PH7X SYSTEMS ®

0.2.0 · CHAPTER 21

Choose the sign-in the new farm will accept

SharePoint Migration Field Guide · Chapter 21

pH7x Systems

2026-11-06

21. Choose the sign-in the new farm will accept

> To SharePoint, one person who signs in two ways is two people, and the content knows only one of them.

A content database carries every permission as stored, each naming a person or group as the old farm's sign-in produced it. The new farm's web applications are built again before the first attach, so their sign-in is a choice, not an inheritance. Keep the method and the content recognises everyone; change it, and the content has to learn who everyone has become before anyone opens it.

> **How will people and processes sign in to each web application on the new farm, and what has to change so that the content still recognises them?**

The decision this chapter leads to is the authentication each web application will accept: per zone, its methods and who uses them, and for a trusted provider, its identity claim and when the people in the content move to it.

Which farms this chapter is for

A SharePoint Server 2016 or 2019 farm moving to Subscription Edition by database attach, whose web applications are created again (Chapter 23). Two methods are already gone. Content web applications "will now only support claims authentication mode", so classic mode becomes claims, as Chapter 23 describes. Basic authentication, unsupported since 14 July 2026, is not available to them on a current build: since the 24H2 update (September 2024), "admins can no longer create new web applications or web app extensions using Basic authentication" (what is deprecated or removed, checked on 6 November 2026). Start from the inventory in Chapter 2, which records each web application's methods, and add who signs in on each zone and what calls it.

What each method gives the new farm

METHOD	WHAT IT OFFERS	WHAT IT ASKS OF THE NEW FARM
Windows, NTLM	Sign-in without a prompt for domain users; "the simplest form of Windows authentication to implement"	Nothing beyond the domain, while Windows retires the protocol
Windows, Negotiate (Kerberos)	Microsoft's recommended Windows option, "the strongest Integrated Windows authentication protocol", able to delegate identity to back ends	Service principal names, clients that reach a domain controller, and NTLM as fallback, since Kerberos alone breaks app authentication
SAML 1.1 trusted provider	WS-Federation sign-in through AD FS or another provider	A token-signing certificate that only one provider in the farm may use, a relying party per web application, HTTPS
OIDC 1.0 trusted provider	Subscription Edition only: Entra ID, AD FS 2016 or later, or another OIDC 1.0 provider, with multifactor authentication and conditional access	HTTPS, and a nonce cookie certificate on every server, handled by SharePoint certificate management from 24H2

Sources for the table: plan user authentication, Kerberos planning, create claims-based web applications, what's new, OIDC with Entra ID and federated authentication, all checked on 6 November 2026.

Methods can share a zone; for several, Microsoft recommends the default zone, since "the result is the same URL for all users" (plan user authentication). A trusted provider's HTTPS changes the URL of a web application served over HTTP today, with the costs Chapter 23 sets out.

We would keep Windows for people too, unless a requirement names what only a trusted provider gives: sign-in from devices outside the domain, multifactor authentication or conditional access, or Microsoft's recommended replacement for Basic. Windows claims on both sides changes no identity in the content; every other choice changes some.

Windows stays on the default zone

Whatever people use, the farm signs in with Windows. Microsoft's planning page says "the crawl component requires NTLM to access content", its SAML and OIDC setup pages require Windows on the default zone for the crawler (federated authentication, OIDC with Entra ID), and a web application with Windows on no zone is not crawled (create claims-based web applications). Crawl the default zone, the only one whose results search maps to each user's zone (best practices for crawling, checked on 6 November 2026). We read Negotiate there, with NTLM as fallback, as meeting all of them. Scripts and systems that call the farm with a Windows account sign in as "the identity of the process" (plan user authentication), and need that zone too.

Windows is retiring the protocol the crawler needs: Windows Server 2025 removed NTLMv1 and deprecated NTLMv2, which "will continue to work but will be removed from Windows Server in a future release" (features removed or no longer developed, checked on 6 November 2026). We do not

know when, or whether SharePoint's crawler will still need NTLM then. We recommend listing every dependency the new farm has on NTLM, the crawler first, so that the change arrives as a list rather than an outage.

Hybrid keeps a Windows zone as well. Microsoft documents hybrid's requests to SharePoint in Microsoft 365 only from a web application "configured to use Integrated Windows authentication with NTLM or Kerberos" (configure server-to-server authentication, checked on 7 November 2026). A farm that moves people to a trusted provider and keeps any hybrid feature (Chapter 25) keeps a Windows web application or zone for it, and lists it beside the crawler.

What changes when people sign in through a provider

A Windows sign-in produces a Windows claim, such as Microsoft's example `i:0#.w|contoso\chris`; a trusted provider's user is identified by the identity claim it sends. The content's permissions name the first, and when SAML users are refused, the most common reason is that "the permissions were assigned to a user's Windows-based account (domain\user) instead of the user's SAML identity claim" (claims troubleshooting, checked on 6 November 2026).

