

ServersCTL WHMCS cPanel Replication Module

1. Requirements and preparation

The module is designed for self-hosted WHMCS 8.13 LTS and 9.x. WHMCS Cloud does not support the required custom add-on and server modules.

Before installation, confirm:

- PHP has the cURL and OpenSSL extensions enabled.
- WHMCS can make outbound HTTPS requests to the configured ServersCTL Partner API.
- You can write to the WHMCS `modules/addons/` and `modules/servers/` directories.
- Each production and recovery node is an enabled cPanel server in WHMCS.
- The WHMCS server hostname exactly matches the normalised hostname reported by the corresponding ServersCTL agent.
- Source and recovery servers have enrolled, recently reporting ServersCTL agents.
- The source pool's Managed DNS configuration controls the protected domains.
- The WHMCS host has a stable public egress IP, or you can approve a new pairing after it changes.

Take a normal WHMCS database and file backup before installing or upgrading any third-party module.

1.a. DNS Requirements for Replication

Replication requires reliable access to update the domain's DNS records. This is especially important during a high-availability event, when ServersCTL activates the replicated cPanel account after the primary server becomes unavailable.

Do not use an API key from the primary cPanel server for DNS management. If that server goes offline, ServersCTL may be unable to update the DNS records and direct traffic to the recovery server.

There are two methods for managing DNS currently. You must use one of these methods to achieve High Availability.

cPanel DNS Cluster

[DNS Clusters | cPanel & WHM Documentation](#)

A cPanel DNS Cluster provides centralised DNS management for your cPanel servers. DNS changes made on the cluster are propagated to its connected servers. When configured appropriately, changes made within WHM or cPanel are also synchronised with the DNS Cluster hosts.

To use a cPanel DNS Cluster with ServersCTL, add an API DNS key from one of your cluster hosts. Customers point their domains to the cluster’s nameservers, and ServersCTL uses the API key to manage the required DNS records.

Cloudflare DNS

Customers using Cloudflare can provide a scoped API token that grants ServersCTL permission to read and update DNS records for the relevant zone. The customer enters the API Key during the order process.

2. Download and install

1. Sign in to ServersCTL.
2. Open **Account** → **Partners**.
3. Under **WHMCS module**, select **Download WHMCS module**.
 - You can also download from the CDN. [ServersCTL WHMCS cPanel Replication Module](#)
4. Extract `serversctl_replication.zip` at the WHMCS root.

The ZIP is rooted at `modules/` and installs both components:

Component	Installed path	Purpose
Addon module	<code>modules/addons/serversctl_replication/</code>	Pairing, admin workspace, inventory, product catalogue, widget and customer continuity pages
Server module	<code>modules/servers/serversctl_protection/</code>	WHMCS provisioning and lifecycle actions for protection services

Do not move the bundled server module into the addon directory.

Activate the addon

1. In WHMCS, open **System Settings → Addon Modules**.
2. Find **ServersCTL Replication**.
3. Select **Activate**.
4. Grant access to the required WHMCS administrator roles.
5. Open the module from the WHMCS addon menu.

Activation creates the module's local mapping tables and the editable **ServersCTL Replication - DNS Cutover** email template. Deactivating the addon later does not stop existing protection at ServersCTL, but WHMCS management is unavailable until it is reactivated.

3. Pair WHMCS with ServersCTL

The current module uses cryptographic installation pairing. Do not create a permanent Partner API key for normal setup.

1. Open **ServersCTL Replication** in WHMCS.
2. Copy the one-time pairing code and note the displayed public source IP.
3. In a separate browser tab, sign in to ServersCTL as the account owner.
4. Open **Account → Partners**.
5. Paste the code under **Connect WHMCS securely**.
6. Select **Approve this WHMCS**.
7. Return to WHMCS and reload the addon.

The code expires after 15 minutes. Approval binds the module identity to the WHMCS domain and observed public egress IP. ServersCTL passwords and permanent API keys never enter WHMCS.

Create a new Partner account from WHMCS

If the provider has no ServersCTL account, use the registration form shown with the pairing code. Enter the company name and owner email, accept the terms, then open the emailed 24-hour claim link. The owner must set a password of at least 12 characters.

