

Network Box SSL Proxy Group Policy Deployment Guide

Active Directory • Windows 11 and Windows Server

Updated 5 October 2026

Deploy the public SSL Proxy certificate authority (CA) certificate to domain-joined Windows computers through Active Directory Group Policy. This establishes CA trust for HTTPS traffic inspected by Network Box; proxy routing and inspection policy are configured separately.

1. Download the deployment certificate

1. From the network served by your Network Box, open its approved GUI address. The standard address is **https://my.network-box.com:4243**; your administrator may provide a different hostname.
2. On the GUI sign-in page, select the **green SSL ribbon** shown below. This opens the certificate download options.

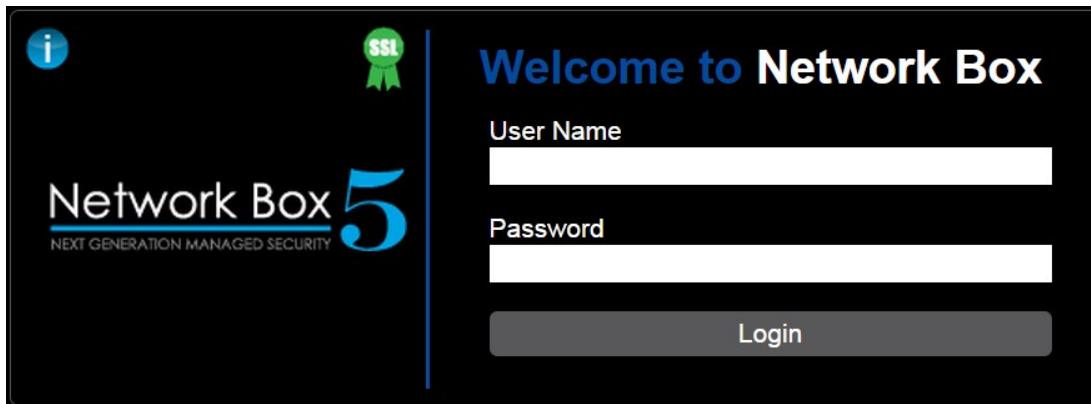


Figure 1. Select the green SSL ribbon on the Network Box GUI sign-in page.

Select **DOWNLOAD** beside **DER** and save the certificate to the computer where you will edit the GPO. **DER is the format to use for this Windows Group Policy procedure.**

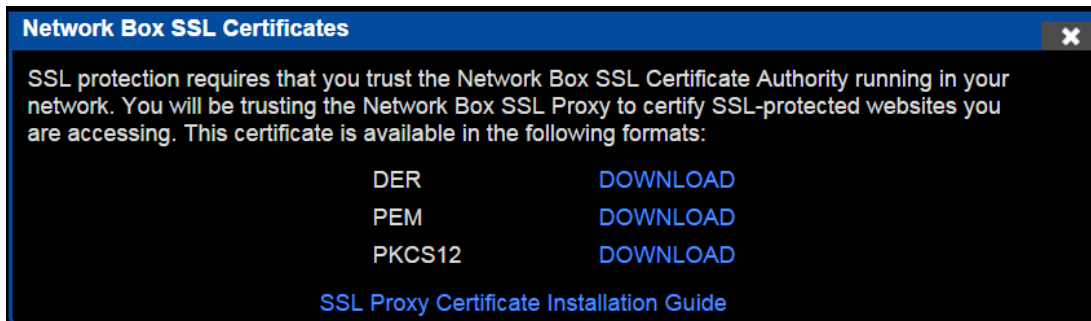


Figure 2. The GUI offers DER, PEM and PKCS12; choose DER for Windows Group Policy.

Confirm the certificate's subject, issuer, validity dates, and fingerprint against your deployment's approved values before distributing it. Compare fingerprints using the same hash algorithm. Use the **public CA certificate**; a CA private key or PKCS12 (.pfx/.p12) file is not required.

2. Configure the Group Policy

Before you begin

- Use **Group Policy Management** on Windows Server or a workstation with the Group Policy Management tools installed through RSAT. The account needs permission to create or edit the GPO and link it to the intended scope.
- Target **AD domain-joined computer accounts**. Devices must be able to receive policy from the domain, including through the corporate VPN where needed. Start with a pilot computer OU or computer security group. [2]
- Confirm that the downloaded file is the intended **root CA certificate**. If your deployment also uses a separate intermediate CA, obtain and verify its public certificate separately.

Create and scope a dedicated GPO

1. Open **Group Policy Management** (gpmc.msc). Expand **Forest > Domains > your domain**.
2. Right-click the pilot OU containing the target **computer accounts**, then select **Create a GPO in this domain, and Link it here**. Use a descriptive name, such as **Network Box SSL Proxy CA**. Alternatively, create a GPO under **Group Policy Objects** and link it to the pilot OU.
3. Confirm that the link is enabled and **Computer Configuration** is enabled. For group filtering, use a **security group containing computer accounts** and grant it **Read** and **Apply Group Policy**. Remove broad Apply permissions that would defeat the pilot scope; retain appropriate Read permissions under **Delegation > Advanced**. [2]

Import the root CA certificate

Right-click the GPO and select **Edit**. In the Group Policy Management Editor, expand this path: [1]

**Computer Configuration > Policies > Windows Settings >
Security Settings > Public Key Policies >
Trusted Root Certification Authorities**

1. Right-click **Trusted Root Certification Authorities** and select **Import**. In the Certificate Import Wizard, select **Next**.
2. Browse to the **DER** certificate downloaded on page 1. If the file is hidden by the filter, select **All Files**. Select the file, then **Open > Next**.
3. Confirm **Place all certificates in the following store** and **Trusted Root Certification Authorities**. Select **Next**, review the summary, then select **Finish**. Confirm the successful import and the certificate entry in the GPO.

