

Single Sign-On Setup Guide

Active Directory (LDAP) + Keycloak + Kerberos
for LAN applications on the **mipl.com** domain

Audience: IT / system administrators who will build and run the SSO server.

Scope: LAN only. Domain-joined PCs get automatic login (Kerberos); workgroup PCs log in once with their AD username and password.

Outcome: one login for every internal application (Node/PM2, PHP/XAMPP, .NET/IIS), with app access controlled by AD groups and each app keeping its own permissions.

Document	Value
Version	1.0 (25 Sep 2026)
Software	Windows Server 2019/2022, Active Directory, AD Certificate Services, Keycloak 26.x, Eclipse Temurin JDK 21, SQL Server, NSSM
How to use	Do the phases in order . Each phase ends with a CHECK. Do not continue until the check passes; that is what keeps the setup error-free.

Contents

1. Values used in this guide	4
2. How the pieces fit together	4
3. Prerequisites checklist	5
4. Phase 1 - Prepare Active Directory	6
4.1 Create the OUs and app-access groups	6
4.2 Create the two service accounts	6
4.3 Create the DNS records	6
4.4 Check time synchronisation	7
5. Phase 2 - Certificates (AD CS)	7
5.1 Confirm the domain controller supports LDAPS	7
5.2 Create a Web Server certificate template (once)	7
5.3 Request the certificate for sso.mipl.com	7
5.4 Export the root CA certificate	8
6. Phase 3 - Install Keycloak	8
6.1 Install Java 21	8
6.2 Create the SQL Server database	8
6.3 Extract Keycloak	8
6.4 Configure keycloak.conf	8
6.5 Build and first start (creates the temporary admin)	9
6.6 Run Keycloak as a Windows service (NSSM)	9
6.7 Firewall: LAN only	10
7. Phase 4 - Realm and LDAP (Active Directory) federation	10
7.1 Create the realm	10
7.2 Realm settings	10
7.3 Add the LDAP provider	10
7.4 Check the default mappers	11
7.5 Add the AD group mapper	12
7.6 Sync and test	12
8. Phase 5 - Kerberos (automatic login on domain PCs)	12
8.1 Register the SPN	12
8.2 Create the keytab	13
8.3 Create krb5.ini on the Keycloak server	13
8.4 Verify the keytab before touching Keycloak	13
8.5 Enable Kerberos in the LDAP provider	13
8.6 Check the browser flow	14

8.7 Group Policy: let browsers send Kerberos to sso.mipl.com	14
8.8 Test Kerberos	14
9. Phase 6 - Register applications (OIDC clients)	15
9.1 Create the 'groups' client scope (once, before the first client)	15
9.2 Create one client per application (example: ERP)	15
9.3 What to give each app developer	15
9.4 Make every app server trust the internal CA	16
9.5 Rules for app-side integration	16
10. Phase 7 - Workgroup PCs	16
11. Final acceptance test	17
12. Troubleshooting	17
13. Operations and maintenance	18
Appendix A - Domain controller setup script	19
Appendix B - Workgroup PC setup script	20
Appendix C - Build order at a glance	20

1. Values used in this guide

Every command in this guide uses the values below. Items marked **(example)** are placeholders: replace them with your real server names and IPs **before** running anything. Write your real values into the right-hand column first.

Item	Value in this guide	Your real value
AD / DNS domain	mipl.com	mipl.com
Kerberos realm (always UPPERCASE)	MIPL.COM	MIPL.COM
NetBIOS domain	MIPL (check: echo %USERDOMAIN%)	
LDAP base DN	DC=mipl,DC=com	DC=mipl,DC=com
Domain controller(s)	dc01.mipl.com (example). Find yours: nltest /dsgetdc:mipl.com	
AD DNS server IP	192.168.1.10 (example)	
LAN subnet	192.168.1.0/24 (example)	
Keycloak server computer name	SRV-KC01 (example). Must not be named SSO	
Keycloak URL (DNS A record)	https://sso.mipl.com	https://sso.mipl.com
Keycloak realm	mipl	mipl
SQL Server for Keycloak	SQLSRV01 (example), database keycloak	
LDAP bind account	svc-keycloak	svc-keycloak
Kerberos service account	svc-kc-http	svc-kc-http
App access groups	APP-ERP, APP-HR, APP-QMS (one per app)	
App URLs	https://erp.mipl.com, https://portal.mipl.com, ...	

NOTE **mipl.com is also a public internet name.** If your company does not own it on the internet, everything in this guide still works on the LAN (your AD DNS answers for it internally), but office PCs cannot reach the real public mipl.com website and public certificate authorities will not issue certificates for it. This guide uses your own internal CA, so that is fine. Do not rename the AD domain.

2. How the pieces fit together

Architecture

```

Domain PC ---(Kerberos ticket, no password prompt)---+
                                                    v
Workgroup PC ---(AD username + password, once)---> Keycloak  https://sso.mipl.com
                                                    |   ^
LDAPS 636 |   | stores its config in SQL Server
                                                    v   |
                                                    Active Directory (users, passwords, APP-* groups)

Keycloak ---(OpenID Connect token: username, groups)---> ERP (PM2) / HR (XAMPP) / QMS (IIS) ...
                                                         each app keeps its OWN permissions + DB

```

Component	What it does	Cost
Active Directory	Single source of users, passwords, lock-outs and app-access groups (APP-*). You manage people only here.	Already licensed
LDAP / LDAPS	The protocol Keycloak uses to read AD users and groups and to check passwords. LDAPS = LDAP over TLS on port 636.	Built into AD
Kerberos	Windows' own login protocol. Lets a domain PC prove who is logged in without typing a password (via SPNEGO in the browser).	Built into AD
Keycloak	The SSO server. Talks LDAP/Kerberos to AD on one side and OpenID Connect (OIDC) to your apps on the other.	Free, open source (Apache 2.0)
AD Certificate Services	Your internal certificate authority. Issues HTTPS certificates that all domain PCs trust automatically.	Built into Windows Server

Rule that keeps this manageable: Keycloak/AD decide *who* the user is and *which apps* they may open. What they can do *inside* an app (modules, approve, edit, delete) stays in that app's own database, exactly as today. Nothing in SSO touches the apps' MS SQL / MySQL / PostgreSQL data.

