Advanced Features

Cron jobs, backups, security tools, handlers, SSH keys, and other advanced DirectAdmin options.

Contents

- Managing Apache Handlers
- Configuring CatchAll Email
- Backup and Restore Options
- Creating and Managing Cron Jobs
- Custom Error Pages Setup
- Managing MIME Types
- Using Login Keys
- Enabling TwoStep Authentication
- PasswordProtected Directories
- Managing SSH Keys
- Editing Nginx Templates
- Using Git in DirectAdmin
- ClamAV Antivirus Overview

DANUMHOST

Managing Apache Handlers

Assign Apache handlers so specific file extensions run with the correct processor.

Apache handlers tell the web server how to process certain file types — for example running `.php` files through the PHP engine.

Add or edit a handler

1. Go to **Advanced Features → Apache Handlers**.
2. Select the domain.
3. View existing handlers or click **Add Handler**.
4. Enter the handler name and file extension (for example handler `application/x-httpd-php82` for extension `.php`).
5. Save the handler.

When you need this

Most sites work with default handlers. Custom handlers are useful for legacy scripts, CGI files, or non-standard extensions. Incorrect handlers can cause downloads instead of execution — revert changes if your site stops working.

DANUMHOST

Configuring CatchAll Email

Route mail sent to any non-existent address on your domain to a single mailbox.

A catch-all address receives email sent to any username at your domain that does not have its own mailbox — for example mail to `anything@yourdomain.com`.

Enable catch-all

1. Go to **Advanced Features → Catch-All E-mail**.
2. Select the domain.
3. Choose the destination mailbox for unmatched addresses.
4. Save the setting.

Security consideration

Catch-all addresses receive large volumes of spam sent to random usernames. Many administrators prefer disabling catch-all and creating only the mailboxes they need. If spam becomes overwhelming, disable catch-all and use specific forwarders instead.

DANUMHOST

Backup and Restore Options

Create and restore account backups from DirectAdmin or JetBackup.

Regular backups protect your website, databases, and email. DirectAdmin offers built-in backup tools; DanumHost also provides JetBackup for scheduled restores.

Create a manual backup

1. Go to **Advanced Features → Create/Restore Backups**.
2. Select what to include: domains, email, databases, and configuration.
3. Choose a destination (local account storage or remote FTP if configured).
4. Start the backup and download the archive when complete.

Restore from backup

1. Open the same backup section and choose **Restore**.
2. Select the backup file and components to restore.
3. Confirm — restoring overwrites current data for selected items.

For automated daily backups and one-click restores, see the JetBackup guide under Extra Features.

DANUMHOST

Creating and Managing Cron Jobs

Schedule scripts and commands to run automatically at set intervals.

Cron jobs run commands on a schedule — perfect for maintenance scripts, report generation, or CMS tasks.

Create a cron job

1. Go to **Advanced Features → Cron Jobs**.
2. Click **Add Cron Job**.
3. Set the schedule using minute, hour, day, month, and weekday fields (or use a preset such as daily).
4. Enter the command — often a PHP script path such as `/usr/local/bin/php /home/user/domains/example.com/public_html/cron.php`.
5. Save the job.

Best practices

- Use full paths to PHP and scripts.
- Redirect output to a log file for debugging.
- Avoid running intensive jobs every minute.

Many applications provide the exact cron command in their documentation — copy it exactly.

DANUMHOST

Custom Error Pages Setup

Replace default server error pages with your own branded 404 and 500 pages.

Custom error pages improve user experience when visitors hit broken links or server errors.

Configure error pages

1. Go to **Advanced Features → Custom Error Pages**.
2. Select the domain.
3. Choose the error code to customize (404, 403, 500, etc.).
4. Enter HTML content or upload a page — include navigation back to your homepage.
5. Save the error page.

Design tips

- Keep messaging friendly and on-brand.
- Include a search box or sitemap link on 404 pages.
- Test by visiting a non-existent URL on your site.

DirectAdmin stores custom error pages per domain. CMS platforms like WordPress may override 404 handling with their own templates.

DANUMHOST

Managing MIME Types

Define how browsers handle file downloads by configuring MIME types.

MIME types tell browsers how to interpret file formats. Adding or correcting MIME types ensures files download or display correctly.

Add a MIME type

1. Go to **Advanced Features → MIME Types**.
2. Select the domain.
3. Click **Add MIME Type**.
4. Enter the file extension (for example `.webp`) and the MIME type (for example `image/webp`).
5. Save.

Common use cases

- Serving modern image formats not in default configuration.
- Forcing specific file types to download rather than display.
- Supporting custom application file extensions.

Incorrect MIME types can cause browsers to mishandle files. Use official IANA MIME type values when possible.

