



Group Internal Root CAs Certificate Store

SSL Certificate Environment Variables for Corporate Networks

[SSL Certificate Environment Variables for Corporate Networks](#)

[What Are SSL Certificate Environment Variables and Why Do You Need Them?](#)

[What You'll Need Before Starting](#)

[The Complete List of SSL Certificate Environment Variables](#)

[Core Variables \(Most Important\)](#)

[Language-Specific Variables](#)

[Python Development](#)

[Node.js Development](#)

[Java Development](#)

[Ruby Development](#)

[Javascript Development](#)

[Version Control](#)

[Cloud Services & APIs](#)

[Container & DevOps Tools](#)

[HashiCorp Tools](#)

[Specialized Tools](#)

[How to Set Up on Windows](#)

[Method 1: Using System Properties \(Recommended\)](#)

[How to Set Up on macOS](#)

[Method 1 - Automated](#)

[What does it do?](#)

[Method 2 - Semi-Manual - Security Engineering Handbook](#)

[Method 3 - Manual - Using Terminal \(Recommended\)](#)

[Verification and Testing](#)

[Test Common Tools](#)

[Check Environment Variables](#)

[Troubleshooting Common Issues](#)

[Problem: Variables not taking effect](#)

[Problem: Connection Errors \(not related to SSL\)](#)

[Problem: Certificate file not found](#)

[Problem: Still Getting SSL Errors](#)

[Problem: Java Applications Still Fail](#)

[Best Practices](#)

[Security Considerations](#)

[Conclusion](#)

What Are SSL Certificate Environment Variables and Why Do You Need Them?



<< I don't really want a lecture... I just want to solve my SSL issues >>

In that case, for MacOS, go to: [Group Internal Root CAs Certificate Store | Method 1 Au](#)

tomated

For Windows, I haven't scripted it so you'll need to read the below to understand the issue (and solve it)...

✉ << Do I have to built a cacert.pem myself ? >>

Well, not really... here's one byt it'll eventually become outdated! [cacert.pem](#)

Up-to-date as of: 3 Sept 2025

If you're working on a corporate network, you've probably encountered SSL certificate errors when trying to use development tools, package managers, or cloud services. These errors typically look like:

This happens because your company uses custom Certificate Authorities (CAs) or proxy servers that intercept SSL traffic.

Most development tools don't automatically trust these corporate certificates, so you need to configure them manually using environment variables.



- "SSL certificate verify failed"
- "CERTIFICATE_VERIFY_FAILED"
- "unable to get local issuer certificate"

What You'll Need Before Starting

1. **Your company's certificate bundle file** - Usually a `.pem` file containing Base64 Root Signing CAs
2. **Administrative access** to modify **system** environment variables on your machine
You can however change the **user** environment variable without needing administrative access.
3. **Knowledge of which development tools you use** - This determines which variables you need to set

The Complete List of SSL Certificate Environment Variables

Core Variables (Most Important)

These work with the most common development tools:

- `SSL_CERT_FILE` - Used by OpenSSL, Python urllib, and many other libraries
- `REQUESTS_CA_BUNDLE` - Python requests library
- `GIT_SSL_CAINFO` - Git version control system
- `NODE_EXTRA_CA_CERTS` - Node.js & npm package manager
- `AWS_CA_BUNDLE` - AWS CLI and SDKs
- `CURL_CA_BUNDLE` - cURL command-line tool

I don't think this is needed on the SOE because cURL inherits what Keychain Access or Windows Certificates Store trust and our provisioning team did a great work at trusted internal Signing Root CAs. However it doesn't hurt to set it anyway...

▼ The bigger list...

Language-Specific Variables

Python Development

- `PIP_CERT` - pip package manager

Node.js Development

- `NODE_EXTRA_CA_CERTS` - Node.js runtime
- `NPM_CONFIG_CAFILE` - npm package manager
- `YARN_CAFILE` - Yarn package manager

Java Development

- `JAVA_TOOL_OPTIONS` - All Java applications (set to `-Djavax.net.ssl.trustStore=/path/to/truststore`)
- `MAVEN_OPTS` - Maven build tool