A .cer or .crt filename alone does not identify its encoding. The public DER CA import does not require a private-key password. Import a **separate intermediate CA** into **Intermediate Certification Authorities** only when your deployment requires it. **Trusted Publishers** is not the store for establishing proxy TLS CA trust.

3. Verify on pilot computers

Allow the GPO change to replicate between domain controllers. Perform these checks on each pilot **endpoint**, using an administrator account.

Refresh computer policy

Open **Command Prompt as administrator** and run: [3, 4]

```
gpupdate /target:computer /force
gpresult /scope computer /r
```

Confirm **Network Box SSL Proxy CA** (or your chosen name) appears under **Applied Group Policy Objects** for the computer. Follow any restart prompt. If a computer was newly added to a filtering group, restart it so its group membership can be refreshed.

Check the installed CA and HTTPS traffic

1. Press **Windows + R**, enter **certlm.msc**, and open the **Local Computer** certificate console. Expand **Trusted Root Certification Authorities > Certificates**. [5]
2. Open the deployed CA certificate. Verify its subject, issuer, validity dates, and fingerprint against the approved certificate. Compare the same hash algorithm; the Windows **Thumbprint** field commonly displays SHA-1.
3. Close and reopen the browser. Visit an HTTPS site that your administrator confirms is selected for Network Box inspection. Open the connection's certificate details and check that the presented chain leads to the expected proxy CA, with no certificate warning.
4. Repeat the test in each browser and business application used by the pilot. After successful validation, extend the GPO link or filtering to the approved production computers.

If a check fails

Symptom	What to check
GPO is not applied	Computer OU and GPO link; Read and Apply permissions; inheritance; WMI filters; domain connectivity and replication. Check the computer policy results, not only user policy.
GPO applies; CA is missing	Verify the certificate entry and root store in the GPO. Refresh computer policy, honor restart prompts, and inspect certlm.msc on the endpoint.
CA is present; HTTPS fails	Check CA identity and validity, device time, the presented certificate chain, and the inspection policy. Use the complete browser error when investigating.
Browser works; application fails	Identify the application's actual trust store. Java, bundled OpenSSL tools, containers, and other runtimes may require their own CA configuration.

A site that is excluded from inspection may load successfully without using the proxy CA. An uninspected site alone does not verify this deployment.

4. Browser support and CA lifecycle

Browsers and other applications

Microsoft Edge and Google Chrome on Windows recognize locally managed roots, including roots distributed through Group Policy. Chrome applies added local trust to TLS over TCP; QUIC has different trust behavior. Check proxy routing and transport if the certificate chain does not show the expected inspection path. [6, 7]

Current Firefox on Windows also searches Windows certificate stores for third-party roots, including Group Policy roots. If you manage this explicitly, Mozilla's **Certificates > ImportEnterpriseRoots** policy can enable it. OS roots used by Firefox may not appear as separate entries in Firefox's certificate manager. [8, 9]

This GPO deploys Windows certificate trust. Applications with their own trust stores—such as Java runtimes, some Python/curl/Git configurations, Node.js, Linux in WSL, and containers—need separate validation and, where required, separate CA installation. See the companion **Network Box SSL Proxy Certificate Installation Guide** for those procedures.

Rotate or retire a proxy CA

For a planned rotation, distribute the new approved CA and verify trust on target computers **before** Network Box starts using it. Include temporarily offline devices in the rollout plan. Keep the old CA only for the approved transition period, then retire it after confirming the new inspection chain works.

Remove the retired CA from every GPO that deploys it, refresh computer policy, and verify its absence on representative endpoints. Identify any remaining copies installed manually or by another management tool, and remove them through their original deployment method. Restart affected applications and confirm the retired CA is no longer trusted. [5, 10]

References

Technical references checked 5 October 2026. Menu labels may vary by Windows version.

1. Microsoft — [Distribute public certificates by Group Policy](#)
2. Microsoft — [Group Policy scope and filtering](#)
3. Microsoft — [gpupdate command](#)
4. Microsoft — [gpresult command](#)
5. Microsoft — [Inspect certificates and manage stores](#)
6. Microsoft — [Edge certificate verification](#)
7. Chromium — [Chrome Root Store FAQ](#)
8. Mozilla — [Set up Certificate Authorities in Firefox](#)
9. Mozilla — [Certificates enterprise policy](#)
10. Microsoft — [Group Policy root-store processing](#)

Screenshot credit: original Network Box GUI reference images from page 1 of SSLProxyCertificate-IE.pdf. Both images are embedded in this guide; appearance may vary by release.