Botanica Condominium

Email & OTP Login

Setup & Administration Guide

WordPress 6.9.1 — Botanica Condo Plugin v1.0

This guide covers:

- Configuring SMTP email delivery via WP Mail SMTP
- How the OTP resident login system works
- Adding and managing resident email accounts
- Testing and troubleshooting
- Security considerations

1. How the OTP Login System Works

The Botanica Condo Plugin uses a passwordless, email-based One-Time Password (OTP) system for resident logins. Residents never create a password — instead, they receive a fresh 6-digit code by email each time they want to log in. The code expires after a configurable number of minutes.

1.1 Login Flow — Step by Step

1	Resident visits the Resident Login page (/resident-login/) and enters their email address.
2	The plugin checks whether that email exists in the Allowed Residents list (wp_bc_allowed_emails table) and is marked active.
3	If found, the plugin generates a random 6-digit OTP. It bcrypt-hashes the code and stores the hash in the database. The plain code is emailed to the resident. It is never stored in plain text.

4	The resident is redirected to the Verify Code page (/verify-code/) and enters the 6-digit code from their email.
5	The plugin verifies the code against the stored hash. If correct and not expired, it creates a PHP session marking the resident as logged in, and redirects them to the page they originally requested (or the homepage).
6	The used token is marked as consumed and cannot be reused. Expired or used tokens are cleaned up automatically each night by a WordPress cron job.

NOTE The login page always displays a success message regardless of whether the email exists in the system. This prevents attackers from using the login page to enumerate valid resident email addresses.

1.2 What Requires a Login

The following content on the site requires a resident to be logged in to access:

- Notices marked "Residents Only" in the admin panel
- All Form downloads (PDFs, DOCX files, etc.)
- All Document downloads and PDF viewers (Bylaws, AGM Minutes, etc.)
- Maintenance articles marked "Residents Only"

Public content (notices not marked residents-only, the calendar, the contact form, and the homepage) is always visible without logging in.

1.3 Session Duration

After a successful OTP verification, the resident's session is maintained by PHP's native session system. The session persists until:

- The resident clicks "Log Out" in the navigation bar
- The browser session ends (browser is fully closed)
- The PHP session expires on the server (default: 24 minutes of inactivity, controlled by the server's php.ini session.gc_maxlifetime)

2. Configuring Email Delivery (SMTP)

WordPress's built-in email function (wp_mail) uses PHP's mail() by default. On most shared or VPS hosts, PHP mail() is either blocked, unreliable, or will be flagged as spam. You must configure an SMTP connection for OTP emails to be delivered reliably.

IMPORTANT If SMTP is not configured, residents will request a login code but never receive it. OTP login will appear broken even though the plugin is working correctly.

2.1 Install WP Mail SMTP

WP Mail SMTP is the recommended free plugin for SMTP configuration. To install:

1 Log in to the WordPress admin panel.

2 Go to Plugins → Add New Plugin.

3 Search for: WP Mail SMTP

4 Click Install Now on the plugin by WPForms, then click Activate.

5 Go to WP Mail SMTP → Settings in the left sidebar.

2.2 Choosing an Email Provider

WP Mail SMTP supports several email providers. The best option depends on your situation:

Setting	Example Value	Notes
`Gmail / Google Workspace`	Free (personal) or paid	Best for small volume. Requires a Google App Password if 2FA is enabled on your account.
`SendGrid`	Free up to 100/day	Reliable transactional email. Free tier is sufficient for a condo site.
`Mailgun`	Free up to 1,000/mo	Developer-friendly. Slightly more setup required.
`SMTP.com / Brevo`	Free tiers available	Good alternatives with simple setup.
`Your hosting SMTP`	Included with hosting	Many hosts (cPanel, Plesk) provide an SMTP server. Check your hosting control panel.

2.3 Configuring WP Mail SMTP with Gmail

Gmail is the most common choice for small sites. Follow these steps:

Step A — Create a Google App Password

1	Go to myaccount.google.com and sign in with the Gmail account you want to send from.
2	Click Security in the left sidebar.
3	Under "How you sign in to Google", ensure 2-Step Verification is turned ON. App Passwords require 2FA to be active.
4	Search for "App passwords" in the search bar at the top of the page, or go to myaccount.google.com/apppasswords.
5	Click Create. Give it a name like "Botanica Condo WordPress".
6	Google will show a 16-character password (e.g. abcd efgh ijkl mnop). Copy it immediately — it will not be shown again.

