



[Home](#) » [KB](#) » [Networking](#) » How to Configure Postfix to Use External SMTP

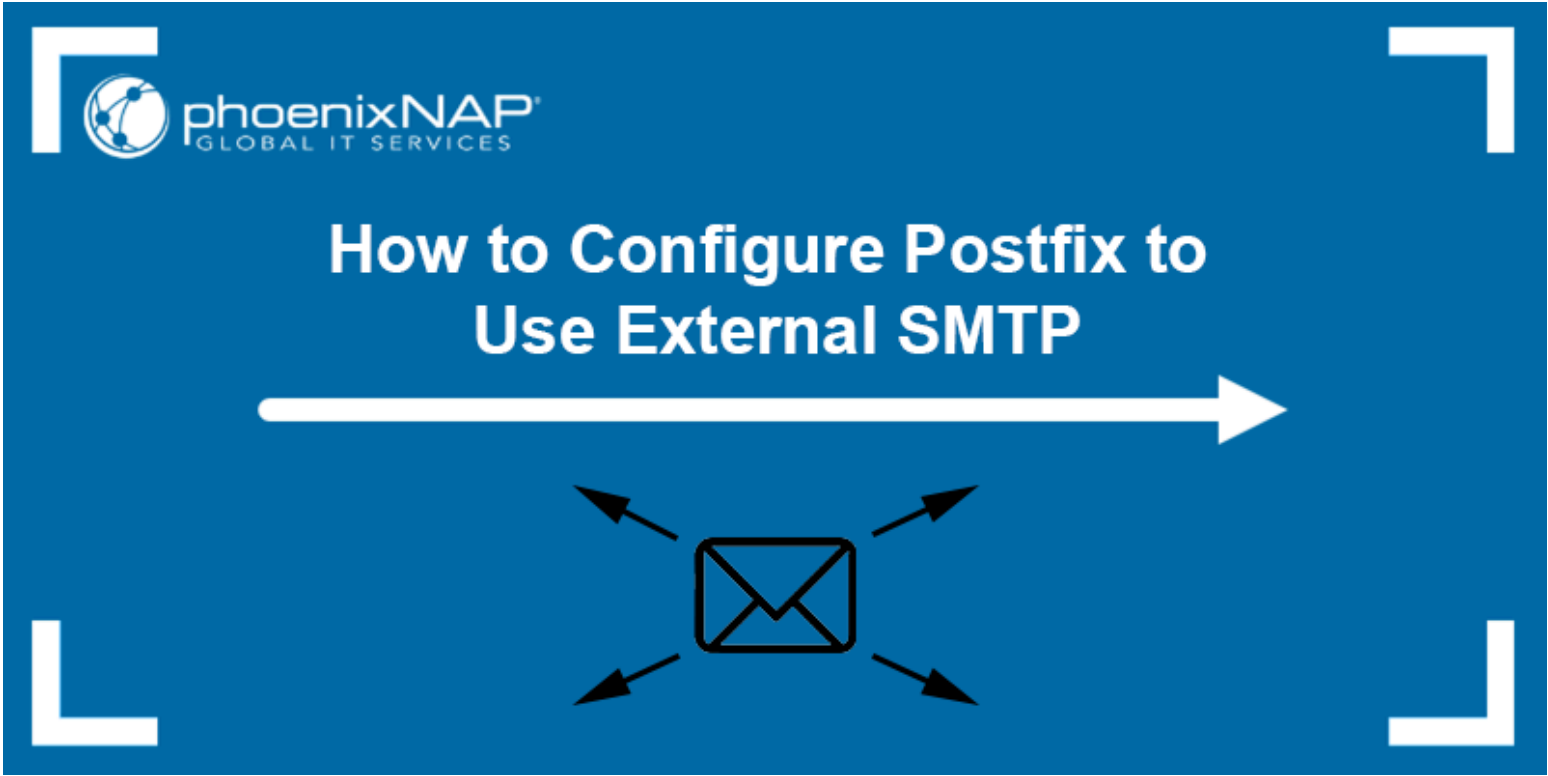
How to Configure Postfix to Use External SMTP

By [Bosko Marijan](#) Published: February 9, 2023

Topics: [Linux](#)

Postfix is a free, open-source **mail transfer agent (MTA)** used for routing and delivering emails. The utility uses the Simple Mail Transfer Protocol (**SMTP**) to transfer emails between servers. The tool is a fast, secure, and light email service solution for Linux servers.

In this tutorial, you will learn how to configure Postfix to use an external SMTP provider.