3. Prerequisites checklist

#	Requirement	How to check
1	A Windows Server (VM is fine) for Keycloak: 4 vCPU, 8 GB RAM, 40 GB disk, domain-joined , static IP. Computer name must not be SSO (e.g. SRV-KC01).	hostname, ipconfig /all
2	Port 443 free on that server (no IIS/Apache on it).	netstat -ano findstr :443 returns nothing
3	AD CS Enterprise CA installed in the domain (needed for LDAPS and HTTPS certificates).	certutil -config - -ping lists your CA
4	SQL Server reachable from the Keycloak server, TCP/IP enabled, Mixed Mode authentication.	Test-NetConnection SQLSRV01 -Port 1433
5	All servers and PCs keep time within 5 minutes of the DC (Kerberos fails otherwise).	w32tm /query /status (Source = a DC)
6	You have Domain Admin rights (for service accounts, SPN, GPO) and local admin on the Keycloak server.	whoami /groups
7	Files downloaded: Keycloak 26.x zip (keycloak.org/downloads), Temurin JDK 21 MSI (adoptium.net), NSSM 2.24 (nssm.cc).	-

IMPORTANT If AD CS is not installed yet, install the **Active Directory Certificate Services** role as an **Enterprise Root CA** on a dedicated server (not on the Keycloak server) before Phase 2. An Enterprise CA automatically publishes its root certificate to every domain PC and gives DCs the certificate they need for LDAPS.

4. Phase 1 - Prepare Active Directory

Run on a domain controller (or any PC with RSAT) as Domain Admin. Appendix A contains one PowerShell script that does 4.1 and 4.2 in one go; the manual steps are shown here so you know what it does.

4.1 Create the OUs and app-access groups

PowerShell (admin) on DC

```
Import-Module ActiveDirectory
$dn = (Get-ADDomain).DistinguishedName # -> DC=mipl,DC=com
New-ADOrganizationalUnit -Name "Service Accounts" -Path $dn
New-ADOrganizationalUnit -Name "App Access" -Path $dn
foreach ($g in "APP-ERP","APP-HR","APP-QMS") {
    New-ADGroup -Name $g -GroupScope Global -GroupCategory Security -Path "OU=App Access,$dn"
}
```

Add users to a group to give them access to that app. Nested groups (e.g. a department group inside APP-ERP) are supported by the mapper configured in Phase 4.

4.2 Create the two service accounts

Account	Purpose	Settings
svc-keycloak	Keycloak reads users/groups from AD with it (LDAP bind).	Password never expires, cannot change password, no admin rights.
svc-kc-http	Owens the Kerberos SPN for sso.mipl.com.	Same as above plus Account tab: tick This account supports Kerberos AES 256 bit encryption .

PowerShell (admin) on DC

```
$ou = "OU=Service Accounts,$((Get-ADDomain).DistinguishedName)"
New-ADUser -Name svc-keycloak -SamAccountName svc-keycloak -UserPrincipalName svc-keycloak@mipl.com `
    -Path $ou -AccountPassword (Read-Host "Password for svc-keycloak" -AsSecureString) `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true
New-ADUser -Name svc-kc-http -SamAccountName svc-kc-http -UserPrincipalName svc-kc-http@mipl.com `
    -Path $ou -AccountPassword (Read-Host "Password for svc-kc-http" -AsSecureString) `
    -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true `
    -KerberosEncryptionType AES256
```

IMPORTANT Use two **different** accounts. Never put the HTTP SPN on the LDAP bind account or on the Keycloak server's computer account.

4.3 Create the DNS records

In **DNS Manager** on the DC, zone **mipl.com**, create **A (Host)** records, not CNAMEs (Kerberos resolves the name to find the SPN; a CNAME makes the browser ask for the wrong SPN):

Name	Type	Points to
sso	A	IP of SRV-KC01 (the Keycloak server)
portal	A	IP of the server hosting the app launcher (later)
erp, hr, ...	A	IP of each application server

4.4 Check time synchronisation

Command Prompt

```
w32tm /query /status          :: run on SRV-KC01 and on a client PC
w32tm /resync                 :: if 'Source' is 'Local CMOS Clock' or the offset is large
```

CHECK Phase 1 is done when: **(a)** `Get-ADUser svc-kc-http -Properties KerberosEncryptionType` shows AES256; **(b)** `nslookup sso.mipl.com` from a PC returns the Keycloak server IP with no 'Aliases' line; **(c)** time offset is under a few seconds.

5. Phase 2 - Certificates (AD CS)

Browsers, Keycloak and the apps must all use HTTPS with certificates from your internal CA. Domain PCs trust the CA automatically; workgroup PCs are handled in Phase 7.

5.1 Confirm the domain controller supports LDAPS

An Enterprise CA automatically gives every DC a certificate. Test it from SRV-KC01:

1. Run `ldp.exe` (installed with RSAT AD DS tools).
2. **Connection → Connect.** Server: `dc01.mipl.com`, Port: 636, tick **SSL**. OK.
3. Success looks like Established connection to `dc01.mipl.com` followed by the RootDSE attributes.

