# Respond to a suspected account or server compromise

Unexpected logins, unfamiliar users, changed files or unexplained outbound traffic deserve investigation. Record what you saw and contact support. A single alert does not prove an intrusion, but you should act when someone may still have access.

# Use a trusted device and contact support

1. Use a device you believe is clean. Open the billing portal by typing its known address, rather than following a link in a suspicious message.
2. Open a support ticket from your account. Give the affected service ID, time and timezone, symptoms and whether the activity appears ongoing.
3. If an attacker is causing harm, tell support that you need urgent containment. Ask about restricting access or isolating the affected service while preserving its disk and logs.
4. Keep a record of actions and times as you work. Avoid reinstalling, restoring over the system or deleting unfamiliar files before you preserve evidence.

If your email account may be compromised, secure it through its provider from the trusted device as well. An attacker with email access may intercept password resets. Tell CloudExa support if you cannot use the normal account-recovery route.

# Secure accounts and credentials

Change exposed passwords to unique values, review recovery methods and enable two-factor authentication. Review known sessions, API keys, SSH keys and subuser access where the panel offers them. Remove access you do not recognise after recording enough detail for investigation. Do not disable a legitimate recovery route without arranging another one.

Follow the account-security guide for panel-specific controls. Rotating a panel password does not necessarily rotate a VPS root password, database password or plugin token. List the secrets an attacker may have obtained, then rotate each at its issuing service. Never paste replacement secrets into a public log.

# Preserve evidence without spreading secrets

Keep relevant authentication, application and panel activity logs with their timestamps. Record suspicious account names, file paths, source addresses and error messages. Save copies in a private location with restricted access. Export only the evidence you need; configuration files can contain additional credentials.

For a VPS you can still inspect, avoid treating its own tools and logs as conclusive evidence of a clean system. A privileged attacker could change them. Support can help plan collection and recovery, but do not assume that restarting a service removes persistence.

If a file or plugin looks suspicious, do not run it on your computer to test it. Record its name, source and modification time, then ask how to preserve it. Keep untrusted archives separate from a known-good backup.

# Contain, then plan recovery

Agree containment with support according to the risk. Restricting network access or disabling a compromised credential can reduce ongoing harm while leaving data available for investigation. Avoid stopping database writes by forcing power off unless the situation requires it and you understand the recovery implications.

Establish how the attacker entered before returning the service to normal use. Patch the affected software, correct access rules and rotate exposed credentials. Select recovery data from a point you have reason to trust. A backup taken after the first intrusion may contain the same problem.

Some incidents require a clean rebuild, but preserve evidence and data first and agree the process before replacing anything. Check application behaviour, accounts and monitoring after recovery. Malware cleanup and data reconstruction are outside the managed OS add-on's listed scope; ask support what assistance is available.

Use the support-ticket checklist to send evidence without exposing passwords, private keys or console access links.

Further reading: NCSC guidance on incident response.

---

Revision #2
Created 2026-11-08 20:06:28 UTC by CloudExa Hosting Admin
Updated 2026-11-08 20:06:28 UTC by CloudExa Hosting Admin