Ubuntu Pro

Canonical Group Ltd

May 16, 2024

CONTENTS

Ubuntu Pro is a comprehensive subscription for open-source software security and management running on Ubuntu LTS. It provides a suite of services, including advanced tooling and optional phone and ticket support, to give you confidence in the security of your Ubuntu infrastructure.

Every organisation faces its own unique set of challenges. Ubuntu Pro empowers you by providing a single point of access to a range of specialist Canonical technologies that you can choose from to suit your needs. You can patch, monitor and harden your Ubuntu estate while having access to expert support.

Ubuntu Pro is also available for free for personal and small-scale commercial use on up to 5 machines.

CHAPTER

ONE

IN THIS DOCUMENTATION

Start here Get started with Ubuntu Pro: *Set up your account*, *attach a machine to your subscription* and learn *how to use the Pro client*

Using the Ubuntu Pro client Step-by-step guides showing you how to *manage services on the command line* with the Pro Client

Understanding Ubuntu Pro Learn more about topics such as the *Canonical Support process*, *what each Pro service provides*, and *how to use Pro in an airgapped setup*

Popular questions

- *Why can't I access my Ubuntu Pro account?*
- *How do I attach a machine to my subscription?*
- *How are active machines calculated?*
- *How do I set up Ubuntu Pro on offline machines?*

CHAPTER

TWO

NEED HELP?

The documentation above should answer most questions, but if you do need further help, consider checking out our FAQ for Ubuntu Pro.

2.1 Start here

For new customers, new users on existing accounts, and new free token users, we recommend the following documentation for a quick start with Ubuntu Pro:

2.1.1 Initial account setup

Instructions on accessing the Ubuntu Pro websites, including troubleshooting guidance for common issues.

Ubuntu Pro: initial account setup

Welcome to Ubuntu Pro, for new subscribers and users.

This page will introduce you to the basics of your Ubuntu Pro subscription. This will ensure that when you need help, you know where to go and how to get it, quickly and efficiently.

On an AWS or Azure metered plan?

Are you on a metered plan purchased directly from AWS or Azure? If so, this document does not apply to you. Instead see:

- Get started with Ubuntu Pro on AWS
- Get started with Ubuntu Pro on Azure

Ubuntu One

The first thing we need you to do is log in.

Access to the Ubuntu Pro customer portals is mediated through **Ubuntu One Single Sign On**. If you have an Ubuntu One account already, go straight to *log in to the Ubuntu Pro dashboard*.

If you do not already have an Ubuntu One account

You will need to know the correct email address for the account (this will be the same email address to which your "Welcome to Ubuntu Pro" message was sent).

If you don't know the address, ask the person who set up your organisation's Ubuntu Pro subscription.

Go to Ubuntu One and select *I do not have an Ubuntu One account*.

Create a new account, using the email address associated with your Ubuntu Pro subscription as the "Preferred email address". If you get a message "An Ubuntu One account already exists with this email", please see *Password reset*.

After verifying your email address, you can access the customer portals. There are three portals:

- Ubuntu Pro dashboard
- Canonical Support Portal
- Landscape (additional set-up will be required)

Ubuntu Pro dashboard

Open the Ubuntu Pro dashboard. This dashboard gives you an overview of your current Ubuntu Pro subscriptions.

Ubuntu Pro token

Here you can see your subscriptions and the **Ubuntu Pro tokens** associated with them. The tokens are required to enable many Ubuntu Pro services. When a service requires your token, get it from here.

For more information about the Ubuntu Pro token, see our dedicated section on *Using the Pro Client*.

Add a secondary user

We recommend that all customers with commercial subscriptions have a secondary user on the Ubuntu Pro dashboard, to ensure continuity of access.

Check *Account users* from the main menu. If a secondary user is not already listed, add one now.

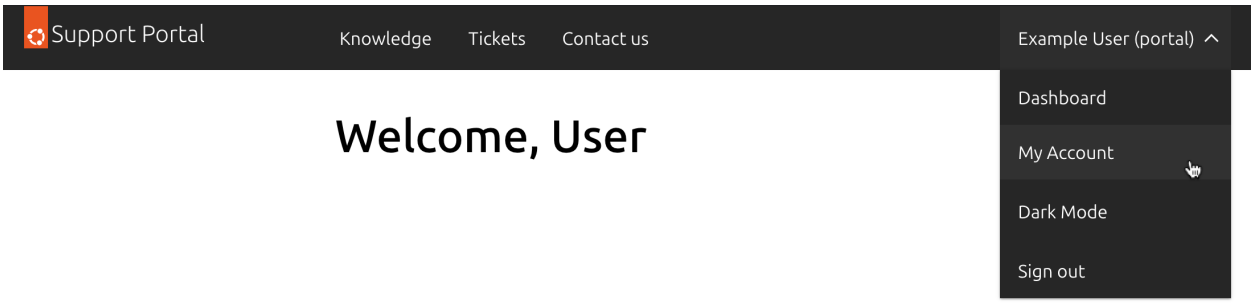
Canonical Support Portal

Open the Canonical Support Portal. The Support Portal provides access to our Knowledge Base. If you have a support contract, this is where to raise support tickets.

Add a secondary user

As before, we recommend adding a secondary user to the portal, to ensure continuity of access.

Open the User menu, and select *My account*.



If a secondary user is not already listed, add one now with the *New user* button. Also select the *Active Ubuntu Pro user* option, so that the new contact is enabled as a Support Portal user.

Landscape

If you have a paid Ubuntu Pro subscription and would like to use Landscape SaaS, contact your Account Manager or Canonical's Customer Success team to request an email invitation to join your Landscape account. Then accept the invitation and follow the instructions. Note that this email may land in your spam folder, so if you have requested it but not seen it, check there (Subject: "You have been invited to the Landscape account [...]", from `noreply+landscape@canonical.com`).

You can find the contact details for Customer Success in the original "Welcome to Ubuntu Pro" message we sent you. If you cannot find the welcome message, go to https://ubuntu.com/ and ask for Customer Success contact details using the LiveChat service.

After initial setup, you can always log into your account at Landscape SaaS.

Once again, we recommend adding a secondary user to the portal, to ensure continuity of access: *Administrators* > *Invite an administrator*.

For information on setting up self-hosted Landscape, refer to *Understanding Landscape*.

If you are having problems accessing the portals, please see *Portal access problems*.

If you have problems with your Ubuntu Pro account

Password reset

The first thing to check is that you have created an Ubuntu One account (note that we do not do this for you). If you have not created an account yet, carefully follow the instructions at *If you do not already have an Ubuntu One account*, then return here.

If that hasn't solved your problem, next check that you are using the correct email address: ask the person who set up your organisation's Ubuntu Pro subscription and try again.

Find the original "Welcome to Ubuntu Pro" message we sent you, and contact the Customer Success team with the details provided. If you cannot find the welcome message, go to https://ubuntu.com/ and ask for Customer Success contact details using the LiveChat service.

Portal access

The Ubuntu Pro portals are:

- Ubuntu Pro dashboard
- Canonical Support Portal
- Landscape SaaS

Users will not have access to the Ubuntu Pro portals unless they have been added as a new user on each one. Simply having an Ubuntu One account does not automatically give a user access.

If you need access to a portal, ask the person who set up your organisation's Ubuntu Pro subscription to add you to the portals required.