Ruby Development

- `BUNDLE_SSL_CA_CERT` - Ruby Bundler

Javascript Development

- `DENO_CERT` - Deno JavaScript runtime

Version Control

- `GIT_SSL_CAINFO` - Git version control system

Cloud Services & APIs

- `AWS_CA_BUNDLE` - AWS CLI and SDKs
- `CLOUDSDK_AUTH_CORE_CUSTOM_CA_CERTS_FILE` - Google Cloud SDK

Container & DevOps Tools

- `DOCKER_CERT_PATH` - Docker Desktop
- `DOCKER_TLS_VERIFY` - Docker TLS verification
- `HELM_CA_FILE` - Helm Kubernetes package manager

HashiCorp Tools

- `CONSUL_CACERT` - Consul
- `VAULT_CACERT` - Vault

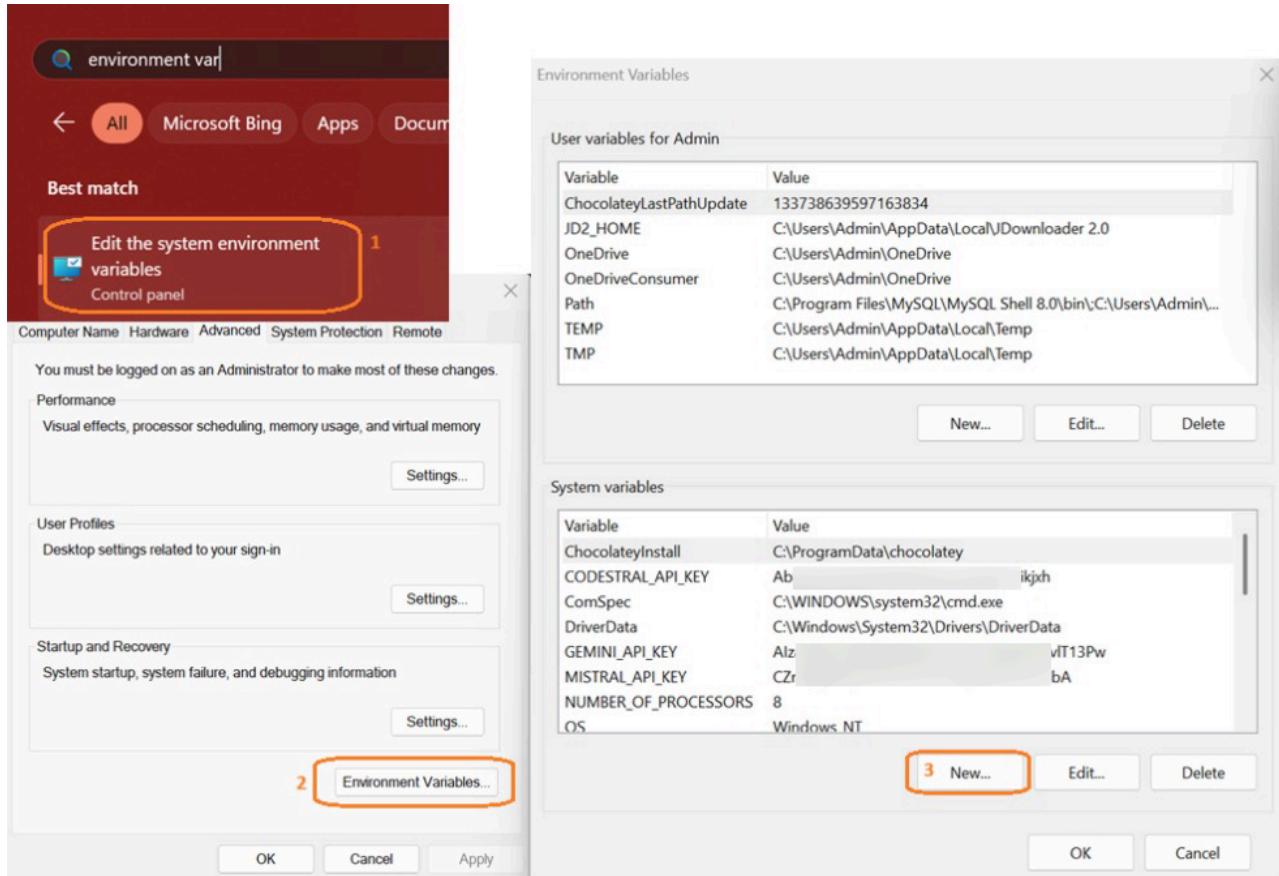
Specialized Tools

- `GRPC_DEFAULT_SSL_ROOTS_FILE_PATH` - gRPC libraries
- `TAPLO_EXTRA_CA_CERTS` - Taplo TOML toolkit