Step B — Enter Settings in WP Mail SMTP

In WordPress, go to WP Mail SMTP → Settings and fill in:

Setting	Example Value	Notes
`From Email`	no-reply@yourdomain.ca	The address residents will see in their inbox. Can be your Gmail address.
`From Name`	Botanica Condominium	Display name shown to residents.
`Mailer`	Other SMTP	Select this option (not the Google / Gmail API option).
`SMTP Host`	smtp.gmail.com	
`Encryption`	TLS	Select TLS (not SSL).
`SMTP Port`	587	Port 587 is standard for TLS.
`Authentication`	ON	Toggle the Authentication switch to on.
`SMTP Username`	your@gmail.com	Your full Gmail address.
`SMTP Password`	(16-char app password)	Paste the App Password from Step A. Include spaces or remove them — both work.

Click Save Settings once all fields are filled in.

2.4 Configuring with Hosting SMTP (cPanel)

If your Ubuntu server is behind a hosting control panel, or if you have access to a mail server, you can use those SMTP credentials instead:

Setting	Example Value	Notes
`SMTP Host`	mail.yourdomain.ca	Your hosting mail server hostname.
`Encryption`	TLS or SSL	Use TLS with port 587, or SSL with port 465.
`SMTP Port`	587 or 465	587 for TLS, 465 for SSL.
`Authentication`	ON	
`SMTP Username`	noreply@botcondo.ca	A real email account on your domain.
`SMTP Password`	(mailbox password)	The password for that email account.

2.5 Sending a Test Email

After saving your SMTP settings, always send a test email before going live:

1. In WordPress admin, go to WP Mail SMTP → Tools.
2. Click the Email Test tab.
3. Enter your own email address in the "Send To" field.
4. Click Send Email.
5. Check your inbox. You should receive a test message within a minute or two. Also check your spam/junk folder.
6. If the email arrives, SMTP is working correctly. If it does not arrive, review the error shown on screen and re-check your credentials.

3. Configuring OTP Settings

The OTP expiry time is configurable from the WordPress admin panel. To adjust it:

1. Log in to the WordPress admin panel.

2 Go to Settings → Botanica Condo.

3 Find the Security section.

4 Set "OTP Code Expiry (minutes)" to your preferred value. The default is 15 minutes.

5 Click Save Settings.

TIP A 15-minute expiry is a good balance between security and convenience. If residents frequently report expired codes, increase it to 20 or 30 minutes. Do not set it below 5 minutes.

3.1 OTP Security Details

For reference, here is how the OTP system protects resident accounts:

- The 6-digit code is generated using PHP's cryptographically secure random_int() function.
- The code is never stored in plain text. Only a bcrypt hash is stored in the database.
- Each token has a separate session reference ID (a 64-character hex string) stored in the PHP session, which is matched server-side during verification.
- Tokens are single-use. Once used, the used_at timestamp is set and the token cannot be used again.
- All previous unused tokens for an email are invalidated when a new login request is made.
- The login page never reveals whether an email address is registered (anti-enumeration).
- Sessions are regenerated on login to prevent session fixation attacks.

4. Managing Resident Email Accounts

Only email addresses in the Residents list can log in. The list is managed entirely from the WordPress admin panel — no database access is required.

4.1 Adding a Single Resident

1 Log in to WordPress admin.

2 Click Residents in the left sidebar.

3 Fill in the Add Resident form: Email (required), Name, Unit Number, and any Notes.

4 Click Add Resident. The resident will immediately be able to use the login page.

4.2 Bulk Import via CSV

To add many residents at once, prepare a CSV file with one resident per line in this format:

```
email,name,unit_number
jsmith@email.com,Jane Smith,412
rbrown@email.com,Robert Brown,205
lwilson@email.com,Laura Wilson,318
```

Important notes about the CSV format:

- No header row is needed — the first line should be data.
- The name and unit columns are optional but recommended.
- If an email already exists in the list, it will be updated (not duplicated).
- Save the file as .csv (plain text, UTF-8 encoding).

