digitalscepter

The Decryption Blueprint:
Building A Two-Tier CA for SSL Inspection

ZACHRY SUM - DIRECTOR OF TECHNICAL SERVICES, DIGITAL SCEPTER
JON ROBINSON - PRESIDENT, DIGITAL SCEPTER

November 19th, 2024

Service Catalog

- Firewall migrations
- Firewall operations - mass upgrades, backups, change/remove/add
- Firewall Healthchecks
- Panorama design
- Zero Trust Network Access
- Network Segmentation
- MFA
- SSL Decryption
- Inbound SSL Inspection
- Remote Access (“Always on”)
- Securing Cloud infrastructure
- Dual ISP redundancy
- Network engineering
- Endpoint Security/EDR/MDR

Contracts

- CMAS
- NASPO
- SPURR
- OMNIA Partners

Vendors

- Palo Alto Networks
- Crowdstrike
- SentinelOne
- Okta
- Arista
- Juniper
- HPe/Aruba
- AWS
- Microsoft/Azure
- Proofpoint
- Zscaler
- Gigamon
- Rapid7
- Knowbe4
- Netskope

Agenda

1. General PKI Overview
2. Disclaimer
3. Offline Root CA Buildout
4. Issuing CA Buildout
5. SSL Inspection With Palo Alto

General PKI Overview

What is PKI?

Public Key Infrastructure is a system designed to create, manage, distribute, use, store, and revoke digital certificates and public-private key pairs

- **Purpose:** Manages creation, distribution, and revocation of digital certificates and public-private key pairs
- **Role:** Enables secure, trusted communication across digital platforms (websites, emails, networks)
- **Applications:** Widely used in HTTPS, secure email, enterprise access, and code signing

Components of PKI

- **Public and Private Keys:** Each user or device within a PKI system has a unique public and private key pair. The public key is openly distributed, while the private key is kept secure. These keys are mathematically linked and work together for secure data exchange.

- **Digital Certificates:** Digital certificates, often issued by trusted Certificate Authorities (CAs), link a public key to an entity's identity. Certificates provide information about the certificate owner, including name, public key, expiration date, and the CA’s digital signature, which certifies its authenticity.

Components of PKI (continued)

- **Certificate Authorities (CA):** CAs are trusted entities responsible for issuing and verifying digital certificates. They validate the identity of certificate applicants before issuing certificates.

- **Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP):** CRLs and OCSPs manage and check the status of certificates, indicating whether a certificate is valid, expired, or revoked.

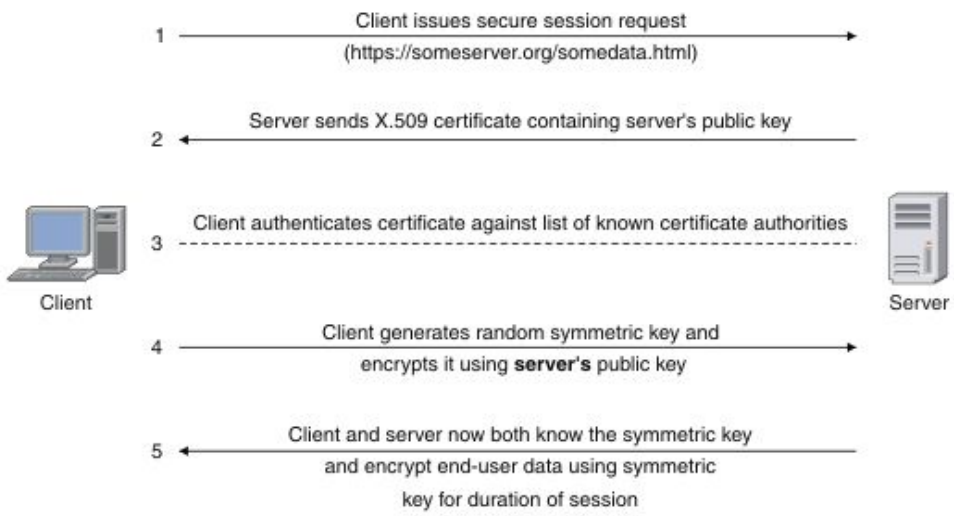
How It Works - According To ChatGPT

- **Me:** Can you diagram how a client and server negotiate an SSL connection?
- **ChatGPT:**

digitalscepter

How It Really Works

- Different cipher suites and key exchange algorithms will have different steps in establishing an SSL/TLS session
- The process sees the client and server exchanging supported protocol versions, cypher suites, etc.
- During this process a key is securely exchanged to convert to symmetric encryption for transmitting data for the remainder of the session



digitalscepter

Disclaimer

digitalscepter

Risks (continued)

When deploying a private CA it's important to understand the risks involved and how to properly secure and maintain your CA

1. **Key Management Risks:** Compromise of the CA's private key or improper key storage can undermine the entire system.
2. **Certificate Management Challenges:** Mismanagement of certificate issuance, revocation, or expiration can lead to security vulnerabilities and outages.
3. **Compliance and Policy Risks:** Failure to adhere to standards or enforce strict policies can result in weak security and exploitation.
4. **Operational Overhead:** High costs, complexity, and reliance on skilled staff make maintaining a secure CA resource-intensive.
5. **Insider Threats:** Malicious or careless insiders with access to the CA can misuse it to issue fraudulent certificates.
6. **Reputation Risks:** Compromise of the CA undermines trust in the organization's infrastructure and services.

Risk Mitigation

It is recommended to consider risk avoidance through the below options:

1. **Use a Trusted Third-Party CA:** Outsource certificate issuance and management to established providers to offload operational and compliance burdens.
2. **Deploy Hardware Security Modules (HSMs):** Securely store private keys to prevent compromise.
3. **Automate Certificate Management:** Use tools to track, issue, renew, and revoke certificates automatically.
4. **Enforce Strict Access Controls:** Limit and monitor access to CA infrastructure to prevent insider threats.
5. **Implement Strong Policies and Audits:** Regularly review and enforce certificate policies and perform security audits.
6. **Adopt a Hybrid Approach:** Use external CAs for public-facing certificates and an internal CA for specific internal needs.

Offline Root CA Buildout

digitalscepter

Before You Start

1. Your root CA is the linchpin to your PKI's integrity
2. If it's compromised, any device that trusted your root CA is at risk, and any service that leveraged certificate authentication should be reviewed for signs of compromise
3. With this in mind, here are some considerations for your root CA:
    a. It should be kept powered off
    b. Only powered up to renew CA certs or publish new CRL
    c. It should not be domain-joined
    d. It should have no network connection
    e. Ideally, keys would be stored on a Hardware Security Module (HSM)
4. Your root CA should only need to issue one certificate, and that is to your Issuing (Intermediate) CA

Build Root CA

1. Once the deployment platform is determined, proceed with installing a hardened Windows installation
2. Create file **C:\Windows\CAPolicy.inf**:

```
[Version]
Signature="$Windows NT$"
[Certsrv_Server]
RenewalKeyLength = 4096
RenewalValidityPeriod = Years
RenewalValidityPeriodUnits = 10
AlternateSignatureAlgorithm = 0
CRLPeriod = Years
CRLPeriodUnits = 10
CRLDeltaPeriod = Days
CRLDeltaPeriodUnits = 0
```

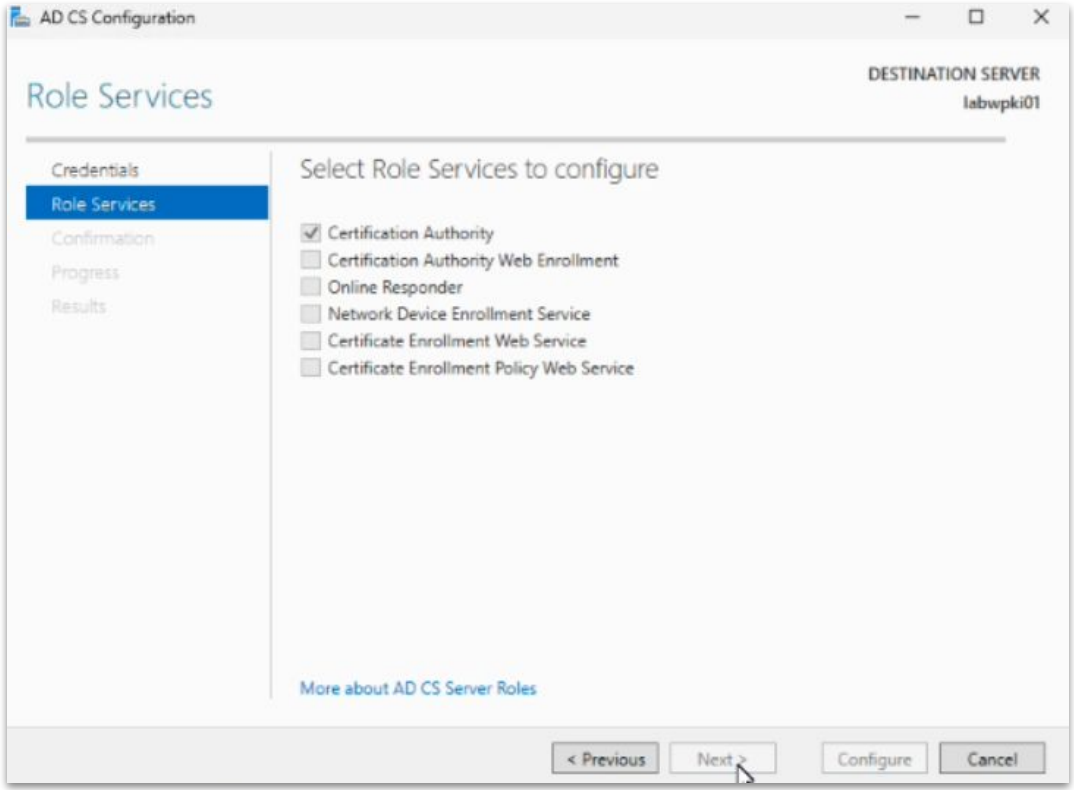
3. In **Server Manager**, install the **Active Directory Certificate Services** Role on the server, selecting only the **Certification Authority** role service during installation

Build Root CA (continued)