IMPORTANT If it fails: on the DC open `certlm.msc` → Personal → Certificates and confirm a certificate issued by your CA with purpose **Server Authentication** and the DC's FQDN exists. If missing, run `certutil -pulse` on the DC (or reboot it) and retest. Do not continue until LDAPS works: plain LDAP (389) with simple bind is blocked on DCs that enforce LDAP signing.

5.2 Create a Web Server certificate template (once)

1. On the CA server open `certsrv.msc`, right-click **Certificate Templates → Manage**.
2. Right-click **Web Server → Duplicate Template**.
3. General: name it **MIPL Web Server**, validity 2 years.
4. Request Handling: tick **Allow private key to be exported**.
5. Security: give **Domain Computers** (or your server admins group) **Read** and **Enroll**.
6. Back in `certsrv`: **Certificate Templates → New → Certificate Template to Issue → MIPL Web Server**.

5.3 Request the certificate for sso.mipl.com

1. On SRV-KC01 open `certlm.msc` (Local Computer). **Personal → All Tasks → Request New Certificate**.
2. Select **MIPL Web Server** and click the link *More information is required*.
3. Subject name: Type **Common name** = `sso.mipl.com`. Alternative name: Type **DNS** = `sso.mipl.com`. Add both, OK, **Enroll**.
4. Right-click the new certificate → **All Tasks → Export → Yes, export the private key → PFX**, tick **Include all certificates in the certification path** → set a password → save as `C:\keycloak\conf\certs\sso.mipl.com.pfx`.

IMPORTANT The DNS entry in the Subject Alternative Name is mandatory. Chrome and Edge ignore the Common Name; without the SAN every browser shows a certificate error.

5.4 Export the root CA certificate

1. In certlm.msc → **Trusted Root Certification Authorities** → **Certificates**, find your CA (e.g. *mipl-CA-ROOT*).
2. Export → **Base-64 encoded X.509 (.CER)** → save as C:\keycloak\conf\certs\mipl-root-ca.pem (the .pem extension matters for Keycloak).
3. Keep a copy as mipl-root-ca.cer on a share for workgroup PCs and app servers (Phases 6 and 7).

CHECK You have sso.mipl.com.pfx and mipl-root-ca.pem in C:\keycloak\conf\certs, and ldp.exe connects to dc01.mipl.com:636 with SSL.

6. Phase 3 - Install Keycloak

6.1 Install Java 21

Run the Temurin JDK 21 MSI on SRV-KC01. In the installer enable **Set JAVA_HOME variable** and **Add to PATH**. Open a **new** Command Prompt and check:

Command Prompt

```
java -version          :: must show version "21..."
echo %JAVA_HOME%       :: e.g. C:\Program Files\Eclipse Adoptium\jdk-21.0.8.9-hotspot
```

6.2 Create the SQL Server database

SQL Server Management Studio

```
CREATE DATABASE keycloak;
GO
CREATE LOGIN keycloak_user WITH PASSWORD = 'Use-A-Strong-Password-Here', CHECK_POLICY = ON;
GO
USE keycloak;
CREATE USER keycloak_user FOR LOGIN keycloak_user;
ALTER ROLE db_owner ADD MEMBER keycloak_user;
GO
```

NOTE SQL Server must allow **SQL Server and Windows Authentication mode** and have **TCP/IP enabled** (SQL Server Configuration Manager), and port 1433 must be open from SRV-KC01. Keycloak creates all its tables on first start.

6.3 Extract Keycloak

Extract the zip so that the folder is exactly C:\keycloak (it must contain bin, conf, lib). Create C:\keycloak\conf\certs if not already there and place the two files from Phase 2 in it.

6.4 Configure keycloak.conf

Replace the contents of C:\keycloak\conf\keycloak.conf with:

C:\keycloak\conf\keycloak.conf

```
# ----- Database -----
db=mssql
db-url=jdbc:sqlserver://SQLSRV01:1433;databaseName=keycloak;encrypt=true;trustServerCertificate=true
db-username=keycloak_user
db-password=Use-A-Strong-Password-Here

# ----- Hostname and HTTPS -----
hostname=https://sso.mipl.com
```

C:\keycloak\conf\keycloak.conf

```
https-port=443
http-enabled=false
https-key-store-file=C:/keycloak/conf/certs/sso.mipl.com.pfx
https-key-store-password=Your-PFX-Password
https-key-store-type=PKCS12

# ----- Trust the internal CA (required for ldaps://) -----
truststore-paths=C:/keycloak/conf/certs/mipl-root-ca.pem

# ----- Health and logging -----
health-enabled=true
log=console,file
log-file=C:/keycloak/data/log/keycloak.log
```

IMPORTANT Use forward slashes (/) in every path in **keycloak.conf**. It is a Java properties file: a backslash is an escape character, so C:\keycloak\conf is silently read as a wrong path. For a named SQL instance use jdbc:sqlserver://SQLSRV01;instanceName=SQLEXPRESS;databaseName=keycloak;... (SQL Browser service must be running), never SQLSRV01\SQLEXPRESS. Restrict this file's NTFS permissions to Administrators and SYSTEM because it contains passwords.

6.5 Build and first start (creates the temporary admin)

Command Prompt (Run as administrator)

```
cd /d C:\keycloak\bin
set KC_BOOTSTRAP_ADMIN_USERNAME=tempadmin
set KC_BOOTSTRAP_ADMIN_PASSWORD=Temp-Strong-Password-1
kc.bat build
kc.bat start --optimized
```

Wait for the line Keycloak 26.x.x on JVM ... started in ...s. Listening on: https://0.0.0.0:443. The first start takes 1-2 minutes while it creates the database tables.

