

PH7X SYSTEMS ®

1.0.0 · CHAPTER 6

Write down what each hybrid feature sends across the boundary, as whom, and who checks it

Hybrid Architecture Field Guide · Chapter 6

pH7x Systems

2026-11-13

6. Write down what each hybrid feature sends across the boundary, as whom, and who checks it

> The trust says which farm is calling. It gives no person anything: what a user gets back is decided by permissions on the side that answers.

Each hybrid feature opens the boundary between your farm and Microsoft's service differently. One sends a browser elsewhere, one pulls a term store in, one pushes out what a crawler gathers. Microsoft documents them on separate pages and assesses none of them together.

> **For each hybrid feature this estate runs, what leaves the farm, in which direction, authenticated as what, and who owns the control that limits it?**

The decision this chapter leads to is a signed security assessment of the planned hybrid configuration: each feature accepted, restricted or refused on what it exposes, with a control, an owner and evidence for every boundary it opens.

What this chapter settles

It settles what each feature sends and receives, what the trust grants, what cloud hybrid search places in the Microsoft 365 index and where, which operations need a privileged identity, and what can be audited. It ends in a control matrix.

It takes the feature list from Chapter 1, the trust, its certificates and its accounts from Chapter 2, and the search architecture from Chapter 3. It hands Chapter 7 the controls to run and Chapter 8 what stays behind on exit. It leaves out the security of SharePoint Online itself, Conditional Access and any mapping to a standard.

Applies to

FACT	SHAREPOINT SERVER 2016	SHAREPOINT SERVER 2019	SUBSCRIPTION EDITION
Product support	Ended 14 July 2026	Ended 14 July 2026	In support, one public update at a time (Chapter 1)
Cloud hybrid search, so index entries outside the network	Removed	Removed	July 2025 public update or later (Chapter 3)
Hybrid auditing (preview)	Ended with the November 2019 public update	Never applied	Never applied
Certificate management and its health rules	No	No	Yes
TLS 1.3, and strong TLS by default	No	No	On Windows Server 2022; not on earlier versions

Sources: BCS retirement, which gives "end of support date of July 14, 2026" for 2016 and 2019, hybrid auditing, SSL certificate management and TLS 1.3 support, all checked on 13 November 2026.

Architecture

Trust boundaries, feature by feature

FEATURE	WHAT CROSSES, AND WHICH WAY	AUTHENTICATED AS	WHAT STAYS ON THE FARM
Hybrid OneDrive, with profiles	The person's browser is redirected to Microsoft 365. New personal files are then stored "in the cloud"	The person. No server call is documented	Existing files and profiles; the on-premises services, still "accessible by users if they've bookmarked the URL"
Hybrid sites features	Farm to Microsoft 365: a site followed on the farm is "added to the followed list in both". Microsoft 365 to farm: app launcher tiles	Not stated. The feature requires the server-to-server trust	Existing followed lists; following people, which "remains in SharePoint Server only"
Hybrid self-service site creation	The browser of a member of the hybrid audience is redirected to group creation in Microsoft 365	The person	Site creation for "on-premises only users"
Hybrid taxonomy and content types	Microsoft 365 to farm, daily: a farm timer job polls for changes. Farm to Microsoft 365, once: a copy an administrator runs	Replication: "The SharePoint in Microsoft 365 APP Identity is used to authenticate to Microsoft 365". Copy: the credential supplied	Local term sets; farm edits, which "will not replicate"
Cloud hybrid search	Farm to Microsoft 365: what the crawler gathers for each item, with its access control list	The feed: not established since the 2025 change (Chapter 3). Onboarding: a Global Administrator	The documents
Outbound federated search	Farm to Microsoft 365: the query. Results return to the farm's Search Center	The farm, under the trust, which lets it "pass user claims to SharePoint in Microsoft 365 using OAuth"	The farm's index and every item in it

Sources for the table: plan hybrid OneDrive, hybrid sites and search, hybrid site following, hybrid self-service site creation, plan hybrid taxonomy, configure hybrid taxonomy, learn about cloud hybrid search and plan server-to-server authentication, all checked on 13 November 2026.

Every remaining call starts on the farm. Three boundaries are closed, because the feature behind each is retired:

- **Inbound federated search**, where Microsoft 365 queried the farm, "has been retired as of September 2024" (hybrid search, checked on 13 November 2026).
- **Hybrid Business Connectivity Services**: "Business Connectivity Services hybrid solutions" were retired in Microsoft 365 from 30 September 2024 (BCS retirement).
- **Hybrid auditing**, which sent farm audit records out: see Auditability, below.

