PH7X SYSTEMS ®

1.0.0 · CHAPTER 2

Match the identities first, then build one trust and give every part of it an owner

Hybrid Architecture Field Guide · Chapter 2

pH7x Systems

2026-11-13

2. Match the identities first, then build one trust and give every part of it an owner

> Hybrid has one trust and two directories. The trust proves which server is calling; only matching identities decide what the person behind the call may see.

Every hybrid feature in this guide rests on two things that are easy to confuse. The first is that a person in Active Directory Domain Services (AD DS) and a person in Microsoft Entra ID are recognisably the same person. The second is that the farm and the tenant trust each other's tokens. Microsoft documents them on different pages, with different accounts, and a farm can have one without the other.

> **Are the farm's users the same people in Microsoft 365, and is there one server-to-server trust whose realm, certificate and accounts somebody owns?**

The decision this chapter leads to is whether the estate is ready to build, or keep, the server-to-server trust: with which identity source, on which web application, by the wizard or by hand, and with a named owner for the realm, the certificate and the privileged accounts.

What this chapter settles

It settles the identity and trust layer under every later chapter: what Microsoft requires of the two directories, what the trust is and what building it changes on the farm, which certificates exist and when they expire, and which accounts hold which roles. It takes from Chapter 1 the list of hybrid features the estate intends to run and the farm's update level. It hands to Chapter 3 a working trust and matched identities for search, to Chapter 4 the profile mappings redirection relies on, and to Chapter 7 a certificate register to watch.

It leaves out the design of directory synchronisation itself, AD FS and other federation services, Conditional Access, and how people sign in to the farm, which is Chapter 21 of the SharePoint Migration Field Guide. Four words are kept apart throughout:

TERM	WHAT IT IS	WHERE MICROSOFT DOCUMENTS IT FOR HYBRID
Identity synchronisation	Copies of AD DS accounts created in Microsoft Entra ID	"you must synchronize your on-premises Active Directory Domain Services user accounts with Microsoft 365" (configure Microsoft 365 for hybrid, checked on 13 November 2026)
Single sign-on	How a person signs in: with single sign-on, "Microsoft 365 is configured to trust the on-premises environment for user authentication" (Microsoft 365 integration, checked on 13 November 2026)	An option beside password synchronisation, not a requirement (below)
Authentication	Proof of who is calling. For the trust, the caller is a server: the protocol "is separate from user authentication and is not used as a sign-in authentication protocol by SharePoint users" (plan server-to-server authentication in SharePoint Server, checked on 13 November 2026)	The trust this chapter builds
Authorisation	What the identified person may see. The same page lists it as a second check: "Verify that the type of access that the server is requesting is authorized"	Permissions on each side, and the mapping of one identity to the other

Applies to

SharePoint Server 2016 and 2019 left support on 14 July 2026 by their servicing policies (2016, 2019, both checked on 13 November 2026). The columns for them are here because Microsoft's hybrid pages still describe them, not because we would build on them.

FACT	SHAREPOINT SERVER 2016	SHAREPOINT SERVER 2019	SUBSCRIPTION EDITION
Identity prerequisites: verified domain, UPN suffix, synchronisation, licences	Documented	Documented	Documented; no update level stated
Server-to-server trust, by wizard or by hand	Documented	Documented	Documented: the wizard page names Subscription Edition as a server it launches from. The manual page marks itself as applying to it, but its text still says "SharePoint 2016 Management Shell"
`Add-PSSnapin Microsoft.SharePoint.PowerShell` in the manual procedure	As written	As written	The cmdlets are a module and load without it (below)
Step 7 of the manual procedure, `Update-FederatedHybridSearchForM365.ps1`	Named	Named	Not named: not established
OpenID Connect 1.0 sign-in for web applications	No	No	Yes: it "only supports SharePoint Server Subscription Edition" (OIDC 1.0 authentication, checked on 13 November 2026)
Certificate management and its four health rules	No	No	Yes, Subscription Edition only
Classic-mode content web applications	Possible	Possible	Removed: "Content web applications will now only support claims authentication mode" (deprecated or removed in Subscription Edition, checked on 13 November 2026)

Architecture

Two directories, one person

Microsoft's five steps on the tenant side are, in order: "Sign up for Microsoft 365. / Register your domain with Microsoft 365. / Assign UPN domain suffixes. / Synchronize accounts with Microsoft 365. / Assign licenses to your users." (configure Microsoft 365 for hybrid). Each one is a condition of identity, not of trust:

- **A verified public domain.** "you must register a public domain that you own (such as contoso.com) in Microsoft 365". `contoso.com` is Microsoft's example and ours.
- **A matching UPN suffix.** You create in AD DS a UPN suffix that matches that domain and "assign the UPN domain suffix to each user account that you want to synchronize or federate".
- **Synchronised accounts.** Directory synchronisation with password synchronisation, or with single sign-on: "you must configure at least one of the two (password synchronization or SSO)".
- **Licences.** "Your users must each have a license in Microsoft 365 in order to be able to use hybrid features."

