

EXHIBIT B · PRO.FILE 10.5

IT Prerequisites Checklist

Everything your IT team prepares before installation day, and the exact values Cre8tive needs back to connect PRO.FILE to your network, mail system, certificates and identity provider.

Accounts & access

Firewall ports

SSL certificates

E-mail via M365

Single sign-on

Dynamic Search

OVERVIEW

How this checklist works

Most installation delays come from one missing firewall rule, certificate or password. This checklist puts them all on the table in advance, so installation day is spent installing.

1 PREPARE

Your IT team provisions servers (see Exhibit A, the Hardware Guide), opens ports, issues certificates and sets up the mail relay and identity provider, following sections A–I.

2 RETURN VALUES

Fill in the **Values returned to Cre8tive** tables. Send secrets (passwords, client secrets, certificate keys) through a secure channel, **never in plain e-mail**.

3 WE CONFIGURE

Cre8tive installs PRO.FILE 10.5 and writes your values into `ProfileConfiguration.xml`, IIS and the ISI.CONTrol Panel, then tests each item with you.

Who does what

CUSTOMER IT your team **CRE8TIVE** we do it **JOINT** together, usually in a remote session

SECTION	TOPIC	PROD	TEST	LEAD
A	Service accounts, AD groups & access	Required	Required	CUSTOMER IT
B	Servers & operating system	Required	Required	CUSTOMER IT
C	Network, DNS & firewall ports	Required	Required	CUSTOMER IT
D	SSL certificates for IIS	Required	Required	JOINT
E	E-mail (Microsoft Graph or SMTP)	Required	Recommended	CUSTOMER IT
F	Single sign-on (Entra ID or ADFS)	Optional	Optional	JOINT
G	Dynamic Search server	Dedicated server	Co-hosted	JOINT
H	Reporting Services (SSRS)	Required	Required	JOINT
I	Antivirus, backup & licences	Required	Required	CUSTOMER IT
J	Summary of values & sign-off	One page to return		CUSTOMER IT

WHY SSL COMES FIRST IN 10.5

HTTPS on the AppServer is the foundation for three 10.5 features: **Dynamic Search** (browsers block the search web app over plain HTTP), **single sign-on** (external identity providers only work with the AppServer in SSL mode) and **secure remote access**. Please treat section D as a blocker for installation.

Environments, timeline and handover

The Cre8tive Standard Deployment Model: what we install, what we need from you to start, and what you receive at the end.

MAIN SYSTEM

Installed first, on the production hardware. It is the training and implementation system during the project. At go-live it is cleaned of non-production data and becomes **Production**.

TEST SYSTEM

Separate, isolated hardware. Deployed at go-live from a clean copy of Production, then used to prove every update, OS/SQL patch, CAD change or new function first.

ADDITIONAL SYSTEMS

DEV, PILOT or TRAINING: separate databases and vaults on the Main or Test infrastructure. Not in the standard budget; ask your Cre8tive project manager.

What Cre8tive needs to start

- ☐ Servers sized per **Exhibit A** with a licensed, patched Windows Server, plus the **Windows** and **SQL Server installation media**. Cre8tive normally installs SQL Server; if your team does, follow the Cre8tive SQL Installation for PLM guide
- ☐ The service accounts, AD groups and consultant access in **section A**
- ☐ A named **troubleshooting contact** who can change firewall, DNS, certificate and account settings during installation
- ☐ ERP integration in scope: an ERP integration user and API access for Cre8 Hub, plus ERP test access

CUSTOMER IT

CUSTOMER IT

CUSTOMER IT

CUSTOMER IT

How the installation runs

- 1 Viability check.** Once access works, Cre8tive confirms the accounts and rights are sufficient and the servers match Exhibit A.
- 2 Installation.** Allow at least **one calendar week per environment** (Main, then Test). Cre8tive installs, configures and checks the out-of-the-box functions, including Reporting Services (section H).
- 3 Post-installation debrief.** A configuration overview with your technical contact. Generated credentials (SQL `sa`, `PLMReports`, encryption-key backups) and project-specific configuration are handed over and stored in your password vault.

