TheOpenRoad Cloud

TheOpenRoad Cloud is a suite of website management products and cloud computing services from TheOpenRoad which include **TheOpenRoad Cloud™ Registrar**, *a domain registration service and web hosting management solution.* It is the best-selling flagship product from TheOpenRoad, and was first released to the public in 2024.

Auto-generated by TheOpenRoad Support.

- Potentially unwanted program (PUP)
- Direct Server Operations (DSO) Team
- DNS Propagation
- About UCEPROTECT and their "Level-3" IP Blacklist
- Issuing SSL Certificates via Certbot
- Basic HTML Layouts

Potentially unwanted program (PUP)

What are Potentially unwanted Programs (PUP)?

A **Potentially Unwanted Program (PUP)** or **Potentially Unwanted Application (PUA)** is software that a user may consider unnecessary, undesirable, or potentially harmful. The terms are commonly used by antivirus, endpoint security, and parental-control products as subjective classification criteria.

PUP's and PUA's are not necessarily classified as traditional malware. However, they may exhibit behaviors that compromise user privacy, reduce system security, degrade performance, or interfere with the normal operation of a computer.

Examples of potentially unwanted behavior

- Displaying intrusive or excessive advertisements (adware).
- Tracking a user's Internet activity or browsing habits and potentially sharing the collected information with advertisers (spyware).
- Injecting advertisements or other content into websites viewed by the user.
- Changing browser settings, search providers, or the default home page without clear consent.
- Installing additional software that the user did not explicitly request.
- Using premium SMS or other paid services that can result in unexpected charges.
- Installing components that weaken the security of the operating system or browser.

Software bundling

One common method of distributing PUP's and PUA's is known as **software bundling**. In this model, a user downloads a legitimate or desired application, but the installer also offers or installs additional software.

For example, a software developer may distribute an application through a third-party download site. That site may use a custom installer or wrapper that presents additional applications during installation. These applications may be unrelated to the software the user originally intended to install.

In some cases, the installer may provide a clear option to decline the additional software. In other cases, the opt-out mechanism may be difficult to find, misleading, preselected, or otherwise designed to encourage the user to accept the installation. Such practices are commonly associated

with *dark patterns* because they can undermine informed user choice.

Risks towards infrastructure security

Certain unwanted applications can modify system or browser settings, weaken security controls, or install components that make the system more vulnerable to attack.

A particularly serious example is the installation of an untrusted root certificate. Root certificates are part of the trust infrastructure used to establish secure HTTPS connections. If an unauthorized certificate is installed and trusted by the operating system or browser, it may potentially allow an attacker or malicious component to intercept encrypted communications without generating the security warnings that users would normally expect.

For this reason, security experts and government agencies have advised users to remove insecure or unauthorized root certificates when they are identified.

About third-party software download websites

Third-party software-download websites can be a significant source of bundled PUP's and PUA's. A download page may advertise legitimate software while providing an installer that has been modified to include additional applications.

Open-source software projects have frequently expressed concern about this practice because third-party distributors may modify or repackage their software without the project's knowledge or authorization.

The safest approach is generally to obtain software directly from the **official project website**, a reputable package manager, or an established application store whenever possible.

In focus

Users can reduce their exposure to potentially unwanted software by following measurable security practices:

- **Download software from official sources.** Prefer the application's official website, a trusted package manager, or a reputable app store.
- **Avoid unfamiliar download portals.** Third-party download sites may repackage legitimate applications with additional software.
- **Use custom or advanced installation options.** These options often reveal additional applications or configuration changes that may otherwise be hidden.
- **Read installation screens carefully.** Do not automatically click *Next*, *Accept*, or *Install* without reviewing what is being offered.
- **Decline unnecessary additional software.** Pay particular attention to preselected checkboxes and offers for browser extensions, system utilities, or security products.
- **Keep antivirus and endpoint protection enabled and up to date.** Security products can detect and block many known PUPs and PUAs.

- **Keep the operating system and applications updated.** Security updates help address vulnerabilities that unwanted software could otherwise exploit.
- **Review installed applications regularly.** Remove software that you do not recognize or no longer need.
- **Check browser extensions.** Remove extensions that were installed without your knowledge or that have unnecessary permissions.
- **Be cautious about security warnings.** Unexpected certificate warnings, browser changes, or requests to install certificates should be investigated rather than automatically accepted.
- **Review trusted root certificates when necessary.** If an unfamiliar certificate has been installed by unwanted software, consult the operating system or browser vendor's security guidance before removing it.
- **Use reputable package managers where available.** Package managers can provide a more controlled and verifiable method of installing software.
- **Do not rely solely on antivirus detection.** Some PUPs may not be malicious enough to trigger traditional malware classifications, so safe download and installation practices remain important.
- **Back up important data.** Maintaining reliable backups can help reduce the impact of unwanted or malicious software installations.