1. Once installation completes, proceed with configuring the Certification Authority role using the settings below:

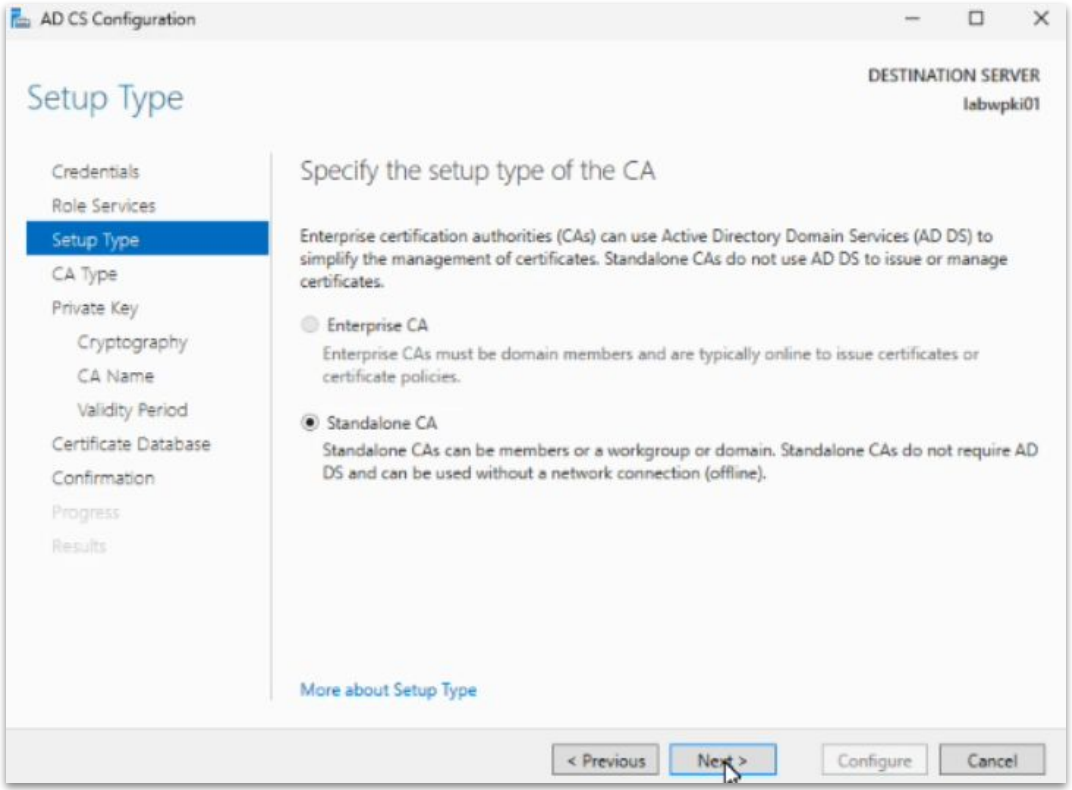
Setting	Value
Specify credentials to configure role services	A user that is a local administrator
Specify the setup type of the CA	Standalone CA
Specify the type of the CA	Root CA
Specify the type of the private key	Create a new private key
Specify the cryptographic Options	RSA#Microsoft Software Key Storage Provider, 4096, SHA256
Specify the name of the CA	Populate common name of your choice, leave other fields
Specify the Validity Period	<=10 years (think golf, lower is better...and more difficult)

Build Root CA (continued)



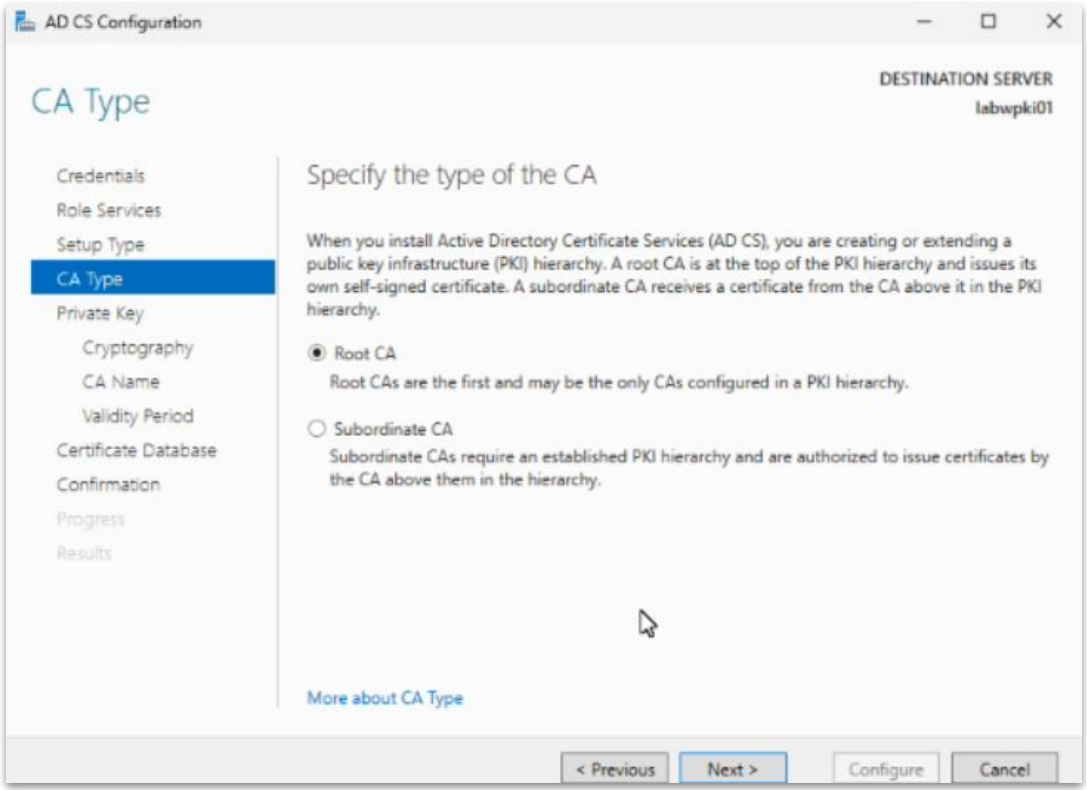
digitalscepter

Build Root CA (continued)



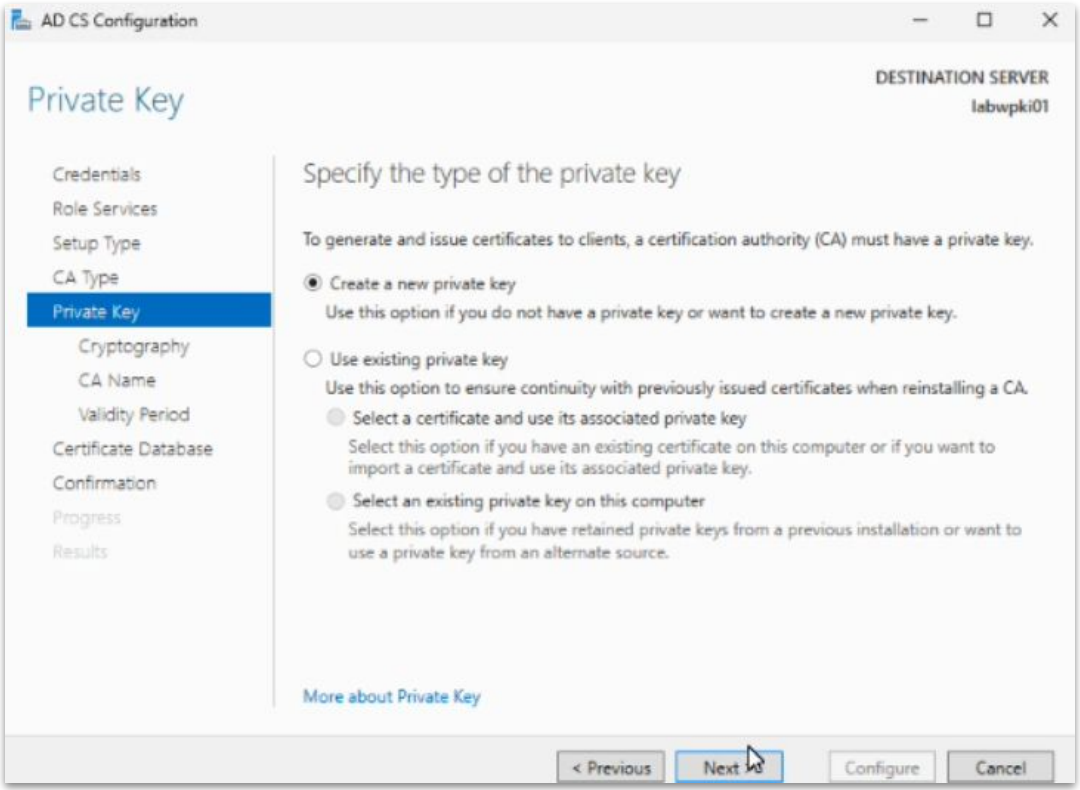
digitalscepter

Build Root CA (continued)



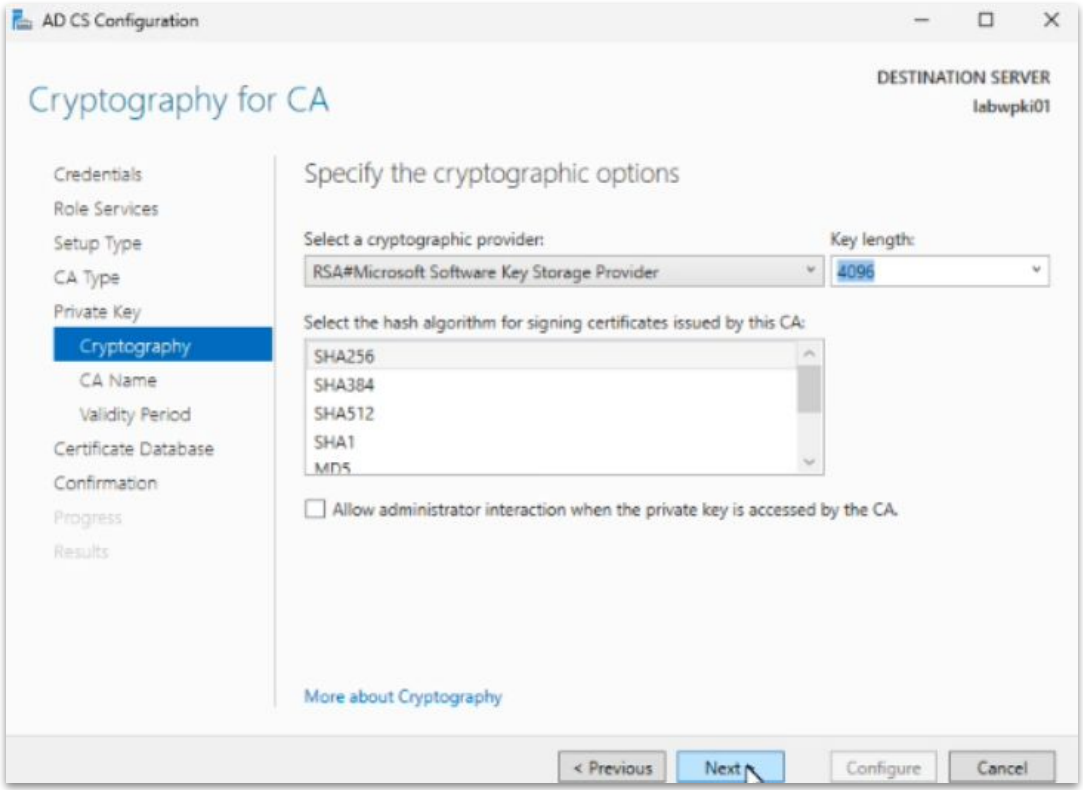
digitalscepter

Build Root CA (continued)