One inbound path remains, and it is optional. With cloud hybrid search, people outside the network open an on-premises result over VPN, or "you enable users to open such links by installing a reverse proxy device for SharePoint Server" (configure cloud hybrid search, checked on 13 November 2026). That is people reaching the farm, not Microsoft 365 reaching it.

Authentication is not authorisation

The trust authenticates a server. Microsoft lists two separate checks, "Verify that the requesting server is trusted" and "Verify that the type of access that the server is requesting is authorized", and says the protocol "is separate from user authentication and is not used as a sign-in authentication protocol by SharePoint users" (plan for server-to-server authentication in SharePoint Server, checked on 13 November 2026). Building it adds no permission for anybody. What a person may see stays with each side's own permissions.

Cloud hybrid search. The farm's permissions travel with each item: "The Microsoft 365 search index stores the ACLs together with the item" (plan cloud hybrid search, checked on 13 November 2026), and "Search results are security trimmed based on the user's Microsoft 365 identity" (learn about cloud hybrid search). Chapter 3 has the mapping. Four consequences matter here:

- **Default security groups.** A member of Domain Users gets no on-premises results, because directory synchronisation excludes groups with "IsCriticalSecurityObject=true". Grant through "the Everyone group, the Authenticated Users group, or a custom group" (plan cloud hybrid search).
- **Broad grants.** `NT AUTHORITY\Authenticated Users` and `Everyone` "are translated to" the tenant's "Everyone except external users" (cloud hybrid search FAQ, checked on 13 November 2026). Read who that group contains in your tenant before the first crawl.
- **SAML.** "Items secured with SAML claims when crawled using Cloud Search Service application will not show up in search results", "by design" (FAQ). Microsoft's workaround, adding the Everyone claim, widens access: we would not use it without the content owner's signature.
- **Custom trimming** "isn't available with cloud hybrid search" (learn about cloud hybrid search). Content that a custom trimmer protects on the farm must not be crawled by the cloud Search service application.

A permission change reaches the index as a "Security update", which "Overwrites an existing document's access control list" (FAQ), sent by the crawler. Microsoft gives no interval. We do not know how long a user removed on the farm still finds the item in Microsoft 365: remove a test user from a test item, crawl, and time it.

For OpenID Connect identities the FAQ says nothing. We do not know how such items are trimmed: query as a user whose only access is through an OpenID Connect claim.

Outbound federated search. Nothing from the farm is indexed outside it. SharePoint in Microsoft 365 answers the query for a federated user "who has permissions to view the root site collection in SharePoint in Microsoft 365" (display federated results in SharePoint Server, checked on 13 November 2026). The only sentence that describes trimming in federated search concerns the retired inbound direction, where the farm "security trims the search results in the context of the user

who sent the search request" (configure a reverse proxy device, checked on 13 November 2026). For outbound, Microsoft documents that user claims are passed, and no more. We would prove it with two federated users who hold different permissions on one tenant site.

What is exposed outside the farm

The index. Microsoft describes it two ways. The overview: "It's the metadata for the content that's indexed, and this metadata is encrypted when it's transferred to the search index in Office 365, so the on-premises content remains secure" (learn about cloud hybrid search). The FAQ: the "Crawler sends the encrypted content to the Indexing API", and an Insert "Creates or overwrites a document's content and access control list". Neither says whether the text extracted from a document is "metadata". We would plan on the FAQ's word, content: it describes the operations, not the intent, and a wrong guess costs least that way. For content that "shouldn't be indexed outside your on-premises network", Microsoft recommends "a combination of cloud hybrid search and hybrid federated search" (hybrid search).

The taxonomy copy. `Copy-SPTaxonomyGroups` sends the term groups you name, "maintaining the IDs of the terms, term sets, and term groups", with "most user information associated with term sets - such as owner and stakeholders" (plan hybrid taxonomy, configure hybrid taxonomy). It is final: "Once a Taxonomy Group is copied, it cannot be re-copied" (Copy-SPTaxonomyGroups, checked on 13 November 2026). Read the term labels for anything confidential first; Chapter 5 has the procedure.

OneDrive. Redirection sends new personal files to Microsoft 365 by design. It moves nothing, and it is not a control: the on-premises OneDrive stays reachable by bookmark (Chapter 4).

Data residency

Microsoft's hybrid pages say what goes to Microsoft 365. They do not say where it is held. No page we read names a geography or a data centre for on-premises items in the index, copied term groups or followed sites, or says how long an item remains after its feature is switched off. Where a tenant's search index is held is a question for the tenant's own data location documentation and your contract with Microsoft. We do not know the answer, and no farm test settles it: get it in writing before content with a residency requirement is crawled.