Single sign-on is optional. Microsoft's FAQ says so in one sentence: "Single sign-on is not a mandatory prerequisite to configure server-to-server authentication or Cloud hybrid search service application." (cloud hybrid search FAQ, checked on 13 November 2026). Synchronisation is not optional.

Microsoft's pages disagree about the word they use for these people. One says: "some or all user accounts in Active Directory are synchronized with Microsoft Entra directory services. We refer to these accounts as federated users." (accounts needed for hybrid, checked on 13 November 2026). Another adds a sign-in method to the definition: a federated user is synchronised "and who accesses resources in both environments by authenticating with the federation identity provider, such as Active Directory Federation Services (AD FS) 2.0" (display hybrid federated search results, checked on 13 November 2026). We would follow the first, because it agrees with the FAQ and with the page that allows password synchronisation alone. In this guide a "federated user" is a synchronised, licensed user on the matching UPN suffix, however they sign in.

What the trust is

The trust is server-to-server authentication over OAuth 2.0. Microsoft describes it as "a trust relationship between your on-premises SharePoint farm and your SharePoint in Microsoft 365 tenant, which uses Microsoft Entra ID as a trusted token signing service" (configure server-to-server authentication, checked on 13 November 2026). It is "required for all hybrid scenarios except hybrid OneDrive" (plan SharePoint Server hybrid, checked on 13 November 2026). The wizard builds it anyway: "For all options, the Hybrid Configuration Wizard configures a server-to-server trust between your SharePoint Server farm and Microsoft 365." (Hybrid Configuration Wizard, checked on 13 November 2026). A farm that ran the wizard only for OneDrive therefore has a trust it may not know about.

PART OF THE TRUST	WHERE IT LIVES	WHAT THE DOCUMENTED PROCEDURE PUTS THERE
Signing certificate, public key only	The SharePoint in Microsoft 365 principal object in the tenant, application ID `00000003-0000-0ff1-ce00-000000000000`	The farm's STS signing certificate, with its start and end dates
Service principal name	The same principal	`00000003-0000-0ff1-ce00-000000000000/*.<public domain name>.com`, always a wildcard
Application principal	The farm's App Management service	The tenant's SharePoint principal, registered with `Register-SPAppPrincipal`
Authentication realm	The farm	The tenant's context ID, set with `Set-SPAuthenticationRealm`
Proxy and trusted token issuer	The farm	A proxy and a trusted security token issuer, both named "ACS", pointing at `https://accounts.accesscontrol.windows.net/<context ID>/metadata/json/1`

The two identifiers this chapter prints, `00000003-0000-0ff1-ce00-000000000000` for SharePoint in Microsoft 365 and `00000001-0000-0000-c000-000000000000` for the Azure Access Control Service, are Microsoft's own application identifiers. Microsoft's procedure prints them, and they are the same in every tenant: they name a Microsoft service and say nothing about your directory. The context ID and the realm are the values that are yours, and this guide never prints one.

What crosses the boundary when it is built is a public key, a wildcard name for your public domain and your tenant's identifier. No user account, password or private key is uploaded by these steps.

The realm change

The farm's authentication realm becomes the tenant's context ID, and stays that way: "the SharePoint farm authentication realm value must always match the tenant context identifier. If you change this value, the farm will no longer participate in hybrid functionality." (configure server-to-server authentication). The wizard does the same, and Microsoft states the cost: "After the authentication realm is changed, existing SharePoint in Microsoft 365 add-ins fail to authenticate. The Hybrid Configuration Wizard attempts to fix this issue automatically." (Hybrid Configuration Wizard). The FAQ gives the symptom: "users will get an HTTP 401 when they're redirected to the add-ins". Microsoft's repair article names what breaks: provider-hosted add-ins registered against the old realm, and a Workflow Manager association, on a "SharePoint 2013 or SharePoint 2016 farm" (KB 4010011, checked on 13 November 2026). It does not name 2019 or Subscription Edition, and it does not say whether high-trust add-ins, which use "a certificate instead of a context token to establish trust" (create high-trust add-ins, checked on 13 November 2026), are among them. We do not know. The test is to list every add-in and workflow association on a copy of the farm, set the realm there, and open each one.