Important: Ensure that each individual user on your organisation's Ubuntu Pro account creates their own Ubuntu One account. Accounts cannot be shared by multiple users. Trying to share accounts will often trigger errors.

2.1.2 Setting up the Ubuntu Pro services

Find out how to set up the Ubuntu Pro Client and attach a machine to your subscription, then explore the tool to see what the various commands can do for you.

How to attach a machine to your Ubuntu Pro subscription

To attach your machine to a subscription, run the following command in your terminal:

```
$ sudo pro attach
```

You should see output like this, giving you a link and a code:

```
ubuntu@test:~$ sudo pro attach
Initiating attach operation...

Please sign in to your Ubuntu Pro account at this link:
https://ubuntu.com/pro/attach
And provide the following code: H31JIV
```

Open the link without closing your terminal window.

In the field that asks you to enter your code, copy and paste the code shown in the terminal. Then, choose which subscription you want to attach to. By default, the Free Personal Token will be selected.

If you have a paid subscription and want to attach to a different token, you may want to log in first so that your additional tokens will appear.

Once you have pasted your code and chosen the subscription you want to attach your machine to, click on the "Submit" button.

The attach process will then continue in the terminal window, and you should eventually be presented with the following message:

```
Attaching the machine...
Enabling default service esm-apps
Updating Ubuntu Pro: ESM Apps package lists
Ubuntu Pro: ESM Apps enabled
Enabling default service esm-infra
Updating Ubuntu Pro: ESM Infra package lists
Ubuntu Pro: ESM Infra enabled
Enabling default service livepatch
Installing snapd snap
Installing canonical-livepatch snap
Canonical Livepatch enabled
This machine is now attached to 'Ubuntu Pro - free personal subscription'
```

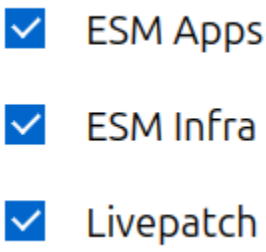
When the machine has successfully been attached, you will also see a summary of which services are enabled and information about your subscription.

Once the Ubuntu Pro Client is attached to your Ubuntu Pro account, you can use it to activate various services, including: access to ESM packages, Livepatch, FIPS, and CIS. Some features are specific to certain LTS releases.

Control of auto-enabled services

Your subscription controls which services are available to you and which ones you can manage via the Ubuntu Pro Dashboard.

Recommended services are auto-enabled by default when attaching a machine. You can choose which of the available services will be automatically enabled or disabled when you attach by toggling them "on" or "off" in the Ubuntu Pro Dashboard.



Available services can always be enabled or disabled on the command line with `pro enable` and `pro disable` after attaching.

If your subscription does not permit you to change the default enabled services via the Dashboard, or if you want to keep the defaults but do not want to auto-enable any services while attaching a particular machine, you can pass the `--no-auto-enable` flag to `attach` in the following way:

```
$ sudo pro attach --no-auto-enable
```

Note: If you want to control which services are enabled during attach, you can *attach with a configuration file* instead.

Get started with Ubuntu Pro Client

The Ubuntu Pro Client (`pro`) provides a simple mechanism for viewing, enabling and disabling Canonical offerings on your system. In this tutorial, we will cover the base `pro` commands that help you to successfully manage Pro on your machine.

Main `pro` commands

When dealing with `pro` through the command line, there are six commands that cover the main functions of the tool. They are:

- `status`
- `attach`
- `refresh`
- `detach`
- `enable`
- `disable`

In this tutorial, we will go through each of these commands and learn how to properly use them. To achieve this without making any modifications to your machine, we will use a Xenial Multipass virtual machine (VM).

Install Multipass

In this tutorial, we will use a Xenial Multipass virtual machine (VM) to avoid making any modifications to your machine. We have chosen Multipass for this tutorial because it allows us to easily launch VMs without requiring any complicated setup.

To install Multipass on your computer, run the following command on your machine:

```
$ sudo snap install multipass
```

Create the Xenial Multipass VM

Now that we have installed Multipass, we can launch our Multipass VM by running this command:

```
$ multipass launch xenial --name dev-x
```

Now we can access the VM by running the command:

```
$ multipass shell dev-x
```

Notice that when you run this command, your terminal username and hostname change to:

```
ubuntu@dev-x
```

This indicates that you are now inside the VM.

Finally, let's run `apt update` and `apt upgrade` on the VM to make sure we are operating on the correct version of Xenial:

```
$ sudo apt update && sudo apt install ubuntu-advantage-tools
```

From now on, every time we say: "run the command" our intention is for you to run that command inside your VM.

Base `pro` commands

status

The `status` command of `pro` will show you the status of any Ubuntu Pro service on your machine. It also helps you to easily verify that your machine is attached to an Ubuntu Pro subscription.

Let's run it on our VM:

```
$ pro status
```

You can expect to see an output similar to this:

```
SERVICE          AVAILABLE  DESCRIPTION
cc-eal           yes        Common Criteria EAL2 Provisioning Packages
cis              yes        Security compliance and audit tools
esm-apps         yes        Expanded Security Maintenance for Applications
esm-infra        yes        Expanded Security Maintenance for Infrastructure
fips             yes        NIST-certified core packages
fips-updates     yes        NIST-certified core packages with priority security updates
livepatch        yes        Canonical Livepatch service
ros              yes        Security Updates for the Robot Operating System
ros-updates      yes        All Updates for the Robot Operating System
```

You can see that the `status` command shows the services available to your machine, while also presenting a short description for each service.

If you also look at the last lines of the output, you can see that this machine is not currently attached to an Ubuntu Pro subscription.

```
This machine is not attached to an Ubuntu Pro subscription.
See https://ubuntu.com/pro
```

attach

We have seen which service offerings are available to us, but to access them we first need to attach an Ubuntu Pro subscription. We can do this by running the `attach` command.

```
$ sudo pro attach
```

You should see output like this, giving you a link and a code:

```
ubuntu@test:~$ sudo pro attach
Initiating attach operation...

Please sign in to your Ubuntu Pro account at this link:
https://ubuntu.com/pro/attach
And provide the following code: H31JIV
```

Open the link without closing your terminal window.

In the field that asks you to enter your code, copy and paste the code shown in the terminal. Then, choose which subscription you want to attach to. By default, the Free Personal Token will be selected, which is fine for the purposes of this tutorial.

Once you have pasted your code and chosen the subscription you want to attach your machine to, click on the "Submit" button.

The attach process will then continue in the terminal window, and you should eventually be presented with the following message:

```
Enabling default service esm-apps
Updating package lists
Ubuntu Pro: ESM Apps enabled
Enabling default service esm-infra
Updating package lists
Ubuntu Pro: ESM Infra enabled
Enabling default service livepatch
Installing canonical-livepatch snap
Canonical livepatch enabled.
This machine is now attached to 'USER ACCOUNT'

SERVICE          ENTITLED  STATUS    DESCRIPTION
cc-eal           yes       disabled  Common Criteria EAL2 Provisioning Packages
cis              yes       disabled  Security compliance and audit tools
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
fips             yes       disabled  NIST-certified core packages
fips-updates     yes       disabled  NIST-certified core packages with priority security␣
↪updates
livepatch        yes       enabled   Canonical Livepatch service
ros              yes       disabled  Security Updates for the Robot Operating System
ros-updates      yes       disabled  All Updates for the Robot Operating System

NOTICES
Operation in progress: pro attach

Enable services with: pro enable <service>
```

(continues on next page)

(continued from previous page)

```
               Account: USER ACCOUNT
        Subscription: USER SUBSCRIPTION
            Valid until: 9999-12-31 00:00:00+00:00
Technical support level: essential
```

From this output, we can see that the `attach` command has introduced the "status" column. This shows which services (specified by your user subscription) have been enabled by default.