Training summary

PUP's and PUA's occupy a category between legitimate software and clearly malicious malware. While some may provide a legitimate function, their installation methods or behavior can create privacy, security, performance, or usability concerns.

Software bundling and deceptive installation practices are common ways for unwanted applications to reach users. Obtaining software from trusted sources, carefully reviewing installation options, maintaining updated security software, and regularly reviewing installed applications can significantly reduce the risk of unwanted software being installed.

About this article

- Written by Gary Phatt, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9

Direct Server Operations (DSO) Team

What is a DSO (Direct Server Operations) team?

The **Direct Server Operations (DSO) Team** is the team responsible for performing hands-on, physical maintenance and operational work on servers and infrastructure within TheOpenRoad Cloud's physical server locations.

Unlike teams that primarily manage infrastructure through remote software tools, the DSO Team operates directly on the physical equipment. This includes servers, networking equipment, storage systems, racks, cabling, power infrastructure, and other hardware deployed within TheOpenRoad Cloud facilities. DSO personnel are distributed across TheOpenRoad Cloud's server locations worldwide, providing *continuous 24/7 operational coverage*.

Primary responsibilities

The primary responsibility of the DSO Team is to perform tasks that require physical access to infrastructure.

- Installing, replacing, or removing server hardware
- Replacing failed components such as drives, memory, power supplies, fans, or other field-replaceable units
- Physically inspecting servers and infrastructure
- Connecting, disconnecting, or replacing network and power cabling
- Racking and unracking equipment
- Performing hardware upgrades and maintenance
- Investigating hardware-related faults
- Assisting with physical infrastructure deployments
- Performing other maintenance procedures that require on-site access

The exact work performed by a DSO Team member depends on the equipment, facility, maintenance procedures, and operational requirements involved.

Distinguishing the difference between physical & remote operations

The DSO Team is primarily concerned with the *physical layer* of TheOpenRoad Cloud's infrastructure.

Not every infrastructure incident requires DSO involvement. Software failures, configuration problems, network-routing issues, application failures, and other incidents that can be resolved remotely are generally handled by the appropriate operational or engineering teams.

For example, if a server is experiencing a software configuration problem but all physical hardware is functioning normally, the incident would typically not require DSO intervention.

Conversely, if a server has experienced a failed power supply, damaged cabling, failed storage device, or another physical fault, DSO personnel may be required to physically access the equipment and perform the necessary maintenance.

An incident may initially appear to be software- or network-related but ultimately require physical intervention. In these situations, the responsible operations or engineering team can coordinate with DSO personnel to perform actions that cannot be completed remotely.

DSO Team objective examples

In these cases, the DSO Team acts as the *physical operations interface* between remote teams and the infrastructure deployed at a server location.

- Physically power-cycling equipment
- Checking physical connections
- Inspecting hardware status indicators
- Reseating or replacing hardware
- Connecting diagnostic equipment
- Verifying the physical state of a server or network device
- Performing other on-site actions requested by the incident-response team

Global operations mission statement

The DSO Team operates across TheOpenRoad Cloud's geographically distributed server locations.

Because infrastructure incidents and maintenance requirements can occur at any time, DSO personnel provide *24/7 coverage*. This allows physical infrastructure work to be performed regardless of the time of day or the geographic location of the affected equipment.

The global distribution of DSO personnel also reduces the dependency on a single physical location and enables on-site assistance at facilities in different regions.

DSO operates alongside, rather than in place of, other infrastructure and engineering teams.

DSO Team responsibilities

A simplified division of responsibilities is:

Scope of task	Typical responsibility

Physical hardware management	DSO Team
Hardware replacement	DSO Team
Physical cabling	DSO Team
On-site inspection and compliance	DSO Team
Software configuration, administration, and maintenance	Appropriate engineering/operations servicing team, or SMU
Application-level issues, debugging, incident outage recovery	Appropriate engineering/operations servicing team, or SMU
Remote infrastructure operations	Appropriate engineering/operations servicing team, or SMU
Physical assistance during remote incidents	DSO Team, *when required*

This separation allows teams to focus on their respective areas of expertise while providing a mechanism for coordinated response when an issue crosses the physical and logical boundaries of the infrastructure.