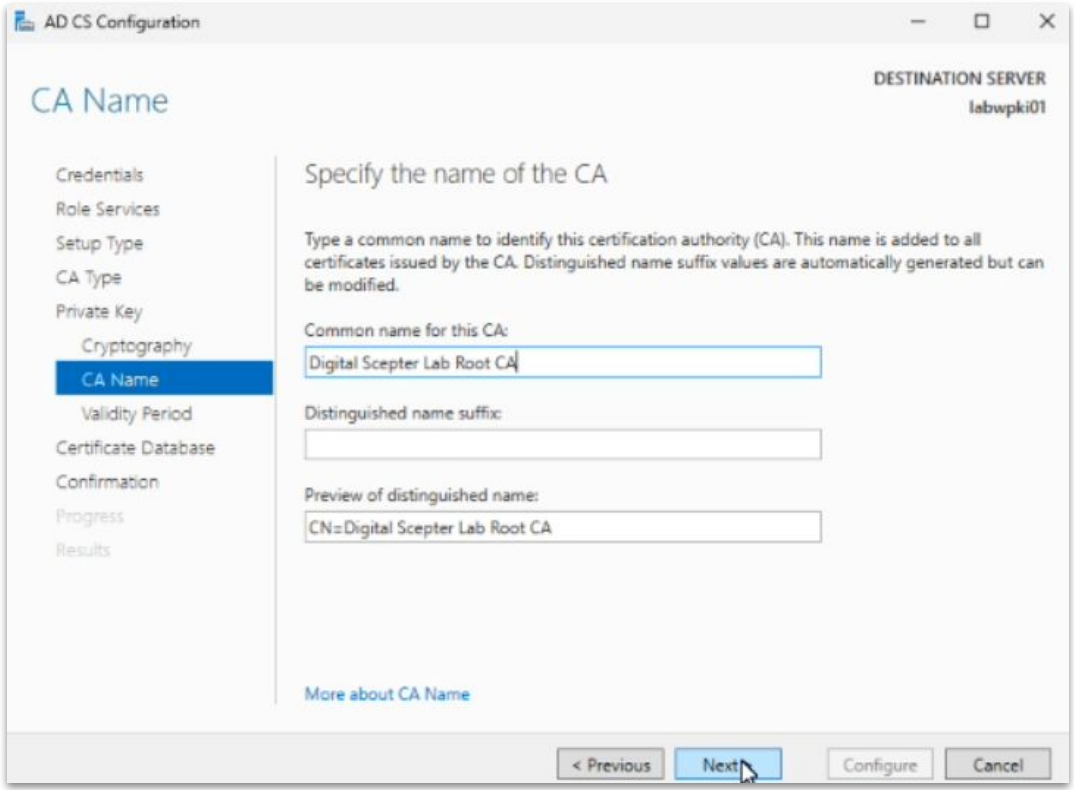
digitalscepter

Build Root CA (continued)



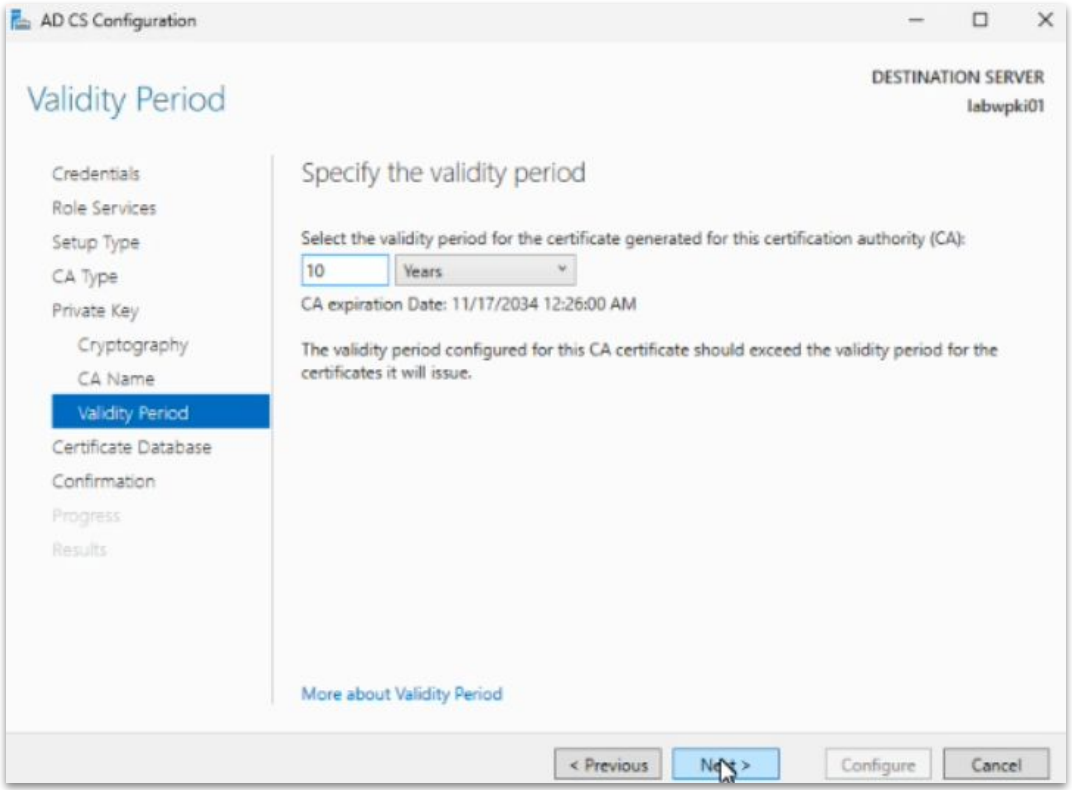
digitalscepter

Build Root CA (continued)



digitalscepter

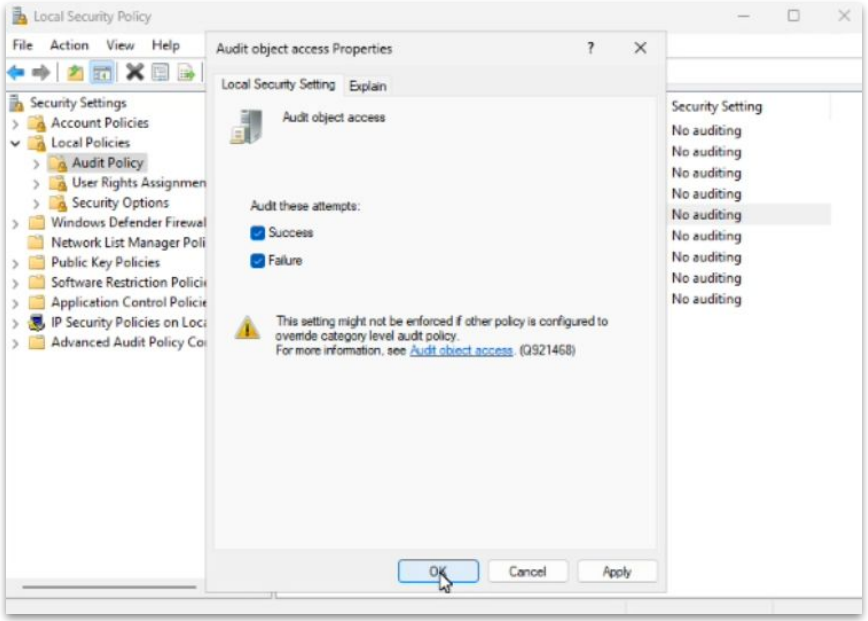
Build Root CA (continued)



digitalscepter

Build Root CA (continued)

1. Open **Local Security Policy** and navigate to **Local Policies** > **Audit Policy**
2. Open **Audit object access** and check **Success** and **Failure**



digitalscepter

Build Root CA (continued)

1. Open an **Administrative Command Prompt** and enter the following commands, modifying the distinguished name for your domain Configuration partition

```
certutil.exe -setreg CA\DSConfigDN "CN=Configuration,DC=your,DC=domain,DC=com"
certutil.exe -setreg CA\ValidityPeriodUnits 5
certutil.exe -setreg CA\ValidityPeriod "Years"
certutil.exe -setreg CA\CRLPeriodUnits 52
certutil.exe -setreg CA\CRLPeriod "Weeks"
certutil.exe -setreg CA\CRLOverlapPeriodUnits 12
certutil.exe -setreg CA\CRLOverlapPeriod "Hours"
certutil.exe -setreg CA\CRLDeltaPeriodUnits 0
certutil.exe -setreg CA\AuditFilter 127
net stop certsvc
net start certsvc
```

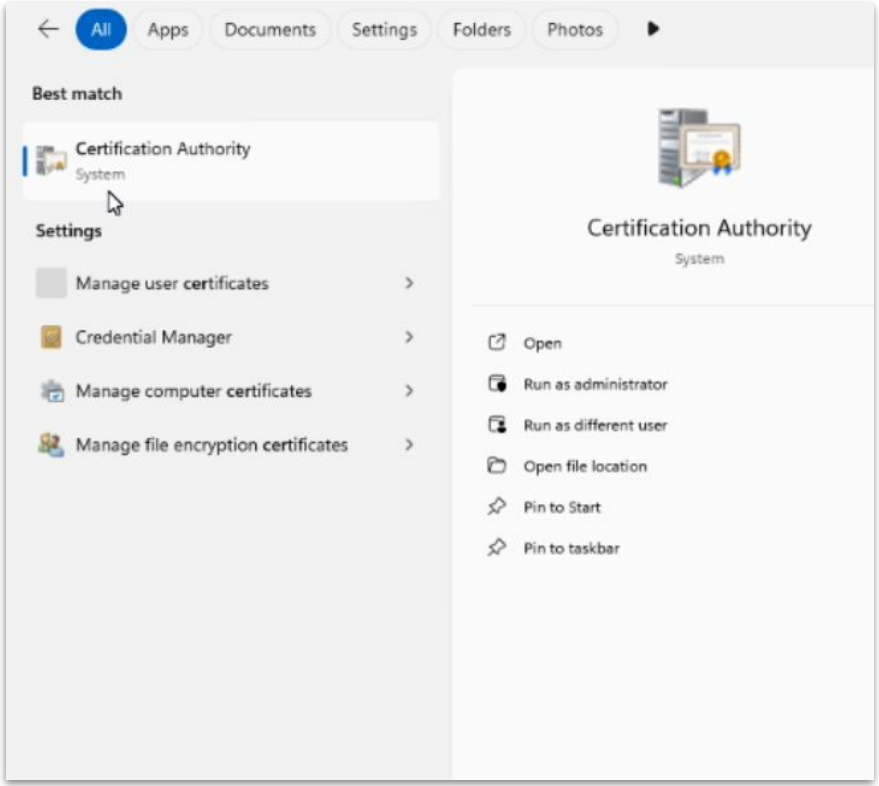
Build Root CA (continued)