”ACS” after 2 April 2026

Azure ACS authentication for SharePoint Online "was retired on April 2, 2026", and the manual procedure still creates an "ACS" proxy against an ACS-hosted endpoint. Microsoft reconciles the two in one statement: "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 is the whole of what is documented. No page explains by what mechanism the on-premises dependency survives, and the retirement FAQ has no question about hybrid or high-trust add-ins (add-ins and ACS retirement FAQ, checked on 13 November 2026). We would follow the retirement page, record that the farm reaches `accounts.accesscontrol.windows.net`, and keep that host in the outbound allow list (Microsoft 365 endpoints).

Matching a person across the trust

A server-to-server request names a user, and the receiving side must find that user. SharePoint Server does this by "rehydrating the user's identity" from one of four attributes: the Windows SID, the AD DS user principal name, the SMTP address or the SIP address, and it "expects only one matching entry in the User Profile service application" (server-to-server authentication and user profiles, checked on 13 November 2026). For hybrid, Microsoft requires two mappings in the User Profile service application, fed by a synchronisation connection to AD DS: "confirm that **User Principal Name** is mapped to **userPrincipalName**" and "confirm that **Work email** is mapped to **mail**" (set up SharePoint Server services for hybrid, checked on 13 November 2026).

For search, the consequence is documented. Cloud hybrid search stores each item's access control list in the Microsoft 365 index, "so the system needs to be able to recognize an on-premises user as the same person in Microsoft 365" (plan cloud hybrid search, checked on 13 November 2026): security trimming is authorisation, and it depends on synchronisation. For OneDrive and profile redirection, Microsoft lists the same two mappings as a requirement of every hybrid configuration but does not say what the redirect does with them. We do not know. The test is one synchronised, licensed pilot user in the redirection audience who selects OneDrive on the farm and arrives in their own OneDrive in Microsoft 365.

Prerequisites

The synchronisation engine is in support. Microsoft's integration page names one tool: "To set up directory synchronization, use Microsoft Entra Connect." For Microsoft Entra Connect Sync, the version history carries a deadline: "Upgrade Microsoft Entra Connect Sync to version 2.6.84.0 or later and configure application-based authentication by April 7, 2027. Legacy authentication is being retired, and synchronization services will stop working after this date if these requirements aren't met." (Entra Connect version history, checked on 13 November 2026). The latest version the page listed on that day was 2.6.92.0, released on 23 September 2026. Version 2.5.190.0 is supported until 2 February 2027; 2.5.79.0 left support on 23 October 2026; and "All Microsoft Entra Connect Sync 1.x versions are unsupported and synchronization doesn't function." The installer "is exclusively available on Microsoft Entra Admin Center" and needs ".NET Framework 4.7.2 and TLS 1.2". If synchronisation stops, new and changed accounts stop matching, and hybrid degrades without an error on the farm.

Cloud Sync is not established for SharePoint hybrid. Microsoft calls Microsoft Entra Cloud Sync its "strategic direction for hybrid identity synchronization" (Cloud Sync decision guide, checked on 13 November 2026), and its comparison has a row for Exchange hybrid and none for SharePoint. The SharePoint hybrid pages name only Microsoft Entra Connect. We do not know whether Cloud Sync satisfies them. We would not move a hybrid farm's directory to Cloud Sync until a test tenant shows a Cloud Sync user getting security-trimmed hybrid results and a working redirect.

Several forests need one synchronisation server. "When you have multiple forests, all forests must be reachable by a single Microsoft Entra Connect Sync server." (cloud hybrid search FAQ).

The farm's services are running, locally. Every hybrid configuration needs the Managed Metadata service application, the User Profile service application and My Sites; hybrid search and sites features also need App Management and the Subscription Settings service (set up SharePoint Server services for hybrid). "Services must be running on the local farm - farms with federated services aren't supported." (hybrid requirements, checked on 13 November 2026).

The tenant is on the list. "Hybrid features are only enabled for tenants in the Hybrid Allow List. To use Hybrid features, contact Microsoft Support to add your tenant to the Hybrid Allow List." (Hybrid Configuration Wizard). Microsoft does not say how long that takes or whether it applies to tenants that already run hybrid, so ask before you schedule anything.

The accounts exist. Microsoft lists four kinds (accounts needed for hybrid, Hybrid Configuration Wizard):

ACCOUNT	WHERE IT LIVES	ROLE MICROSOFT STATES	USED FOR
Global Admin	Microsoft 365 and Microsoft Entra ID	"A Microsoft 365 Global Admin, either with or without multi-factor authentication (MFA) enabled for the account"	The wizard, the manual procedure's `Connect-MgGraph` sign-in, search onboarding
Farm administrator	AD DS	Farm Administrators group; "A service application administrator (Full Control) for the User Profile Service"; **securityadmin** on the SQL Server instance; **db_owner** on the databases to be updated; local Administrators on the server	Running the wizard, elevated, from a farm server; the PowerShell steps
AD Domain Admin	AD DS	Domain Admins group	"to configure and test AD, ADFS, DNS, and certificates"
Federated users	AD DS, synchronised	Licensed, on the alternative UPN suffix, with permissions in both environments	Testing

Service accounts are outside that table: it "does not include service accounts, which may have specific requirements for service applications and features". Chapter 3 covers the search accounts.