1. From another PC open <https://sso.mipl.com/admin> and log in as **tempadmin**.
2. Realm **master** → **Users** → **Add user**: create your permanent admin (e.g. kc-admin), set a password (Credentials tab, Temporary OFF).
3. **Role mapping** → **Assign role** → filter by realm roles → assign **admin**.
4. Log out, log in as the new admin, then delete **tempadmin**.
5. Stop Keycloak with **Ctrl+C** and close that Command Prompt (the bootstrap variables must not be reused).

NOTE Whenever you change a *build option* in keycloak.conf (db, health-enabled) you must run `kc.bat build` again before starting, otherwise Keycloak refuses to start with *build time options differ*. Runtime options (passwords, paths, hostname) only need a restart.

6.6 Run Keycloak as a Windows service (NSSM)

Copy `nssm.exe` (win64 folder of the NSSM zip) to C:\keycloak\nssm.exe, then:

Command Prompt (Run as administrator)

```
cd /d C:\keycloak
nssm install Keycloak C:\keycloak\bin\kc.bat
nssm set Keycloak AppParameters "start --optimized"
nssm set Keycloak AppDirectory C:\keycloak\bin
nssm set Keycloak AppEnvironmentExtra "JAVA_HOME=C:\Program Files\Eclipse Adoptium\jdk-21.0.8.9-hotspot"
nssm set Keycloak AppStdout C:\keycloak\data\log\service.log
nssm set Keycloak AppStderr C:\keycloak\data\log\service.log
```

Command Prompt (Run as administrator)

```
nssm set Keycloak Start SERVICE_AUTO_START
nssm start Keycloak
```

NOTE Use your exact JAVA_HOME path from step 6.1. Setting it in NSSM avoids the classic problem where a newly installed Java is not visible to services until the server reboots.

6.7 Firewall: LAN only

PowerShell (admin) on SRV-KC01

```
New-NetFirewallRule -DisplayName "Keycloak HTTPS (LAN only)" -Direction Inbound -Protocol TCP -
-LocalPort 443 -RemoteAddress 192.168.1.0/24 -Action Allow
```

Do **not** open port 9000 (management/health); it is for local checks only. Make sure the router has no port-forward to this server.

CHECK (a) `sc query Keycloak` shows RUNNING after a reboot of SRV-KC01; (b) on SRV-KC01, `curl -k https://localhost:9000/health/ready` returns "status": "UP"; (c) from a domain PC, `https://sso.mipl.com` opens with a **padlock and no warning**.

7. Phase 4 - Realm and LDAP (Active Directory) federation

7.1 Create the realm

Admin console → realm dropdown (top-left) → **Create realm** → Realm name `mipl` → Create. All users and apps go in this realm. Never use the **master** realm for users or apps.

7.2 Realm settings

Where (realm mipl)	Setting	Value
Realm settings → Login	User registration / Forgot password / Remember me	All OFF (AD owns passwords)
Realm settings → Sessions	SSO Session Idle / SSO Session Max	8 hours / 12 hours
Realm settings → Security defenses → Brute force detection	Mode	Lockout temporarily (AD's own lockout policy still applies too)
Realm settings → General	Frontend URL	Leave empty (hostname comes from keycloak.conf)

7.3 Add the LDAP provider

User federation → Add LDAP providers. Fill in every field below; fields not listed keep their default.

Section / field	Value	Why
UI display name	<code>mipl-ad</code>	
Vendor	Active Directory	Pre-fills AD defaults
Connection URL	<code>ldaps://dc01.mipl.com:636</code> (2 DCs: <code>ldaps://dc01.mipl.com:636</code> <code>ldaps://dc02.mipl.com:636</code>)	Must be the DC's FQDN, not an IP, or TLS hostname check fails. Space-separated = failover
Enable StartTLS	OFF	Already TLS via ldaps

Section / field	Value	Why
Use Truststore SPI	Always	Uses truststore-paths from keycloak.conf
Connection pooling	ON	
Bind type / Bind DN	simple / CN=svc-keycloak,OU=Service Accounts,DC=mipl,DC=com	
Bind credentials	svc-keycloak password	Click Test connection , then Test authentication
Edit mode	READ_ONLY	Keycloak never writes to AD
Users DN	DC=mipl,DC=com	Whole domain; filter below narrows it
Username LDAP attribute	sAMAccountName	Default is cn (full name). Must change before first sync
RDN LDAP attribute	cn	
UUID LDAP attribute	objectGUID	
User object classes	person, organizationalPerson, user	
User LDAP filter	(&(objectCategory=person)(objectClass=user)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))	Real users only, skips disabled accounts
Search scope	Subtree	
Pagination	ON	AD returns max 1000 results without it
Import users / Sync registrations	ON / OFF	
Kerberos integration	Leave OFF for now	Enabled in Phase 5
Periodic full sync	ON, every 86400 s	Once a day
Periodic changed users sync	ON, every 300 s	Every 5 minutes
Cache policy	DEFAULT	

NOTE Both **Test connection** and **Test authentication** must show success before you click Save. Passwords are always checked live against AD at login, so a disabled AD account or a changed password takes effect immediately, not only after the next sync.