Prerequisites

- A system running Linux.
- An account with **root** privileges.
- Access to the terminal (**Ctrl+Alt+T**).

NEED CONNECTIVITY?
Tap into the Network Hub of Arizona!

- Full-service data center
- 40+ carriers
- Direct links to major public cloud providers
- 9 Tbps Global network backbone

[Learn More](#)

Contents

1. Step 1: Install Postfix
2. Step 2: Configure Postfix
 - 2.1. Enable Authentication
 - 2.2. Edit the Configuration Files
 - 2.3. Secure the Credentials
 - 2.4. Restart Postfix
3. Step 3: Test SMTP Server
4. Step 4: Set up Email Forwarding
5. Step 5: Enable SMTP Encryption

Subscribe to our newsletter

SUBSCRIBE





Step 1: Install Postfix

Depending on which system you are using, run one of the following commands to install Postfix:

- **For Debian-based distributions:**

Update the system package repository:

```
sudo apt update
```

[Copy](#)

Install Postfix on Ubuntu/Debian/LinuxMint by running:

```
sudo apt install postfix -y
```

[Copy](#)

The command installs Postfix, and the `-y` flag answers **Yes** to any prompts during the installation.

The configuration wizard appears after installation. Move on to step two to configure Postfix.

- **For RHEL-based distributions:**

Update the system package repository:

```
sudo yum update
```

[Copy](#)

Install Postfix on CentOS/RHEL/Rocky Linux by running:

```
sudo yum install postfix -y
```

[Copy](#)

After installation, check the Postfix service status by running:

```
sudo service postfix status
```

[Copy](#)

```
bosko@pnap:~$ sudo service postfix status
● postfix.service - Postfix Mail Transport Agent
   Loaded: loaded (/lib/systemd/system/postfix.service; enabled; vendor prese
   Active: active (exited) since Tue 2023-02-07 09:57:26 EST; 1h 13min ago
     Docs: man:postfix(1)
   Process: 6185 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 6185 (code=exited, status=0/SUCCESS)
       CPU: 1ms

Feb 07 09:57:26 pnap systemd[1]: Starting Postfix Mail Transport Agent...
Feb 07 09:57:26 pnap systemd[1]: Finished Postfix Mail Transport Agent.
lines 1-10/10 (END)
```

The output states that Postfix is active.

Step 2: Configure Postfix

Postfix uses the relay host configuration directive to send emails to external domains. The directive must contain the hostname or **IP address** of the remote SMTP server or SMTP service you want to use. For example, use SendGrid, Mandrill, Mailgun, or any other external SMTP provider.



Important: The latest update from some major providers (including Google, Microsoft, and Yahoo) complicates the setup as they no longer allow less secure apps to sign into the account. This update causes the mail delivery to fail.

The Postfix configuration files are *main.cf* and *master.cf*, located in the */etc/postfix/* directory.

After the installation, the **Postfix configuration wizard** appears. If it does not show up automatically, run the following command to start it:

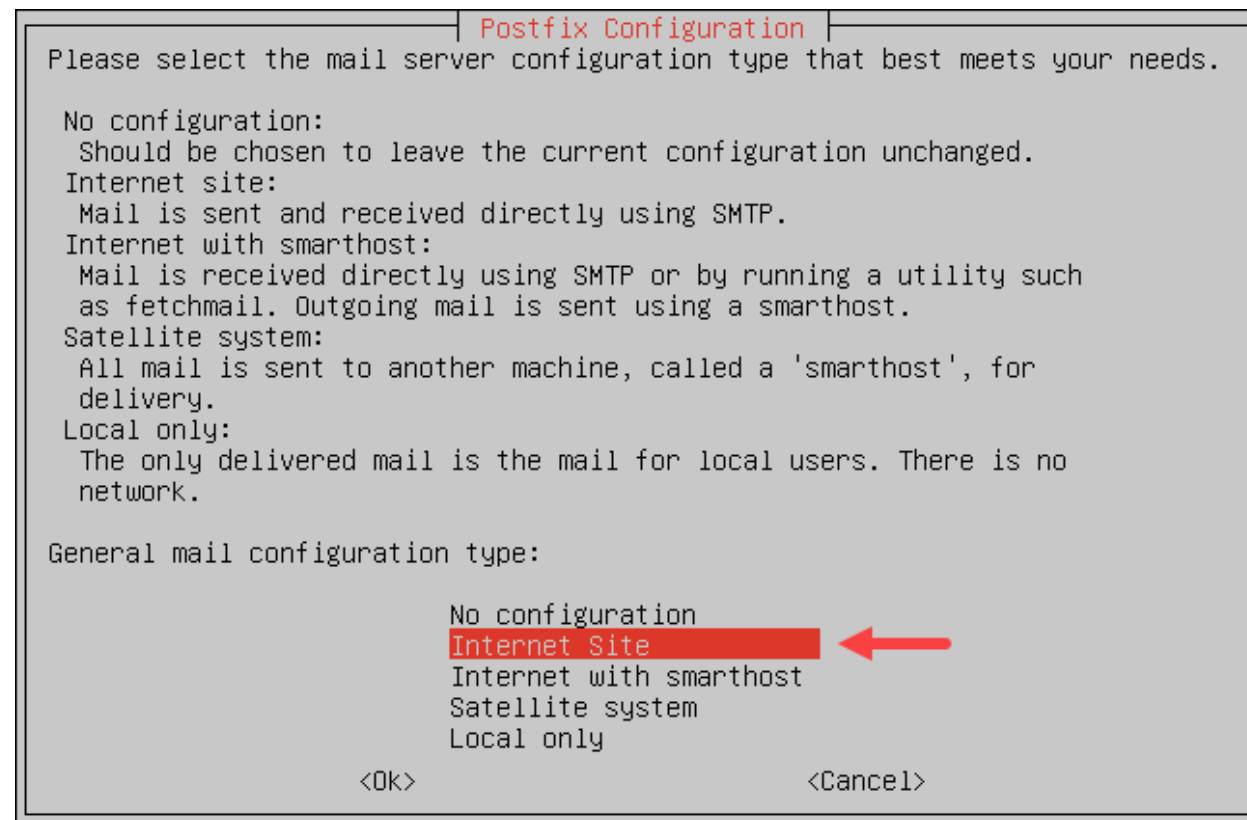
sudo dpkg-reconfigure postfix

Copy

Follow the steps below to set up Postfix:

1. Select the configuration type:

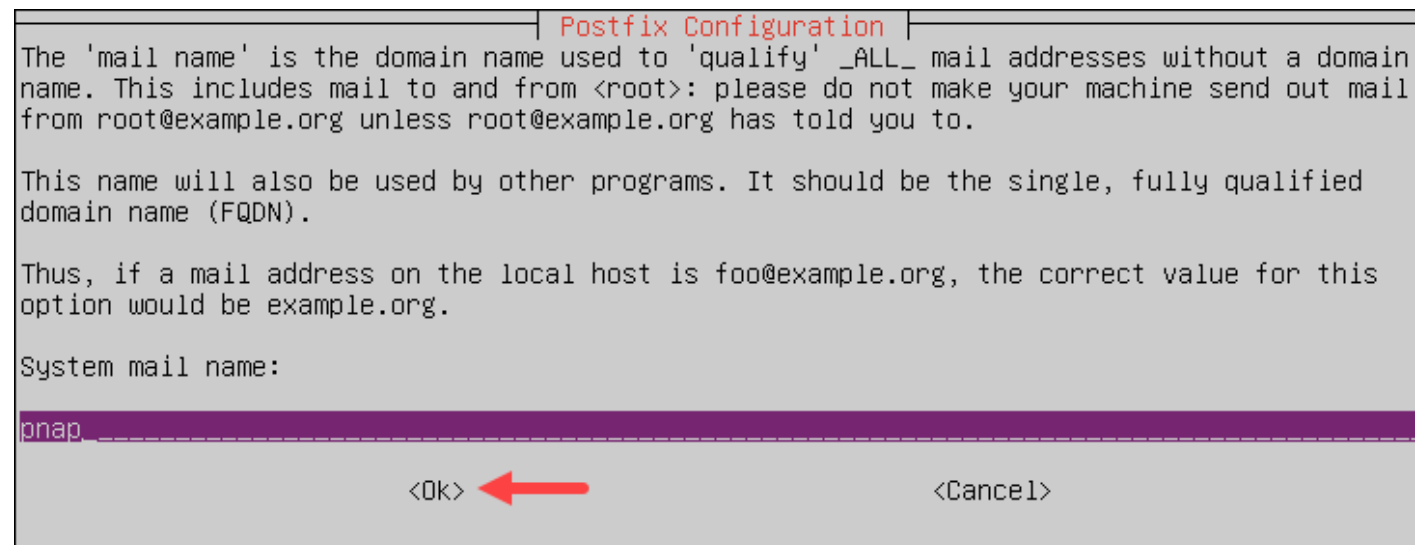
Choose the **Internet Site** mail configuration type. Press **TAB** to select **Ok** and **Enter** to confirm.