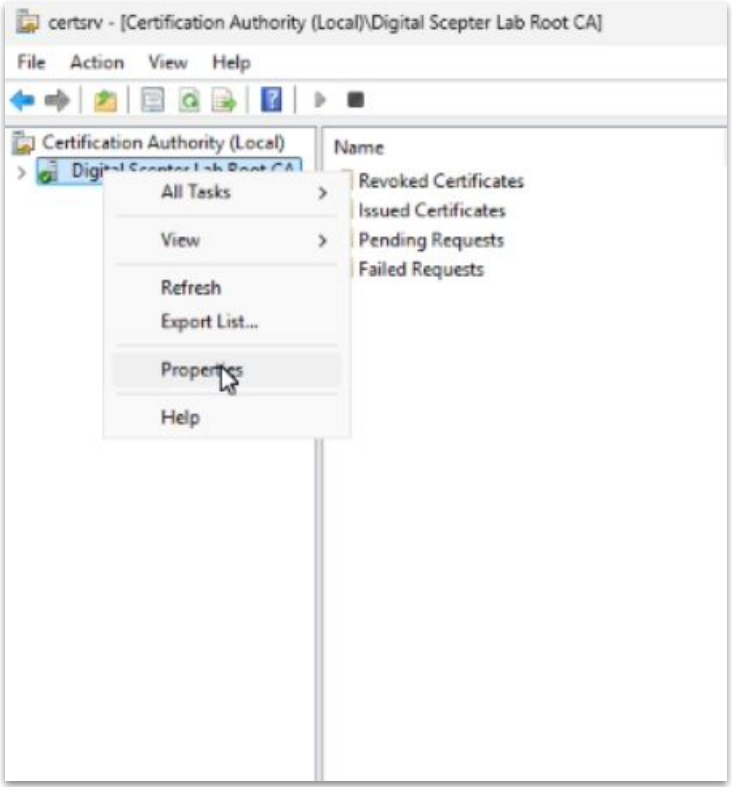
1. Open **Certification Authority** right click your CA and select **Properties**
2. Click **Extensions**
3. Select the **file://...** location and click **Remove**
4. Click **Add** and enter path found in chart below
5. Check box **Include in CRLs...** and **Include in the CDP extension...**
6. Click **Select Extension** dropdown and select **Authority Information Access**
7. Select the **file://...** location and click **Remove**
8. Click **Add** and enter path found in chart below
9. Check box **Include in the AIA extension...**
10. Make sure to update italicized values with your own

Setting	Value
CDP Extension Location	http://*pki.your.domain.com*/CertData/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
AIA Extension Location	http://*pki.your.domain.com*/CertData/<ServerDNSName>_<CaName><CertificateName>.crt

digitalscepter

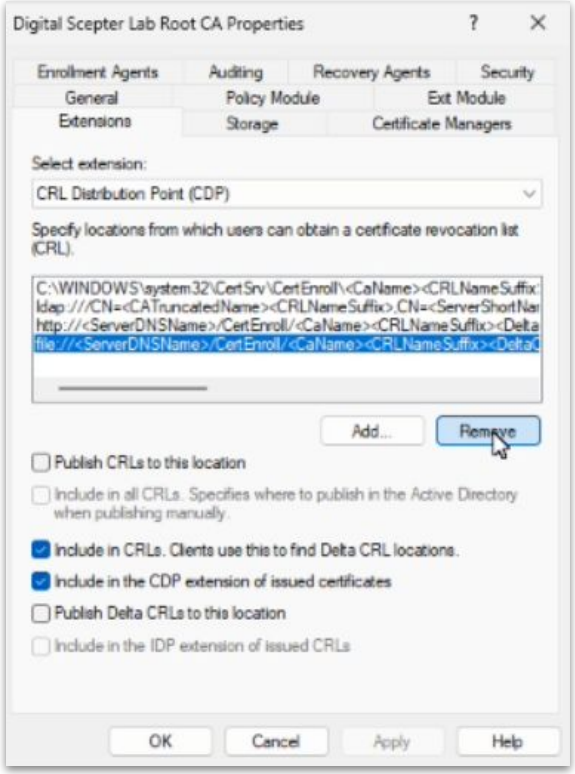
Build Root CA (continued)

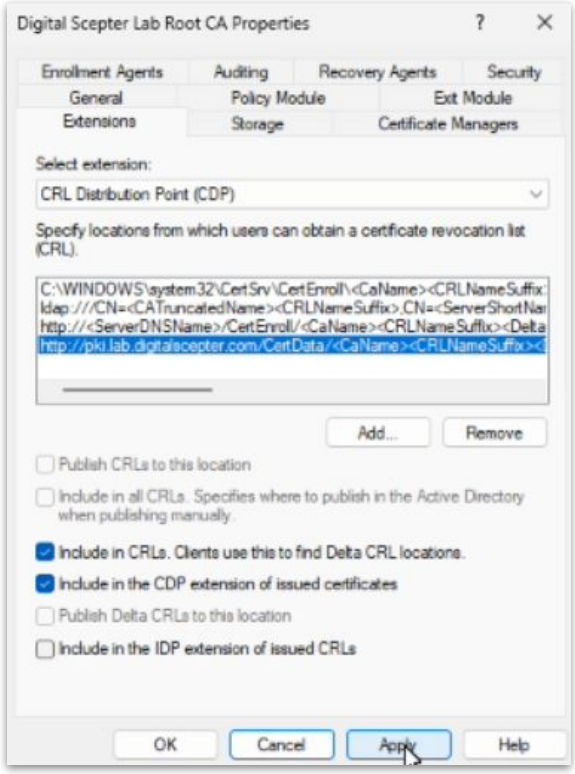




digitalscepter

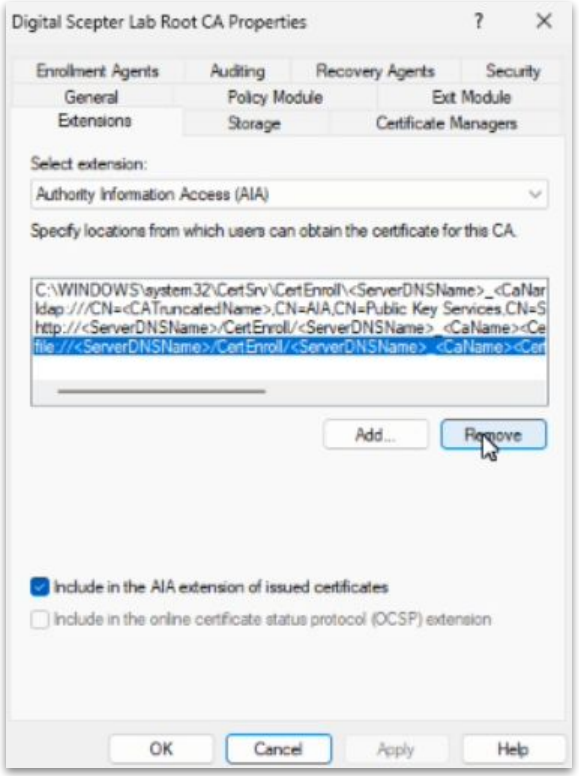
Build Root CA (continued)

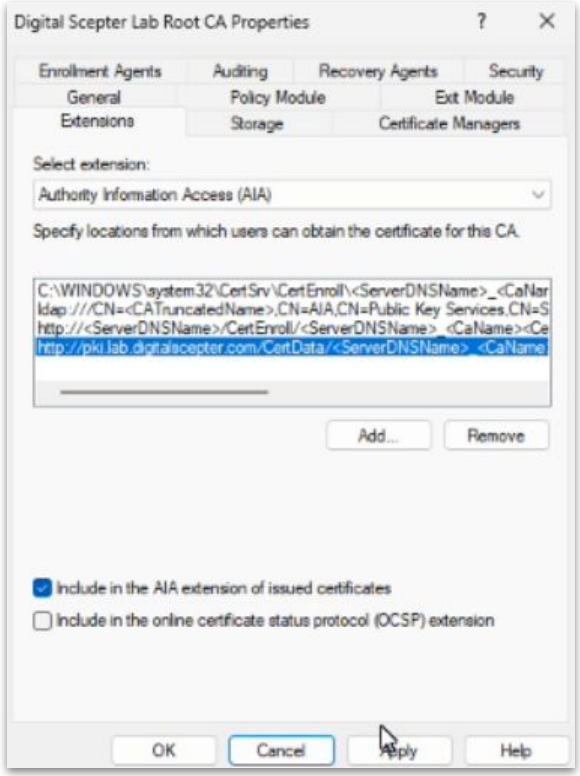




digitalscepter

Build Root CA (continued)

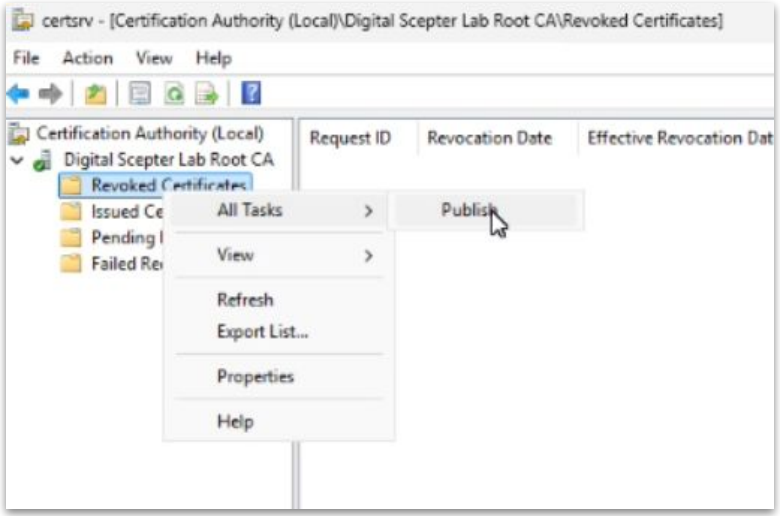


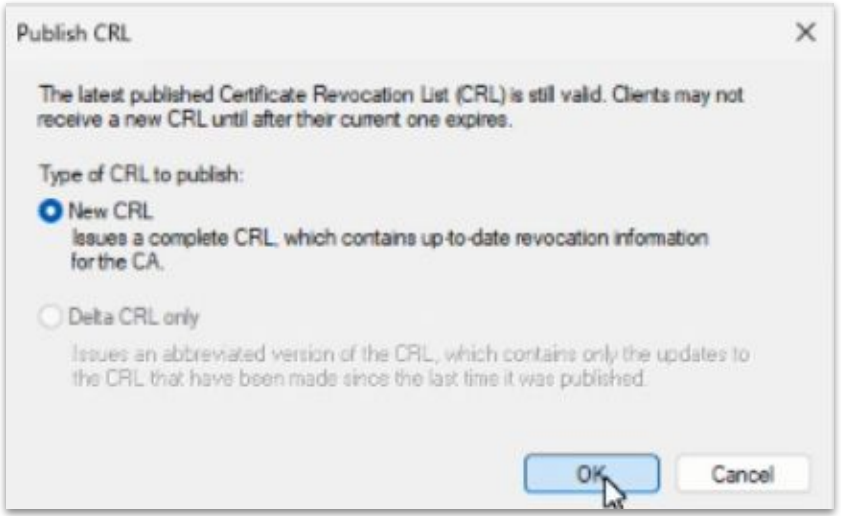


digitalscepter

Build Root CA (continued)