7.4 Check the default mappers

Open the provider → **Mappers** tab. Keycloak created these automatically; verify them:

Mapper	LDAP attribute	Note
username	sAMAccountName	Must match the Username LDAP attribute above
first name / last name	givenName / sn	
email	mail	May be empty for some AD users; apps must not rely on it
MSAD account controls	-	Keep it: handles disabled, locked and must-change-password states

Mapper	LDAP attribute	Note
Kerberos principal attribute mapper (if listed)	userPrincipalName	Only correct if every user's UPN ends in @mipl.com. See 8.5

7.5 Add the AD group mapper

Mappers tab → **Add mapper** → Mapper type **group-ldap-mapper**:

Field	Value
Name	app-access-groups
LDAP Groups DN	OU=App Access,DC=mipl,DC=com
Group Name LDAP Attribute / Group Object Classes	cn / group
Preserve Group Inheritance	OFF
Ignore Missing Groups	ON
Membership LDAP Attribute / Membership Attribute Type	member / DN
Mode	READ_ONLY
User Groups Retrieve Strategy	LOAD_GROUPS_BY_MEMBER_ATTRIBUTE_RECURSIVELY (supports nested AD groups)
Drop non-existing groups during sync	OFF

Save, then on the mapper page choose **Action** → **Sync LDAP groups to Keycloak**.

7.6 Sync and test

1. Provider page → **Action** → **Sync all users**. The message shows how many users were imported.
2. **Users** menu → search *. Usernames must be login names (e.g. chandan.singh), not full names.
3. Open a user in APP-ERP → **Groups** tab shows APP-ERP.
4. Open <https://sso.mipl.com/realms/mipl/account> in a private window and log in with an AD username and password.

CHECK Users appear with login names, groups show on the user, and an AD user can log in to the account page with their Windows password. If usernames are full names, see Troubleshooting row 'Usernames are full names'.

8. Phase 5 - Kerberos (automatic login on domain PCs)

Do this only after Phase 4 works. If Kerberos ever breaks, users simply get the normal login form, so nothing stops working.

8.1 Register the SPN

Command Prompt (admin) on DC

```
setspn -S HTTP/sso.mipl.com MIPL\svc-kc-http
setspn -Q HTTP/sso.mipl.com           :: must list ONLY svc-kc-http
setspn -X                             :: must end with "found 0 group of duplicate SPNs"
```

8.2 Create the keytab

Command Prompt (admin) on DC

```
ktpass /out C:\temp\sso.keytab /princ HTTP/sso.mipl.com@MIPL.COM /mapuser MIPL\svc-kc-http ^
/pass * /ptype KRB5_NT_PRINCIPAL /crypto AES256-SHA1
```

- Type the svc-kc-http password when prompted (ktpass sets it on the account, so the keytab and AD always match).
- Hostname lowercase, realm UPPERCASE, exactly as shown.
- A warning about the account's UPN being changed is normal.
- Copy sso.keytab to C:\keycloak\conf\sso.keytab on SRV-KC01, then delete it from C:\temp. Set NTFS permissions to Administrators and SYSTEM only: it works like a password.

8.3 Create krb5.ini on the Keycloak server

C:\Windows\krb5.ini (add a second 'kdc = dc02.mipl.com' line if you have 2 DCs)

```
[libdefaults]
    default_realm = MIPL.COM
    default_tkt_enctypes = aes256-cts-hmac-sha1-96
    default_tgs_enctypes = aes256-cts-hmac-sha1-96
    permitted_enctypes = aes256-cts-hmac-sha1-96

[realms]
    MIPL.COM = {
        kdc = dc01.mipl.com
    }

[domain_realm]
    .mipl.com = MIPL.COM
    mipl.com = MIPL.COM
```

8.4 Verify the keytab before touching Keycloak

Use Java's own Kerberos tools (full path, because Windows also has a different klist.exe):

Command Prompt on SRV-KC01

```
"%JAVA_HOME%\bin\klist" -k -t C:\keycloak\conf\sso.keytab
:: expect: HTTP/sso.mipl.com@MIPL.COM

"%JAVA_HOME%\bin\kinit" -k -t C:\keycloak\conf\sso.keytab HTTP/sso.mipl.com@MIPL.COM
:: expect: "New ticket is stored in cache file ..."
```

IMPORTANT If kinit fails here, Keycloak will fail too. Fix the keytab first (Troubleshooting section) instead of changing Keycloak settings. Afterwards delete the test ticket cache file it names.

8.5 Enable Kerberos in the LDAP provider

User federation → mipl-ad → section Kerberos integration:

Field	Value
Allow Kerberos authentication	ON
Kerberos realm	MIPL.COM
Server principal	HTTP/sso.mipl.com@MIPL.COM
Key tab	C:/keycloak/conf/sso.keytab

Field	Value
Kerberos principal attribute	Leave empty , unless every user's userPrincipalName ends with @mipl.com (then userPrincipalName is fine). Empty = username + @MIPL.COM, which always matches sAMAccountName.
Use Kerberos for password authentication	OFF (LDAP checks passwords typed in the form)
Debug	OFF (turn ON temporarily only when troubleshooting)

Save, then restart the service: `nssm restart Keycloak`.

8.6 Check the browser flow

Authentication → Flows → browser. The **Kerberos** step must be **Alternative** (Keycloak usually sets this automatically when you save 8.5).

IMPORTANT Never set Kerberos to **Required**: workgroup PCs, phones and local accounts cannot do Kerberos and would be locked out. **Alternative** = try Kerberos silently, otherwise show the login form.

8.7 Group Policy: let browsers send Kerberos to sso.mipl.com

1. **Group Policy Management** → edit a GPO linked to the OU(s) containing your domain computers.
2. **Computer Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Security Page → Site to Zone Assignment List.**
3. Enabled → Show → Value name `https://sso.mipl.com`, Value 1 (Local intranet).
4. Optional, for Chrome/Edge with their ADMX templates installed: policy **AuthServerAllowlist** = `sso.mipl.com`.
5. On a test PC: `gpupdate /force`, then log off and on.