Operational model

A typical DSO request can be summarized as follows:

1. An issue or maintenance requirement is identified.
2. The responsible team determines whether physical intervention is required.
3. A request is provided to the DSO Team with the required equipment, location, and action details.
4. A DSO Team member accesses the affected infrastructure on-site.
5. The requested physical operation is performed.
6. The result is reported back to the requesting team.
7. Further remote or engineering work is performed if necessary.

This model allows remote teams to continue handling logical and software-level operations while DSO personnel handle actions that require a physical presence.

Training summary

The **Direct Server Operations (DSO) Team** is TheOpenRoad Cloud's dedicated physical infrastructure operations function. DSO personnel work directly with the hardware and physical infrastructure supporting cloud services, performing maintenance, replacements, inspections, installations, and other tasks that require on-site access.

DSO is not generally responsible for resolving non-physical infrastructure incidents. Instead, the team provides specialized physical capabilities and can assist other operational teams whenever an incident or maintenance procedure requires someone to interact directly with equipment.

With personnel distributed across TheOpenRoad Cloud's server locations and operating *24 hours a day, 7 days a week*, the DSO Team provides continuous physical support for the infrastructure on which TheOpenRoad Cloud services operate.

About this article

- Written by Gary Phatt, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9

DNS Propagation

What is DNS Propagation?

DNS Propagation is the term used to describe the effect of DNS changes across DNS servers and resolvers on the internet.

When DNS records are updated, such as an A, CNAME, MX, or TXT record, the change may not be immediately visible to every user. DNS resolvers temporarily store DNS records in their cache based on the record's *Time to Live (TTL)* value. As cached records expire, resolvers query the authoritative DNS server again and retrieve the updated information.

As a result, DNS changes may take some time to become visible globally. The propagation time depends primarily on the record's TTL, DNS caching behavior, and the resolver being used.

Understanding the DNS propagation process

- A DNS record is updated on the authoritative DNS server.
- DNS resolvers continue serving the previously cached record until its TTL expires.
- Once the cached record expires, the resolver requests the updated record.
- The resolver caches the new record according to its TTL.
- Users querying through that resolver begin receiving the updated DNS information.

Because different DNS resolvers may have cached the previous record at different times, a DNS change can appear to propagate gradually rather than becoming effective everywhere simultaneously.

> DNS propagation is not a single process that occurs across the entire internet. It is primarily the result of DNS caching and the expiration of cached records at individual resolvers.

DNS propagation timeframe

The average timeframe for DNS propagation to resolve globally is between 24-48 hours. If DNS changes are taking longer than expected to take effect, verify that the updated records are correctly configured on the authoritative DNS server. You can also check the record from multiple DNS resolvers to determine whether the old value is still being cached. *Several TheOpenRoad technicians and server engineers have reported that the DNS resolver from Cloudflare usually updates the quickest.*

If the previous record has not expired, you also may need to wait for its TTL to elapse. If the issue persists beyond the expected propagation period, review your DNS configuration for conflicting or incorrect records and contact your DNS provider or hosting provider for further assistance. *If you*

are a TheOpenRoad Cloud customer, you may contact our Live Chat Support.

Helpful resources

- DNSchecker.org - DNS Propagation Check Tool

About this article

- Written by Gary Phatt, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9

About UCEPROTECT and their "Level-3" IP Blacklist

This announcement, published on TheOpenRoad Foundry by TheOpenRoad Customer support; is information regarding **UCEPROTECT** and their "*Level-3*" IP blacklisting service, primarily aimed towards email blocking.

TheOpenRoad Customer Support receives a daily average of ~36 customer support tickets per hour on business days, and ~19 per hour on weekends/public holidays. We're publishing this announcement because this has become a frequently asked question (FAQ) recently, primarily from TheOpenRoad customers involved with web hosting, and corporate domain management solutions.

Understanding UCEPROTECT

In reference to UCEPROTECT's official website, this specific blacklist (Level-3) should not be used lightly to block incoming traffic; as this RBL can, and does blacklist entire ASN's, or even entire hosting providers/ISP's. The general consensus about this RBL blacklist is that: when you use this blacklist, you will absolutely be blocking legitimate traffic as well.

According to UCEPROTECT, which also proclaims themselves as "*UCEPROTECT-Orga*":

> “ This blacklist has been created for HARDLINERS. It can, and probably will cause collateral damage to innocent users when used to block email.

> “ The recommended use of Level 3 is incorporating it into a scoring system, to give e.g. 2 points on a ‘match’ where 5 or more points trigger a spam tag.