Customer provisioning remains locked until the claim is completed.

4. Configure the addon

Open **System Settings → Addon Modules → ServersCTL Replication → Configure**.

Setting	Recommended value	Effect
API Base URL	Production Partner API URL ending in <code>/api/partner/v1</code>	Selects the ServersCTL control plane
Legacy API Key (migration only)	Empty	Used once only when upgrading an old key-based installation
Customer-facing brand name	Your hosting brand	Overrides the WHMCS company name in customer continuity pages
Customer-facing logo URL	HTTPS SVG or PNG	Overrides the WHMCS theme logo; a transparent image at least 320 px wide is recommended
Dark continuity experience	On	Uses the dark continuity workspace; disable to retain the light WHMCS presentation
WHMCS status-area visibility	Off initially	<code>authenticated</code> or <code>public</code> exposes only aggregate, redacted status data to compatible templates
Customer target choice	Automatic	<code>choose-one</code> or <code>choose-multiple</code> lets customers select from approved destinations
Allow Cloudflare DNS	As required	Lets customers choose Cloudflare and enter a scoped token during purchase
Allow customer test cutover	According to policy	Shows guarded recovery and failback controls to eligible customers
Customer recovery action	Replicate & Cut Over	Takes and restores a fresh copy before DNS movement; DNS only uses the latest verified copy
DNS cutover email notifications	On	Sends the editable WHMCS template after manual or automatic routing changes
Offer weekly/daily/8-hour/4-hour/hourly replication	Match your catalogue	A frequency appears only when enabled, priced in WHMCS and allowed by the Partner plan

The Partner API is the feature authority. Editing the open-source PHP module cannot grant schedules, targets, manual sync or storage capability that the Partner account does not have.

5. Connect servers and destinations

Open **ServersCTL Replication** → **Servers & destinations**.

The setup sequence is:

1. **Connect servers** — install the ServersCTL agent on each cPanel server involved.
2. **Choose account servers** — select the source pool containing live WHMCS accounts.
3. **Allow destinations** — choose the recovery cPanel servers customers may use.
4. **Protect accounts** — return to **Account protection** and enable services.

Existing ServersCTL fleet

Select the existing source cPanel pool and approved recovery destinations. Add the provider's HTTPS support URL, then save.

New fleet

The guided setup can create a cPanel pool and enrol a server:

1. Enter the server connection details.
2. Verify the displayed SSH host fingerprint against a trusted source.
3. Explicitly confirm the fingerprint.
4. Allow WHMCS to check root privilege, supported Linux/cPanel software and available disk space.
5. Wait for the agent installation and fresh heartbeat.

The SSH password is held only for the current PHP request and is not saved or sent to ServersCTL. WHMCS constructs the fixed install command locally and verifies the signed release manifest and file hashes before executing the downloaded agent as root.

6. Create and price the protection catalogue

From **Servers & destinations**, select **Create protection catalogue**.

The action is idempotent and can safely repair an existing catalogue. It creates:

- Weekly replication addon.
- Daily replication addon.
- 8-hour replication addon.
- 4-hour replication addon.
- Hourly replication addon.
- Additional Replication Target addon.

Weekly pricing is created at zero by default. Premium frequency addons remain disabled until the provider sets recurring prices in WHMCS.

Configure sales

1. Open the generated WHMCS product addons.
2. Set recurring prices for every billing cycle and currency you intend to sell.
3. Enable only the addon frequencies you want customers to order.
4. Confirm those same frequencies are enabled in the ServersCTL Replication addon settings.
5. Verify the Partner Capacity card allows them.

Customers see only the intersection of host-enabled, WHMCS-priced and Partner-authorized frequencies. The first selected destination is included in the frequency addon; each additional selected destination adds one **Additional Replication Target** line.

Do not manually create or request internal ServersCTL product IDs.

7. Protect existing accounts

Open **ServersCTL Replication** → **Account protection**.

