

# SAP-ERP Portal — DNS & HTTPS Setup Guide

Internal reference: friendly hostnames (erp.mipl.com, app1.mipl.com, app2.mipl.com) via internal DNS + Apache reverse proxy, secured with a certificate issued by the internal MIPL Active Directory Certificate Authority.

---

## Environment

| Component                      | Machine / Address                          | Notes                                                         |
|--------------------------------|--------------------------------------------|---------------------------------------------------------------|
| Application server             | 10.9.11.210                                | Runs the Node.js portal (PM2, port 5000) and XAMPP Apache (re |
| Internal DNS server            | 192.9.201.201 (adc.mipl.com)               | Windows Server — AD DS + DNS + AD CS roles                    |
| Internal Certificate Authority | adc.mipl.com                               | Issues the HTTPS certificate used by Apache                   |
| Internal domain / zone         | mipl.com                                   | Forward lookup zone on the DNS server                         |
| Target hostnames               | erp.mipl.com, app1.mipl.com, app2.mipl.com | All resolve to 10.9.11.210 via a wildcard DNS record          |

## How it fits together

A browser resolves **erp.mipl.com** to 10.9.11.210 via internal DNS, then connects to Apache on port 80/443. Apache terminates the connection (and, for HTTPS, the TLS handshake) and silently forwards the request to the Node.js portal listening on **127.0.0.1:5000**, managed by PM2. This is what removes the need to type a port number, and lets several apps share the same server on the same ports, routed purely by hostname.

## Part A — DNS Configuration

### A1. Add a wildcard DNS record

On the DNS server (192.9.201.201 / adc.mipl.com):

- 1 Open **Server Manager** → **DNS**, right-click the server → **DNS Manager** (or run `dnsmgmt.msc` directly).
- 2 Expand the server → **Forward Lookup Zones** → open the **mipl.com** zone.
- 3 Right-click inside the zone → **New Host (A or AAAA)...**
- 4 Name: \* IP address: 10.9.11.210
- 5 Leave "Create associated pointer (PTR) record" unchecked. Click **Add Host** → **Done**.

The wildcard means **any** subdomain of mipl.com (erp, app1, app2, and anything added later) resolves to 10.9.11.210 automatically — no further DNS changes needed when a new app is added, only a new entry in the Apache config (Part B).

### A2. Verify DNS resolution

From any domain-joined PC:

```
nslookup erp.mipl.com
# Expected: Address: 10.9.11.210
```

### A3. Workgroup (non-domain) PCs

A PC that is not joined to the mipl.com domain will not automatically use 192.9.201.201 as its DNS server.

For each such machine, either:

- Set its Preferred DNS server to 192.9.201.201 in the network adapter's IPv4 settings, *or*
- Add explicit entries to `C:\Windows\System32\drivers\etc\hosts`:

```
10.9.11.210    erp.mipl.com
10.9.11.210    app1.mipl.com
10.9.11.210    app2.mipl.com
```

## Part B — Apache Reverse Proxy (removes the port number)

This is done on **10.9.11.210**, using the Apache that ships with XAMPP (D:\apps\xampp74\apache). It listens on port 80/443 and silently forwards to the Node app on port 5000 (managed separately by PM2 — Apache does not need to know or care how the Node process is supervised).

### B1. Enable the proxy modules

Edit D:\apps\xampp74\apache\conf\httpd.conf and remove the leading # from **both** of these lines (both are required — missing just mod\_proxy\_http causes an "AH01144: No protocol handler" error later):

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

Also confirm this line is present and uncommented (usually further down the same file):

```
Include conf/extra/httpd-vhosts.conf
```

### B2. Add a virtual host per application

Edit D:\apps\xampp74\apache\conf\extra\httpd-vhosts.conf:

```
<VirtualHost *:80>
    ServerName erp.mipl.com
    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:5000/
    ProxyPassReverse / http://127.0.0.1:5000/
</VirtualHost>

<VirtualHost *:80>
    ServerName app1.mipl.com
    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:<APP1_PORT>/
    ProxyPassReverse / http://127.0.0.1:<APP1_PORT>/
</VirtualHost>

<VirtualHost *:80>
    ServerName app2.mipl.com
    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:<APP2_PORT>/
    ProxyPassReverse / http://127.0.0.1:<APP2_PORT>/
</VirtualHost>
```

Replace <APP1\_PORT> / <APP2\_PORT> with the actual ports those applications listen on.