Auditability

Hybrid auditing is gone. "Microsoft has ended support for the SharePoint Hybrid Auditing (Preview)", which applied to 2016 only: "It is no longer available in SharePoint Server 2016 as of the November 2019 Public Update", and "it has been disabled in the Microsoft 365 service. Existing data is available in the Unified Audit Log but no new data can be sent from SharePoint Server to the Unified Audit Log" (hybrid auditing). No hybrid feature now joins the two audit trails, and what each side's own audit records is outside the hybrid documentation.

Not established: whether a federated query, a crawl feed, a replication run or the wizard's changes appear in either side's audit log. We do not know. Run each once in a test environment at a known minute and search both logs for it.

Azure ACS after 2 April 2026

The trust's proxy and token issuer are named "ACS" and point at an ACS-hosted endpoint (Chapter 2). Azure ACS authentication for SharePoint Online "was retired on April 2, 2026", and the same page says: "SharePoint Server running on-premises can, if configured by the farm admins, depend on Azure ACS for hybrid scenarios (e.g. hybrid search) and low trust auth for custom applications. The retirement of Azure ACS however is not impacting any of the SharePoint on-premises use cases and no action is required from SharePoint on-premises farm admins." (Azure ACS retirement, checked on 13 November 2026).

That statement does not cover the mechanism by which the on-premises dependency continues, how long it will, whether the cloud hybrid search service introduced in 2025 uses it, or high-trust add-ins by name. We would record the dependency as a risk with an owner, and read that page again at every public update.

Prerequisites

- Chapter 1's decision record, Chapter 2's Identity and Trust Matrix with its Certificate Register, and Chapter 3's search decision.
- A list of how access is granted on the content to be crawled: Everyone, Authenticated Users, Domain Users, SAML or OpenID Connect claims, custom trimmers.
- A named owner for the farm, the tenant and the content.

Decision criteria

Accept a feature when what it sends is written down and each control that applies has an owner. Otherwise:

IF THIS IS TRUE	THEN
Content has a residency requirement and the tenant's data location is not confirmed in writing	Keep it out of the cloud Search service application's content sources
Access is granted through SAML claims or a custom trimmer	Not cloud hybrid search for that content
Access is granted to Everyone or Authenticated Users	Crawl only after the content owner accepts "Everyone except external users"
A reverse proxy and its public certificate exist only for inbound search or hybrid BCS	We would retire them: nothing documented still calls the farm
People must open on-premises results from outside	VPN, or a reverse proxy assessed as what it is, the publication of the farm to people
Nobody will hold Global Administrator for the session, under record	Stop: Microsoft documents no lesser role

Procedure

Microsoft documents no security assessment for hybrid. This is the order we would follow, before the wizard runs or before the next change to an existing trust.

1. List the features, and strike any that depends on a retired boundary.
2. For each, copy its row from the trust boundary table and make it specific: which web application, content sources, term groups and audience.
3. Classify the content each feature touches, record how access to it is granted, and write the content sources and crawl rules that exclude what must stay.
4. Put the residency question to the tenant's owner and to Microsoft, in writing.
5. List every privileged operation (Security, below) with the person, the account and the window.
6. Confirm an owner and an end date for each entry in the certificate register, then fill the control matrix: one owner and one piece of evidence per row.
7. Run the tests in Verify on a test farm, and record what is still unknown as unknown.
8. Have the owners of the farm, the tenant and the content sign.

Verify

Some of these checks are documented. The rest are tests you run with your own accounts: ours, not Microsoft procedures.

WHAT	HOW	EXPECTED
The trust	Documented: Chapter 2's checks	Realm equals the tenant's ID; one service principal name carries your domain
The cloud index	Documented: the `IsExternalContent:true` query (Chapter 3)	Only content from the sources you chose
Trimming, cloud hybrid search	Test: the query as a user with access and as one without	The second sees nothing on-premises
Permission removal	Test: remove a user from an item, crawl, query	The item disappears; record how long it took
Trimming, federated search	Test: two federated users with different permissions on a tenant site	Each sees only what their permissions allow
Results from outside	Test: open an on-premises result off the network, without VPN	It does not open, unless you published the farm

When it fails

WHAT YOU SEE	DOCUMENTED CAUSE	WHAT TO LOOK AT
People find nothing on-premises in Microsoft 365	Access through Domain Users, or an account that is not synchronised	The item's ACL; Chapter 2
Items secured by a trusted provider never appear	SAML claims cannot be mapped, "by design"	Whether that content belongs in cloud hybrid search
An item is found by people who should not find it	None documented	A broad grant, or a custom trimmer that does not apply; fix the grant on the farm and crawl
Hybrid stops after the STS certificate is replaced	A hybrid farm needs "additional steps required to upload the STS certificate to Azure"	The certificate on the tenant's principal; Chapter 2

Security

Certificates and TLS

The trust is signed by the farm's STS certificate. "The default STS certificate does not need to be re-newed. Renewal only applies after the STS certificate has been replaced." A replacement needs "2048 bit encryption or higher", a maintenance window and every server, and will "expire within 1 to 3 years" (replace the STS certificate, checked on 13 November 2026). The upload to the tenant that must follow is where the documentation has a gap: Chapter 2 has the procedure. We would keep the built-in certificate.