NOTE If a *Site to Zone Assignment List* GPO already exists, add the entry to that one. Two GPOs setting the same list overwrite each other. Edge and Chrome read this Windows setting; Firefox needs `network.negotiate-auth.trusted-uris = https://sso.mipl.com` (Firefox policy or `about:config`).

8.8 Test Kerberos

Command Prompt on a domain PC (normal user)

```
klist purge :: on a domain PC, logged in as a domain user
start msedge https://sso.mipl.com/realms/mipl/account
klist | findstr /i "HTTP/sso.mipl.com" :: a ticket for HTTP/sso.mipl.com must be listed
```

CHECK On a domain PC the account page opens **without a login form**, and `klist` shows `HTTP/sso.mipl.com @ MIPL.COM`. On a workgroup PC the same URL shows the login form.

9. Phase 6 - Register applications (OIDC clients)

9.1 Create the 'groups' client scope (once, before the first client)

1. **Client scopes** → **Create client scope**: Name groups, Type **Default**, Protocol **OpenID Connect**, Include in token scope ON → Save.
2. **Mappers** → **Configure a new mapper** → **Group Membership**: Name groups, Token Claim Name groups, **Full group path OFF**, Add to ID token ON, Add to access token ON, Add to userinfo ON → Save.

Type **Default** means every client created afterwards gets it automatically. For a client created earlier: client → **Client scopes** tab → **Add client scope** → **groups** → **Default**.

9.2 Create one client per application (example: ERP)

Wizard step	Field	Value
General settings	Client type / Client ID / Name	OpenID Connect / erp / SAP ERP
Capability config	Client authentication	ON (confidential client with secret)
	Standard flow / Direct access grants	ON / OFF
	Implicit flow / Service accounts / Device grant	OFF / OFF / OFF
	PKCE Method (if shown)	S256
Login settings	Root URL / Home URL	https://erp.mipl.com
	Valid redirect URIs	https://erp.mipl.com/auth/callback (exact path your app uses)
	Valid post logout redirect URIs	https://erp.mipl.com/*
	Web origins	https://erp.mipl.com

After saving: **Credentials** tab → copy the **Client secret** and give it to the app's developer through your password vault. Repeat for each app (hr, qms, portal).

IMPORTANT Do not use wildcards like https://* or * in Valid redirect URIs. The value must match what the app sends, character for character, or login ends with *Invalid parameter: redirect_uri*.

9.3 What to give each app developer

Setting	Value
Issuer / Discovery URL	https://sso.mipl.com/realms/mipl https://sso.mipl.com/realms/mipl/.well-known/openid-configuration
Client ID / Client secret	erp / (from Credentials tab)
Redirect URI	https://erp.mipl.com/auth/callback
Scopes	openid profile email
User identifier claim	preferred_username = AD login name, always lowercase in Keycloak. Compare case-insensitively with the app's own users table.
Access check	Reject the login unless the groups claim contains APP-ERP.
Logout	Redirect to end_session_endpoint (from discovery) with id_token_hint and post_logout_redirect_uri.

9.4 Make every app server trust the internal CA

Apps call Keycloak over HTTPS from the server side, so each app runtime must trust `mip1-root-ca`, otherwise the login callback fails with a certificate error.

App platform	What to do
Node.js / PM2	Set environment variable <code>NODE_EXTRA_CA_CERTS=C:\certs\mip1-root-ca.pem</code> in the PM2 ecosystem file (env section), then <code>pm2 restart <app> --update-env</code> . It is read only at process start.
PHP / XAMPP	Append the contents of <code>mip1-root-ca.pem</code> to the CA bundle named in <code>php.ini</code> by <code>curl.cainfo</code> and <code>openssl.cafile</code> (create them pointing to one bundle file if empty). Restart Apache.
.NET / IIS	Nothing if the server is domain-joined (the root CA arrives by Group Policy). Otherwise import the <code>.cer</code> into Local Computer → Trusted Root.
Any	Each app must itself be served over HTTPS on its own name (e.g. <code>erp.mipl.com</code>), with a certificate from the MIPL Web Server template.

9.5 Rules for app-side integration

- Keep each app's own permissions/roles tables unchanged. SSO only replaces the password check.
- Link users by `preferred_username` (store it, or Keycloak's sub, in a new `sso_subject` column). Do not rely on email.
- A user in APP-ERP who has no user row in the app gets a clear 'Not set up in ERP, contact admin' page, not an automatic admin account.
- Keep one local break-glass admin login per app for when Keycloak is down.
- Always check the groups claim in the app. Hiding an app tile in a portal is not security.

10. Phase 7 - Workgroup PCs

Workgroup PCs are not domain members, so they never receive Group Policy. They still get full SSO: the user types their AD username and password once in the Keycloak form, and every app opens without login until the SSO session ends. Each workgroup PC needs two things:

Need	Why	How
AD DNS server as DNS	Otherwise <code>sso.mipl.com</code> and app names do not resolve	Best: DHCP scope option 006 = AD DNS IP. Or per PC (script in Appendix B).
Root CA trusted	Otherwise every app shows a certificate warning	<code>certutil -addstore -f Root mip1-root-ca.cer</code> (admin)

- Do **not** add `sso.mipl.com` to the Local intranet zone on workgroup PCs; that makes the browser show a Windows password pop-up instead of the Keycloak form.
- Users on shared PCs must use the portal/app **Logout** button (it ends the Keycloak session for all apps).
- Every person needs an AD user account even though their PC is not joined to the domain.