DANUMHOST

Using Login Keys

Generate one-time or restricted login keys for secure DirectAdmin access.

Login keys let you access DirectAdmin without sharing your main password — useful for developers or temporary access.

Create a login key

1. Go to **Advanced Features → Login Keys**.
2. Click **Create Login Key**.
3. Set an expiry date and optional IP restriction.
4. Choose permission level — full access or limited to specific features.
5. Generate the key and copy the login URL provided.

Security tips

- Set short expiry times for temporary contractors.
- Restrict keys to known IP addresses when possible.
- Revoke keys immediately when no longer needed.

Never post login key URLs in public tickets or chat channels.

DANUMHOST

Enabling TwoStep Authentication

Add two-factor authentication to protect your DirectAdmin account.

Two-step authentication (2FA) adds a second verification step beyond your password, significantly improving account security.

Enable 2FA

1. Go to **Advanced Features → Two-Step Authentication**.
2. Choose an authenticator app method (Google Authenticator, Authy, etc.).
3. Scan the QR code with your authenticator app.
4. Enter the verification code to confirm setup.
5. Save backup codes in a secure location.

Logging in with 2FA

After entering your password, provide the six-digit code from your authenticator app. Codes rotate every 30 seconds. If you lose access to your app, use a backup code or contact DanumHost support for account recovery.

DANUMHOST

PasswordProtected Directories

Restrict access to folders on your website with username and password authentication.

Password-protected directories require visitors to enter credentials before viewing content — ideal for staging sites or private downloads.

Protect a directory

1. Go to **Advanced Features → Password Protected Directories**.
2. Select the domain.
3. Navigate to the folder you want to protect (for example `/private`).
4. Enable password protection for that directory.
5. Create a username and password for authorized users.
6. Save.

Testing

Visit the protected URL in a private browser window. You should see a login prompt. Share credentials only with intended users. Remove protection when the content should be public again.

DANUMHOST

Managing SSH Keys

Add SSH public keys for secure shell and SFTP access without passwords.

SSH keys provide secure, passwordless authentication for terminal and SFTP connections to your account.

Add an SSH public key

1. Generate a key pair on your computer with `ssh-keygen` if you do not have one.
2. Go to **Advanced Features → SSH Keys** (or SSH Key Management).
3. Click **Add Key**.
4. Paste your public key (the `.pub` file contents).
5. Save the key.

Connect via SSH

- **Host:** your server hostname or IP
- **Port:** 22 (or the port shown in your account)
- **User:** your DirectAdmin username

SSH access may require a hosting plan that includes shell access. Never share your private key — only the public key belongs on the server.

DANUMHOST

Editing Nginx Templates

Customize Nginx configuration snippets for your domain when permitted.

On Nginx-powered DirectAdmin setups, custom templates let advanced users adjust server behaviour for specific domains.

Edit templates

1. Go to **Advanced Features → Nginx Templates** (visible on supported configurations).
2. Select the domain or template type.
3. Add custom directives such as cache headers, redirect rules, or proxy settings.
4. Save and allow DirectAdmin to rebuild the Nginx configuration.

Caution

Syntax errors in Nginx templates can prevent your site from loading. Make small changes, test immediately, and keep a copy of the original template. If your site returns a 502 error after editing, revert the template or contact DanumHost support.

DANUMHOST

Using Git in DirectAdmin

Deploy and manage website code with Git repositories in DirectAdmin.

DirectAdmin includes Git integration so you can clone repositories and deploy updates without manual FTP uploads.

Set up a repository

1. Go to **Advanced Features → Git**.
2. Select the domain and target directory.
3. Enter the repository URL (HTTPS or SSH).
4. Provide credentials or deploy keys if the repository is private.
5. Clone the repository.

Deploy updates

Use the pull or deploy action to fetch the latest commits. Some setups support webhooks for automatic deployment on push. Ensure your document root points to the correct subdirectory (for example `public` in Laravel apps).

DANUMHOST

ClamAV Antivirus Overview

Understand how ClamAV scans email and files for malware on your account.

ClamAV is an open-source antivirus engine integrated with DirectAdmin to scan incoming email and optionally uploaded files for malware.

Email scanning

When enabled by your host, ClamAV checks attachments and message content before delivery. Infected messages are typically quarantined or rejected with a notification to administrators.

Configuration

1. ClamAV settings are usually managed at server level by DanumHost.
2. Users may see scan results or quarantine options under **Advanced Features → ClamAV** if exposed.
3. Report false positives to support with the full message headers.

Best practices

Keep applications updated, avoid executing untrusted uploads, and combine ClamAV with SpamAssassin for layered email protection.

Downloaded from https://danumhost.co.uk/knowledgebase/category/advanced-features on 30-OCT-2026 10:01AM

DANUMHOST