Login with Code: Flexible Passcode-Based Authentication

Magic Login Pro · https://handyplugins.co/docs/magic-login-with-code/

With **Magic Login 2.4**, we introduced the `{{MAGIC_LOGIN_CODE}}` placeholder, allowing users to log in using a **passcode** instead of a login link. This feature improves the **login experience**, particularly for SMS-based authentication, where character limits and security concerns exist.

Unlike traditional OTPs, Magic Login Codes offer flexibility by allowing **multiple uses** (configurable with token validity settings) and **customizable formats** via filters.

How Magic Login Code Works

When `{{MAGIC_LOGIN_CODE}}` is detected in an **email or SMS message**, Magic Login:

1. **Generates a login code** dynamically based on the delivery method.
2. **Displays a code input form** instead of a login link on the login page.
3. **Validates the code** using:
    - **Token Validity Count** – Controls how many times a code can be used.
    - **TTL (Time-to-Live)** – Defines how long a code remains valid.

Token Validity and TTL are not new features—they have always been part of Magic Login. The key enhancement in **2.4** is that the login method **automatically adapts** when `{{MAGIC_LOGIN_CODE}}` is used in templates.

Code Generation: Context-Aware Passcodes

The **default format** of login codes depends on the delivery method:

Context	Code Format	Example
SMS	6-digit PIN	`854321`

Context	Code Format	Example
Email	10-character alphanumeric (uppercase, no confusing characters)	`XK5T7P1M9Q`

For SMS – A **6-digit PIN** is used for easy entry.

For Email – An **10-character alphanumeric code** improves security.

How to Use Magic Login Code in SMS & Email

To enable **code-based login**, add `{{MAGIC_LOGIN_CODE}}` to your **SMS or email content**.

Example: SMS Content

```
Your login code: {{MAGIC_LOGIN_CODE}}. Enter it on the website to log in.
```

Example: Email Content

```
Use this passcode to log in: {{MAGIC_LOGIN_CODE}}. Or follow the link {MAGIC_LINK}}
```

If the template contains `{{MAGIC_LOGIN_CODE}}`, Magic Login **automatically switches** to code-based authentication, displaying a **code input form** instead of a login link. However, you can also use the link together too. It's not blocking the links.

Customizing Login Codes with Filters

While Magic Login provides a **default** login code format, you can **fully customize** it using the `magic_login_create_user_token` filter.

Modify SMS Code Length

If you want to **send a 10-character code** instead of a 6-digit PIN for SMS:

```
add_filter( 'magic_login_create_user_token', function( $new_token, $user_id, $context ) {
    if ( $context === 'sms_code' ) {
        return wp_rand( 1000000000, 9999999999 ); // 10-digit numeric code
    }
    return $new_token;
}, 10, 3 );
```

Increase Email Code Complexity

```
add_filter( 'magic_login_create_user_token', function( $new_token, $user_id, $context ) {
    if ( $context === 'email_code' ) {
        return strtoupper( substr( str_shuffle( 'ABCDEFGHJKLMNPQRSTUVWXYZ23456789!@#$%&*' ), 0, 12
) );
    }
    return $new_token;
}, 10, 3 );
```

Why Use Login Codes Instead of Links?

While **login links** are convenient, **Magic Login Codes** provide several benefits:

Shorter SMS Messages – Login links can exceed **300-character SMS limits**, while a **6-digit code is compact**.
More Secure for SMS – Links in SMS can be **phishing risks**, whereas a **PIN code minimizes this concern**.
Easier to Enter – Users can **memorize** a short PIN and type it quickly.
Works with Email – Users can receive either a **login link or passcode**, based on preferences.
Multi-use flexibility – Unlike OTPs, Magic Login Codes **can allow multiple uses** if configured.

Security Considerations & Best Practices

Since **SMS-based authentication** has security risks (e.g., **SIM swapping, interception**), we recommend:

Short Token TTL (Time-to-Live) – Reduce expiration time to **minimize attack windows**.
Enable Rate-Limiting – Prevent brute-force attempts by limiting login attempts per phone number.
Use Multi-Factor Authentication (MFA) – Add extra security for sensitive accounts.
Use Token Validity Count – Limit how many times a code can be used within a session.
Customize Codes with Filters – Adjust complexity and length as needed.

Final Thoughts

Magic Login 2.4 introduces **Magic Login Codes**, giving users a **flexible, secure, and efficient** way to authenticate without relying on long login links. By leveraging **context-aware code generation,**

TTL, validity limits, and filters, site owners can **fully customize the login experience** while keeping security in check.