server MANIA

NEW SERVER SETUP **CHECKLIST**

Whenever you receive the login credentials for a new server, there are some critical first steps to get your server secure and performing optimally.

In this guide, we'll share our recommended steps you should perform once you receive your new server details. Remember, we offer a **comprehensive server management solution** if you wish to have our team of expert server administrators take care of these tasks for you.

Change Administrator / Root Password

Any login credentials transmitted via plain text over email and that are accessible by a third party are inherently insecure. Changing the admin password is always recommended and it should be stored in a secure password manager.

Once logged in, use the **passwd** command to set a new root password.

Change the administrator account password in the Control Panel. Set a strong password policy in the server settings at this time.

Create A Separate Admin User

System activities should never be run as the primary root and administrator user. Creating a separate user with sudo or admin privileges is the safest approach.

Visit our Knowledge Base article on sudo to learn more.

Create a new administrator account in the Control Panel.

Disable Root Login

Servers are constantly targeted by brute-force to the root username. When root login is disabled, this lowers the risk of server intrusion.

Open the SSH Configuration:
sudo nano /etc/ssh/sshd_config
Set permitRootLogin=no
Restart sshd: sudo systemctl restart sshd

Disable the administrator user in the Control Panel. You should disable the guest login as well.

Change the Default SSH Port

Changing the default SSH port protects against automated bots that will try and brute-force on the default SSH port 22. While it will not stop more sophisticated intrusions, it is a good way to reduce those automated connections.

🐧 Open the SSH Configuration:

```
sudo nano /etc/ssh/sshd_config
```

Change the line with Port

Restart SSH: sudo service sshd restart

⊞ On Windows, this step is not typically required.

Generate an SSH Key Pair

Disabling password login via SSH and instead connecting with an SSH key is another great way to secure the most common intrusion point into a server.

🐧 Use the **ssh-keygen** command to create an SSH key on your computer and the **ssh-copy-id** command to copy the SSH key to the server:

```
ssh-copy-id root@SERVER-IP
```

⊞ On Windows, this step is not typically required.

Update Server Software

There is no better way to secure a server than to ensure it is always up to date with the latest OS and application software. Keeping your server up to date will protect against many common attacks.

🐧 apt-get upgrade or yum upgrad

⊞ Perform a system update in the control panel.

Set the System Time

It's important that all logs and system activities are recorded with the proper time so that you can effectively troubleshoot issues. On Windows, an improperly set time can also cause other server issues.

🐧

```
sudo timedatectl set-time YYYY-MM-DD
```

⊞ Configure the Date and Time by right-clicking on the clock in the bottom right-hand corner.

Disable or uninstall unused services

Unused services not only waste system resources, but also expose the server to unnecessary risk if the software is to become compromised. Removing unneeded software is an essential step in maintaining server security.

apt remove or yum remove package commands can be used to uninstall a package.

Add or remove software using the Control Panel.

Configure Two Factor Authentication

While this step is optional, two-factor authentication is another way to further restrict login access in the event that an SSH key was to become compromised.

```
Sudo apt-get install libpam-google-authenticator
```

Run the **google-authenticator** command to generate a secret key.

2FA is currently unavailable on Windows Server.

Enable and Configure the Firewall

Installing and configuring the firewall to only allow traffic required for your applications will greatly increase server security.

```
sudo apt install ufw
```

Open the Windows Firewall and configure as necessary.

Install Fail2ban

Fail2Ban is an intrusion prevention software framework that protects computer servers from brute-force attacks.

```
sudo apt install fail2ban -y
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo service fail2ban restart
```

On Windows, this step is not required.

Install Anti-Malware and Anti-Virus Software

We recommend installing an anti-virus software which can actively scan and quarantine viruses and malware detected on the system.

For Linux, we recommend ClamAV.

For Windows, we recommend using the built-in Windows Defender.

Install the Cloud Backup Agent

The last critical step which you should take when setting up a new server is configuring remote cloud backups. Every ServerMania server includes 50GB of cloud backup for free.

Visit our Knowledge Base to learn more about installing the cloud backup agent.

Now that you've performed all the essential server security steps, you need to keep your server monitored and up to date. Make sure that you login to the server frequently to review logs and update server software. The best way to keep a server secure is to limit server software to only essential items and remove any unnecessary packages.

NEED HELP WITH YOUR SERVER MANAGEMENT?

We offer a comprehensive lineup of server management packages from proactive server monitoring all the way up to complete server management. Contact us today to learn more!

SERVER MANAGEMENT

CONTACT US