Decision criteria

Wizard or manual. Microsoft's answer is the wizard: "We recommend using the SharePoint Hybrid Configuration Wizard to establish the Server-to-Server authentication". The manual steps are for when you are "unable to use the Hybrid Configuration Wizard for any reason". We would use the wizard, and read the manual page first, because it is the only place Microsoft writes down what the wizard leaves on the farm.

Which certificate. "Using the inbuilt STS certificate is the recommended approach when configuring hybrid workloads." (hybrid requirements). If you intend a certificate of your own, "replace the default certificate before you begin the hybrid configuration process" (plan connectivity from Microsoft 365, checked on 13 November 2026). We would keep the built-in one: a replacement adds an expiry date and a gap in the documentation (see Security).

Which web application. Microsoft's pages disagree on the protocol. One: "federated users can send requests to SharePoint in Microsoft 365 from any SharePoint Server web application that's configured to use Integrated Windows authentication with NTLM or Kerberos." (configure server-to-server authentication). Another: "Integrated Windows authentication using NTLM is required to allow the SharePoint in Microsoft 365 Authentication service to pass user claims to SharePoint in Microsoft 365 using OAuth." (plan server-to-server authentication, checked on 13 November 2026). We would plan on NTLM: two planning pages require it, and the first page's own verification step checks "that Integrated Windows authentication and NTLM are selected". A web application without it must be recreated or extended with NTLM (plan server-to-server authentication). Kerberos-only is not established: prove it with a hybrid query from a Kerberos-only zone on a test farm before relying on it.

Sign-in through OIDC or SAML. The requirement text predates Subscription Edition and never mentions OpenID Connect; the OIDC pages never mention hybrid. Whether a web application whose users sign in with OIDC or SAML can originate hybrid calls is not established. We do not know. The test is a federated user signing in through that provider on a test farm and running a hybrid query, or following a redirect, from that zone. One related fact is documented, and it concerns authorisation, not sign-in: "Items secured with SAML claims when crawled using Cloud Search Service application will not show up in search results", because there is no "way to map an on-premises SAML identity to a Microsoft 365 user"; cloud hybrid search "only supports Windows identity that has been synced to Microsoft Entra ID" (cloud hybrid search FAQ). OIDC identities are not mentioned there either.

Conditions that stop the work. No verified domain or no matching UPN suffix; a synchronisation engine below 2.6.84.0 with no plan for 7 April 2027; a farm that consumes its services from another farm; a tenant not on the Hybrid Allow List; add-ins or Workflow Manager on the farm with nobody to retest them after the realm changes; and nobody willing to hold Global Administrator for the session.

Procedure

With the wizard

1. Complete the five tenant steps and the farm's services (Prerequisites).
2. "Log in to the console of a SharePoint Server farm server as a farm admin", and "From the farm server, connect to Microsoft 365 as a global admin" (run Hybrid Configuration Wizard, checked on 13 November 2026). Turn off any pop-up blocker. The server needs .NET Framework 4.6.2.
3. Open the wizard. Microsoft gives two entry points, a direct link on that page and the Hybrid picker under More features in the SharePoint admin center, and does not say which is current.
4. Validate the credentials, let it check prerequisites (App Management instance, application and proxy online; User Profile proxy online; the `SPO365LinkSettings` cmdlet reachable), and select the features Chapter 1 decided.
5. Retest every add-in and workflow association, then run the checks in Verify.

The wizard "doesn't uninstall features": deselecting one on a later run leaves it installed.

By hand, as Microsoft documents it today

Run it in one Windows PowerShell window on a farm web server, in the order shown, and keep the buffer: Microsoft advises capturing all of it. Install "Microsoft Graph PowerShell" and the "SharePoint in Microsoft 365 Management Shell" first. If the primary web application uses HTTP, OAuth over HTTP must be enabled on every web server (`$serviceConfig.AllowOAuthOverHttp = $true`); with SSL the step is not needed.