The inventory cross-references active WHMCS shared-hosting and reseller services with live cPanel `listaccts` data. It identifies protected, unprotected, missing and unmatched accounts.

To protect a matched service:

1. Find the customer and cPanel account.
2. Select an approved recovery destination.
3. Choose the replication policy and permitted customer actions.
4. Start protection.
5. Confirm that the account reports an active protection state and a recovery point after the first completed copy.

Admin-managed accounts

Select **Manually protect an account** to show discovered cPanel accounts that do not match a WHMCS service. These are labelled **Admin-managed**.

Protecting an Admin-managed account does not create or modify a WHMCS client, hosting service, order or invoice. It is excluded from customer ordering.

Other administration tabs

- **Infrastructure map** embeds the real, read-only and redacted cPanel pool overview, including linked Cloud DR recovery agents referenced by the pool's protection jobs. Use **Open fullscreen** for the wallboard view.
- **Servers & destinations** controls source, recovery and support routing and creates the protection catalogue.
- **DNS credentials** manages per-customer Cloudflare credentials and bindings. Customers are labelled by domain, cPanel account, WHMCS customer and service number.

8. Customer ordering and continuity console

The customer opens the provider-branded **Hosting Protection** or **Account Continuity** page in WHMCS.

The purchase wizard:

1. Lists eligible active shared-hosting or reseller accounts owned by that customer.
2. Lets the customer choose an available replication frequency.
3. Uses automatic target selection by default, or offers approved targets according to module policy.
4. Lets the customer choose cPanel DNS or Cloudflare when enabled.
5. Creates an addon-only WHMCS order attached to the parent hosting service.
6. Provisions protection after invoice payment or staff activation. ServersCTL activation completes before WHMCS marks the order active; a rejected remote activation leaves the add-on pending for a safe retry. Retrying that account reuses the same add-on and cannot create duplicate active protection billing.

For Cloudflare, the customer must supply the 32-character Account ID and an API token with Zone DNS read/edit access to the exact zone. Successful credential verification immediately creates the domain-specific Managed DNS binding, even when a later protection step needs to be retried. The secret is encrypted only while the order is pending and is removed from WHMCS after successful activation.

Weekly zero-value orders are closed as paid immediately and do not remain in the customer's unpaid-invoice count.

The continuity console can show:

- Current live and standby server roles.
- Last protected copy and replication schedule.
- Recovery readiness and recent activity.
- Manual replication when allowed.
- DNS and credential state.
- Guarded recovery and failback when allowed.
- A customer self-service **Remove protection** action when safe.

Customer pages use the provider's brand. They do not display ServersCTL pricing, upgrade prompts or support links.

9. Recovery, DNS and lifecycle behavior

Recovery requirements

Recovery preflight checks:

- An active protected customer and valid entitlement.
- A completed protected copy.
- A reachable receiving agent and standby endpoint.
- Website/TLS readiness.
- Authoritative DNS control for the protected domain.
- An exact enabled WHMCS cPanel server matching the destination hostname.

For host-managed DNS, customer readiness messages use the WHMCS company/Customer Brand Name only. Credential labels, DNS hostnames and key timestamps remain operator-only.

The confirmation is one-time and expires. Never use a stale preflight for a later cutover.

DNS only

Uses the latest verified protected copy, then moves all enabled cPanel account A records together. This includes the apex and service names such as `mail`, `webmail`, `cpanel` and `ftp`.

Replicate & Cut Over

Starts a durable workflow that:

1. Takes a fresh full account copy.
2. Restores it to the recovery server.
3. Waits for agent, DNS, HTTP and TLS readiness.
4. Re-runs safety checks.
5. Moves authoritative DNS.
6. Updates the WHMCS hosting service's assigned server.

The workflow continues if the browser closes. A workflow is claimed by only one evaluator before routing changes begin, so overlapping scheduler runs cannot repeat confirmation or overwrite a successful cutover with a stale-route error. After cutover, native WHMCS cPanel login and quick actions use the active recovery host. Failback restores DNS and the WHMCS server assignment to production. If the synchronous WHMCS request is delayed after routing changes, the modal polls authoritative state and completes as soon as the requested route is visible.