1. Open **Certification Authority** and expand your CA, right-click **Revoked Certificates** and click **All Tasks** > **Publish**. Select **New CRL** and click **OK**

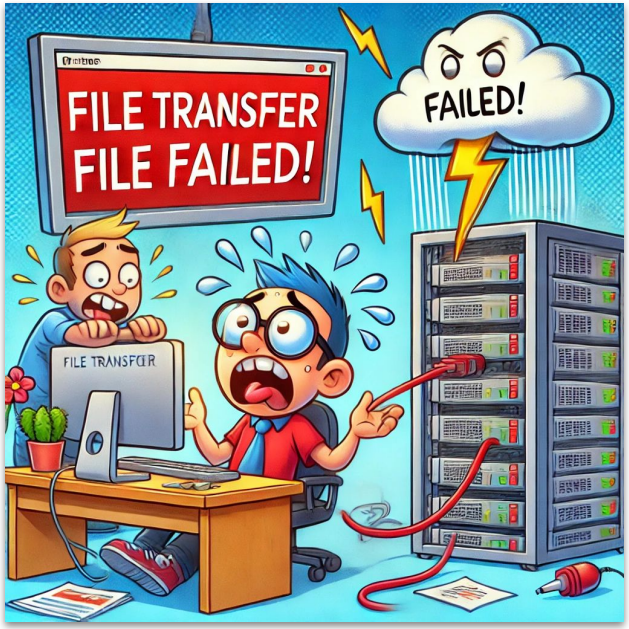




digitalscepter

Build Root CA (continued)

1. We should now have two files in **C:\Windows\System32\CertSrv\CertEnroll**
   a. One certificate (the root CA certificate which contains the public key only)
   b. One CRL that we published in the prior step
2. These need to be copied to the CertData folder on the Issuing CA
3. But wait, you don't have a network connection
4. Whether virtualized or physical, USB device is generally your best bet
5. For virtual, an existing hard disk is an option
6. Can do virtual floppy too depending on hypervisor



digitalscepter

Build Root CA (finished?)

1. You're DONE!
2. Ok, with the root only
3. So you're half done!
4. Well, a little less than half actually, there's this thing–nevermind, we'll get to it

Issuing CA Buildout

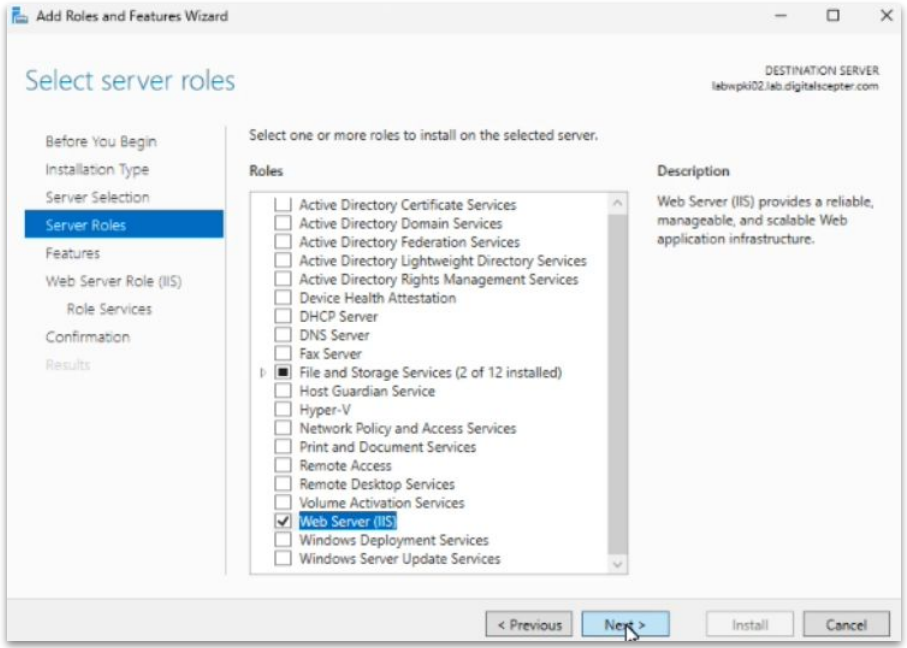
digitalscepter

Before You Start

1. Your issuing CA will be domain-joined
2. This will simplify cert deployment, renewal, etc.
3. Permissions on cert templates are paramount
    a. If these are too lax, certificates can be provisioned and misused, exposing the organization to significant risk
4. CDP, AIA and OCSP provide end users certificate revocation information as well as your CA certificates when they weren't provided as part of the server chain. This is primarily pulled via http/https.
5. If users outside of your network will need to access services using internal certificates, then you will likely need to make these services available from outside your network
6. In this case a separate server on a DMZ network would be ideal for hosting these files
7. If it is purely internal, it is not uncommon to keep this local to the issuing CA
8. For purpose of this buildout, we will consolidate these functions to the issuing CA

Prepare Issuing CA

1. In **Server Manager**, install the **Web Server (IIS)** role on the server, leaving all defaults selected



digitalscepter

Prepare Issuing CA (continued)

1. Open **IIS Manager** and expand your server > Sites, and right-click **Default Web Site** then click **Add Virtual Directory**
   a. Alias: CertData
   b. Physical Path: C:\CertData
2. Click **CertData** virtual directory and double-click **Directory Browsing**. Click **Enable** in the Actions column
3. Enable Double Escaping on Default Web Site (required to host delta CRL's)

```
C:\Windows\System32> cd %windir%\system32\inetsrv
C:\Windows\System32\inetsrv> Appcmd set config "Default Web Site" /section:system.webServer/Security/requestFiltering -allowDoubleEscaping:True
C:\Windows\System32\inetsrv> iisreset
```

Build Issuing CA

1. Create file **C:\Windows\CAPolicy.inf**, replacing italicized values below:

```
[Version]
Signature = "$Windows NT$"
[PolicyStatementExtension]
Policies = AllIssuancePolicy,InternalPolicy
[AllIssuancePolicy]
OID = 2.5.29.32.0
[InternalPolicy]
OID = 1.2.3.4.1455.67.89.5
Notice = "Digital Scepter Lab Certification Authority and any issued certificates are for internal usage only."
URL = http://pki.lab.digitalscepter.com/cps.html
[Certsrv_Server]
RenewalKeyLength = 4096
RenewalValidityPeriod = Years
RenewalValidityPeriodUnits = 5
AlternateSignatureAlgorithm = 0
LoadDefaultTemplates = 1
```

2. Install **Active Directory Certificate Services** Role on the server, selecting the **Certification Authority** and **Certificate Authority Web Enrollment** role services during installation

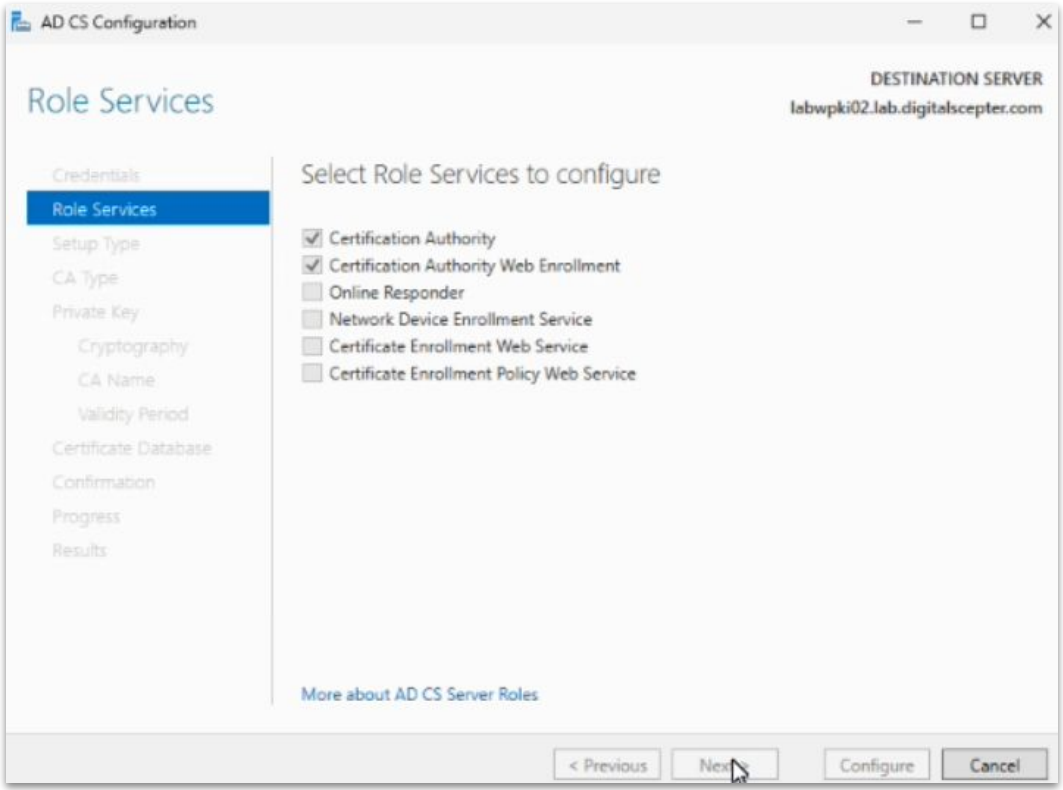
digitalscepter

Build Issuing CA (continued)

1. Once installation completes, proceed with configuring the **Certification Authority** and **Certification Authority Web Enrollment** roles using the settings below:

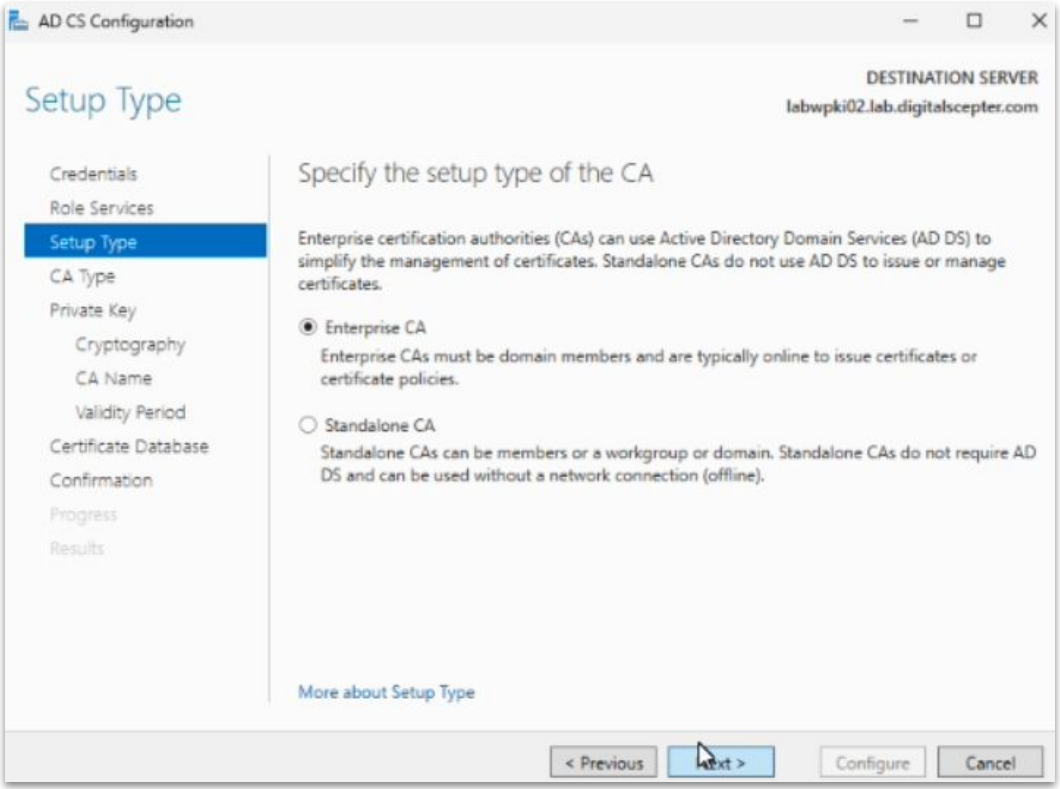
Setting	Value
Specify credentials to configure role services	A user that is both a local administrator and member of **Enterprise Admins**
Specify the setup type of the CA	Enterprise CA
Specify the type of the CA	Subordinate CA
Specify the type of the private key	Create a new private key
Specify the cryptographic Options	RSA#Microsoft Software Key Storage Provider, 4096, SHA256
Specify the name of the CA	Populate common name of your choice, leave other fields
Request a certificate from parent CA	Save a certificate request to file on the target machine

Build Issuing CA (continued)



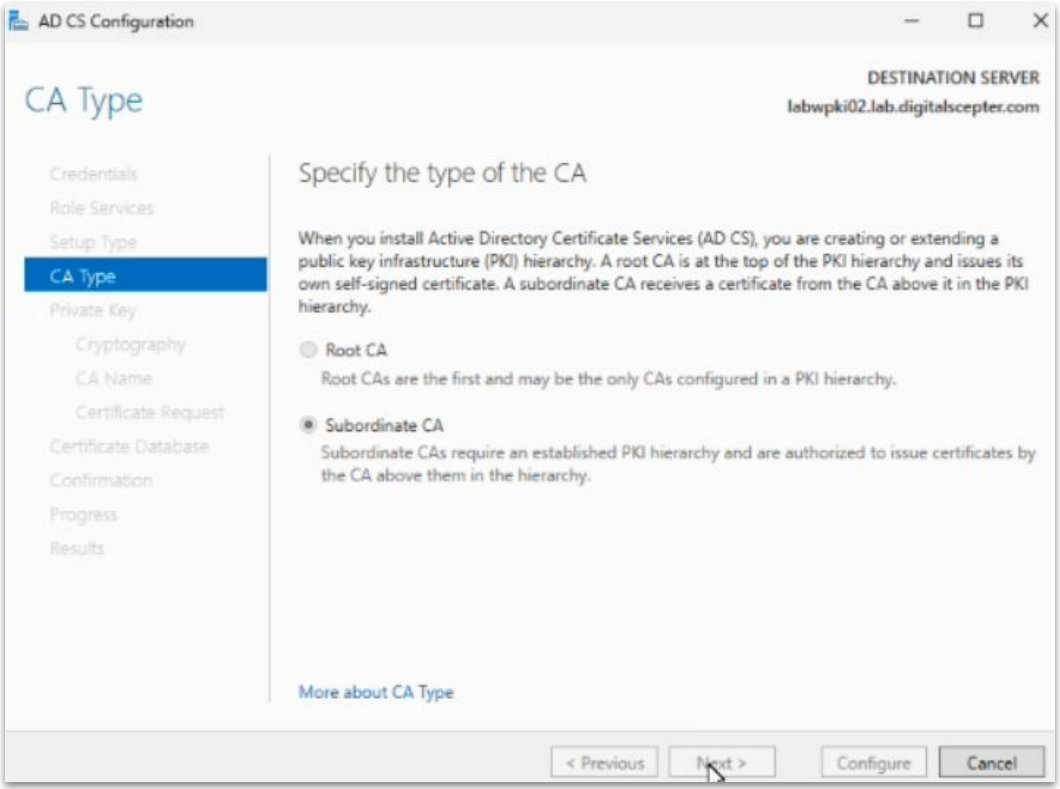
digitalscepter

Build Issuing CA (continued)



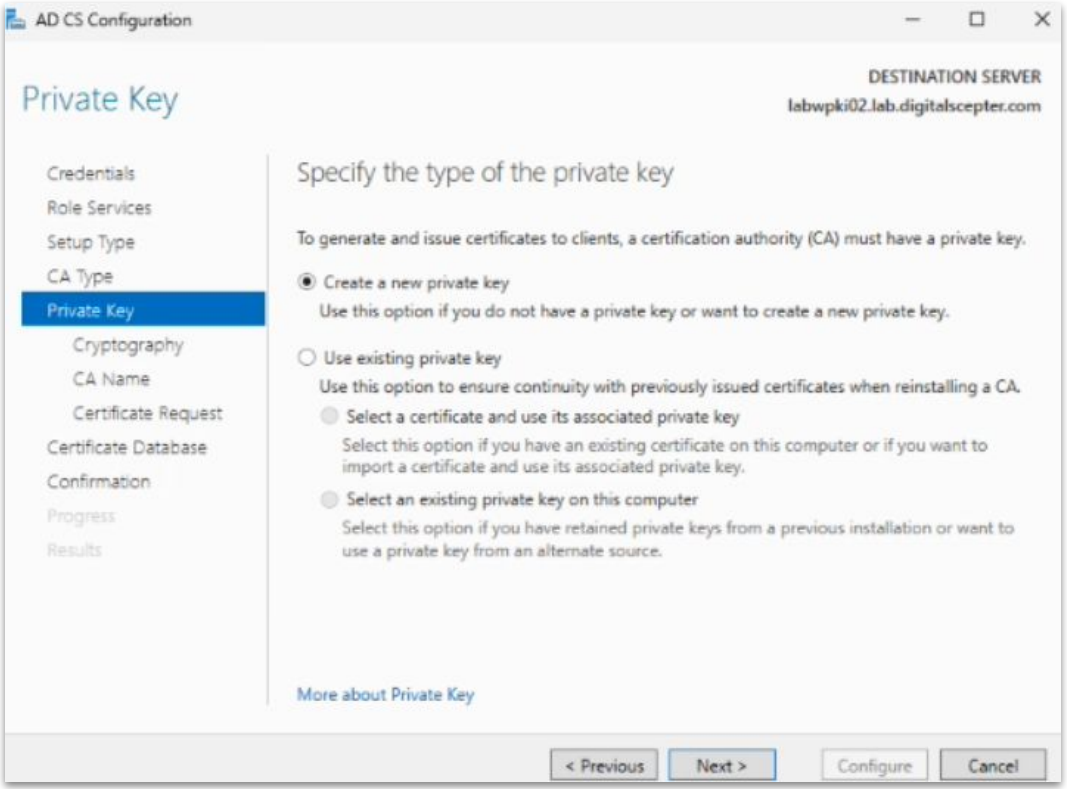
digitalscepter

Build Issuing CA (continued)



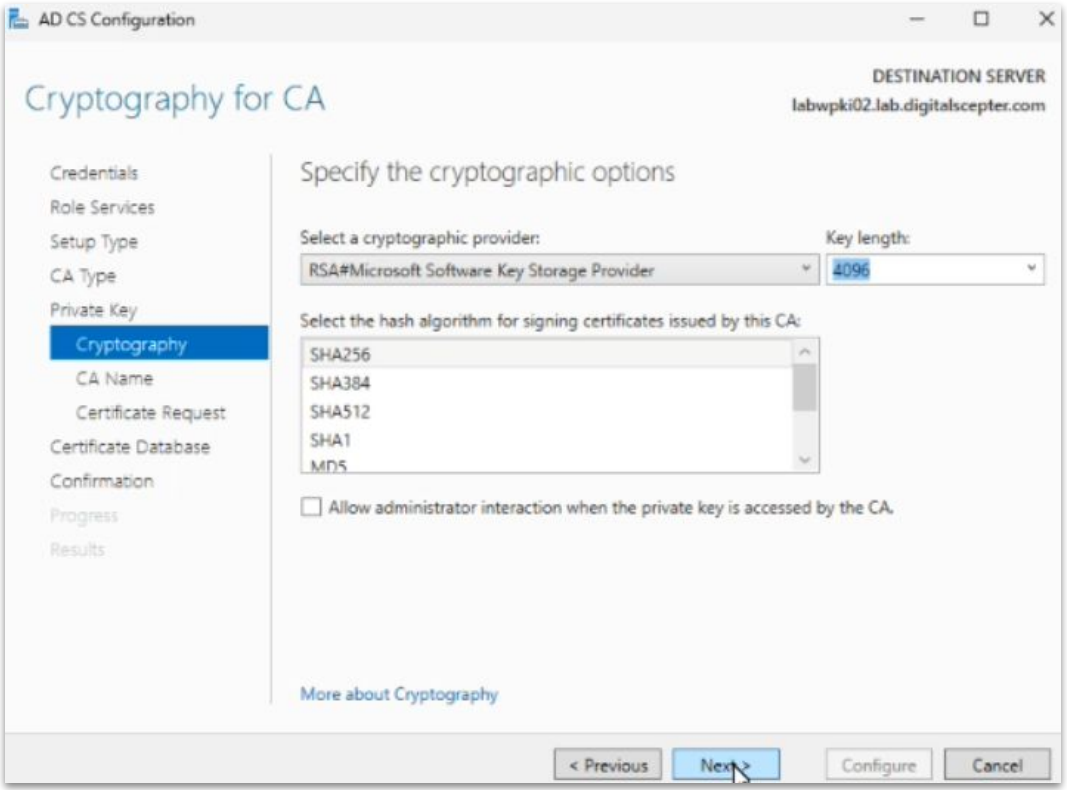
digitalscepter

Build Issuing CA (continued)