SECTION A

A Service accounts, AD groups & access

Create these in Active Directory before installation day. Names can follow your own standard; the Turnkey defaults are shown.

ACCOUNT / GROUP	PURPOSE & RIGHTS
PROCAD AD service account	Runs the core PRO.FILE services (archive/cache server, AppServer pool) and connects PRO.FILE to SQL Server. Only this account (and your backup) can write to the vault. Local administrator on every PLM server; sysadmin on the PLM SQL instance. Member of PLM_Admins .
NDF AD service account	Runs the NDF Job Server that creates PDF and other neutral files. Local administrator on the NDF workstation only. Member of PLM_Admins .
PLM_Users AD security group	Every PRO.FILE user. Read access to the shared PLM documentation, and run rights in Reporting Services (SSRS) for PRO.FILE Web Reports.
PLM_Admins AD security group	PRO.FILE administrators (also members of PLM_Users). Read/write on the PLM documentation share; manage rights in SSRS to create and change Web Reports.
SQL sa · PLMReports	Created by Cre8tive with generated 32-character passwords and handed to your IT team. sa is not used by any PLM service. PLMReports is a read-only login used only by the SSRS data source.

HOW CRE8TIVE CONSULTANTS WORK

- ☐ **Named VPN account per consultant, with MFA**, plus RDP to the PLM servers. Shared or service accounts are never used to sign in to the VPN **IT**
- ☐ On the servers, work runs as the **PROCAD** service account; inside PRO.FILE, as the built-in admin **procad**. On the NDF workstation, as **NDF** **CRE8TIVE**
- ☐ NDAs with your company and named consultants can be arranged if your policy requires them **JOINT**
- ☐ No VPN possible? TeamViewer or Splashtop work with **paid licences provided by you** and MFA on, but are slower and less secure **IT**

HEADLESS NDF WORKSTATION

- ☐ CAD system installed and licensed with **no sign-in or licence prompt** **IT**
- ☐ **Sysinternals Autologon** signs the NDF account in after every reboot or interruption, so processing resumes on its own. It stores the password encrypted, never in plain text in the registry **JOINT**
- ☐ Machine dedicated to NDF, in a secured location; console and RDP access limited to **PLM_Admins** **IT**

AFTER GO-LIVE

Rotate the PROCAD, NDF and **procad** passwords, keep them in your password vault, and disable consultant VPN accounts until support work is needed.

VALUES RETURNED TO CRE8TIVE

ITEM	EXAMPLE / NOTES	YOUR VALUE
Service account names	COMPANY\PROCAD · COMPANY\NDF (passwords entered in session)	
AD group names	PLM_Users · PLM_Admins	
Consultant remote access	VPN + RDP with MFA; named accounts issued	
Troubleshooting contact	Name, phone, hours	

SECTION B

B Servers & operating system

Provision each server for your tier in Exhibit A (Hardware Guide), then confirm the items below.

VIRTUAL MACHINES

- ☐ Servers provisioned per the Exhibit A tier: AppServer, SQL Server, Dynamic Search (production), NDF workstation, plus the test environment CUSTOMER IT
- ☐ CPU at **≥ 3.0 GHz** sustained clock; vCPUs split across **2 virtual sockets** (e.g. 2 sockets × 2 cores) CUSTOMER IT
- ☐ NVMe / SSD volumes created and formatted as separate drives: OS, vault (prodata), SQL data, SQL log / backup, Solr index CUSTOMER IT
- ☐ All PLM servers in **one location / cloud region**, with a fast VM-host-to-storage link CUSTOMER IT