How to Set Up on Windows

Method 1: Using System Properties (Recommended)

1. Press `Win + R`, type `sysdm.cpl`, and press Enter
2. Click the "Advanced" tab
3. Click "Environment Variables"
4. Under "User variables" (for your account only) or "System variables" (for all users), click "New"
5. Enter the variable name (e.g., `SSL_CERT_FILE`)
6. Enter the full path to your certificate bundle (e.g., `C:\\certs\\company-bundle.pem`)
7. Click OK to save
8. Repeat for each variable you need



Method 2: Using Command Prompt (PowerShell)

```

1 # Set for current user
2 [Environment]::SetEnvironmentVariable("SSL_CERT_FILE", "C:\certs\company-bundle.pem",
  "User")
3 [Environment]::SetEnvironmentVariable("REQUESTS_CA_BUNDLE", "C:\certs\company-bundle.pem",
  "User")
4 [Environment]::SetEnvironmentVariable("CURL_CA_BUNDLE", "C:\certs\company-bundle.pem",
  "User")
5
6 # For system-wide (requires admin privileges)
7 [Environment]::SetEnvironmentVariable("SSL_CERT_FILE", "C:\certs\company-bundle.pem",
  "Machine")

```

Method 3: Create a Batch Script

Create a file called `setup-certs.bat`:

```

1 @echo off
2 set CERT_PATH=C:\certs\company-bundle.pem
3
4 setx SSL_CERT_FILE "%CERT_PATH%"
5 setx REQUESTS_CA_BUNDLE "%CERT_PATH%"
6 setx CURL_CA_BUNDLE "%CERT_PATH%"
7 setx GIT_SSL_CAINFO "%CERT_PATH%"
8 setx NODE_EXTRA_CA_CERTS "%CERT_PATH%"
9 setx NPM_CONFIG_CAFILE "%CERT_PATH%"
10 setx PIP_CERT "%CERT_PATH%"
11 setx AWS_CA_BUNDLE "%CERT_PATH%"

```

```
12
13 echo Certificate environment variables have been set!
14 echo Please restart your command prompt or IDE for changes to take effect.
15 pause
```

Run this batch file as Administrator.

How to Set Up on macOS

Method 1 - Automated

```
1 git clone https://github.com/Enelass/proxy-ssl-trust.git
2 proxy-ssl-trust/SSL/PEM_Var.sh
```

What does it do?

