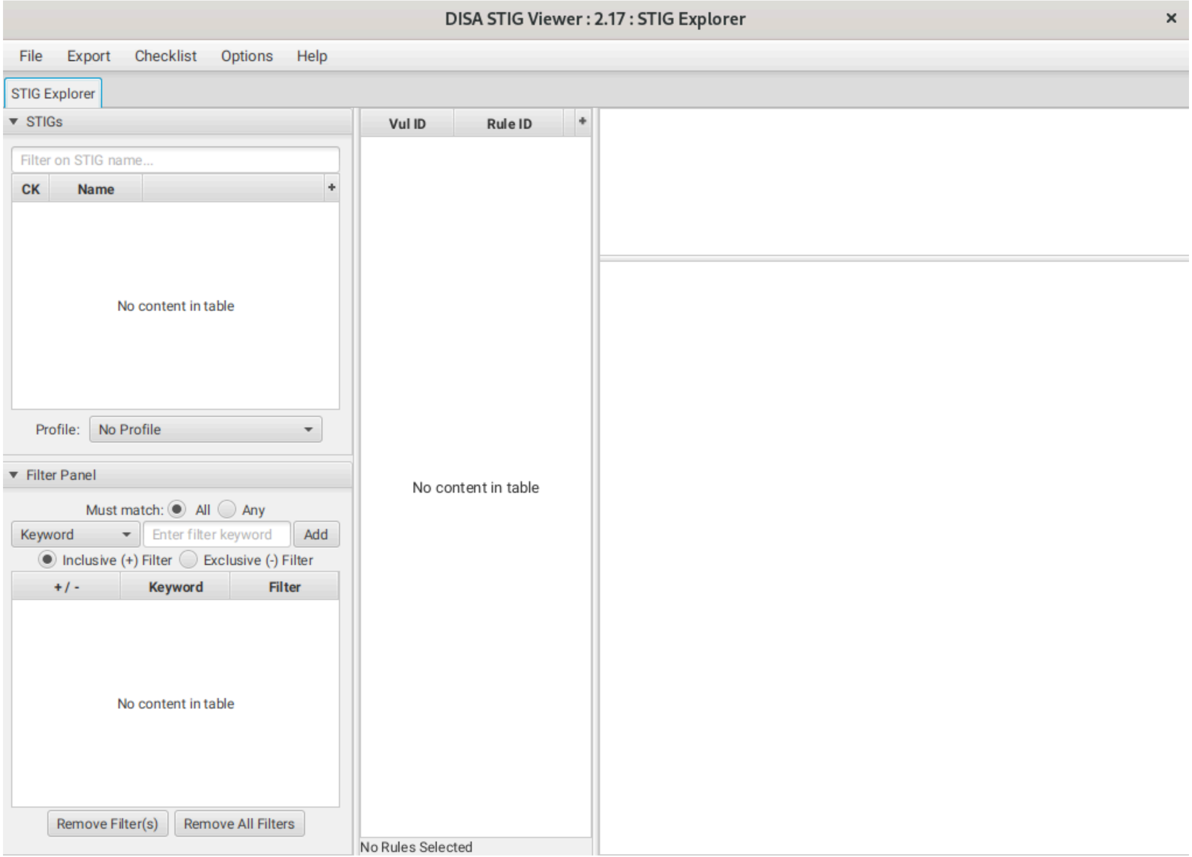


FIGURE 6: DISA STIG VIEWER—MAIN WINDOW

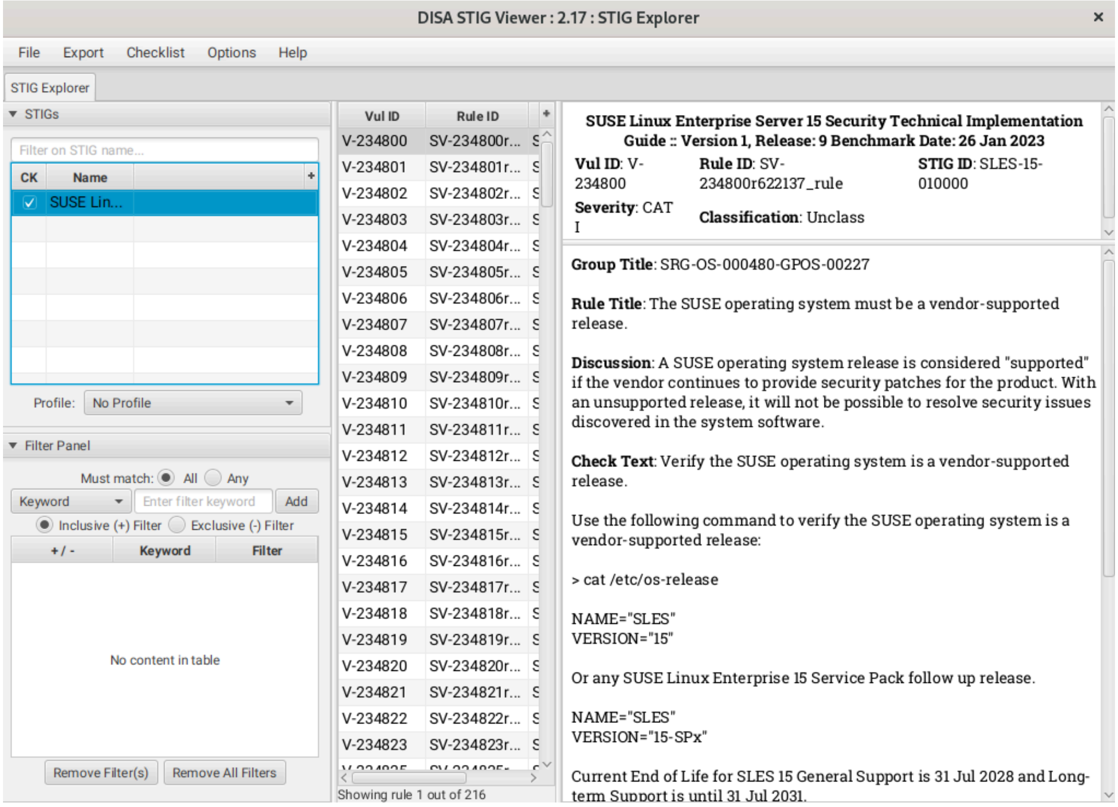
6.2 Using DISA STIG Viewer

To view a Security Technical Implementation Guide for SUSE Linux Enterprise, you have the following two options.

PROCEDURE 1: IMPORTING FROM A ZIP ARCHIVE

You can download a ZIP archive with the STIG checklist for your SUSE Linux Enterprise version (12 or 15).

1. Go to https://public.cyber.mil/stigs/downloads/ ↗.
2. In the *Search* field, enter SUSE and select and download the Security Technical Implementation Guide checklist that matches the SUSE Linux Enterprise system you want to harden.
3. In *DISA STIG Viewer*, click *File* › *Import STIG* and select the downloaded ZIP archive.
4. Enable the checkbox beneath the entry in the *STIG Explorer* panel to show the individual rules in the middle panel and details for each rule on the right-hand side.



Vul ID	Rule ID
V-234800	SV-234800r...
V-234801	SV-234801r...
V-234802	SV-234802r...
V-234803	SV-234803r...
V-234804	SV-234804r...
V-234805	SV-234805r...
V-234806	SV-234806r...
V-234807	SV-234807r...
V-234808	SV-234808r...
V-234809	SV-234809r...
V-234810	SV-234810r...
V-234811	SV-234811r...
V-234812	SV-234812r...
V-234813	SV-234813r...
V-234814	SV-234814r...
V-234815	SV-234815r...
V-234816	SV-234816r...
V-234817	SV-234817r...
V-234818	SV-234818r...
V-234819	SV-234819r...
V-234820	SV-234820r...
V-234821	SV-234821r...
V-234822	SV-234822r...
V-234823	SV-234823r...

SUSE Linux Enterprise Server 15 Security Technical Implementation Guide :: Version 1, Release: 9 Benchmark Date: 26 Jan 2023

Vul ID: V-234800 **Rule ID**: SV-234800r622137_rule **STIG ID**: SLES-15-010000

Severity: CAT I **Classification**: Unclass

Group Title: SRG-OS-000480-GPOS-00227

Rule Title: The SUSE operating system must be a vendor-supported release.

Discussion: A SUSE operating system release is considered "supported" if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.

Check Text: Verify the SUSE operating system is a vendor-supported release.