OPERATING SYSTEM

- ☐ Windows Server 2022 / 2025 (per the Revalize Product Release Matrix), fully patched, **joined to the domain** CUSTOMER IT
- ☐ Server names of **15 characters or fewer**, or the FQDN is used everywhere. DNS aliases are welcome and make later server moves easier CUSTOMER IT
- ☐ Time synchronisation with the domain on every server (required for tokens and SSO) CUSTOMER IT
- ☐ Microsoft SQL Server Standard or higher installed or ready to install: collation `Latin1_General_CI_AS`, mixed-mode authentication, Client Connectivity SDK, SSRS and SSMS JOINT
- ☐ Any **older PRO.FILE versions** on reused servers are fully uninstalled (no in-place updates), and the legacy environment variable `DBANWPFAD` is removed from servers and workstations JOINT
- ☐ IIS role installed with Windows Authentication, HTTP Redirection, .NET Extensibility 4.5, ASP.NET 4.5, WebSocket Protocol, WCF HTTP Activation, IIS Management Console. Cre8tive can do this during installation JOINT
- ☐ Outbound internet from the servers to Microsoft and Revalize download sites during installation, or installers staged locally CUSTOMER IT

VALUES RETURNED TO CRE8TIVE

ITEM	EXAMPLE / NOTES	YOUR VALUE
AppServer (prod) host name & IP	plmapp01 · 10.0.10.21	
SQL Server (prod) host \ instance	plmsql01 or plmsql01\PLM	
Dynamic Search (prod) host name & IP	plmsearch01 · 10.0.10.23	
NDF + test AppServer / SQL hosts	plmndf01 · plmapp-t01 / plmsql-t01	

SECTION C

Network, DNS & firewall ports

Open these paths on every firewall, VLAN boundary and Windows Firewall between the machines. Tell us about any subnet or firewall between servers in advance.

FROM	TO	PURPOSE	PORT / PROTOCOL
Clients, Job Server, NDF	AppServer	PRO.FX AppServer, IdentityServer, web apps	TCP 443 (80 → 443 redirect)
AppServer	SQL Server	PRO.FILE database	TCP 1433*
AppServer	SQL Server	Distributed transactions / file share	DTC 135 + dynamic, SMB 445
AppServer	Archive / cache server	Vault and cache (if on separate machines)	TCP 7600 / 7605
AppServer, clients	Report server (SSRS)	Reports	TCP 80 / 443
AppServer (Cre8 Hub)	ERP system	Cre8 Hub Integrations (ERP API)	TCP 443 or ERP API port
AppServer	Dynamic Search server	Solr search index	TCP 8983
AppServer	Dynamic Search server	Indexer service	TCP 9995
Dynamic Search server	AppServer (IdentityServer)	Access-token validation	TCP 443
Dynamic Search server	SQL Server	Metadata and permissions	TCP 1433*
AppServer	Microsoft 365 / mail relay	Outbound e-mail	443 Graph · 25 / 587 SMTP
Clients, AppServer	Entra ID / ADFS	Single sign-on	TCP 443 (outbound)
Clients	AutoVue server (optional)	Live viewing	TCP 7090
AutoVue server	AppServer	AutoVue Tomcat to AppServer	TCP 443

* Or your SQL instance's fixed port. Rows in red are new in 10.5 and needed only when Dynamic Search runs on its own server. Allow Solr (8983) and Indexer (9995) **only from the AppServer**; Tika (9998) stays local to the Dynamic Search server.

DNS

- ☐ A DNS name for the AppServer that users will use everywhere (e.g. `plm.company.com`). It must resolve from every zone that will use PRO.FILE: LAN, VPN and, if needed, the internet CUSTOMER IT
- ☐ A DNS name for the Dynamic Search server (e.g. `plmsearch.company.com`) CUSTOMER IT
- ☐ Optional HTTP → HTTPS redirect on IIS or on your load balancer / reverse proxy JOINT

VALUES RETURNED TO CRE8TIVE

ITEM	EXAMPLE / NOTES	YOUR VALUE
AppServer public FQDN	plm.company.com · the name users and SSO will use	
Dynamic Search FQDN	plmsearch.company.com	
SQL port (if not 1433)	Fixed port of the named instance	
Firewall rules confirmed	Date and name of the person who opened them	

SECTION D

D SSL certificates for IIS

The AppServer site in IIS is bound to HTTPS on port 443 with a certificate from your certificate authority. Every PLM web component on that site uses it: the AppServer, the IdentityServer and the Dynamic Search web app.