Subscription Edition's certificate management covers "the lifecycle of SSL certificates in your SharePoint farm" (SSL certificate management), with four health rules that warn weekly from 60 days before expiry and daily from 15 (health analyzer rules, checked on 13 November 2026). Microsoft does not say they cover the STS certificate, and documents no health rule for the trust, so Chapter 7 watches both by hand.

Subscription Edition "by default supports TLS 1.3 when deployed with Windows Server 2022", and TLS 1.3 "isn't available and isn't supported" on earlier versions of Windows Server (TLS 1.3 support). There its SSL bindings also require that "The SSL/TLS protocol version negotiated must be TLS 1.2 or higher", with cipher suites that "support forward secrecy", unless somebody has set "Allow Legacy Encryption" (strong TLS encryption, checked on 13 November 2026). Both rules protect connections made to the farm; neither page mentions the farm's own calls to Microsoft 365 (Chapters 1 and 3).

Service identities and privileged operations

OPERATION	IDENTITY MICROSOFT NAMES	NOT ESTABLISHED
The Hybrid Configuration Wizard	A farm administrator, and "A Microsoft 365 Global Admin, either with or without multi-factor authentication (MFA) enabled", on a farm server	Any lesser role
Cloud hybrid search onboarding	"Global Administrator or above", on a farm server; "Accept the requested permissions."	What the consent grants, and to what
The taxonomy copy	"Your Microsoft 365 global admin credentials" on one page; on the cmdlet's page, "a Term Store Administrator's credential is needed"	Which is enough
Taxonomy replication	The timer service account, which "must be a term store admin in SharePoint Server"; the app identity towards Microsoft 365	What that identity may do in the tenant
The crawl	A default content access account with "at least read access to the content to crawl"	Nothing: scope it yourself

Sources: Hybrid Configuration Wizard, checked on 13 November 2026; configure cloud hybrid search, configure hybrid taxonomy and Copy-SPTaxonomyGroups. Chapter 2 lists the accounts in full.

The wizard's page asks for a Global Administrator and also says: "Global Administrator is a highly privileged role that should be limited to emergency scenarios when you can't use an existing role." No lesser role is documented for the wizard or the onboarding, and the sign-in happens on a farm server. These are recommendations, not Microsoft's procedure:

- We would use a named account with multi-factor authentication, given the role for the session and removed from it the same day.
- We would run the session on a server at the current public update (security updates), with nobody else signed in.

- We would capture the consent screen before accepting it, since Microsoft does not print what it grants.
- We would give the content access account read access to the chosen content sources and nothing else.

Governance control matrix

The frequencies are ours. Nothing in this table is a claim of conformity to anything.

CONTROL	WHAT IT PREVENTS	OWNER	EVIDENCE	WE WOULD CHECK
Feature register, each feature with its need	A trust nobody remembers	Farm owner	The signed decision record	Yearly, and at every change
Content sources reviewed against classification	Content indexed outside the network that should not be	Content owner	The signed list of sources	Before each new source
Review of broad grants on crawled content	Items open to all internal users in Microsoft 365	Content owner	Permission report for Everyone and Authenticated Users	Before the first crawl; quarterly
Trimming test with two accounts	Results shown to the wrong person	Search owner	Dated test result	After each public update
Global Administrator for the session only, consent captured	A standing privileged account; permissions nobody can name	Tenant owner	Role assignments before and after; the captured screen	At each run
Certificate register	A trust that stops at an expiry	Farm owner	End dates on the farm and on the tenant's principal	Monthly
Term store changes made in Microsoft 365 only	Farm edits overwritten at the next replication	Taxonomy owner	Term store administrators on both sides	Quarterly
Azure ACS dependency recorded	A retirement that arrives unread	Farm owner	The retirement page, read and dated	At each public update
Residency answer on file	Content held where a contract forbids	Tenant owner	Microsoft's written answer	Before new content

Rollback and recovery

Removing a feature does not remove what it sent. Chapter 8 has the order of removal; this is what stays:

- **The index.** After the content sources and the service application are deleted, removing every on-premises item means you "contact the support team for further guidance" (removing hybrid scenarios, checked on 13 November 2026).
- **Copied term groups and content types.** No documented step reverses the copy.