Use the following command to verify the SUSE operating system is a vendor-supported release:

> cat /etc/os-release

NAME="SLES"
VERSION="15"

Or any SUSE Linux Enterprise 15 Service Pack follow up release.

NAME="SLES"
VERSION="15-SPx"

Current End of Life for SLES 15 General Support is 31 Jul 2028 and Long-term Support is until 31 Jul 2031.

PROCEDURE 2: IMPORTING FROM XCCDF XML

Use the `oscap` command-line tool to generate an XCCDF XML file that can be opened with *DISA STIG Viewer*.

1.
```
> sudo oscap xccdf eval❶ \
      --profile stig❷ \
      --stig-viewer /tmp/results_stig.xml❸ \
      /usr/share/xml/scap/ssg/content/ssg-sle15-ds.xml❹
```

❶ Calls the `oscap xccdf` module and tells it to perform an evaluation (vulnerability scan).

❷ Tells `oscap` to use the `stig` profile for the scan.

❸ Saves the results of the evaluation to `/tmp/results_stig.xml`. This is an XCCDF XML file that can be imported into *DISA STIG Viewer*.

❹ Specifies the `SCAP Security Guide` policy file to use. In this example, we use a policy file in the `DataStream` format that applies to SUSE Linux Enterprise code 15.

2. In *DISA STIG Viewer*, click *File* › *Import STIG* and select the XML file you generated.

3. Enable the checkbox beneath the entry in the *STIG Explorer* panel to show the individual rules in the middle panel.

For more information about *DISA STIG Viewer*, refer to the comprehensive *STIG Viewer 2.x User Guide*, which is available for download at https://public.cyber.mil/stigs/downloads/ ↗, or the README file that you can access from within *DISA STIG Viewer* by selecting *Help* › *View Readme*.

7 Legal Notice

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors nor the translators shall be held liable for possible errors or the consequences thereof.

GNU Free Documentation License

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/ ↗.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with...Texts.” line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.