11. Final acceptance test

#	Test	Expected result
1	Domain PC, domain user in APP-ERP, opens https://erp.mipl.com	Logged in, no password asked
2	Same user opens a second app they are in (e.g. HR)	Logged in immediately
3	Domain user NOT in APP-ERP opens ERP	Access denied page from the app
4	Workgroup PC opens ERP	Keycloak form; AD username + password works; padlock, no warnings
5	Workgroup PC, after step 4, opens HR	Logged in without password
6	Wrong password 5+ times	Temporary lockout message (Keycloak and/or AD policy)
7	Admin disables the user in AD, user tries a new login	Login refused
8	Admin removes user from APP-ERP, user logs in again	ERP refuses; other apps still work
9	Logout from portal/app on a shared PC, then open any app	Login form shown again
10	Reboot SRV-KC01	Keycloak service starts by itself; test 1 passes again
11	From outside the LAN (mobile data)	sso.mipl.com not reachable

NOTE Test 7 note: a user who was already logged in keeps their current session until it expires (SSO Session Idle). To cut them off immediately: realm mipl → **Users** → user → **Sessions** → **Sign out**.

12. Troubleshooting

Logs: C:\keycloak\data\log\keycloak.log and service.log. For Kerberos problems set **Debug ON** in the provider's Kerberos section temporarily, reproduce, then read the log.

Symptom / log message	Cause	Fix
Service stops at start: <i>Unable to connect / Login failed for user (SQL)</i>	SQL TCP/IP off, Windows-only auth, firewall 1433, wrong instance syntax	Enable TCP/IP + Mixed mode, open 1433, use ;instanceName= form, restart
<i>The following build time options have values that differ</i>	keycloak.conf build option changed	kc.bat build then nssm restart Keycloak
Keycloak cannot find the PFX or truststore	Backslashes in keycloak.conf	Use forward slashes in all paths
<i>Address already in use on 443</i>	IIS/Apache/another app on 443	Move that app or use https-port=8443 (URL becomes https://sso.mipl.com:8443 everywhere)
Browser certificate warning on sso.mipl.com	No SAN, PFX without chain, or root CA not trusted on that PC	Re-issue with DNS SAN (5.3), export with chain, trust root CA (Phase 7)
LDAP Test connection: <i>PKIX path building failed</i>	Keycloak does not trust the DC certificate	Check truststore-paths file is Base-64 .pem, restart Keycloak
LDAP Test connection: <i>No subject alternative DNS name matching</i>	URL uses IP or short name	Use the DC FQDN exactly as in its certificate
LDAP Test connection: timeout / refused	DC has no LDAPS certificate or 636 blocked	Test with ldp.exe (5.1)

Symptom / log message	Cause	Fix
Test authentication: LDAP error 49 with <i>data 52e / 775 / 532</i>	Bad bind DN or password / account locked / password expired	Correct svc-keycloak details or unlock it
Only 1000 users imported	Pagination OFF	Turn Pagination ON, Sync all users
Username are full names	Username LDAP attribute left as cn	Set sAMAccountName (field + username mapper), Action → Remove imported users , then Sync all users
Token has no groups claim	Scope not on the client, token toggles off, group mapper not synced	9.1 + client's Client scopes tab; Sync LDAP groups (7.5)
Groups look like /APP-ERP	Full group path ON	Turn it OFF in the groups mapper
Domain PC still shows the login form	Site opened by IP/short name, zone GPO not applied, local (non-domain) login, no HTTP ticket in klist	Use https://sso.mipl.com; gpupdate /force; log in as a domain user; check SPN (8.1)
<i>Checksum failed / KRB_AP_ERR_MODIFIED</i>	Keytab does not match svc-kc-http password, or SPN on another account	Check setspn -Q, rerun ktpass (8.2), replace keytab, restart
<i>Encryption type ... is not supported/enabled</i>	AES not enabled for the account or client ticket is RC4	Tick AES 256 on svc-kc-http, rerun ktpass, client klist purge + log off/on
<i>Clock skew too great</i>	Time difference over 5 minutes	w32tm /resync on the server/PC
Kerberos accepted but user not found	Kerberos principal attribute set to userPrincipalName but UPN suffix is not @mipl.com	Clear the field (8.5)
Workgroup PC: <i>site can't be reached</i>	PC not using AD DNS	Phase 7 DNS step; nslookup sso.mipl.com
Workgroup PC gets a Windows password pop-up	sso.mipl.com in its Intranet zone	Remove it from the zone
App: <i>Invalid parameter: redirect_uri</i>	Redirect URI mismatch	Make 9.2 value identical to the app's
Node app: <i>self-signed certificate in certificate chain / unable to verify the first certificate</i>	Node does not trust the internal CA	NODE_EXTRA_CA_CERTS (9.4), restart with --update-env
App: <i>issuer mismatch / invalid token</i>	App configured with IP, port or http URL	Use exactly https://sso.mipl.com/realms/mipl

13. Operations and maintenance

Task	How
Give a user access to an app	Add them to the app's AD group (APP-ERP ...). Effective at their next login, no Keycloak change. Their permissions inside the app are still set in the app.
Employee leaves	Disable the AD account. New logins are refused at once; to end open sessions use Users → Sessions → Sign out.
Add a new application	Create AD group APP-XXX (OU=App Access), Sync LDAP groups, create a client (9.2), give the developer the values in 9.3.
svc-kc-http password changed	Kerberos stops working until you rerun ktpass (8.2), replace the keytab and restart Keycloak. Best: never change it (Password never expires).
svc-keycloak password changed	Update Bind credentials in the LDAP provider immediately.
Certificate renewal (every 2 years)	Re-request sso.mipl.com (5.3), replace the PFX with the same name and password, nssm restart Keycloak. Put a reminder 30 days before expiry.