The page then loads modules and signs in:

```
Add-PSSnapin Microsoft.SharePoint.PowerShell
Import-Module Microsoft.PowerShell.Utility
Import-Module Microsoft.Graph
Connect-MgGraph -Scopes "Group.ReadWrite.All","RoleManagement.ReadWrite.Directory","Organization.ReadWrite.All"
```

Microsoft's documented commands, quoted as its page prints them. Not run by us: try them on a test farm first.

"You need to sign in using a Microsoft 365 global admin account." On Subscription Edition the first line conflicts with another page: "You don't have to launch the SharePoint Management Shell or use the Add-PSSnapin cmdlet to access the SharePoint Server cmdlets." (new in Subscription Edition, checked on 13 November 2026). We would follow the Subscription Edition page and leave the snap-in line out there. Microsoft does not say whether the line fails on Subscription Edition.

STEP	WHAT IT DOES	COMMANDS AS WRITTEN
1	Sets variables	`$spcn="*.<public_root_domain_name>.com"` ; `$spsite=Get-Spsite <principal_web_application_URL>` ; `$site=Get-Spsite $spsite` ; `$spoappid="00000003-0000-0ff1-ce00-000000000000"` ; `$spocontextID = (Get-MgOrganization).Id` ; `$metadataEndpoint = "https://accounts.accesscontrol.windows.net/" + $spocontextID + "/metadata/json/1"`
2	Adds the STS certificate, "public key only", to the SharePoint principal	`$Cert = (Get-SPSecurityTokenServiceConfig).LocalLoginProvider.SigningCertificate` , then `Get-MgServicePrincipal` to read the principal's `KeyCredentials` , then `Update-MgServicePrincipal -ServicePrincipalId $principal.Id -KeyCredentials $keyCredentials`
3	Adds the wildcard service principal name	`$msp = Get-MgServicePrincipal -Filter "AppId eq '$spoappid'"` ; `Update-MgServicePrincipal -ServicePrincipalId $msp.Id -BodyParameter $params`
4	Registers the principal with the farm	`$appPrincipal = Register-SPAppPrincipal -site $site.rootweb -nameIdentifier $sponameidentifier -displayName "SharePoint"`
5	Sets the realm	`Set-SPAuthenticationRealm -realm $spocontextID`
6	Creates the proxy and the trusted token issuer	`New-SPAzureAccessControlServiceApplicationProxy -Name "ACS" -MetadataServiceEndpointUri $metadataEndpoint -DefaultProxyGroup` ; `New-SPTrustedSecurityTokenIssuer -MetadataEndpoint $metadataEndpoint -IsTrustBroker:$true -Name "ACS"`
7	"Update Hybrid federated search", required "Starting October 2021"	`Update-FederatedHybridSearchForM365.ps1 -HybridWebApp YourHybridWebApplication -Force` , signed in with a "Microsoft 365 Application Administrator account"
8	SharePoint Server 2013 only	Not applicable

Take the full text of each step from Microsoft's page, not from this table. Three defects in that page matter:

- In step 2 the published filter is `"AppId eq '$spoappid'”` , closed with typographic quotation marks. Pasted as printed, we would not expect it to parse; step 3 prints the same filter with straight ones.
- Step 2 keeps the principal's existing certificates and adds yours. It removes nothing, so old certificates stay on the principal until somebody removes them.
- Step 7's script "must be run on a server where SharePoint On-Premises is installed (2013, 2016, or 2019)" and "attempts to install the required module dependencies (MSOnline, AzureAD)". Subscription Edition is not named, and those modules "are deprecated" (upgrade to Microsoft Graph PowerShell, checked on 13 November 2026). We do not know whether a Subscription Edition farm needs step 7 or can run it. The test is an outbound federated query on a test farm after steps 1 to 6: if SharePoint Online results appear, it did not need it. Chapter 3 takes this further.

Verify

Microsoft documents a check for each manual step, and they are worth running after the wizard too:

CHECK	DOCUMENTED METHOD	EXPECTED RESULT
Web application	Central Administration, Manage web applications, Authentication Providers, the zone of the search centre	"Integrated Windows authentication and NTLM are selected"
Service principal name	`$msp = Get-MgServicePrincipal -Filter "AppId eq '$spoappid'"`, then `$msp.ServicePrincipalNames`	One entry of the form `00000003-0000-0ff1-ce00-000000000000/*.<public domain name>.com`, "the *only* SPN in the list that includes your public root domain name"
Application principal	`$appPrincipal | fl`	A registered principal named **SharePoint Online**
Realm	`$spocontextID`, then `Get-SPAuthenticationRealm`	"These GUIDs should be identical."
Trusted token issuer	`Get-SPTrustedSecurityTokenIssuer`	**RegisteredIssuerName** is `00000001-0000-0000-c000-000000000000@<context ID>`
Proxy	Central Administration, Security, General Security, Manage trust	An entry whose name begins with **ACS**
Profile mappings	The user properties of the User Profile service application, as the set-up page describes	**User Principal Name** mapped to **userPrincipalName**; **Work email** mapped to **mail**
Hybrid settings	`Get-SPO365LinkSettings`, which Microsoft describes as "display current hybrid configurations in the farm" (Get-SPO365LinkSettings, checked on 13 November 2026)	The redirection settings Chapter 4 expects. The reference lists it as applicable up to SharePoint Server 2019; the wizard checks for it on every version

