PH7X SYSTEMS®

0.0.0 · CHAPTER 13

Permissions

SharePoint Migration Field Guide · Chapter 13

pH7x Systems

2026-08-08

13. Permissions

> Here, permissions are not security. They are migration evidence.

A permissions review normally asks whether access is correct. That is a real question and it is not this one. This chapter reads the same information for a different purpose:

> **Who can access what, and what does that tell you about the work you are about to do?**

Chapter 2 counted the estate. This chapter reads five specific facts about it, and turns them into an estimate of how much of your project is permission work, how much of that sits on the critical path, and which parts have to be decided before a wave plan means anything.

The five facts are each a short technical answer, and the Knowledge articles behind this book give the commands that produce them. What none of them gives you is the reading of all five together, which is the only thing that changes a plan.

Five readings, and what each one is evidence of

WHAT YOU READ	WHAT IT IS EVIDENCE OF
Who administers each site	whether a wave has anyone who can accept it
Where inheritance is broken	how much of the estate cannot be moved as a block
Which sites are group-connected	whether membership lives in SharePoint at all
The sharing capability of each site	what the destination will allow you to reproduce
The default sharing link type	what your users will produce after the move

Read down that right-hand column and the shape of the chapter appears. Not one of those is about whether access is correct. Every one of them changes the calendar, the scope, or who has to agree.

Administrators are the wave plan

Chapter 1 asked you to name validators, and said that a wave with no named validator passes on silence. This is where that abstraction becomes a list.

A site with no human administrator has nobody who can accept its content after a move. A site whose only administrator is a service account, a departed employee, or a group nobody maintains has the same problem wearing a name. **We recommend treating the administrator list as the first draft of your wave plan**, because the sites that cannot be accepted are the sites that will hold the project open at the end.

Two of our governance rules read this fact, and both are `convention` rather than documented requirement: a site should have at least two owners, and at least one administrator who is a person. Microsoft publishes no such requirement, and we say so in the rules. The reason is operational rather than technical: one owner is one holiday away from nobody, and a group with no human in it accepts nothing.

The migration consequence is not "fix the owners". It is that **every site without a reachable human owner is a site whose validation has no date**, and a project plan that assigns those sites to week six is a plan that finds out in week six.

Broken inheritance is the unit of work

Inheritance is the mechanism that lets a site move as one thing. Where it is intact, permissions travel as a block. Where it is broken, each break is a decision, and decisions do not parallelise.

There are three numbers here, and they are not the same kind of number.

100,000 items. Once a list or library passes this, you can no longer break or reinherit permission inheritance on it at all (SharePoint limits, manage permission scopes, checked on 5 August 2026). This is a hard limit at the destination, and chapter 3 already treated it as one: it does not make the migration expensive, it removes an option for that library.

50,000 unique permission scopes. The documented ceiling per list or library (same sources, checked on 6 August 2026). A library above it is not a costing problem; it is a library that cannot arrive intact.

5,000 unique permission scopes. Microsoft's guidance rather than a limit: past this the list still works and performance degrades. It is the number that tells you a library needs redesign rather than a copy.

Notice the pattern, because it is the reason this chapter exists. The same property, counted, means three different things at three different values: *redesign this*, *this cannot arrive*, *this cannot be changed at the destination*. A report that prints "unique permissions: 61,204" and stops has told you nothing about your project.

We recommend counting scopes per library and sorting descending, because the distribution matters more than the total. Sixty thousand scopes spread over four hundred libraries is a tidy estate with one bad habit. Sixty thousand in one library is a rebuild, and it is on the critical path.

Group-connected sites move their membership elsewhere

A site connected to a Microsoft 365 group does not hold its own membership. Owners and members live on the group, and the site follows.

For a migration this is good news and a trap in the same fact. Good news, because membership travels with the group rather than being rebuilt. A trap, because a permissions inventory that reads only the site will report those sites as having fewer administrators than they do, and because anything granted **directly on the site**, outside the group, is invisible to whoever is looking at the group and will not travel with it.