### B3. Port 80 must be free, and open on the firewall

- 1 Confirm nothing else on 10.9.11.210 is already using port 80 (IIS, another web server, etc.) — netstat -ano | findstr :80
- 2 Open the port on Windows Firewall: netsh advfirewall firewall add rule name="HTTP 80" dir=in action=allow protocol=TCP localport=80
- 3 Restart Apache from the XAMPP Control Panel (Stop, then Start — not just Reload).

### B4. Test

```
http://erp.mipl.com    (no port number)
```

Should load the portal exactly as <http://10.9.11.210:5000> did before.

## Part C — HTTPS Certificate (Internal CA)

Because **mipl.com** is an internal-only name, a public certificate authority (like Let's Encrypt) cannot issue a certificate for it. Instead, the certificate is issued by the organisation's own internal CA (Active Directory Certificate Services, running on `adc.mipl.com`). Domain-joined PCs trust this CA automatically; workgroup PCs need one manual step (Part D).

### C1. Allow the certificate to carry Subject Alternative Names (SAN)

By default, a Windows CA ignores any Subject Alternative Name supplied in a certificate request, for security reasons. Modern browsers **require** a matching SAN and ignore the plain Common Name — skipping this step causes a `NET::ERR_CERT_COMMON_NAME_INVALID` error later. On the CA server (`adc.mipl.com`), as Administrator:

```
certutil -setreg policy\EditFlags +EDITF_ATTRIBUTESUBJECTALTNAME2
net stop certsvc
net start certsvc
```

### C2. Grant Enroll permission on the Web Server template

The built-in **Web Server** certificate template only allows Domain/Enterprise Admins to enroll by default. On the CA server, run `certtmpl.msc` → right-click **Web Server** → **Properties** → **Security** → add the relevant user or computer account → allow **Enroll** (and Read).

### C3. Generate a private key + CSR (with SAN) on 10.9.11.210

XAMPP's bundled OpenSSL looks for its config in a hardcoded default path that doesn't exist on this install — point it at the real one first:

```
cd D:\apps\xampp74\apache\bin
set OPENSSL_CONF=D:\apps\xampp74\apache\conf\openssl.cnf

openssl req -new -newkey rsa:2048 -nodes -keyout erp.mipl.com.key -out erp.mipl.com.csr ^
  -subj "/CN=erp.mipl.com/O=MIPL/C=IN" ^
  -addext "subjectAltName=DNS:erp.mipl.com,DNS:app1.mipl.com,DNS:app2.mipl.com"
```

This produces `erp.mipl.com.key` (private key — stays on this server) and `erp.mipl.com.csr` (the request). One certificate covers all three hostnames via SAN.

### C4. Submit the request to the internal CA

```
certreq -submit -attrib "CertificateTemplate:WebServer" erp.mipl.com.csr erp.mipl.com.crt
```

A dialog appears to pick the CA (auto-discovered via AD) — select the one on `adc.mipl.com`. If issued immediately, the signed certificate is saved as `erp.mipl.com.crt`. If it instead returns "Pending", an administrator must approve it on the CA (Certification Authority console → Pending Requests → right-click → Issue), then retrieve it:

```
certreq -retrieve <RequestID> erp.mipl.com.crt
```

### C5. Export the CA's root certificate

On the CA server: `certsrv.msc` → right-click the CA name → **Properties** → **General** → **View Certificate** → **Details** → **Copy to File** → export as **Base-64 encoded X.509 (.CER)**. Save it as `ca-root.crt` and copy it to 10.9.11.210.

## C6. Install the certificate in Apache

- 1 Create the folder and move the files in: D:\apps\xampp74\apache\conf\ssl\ should contain erp.mipl.com.crt, erp.mipl.com.key and ca-root.crt.
- 2 In httpd.conf, uncomment:

```
LoadModule ssl_module modules/mod_ssl.so
Include conf/extra/httpd-ssl.conf
```

Add the SSL virtual host in httpd-vhosts.conf:

```
<VirtualHost *:443>
    ServerName erp.mipl.com
    SSLEngine on
    SSLCertificateFile "D:/apps/xampp74/apache/conf/ssl/erp.mipl.com.crt"
    SSLCertificateKeyFile "D:/apps/xampp74/apache/conf/ssl/erp.mipl.com.key"
    SSLCertificateChainFile "D:/apps/xampp74/apache/conf/ssl/ca-root.crt"

    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:5000/
    ProxyPassReverse / http://127.0.0.1:5000/
</VirtualHost>
```

Make sure only **one** "Listen 443" line exists across the whole config (it already exists by default in httpd-ssl.conf — adding a second one anywhere else stops Apache from starting).