1 In WordPress admin, go to Residents.

2 Click the "Bulk Import via CSV" expandable section.

3 Click Choose File and select your .csv file.

4 Click Import CSV. A confirmation message will show how many residents were imported or updated.

4.3 Disabling and Re-enabling a Resident

If a resident moves out or you need to temporarily revoke access, you can disable their account without deleting it:

1 Go to Residents in the WordPress admin sidebar.

2 Find the resident in the table.

3 Click Disable next to their name. Their row will appear greyed out.

4 To restore access, click Enable. They can log in immediately.

NOTE Disabling a resident invalidates future login attempts but does not end any active session they currently have open. If you need to immediately end an active session, you would need to clear PHP sessions on the server.

4.4 Removing a Resident Permanently

To permanently remove a resident from the login list:

- Go to Residents and click Remove next to their name.
- Confirm the deletion when prompted.
- This action cannot be undone. Re-add them manually if needed.

5. Troubleshooting

5.1 Resident Not Receiving OTP Email

Symptom / Cause	Fix
SMTP not configured	Install WP Mail SMTP and configure credentials (see Section 2).
Email in spam/junk folder	Ask resident to check spam. Add the From email to their contacts.
Wrong email address in Residents list	Check the Residents list for typos. Email addresses are case-insensitive.
Resident email is disabled	Go to Residents and click Enable next to their name.
Gmail App Password not accepted	Ensure 2FA is ON in Google account. Regenerate the App Password and re-enter it.
SMTP port blocked by firewall	Try port 465 with SSL instead of 587 with TLS, or ask your host to unblock outbound SMTP.
Hosting blocks outbound email	Some VPS/cloud providers block port 25, 465, and 587. Use a third-party SMTP relay like SendGrid.

5.2 "Invalid or Expired Code" Error

- The most common cause is waiting too long. The default code expiry is 15 minutes.
- Each new login request invalidates the previous code. If the resident clicked "Send Login Code" twice, only the most recent code is valid.
- Check that the server clock is accurate. OTP expiry is time-based. Run sudo timedatectl on the server to verify the time zone and sync status.
- Ask the resident to copy-paste the code rather than typing it manually.

5.3 Login Page Redirects Back to Login

- This usually means the PHP session is not persisting. Verify that session_start() is not being called before WordPress boots (the plugin handles this at init priority 1).
- Check that the server has a writable PHP session directory: /var/lib/php/sessions/ on Ubuntu. Run sudo chmod 1733 /var/lib/php/sessions/ if permissions are wrong.
- On sites behind a reverse proxy (HAProxy), ensure the session cookie is being passed through. Check that the proxy is not stripping Cookie headers.

5.4 Checking Server-Side Email Logs

To verify whether WordPress is even attempting to send the email, install the WP Mail SMTP Email Log add-on or use the free plugin "WP Mail Log". Alternatively, check the server mail log:

```
sudo tail -f /var/log/mail.log
```

Look for entries from the time of the login attempt. A successful dispatch will show status=sent. Authentication errors will show connection refused or relay access denied.

6. Security Checklist

Before going live with resident logins, verify each of the following:

□ SSL/HTTPS is active on the site. OTP codes sent over plain HTTP can be intercepted. Activate a Let's Encrypt certificate via your hosting panel.

□ The WordPress admin URL (wp-admin) is protected. Consider IP-restricting it or adding a two-factor plugin for admin accounts.

□ The SMTP password in WP Mail SMTP is stored encrypted. WP Mail SMTP encrypts credentials by default.

□ WordPress and all plugins are kept up to date. Outdated plugins are the leading cause of WordPress compromises.

□ An automated backup is configured (UpdraftPlus recommended) with backups stored off-server.

□ The wp-content/uploads directory does not allow direct PHP execution. The Botanica Condo Plugin serves files via a proxy — verify uploaded files are not directly accessible by URL.

□ The OTP expiry is set to 15 minutes or less.

□ Unused admin accounts have been removed from WordPress.

End of Guide