- **Files in OneDrive.** Setting redirection to None stops the redirect; what becomes of files stored in Microsoft 365 meanwhile is not documented.
- **In the tenant.** The certificate and service principal name on SharePoint's principal, and whatever the onboarding consent created. The removal page mentions neither: agree their removal with the tenant's owner.

If the STS certificate's private key may be exposed, the documented action is replacement on every server, then the upload. That upload adds a certificate and removes none (Chapter 2). We do not know that the old key stops being accepted: test it, and involve Microsoft Support.

Working documents

The Hybrid Architecture Advisor generates these in the browser from your answers. What you did not answer is left as unknown, never filled in.

- **Security Assessment (Word).** The trust boundary table for your features, the exposure and residency answers, the privileged operations, and a signature block.
- **Risk Register (Excel).** One row per open risk from this chapter, each with an owner and a review date. Its **Governance Control Matrix** sheet is the table above, with your owners, evidence and dates.
- **Validation Checklist (Excel), security rows.** The checks and tests in Verify, each marked documented or own test, with its result and a signature column.

Sources

- Business Connectivity Services (BCS) retirement in Microsoft 365, checked on 13 November 2026
- Configure SharePoint Hybrid Auditing in SharePoint 2016 (Preview), checked on 13 November 2026
- SSL certificate management operations, checked on 13 November 2026
- Transport Layer Security (TLS) 1.3 Support, checked on 13 November 2026
- Plan hybrid OneDrive, checked on 13 November 2026
- SharePoint hybrid sites and search, checked on 13 November 2026
- Hybrid site following, checked on 13 November 2026
- Hybrid self-service site creation, checked on 13 November 2026
- Plan hybrid SharePoint in Microsoft 365 taxonomy and hybrid content types, checked on 13 November 2026
- Configure hybrid SharePoint taxonomy and hybrid content types, checked on 13 November 2026
- Learn about cloud hybrid search for SharePoint in Microsoft 365, checked on 13 November 2026
- Plan server-to-server authentication, checked on 13 November 2026

- Hybrid search in SharePoint in Microsoft 365, checked on 13 November 2026
- Configure cloud hybrid search - roadmap, checked on 13 November 2026
- Plan for server-to-server authentication in SharePoint Server, checked on 13 November 2026
- Plan cloud hybrid search for SharePoint in Microsoft 365, checked on 13 November 2026
- Cloud hybrid search service (Cloud SSA) FAQ, checked on 13 November 2026
- Display hybrid federated search results in SharePoint Server, checked on 13 November 2026
- Configure a reverse proxy device for SharePoint Server hybrid, checked on 13 November 2026
- Copy-SPTaxonomyGroups, checked on 13 November 2026
- Azure ACS retirement in Microsoft 365, checked on 13 November 2026
- Replace the STS certificate for SharePoint Server, checked on 13 November 2026
- New health analyzer rules for SSL certificates, checked on 13 November 2026
- Strong Transport Layer Security (TLS) Encryption, checked on 13 November 2026
- Hybrid Configuration Wizard in the SharePoint admin center, checked on 13 November 2026
- Removing SharePoint hybrid scenarios, checked on 13 November 2026

Related pages on this site

- Chapter 2 of this guide: the trust, its certificates and its accounts.
- Chapter 3: hybrid search, and the checks this chapter reuses.
- Chapter 7: running the controls. Chapter 8: the exit.
- Hybrid SharePoint, Java and .NET integration: trust boundaries, for boundaries beyond Microsoft's own features.
- SharePoint Server security updates and the Hybrid Architecture Advisor.

Before you continue

- [ ] Every feature kept has a row saying what crosses the boundary, in which direction and authenticated as what, and none depends on a retired boundary
- [ ] The cloud Search service application's content sources are signed by the content's owner, on the assumption that indexed content leaves the network
- [ ] Grants to Everyone, Authenticated Users, Domain Users and SAML or OpenID Connect claims on crawled content are listed, each with a decision
- [ ] The residency question has a written answer from Microsoft, or the content it concerns is excluded from the crawl
- [ ] Each privileged operation has a named person, an account, a window and a record that the role was removed afterwards
- [ ] The trimming tests ran with two accounts, for both searches, and a reverse proxy kept from an inbound design is retired or assessed

- [ ] The control matrix has an owner and evidence on every row, and the assessment is signed