Directory Integration (LDAP / Active Directory)

Information Request — We360 On-Premise Deployment

Prepared for:		**Date:**	
Your We360 contact:		**Return by:**	

Purpose. We are enabling directory-based sign-in — and, optionally, silent Single Sign-On (SSO) — for your users in your on-premise We360 deployment. To configure this on our side, we need some information about your directory environment. Please complete the 'Your value' column in each table and return this document to your We360 contact.

Before you start

- You do **not** need to install or change anything yet — this is an information-gathering step.
- **Do not put passwords, secrets, or key files in this document.** Items marked **(secure)** must be sent through the secure channel we provide separately.
- If a field doesn't apply or you're unsure, leave it blank and add a note — we'll follow up.

1. Directory server

What kind of directory you run and how we reach it over the network.

Item	What it means / why we need it	Your value
Directory type	Microsoft Active Directory, or another LDAP server (OpenLDAP, 389 DS, etc.). This determines how we read your users.	
Version	e.g. Windows Server 2019 AD, or OpenLDAP 2.6.	
Host name(s) (FQDN)	Fully-qualified hostname(s) of the directory / domain-controller servers we connect to, e.g. `dc1.corp.example.com`. List more than one if you have redundant controllers.	
Port	LDAP port — standard is **389** (plain) or **636** (LDAPS/TLS). We strongly prefer LDAPS.	
Encryption	Is the connection over **LDAPS (TLS)**, **StartTLS**, or plain?	
TLS / CA certificate (secure)	If LDAPS uses a certificate from a **private / internal CA**, we need the CA (root / intermediate) certificate so we can trust it. A public CA needs nothing.	

2. Service (bind) account

We connect to your directory using a dedicated **read-only** account to look up users. Please create this account (or nominate an existing one) with read access to the users in scope.

Item	What it means / why we need it	Your value
Bind account DN	The account's full distinguished name, e.g. `CN=svc-we360,OU=Service Accounts,DC=corp,DC=example,DC=com`.	

Item	What it means / why we need it	Your value
Bind account password (secure)	The account's password. Please set it to not expire, or tell us the rotation policy. Send securely — not in this document.	
Permissions	Confirm the account can **read** user objects and their attributes in the areas listed in section 3. No write access is required.	

3. Directory structure (where your users live)

So we search the right part of the tree and don't pull in the wrong accounts.

Item	What it means / why we need it	Your value
Base DN	The root of your directory, e.g. `DC=corp,DC=example,DC=com`.	
Users DN / OU	The specific container(s) holding the user accounts that should be able to log in, e.g. `OU=Employees,DC=corp,DC=example,DC=com`.	
Scope / filtering	Should **all** users under that OU get access, or only a subset (e.g. members of a specific group)? If a group, give its name / DN.	
Multiple domains?	If more than one domain / forest has users who need access, list them — this may change the approach.	

4. User attributes

Which fields in your directory hold the login name, email, and name, so we map your users correctly.

Item	What it means / why we need it	Your value
Login username attribute	**What your users type as their username.** In AD this is usually `sAMAccountName` (e.g. `jdoe`) or `userPrincipalName` (e.g. `jdoe@corp.example.com`). Tell us which they'll use.	
Email attribute	The attribute holding the user's email (AD default `mail`). We use email as the primary identifier — please confirm your users **have email populated**.	
First / last name	Usually `givenName` and `sn`.	
Unique ID attribute	A stable, never-changing identifier so renames don't create duplicates. AD default `objectGUID`; OpenLDAP `entryUUID`.	

5. Kerberos / Single Sign-On (optional)

Complete this section **only** if you want users logged in automatically from their existing Windows domain session (no username / password prompt). Skip it if you only want directory username / password login.

Item	What it means / why we need it	Your value
Kerberos realm	Your Kerberos realm — normally your AD domain in UPPERCASE, e.g. `CORP.EXAMPLE.COM`.	

Item	What it means / why we need it	Your value
KDC host name(s)	The Key Distribution Center servers — normally your domain controllers, e.g. `dc1.corp.example.com`.	
Machines domain-joined?	Confirm end-user PCs are joined to this AD domain. Silent SSO only works if they are.	
Service account + SPN + keytab (secure)	We will run the login service at a hostname we will confirm with you. Your AD admin must register a Service Principal Name of the form `HTTP/<that-host>@REALM` and generate a **keytab** (AES256), then send us the keytab securely. We'll give you the exact hostname and the single command to run.	
Encryption types	Confirm the service account / domain supports **AES** (not RC4-only).	
Browser management	Silent SSO needs users' browsers configured to trust our login host. Can you push browser policy via **GPO / MDM** (Chrome / Edge / Firefox)? We'll supply the exact values.	

6. Network & environment

Connectivity and prerequisites between the We360 login service and your directory.

Item	What it means / why we need it	Your value
Firewall / connectivity	Confirm the We360 server can reach your directory on the LDAP(S) port (389 / 636) and, for SSO, the KDC on port **88** (TCP/UDP).	
DNS	Confirm the directory / KDC hostnames resolve from the We360 server.	
Time synchronization	Kerberos requires clocks within ~5 minutes. Confirm your servers and clients sync to NTP / AD time.	

7. Test accounts (optional)

Optional but recommended — so we can validate the integration end-to-end before rollout.

Item	What it means / why we need it	Your value
Test user(s) (secure)	1–2 non-critical accounts (username + password) we can use to verify login. Send credentials securely.	
Expected group / scope	Which group / OU these test users belong to, so we confirm scoping works.	

How to return this: fill in the 'Your value' column and send the document back to your We360 contact. For every item marked **(secure)** — passwords, certificates, keytab, test credentials — use the secure channel we provide. Do not email them or include them in this document.

We will handle separately: the exact login-service hostname, the SPN registration command, and the browser policy values. You do not need those to complete this form.