PDServer certificate pinning and certificate changes

Certificate pinning lets Print Director clients trust the specific PDServer TLS certificate configured for their server. A different certificate is rejected even when Windows trusts its issuer. WebSockets remain available for agent connections.

This is a planned migration in the upcoming release. Installing the update does not enable pinning or remove an existing deployment CA from Windows. Arrange activation with your Print Director administrator or support partner.

Before activation

- Upgrade all PDServers and clients, including agents, Resource Manager and PDReports. Account for offline machines before enabling the policy.
- Configure encrypted SQL connections that validate the SQL server certificate. SQL must use independently managed certificate trust.
- Inventory the certificates actually presented by each PDServer. Direct Kestrel TLS and pass-through proxies are supported. A proxy that terminates TLS with a different certificate needs a separate configuration design before activation.
- Identify Windows SSL Internet-Port queues connecting to remote agent IPPS services. These connections use the Windows spooler and need independently verified replacement trust before the deployment root can be removed.

An administrator verifies the current certificate, enables its pin, then checks online reconnects and SQL-offline restarts on every client. Existing certificates and aliases can remain in use. The pin is SHA-256 of the complete public certificate; a Windows certificate thumbprint or the hash of a PFX file is not interchangeable with it.

Changing a pinned certificate

Pinning changes the renewal procedure. An enabled PDServer keeps its current certificate instead of automatically replacing it when addresses or the issuing CA change. Schedule replacement before expiry. A missing or expired pinned certificate needs an authorized replacement before PDServer can start.

1. Prepare the replacement while the existing certificate is still valid. Print Director can stage a separate CA-issued candidate without changing the running identity.
2. Distribute the replacement as the next permitted certificate. Confirm every client has received both current and next pins, including clients that normally operate offline.
3. Activate the replacement during a maintenance window and verify agent, Resource Manager, payload and peer-server connections, plus affected printer connections.
4. Retire the old pin only after every client has successfully reconnected. Refresh offline caches and restart persistent connections as part of that step.

Renewing with the same private key still changes the certificate and requires this procedure. Preserve a secure rollback copy until the change is verified. Do not bypass a pin mismatch by enabling an accept-all certificate policy.

Removing the deployment root from Windows

Pinning protects the PD connections that use it. While the deployment CA remains in the Windows machine trusted-root store, its signing key can still authorize unrelated TLS certificates for clients using that store.

Root removal is a separate per-machine step. First verify independently trusted SQL and spooler IPPS connections, then remove only the exact approved deployment CA and disable its automatic re-import. Confirm that agent refresh, restart and Group Policy do not add it back. Keep customer-managed roots intact.

The deployment CA itself does not need reissuing for pinning. It can continue serving certificate consumers that still need it. A machine that must retain the root for compatibility has not completed this security migration.

Your support partner can use the versioned `Tools/Security` migration scripts supplied with the source/support package. Their verification switches require operator evidence; they do not automatically certify fleet readiness.

Print Director version at time of publish: 2.5.15.3. Publish date: 29/10/2026.