TheOpenRoad Customer Support does not encourage our customers to utilize this RBL blacklist in order to block traffic, if we were to say this to you bluntly: "*It's overkill!*"

We monitor this RBL system, like all other providers for purely informational purposes because our core principle is that the end user of our products and solutions should be able to quickly know weather you are blocked from this blacklist system or not.

Delisting from UCEPROTECT

We know that many of you reading this might also be intensely interested in being delisted from this RBL blacklisting service, and as your hosting provider; we feel obligated to tell you the facts and truth to the best of our knowledge. We know how these blacklisting services operate, how they operate, and we know they can be difficult to work with; we have and still continue to negotiate with these organizations running IP blacklists.

UCEPROTECT offers a de-listing service in the form of a paid service charge, TheOpenRoad Customer Support does not support nor advise someone to pay money in order to de-list an IP address, especially in the common event where you have done nothing wrong, and your have had your innocent IP blacklisted automatically for no reason.

We ask that if possible, you ignore UCEPROTECT as a priority and disregard it as a major factor in deciding your reputation. Several TheOpenRoad customers have reported to us that on occasion, you may be delisted automatically at a completely random point in time; and then be relisted again shortly after for no apparent reason at all.

If you use a 3rd party IP monitoring service (we recommend HetrixTools), you have the option to opt-out of this RBL and ignore it completely from your account by following this external guide published.

Helpful resources

- HetrixTools Documentation - Ignore A Blacklist

About this article

- Written by Marv Eaton, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

Issuing SSL Certificates via Certbot

You can issue a free SSL Certificate signed by Let's Encrypt; a non profit organization, using **Certbot**. It's a free, open-source software tool that helps website administrators obtain and install SSL/TLS certificates.

Its primary purpose is to enable HTTPS on websites by automating certificate issuance, installation, and renewal.

Install Certbot from the command terminal

> The commands provided are compatible with Ubuntu 22.04, CentOS uses `yum`, and AlmaLinux uses `dnf`.

1. Update system packages

```
sudo apt update
```

2. Install Certbot and its related plugin

```
sudo apt install -y certbot python3-certbot-nginx
```

3. If above command succeed without error, check version

```
certbot --version
```

If you see an up-to-date version (e.g. `certbot 1.32.0`), you may proceed.

Issuing SSL certificates using Certbot

1. Make sure your site is accessible over HTTP. Open your domain (e.g. `example.com`) in a browser. Certbot verifies domain ownership via **port 80**.

2. Run Certbot

```
sudo certbot --nginx
```

During the setup process, Certbot will do the following:

- Detect virtual hosts present
- Prompt you to choose the domain of your choice
- Automatically configure HTTPS

> Certbot will also modify your Nginx/Apache config to add an HTTPS redirect.

Test your setup. Open your website in a browser! if everything works, you'll see a padlock icon and the `https://` prefix.

If you'd like, you can also test via the command line:

```
curl -I https://example.com
```

Automatic renewal information

By default, Certbot installs a cron job or `systemd-timer` for automatic certificate renewal. You can test the renewal manually by running the command in the terminal below.

```
sudo certbot renew --dry-run
```

If you see a return of `Congratulations, all renewals succeeded`, everything is OK and working as intended.

Your site is now protected with a free SSL certificate from Let's Encrypt, and Certbot will automatically manage renewals when needed.

About this article

- Written by Gary Phatt, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9

Basic HTML Layouts

Introduction

HTML Documents should start with a document type declaration:

```
<!DOCTYPE html>
```

Apart from the document type declaration, the document itself begins with `<html>` and ends with `</html>`.

In application

Here is the above specified in a full HTML document which works even when you replicate the document in your text editor of choice, export it as a HTML document, and navigate to it using your web browser of choice.

```
<!DOCTYPE html>
<html>
<body>

<h1>This is a heading.</h1>
<p>And, this is a paragraph.</p>

</body>
</html>
```

Understanding <!DOCTYPE> and the reason for declaration

The `<!DOCTYPE>` declaration not only represent the document type to the web browser/client, it also helps display web pages correctly. It needs to appear a maximum of one time per document, at the very top of the page before any succeeding HTML tags.

The `<!DOCTYPE>` declaration is also not case-sensitive, the `<!DOCTYPE>` declaration for HTML5 is presented below.

```
<!DOCTYPE html>
```

About this article

- Written by Marv Eaton, a TheOpenRoad Support employee.
- Still need help? Please write to us in the comment section below or contact TheOpenRoad support.

TheOpenRoad™

Please rate your experience with this article today:

When you select a number, *1 being the lowest and 9 being the highest*; the page will refresh and your feedback will be submitted to TheOpenRoad.

1 2 3 4 5 6 7 8 9