CERTIFICATE REQUIREMENTS

- ☐ Issued by a CA that **every client trusts**: your internal enterprise CA (root distributed by GPO) or a public CA. Self-signed certificates are for lab tests only IT
- ☐ Subject / SAN contains the AppServer FQDN users will type, e.g. `plm.company.com`. Add the server's own FQDN as a second SAN IT
- ☐ RSA 2048-bit or higher, SHA-256, Server Authentication EKU. Wildcards (`*.company.com`) are fine; tell us if you use one IT
- ☐ Delivered as **.pfx with private key** (password sent separately), or enrolled directly into the AppServer's computer store IT
- ☐ One certificate per environment (prod and test), each with a recorded expiry date and renewal owner. An expired certificate stops all PLM sign-ins IT

WHERE CERTIFICATES ARE USED

SERVER	CERTIFICATE
AppServer (IIS)	Required. HTTPS binding on 443 for the PLM site.
Test AppServer	Required for Dynamic Search and SSO testing.
SSRS	Recommended if reports are opened over HTTPS.
AutoVue (optional)	Its Tomcat must trust the AppServer certificate chain.
Dynamic Search server	Not required. Its services are reached from the AppServer only; it validates tokens against the AppServer over HTTPS.

HOW CRE8TIVE APPLIES IT CRE8TIVE

- 1 Import the certificate and bind it to the PLM web site in IIS: type `https`, port `443`. Optionally enable *Require SSL*.
- 2 Set the matching attributes on `ContainerConfigurationSet` in `%ALLUSERSPROFILE%\Procad\PROFX\ProfileConfiguration.xml`, then restart IIS.
- 3 Point existing Desktop Clients at the HTTPS address (cached `ProfileConnections.json` entries are reset).

```

<!-- ProfileConfiguration.xml : values derived from your certificate -->
<ContainerConfigurationSet ...
  RequireSsl="true"           <!-- IIS "Require SSL" enabled -->
  HttpsPort="443"
  SslCertStoreName="WebHosting" <!-- or "My" (Personal) - the store you imported into -->
  SslCertSubjectName="plm.company.com" <!-- only if several certificates are in the store -->
  SslHostingServerName="plmapp01.company.com" <!-- only for wildcard certificates -->

```

VALUES RETURNED TO CRE8TIVE

ITEM	USED FOR	YOUR VALUE
Subject / SAN names · wildcard?	<code>SslCertSubjectName</code> ; wildcard triggers <code>SslHostingServerName</code>	
Delivery: .pfx file or enrolled store	<code>SslCertStoreName</code> (WebHosting / My)	
Expiry date, renewal owner · HTTPS only (Y/N)	Renewal planning; <code>RequireSsl</code> and HTTP redirect	

SECTION E

E-mail: Microsoft Graph or SMTP

PRO.FILE sends e-mail from the AppServer: workflow task notifications, process escalation e-mails, "notify" messages and Generic Job Server error alerts. No relay server is needed.

CHOOSE A ROUTE

- ☐ **Microsoft 365 · Route A (recommended): Microsoft Graph.** Entra app with the Graph **application** permission `Mail.Send`, admin consent, limited to the sender mailbox (Exchange Online RBAC for Applications). No port 25, no static IP IT
- ☐ **Microsoft 365 · Route B: connector to your MX endpoint.** Static, unshared public IP; outbound TCP 25 open; inbound connector authenticated by that IP; IP added to SPF. Not supported from Azure-hosted servers IT
- ☐ **Other mail systems:** an internal SMTP relay that accepts mail **only** from the PLM servers' IPs (never an open relay), on port 25 or 587 with STARTTLS IT
- ☐ A sender address in your mail domain, such as `plm-noreply@company.com` (a shared mailbox works for Route A) IT
- ☐ PLM users have their e-mail addresses filled in. Escalation mails only reach users with an address JOINT

NO LONGER USED

The Windows **SMTP Server (IIS 6) relay**: removed in Windows Server 2025 and unsupported by Microsoft for Microsoft 365. **Port 465**: PRO.FILE's mail client uses STARTTLS only. The connection filter **IP Allow List**: it bypasses SPF, DKIM and DMARC.