After the command ends, `pro` displays the new state of the machine. This status output is exactly what you see if you run the `status` command. Let's confirm this by running the `status` command again:

```
$ pro status
```

Note: You may be wondering why the output of `status` is different depending on whether `pro` is attached or unattached. For more information on why this is, refer to our explanation on the different columns.

Finally, another useful bit at the end of the output for both `attach` and `status` is the contract expiration date:

```
    Account: USER ACCOUNT
Subscription: USER SUBSCRIPTION
Valid until: 9999-12-31 00:00:00+00:00
```

The `Valid until` field describes when your contract will expire, so you can be aware of when it needs to be renewed. Note that if you are using a free token, you will not see this part of the output since free tokens never expire.

refresh

Although *free* tokens never expire, if you buy an Ubuntu Pro subscription and later need to renew your contract, how can you make your machine aware of it?

This is where the `refresh` command comes in:

```
$ sudo pro refresh
```

This command will "refresh" the contract on your machine. It's also really useful if you want to change any definitions on your subscription.

For example, let's assume that you now want `cis` to be enabled by default when attaching. After you modify your subscription on the Ubuntu Pro website to enable it by default, running the refresh command will process the changes you made, and `cis` will then be enabled.

Hint: The `refresh` command does more than just update the contract in your machine. If you would like more information about the command, take a look at this deeper explanation.

enable

There is another way to enable a service that wasn't activated during `attach` or `refresh`. Let us suppose that you now want to enable `cis` on the machine manually. To achieve this, you can use the `enable` command.

Let's try enabling `cis` on our VM by running:

```
$ sudo pro enable cis
```

After running the command, you should see output similar to this:

```
One moment, checking your subscription first
Updating package lists
Installing CIS Audit packages
CIS Audit enabled
Visit https://ubuntu.com/security/cis to learn how to use CIS
```

We can then confirm that `cis` is now enabled by using the `status` command again:

```
$ pro status
```

And you should see:

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
cc-eal           yes       disabled  Common Criteria EAL2 Provisioning Packages
cis              yes       enabled   Security compliance and audit tools
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
fips             yes       disabled  NIST-certified core packages
fips-updates     yes       disabled  NIST-certified core packages with priority security␣
↪updates
livepatch        yes       enabled   Canonical Livepatch service
ros              yes       disabled  Security Updates for the Robot Operating System
ros-updates      yes       disabled  All Updates for the Robot Operating System
```

We can see now that `cis` is marked as `enabled` under "status".

disable

What happens if you don't want a service anymore?

All you need to do is disable that service through `pro`. For example, let's say we changed our mind about `cis` after enabling it, and we now want to disable it instead. We can turn it off by running `disable` on our VM:

```
$ sudo pro disable cis
```

Let's now run `pro status` to see what happened to `cis`:

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
cc-eal           yes       disabled  Common Criteria EAL2 Provisioning Packages
cis              yes       disabled  Security compliance and audit tools
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
fips             yes       disabled  NIST-certified core packages
```

(continues on next page)

(continued from previous page)

```
fips-updates     yes       disabled  NIST-certified core packages with priority security␣
↪updates
livepatch        yes       enabled   Canonical Livepatch service
ros              yes       disabled  Security Updates for the Robot Operating System
ros-updates      yes       disabled  All Updates for the Robot Operating System
```

Now we can see that `cis` status has gone back to being disabled.

Important: The `disable` command doesn't uninstall any package that was installed by the service, or undo any configuration that was applied to the machine – it only removes the access you have to the service.

---

detach

Finally, what if you decide you no longer want this machine to be attached to an Ubuntu Pro subscription?

To disable all of the Ubuntu Pro services and remove the subscription you stored on your machine during `attach`, you can use the `detach` command:

```
$ sudo pro detach
```

Just like the `disable` command, `detach` will not uninstall any packages that were installed by any of the services enabled through `pro`.

Success!

Congratulations! You successfully ran a Multipass VM and used it to try out the six main commands of the Ubuntu Pro Client.

If you want to continue testing the different features and functions of `pro`, you can run the command:

```
$ pro help
```

This will provide you with a full list of all the commands available, and details of how to use them. Feel free to play around with them in your VM and see what else `pro` can do for you!

Close down the VM

When you are finished and want to leave the tutorial, you can shut down the VM by first pressing `CTRL + D` to exit it, and then running the following commands to delete the VM completely:

```
$ multipass delete dev-x
$ multipass purge
```

Next steps

If you would now like to see some more advanced options to configure `pro`, we recommending taking a look at our how-to guides.

If you have any questions or need some help, please feel free to reach out to the `pro` team on *#ubuntu-server* on Libera IRC – we're happy to help!

Alternatively, if you have a GitHub account, click on the "Give feedback" link at the top of this page to leave us a message. We'd love to hear from you!

2.1.3 Accessing technical support

For Ubuntu Pro customers with support contracts, these instructions will show you how to open a support case, including best practices to ensure you get the most out of Canonical support.

How to open a case

To get the best (and fastest possible) results from Canonical Support, take a few moments to ensure that you provide us with the information we need to help you:

Log in to the Support Portal.

Search the Canonical Knowledge Base for articles relevant to your case - your issue may already have a solution.

If no solution is available in the Knowledge Base, select the **New ticket** button on the homepage.

Complete the ticket form. Most fields are self-explanatory, but note:

Description - include:

- exact time & date the problem occurred
- what the steps or actions you took
- what was the result of that action
- what you expected or wanted to happen
- any other information you think is relevant
- any logs, error messages, screenshots

Impact - tell us how the problem affects your organisation

If you are able to share a *sosreport* (below), this will help us respond faster and more accurately.

Sosreports

Canonical uses sosreports, or "state of system" reports, to diagnose and resolve problems. These comprise system logs and configuration data.

When you report a problem with your Ubuntu machine, you can generate and send a sosreport from the affected machine straight away.

Refer to the following articles for information on using sosreports:

- Installing the sosreport tool and generating a sosreport
- Sending a sosreport to Canonical

- Sosreports, data and security

2.2 Using the Pro Client

2.2.1 Configure the Pro client

After you have installed and set up the Pro Client using the instructions in our *setting up the Pro services* section, you may want to configure the tool further.

How to attach with a configuration file

To attach with a configuration file, you must run `pro attach` with the `--attach-config` flag, passing the path of the configuration file you intend to use.

When using `--attach-config` the token must be passed in the file rather than on the command line. This is useful in situations where it is preferred to keep the secret token in a file.

Optionally, the attached config file can be used to override the services that are automatically enabled as a part of the attach process.

Get an Ubuntu Pro token

Retrieve your Ubuntu Pro token from the Ubuntu Pro portal. Log in with your "Single Sign On" credentials, the same credentials you use for https://login.ubuntu.com.

After you have logged in you can go to the Ubuntu Pro Dashboard associated with your user account. It will show you all subscriptions currently available to you and for each associated token.

Note that even without buying anything you can always obtain a free personal token that way, which provides you with access to several of the Ubuntu Pro services.

