

Access Control 101 in Wild Apricot: How the System Decides What People Can See and Do

Santa Barbara Newcomers Club – Tech Chair Reference Guide

Last updated: December 2025

I. Introduction: What Is Access Control in Wild Apricot?

When someone visits the SBNC website or logs into the Wild Apricot admin dashboard, Wild Apricot must decide:

“Who is this person? What should they be allowed to see, do, or change?”

This is governed by **access control**, which is a set of built-in tools that determine:

- Which pages or events someone can **view**
- Which features they can **edit or administer**
- Which files, directories, and member data they can **access**

Unlike modern platforms with role-based or record-level permissions, **Wild Apricot uses a simpler, page- and module-based permission model**. It’s effective but limited, and understanding how it works is essential to protecting member privacy, data integrity, and club operations.

II. The 5 Access Control Mechanisms in WA

| Mechanism | What It Controls | Who It Affects |
|-----------------------------|----------------------------------------------------------------------|-----------------------------|
| 1. Login State | Whether a visitor is considered “public” or “logged-in” | Everyone |
| 2. Membership Level | What type of member someone is (Newbie, Newcomer, etc.) | Members |
| 3. Membership Status | Whether a member is Active, Lapsed, Pending, etc. | Members |
| 4. Groups | Ad hoc lists of members for segmentation (e.g., Event Chairs, Board) | Members |
| 5. Admin Role | Whether someone is an Admin and what they can administer | Admins only (board, chairs) |

Each of these can **restrict or allow access** to content — but they affect different parts of the system.

III. What Happens When Someone Visits sbnewcomers.org?

1. Public Visitor (Not Logged In)

- Sees only pages marked “**Anyone can access**”
- Cannot register for members-only events
- Cannot see the member directory or hidden photo galleries

2. Logged-In Contact Without Membership Level

- May see custom content if added to a group (e.g., event volunteers)
- Still blocked from member-only areas unless explicitly granted access

3. Logged-In Member

- Sees content and events based on:
 - Their **membership level** (e.g., Extended Newcomer)

- Their **group membership** (e.g., Board, Event Chairs)
- Whether the page/event is restricted to their group/level

4. Admin (Restricted or Full)

- Access to the **Admin Dashboard**
 - Modules and actions depend on their **Admin Role** and assigned permissions
-

IV. Mechanism Breakdown: What Each Can and Cannot Do

1. Login State

- Pages and events can be marked as:
 - Public (Anyone)
 - Members Only
- File downloads and photo galleries can also be hidden from public users

2. Membership Level

- Used to:
 - Show different pricing or registration access for events
 - Restrict access to certain pages
 - Include/exclude members from directories

3. Membership Status

- Active members can:
 - Register for events
 - Access member-only areas
- Lapsed or suspended members are typically blocked from participation

4. Groups

- Used to:
 - Restrict access to pages (e.g., Board-only documents)

- Target emails (e.g., Hike Chairs)
- Allow registrations for restricted events
- **Groups do not** grant admin permissions

5. Admin Roles

- Three types:
 - **Full Admin** – All access
 - **Restricted Admin** – Assigned by module and optionally by event category
 - **Read-Only Admin** – See everything, edit nothing

Admins can be allowed to:

- Manage events (by category)
- Send emails (all or just to groups)
- Access finances or membership details

V. Why and How SBNC Uses Admin Roles

We use **Admin Roles** to delegate key responsibilities to board members and volunteers without exposing the full system.

| Admin Role | Who Gets It | What It Allows Them To Do |
|-------------------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Full Admin | VP of Technology, President | Full site and data access; used for platform maintenance and emergency control |
| Restricted Admin | VP Activities, Treasurer, Event Chairs, Posting, Communications | Limits access to specific modules (Events, Finance, Website, etc.), allowing division of labor and reduced risk |
| Read-Only Admin | Rare (audit use only) | Allows oversight without risk of accidental edits |

Why we use them:

- Prevent accidental deletion or data exposure

- Match permissions to roles and responsibilities
 - Allow volunteer Event Chairs to manage their own events without seeing club-wide data
-

VI. How SBNC Uses These Controls Today

| Goal | Mechanism Used |
|---------------------------------------------------|------------------------------------------|
| Hide pages and albums from public | Page access + Login state |
| Show special pricing for certain members | Membership level |
| Restrict event editing to certain chairs | Admin Role + Event Category (planned) |
| Let Board Members access Admin tools | Admin Role |
| Give registrant lists to Event Chairs | Group-based communication |
| Allow only Extended Newcomers into certain events | Membership level or group |

VII. Gaps and Vulnerabilities in Our Setup

1. We do not currently use Event Categories

- As a result, Restricted Admins may have access to **all events**, not just their own
- This exposes us to accidental edits or deletions by untrained volunteers

2. We grant too many Full Admin privileges

- Full Admins can delete any data, change any setting, and access all financials
- This is risky in an environment with frequent role turnover and minimal training

3. There's no audit trail

- WA does not log changes made by Restricted Admins
- Accidental or malicious edits are hard to trace

4. Passwords may be shared

- Volunteers sometimes reuse or hand off credentials, exposing the system to phishing or breach

5. Tagging is misunderstood

- Some admins think contact tags restrict access — they don't
- This false belief can lead to misconfigured security

VIII. How to Better Align Controls with Board and Chair Needs

| Board/Chair Need | Recommended Configuration |
|-------------------------------------------|------------------------------------------------------|
| Event Chairs only manage their own events | Use Event Categories + Restricted Admin roles |
| Board access to documents & pages | Use Groups + Page access restrictions |
| Posting volunteers draft events only | Restricted Admin + no finance/membership modules |
| Treasurer sees only financials | Restricted Admin + Finance module only |
| Committee-only pages | Restrict pages by Group |
| Custom event invitations | Email to Groups |

IX. Proposal: Reducing Vulnerabilities

To protect member data and streamline operations, we recommend:

1. Implement and use Event Categories

- Define categories for Hikes, Social, Wine & Dine, etc.
- Limit each admin to only the category they manage

2. Audit and minimize Full Admins

- Only the VP of Technology and President should retain Full Admin rights

- Use Restricted Admin roles for everyone else

3. Avoid credential sharing

- Use individual admin accounts and enforce password discipline

4. Train all new admins

- Provide onboarding materials explaining what their permissions allow

5. Document every permission

- Keep an updated admin matrix (who has access to what)

6. Quarterly access review

- Remove or reassign access as roles change
-

X. Conclusion

By tightening our access controls and documenting our use of Wild Apricot's tools, we can better support the board, protect our members, and reduce costly administrative errors.

Prepared for: SBNC Board, VP Technology, Incoming Tech Chairs

Prepared by: Ed Forman with documentation support from ChatGPT