2. Enter the system mail name:

The system mail name is a fully qualified **domain name** (FQDN) that the system uses in banners, delivery status notifications, etc.

Enter the system mail name and press **Tab** to select **Ok** and **Enter** to confirm:



Postfix is now set up with the default configuration. Then, you must edit the `/etc/postfix/main.cf` configuration file to get it to work with external SMTP.

Enable Authentication

Install the pluggable authentication modules within the `libsasl2-modules` package on Debian-based systems or the `cyrus-sasl-p` `lain` package for RHEL systems. The packages enable authentication when using Postfix.

- Run the following command on Debian-based systems:

```
sudo apt install libsasl2-modules postfix
```

Copy

- For RHEL-based systems, run:

```
yum install cyrus-sasl-plain
```

Copy

Edit the Configuration Files

Use a [text editor](#) to edit the `/etc/postfix/sasl_passwd` and `/etc/postfix/main.cf` configuration files to complete the setup.

Follow the steps below:

1. Configure SMTP username and password:

The `/etc/postfix/sasl_passwd` file contains the usernames and passwords for the external SMTP server. Open the `/etc/postfix/sasl_passwd` file, and the text editor creates it if the file doesn't exist:

```
sudo nano /etc/postfix/sasl_passwd
```

Copy

Add the following line to the file:

```
[mail.isp.example]:587 username:password
```

Copy

Replace `[mail.isp.example]` with the provider's hostname.

Replace `username` and `password` with the SMTP provider credentials. You can also specify an [API key](#) if the provider allows it.

Save the changes and exit.

2. Create Hash Database File:

Create a Hash database `sasl_passwd.db` file in the `/etc/postfix/` directory using the `postmap` command. This file is used for querying Postfix lookup tables.

Run the following command:

```
sudo postmap /etc/postfix/sasl_passwd
```

Copy

3. Set up Hostname:

Set up the hostname parameter and relay server in the `/etc/postfix/main.cf` configuration file. Run:

```
sudo nano /etc/postfix/main.cf
```

Copy

Find the `myhostname` parameter and ensure it is the FQDN you configured in the wizard after the installation.

4. Set up Relay Server:

The final edit in the `/etc/postfix/main.cf` file is related to the settings needed for Postfix to use the external SMTP server. The settings instruct Postfix to deliver emails via a relay host, which is an external SMTP server.

Find and update the following line of the configuration file as follows:

```
relayhost = [SMTP-SERVER-ADDRESS]:587
```

Copy

- Replace **SMTP-SERVER-ADDRESS** with the SMTP server IP address or hostname.

Add the following lines to the end of the file:

```
smtp_sasl_auth_enable = yes
smtp_sasl_security_options = noanonymous
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_use_tls = yes
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
```

Copy

Save the changes and exit the editor.

Secure the Credentials

Secure your email password and hash DB files to ensure only the root user can access them.

Run the following commands to **change the file permissions** for `sasl_passwd` and `sasl_passwd.db`:

```
sudo chown root:root /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
sudo chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

Copy

Restart Postfix

Complete the configuration by restarting the Postfix service to make sure the changes take effect. Run:

```
sudo systemctl restart postfix
```

Copy

By default, the SMTP protocol runs at port number 25. Verify that TCP port 25 is in a listening state on 127.0.0.1. Use the **netstat command**:

```
sudo netstat -tulpn | grep :25
```

Copy


```
bosko@pnap:~$ sudo netstat -tulpn | grep :25
tcp        0      0 0.0.0.0:25          0.0.0.0:*          LISTEN
6182/master
tcp6       0      0 :::25              :::*                LISTEN
6182/master
```

The output shows that port 25 is in the listening state, which means the **port is open**.

Step 3: Test SMTP Server

Test the SMTP server by sending an email. Use the **mail command**, available as part of the **mailutils** package, or use Postfix's **sendmail** utility. Both options include an interactive mode and accept piped input.

For example, the syntax for using the interactive **sendmail** utility is:

```
sendmail recipient@domain.com
From: youraddress@domain.com
Subject: Email subject
This is the email body.
```

Copy

To send the email and exit interactive mode, press **Ctrl+D**.

Alternatively, send an email by piping the **echo command** output to the **mail** command. Use the following syntax:

```
echo "This is the email body." | mail -s "Email subject" -a "From: youraddress@domain.com" recipient@domain.com
```

Copy

After sending the email, verify that it was sent by checking the mail log file with the **tail command**:

```
sudo tail -f /var/log/mail.log
```

Copy

```
bosko@pnap:~$ sudo tail -f /var/log/mail.log
Feb  7 09:57:41 pn timerd: E8001C1895: uid=1000 from=<[redacted]>
Feb  7 09:57:41 pn postfix/cleanup[6193]: E8001C1895: message-id=<20230207145741.E8001C1895@smtp.sendgrid.net>
Feb  7 09:57:41 pn postfix/qmgr[6184]: E8001C1895: from=<[redacted]>, size=338, nrcpt=1 (queue active)
Feb  7 09:57:42 pn postfix/smtp[6187]: E8001C1895: to=<[redacted]>, relay=smtp.sendgrid.net[52.57.139.126]:587, delay=0.98, delays=0.02/0/0.63/0.32, dsn=2.0.0, status=sent (250 Ok: queued as H829LXM0TFmzWAZFSsrhw)
Feb  7 09:57:42 pn postfix/qmgr[6184]: E8001C1895: removed
```

The output shows that the email was sent, which relay server was used, and the recipient and sender addresses.

Step 4: Set up Email Forwarding

Email forwarding is useful when aggregating messages from different mailboxes into a single account. Postfix allows users to set up email forwarding by making a few changes in the main configuration file.

Follow the steps below to set up email forwarding in Postfix:

1. Open the `/etc/postfix/main.cf` configuration file and paste the following lines at the end of the file:

```
virtual_alias_domains = domain.com
virtual_alias_maps = hash:/etc/postfix/virtual
```

Copy

Replace `domain.com` with the domain Postfix uses to receive emails. Specify multiple domains by separating them with a space.

The `virtual_alias_maps` parameter contains the path to the file that specifies the mapping for email forwarding.

2. Create the `/etc/postfix/virtual` file and add the emails you want to forward and the destination emails.

For example, to forward emails from `address@domain.com` to `destination@domain.com`, enter the following line in the file:

```
address@domain.com destination@domain.com
```

Copy

Save the file and exit.

3. Update the Postfix lookup table:

```
postmap /etc/postfix/virtual
```

Copy

4. Reload the Postfix service:

```
sudo systemctl restart postfix
```

Copy

Step 5: Enable SMTP Encryption

SMTP encryption involves the installation of a [TLS](#) certificate for your domain name. Depending on your preferences, use a paid certificate or a free one from Let's Encrypt.



Important: Enforcing TLS encryption can cause mail delivery issues for SMTP hosts that don't have TLS configured or don't support TLS.

Follow the steps below to enable SMTP encryption:

1. Install the `certbot` client to configure the certificate:

- On Debian-based distributions, run:

```
sudo apt install certbot -y
```

[Copy](#)

Wait for the installation to complete.

- On RHEL-based distributions, **certbot** is not available in the default repository. First, enable the EPEL repository, and then install **certbot**:


```
yum install epel-release  
yum install certbot python2-certbot-apache mod_ssl
```

[Copy](#)

2. Configure the firewall:

Allow **port** 80 and enable domain verification. If you are using the **ufw firewall**, run:

```
sudo ufw allow 80
```

[Copy](#)

```
bosko@pnap:~$ sudo ufw allow 80  
Rules updated  
Rules updated (v6)
```

The output states that rules have been updated, which means HTTP is now allowed on port 80, and **certbot** can bind TCP to port 80.

3. Obtain the certificates:

When issuing certificates on a server that isn't running as a web server, run **certbot** with the **--standalone** flag. The syntax is:

```
sudo certbot certonly --standalone --rsa-key-size 4096 --preferred-challenges http -d your.c  
omain
```

[Copy](#)

Replace **your.domain** with your domain name.

An interactive configuration script starts.

4. Configure **certbot**:

The **certbot** configuration script prompts to provide the necessary information. Enter a contact email for the domain and agree to the Terms of Service.