The attach config file

An attach config file looks like this:

```
token: YOUR_TOKEN_HERE  # required
enable_services:        # optional list of service names to auto-enable
  - esm-infra
  - esm-apps
  - cis
```

And can be passed via the CLI with the following command:

```
sudo pro attach --attach-config /path/to/file.yaml
```

How to configure a proxy

The Ubuntu Pro Client can be configured to use an HTTP/HTTPS proxy as needed for network requests. It will also honour the `no_proxy` environment variable (if set) to avoid using local proxies for certain outbound traffic. In addition, the Ubuntu Pro Client will automatically set up proxies for all programs required for enabling Ubuntu Pro services. This includes APT, snaps, and Livepatch.

HTTP/HTTPS proxies

To configure standard HTTP and/or HTTPS proxies, run the following commands:

```
$ sudo pro config set http_proxy=http://host:port
$ sudo pro config set https_proxy=https://host:port
```

After running the above commands, Ubuntu Pro Client will:

1. Verify that the proxy is working by using it to reach `api.snapcraft.io`
2. Configure itself to use the given proxy for all future network requests
3. Configure `snapd` (if `snapd` is installed) to use the given proxy
4. Configure Livepatch (if Livepatch has already been enabled) to use the given proxy:
    1. If Livepatch is enabled after the `config` command, Ubuntu Pro Client will configure Livepatch to use the given proxy at that time.

To remove HTTP/HTTPS proxy configuration, run the following:

```
$ sudo pro config unset http_proxy
$ sudo pro config unset https_proxy
```

After running the above commands, Ubuntu Pro Client will also remove proxy configuration from `snapd` (if installed) and Livepatch (if enabled).

APT proxies

APT proxy settings are configured separately. To have Ubuntu Pro Client manage your global APT proxy configuration, run the following commands:

```
$ sudo pro config set global_apt_http_proxy=http://host:port
$ sudo pro config set global_apt_https_proxy=https://host:port
```

After running the above commands, Ubuntu Pro Client will:

1. Verify that the proxy works by using it to reach `archive.ubuntu.com` or `esm.ubuntu.com`.
2. Configure APT to use the given proxy by writing an apt configuration file to `/etc/apt/apt.conf.d/90ubuntu-advantage-aptproxy`.

> **Caution:** Any configuration file that comes later in the `apt.conf.d` directory could override the proxy configured by the Ubuntu Pro Client.

To remove the APT proxy configuration, run the following:

```
$ sudo pro config unset global_apt_http_proxy
$ sudo pro config unset global_apt_https_proxy
```

Note: Starting in Pro Client version 27.9, APT proxy config options changed. The old settings: `apt_http_proxy` and `apt_https_proxy` will still work and will be treated the same as `global_apt_http_proxy` and `global_apt_https_proxy`, respectively.

Pro-service-only APT proxies

To set an APT proxy that will only be used for Ubuntu Pro services, use the following commands instead:

```
$ sudo pro config set ua_apt_http_proxy=http://host:port
$ sudo pro config set ua_apt_https_proxy=https://host:port
```

Authenticate your proxy server

If your proxy server requires authentication, you can pass the credentials directly in the URL when setting the configuration, as in:

```
$ sudo pro config set https_proxy=https://username:password@host:port
```

Check the configuration

To see which proxies Ubuntu Pro Client is currently configured to use, you can use the `show` command.

```
$ sudo pro config show
```

The above will output something that looks like the following if there are proxies set:

```
http_proxy              http://proxy
https_proxy             https://proxy
global_apt_http_proxy   http://aptproxy
global_apt_https_proxy  https://aptproxy
```

Or it may look like this if there are no proxies set:

```
http_proxy              None
https_proxy             None
global_apt_http_proxy   None
global_apt_https_proxy  None
```

2.2.2 Enable and disable Pro services

Discover how to enable and manage Ubuntu Pro services individually using the Pro Client.

How to manage Anbox Cloud

To use Anbox, you will need to enable it directly through the Ubuntu Pro Client (`pro`), which will install all the necessary snaps and set up the APT sources needed for the service.

Note: Anbox Cloud is supported on 20.04 and 22.04 releases.

Make sure `pro` is up-to-date

All systems come with `pro` pre-installed through the `ubuntu-advantage-tools` package. To make sure that you're running the latest version of `pro`, run the following commands:

```
sudo apt update && sudo apt install ubuntu-advantage-tools
```

Check the status of the services

After you have *attached your subscription* and updated the `ubuntu-advantage-tools` package, you can check which services are enabled by running the following command:

```
pro status
```

This will show you which services are enabled or disabled on your machine (output truncated for brevity):

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
livepatch        yes       enabled   Canonical Livepatch service
realtime-kernel  yes       disabled  Ubuntu kernel with PREEMPT_RT patches integrated
```

Enable Anbox

To enable Anbox Cloud, run:

```
$ sudo pro enable anbox-cloud
```

Important: The Anbox Cloud service can only be installed on **containers** using the `--access-only` flag. This option will only set up the APT sources for Anbox, but not install any of the snaps.

You should see output like the following, indicating that Anbox Cloud was correctly enabled on your system:

```
One moment, checking your subscription first
Installing required snaps
Installing required snap: amc
Installing required snap: anbox-cloud-appliance
Installing required snap: lxd
Updating package lists
Anbox Cloud enabled
To finish setting up the Anbox Cloud Appliance, run:

$ sudo anbox-cloud-appliance init

You can accept the default answers if you do not have any specific
configuration changes.
For more information, see https://anbox-cloud.io/docs/tut/installing-appliance
```

You have probably noticed that the output states an **additional step** is required to complete the Anbox Cloud setup. Let us run the required command:

```
$ sudo anbox-cloud-appliance init
```

You can now confirm that the service is enabled by running the `pro status` command again. It should contain the following line for `anbox-cloud`:

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
anbox-cloud      yes       enabled   Scalable Android in the cloud
```

Disable the service

If you wish to disable Anbox, you can use the following command to disable it:

```
sudo pro disable anbox-cloud
```

Note that this command will only remove the APT sources, but will not uninstall the snaps.

To also purge the service, removing all the APT packages installed with it, see *how to disable and purge services*.

How to enable CIS or USG

On Ubuntu 20.04 LTS (Focal) and later releases, CIS was replaced by USG. If you are running Focal (or a later release) and want to enable `usg`, then select the **USG** tab below.