The reading is: for each site, is membership in SharePoint or in the group, and does the site carry direct grants on top? A site with both has two sources of truth, and reproducing it at the destination means reproducing both.

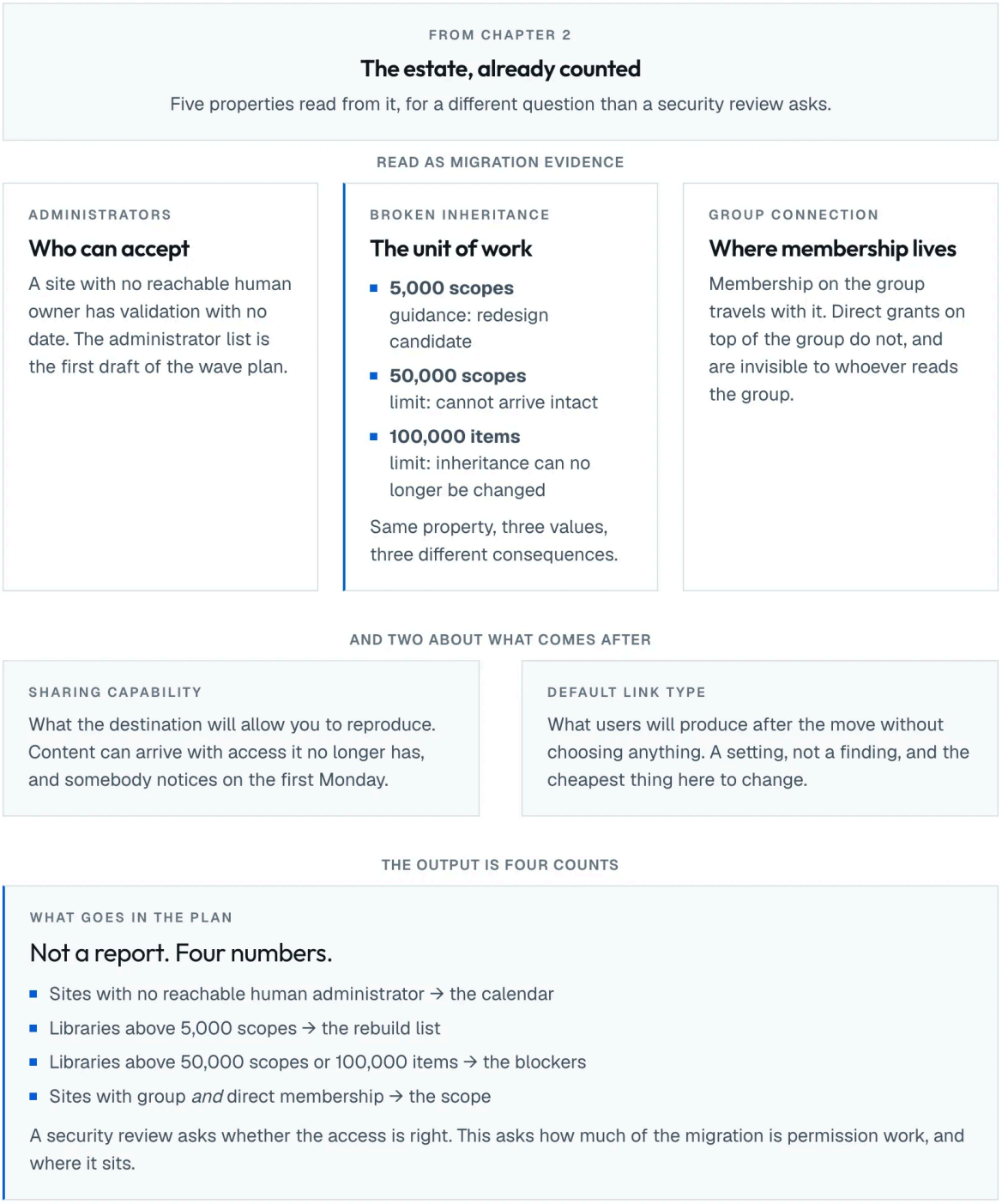

Figure 13.1. The same five facts, read as migration evidence rather than as a security review.

