

UNCLASSIFIED



CANONICAL UBUNTU 24.04 LTS STIG CHEF DOCUMENTATION

Version 1, Release 3

12 November 2025

Developed by DISA for the DOD

UNCLASSIFIED

TABLE OF CONTENTS

	Page
1. BACKGROUND	1
2. INSTALLATION	2
2.1 Download and Install the Chef Client.....	2
2.2 Cookbooks.....	2
3. CONFIGURATION.....	3
3.1 Simple.....	3
3.2 Custom.....	3
4. CONTENT EXTRACTION.....	4

1. BACKGROUND

Chef is an open-source, cross-platform configuration management solution used to define and enforce system and application configurations. This package provides Chef configurations that implement most of the Canonical Ubuntu 24.04 LTS STIG. While the content has been tested during development, all possible system and environmental factors could not be tested. Before using this content in a production environment, perform testing with the intended settings in your own test environment. There is no mandate to use this content; it is published as a resource to assist in the application of security guidance to your systems. Use it in the manner and to the extent that it assists with this goal.

2. INSTALLATION

The following instructions are for standalone installation using [chef-client](#)¹ for testing purposes. A production environment will likely use Chef Server and Chef Clients. Refer [here](#)² for details.

2.1 Download and Install the Chef Client

1. Download the Ubuntu 24.04 x64 Chef Client `.deb` from [here](#)³.
2. Install by running the following example command:

```
sudo dpkg -i <DOWNLOADED_PACKAGE_NAME>.deb
```

2.2 Cookbooks

1. Unzip `ubuntu2404STIG-chef.zip`.
2. Run the included `install.sh` script. This script unzips the included cookbook inside the cookbook directory.

¹ https://docs.chef.io/ctl_chef_client.html

² https://docs.chef.io/server_components.html

³ https://omnitruck.chef.io/stable/chef/download?p=ubuntu&pv=24.04&m=x86_64

3. CONFIGURATION

3.1 Simple

To apply the default STIG Chef configuration to the local machine only, run the **enforce.sh** script to enforce the STIG. To tailor the configuration, follow the steps in the next section.

3.2 Custom

To customize, adjust the attributes in the `cookbooks\ubuntu2404STIG\attributes\default.rb` file. This file contains configuration data to define which configuration settings to manage and the values for these settings. Edit this configuration file in a text editor to best suit each system's requirements as needed. For example, to turn off STIG rule ID 270656, set the "Manage" attribute equal to **false**. To set STIG rule ID 270732's minimum password length to 20, set the "`_etc_security_pwquality_conf_Line`" attribute to **'minlen = 20'**.

```
default['ubuntu2404STIG']['stigrule_270656']['Manage'] = false
default['ubuntu2404STIG']['stigrule_270656']['Setting']['audit_Action'] =
:install

default['ubuntu2404STIG']['stigrule_270732']['Manage'] = true
default['ubuntu2404STIG']['stigrule_270732']['Setting']['_etc_security_pwquali
ty_conf_Line'] = 'minlen = 15'
```

For more information on attributes, refer [here](#).

Note: While useful for testing, this approach is not recommended for a production Chef Server environment. Rather than changing the cookbook defaults, which may change in future versions of the cookbook, attributes should be overridden using Chef capabilities such as [roles](#) or [environments](#).

4. CONTENT EXTRACTION

This compliance extraction methodology returns results based on a system's compliance with the enforcement content. This may be different from STIG compliance. For example, multiple values may be allowed by the STIG but will be marked as "fail" if the value does not match the single exact value in the enforcement content. Additionally, if a value is customized in such a way to violate a STIG rule, it will be marked as "pass" since it matches the enforcement content's expected value.

At the completion of a successful Chef run, content extraction of the configuration results into XCCDF results can be performed via a Chef handler. Use of this handler can be controlled by modifying the following variable in the `cookbooks/ubuntu2404STIG/attributes/default.rb` file:

```
default['ubuntu2404STIG']['XCCDF_result']['Manage'] = true
```

Configuration of the handler is controlled by modifying the following variables in the `cookbooks/ubuntu2404STIG/recipes/default.rb` file:

```
chef_handler 'Chef::Handler::StigXml' do
  source "#{Chef::Config[:file_cache_path]}/stig_xml.rb"
  arguments :stigName => ' U_CAN_Ubuntu_24-04_LTS_STIG_V1R3_Manual-
xccdf.xml', :path => '/path/where/to/write/results.xml'
```

The above resource controls the arguments to the handler writing the XCCDF results file to the `:path` using the manual STIG named `:stigName`. The XCCDF results file is output by default as `/tmp/xccdf-results.xml` if no `:path` is provided.

Note: The STIG name provided above should match the STIG release and version number for which the Chef content is built.

Chef provides a means of checking compliance without enforcement called `--why-run` mode. To use this mode, run the following:

```
chef-client -z -o ubuntu2404STIG --why-run
```

Note: For the content extraction handler to function, a prior run without `--why-run` must have completed successfully.