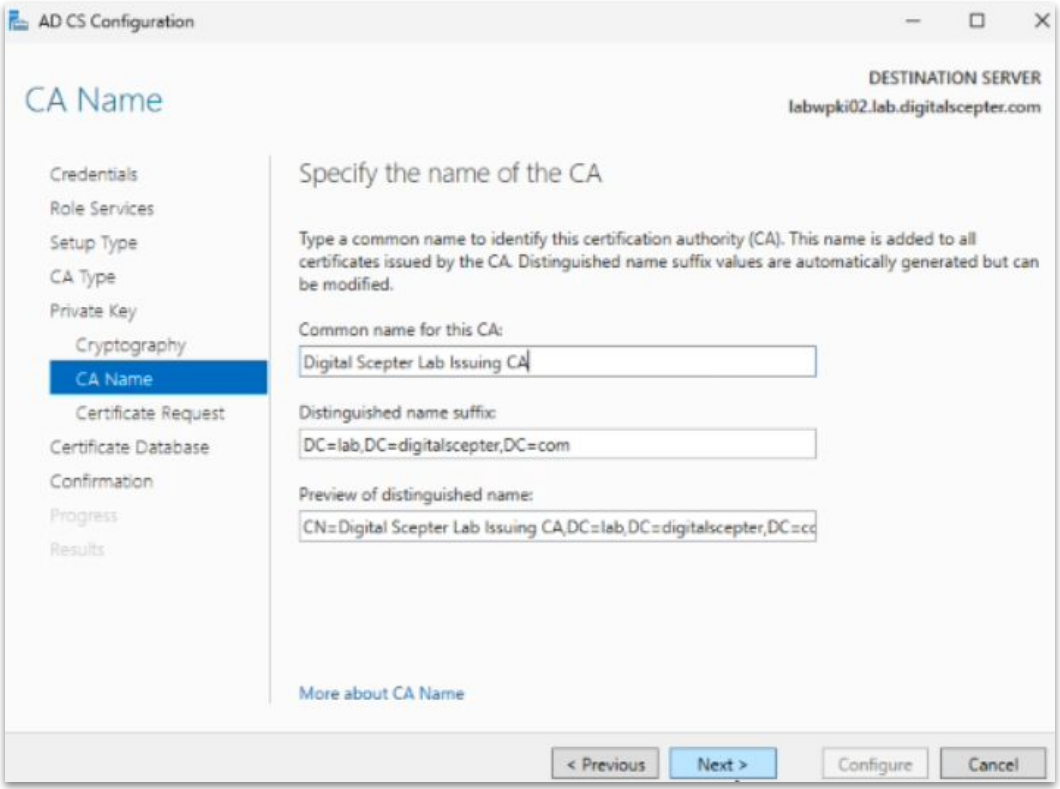
digitalscepter

Build Issuing CA (continued)



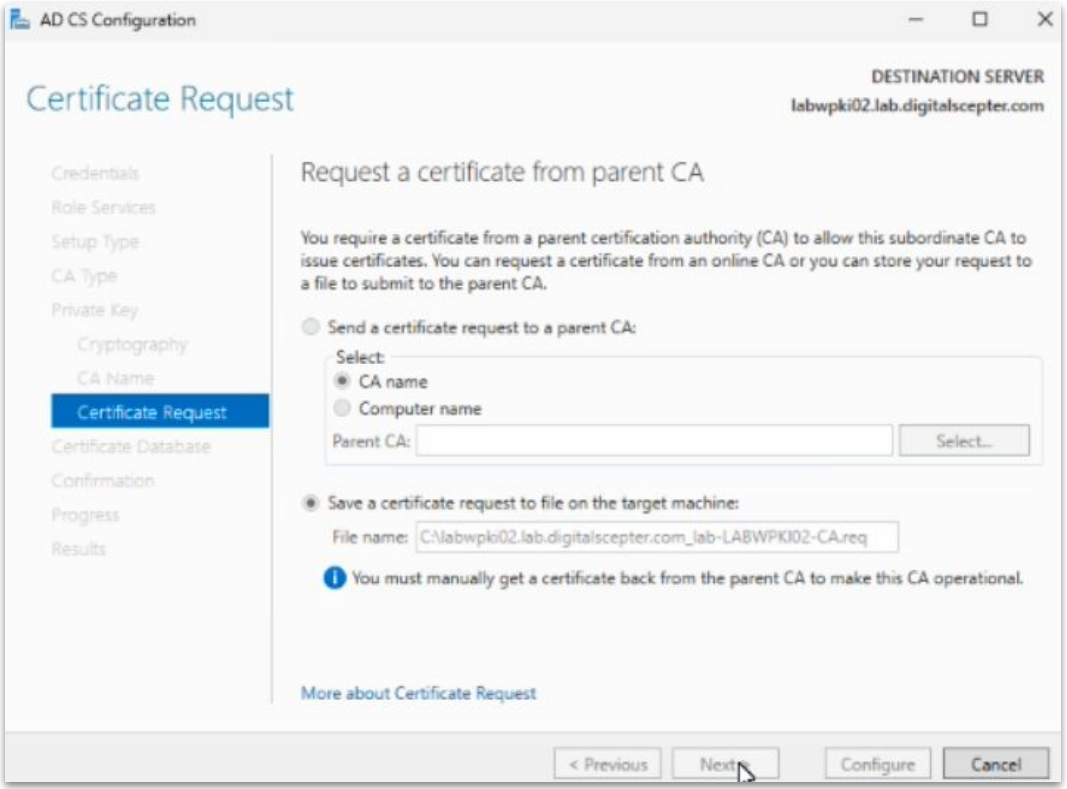
digitalscepter

Build Issuing CA (continued)



digitalscepter

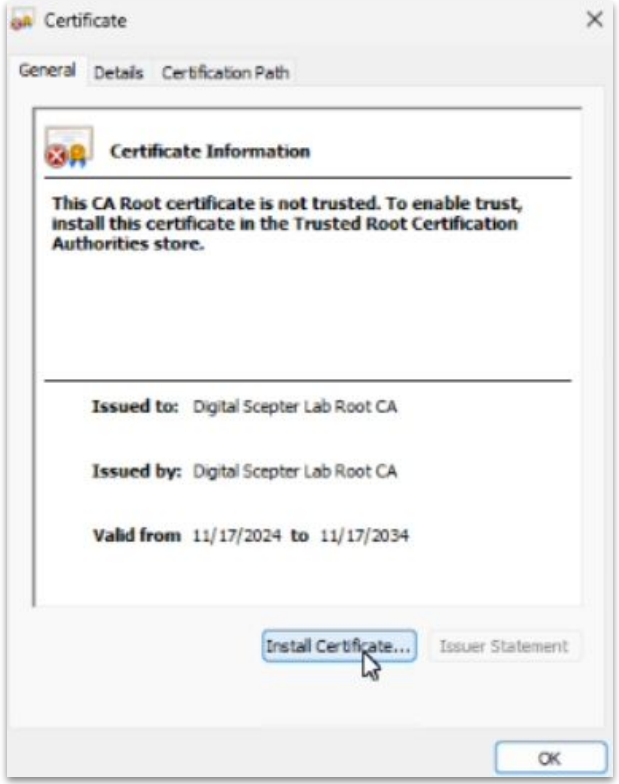
Build Issuing CA (continued)



digitalscepter

Build Issuing CA (continued)

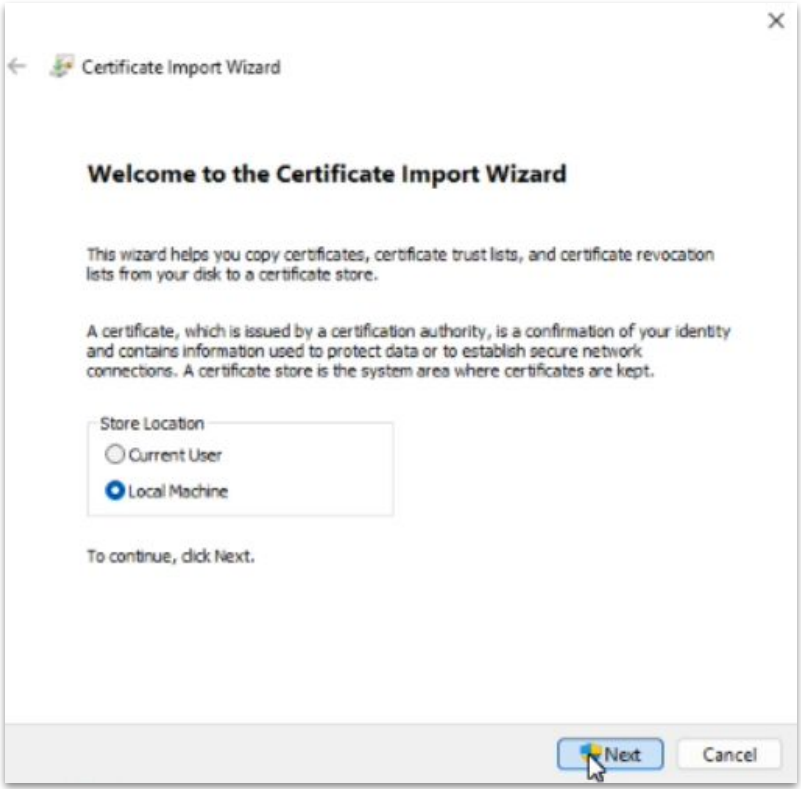
1. Navigate to **C:\CertData** and double-click the CA certificate file that was copied here earlier. Click **Install Certificate**



digitalscepter

Build Issuing CA (continued)

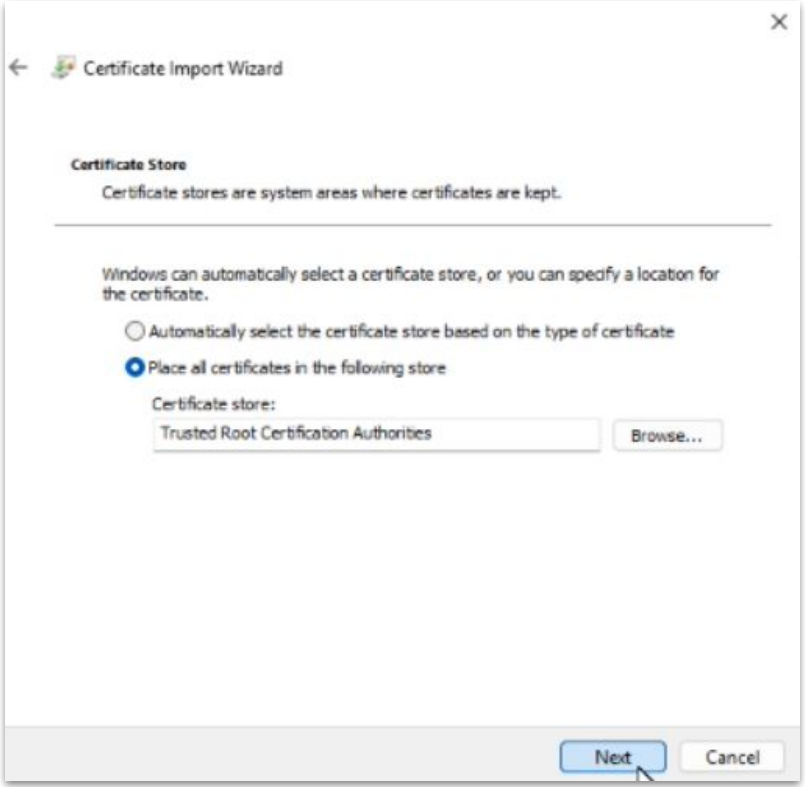
1. Click **Local Machine** and then **Next**



digitalscepter

Build Issuing CA (continued)