Sharing tells you what the destination will allow

The two sharing facts are about the future rather than the present.

Sharing capability is what the site permits: which kinds of external sharing are possible at all. It bounds what you can reproduce. A site that today shares with anonymous links, moving to a destination or a tenant configuration that forbids them, has content that will arrive with access it no longer

has, and somebody will notice on the first Monday.

The default sharing link type is what your users will produce after the move without choosing anything. It is a setting, not a finding, and it is the cheapest thing in this chapter to change. Our rule on it is `documented-guidance`, and the guidance is Microsoft's own: they wrote a page about how to set it to something more restrictive while still allowing users to choose otherwise.

Both belong in the migration record for the same reason: they are the two places where a migration silently changes what people can do, without anybody deciding that it should.

Turning five facts into an estimate

The output of this chapter is not a permissions report. It is four numbers you can put in a plan:

```
Sites with no reachable human administrator      → validation with no owner
Libraries above 5,000 scopes                     → redesign candidates
Libraries above 50,000 scopes, or 100,000 items  → cannot arrive as they are
Sites with both group and direct membership      → two sources to reproduce
```

Each line is a count, each count came from a documented property, and each one changes a different part of the project: the calendar, the scope, the blockers, and the rebuild list respectively.

That is the difference between this chapter and a permissions audit. An audit asks whether the access is right. **This asks how much of your migration is permission work, and where it sits.** The first question is important and belongs to whoever owns governance. The second one belongs to whoever owns the date.

When a permissions review misleads

It reports totals instead of distributions. One number for the tenant hides the one library that is the whole problem.

It treats every broken inheritance as equal. Three thresholds, three different consequences, and only one of them is a hard limit.

It reads sites and ignores groups. Group-connected sites report fewer administrators than they have, and their direct grants go unread.

It confuses a setting with a finding. The default sharing link type is a choice somebody can make this afternoon. Counting it alongside a library that cannot be moved gives them the same weight, and they do not have the same weight.

It answers the security question. Whether access is correct is a real and separate piece of work. Answering it here produces a document that is too long for the plan and too shallow for governance, and satisfies neither.

Out of scope

Whether the current access is correct. That is a governance review, with a different audience and a different definition of done. It uses the same five readings and asks a different question of them.

Designing permissions at the destination. How the target environment should be structured is chapter 6, governance before technology, and it decides a stance rather than reading an estate.

Remediating what you find. This chapter produces counts and consequences. Turning those into work, and that work into money, is chapter 5.

How to read each property. The commands, their output and their limits live in the Knowledge articles, which carry the version they were tested against. Repeating them here would create a second answer that ages separately.

Before you continue

- [ ] Every site has a named administrator who is a person and is reachable
- [ ] Sites with no reachable human owner are listed, and none of them is scheduled as though it had one
- [ ] Unique permission scopes are counted per library and sorted, not totalled
- [ ] Libraries above 5,000 scopes are marked for redesign, and those above 50,000 scopes or 100,000 items are marked as unable to arrive as they are
- [ ] Group-connected sites are identified, and any direct grants on top of the group are recorded separately
- [ ] The sharing capability and the default link type of each site are recorded as they are today
- [ ] The four counts are in the plan, each against the part of the project it changes

The commands behind each of these readings are in the Knowledge, with the PnP.PowerShell version they were tested against. This chapter is what to do with the five answers together.

---

pH7x Systems. Chapter 13 of the SharePoint Migration Field Guide, published 8 August 2026 at ph7x.com/guide. The guide is being written one chapter at a time; the chapters that exist are listed there.