The farm-side reads fit in one script for the trust's owner to keep:

```
# Farm server, Windows PowerShell as a farm administrator. Reads the trust; changes nothing.
Write-Host "Writing the realm, the trusted token issuers, the STS signing certificate and the hybrid settings to trust.txt"
Get-SPAuthenticationRealm | Out-File .\trust.txt
Get-SPTrustedSecurityTokenIssuer | Format-List * | Out-File .\trust.txt -Append
(Get-SPSecurityTokenServiceConfig).LocalLoginProvider.SigningCertificate | Format-List Subject, Thumbprint, NotBefore, NotAfter | Out-File .
Get-SPO365LinkSettings | Format-List * | Out-File .\trust.txt -Append
```

Parsed, not yet run: try it on a test farm first.

Microsoft's page ends by telling you to "check your SSO and Directory Synchronization setup" and names no command for it. We would test with one federated user who has "permissions to SharePoint Server site collections and resources in both environments" and the licence and UPN suffix the accounts page requires.

When it fails

WHAT YOU SEE	DOCUMENTED CAUSE	WHAT TO LOOK AT
Provider-hosted add-ins return HTTP 401 after hybrid is configured; a workflow association stops	The realm changed; token issuers are still tied to the old realm. The ULS log reads "The issues of the token is not a trusted issuer." (KB 4010011, spelling as published)	Microsoft's repair in KB 4010011: re-register each add-in against the new realm and reapply its permissions; register Workflow Manager again
The farm stops taking part in hybrid	The realm no longer matches the tenant's context ID, often because a farm setup script set it again	`Get-SPAuthenticationRealm` against the tenant's ID; "update the setup scripts with this new value before you run them again"
A user gets nothing from the other side, or the wrong person's view	The user is not synchronised, not licensed, or not on the matching UPN suffix; or the profile holds no current SID, UPN, SMTP or SIP value; or more than one profile matches, which "returns an error condition that multiple user profiles were found"	The account in both directories, then the two profile mappings
A user is denied something their group grants	"If a user profile and the relevant group memberships for the user are not synchronized, SharePoint Server may incorrectly deny access to a given resource."	Profile and group synchronisation on the farm
Outbound search returns only local results; the ULS log shows an OAuth2 request ending in " (404) Not Found."	The Search service application proxy is deployed in partition mode (online content not displayed, checked on 13 November 2026, written for SharePoint 2013)	The proxy; Chapter 3
New starters never match	Synchronisation has stopped: a retired Microsoft Entra Connect version "might unexpectedly stop working"	The engine's version against the version history
OAuth calls fail on a farm without SSL	"By default, OAuth in SharePoint Server requires **HTTPS**."	The primary web application's protocol, and `AllowOAuthOverHttp` on every web server

Beyond these, Microsoft's only instruction is to check the ULS logs, and for the wizard's script, "contact Microsoft Support". It names no ULS category for the trust itself.

Security

Privilege. The wizard, the manual sign-in and search onboarding each ask for a Global Administrator, on pages that also say: "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 any of them; only step 7 names Application Administrator. Whether a lesser role works is not established, and we would not publish a guess. We would hold the role for the session only, on a named account with multi-factor authentication, which the wizard supports, and record who held it and when. The manual connection also requests three write scopes in Microsoft Graph; record that consent.

The built-in certificate. "The default STS certificate does not need to be renewed. Renewal only applies after the STS certificate has been replaced." (replace the STS certificate, checked on 13 November 2026). The copy on the tenant's principal carries the certificate's own end date all the same (step 2 writes `EndDateTime = $Cert.NotAfter`), so read that date and put it in the register.