WHERE CRE8TIVE CONFIGURES IT

ISI.CONTrOl Panel → Configuration parameters → Services → **MailService** (Modus → Transport; Office365; SmtP). Job Server error alerts are sent over SMTP only, so with Route A also set up Route B if you want them.

VALUES RETURNED TO CRE8TIVE

ITEM	PRO.FILE PARAMETER	YOUR VALUE
Route / transport	Modus → Transport: Graph (A), SMTP connector (B), SMTP relay	
Sender address	AzureSenderUPN (Graph) / E-mail address of the sender (SMTP)	
Graph: tenant ID / client ID	<code>EntraIdTenantId</code> / <code>AzureApplicationClientId</code>	
Graph: client secret · expiry	<code>AzureApplicationClientSecret</code> . Send securely ; expiry date for renewal	
SMTP server name · port	MX endpoint (Route B) or relay host · 25 or 587	
SMTP STARTTLS / authentication	Security (Y/N) · authentication (Y/N, relay only; password sent separately)	
Job Server alert / test recipients	Error notifications; go-live test mailbox	

SECTION F

F Single sign-on

With SSO, users click **Sign in with Microsoft** in the Desktop Client and the web apps and log in with their corporate account, including MFA. PRO.FILE supports **Microsoft Entra ID** (cloud, recommended) and **ADFS** (on-premises).

PREREQUISITE

External identity providers only work when the AppServer runs in **SSL mode** (section D), and the redirect URLs below must use the exact FQDN from the certificate.

Option 1 · Microsoft Entra ID RECOMMENDED

Requires an Entra (Azure AD) tenant with the user accounts. Your Entra administrator completes these steps at

<https://entra.microsoft.com>:

- 1 **App registrations** → **New registration**. Name it, e.g. *PRO.FILE PLM*. Under *Supported account types*, choose single tenant unless external (guest) accounts must sign in; guests must first be invited to your directory.
- 2 On the overview page, note the **Application (client) ID** and the **Directory (tenant) ID**.
- 3 **Certificates & secrets** → **New client secret**. Choose an expiry and copy the secret **Value** immediately, not the Secret ID. It cannot be shown again.
- 4 **Authentication** → **Add a platform** → **Web**. Add the redirect URI and the front-channel logout URL:
<https://plm.company.com/procad/identityserver/signin-oidc-az>
<https://plm.company.com/procad/identityserver/signout-oidc-az>
 Use your AppServer FQDN, all lower-case, exactly as shown. Entra compares redirect URIs case-sensitively.
- 5 Optionally restrict sign-in to a security group (*Enterprise applications* → *Properties* → *Assignment required*) and apply your Conditional Access / MFA policies.

VALUES RETURNED TO CRE8TIVE · ENTRA ID

ITEM	BECOMES IN PROFILECONFIGURATION.XML	YOUR VALUE
Directory (tenant) ID	<code>Authority = https://login.microsoftonline.com/{tenant ID}/v2.0</code>	
Application (client) ID	<code>ClientId</code>	
Client secret value	<code>Secret</code> . Send securely	sent separately
Client secret expiry date	Renewal reminder. SSO stops when it expires	
Redirect URIs registered (Y/N)	signin-oidc-az / signout-oidc-az	

```

<!-- ProfileConfiguration.xml : written by Cre8tive from the values above -->
<AppServerConfiguration>
  <IdentityServer>
    <Providers>
      <Provider Name="EntraID" Enabled="true"
        Authority="https://login.microsoftonline.com/{Directory (tenant) ID}/v2.0"
        ClientId="{Application (client) ID}"
        Secret="{client secret value}" />
    </Providers>
  </IdentityServer>
  <ContainerConfigurationSet ... IdentityServerEnabled="true" RequireSsl="true">