Make sure `pro` is up-to-date

All systems come with `pro` pre-installed through the `ubuntu-advantage-tools` package. To make sure that you're running the latest version of `pro`, run the following commands:

```
sudo apt update && sudo apt install ubuntu-advantage-tools
```

Check the status of the services

After you have *attached your subscription* and updated the `ubuntu-advantage-tools` package, you can check which services are enabled by running the following command:

```
pro status
```

This will show you which services are enabled or disabled on your machine (output truncated for brevity):

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
livepatch        yes       enabled   Canonical Livepatch service
realtime-kernel  yes       disabled  Ubuntu kernel with PREEMPT_RT patches integrated
```

Enable the service

To access the tooling, first enable the software repository as follows:

CIS

```
$ sudo pro enable cis
```

USG

```
$ sudo pro enable usg
```

You should see output like the following, indicating that the package has been installed:

CIS

```
Updating CIS Audit package lists
Updating standard Ubuntu package lists
Installing CIS Audit packages
CIS Audit enabled
Visit https://ubuntu.com/security/cis to learn how to use CIS
```

USG

```
Updating Ubuntu Security Guide package lists
Ubuntu Security Guide enabled
Visit https://ubuntu.com/security/certifications/docs/usg for the next steps
```

Once the feature is enabled you can follow the documentation for both the CIS and USG tooling, to run the provided hardening audit scripts.

Disable the service

If you wish to disable the service, you can use the following command:

CIS

```
$ sudo pro disable cis
```

USG

```
$ sudo pro disable usg
```

You can verify that the service has been correctly disabled by once again running the `pro status` command.

Note that this command will only remove the APT sources, but not uninstall any of the packages installed with the service.

To purge the service, removing all APT packages installed with it, see *how to disable and purge services*. This does not remove any of your configuration, it only removes the packages.

How to manage Expanded Security Maintenance (ESM) services

For Ubuntu LTS releases, ESM for Infrastructure (`esm-infra`) and ESM for Applications (`esm-apps`) are automatically enabled after you attach the Ubuntu Pro Client subscription to your account. However, if you chose to disable them initially, you can enable them at any time from the command line using the Ubuntu Pro Client (`pro`).

Make sure `pro` is up-to-date

All systems come with `pro` pre-installed through the `ubuntu-advantage-tools` package. To make sure that you're running the latest version of `pro`, run the following commands:

```
sudo apt update && sudo apt install ubuntu-advantage-tools
```

Check the status of the services

After you have *attached your subscription* and updated the `ubuntu-advantage-tools` package, you can check which services are enabled by running the following command:

```
pro status
```

This will show you which services are enabled or disabled on your machine (output truncated for brevity):

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
livepatch        yes       enabled   Canonical Livepatch service
realtime-kernel  yes       disabled  Ubuntu kernel with PREEMPT_RT patches integrated
```

Enable esm-apps and esm-infra

If either of the esm-apps or esm-infra services are disabled and you want to enable them, run the following command to enable ESM-Infra:

```
sudo pro enable esm-infra
```

Or the following for ESM-Apps:

```
sudo pro enable esm-apps
```

Update your packages

When you enable the ESM-Infra and/or ESM-Apps repositories, especially on Ubuntu 14.04 and 16.04, you may see a number of package updates available that were not available previously.

Even if your system indicated that it was up to date before enabling esm-infra or esm-apps, make sure to check for new package updates after you enable them:

```
sudo apt upgrade
```

If you have cron jobs set to install updates, or other unattended upgrades configured, be aware that this will likely result in a number of packages being updated with the esm-infra and esm-apps content.

Running apt upgrade will apply all available package updates, including the ones in esm-infra and esm-apps.

Disable the services

If you wish to disable the services, you can use the following command to disable ESM-Infra:

```
sudo pro disable esm-infra
```

Or the following command to disable ESM-Apps:

```
sudo pro disable esm-apps
```

Note that this command will only remove the APT sources, but not uninstall the packages installed with the services.

To purge the services, removing the APT packages installed with them, see *how to disable and purge services*.

Notes

- For more information about ESM-Apps and ESM-Infra, see our explanatory guide.

How to enable esm-infra-legacy on Trusty

The `esm-infra-legacy` service can be enabled with the Legacy Support add-on to grant an additional two years of extended security coverage. This service is only available on 14.04 LTS (Trusty), since the release has reached the end of its support period for `esm-infra`. Check out this article to learn more about the expansion of Long Term Support for Trusty and how to contact Canonical to purchase this additional support.

Make sure `ua` is up-to-date

All Trusty systems come with `ua` pre-installed through the `ubuntu-advantage-tools` package. To make sure that you're running the latest version of `ua`, run the following commands:

```
sudo apt update && sudo apt install ubuntu-advantage-tools
```

Note that on Trusty, Ubuntu Pro is referred to by its previous name: "Ubuntu Advantage" (or `ua`).

Check the status of the services

After you have attached to a Pro subscription and updated the `ubuntu-advantage-tools` package, you can check which services are enabled by running the following command:

```
sudo ua status
```

This will show you which services are enabled or disabled on your machine, (output truncated for brevity). With the addition of Legacy Support, it will now show the esm-infra-legacy service on Trusty:

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
esm-infra-legacy yes       disabled  Expanded Security Maintenance for Infrastructure on␣
↪Legacy Instances
livepatch        yes       enabled   Canonical Livepatch service
```

Enabling esm-infra-legacy

If you are entitled to the `esm-infra-legacy` service as shown above, you can enable it by running:

```
sudo ua enable esm-infra-legacy
```

What if `esm-infra-legacy` is not entitled?

If `ua status` shows that you are not entitled to the service, you will first need to buy access to the service, as mentioned at the top of this page.

Once you have purchased the Legacy Support add-on, run the following command on your machine to refresh the contract definitions:

```
sudo ua refresh
```

After refreshing the contract data, you can confirm that the service is now entitled by running:

```
sudo ua status
```

The output should now show that you are entitled to the `esm-infra-legacy` service, and you can now enable the service as outlined *in the enablement section*.

Trusty caveats

There are some known caveats for the Trusty version of *ubuntu-advantage-tools*:

Disabling `esm-infra` also disables `esm-infra-legacy`

If you disable `esm-infra`, this will (due to internal dependencies) also disable `esm-infra-legacy`. Although updates will **only** be applied via `esm-infra-legacy`, we recommend keeping both services enabled. This is not true in reverse: if you want to disable `esm-infra-legacy`, doing so will not disable `esm-infra`.

`do-release-upgrade` fails if packages are installed from `esm-infra`

If `esm-infra` is enabled **and** packages are installed from that source, the `do-release-upgrade` operation will fail since there will be an APT dependency issue when performing the operation.

You can address this issue by running `do-release-upgrade` with the following command:

```
sudo RELEASE_UPGRADER_ALLOW_THIRD_PARTY=1 do-release-upgrade
```

It is important to note that you will need to re-enable the Ubuntu Pro services again once you have upgraded to Xenial, since Trusty lacks the correct mechanisms to re-enable the Pro services automatically after a `do-release-upgrade`.

Note that this is only the case when upgrading from Trusty to Xenial. The Ubuntu Pro Client is fully supported from Xenial onward, where these issues have already been fixed.

Why 14.04 (Trusty) no longer receives new Ubuntu Pro Client features

For a further reduced risk of regressions on 14.04 (Trusty) the Pro client package is almost frozen. Hence it is not receiving regular new features like newer Ubuntu LTS releases do. Beyond version 19.7 there won't be updates except any critical CVE maintenance or features explicitly targeted for Trusty (like `esm-infra-legacy` in 2024).

Version 19.7 has full-featured support of the applicable Ubuntu Pro service offerings `esm-infra`, `esm-infra-legacy` and `livepatch`.

How to manage FIPS

Note: FIPS is supported on Ubuntu 16.04, 18.04 and 20.04 releases.

Caution: Disabling FIPS is not recommended: only enable FIPS on machines intended expressly to be used for FIPS.

To use FIPS, one can either launch existing Ubuntu premium support images which already have the FIPS kernel and security pre-enabled on first boot at AWS Ubuntu Pro FIPS images, Azure Pro FIPS images, and GCP Pro FIPS images.

Alternatively, you can enable FIPS using the Ubuntu Pro Client, which will install a FIPS-certified kernel and core security-related packages such as `openssh-server/client` and `libssl`.

To enable FIPS, run:

```
$ sudo pro enable fips
```

You should see output like the following, indicating that the FIPS packages have been installed:

```
Installing FIPS packages
FIPS enabled
A reboot is required to complete install.
```

Enabling FIPS should be performed during a system maintenance window since this operation makes changes to underlying SSL-related libraries and requires a reboot into the FIPS-certified kernel.

Caution: Once you enable FIPS, enabling some Pro services will not be possible. For a complete view of which services are incompatible with FIPS, refer to the services compatibility matrix.

How to disable FIPS

If you wish to disable FIPS, you can use the following command:

```
sudo pro disable fips
```

Note that this command will only remove the APT sources, but not uninstall the packages installed with the service. Your system will **still have the FIPS packages installed** after FIPS is disabled.

To purge the service, removing the APT packages installed with it, potentially removing also the FIPS kernel, see *how to disable and purge services*.

How to manage Landscape

You can register a machine with Landscape via the `pro enable landscape` command. You can register interactively for convenience, or non-interactively which is useful for hands-off automation.

To register a machine, you'll need (as a minimum) your Landscape Account Name and a name for the machine you are registering. If you're not using Landscape SaaS, then you'll also need the URL of your hosted Landscape server.

Enable interactively

To register your machine by interactively providing your Landscape account details at the CLI, run:

```
sudo pro enable landscape
```

This command will install `landscape-client` and start up an interactive wizard to complete the Landscape registration for the machine.

Enable non-interactively

If you know the details of your Landscape setup then you can register a machine without using the wizard. Under the hood, `pro` installs and executes `landscape-config`, so you can pass any parameters supported by `landscape-config` to `pro enable landscape` after a `--`.

You should also use the `--assume-yes` flag to automatically accept the defaults for any un-provided parameters.

The command to enable Landscape takes the following format:

```
sudo pro enable landscape \
<pro enable parameters> \
-- \
<landscape-config parameters>
```

Which, when the parameters are added, should look something like this:

```
sudo pro enable landscape \
--assume-yes \
-- \
--account-name <my-account> \
--computer-title <my-computer>
```

That command will install `landscape-client` and pass the provided parameters after `--` to the `landscape-config` tool to automatically register the machine.

What next?

After successfully running `pro enable landscape`, either interactively or non-interactively, an administrator of your Landscape account will need to go to the "Pending Computers" page in Landscape to accept the machine you just registered.

And that's it! The machine should now appear in the Landscape dashboard for management.

How to manage Livepatch

For Ubuntu LTS releases, Livepatch is automatically enabled after you attach your Ubuntu Pro subscription. However, you can choose to disable it initially via the dashboard, and then enable it at a later time from the command line using the Ubuntu Pro Client (`pro`).

Make sure `pro` is up-to-date

All systems come with `pro` pre-installed through the `ubuntu-advantage-tools` package. To make sure that you're running the latest version of `pro`, run the following commands:

```
sudo apt update && sudo apt install ubuntu-advantage-tools
```

Check the status of the services

After you have *attached your subscription* and updated the `ubuntu-advantage-tools` package, you can check which services are enabled by running the following command:

```
pro status
```

This will show you which services are enabled or disabled on your machine (output truncated for brevity):

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
livepatch        yes       enabled   Canonical Livepatch service
realtime-kernel  yes       disabled  Ubuntu kernel with PREEMPT_RT patches integrated
```

How to enable Livepatch

Important: Once you enable Livepatch, enabling some Pro services will not be possible until Livepatch is disabled again. For a complete view of which services are compatible with Livepatch, refer to the services compatibility matrix..

If Livepatch is disabled and you want to enable it, run the following command:

```
$ sudo pro enable livepatch
```

You should see output like the following, indicating that the Livepatch snap package has been installed successfully:

```
One moment, checking your subscription first
Installing snapd
Updating package lists
Installing canonical-livepatch snap
Canonical livepatch enabled.
```

Check Livepatch status after installation

If you're interested in the detailed status of the Livepatch client once it has been installed, use the following command:

```
$ sudo canonical-livepatch status
```

Unsupported kernels

Although you can enable Livepatch on an unsupported kernel, since patches are kernel-specific, you will not receive any updates from Livepatch if your kernel is not supported.

The `pro status` command will warn you in its output if Livepatch is not supported:

```
SERVICE          ENTITLED  STATUS    DESCRIPTION
esm-apps         yes       enabled   Expanded Security Maintenance for Applications
esm-infra        yes       enabled   Expanded Security Maintenance for Infrastructure
livepatch        yes       warning   Current kernel is not supported
```

(continues on next page)

(continued from previous page)

```
realtime-kernel  yes       disabled  Ubuntu kernel with PREEMPT_RT patches integrated

NOTICES
The current kernel (5.19.0-46-generic, amd64) is not supported by livepatch.
Supported kernels are listed here: https://ubuntu.com/security/livepatch/docs/kernels
Either switch to a supported kernel or `pro disable livepatch` to dismiss this warning.
```

The `canonical-livepatch status` command will also warn you if your kernel is unsupported (output truncated for brevity):

```
...
server check-in: succeeded
kernel state:  kernel not supported by Canonical
patch state: ✓ no livepatches needed for this kernel yet
...
```

You can also check the kernel support matrix to see if your kernel is supported by Livepatch. To find out more, refer to this explanation of how Livepatch works.

How to disable Livepatch

Enabling Livepatch installs the Livepatch client as a snap package, and there are a few possible ways to disable it. The simplest is to use the Pro Client:

```
sudo pro disable livepatch
```

If you also want to remove the Livepatch client from your machine, you can then use the following command:

```
snap remove canonical-livepatch
```

For other options, you can also refer to the Livepatch documentation.

Notes

- For more information about the Livepatch client and how to use it, refer to the official Livepatch client documentation.
- Livepatch is not compatible with FIPS-certified kernels or with the real-time kernel, and should not be enabled if you wish to use those services. If Livepatch is enabled and you try to enable an incompatible service, `pro` will notify you and offer to disable Livepatch first.

How to manage real-time kernel

Pre-requisites

The real-time kernel is currently only supported on Ubuntu 22.04 LTS (Jammy). For more information, feel free to contact our real-time team.

Enable and auto-install

Important: Once you enable real-time kernel, enabling some Pro services will not be possible. For a complete view of which services are compatible with real-time kernel, refer to the services compatibility matrix..

To `enable` the real-time kernel through the Ubuntu Pro Client, please run:

```
$ sudo pro enable realtime-kernel
```

You'll need to acknowledge a warning, and then you should see output like the following, indicating that the real-time kernel package has been installed.

```
One moment, checking your subscription first
The Real-time kernel is a beta version of the 22.04 Ubuntu kernel with the
PREEMPT_RT patchset integrated for x86_64 and ARM64.

This will change your kernel. You will need to manually configure grub to
revert back to your original kernel after enabling real-time.

Do you want to continue? [ default = Yes ]: (Y/n) yes
Updating package lists
Installing Real-time kernel packages
Real-time kernel enabled
A reboot is required to complete install.
```

After rebooting you'll be running the real-time kernel!