Task	How
Backups (daily)	SQL database keycloak and folder C:\keycloak\conf (conf, certs, keytab) to a secured location.
Upgrade Keycloak	Back up the database, stop the service, extract the new version to a new folder, copy conf over, kc.bat build, point NSSM to the new folder, start. The database is migrated automatically.
Remote access later	Use a VPN so remote users are on the LAN. Do not port-forward Keycloak to the internet.

Appendix A - Domain controller setup script

Run in an **elevated PowerShell on a domain controller**. It is safe to run twice (it skips what already exists). It prompts for the two service-account passwords; ktpass prompts for the svc-kc-http password once more.

Setup-MiplSso.ps1

```
# MIPL SSO - AD preparation (OUs, groups, service accounts, SPN, keytab)
Import-Module ActiveDirectory
$ErrorActionPreference = "Stop"
$dn      = (Get-ADDomain).DistinguishedName      # DC=mipl,DC=com
$svcOU   = "OU=Service Accounts,$dn"
$appOU   = "OU=App Access,$dn"
$groups  = "APP-ERP","APP-HR","APP-QMS"          # add one per application

foreach ($ou in "Service Accounts","App Access") {
    if (-not (Get-ADOrganizationalUnit -Filter "Name -eq '$ou'" -SearchBase $dn -SearchScope OneLevel)) {
        New-ADOrganizationalUnit -Name $ou -Path $dn; Write-Host "Created OU $ou"
    }
}

foreach ($g in $groups) {
    if (-not (Get-ADGroup -Filter "Name -eq '$g'")) {
        New-ADGroup -Name $g -GroupScope Global -GroupCategory Security -Path $appOU
        Write-Host "Created group $g"
    }
}

function New-SvcAccount($name, [switch]$Aes) {
    if (Get-ADUser -Filter "SamAccountName -eq '$name'") { Write-Host "$name exists"; return }
    $p = @{ Name=$name; SamAccountName=$name; UserPrincipalName="$name@mipl.com"; Path=$svcOU
        AccountPassword=(Read-Host "Password for $name" -AsSecureString)
        Enabled=$true; PasswordNeverExpires=$true; CannotChangePassword=$true }
    if ($Aes) { $p.KerberosEncryptionType = "AES256" }
    New-ADUser @p; Write-Host "Created $name"
}

New-SvcAccount "svc-keycloak"
New-SvcAccount "svc-kc-http" -Aes

setspn -S HTTP/sso.mipl.com MIPL\svc-kc-http
setspn -X

New-Item -ItemType Directory -Force C:\temp | Out-Null
ktpass /out C:\temp\sso.keytab /princ HTTP/sso.mipl.com@MIPL.COM /mapuser MIPL\svc-kc-http `
    /pass * /ptype KRB5_NT_PRINCIPAL /crypto AES256-SHA1

Get-ADUser svc-kc-http -Properties KerberosEncryptionType,ServicePrincipalNames |
    Format-List Name,KerberosEncryptionType,ServicePrincipalNames
Write-Host "Copy C:\temp\sso.keytab to SRV-KC01 C:\keycloak\conf\ and delete it here."
```

Appendix B - Workgroup PC setup script

Run in an **elevated PowerShell on each workgroup PC**. Skip the DNS part if your DHCP server already hands out the AD DNS server. Put `mipl-root-ca.cer` on a share or USB stick first.

Prepare-WorkgroupPc.ps1

```
# MIPL SSO - workgroup PC preparation
$dnsServer = "192.168.1.10"           # AD DNS server IP (example - change it)
$rootCa    = "\\fileserver\it\mipl-root-ca.cer" # path to the exported root CA (change it)

# 1. Use AD DNS on the active network adapter(s)
Get-NetAdapter | Where-Object Status -eq "Up" | ForEach-Object {
    Set-DnsClientServerAddress -InterfaceIndex $_.ifIndex -ServerAddresses $dnsServer
    Set-DnsClient -InterfaceIndex $_.ifIndex -ConnectionSpecificSuffix "mipl.com"
}
Clear-DnsClientCache

# 2. Trust the MIPL root CA for the whole machine
Import-Certificate -FilePath $rootCa -CertStoreLocation Cert:\LocalMachine\Root | Out-Null

# 3. Checks
Resolve-DnsName sso.mipl.com
(Invoke-WebRequest https://sso.mipl.com/realms/mipl/.well-known/openid-configuration `
    -UseBasicParsing).StatusCode # expect 200 with no certificate error
```

Appendix C - Build order at a glance

Phase	Work	Done when
1 AD	OUs, APP-* groups, svc-keycloak, svc-kc-http (AES256), DNS A records, time	nslookup sso.mipl.com returns the server IP with no alias
2 Certificates	LDAPS on DC, MIPL Web Server template, sso.mipl.com PFX, root CA .pem	ldp.exe connects to DC on 636 with SSL
3 Keycloak	Java 21, SQL database, keycloak.conf, build, admin, NSSM service, firewall	https://sso.mipl.com opens with padlock after reboot
4 LDAP	Realm mipl, LDAP provider, mappers, group mapper, sync	AD user logs in to the account page with Windows password
5 Kerberos	SPN, keytab, krb5.ini, kinit test, enable in provider, browser flow, GPO	Domain PC opens the account page with no form
6 Apps	groups client scope, one client per app, CA trust on app servers	Test 1-3 of the acceptance test pass
7 Workgroup	DNS + root CA on each workgroup PC	Tests 4-5 pass