```

SECTION F · CONTINUED

Option 2 · ADFS (on-premises)

For fully on-premises environments. Requires a working ADFS farm, usually at `https://adfs.company.com`. Your ADFS administrator completes these steps in **ADFS Management**:

- 1 **Application Groups** → **Add Application Group**, template *Server application accessing a web API*.
- 2 Redirect URI: `https://plm.company.com/procad/identityserver` (no trailing slash). Note the generated **Client identifier**.
- 3 Generate a **shared secret** and copy it now. It cannot be copied later.
- 4 Web API identifier: the same IdentityServer URL. Access control policy: *Permit everyone* (or your own group policy). Permitted scope: **openid**.
- 5 Enable **Forms** (extranet and intranet) and **Windows** (intranet) as primary authentication methods.
- 6 For seamless browser sign-in: add `Mozilla/5.0` to `WiaSupportedUserAgents`, set `ExtendedProtectionTokenCheck` to `None`, then restart the `adfsrv` service.
- 7 By GPO: add the AppServer URL to the **Local intranet** zone and enable Integrated Windows Authentication. For Firefox, add the ADFS URL to `network.negotiate-auth.trusted-uris`.

VALUES RETURNED TO CRE8TIVE · ADFS

ITEM	BECOMES IN PROFILECONFIGURATION.XML	YOUR VALUE
ADFS authority URL	<code>Authority</code> , normally <code>https://adfs.{domain}/adfs</code>	
Client identifier	<code>ClientId</code>	
Shared secret	<code>Secret</code> . Send securely	sent separately
Intranet zone / WIA deployed by GPO (Y/N)	Client-side seamless sign-in	

```
<Provider Name="AD" Enabled="true"
  Authority="https://adfs.company.com/adfs"
  ClientId="{client identifier}" Secret="{shared secret}" />
```

After the provider is configured

USERS LINK THEIR ACCOUNT ONCE

In the Desktop Client: **User settings** → **User** → **Authentication**, pencil icon, then sign in with the corporate account. From then on the login dialog shows **Sign in with Microsoft**. Links can be removed at any time.

WINDOWS AUTOLOGIN IS SEPARATE

PRO.FILE's mapped Windows autologin (Windows login stored on the PLM user) keeps working alongside SSO. Cre8tive can map users in bulk during user import.

- ☐ Pilot users identified to test SSO in the **test** environment first (use a separate app registration or redirect URI for the test FQDN) [JOINT](#)

- ☐ Client-secret renewal added to your IT calendar, at least 30 days before expiry [CUSTOMER IT](#)

SECTION G

G Dynamic Search server

In production, Dynamic Search runs on its own server so indexing never slows down the AppServer. In test, it is co-hosted on the test AppServer and talks over `localhost`.

DYNAMIC SEARCH SERVER (PRODUCTION)

- ☐ Server provisioned per the Hardware Guide: ≥ 4 vCPU at ≥ 3 GHz, 32 GB RAM, fast SSD index volume of 300 GB
- ☐ .NET Framework 4.8 and **Microsoft OpenJDK 17** (or later) installed IT JOINT
- ☐ Firewall: AppServer → this server on **8983** and **9995** only; this server → SQL (1433) and → AppServer (443) IT
- ☐ Database access for the Indexer. It uses the PLM database login from `ProfileConfiguration.xml`; with Integrated Security, grant the server's computer account access to the PLM database JOINT
- ☐ Antivirus excludes the Solr index folder `C:\ProgramData\Procad\DynamicSearch` IT

ON THE APPSERVER

- ☐ HTTPS binding in place (section D) JOINT
- ☐ **.NET 10 Hosting Bundle** installed *after* IIS. If IIS is added later, the bundle is reinstalled CRE8TIVE
- ☐ PRO.FILE Web Apps installed with the *Dynamic Search* feature CRE8TIVE