Email notifications

When enabled, manual and automatic cutovers send **ServersCTL Replication - DNS Cutover** through WHMCS. Edit this template under the normal WHMCS email-template settings. Duplicate notifications for the same active server are suppressed.

Suspension, cancellation and termination

- Addon suspension pauses the customer's protection access.
- Unsuspension resumes it.
- Addon cancellation or termination requests guarded cleanup.
- Successful parent cPanel service termination cascades cleanup to mapped protection addons.
- Future-dated cancellation does not remove protection before WHMCS terminates the service.
- Cleanup waits if DNS is still routed to recovery and is retried by daily WHMCS maintenance after the safety condition is resolved.
- Removing protection leaves the parent hosting service intact.
- Open continuity consoles poll live state and automatically reconcile to the unprotected view when protection is removed in another tab or by staff; customers do not need to refresh manually.

The WHMCS cron is also used to reconcile the hosting service's assigned server with the authoritative DNS-active node after automatic cutover or an interrupted request.

10. Upgrade, disconnect and deactivate

Upgrade

1. Back up WHMCS.
2. Download the latest ZIP from **Account → Partners**.
3. Extract it over the existing module directories.
4. Open the addon and verify health, pairing and the installed version.
5. Run **Create protection catalogue** to repair catalogue definitions without duplicating them.
6. Test one non-production or designated recovery-test service.

An installation upgraded from an old key-based release can use its legacy Partner key once to bind the exact installation identity. The module clears the key after successful migration. Old API values containing only the ServersCTL site origin are resolved to `/api/partner/v1`.

Disconnect

Disconnect from **ServersCTL → Account → Partners**, not by deleting database rows. Disconnect revokes the selected installation's access while retaining imported infrastructure and protection records.

Deactivate

WHMCS addon deactivation leaves active protection running at ServersCTL. Reactivate and pair the addon to manage it again.

11. Troubleshooting

Pairing code is missing or expired

Reload the addon page and request a fresh code. Approve it within 15 minutes while signed in as the ServersCTL account owner.

Module returns an IP or authentication error

Compare the WHMCS server's current public egress IP with the IP shown under **Account** → **Partners**. A changed IP requires fresh pairing.

“PHP OpenSSL is required”

Enable the PHP OpenSSL extension for the PHP runtime serving WHMCS, then restart the relevant PHP/web service and reactivate the addon.

Connection fails

Confirm the API URL is HTTPS and ends in `/api/partner/v1`, PHP cURL is enabled, DNS resolves and the WHMCS server can make outbound HTTPS requests. Do not work around the error by adding a permanent Partner key.

No accounts are listed

Confirm:

- The source pool is selected.
- Its cPanel agents are live.
- The WHMCS products are shared-hosting or reseller services in Active or Suspended state.
- The WHMCS cPanel username matches a discovered live account.
- The cPanel server hostname matches the ServersCTL agent hostname.

Use **Manually protect an account** only for accounts intentionally not sold through WHMCS.

A frequency does not appear to customers

It must be enabled in addon settings, have a valid recurring WHMCS price and be allowed by the Partner plan. Check all three.

Recovery preflight cannot map the destination

Add the recovery node as an enabled cPanel server in WHMCS. Its hostname must exactly match the hostname reported by the ServersCTL agent.

Cloudflare recovery is disconnected

Open the customer's DNS page, add a scoped Cloudflare credential and bind it to the exact protected domain. Credentials belonging to another customer or the provider's general DNS vault are not used as fallback.

Cancellation remains pending

Check whether authoritative DNS still points to recovery. Return service to production first. Daily WHMCS maintenance retries cleanup after the safety condition is satisfied.

Safe release test

Use only a designated recovery-test account. Verify a completed fresh copy, recovery preflight, authoritative DNS movement, HTTP response, WHMCS server reassignment and successful fallback. Never run destructive recovery testing against an unrelated customer.

Revision #4

Created 2026-08-10 11:05:14 UTC by ServersCTL

Updated 2026-08-10 15:29:44 UTC by ServersCTL