AVERY DENNISON

Research Memorandum

To:
From: Bob Fermin
Department: Engineering Technology, Coating Technology Group
Date: 14 July 2026
Subject: **Coreform RLM License Server Setup Guide**

Abstract

This document serves as a comprehensive, technical record of the deployment, configuration, and optimization of the Reprise License Manager (RLM) for Coreform Cubit on a corporate Linux machine. It outlines the successful configurations, security workarounds, and command procedures necessary to deploy a resilient, automated, and secure corporate license server.

1 System and Environment Summary

The licensing environment is built on the following specifications:

- **License Server Hostname:** `<linux-host>`
- **RLM Executable Path:** `/opt/Coreform-RLM-Server/Coreform-RLM-Server-2025.12/rlm`
- **ISV Vendor Daemon Path:** `/opt/Coreform-RLM-Server/Coreform-RLM-Server-2025.12/csimsoft`
- **Service Architecture:** Guided under a non-root systemd service executing as the dedicated system user `rlm`.

2 Step 1: File Ownership and Permissions Verification

To ensure the low-privilege `rlm` user can read license files and execute the binaries without standard permission constraints, the correct file permissions must be established.

```
# Assign ownership of the directory and contents to the 'rlm' user
sudo chown -R rlm:rlm /opt/Coreform-RLM-Server/Coreform-RLM-Server-2025.12/

# Make both the RLM manager and the csimsoft vendor daemon executable
```

```
sudo chmod +x /opt/Coreform-RLM-Server/Coreform-RLM-Server-2025.12/rlm
sudo chmod +x /opt/Coreform-RLM-Server/Coreform-RLM-Server-2025.12/csimsoft
```

3 Step 2: License File Port Modifications

Default RLM settings often bind to privileged ports below 1024 (such as port 1 or default fallback 503). Because the daemon runs under a restricted `rlm` user account, the Linux kernel blocks these low-port binds.

The configuration was updated to utilize standard, non-privileged TCP ports. Modify the license file (`*.lic`) inside the server directory as follows:

Listing 1: Successful configuration in the license file

```
HOST <linux-host> 0010183d6db6 5053
ISV csimsoft port=5055
```

- **Port 5053:** Configured for primary RLM server communications.
- **Port 5055:** Locked to the `csimsoft` vendor daemon, preventing ephemeral port cycling and facilitating clean corporate firewall exceptions.

4 Step 3: Port De-confliction

An orphaned background process from a manual root execution may hold the active web administration port (5054). This prevents the systemd unit from initializing. Terminate all orphaned background instances before starting the official service:

```
# Kill any background ghost instances running outside systemd
sudo killall rlm
```

5 Step 4: Systemd Service Configuration

To secure the server against unplanned reboots, the service must be registered under systemd. The service unit file should be placed at `/etc/systemd/system/rlm-coreform.service`.

Enable and register the service to guarantee persistence across boots:

```
# Reload systemd configuration changes
sudo systemctl daemon-reload

# Enable the service to automatically spin up at boot
sudo systemctl enable rlm-coreform
```

```
# Start the automated license manager
sudo systemctl start rlm-coreform
```

6 Step 5: Verifying Server Socket State

Once initialized, ensure all ports are actively listening on IPv4 interface networks:

```
sudo ss -tulpn | grep -E '5053|5054|5055'
```

A successful verification output should resemble the following:

```
udp UNCONN 0 0 0.0.0.0:5053 0.0.0.0:* users:(("csimsoft",pid=7996,fd=5),("rlm",
    pid=7992,fd=5))
tcp LISTEN 0 128 0.0.0.0:5054 0.0.0.0:* users:(("rlm",pid=7992,fd=4))
tcp LISTEN 0 5 *:5053 *:* users:(("csimsoft",pid=7996,fd=3),("rlm",pid=7992,fd=3))

tcp LISTEN 0 5 *:5055 *:* users:(("csimsoft",pid=7996,fd=6))
```

7 Step 6: Bypassing Corporate HTTP Blocks (SSH Tunneling)

If corporate firewalls or policies prevent direct unencrypted HTTP connections to the server console over port 5054, configure a secure SSH tunnel from the remote administrator's local workstation.

If the local port 5054 on the desktop workstation is already in use, map the server's console to port 8080 locally:

```
# Establish a secure IPv4 port forwarding tunnel from your local machine
ssh -L 8080:127.0.0.1:5054 user@<linux-host>
```

Once connected, navigate to the local browser at:
http://127.0.0.1:8080

This maps traffic securely over SSH to view the live dashboard statistics.

8 Step 7: Client Performance and Display Optimization

For corporate desktop environments utilizing X11 forwarding or remote desktop infrastructure, Cubit may report driver errors. To suppress the warning:

```
libEGL warning: DRI2: failed to authenticate
```

and force Qt fallback rendering, export the following environment variables locally before executing Cubit:

```
# Suppress authentication warnings by forcing Qt's EGL integration pipeline
export QT_XCB_GL_INTEGRATION=xcb_egl

# Alternative: Force Mesa to run entirely via CPU software rasterization
export LIBGL_ALWAYS_SOFTWARE=1
```