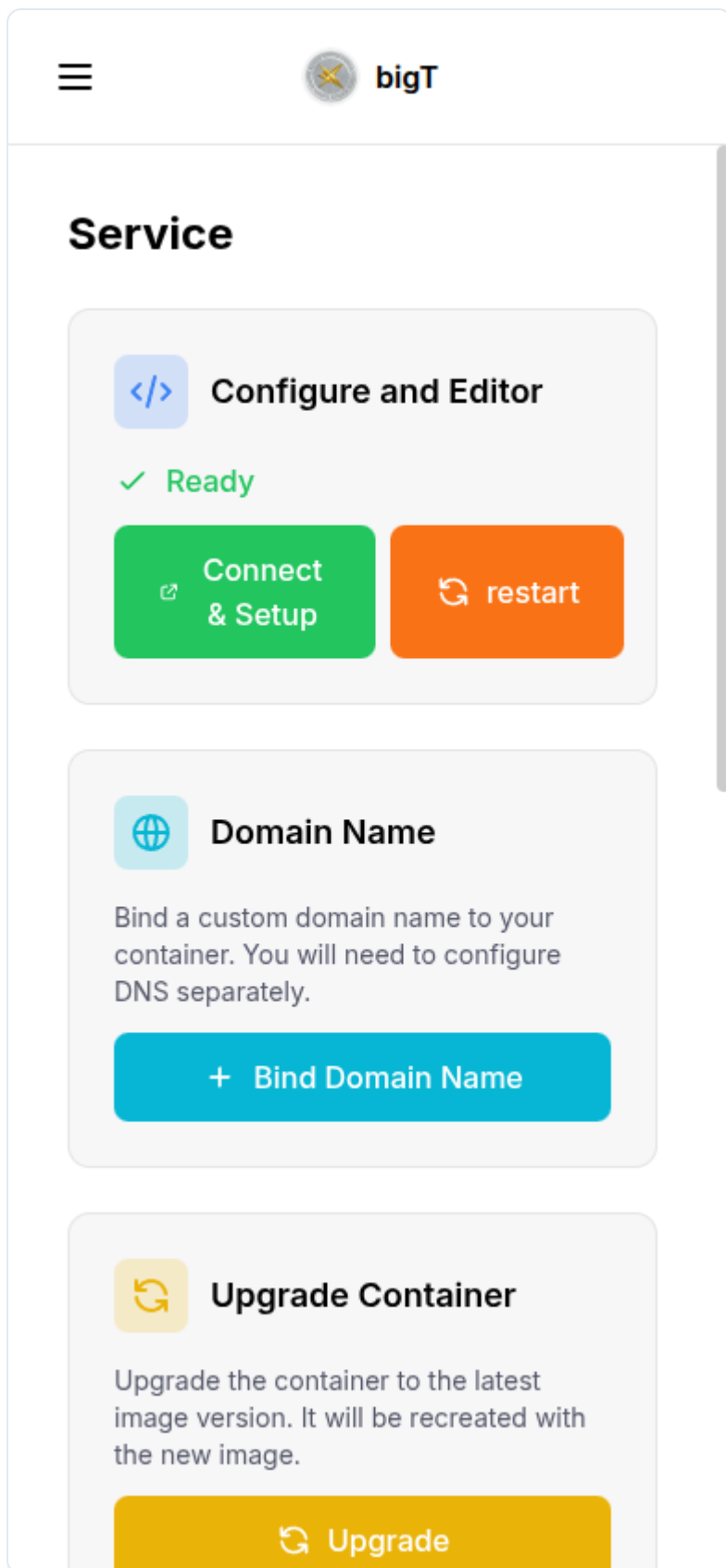


This guide demonstrates the service dashboard features:
monitoring container status, connecting to your AI
workspace, managing the container, and configuring VPN
access.

BigT.AI — Service Dashboard — Container Management &
LLM Configuration

1. Configure & Editor

The service dashboard's primary card shows your container's current state with a green **Ready** badge when deployed.



Two buttons are available when the container is ready:

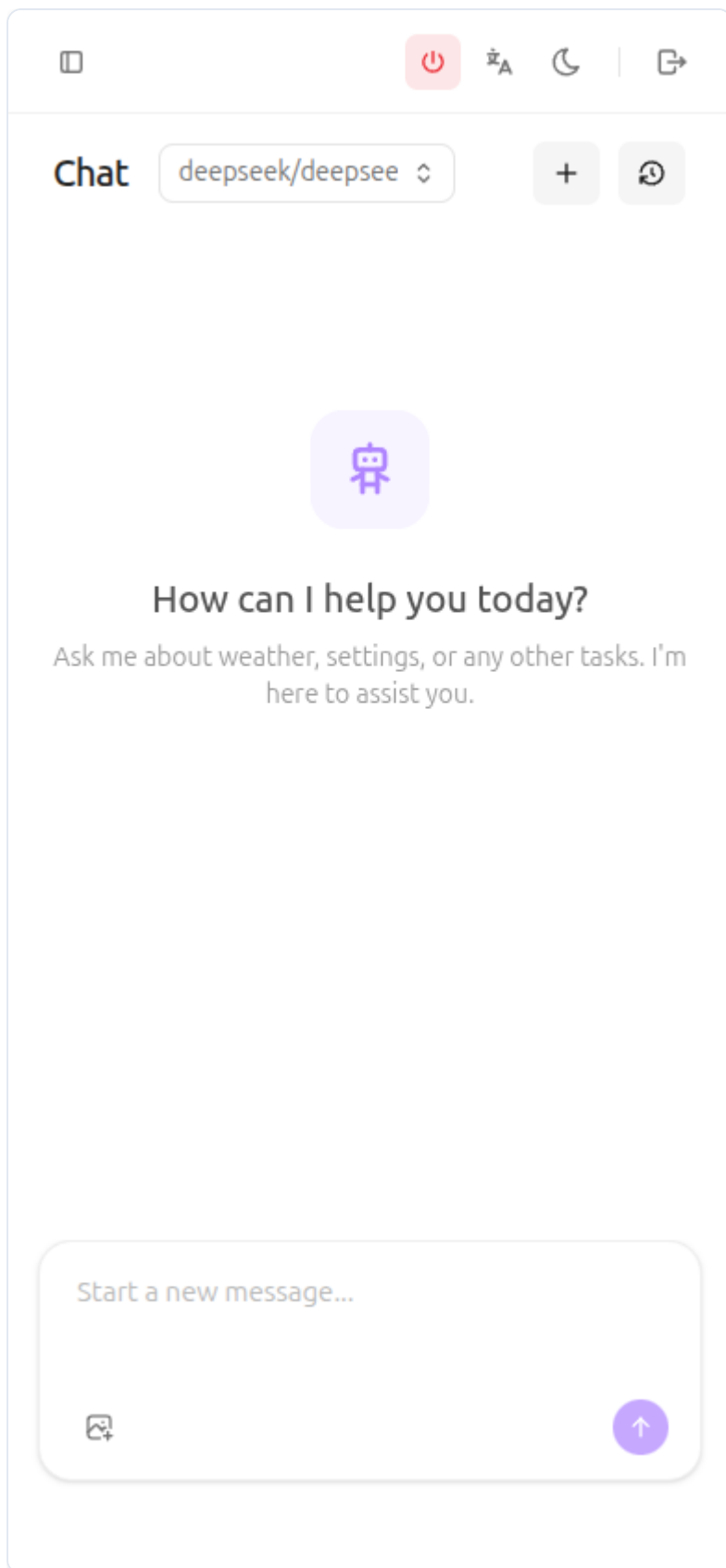
- **Connect & Setup** — Opens the picoclaw launcher workspace via SSO (one-time HMAC-signed token). The agent's chat interface, file browser, public wiki, and settings are accessible through this workspace.

- **Restart** — Reboots the container services with a progress indicator.

If no active workspace exists, a link to [/new-ai](#) is shown to provision one.

2. Agent Workspace

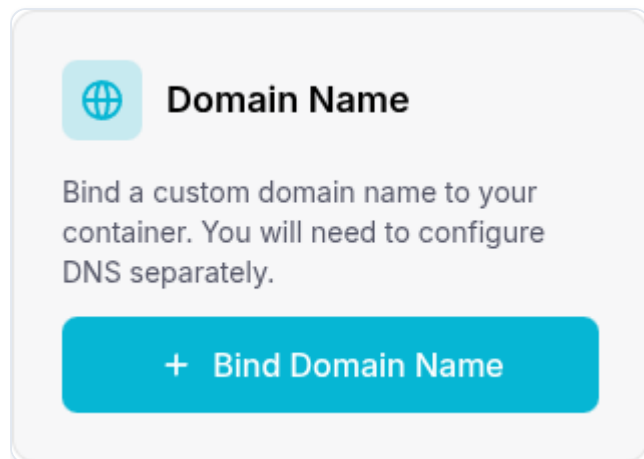
Connect via SSO from the service page to open your AI workspace.



The picoclaw launcher workspace provides a chat interface to send messages and receive AI responses, a data page to upload files, a public wiki for documentation, and settings to configure channels and tools. The SSO URL includes the selected language (`&lng=<lang>`).

3. Domain Name

Bind a custom domain to your container for branded access.



The **Domain Name** card shows the current custom domain (if bound) with a **Manage** button, or a **Bind Domain Name** button to add one. The modal displays DNS setup instructions (A record to server IP) and supports binding or removing the domain.

4. Upgrade Container

Update your container to the latest image version.

Click **Upgrade** to check versions. The modal shows the currently deployed version vs. the latest available version with an **Upgrade** confirmation button. The container is recreated with the new image and a success message is shown for 5 seconds.

5. Delete Container

Permanently remove your container and all associated data.

This red-themed danger card requires typing the safe name into a confirmation input before the **Delete Container** button becomes active. After deletion, the UI refreshes to show no active workspace.

6. VPN / Proxy

Secure remote access via VLESS+REALITY proxy.

 **VPN / Proxy**

Use VLESS+REALITY proxy to securely access your AI agent from anywhere. Scan the QR code with Hiddify-Next or any VLESS-compatible client.

 Google Play

 App Store

 GitHub

SHARE LINK 

vless://189370b2-55aa-47a4-8c5a-eaaf14aff245@85.214.37.95:29014?encryption=none&security=reality&type=tcp&flow=xtls-rprx-vision&sni=www.microsoft.com&pbk=U1V2bvt28S6r6_7JoF8bQoU3UGNPh1uD-qsLjMDIM3I&fp=chrome&sid=90df99b647225ba2#2336dcd87562



 Refresh

The **VPN / Proxy** card provides download links for Hiddify-Next (Google Play, App Store, GitHub releases). Click **Show VPN Config** to fetch the VLESS share link and QR code. A **Refresh** button regenerates the config. All traffic is obfuscated as regular HTTPS.

7. LLM

Single-click SSO to the LLM router at llm.bigt.ai.

The **LLM** card has a single button that performs SSO via JWT, redirecting to the LLM router's SSO endpoint for API key and model management.

Full Demo Flow

Complete service dashboard workflow:

```
// 1. Check container status on Configure & Editor card
// 2. Connect to agent workspace via SSO
// 3. Bind a custom domain (optional)
// 4. Upgrade container to latest version
// 5. Delete container (if needed)
// 6. Configure VPN for remote access
// 7. Open LLM router for model management
```