A replacement certificate. It must use "2048 bit encryption or higher", is replaced "during a maintenance window as the SharePoint Timer Service (SPTimerV4) must be restarted", "on every server in the farm", by a SharePoint Shell Administrator, with `Set-SPSecurityTokenServiceConfig -ImportSigningCertificate $cert`, `iisreset` and `Restart-Service SPTimerV4`. Such certificates "expire within 1 to 3 years". For a hybrid farm the page then sends you elsewhere for "additional steps required to upload the STS certificate to Azure", and that is a gap. The article it points to is about add-ins, and its function depends on `Install-Module -Name MSOnlineExt` and `Connect-MsolService` (use ACS to authorise provider-hosted add-ins, checked on 13 November 2026), from a module Microsoft lists as deprecated. The hybrid requirements page, for its part, labels a link "Replace the STS certificate" that leads to a page with no replacement steps. Step 2 of the manual procedure is the documented Microsoft Graph route for uploading a certificate, but no page says it is the renewal procedure. We would rehearse a replacement on a test farm, upload with step 2, and confirm a hybrid query before and after.

Certificate management in Subscription Edition. It covers "the lifecycle of SSL certificates in your SharePoint farm" (SSL certificate management, checked on 13 November 2026), with four health rules: "Certificate notification contacts haven't been configured", "Upcoming SSL certificate expirations" (weekly, 15 to 60 days ahead), "SSL certificates are about to expire" (daily, within 15 days) and "SSL certificates have expired" (health analyzer rules for SSL certificates, checked on 13 November 2026). Microsoft does not say that the feature or its rules cover the STS signing certificate, and it documents no health rule for the hybrid trust. Treat the STS certificate as unwatched until you have seen a rule report it.

The public certificate. Only inbound scenarios, where Microsoft 365 calls the farm, need a reverse proxy and a "Secure Channel SSL certificate": wildcard or SAN, "issued by a public root certification authority", at least 2048-bit (plan connectivity from Microsoft 365). Inbound federated search retired in September 2024 (plan SharePoint Server hybrid). An estate with outbound features only needs none of it for hybrid, and Chapter 6 decides what happens to a proxy kept from an older design.

Exposure. The trust lets the farm ask SharePoint in Microsoft 365 for content on behalf of a named user. What limits it is authorisation on each side: the user's permissions in the tenant, and identities that match exactly one person. The wildcard service principal name "lets SharePoint in Microsoft 365 validate connections with *any host* in that domain", which is broader than one farm; note which farms in that domain share the tenant.

Rollback and recovery

Microsoft documents one removal step for the trust, as the last step of removing hybrid: "delete the **Azure Access Control Service Application Proxy** and **SharePoint Application Principal Management Service Application Proxy** created by the Hybrid Configuration Wizard". In Central Administration, Manage service applications, delete the one named **ACS** and the one named **SharePoint App Management Proxy**, then "Perform an iisreset on all SharePoint Servers in the farm." (removing SharePoint hybrid scenarios, checked on 13 November 2026). The features come off first; Chapters 3, 4 and 5 hold those steps and Chapter 8 the order.

The wizard is not a way back: "This isn't designed to undo the changes once the wizard completes. … re-running the wizard doesn't clean up the trust." (cloud hybrid search FAQ).

What Microsoft does not document:

- **Reverting the realm.** No page tells you to set it back, and none says what the earlier value was, so record it before the first change. Changing it again has the same effect as changing it the first time: KB 4010011 warns that access tokens "created for a specific realm won't work after you change the `SPAuthenticationRealm` value", so add-ins registered since hybrid was configured would be the ones to fail. We would leave the realm alone on exit unless something requires the old value.
- **The trusted token issuer.** The removal page deletes the proxy named ACS and does not mention the trusted security token issuer of the same name. We do not know whether deleting the proxy removes it. The test is `Get-SPTrustedSecurityTokenIssuer` before and after, on a test farm.
- **What stays in the tenant.** The certificate and the service principal name on the SharePoint principal are not mentioned. They belong to the tenant's owner; we would agree their removal there, and record the decision either way.
- **Recovery after a farm rebuild.** Whether a trust survives a database attach to a new farm is not established. An attach brings content, not configuration (Chapter 25 of the SharePoint Migration Field Guide), so plan to build the trust again and to upload the new farm's certificate.

Working documents

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

- **Identity and Trust Matrix (Excel).** One row per part of this chapter: the verified domain and UPN suffix, the synchronisation engine and its version against the 7 April 2027 deadline, the sign-in method, the web application and its authentication, the realm before and after, the trusted token issuer, and each account with the role it holds. Its **Certificate Register** sheet lists the STS signing certificate, the copy on the tenant's principal, any replacement and any public certificate, each with thumbprint, end date and owner.
- **Configuration and Validation Runbook (Word), identity and trust part.** The wizard route and the manual route as steps, with the expected result of each check in Verify and a place for who ran it and when.
- **Validation Checklist (Excel), identity rows.** The checks in Verify and the pilot-user tests this chapter names, each with its result and a signature column.