WHAT	WHAT CHANGES WITH A TRUSTED PROVIDER	WHAT YOU DECIDE
People in the content	Permissions name Windows claims until `Convert-SPWebApplication -From CLAIMS-WINDOWS -To CLAIMS-TRUSTED-DEFAULT` rewrites them, per web application or database, with a skip list and a documented reverse	Who moves, where and when
Groups	Membership arrives as claims in the token; claims without a mapping are discarded	The group claim you map, and proof that group permissions still open
People Picker	It resolves "any value that is entered, even if it's not a valid claim", unless imported profiles or a custom claims provider resolve names; server-to-server requests also find users through those profiles	Which of the two, and an import that carries the identity claim
Service accounts	Nothing: they keep Windows on the default zone	The skip list that keeps them out of the conversion

Sources for the table: migrate Windows claims to SAML claims, enhanced People Picker and server-to-server authentication and user profiles, checked on 6 November 2026. None of them says whether the conversion rewrites permissions granted to groups.

For Entra ID, the picker is the constraint: the profile-backed picker resolves groups only by SID, cloud-only Entra groups have none, and AD Import reads only on-premises Active Directory. For cloud-only users or groups, "a Custom Claims Provider may be the only solution" (enhanced People Picker).

Choose the identity claim once

The identity claim is declared when the trusted provider is created, and "only the owner of the IP-STS knows which value in the token will always be unique for each user" (plan user authentication). The same page names UPN and email as frequent choices, and Microsoft's Entra claims reference calls email "mutable over time" and the UPN "not a durable identifier for the user" (optional claims, checked on 6 November 2026). SharePoint identifies the provider's users by that value, so we recommend agreeing it with the provider's owner, writing down what happens to a person's access the day theirs changes, and rehearsing that day.

Convert on the new farm, after the attach

Microsoft documents the conversion from Windows claims to SAML claims for existing web applications, from 2013 to Subscription Edition, without saying on which farm to run it (migrate Windows claims to SAML claims). Its OIDC pages do not describe converting existing users, so only a rehearsal establishes whether the same conversion serves an OIDC provider. We would convert on the new farm, after each attach and before anyone signs in, so that the source and its backups keep the old identities for the rollback in Chapter 23.

```
# Rehearsal farm, on a copy. Moves the Windows claims users of one content database.
$db = Get-SPContentDatabase "<DatabaseName>"
$tp = Get-SPTrustedIdentityTokenIssuer "<ProviderName>"
Write-Host "Converting Windows claims in $($db.Name) to $($tp.Name), skipping skip.csv"
Convert-SPWebApplication -Identity "https://<url>" -Database $db -From CLAIMS-WINDOWS -To CLAIMS-T
    -TrustedProvider $tp -SourceSkipList .\skip.csv -LoggingDirectory .\convert-logs
```

Test the choice before the first attach

On the rehearsal farm, with each web application built as decided and no content yet:

- Create a site collection with a Windows and a trusted-provider administrator, as Microsoft's setup pages do, and sign in as each on every zone.
- In the People Picker, a real user and a real group resolve; an invented name does not.
- Crawl the default zone and search as a user of each method: each finds only what they may open, at their own zone's URL.
- Run every scheduled script and process that calls the farm, under its own account.

Then test a copy of each content database with `Test-SPContentDatabase -ExtendedCheck`, which "checks for inconsistent authentication modes", claims or classic (Test-SPContentDatabase, checked on 6 November 2026), not which provider the database's people belong to. So attach the copy, convert it, crawl it, and sign in as a sample of users and groups whose access you read on the old farm, the two reads of Chapter 8.

Out of scope

Forms-based sign-in, which Subscription Edition still supports (plan user authentication); the design of the identity provider itself; add-in authentication, Chapter 18; the identities integrations use, Chapter 22; permissions, Chapter 13; the attach, Chapter 23. The Subscription Edition migration pack generates the test that sites open for each sign-in method in use.

Before you continue

- [ ] Every old web application and zone is listed with its methods, its users and what calls it
- [ ] Each new web application's zones are decided: Windows on the default zone, HTTPS wherever a trusted provider signs people in
- [ ] A trusted provider's identity claim, and what happens when a value changes, are agreed with its owner
- [ ] The People Picker resolves only real users and groups
- [ ] The conversion and its skip list are rehearsed on copies, with the farm and window written down
- [ ] On the rehearsal farm, a user of each method signed in on each zone and searched, and every process ran
- [ ] Every dependency on NTLM is listed, the crawler first
- [ ] Any web application or zone a hybrid feature uses keeps Windows sign-in