1. It downloads a Public CA Store from the Mozilla foundation containing all Public Root CAs
2. It extract each Trusted Signing Root CAs from Keychain and add it to the store above.
(Expired, untrusted, leaf and Intermediate CAs are excluded)
 - a. Group Internal Root CAs are added so that internal *.cba are trusted
 - b. SSL Forward Inspection CAs (Prisma) are trusted
 - c. and others...
3. It checks the certificate store against corrupted entries...
4. It creates the environment variables in your default Shell config (whether that is **bash** , **zsh** or **fish** ...)

```

Summary: The purpose of this script is to provide various CLI on MacOS with environment variables referencing a custom PEM certificate store including public and internal Root certificate authorities. This will resolve number of connectivity issues where CLI not relying on the MacOS Keychain Access can still trust internally signed servers using an Internal Root CA and trust https connections where SSL forward inspection is performed and signed on a fly by a proxy/ngfw internal CA.
Author: florian@photonsec.com.au          github.com/Enelass
Runtime: currently running as bidabefl
This script was invoked directly... Setting variable for standalone use...
2025-09-03 14:52:08 Info  - --- SCRIPT: /Users/bidabefl/Github/proxy-ssl-trust/SSL/PEM_Var.sh ---
2025-09-03 14:52:08 Info  - This script will download a public Certificate Store and add Internal CAs to it
2025-09-03 14:52:08 Info  - It will then create environment variable in the user shell config and reference it...
2025-09-03 14:52:08 Info  - Downloading and/or locating custom PEM certificate
2025-09-03 14:52:08 Warning - Custom PEM certificate exists already. It will not be retrieved from the internet...
2025-09-03 14:52:08 Info  - Custom PEM certificate can be found at /Users/bidabefl/.config/cacert/cacert.pem
2025-09-03 14:52:08 Info  - --- SCRIPT: /Users/bidabefl/Github/proxy-ssl-trust/SSL/PEM_Check.sh ---
2025-09-03 14:52:08 Info  - The purpose of this script is to scan a PEM Certificate Store to ensure its integrity...
Summary: This script checks the integrity of PEM files containing certificates by parsing them and validating each certificate using OpenSSL.
It reads the PEM file, lists the certificates, and verifies each one. If any certificate is invalid, it logs an error. The script shows a progress bar as it processes the certificates. Additionally, it provides an option to input the PEM file path if not specified.
Author: florian@photonsec.com.au          github.com/Enelass
2025-09-03 14:52:08 Info  - Processing certificates in /Users/bidabefl/.config/cacert/cacert.pem. Please wait...
2025-09-03 14:52:12 Success - No issue within this Certificate Store
2025-09-03 14:52:17 Info  - It will be patched with Internal Root CAs from the MacOS Keychain Access:
2025-09-03 14:52:17 Info  - CBA Engineering JSS Built-in Certificate Authority was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - CBA Group Root CA G3 was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - CBA Group Test Root CA G3 was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - CBA SOE Root G1 was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - CBAInternalRootCA was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - Charles Proxy CA [21 Jun 2017, C02RH0YDFVH8] was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - Commonwealth Bank of Australia CA was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - prisma2.np was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - prisma2025cdsa.cba was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - prisma2025cdsa.np was already trusted in our custom certificate store
2025-09-03 14:52:17 Info  - prisma3rsa.cba was already trusted in our custom certificate store
2025-09-03 14:52:17 Success - Custom Certificate Store now includes our internal Root CAs
2025-09-03 14:52:17 Info  - Looking for CA related Environment Variables in Shell Config /Users/bidabefl/.zshrc
2025-09-03 14:52:17 Warning - AWS_CA_BUNDLE was already set in in the user's Shell Config file
2025-09-03 14:52:17 Info  - curl actually export AWS_CA_BUNDLE="/Users/bidabefl/.config/cacert/cacert.pem"
2025-09-03 14:52:17 Info  - If this entry is incorrect, please correct it manually with a text editor...
2025-09-03 14:52:17 Warning - GIT_SSL_CAINFO was already set in in the user's Shell Config file
2025-09-03 14:52:17 Info  - export GIT_SSL_CAINFO="/Users/bidabefl/.config/cacert/cacert.pem"
2025-09-03 14:52:17 Info  - If this entry is incorrect, please correct it manually with a text editor...
2025-09-03 14:52:17 Warning - NODE_EXTRA_CA_CERTS was already set in in the user's Shell Config file
2025-09-03 14:52:17 Info  - export NODE_EXTRA_CA_CERTS="/Users/bidabefl/.config/cacert/cacert.pem"
2025-09-03 14:52:17 Info  - If this entry is incorrect, please correct it manually with a text editor...
2025-09-03 14:52:17 Warning - REQUESTS_CA_BUNDLE was already set in in the user's Shell Config file
2025-09-03 14:52:17 Info  - export REQUESTS_CA_BUNDLE="/Users/bidabefl/.config/cacert/cacert.pem"
2025-09-03 14:52:17 Info  - If this entry is incorrect, please correct it manually with a text editor...
2025-09-03 14:52:17 Warning - SSL_CERT_FILE was already set in in the user's Shell Config file
2025-09-03 14:52:17 Info  - export SSL_CERT_FILE="/Users/bidabefl/.config/cacert/cacert.pem"
2025-09-03 14:52:17 Info  - If this entry is incorrect, please correct it manually with a text editor...

```

Output

Method 2 - Semi-Manual - Security Engineering Handbook

⚠ The command below will work, but it will trust all certificates in the Keychain, including Leaf and Intermediate CAs, which is unnecessary. Worse, it will also add untrusted and expired certificates.