CRE8TIVE THEN

- Installs the Indexer, Solr and Tika services and sets up port proxies so Solr and Tika answer on the server's FQDN.
- Writes the `DynamicSearch` block into `ProfileConfiguration.xml` on **both** the AppServer and the Dynamic Search server.
- Creates one Solr core per tenant, starts the initial index and checks the status page in the ISI.CONTROL Panel.

```

<!-- ProfileConfiguration.xml on BOTH the AppServer and the Dynamic Search server -->
<ContainerConfigurationSet ... RequireSsl="true" IdentityServerEnabled="true">
  <DynamicSearch Enabled="true"
    BackendServiceUrl="http://plmsearch.company.com:8983"      <!-- Solr -->
    IndexingServiceUrl="http://plmsearch.company.com:9995"    <!-- Indexer -->
    FileIndexingServiceUrl="http://plmsearch.company.com:9998" <!-- Tika -->
    Authority="plm.company.com/procad/identityserver"          <!-- no https:// -->
    Secret="{GUID generated by Cre8tive}" />
</ContainerConfigurationSet>
<TenantConfigurationSet>
  <Configuration Tenant="Profile" ... DynamicSearchEnabled="true" />

```

VALUES RETURNED TO CRE8TIVE

ITEM	BECOMES	YOUR VALUE
Dynamic Search server FQDN	<code>BackendServiceUrl</code> , <code>IndexingServiceUrl</code> , <code>FileIndexingServiceUrl</code>	
AppServer FQDN (IdentityServer)	<code>Authority</code> (host + /procad/identityserver)	
Firewall rules 8983 / 9995 / 443 / 1433 open (Y/N)	Service connectivity	
DB access method	SQL login (anw) or Integrated Security computer account	
Tenants to index	<code>DynamicSearchEnabled</code> per tenant; one Solr core each	

H Reporting Services (SSRS)

The Turnkey reports run in SQL Server Reporting Services on the SQL server. Users open them inside PRO.FILE, which shows the report page in an embedded browser, so Windows must sign them in silently.

PREPARE

- ☐ **Product:** SQL Server 2022 Reporting Services (SQL Server 2019 / 2022) or Power BI Report Server (SQL Server 2025), with the SQL Server **product key** (Standard or higher) IT
- ☐ A **DNS name** for the report server (e.g. `plmreports.company.com`) with a certificate (section D); clients → report server on **TCP 443** IT
- ☐ `PLM_Users` and `PLM_Admins` exist and are populated (section A); every `PLM_Admins` member is also in `PLM_Users` IT
- ☐ **Root folder** for the PLM reports: Home (/) on a dedicated report server, or its own folder (e.g. `/PLM`) when the report server is shared with other applications JOINT

GROUP POLICY FOR SILENT SIGN-IN

- ☐ **Site to Zone Assignment List:** add `https://<report server>` and `https://<PLM AppServer>` (and the Dynamic Search host) to the **Local intranet** zone IT
- ☐ Using the **Trusted sites** zone instead? Set its **Logon options** to *Automatic logon with current user name and password* IT
- ☐ Microsoft Edge policy `AuthServerAllowlist` lists the same servers, so Edge and the PRO.FILE embedded viewer use the signed-in Windows account IT
- ☐ Test on a user PC: a Web Report opens inside PRO.FILE **without a login prompt** JOINT

HOW CRE8TIVE CONFIGURES IT CRE8TIVE

- 1 Install** Reporting Services as the PROCAD account with your product key.
- 2 Restore the Turnkey report catalog** (`ReportServer`, `ReportServerTempDB`): owner `sa`, simple recovery.
- 3 Configuration Manager:** virtual service account; HTTPS on 443 with your certificate; existing database with service credentials; web portal `/Reports`; restore the Turnkey encryption key, then **back up the new key**.
- 4 Data source** `/Profile` points to the PLM database with the read-only `PLMReports` login (stored SQL credentials).
- 5 Security:** remove *Everyone*. Site: `PLM_Admins` = System Administrator, `PLM_Users` = System User. Root folder: `PLM_Admins` = Content Manager, `PLM_Users` = Browser.
- 6 PRO.FILE Web Reports** and the Cre8tive solutions point to `https://<report server>/ReportServer`; a report is opened from PRO.FILE to verify.