Sources

- Configure Microsoft 365 for SharePoint hybrid, checked on 13 November 2026
- Microsoft 365 integration with on-premises environments, checked on 13 November 2026
- Plan for server-to-server authentication in SharePoint Server, checked on 13 November 2026
- Updated Product Servicing Policy for SharePoint Server 2016, checked on 13 November 2026
- Updated Product Servicing Policy for SharePoint Server 2019, checked on 13 November 2026
- OpenID Connect 1.0 authentication, checked on 13 November 2026
- What's deprecated or removed from SharePoint Server Subscription Edition, checked on 13 November 2026
- Cloud hybrid search service (Cloud SSA) FAQ, checked on 13 November 2026
- Accounts needed for hybrid configuration and testing, checked on 13 November 2026
- Display hybrid federated search results in SharePoint Server, checked on 13 November 2026
- Configure server-to-server authentication from SharePoint Server to SharePoint in Microsoft 365, checked on 13 November 2026
- Plan SharePoint Server hybrid, checked on 13 November 2026
- Hybrid Configuration Wizard in the SharePoint admin center, checked on 13 November 2026
- Provider-hosted add-ins stop working and HTTP 401 error after you configure SharePoint farm hybrid features (KB 4010011), checked on 13 November 2026
- Create high-trust SharePoint Add-ins, checked on 13 November 2026
- Azure ACS retirement in Microsoft 365, checked on 13 November 2026
- FAQ - SharePoint Add-In and Azure ACS retirement in Microsoft 365, checked on 13 November 2026
- Server-to-server authentication and user profiles in SharePoint Server, checked on 13 November 2026
- Set up SharePoint Server services for hybrid environments, checked on 13 November 2026
- Plan cloud hybrid search for SharePoint in Microsoft 365, checked on 13 November 2026
- Microsoft Entra Connect: Version release history, checked on 13 November 2026
- Migrate from Microsoft Entra Connect Sync to Cloud Sync: decision guide, checked on 13 November 2026
- Hardware and software requirements for SharePoint hybrid, checked on 13 November 2026
- Plan connectivity from Microsoft 365 to SharePoint Server, checked on 13 November 2026
- Plan server-to-server authentication, checked on 13 November 2026
- Run Hybrid Configuration Wizard, checked on 13 November 2026
- New and improved features in SharePoint Server Subscription Edition, checked on 13 November 2026
- Upgrade from Azure AD PowerShell to Microsoft Graph PowerShell, checked on 13 November 2026
- Get-SPO365LinkSettings, checked on 13 November 2026
- SharePoint Online content isn't displayed in a SharePoint on-premises search, checked on 13 November 2026
- Replace the STS certificate for SharePoint Server, checked on 13 November 2026
- Use ACS to authorize low-trust provider-hosted add-ins on an on-premises SharePoint site, checked on 13 November 2026
- SSL certificate management operations, checked on 13 November 2026
- New health analyzer rules for SSL certificates, checked on 13 November 2026
- Removing SharePoint hybrid scenarios, checked on 13 November 2026

Related pages on this site

- Chapter 1 of this guide: readiness and the architecture decision this chapter builds on.
- Chapter 3: hybrid search, which uses this trust and these identities for security trimming.
- Chapter 4: hybrid OneDrive and sites, which use the profile mappings.
- Chapter 6: security, compliance and governance, including the reverse proxy question.
- Chapter 7: operations and monitoring, which takes over the Certificate Register.
- Chapter 8: exit, and the order in which the trust comes off.
- SharePoint Migration Field Guide, Chapter 21 (authentication), Chapter 25 (which hybrid features an estate keeps) and Chapter 42 (keeping Subscription Edition supported).
- Hybrid SharePoint, Java and .NET integration: trust boundaries.
- Hybrid Architecture Advisor and Microsoft 365 endpoints.

Before you continue

- [ ] The public domain is verified in the tenant, and every hybrid user is synchronised, licensed and on the matching UPN suffix
- [ ] The synchronisation engine is a supported version, with a dated plan for 2.6.84.0 or later and application-based authentication before 7 April 2027
- [ ] **User Principal Name** maps to **userPrincipalName** and **Work email** to **mail**, and a pilot user resolves to exactly one profile
- [ ] The web application that will originate hybrid calls uses Integrated Windows authentication with NTLM, or a test has proved the alternative
- [ ] Every add-in and workflow association is listed, with somebody named to retest it after the realm changes, and the realm's earlier value is written down
- [ ] The realm, the trusted token issuer, the service principal name and the hybrid settings were read with the documented checks and match what this chapter says to expect
- [ ] The Certificate Register holds the STS signing certificate and the copy on the tenant's principal, each with an end date and an owner
- [ ] The Global Administrator session has a named holder and a record, and the removal step for the trust is known before the trust is built