```
bosko@pnap:~$ sudo certbot certonly --standalone -d [redacted]
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices) ←
(Enter 'c' to cancel): [redacted]

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree? ←
-----
(Y)es/(N)o: █
```

After the process completes, the certificates are stored under `/etc/letsencrypt/live/<your.domain>/`.

5. Add the new certificates to the Postfix configuration file:

Use the syntax below:

```
sudo postconf -e 'smtpd_tls_cert_file = /etc/letsencrypt/live/your.domain/fullchain.pem'
sudo postconf -e 'smtpd_tls_key_file = /etc/letsencrypt/live/your.domain/privkey.pem'
```

Copy

Replace `your.domain` in the commands with the email server's domain name.

6. Apply the changes by restarting Postfix:

```
sudo systemctl restart postfix
```

Copy

7. Send an email to test the setup.

Follow the steps outlined in the Test SMTP Server section to send a test email. This time the email is less likely to end up in spam since it is no longer unencrypted.



Conclusion

This tutorial showed how to install and configure Postfix to use an external SMTP server to send and receive emails. You also learned how to add SMTP encryption and forward emails.

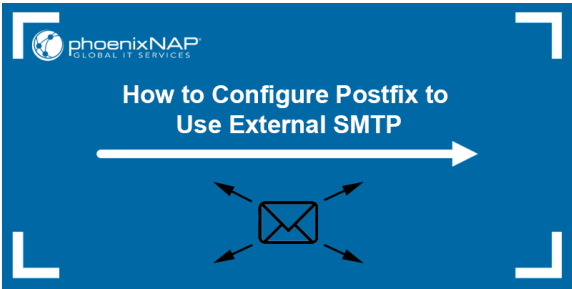
If you are using Office 365, check out our tutorial for [backing up Office 365 emails](#), or learn [why you should back up Office 365 data](#).

Was this article helpful?

Yes

No

Next you should read



[Networking](#), [SysAdmin](#)

How to Use the Linux mail Command

[Networking](#), [Web Servers](#)

Server OS Types & How to Choose

[Networking](#), [SysAdmin](#)

IMAP vs. POP3 vs. SMTP: What Are the Differences?

[Networking](#), [SysAdmin](#), [Web Servers](#)

What is SSH?

CONTACT US

- [Get a Quote](#)
- [Support \(1-855-330-1509\)](#)
- [Sales \(1-877-588-5918\)](#)



COLOCATION

- [Phoenix](#)
- [Ashburn](#)
- [Amsterdam](#)
- [Atlanta](#)
- [Belgrade](#)
- [Singapore](#)
- [Shipping Instructions](#)

RECENT POSTS

- [Java List Interface: Definition, Usage, Examples](#)
- [Linux Restart Command: How to Use reboot With Examples](#)
- [How to Read a File Line by Line in Python](#)

SERVERS

- [Bare Metal Cloud](#)
- [Dedicated Servers](#)
- [Database Servers](#)
- [Virtualization Servers](#)
- [High Performance Computing \(HPC\) Servers](#)
- [Dedicated Streaming Servers](#)
- [Dedicated Game Servers](#)
- [Dedicated Storage Servers](#)
- [SQL Server Hosting](#)
- [Dedicated Servers in Amsterdam](#)
- [Cloud Servers in Europe](#)
- [Big Memory Infrastructure](#)

BUY NOW

CLOUD SERVICES

- [Data Security Cloud](#)
- [Managed Private Cloud](#)
- [Object Storage](#)

SOLUTIONS

- [Disaster Recovery](#)
- [Web Hosting Reseller](#)
- [SaaS Hosting](#)

COMPLIANCE

- [HIPAA Ready Hosting](#)
- [PCI Compliant Hosting](#)
- [Privacy Center](#)
- [Do not sell or share my personal information](#)

NEEDS

- [Disaster Recovery Solutions](#)
- [High Availability Solutions](#)
- [Cloud Evaluation](#)

INDUSTRIES

- [Web Hosting Providers](#)
- [Legal](#)
- [MSPs & VARs](#)
- [Media Hosting](#)
- [Online Gaming](#)
- [SaaS Hosting Solutions](#)
- [Ecommerce Hosting Solutions](#)

COMPANY

- [About phoenixNAP](#)
- [IaaS Solutions](#)
- [Customer Experience](#)
- [Platform](#)
- [Schedule Virtual Tour](#)
- [Open Source Community](#)
- [Resource Library](#)
- [Press](#)
- [Events](#)
- [Careers](#)

PROMOTIONS

Python time.sleep(): How to Delay Code Execution

How to Install Docker on Windows

BMC PORTAL

- Contact Us
- Legal
- Privacy Policy
- Terms of Use
- DMCA
- GDPR
- Sitemap
- Blog
- Resources
- Knowledge Base
- IT Glossary
- GitHub
- RFP Template

© 2025 phoenixNAP | Global IT Services. All Rights Reserved.