VALUES RETURNED TO CRE8TIVE

ITEM	EXAMPLE / NOTES	YOUR VALUE
Report server DNS name	<code>plmreports.company.com</code>	
Web portal · web service URL	<code>https://.../Reports</code> · <code>https://.../ReportServer</code>	
PLM reports root folder	<code>/</code> (Home) or e.g. <code>/PLM</code>	
Product & edition	SSRS 2022 or Power BI Report Server · Standard / Enterprise	
AD groups confirmed (Y/N)	<code>PLM_Users</code> and <code>PLM_Admins</code> created and populated	
GPO applied (Y/N) · policy name	Zone assignment, logon option, Edge <code>AuthServerAllowlist</code>	
Encryption key backup	File location · vault entry (never the password)	

SECTION I

I Antivirus, backup & licences

Operating rules that keep PRO.FILE fast and recoverable, and the licences that must be in place before installation.

ANTIVIRUS

- ☐ No on-access scanning of the vault (**prodata**); scheduled nightly scan instead IT
- ☐ Exclusions for SQL data and log files (**.mdf** , **.ldf** , **.ndf**), SQL backup folder and the Solr index IT
- ☐ Only one antivirus product per server. Windows Defender uninstalled if a third-party product is used IT
- ☐ Agreement that antivirus may be temporarily *uninstalled* for performance troubleshooting JOINT

BACKUP & MAINTENANCE

- ☐ SQL maintenance plan in place: index and statistics maintenance plus integrity checks JOINT
- ☐ Nightly **full, copy-only** PLM database backup to local disk, kept alongside any central backup JOINT
- ☐ Recovery model **simple** (no transaction-log backups) for systems up to about 500 users JOINT
- ☐ Vault (**prodata**) backed up in the same window as the database IT
- ☐ Daily AppServer application-pool recycle scheduled outside working hours CREATIVE

LICENCES READY

- ☐ Microsoft SQL Server Standard (or higher) licences, including Software Assurance for Azure-hosted SQL IT
- ☐ ERP licence for the Cre8 Hub integration user, if your ERP requires one (only when ERP integration is in scope) IT
- ☐ One dedicated CAD licence for each CAD system processed on the NDF workstation IT
- ☐ PRO.FILE licence file received from Cre8tive / Revalize CREATIVE

SECTION J



Summary & sign-off

Check off each block when its values are with Cre8tive. When every row is green, we are ready to schedule installation.

BLOCK	DELIVERED TO CRE8TIVE	DATE
☐ A · Accounts & access	PROCAD and NDF accounts, PLM_Users / PLM_Admins, consultant VPN with MFA	
☐ B · Servers	Host names, IPs, OS and SQL readiness	
☐ C · Network & DNS	FQDNs, SQL port, firewall rules confirmed	
☐ D · SSL certificate	Certificate (.pfx + password, separately), names, expiry	
☐ E · E-mail	Route, sender, Graph IDs + secret, or SMTP server, port, TLS	
☐ F · Single sign-on	Tenant ID, client ID, secret value + expiry (or ADFS equivalents)	
☐ G · Dynamic Search	Search server FQDN, firewall, DB access, tenants	
☐ H · Reporting	Report server URL, root folder, AD groups confirmed, GPO applied	
☐ I · Operations	AV exclusions, backup, maintenance, licences	

SENDING SECRETS

Send passwords, client secrets and certificate passwords through your secure file-share or password manager, or enter them yourself during the installation session. Please never send them in the same e-mail as this checklist.

SIGN-OFF

NAME	ROLE	SIGNATURE	DATE
Customer IT			
Customer project lead			
Cre8tive project lead			



Cre8tive Technology & Design

Based on the PRO.FILE 10.5 administration and installation manuals. Guidance is provided in consideration of all Revalize best practices and in cooperation with Revalize.