## C7. Firewall + restart + test

- 1 Open port 443: netsh advfirewall firewall add rule name="HTTPS 443" dir=in action=allow protocol=TCP localport=443
- 2 Restart Apache from the XAMPP Control Panel.
- 3 If it fails to start, run httpd.exe -t from D:\apps\xampp74\apache\bin to print the exact config error.
- 4 Test from a domain-joined PC: https://erp.mipl.com — should show a trusted padlock, no warning.

## Part D — Workgroup (Non-Domain) PCs

Domain-joined PCs trust the internal CA automatically. A PC that is **not** joined to the mipl.com domain never receives that trust automatically, and will always show a security warning until it is set up manually — once per machine.

### D1. Name resolution (see also Part A3)

Either point its DNS server at 192.9.201.201, or add hosts-file entries for each app hostname.

### D2. Import the CA root certificate (required for HTTPS to show as trusted)

Copy `ca-root.crt` to the machine, then as Administrator:

```
certutil -addstore -f "ROOT" ca-root.crt
```

### D3. Firefox needs one extra step

Firefox keeps its own certificate store — it does not read the Windows trust store by default, so step D2 alone will not satisfy Firefox. Either:

- **Recommended:** in Firefox, open `about:config`, set `security.enterprise_roots.enabled` to `true`, restart Firefox. (This can be pushed to many PCs at once via a Firefox enterprise policy file / GPO ADMX template.)
- **Or** import `ca-root.crt` directly into Firefox: Settings → Privacy & Security → Certificates → View Certificates → Authorities → Import → check "Trust this CA to identify websites".

# Troubleshooting Log

Issues actually hit while setting this up, and their fixes — kept here for next time.

| Symptom                                                                                                                              | Cause                                                                  | Fix                                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Apache: "Invalid command 'ProxyPreserveHost'" mod_proxy_http not loaded                                                              | ProxyPreserveHost                                                      | Uncomment both LoadModule lines in httpd.conf (Part B1)                                                                         |
| Browser: 500 Internal Server Error; mod_proxy loaded but mod_proxy_http still commented. Mod log shows AH01144 "No protocol handler" | mod_proxy_http not loaded                                              | Still commented. Uncomment module proxy_http_module specifically                                                                |
| openssl: "Can't open C:\Apache24\openssl.conf: [Errno 2] No such file or directory"                                                  | openssl.conf not found                                                 | Path of openssl.conf is not correct. It should be C:\Program Files\Apache Software Foundation\Apache2.4\apache\conf\openssl.cnf |
| certreq: "Denied by Policy Module. ... Requesting identity not found in the local machine's certificate store"                       | Requesting identity not found in the local machine's certificate store | Start the Web Server (Part C2); if the machine is not domain-joined, use the local machine's certificate store                  |
| Apache fails to start after adding the SSL module                                                                                    | SSL module not loaded                                                  | Check the path of the SSL module. It should be C:\Program Files\Apache Software Foundation\Apache2.4\apache\mod_ssl\mod_ssl.c   |
| Browser: NET::ERR_CERT_AUTHORITY_INVALID                                                                                             | Browser doesn't trust the issuing CA                                   | On a PC: gpupdate /force, or check certmgr.msc has the CA under Trusted Root Certification Authorities                          |
| Browser: NET::ERR_CERT_COMMON_NAME_INVALID                                                                                           | Common Name (CN) does not match the domain name                        | Enable SSL in the host (Part C1) and reissue the certificate with the correct CN                                                |
| Works in Chrome/Edge but not Firefox                                                                                                 | Firefox uses its own certificate store                                 | Enable Windows enterprise_roots.enabled in about:config, or import the certificate into Firefox                                 |

Prepared as an internal setup reference for the SAP-ERP portal (mipl.com internal network).