Enable and manually install

Important: The `--access-only` flag was introduced in Pro Client version 27.11

If you would like to enable access to the real-time kernel APT repository but not install the kernel right away, use the `--access-only` flag when you enable it, as follows:

```
$ sudo pro enable realtime-kernel --access-only
```

With this extra flag you'll see output like this:

```
One moment, checking your subscription first
Updating package lists
Skipping installing packages: ubuntu-realtime
Real-time kernel access enabled
```

To install the kernel you can then run:

```
$ sudo apt install ubuntu-realtime
```

You'll need to reboot after installing to boot into the real-time kernel.

Notes

- Real-time kernel is not compatible with Livepatch. If you wish to use the real-time kernel but Livepatch is enabled, `pro` will warn you and offer to disable Livepatch first.

If you disable a service and also want to remove all the associated files, refer to our *disable and purge* guide.

Disabling and purging services

All services enabled using the Pro Client can be disabled using the command line with a command that follows this structure:

```
$ sudo pro disable <service-name>
```

When you disable a service, the Pro Client will remove all access to that specific service's packages and sources in your system. However, only the access is removed – the packages (debs, snaps) installed when the service was enabled will remain installed on your system.

For example, the command:

```
$ sudo pro disable esm-apps
```

will remove the `sources.list` entry for `esm-apps`, and also the authentication information that granted access to the packages. It will **not** remove the debs installed from the `esm-apps` repository.

In the same way, the command:

```
$ sudo pro disable livepatch
```

disables the Livepatch service, but the `canonical-livepatch` snap will remain installed on the system (although inactive).

If there are other services which depend on the service being disabled, those need to be disabled too. A prompt in the CLI will list those services and ask to disable them. The `--assume-yes` flag can be used to automatically accept this prompt.

What does `purge` mean in this context?

Disabling and **purging** a service has a similar effect to what is done by ppa-purge: it removes access to the sources (from where the service packages are obtained), and then makes a best-effort attempt to downgrade those packages back to their Ubuntu versions (the ones published in the Ubuntu Archive).

If a package is specific to the given service (`ubuntu-fips` for the FIPS-related services, for example) then that package will be removed during the purge process, when possible.

> **Warning:** The operation of reverting or uninstalling packages may leave the system in an undesired state, due to packages not meeting dependencies (partial or broken system caches) or due to the removal of kernels when alternative kernels are not working properly. Therefore, the `purge` feature is aimed at users/administrators who understand the impacts.

Using the CLI to disable and purge a service

First of all, it is important to note that this is an **experimental feature**, so although it is available it should be used with caution.

To purge a service, use the CLI command:

```
$ sudo pro disable <service-name> --purge
```

We recommend only using purge when you are able to monitor the screen. Since the purge feature has the potential to do serious accidental damage to a system if used unattended (for example, in a script), the `--assume-yes` flag was made incompatible with the `--purge` flag.

Since packages are being uninstalled/reinstalled, the execution of the `disable` command with `--purge` may take a while to complete.

What happens when I purge...

livepatch, realtime-kernel, landscape

These services do not currently support the `--purge` operation.

anbox, cc-eal, cis/usg, esm-apps, esm-infra*, ros (and ros-updates)

When these services are disabled with `--purge`, the sources and authentication will be removed first. Then, packages that are only available in the service-specific APT repository will be removed from the system.

The origin is detected based on the `origin` metadata defined in `apt` for all packages in this repository.

Then, for the packages that are also present in the Ubuntu archives, there will be a downgrade to the highest possible version in the archive. Downgrade operations are the most common because the packages for specific services usually have higher version strings than their counterparts in the archive.

Note that purging a service often results in the installation of newer versions of packages than were originally present in the system (i.e., before the given service was enabled). It is important to use the latest versions available in the archive to guarantee that dependency chains are resolved – in other words, that there are no broken dependencies between packages.

Note: * Disabling `esm-infra` with `--purge` *may* involve removing a kernel, see below for more information.

FIPS (and fips-updates/fips-preview)

In the case of FIPS-related services (and in some cases, `esm-infra`), there is an extra consideration when purging the packages: there may be Linux kernel packages among the ones to be removed or downgraded.

In this case, the Pro Client will look for at least one more kernel installed in the system. This check is performed while examining the installed `apt` packages, and matching the version strings to `vmlinu[z|x]` files in `/boot`.

If no other kernel is found in the system, then the current kernel cannot be removed. The Client will warn the user and abort the operation.

Kernels which are manually compiled and installed, or that are not shipped in Ubuntu as APT packages will *not* be considered and validated.

If another Ubuntu kernel is found in the system, `--purge` will proceed to remove and downgrade packages normally. In the process, the user will be warned that a kernel is being removed, and that it is their responsibility to make sure the alternative kernels can be booted and are working.

A reboot is always needed when kernel packages are changed when purging a service.

2.3 Understanding Ubuntu Pro

2.3.1 Ubuntu Pro services

For all Ubuntu Pro customers and users, here you'll find details about the tools included in your Pro subscription and more information about topics such as how active machines are calculated.

What is included in Ubuntu Pro?

Overview

Service	Ubuntu Pro (infra-only)	Ubuntu Pro
Security patching for Ubuntu Main repository for 10 years (ESM-infra)	Yes	Yes
Security patching for Ubuntu Universe repository for 10 years (ESM-apps) (Ubuntu 16.04 LTS onwards)	No	Yes
Kernel Livepatch to avoid unscheduled reboots	Yes	Yes
Real-time kernel (Ubuntu 22.04 LTS onwards)	Yes	Yes
NIST-certified FIPS crypto-modules (pending for Ubuntu 22.04 LTS)	Yes	Yes
USG hardening with CIS and DISA-STIG profiles (DISA-STIG tooling & automation for Ubuntu 20.04 LTS and 22.04 LTS)	Yes	Yes
Systems Management with Landscape (SaaS or self-hosted)	Yes	Yes

Security feature focus

Expanded Security Maintenance Infra + Apps

There are two Expanded Security Maintenance streams offered by Canonical:

ESM infra: this stream expands the scope of security maintenance for Ubuntu LTS releases for packages in the Ubuntu Main repository from 5 years to 10 years;

ESM apps: this stream expands the scope of security maintenance to include packages in the Ubuntu Universe repository for the full 10 years of an Ubuntu LTS release's lifecycle. That's around 25,000 additional packages per Ubuntu LTS release.

These commands show the source of packages on your Ubuntu system, how many packages are from the Ubuntu Universe or Ubuntu Main repositories, as well as how many security patches are already available for those packages under the ESM services.

```
$ pro security-status

$ pro security-status --esm-apps
```

(continues on next page)

(continued from previous page)

```
$ pro security-status --esm-infra
```

For further information on accessing ESM, refer to *how to enable ESM infra and apps using the Ubuntu Pro client*

The expected security maintenance dates for Ubuntu LTS releases since 14.04 LTS, including ESM periods:

Release	Patched Until	Repositories
14.04 LTS	April 2024	Main
16.04 LTS	April 2026	Main & Universe
18.04 LTS	May 2028	Main & Universe
20.04 LTS	April 2030	Main & Universe
22.04 LTS	April 2032	Main & Universe

Livepatch

The Ubuntu Livepatch service is designed to help you remain secure while avoiding unscheduled reboots. It does this by providing patches for High and Critical CVEs in the Ubuntu Kernel, which are applied while the system is running.