Also you will still have to declare the environment variables via `export` in your Shell config file (`~/.zshrc`, `~/.bashrc` or `~/.bash_profile`)

```

security find-certificate -a -p
/Library/Keychains/System.keychain
/System/Library/Keychains/SystemRootCertificates.keychain
~/Library/Keychains/login.keychain-db >
~/ca_bundle.pem

```

source: <https://engineering-handbook.pages.commbank.io/knowledge-base/mac-guides/CBA-root-certificate#instructions-terminal>

Method 3 - Manual - Using Terminal (Recommended)

Add these lines to your shell profile file (`~/.zshrc` for zsh or `~/.bash_profile` for bash):

```
1 # SSL Certificate Configuration
2 export CERT_PATH="/Users/Shared/certs/company-bundle.pem"
3
4 # Core variables
5 export SSL_CERT_FILE="$CERT_PATH"
6 export REQUESTS_CA_BUNDLE="$CERT_PATH"
7 # export ... etc
8 # export CURL_CA_BUNDLE="$CERT_PATH" - Unnecessary because curl actually uses the Keychain Access which already trust those Internal Root Signing CAs
```

After editing the file, run:

```
1 source ~/.zshrc # or source ~/.bashrc
```

Verification and Testing

After setting up the environment variables, verify they're working:

Test Common Tools

```
1 # Test curl
2 curl -vI https://google.com
3
4 # Test Python requests
5 python -c "import requests; print(requests.get('https://google.com').status_code)"
6
7 # Test npm
8 npm config get cafile
9
10 # Test Git
11 git config --get http.sslCAInfo
```

Check Environment Variables

Windows (Command Prompt):

```
1 echo %SSL_CERT_FILE%
2 set | findstr CERT
```

Windows (PowerShell):

```
1 $env:SSL_CERT_FILE
2 Get-ChildItem Env: | Where-Object Name -like "*CERT*"
```

macOS/Linux:

```
1 echo $SSL_CERT_FILE
2 env | grep CERT
```

Troubleshooting Common Issues

Problem: Variables not taking effect

Solution: Restart your terminal, command prompt, or IDE completely. Environment variables are only loaded when a new process starts.

Problem: Connection Errors (not related to SSL)

- See [CLI - Why you should not set CNTLM nor Prisma](#)

Problem: Certificate file not found

Solution:

- Verify the certificate file exists at the specified path
- Check file permissions (must be readable)
- Use forward slashes (/) in paths, even on Windows when possible

Problem: Still Getting SSL Errors

Solutions:

1. **Verify certificate format** - Should be PEM format with proper headers
2. **Check if you need additional certificates** - Some tools may require the full certificate chain
3. **Tool-specific configuration** - Some tools have their own certificate settings that override environment variables
4. **Possibly Strict-Validation Issue**, like with Python 3.13: [SSL Trust - Missing "Authority Key Identifier"](#)

Problem: Java Applications Still Fail

Solution: Java uses a different certificate store format. You may need to:

1. Import certificates into Java's truststore using `keytool`
2. Set `JAVA_TOOL_OPTIONS` to point to a custom truststore file

Best Practices

1. **Store certificates in a standard location:**
 - Windows: `C:\\\\certs\\\\` or `%PROGRAMDATA%\\\\certs\\\\`
 - macOS: `/Users/Shared/certs/` or `~/.config/cacert/`
2. **Use a single certificate bundle file** when possible to avoid maintaining multiple copies
3. **Keep certificates updated** - Check what certificates are trusted in the OS Certificate Store
(this is maintained by our provisioning teams SCCM & JAMF)

Security Considerations

- **File permissions:** Ensure certificate files are readable but not writable by unauthorised users
- **Path security:** Store certificates in secure locations that regular users cannot modify
- **Regular updates:** Keep certificates current to maintain security
- **Note on sensitivity:** These certificate bundles contain only public CA certificates for establishing trust; they do not include private keys and are not used for decryption.)

Conclusion

Setting up SSL certificate environment variables properly will save you countless hours of debugging SSL errors in corporate environments.

While it may seem overwhelming at first, most developers only need to set up the variables for the tools they actually use.

Start with the core variables (`SSL_CERT_FILE` , `REQUESTS_CA_BUNDLE` ,
`CURL_CA_BUNDLE`) and add language-specific ones as needed.

Remember to restart your development environment after making changes,

With this setup complete, your development tools should work seamlessly within our corporate network environment.