Ubuntu Livepatch addresses vulnerabilities in the running Linux kernel, in memory. When using Livepatch, you should also use the normal update tools to install all available standard updates to the Linux kernel, including lower severity vulnerabilities or vulnerabilities that cannot be live patched. This means that when you do eventually reboot into a newer kernel, there are no vulnerabilities.

To check whether a Livepatch has been applied to a specific CVE, run:

```
$ canonical-livepatch status --verbose
```

- Livepatch documentation
- *How to enable Livepatch using the Ubuntu Pro client*

Compliance features

Your Ubuntu Pro subscription includes several services and tools that address compliance and regulatory requirements: FIPS, the Ubuntu Security Guide, and the CIS hardening tool.

FIPS

Canonical has FIPS 140-2 modules for Ubuntu 16.04 LTS, 18.04 LTS and 20.04 LTS. We are currently in the process of obtaining FIPS 140-3 modules for 22.04 LTS. We will announce on our blog and in the Ubuntu Pro newsletter when the validation process for 22.04 LTS is complete - make sure to subscribe if you want to be kept updated.

Security patching with FIPS

Each FIPS 140 certificate for a package can take several months to complete and is valid for 5 years. However, as vulnerabilities happen security-critical fixes may need to be included faster than a certification cycle. For that, we provide two ways to consume validated packages: a stream called fips, where the exact packages validated by NIST are present; and another stream called fips-updates where the validated packages are present, but are updated with security fixes. The fips-updates stream also allows access to the packages during the validation phase, enabling early application development and testing. Both streams are re-validated periodically during Ubuntu standard support phase.

- FIPS documentation
- *How to enable FIPS using the Ubuntu Pro client*

USG for hardening Ubuntu 20.04 LTS and 22.04 LTS

The Ubuntu Security Guide (USG) provides tooling for the auditing and hardening of Ubuntu systems to meet **CIS** (for Ubuntu 20.04 LTS and 22.04 LTS) and **DISA STIG benchmarks** (for Ubuntu 20.04 LTS). The USG also allows for environment-specific customisation.

This tooling is designed to help you to harden Ubuntu systems quickly and correctly. We recommend using the tool to create a hardened golden image, which you can then disseminate across your organisation. The tool can also audit your compliance after hardening.

How to enable the USG using the Ubuntu Pro client

CIS hardening tool for Ubuntu 16.04 LTS and 18.04 LTS

If you need to harden Ubuntu systems running either 16.04 LTS or 18.04 LTS, you will need to use an older version of our tooling, the CIS hardening tool. The tool also has an audit function, enabling you to monitor the ongoing compliance of Ubuntu instances after hardening is complete.

How to enable the CIS hardening tool using the Ubuntu Pro client

Landscape

Landscape is Canonical's system management tool for Ubuntu machines and is included in every tier of Ubuntu Pro.

There are 3 versions of Landscape:

Feature comparison	Landscape SaaS	Managed Landscape	Self-hosted Landscape
Managed by Canonical	Yes	Yes	No
Canonical SLA	No	Yes	No
Works without internet	No	No	Yes
Repository management	No	Yes	Yes
Bring your own SSO and IAM	No	Yes	Yes
Multi-tenant	Yes	No	No
Software and hardware inventory	Yes	Yes	Yes
Security, compliance, hardening, reports	Yes	Yes	Yes

Getting started with Landscape

Landscape SaaS

Before you can access your Landscape SaaS account for the first time, you need to follow the steps under *Account set-up*.

Self-hosted Landscape

After setting up your self-hosted Landscape server, you need to choose a licensing mechanism. There are two options for self-hosted Landscape: the new, Pro client method and the old, licence.txt file method.

Pro client method

For customers running Landscape version 23.03 or newer and landscape-client version 23.02 or newer, please use the Pro client method to license your Landscape server.

1. Ensure the Pro client is *installed and attached to your Pro token* on the system you wish to register to Landscape.
2. Then *enable Landscape* to initiate the registration process.
3. Landscape will detect your Pro entitlement via the Pro token and create a licence for your machine.

Licence.txt file method

For customers on an older version of Landscape or landscape-client than those specified above, please download your `licence.txt` file from your Landscape SaaS account. You will need to re-download and apply new `licence.txt` files every time you purchase new Ubuntu Pro licences and after every renewal.

Tip: New `licence.txt` files become available on their start date. For renewal customers, this is the day after your old licences expire.

- Landscape documentation: our main set of documentation on Landscape SaaS and self-hosted Landscape
- Knowledge Base - Landscape section: content published by Canonical Support, typically addressing FAQs and providing workarounds for bugs
- GitHub - script repository for Landscape: a collection of scripts to make Landscape more powerful

Active machine count

The Ubuntu Pro dashboard displays an "active machine" count for each subscription to Ubuntu Pro. This is the number of online machines attached to your Pro token that have pinged Canonical servers within the last 24 hours.

Consumption of the following services is registered under active machines:

- ESM-Infra and ESM-Apps
- Livepatch
- USG
- CIS
- FIPS

Machines registered to Landscape are not included.

Tip: If you detach a machine from your Ubuntu Pro token, the reduction in active machine count will take place 24 hours later.

Customers with unlimited guest support

If you have licensed an entire virtual cluster to Ubuntu Pro at the physical host level, you are eligible for unlimited guest support. The Ubuntu Pro dashboard will display your license type as physical, however you should use the Pro token associated with that subscription on your virtual machines.

As you attach machines, you will see your active machine count go above your license count. This is expected behaviour and will not impact your access to the Pro services.

2.3.2 Canonical support

For paying customers with Ubuntu Pro, you'll find information here about what is included in your support contract.

Canonical Support: overview and process

Ubuntu Pro includes self-service support, that can be upgraded to comprehensive support contract.

Support contract options

Your account will include different levels of support according to the options in your organisation's contract:

Response options

- *24/5*: Monday to Friday (in your timezone)
- *24/7*: any time of day, every day

Coverage options

- *Infra-only*: Ubuntu main repository (~2,300 packages)
- *Full Pro*: Ubuntu main and universe repositories (~25,000 packages)

Storage: up to 192TB of Ceph or Swift raw storage per covered machine

Products covered: Kubernetes, OpenStack, Ceph, MAAS, LXD

Severity levels and response times

For support contracts only; self-service support does not qualify.

Severity Level	Weekday	24.7
1 - Core functionality critical impact / service down	4 hours excl. weekends and holidays	1 hour
2 - Core functionality severely degraded	8 business hours	2 hours
3 - Standard support request	12 business hours	6 hours
4 - Non-urgent request	24 business hours	12 hours

Business hours are defined as 08:00 to 18:00 Monday to Friday, local to the customer HQ, unless another location has been agreed.

For further information about what is covered under your support contract, refer to the Ubuntu Pro Service Description.

Support case lifecycle

Ubuntu Pro for airgapped environments

Customers with a paid subscription to Ubuntu Pro can set up the included services in environments with limited or no network connectivity.

Paying customers with Support Portal access should refer to the following articles from our Knowledge Base for instructions on how to set up Ubuntu Pro in offline environments:

- Ubuntu Pro client external access requirements: this article outlines the specific ports and URLs needed for each Ubuntu Pro bitstream service.
- Get started with Ubuntu Pro in an airgapped environment.
- For instructions on how to create local mirrors to make the Pro services available to offline systems, search in the Knowledge Base for "SERVICE_NAME offline".

If you need to use the Pro services in an offline environment but do not have a paid subscription, you can purchase one in our online shop.