1. Click **Place all certificates in the following store** then **Browse** and select **Trusted Root Certification Authorities**



digitalscepter

Build Issuing CA (continued)

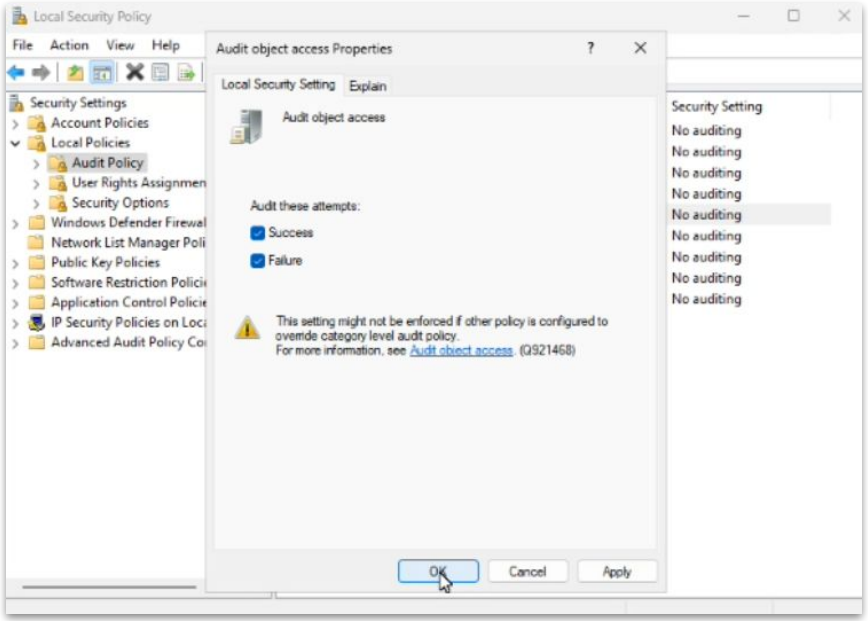
1. Copy the certificate request created earlier to the root CA…
2. I'm sorry, it's this again, get your virtual 5 ¼" floppy ready to move some files back and forth
3. Once you have it on the root, you can open the **Certification Authority** console and right-click your CA name, then click **All Tasks** > **Submit New Request…**
4. Browse to your cert request and click **OK.**
5. Select **Pending Requests** then right-click the single request in the window and click **All Tasks** > **Issue**
6. Select **Issued Certificates** and double-click the only issued certificate. Go to **Details** tab and click **Copy to File…**
7. Select **P7B** format and choose a location to save this. I'd recommend your virtual floppy drive, because guess what. This is going back to your Issuing CA

Build Issuing CA (continued)

1. With your signed certificate back on the issuing CA, we want to open **Certification Authority** and right-click your CA name, then click **All Tasks** > **Install CA Certificate**
2. Select the certificate you copied over from the root CA and click **Open**. The cert will be installed and you should now be able to right-click your CA name, click **All Tasks** > **Start Service**

Build Issuing CA (continued)

1. Open **Local Security Policy** and navigate to **Local Policies** > **Audit Policy**
2. Open **Audit object access** and check **Success** and **Failure**



digitalscepter

Build Issuing CA (continued)

1. Open an **Administrative Command Prompt** and enter the following commands. These will allow your CA to issue certificates with expiration dates up to 3 years out.

```
certutil.exe -setreg CA\ValidityPeriodUnits 3
certutil.exe -setreg CA\ValidityPeriod "Years"
certutil.exe -setreg CA\AuditFilter 127
net stop certsvc
net start certsvc
```

Build Issuing CA (continued)

1. Open **Certification Authority** right click your CA and select **Properties**
2. Click **Extensions**
3. Click **Add** and enter path found in chart below
4. Check box **Include in CRLs…** and **Include in the CDP extension…**
5. Click **Select Extension** dropdown and select **Authority Information Access**
6. Click **Add** and enter path found in chart below
7. Check box **Include in the AIA extension…**
8. Make sure to update italicized values with your own

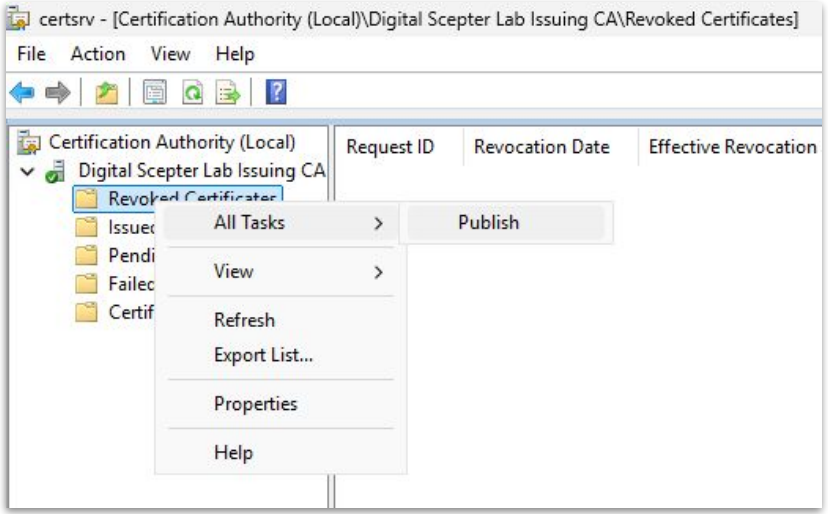
Setting	Value
CDP Extension Location	http://*pki.yourdomain.com*/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
AIA Extension Location	http://*pki.yourdomain.com*/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt

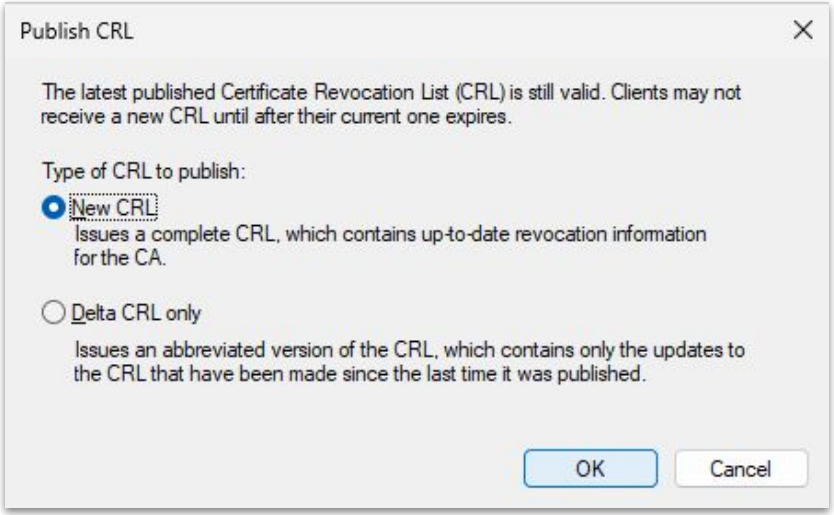
Build Issuing CA (continued)

1. Open **IIS Manager** and expand your server > Sites, Default Web Site and click **CertEnroll**
2. Double-click **Directory Browsing** and click **Enable** in the Actions column
3. We did this earlier with the CertData virtual directory, so this likely feels familiar

Build Issuing CA (continued)

1. Open **Certification Authority** and expand your CA, right-click **Revoked Certificates** and click **All Tasks** > **Publish**. Select **New CRL** and click **OK**





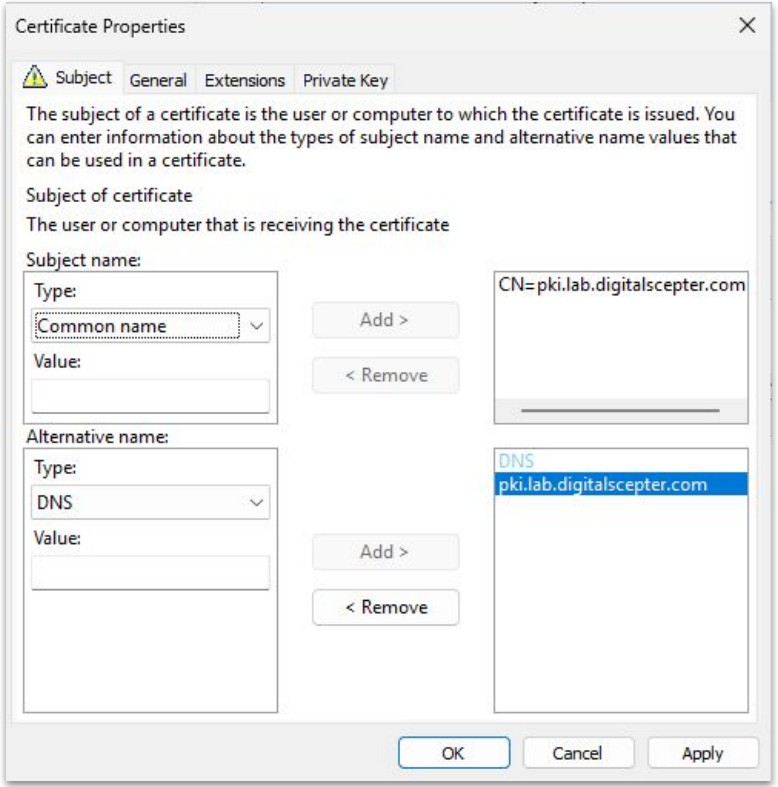
digitalscepter

Build Issuing CA (continued)

1. We need to create a certificate for pki.lab.digitalscepter.com so we can enable https on our Certificate Authority Web Enrollment website
2. Run **certlm.msc** to open your Local Machine certificate store.
3. Right-click **Personal** and click **All Tasks** > **Advanced Operations** > **Create Custom Request**
4. Under Template select **Web Server** then click **Details** and **Properties** when under the Active Directory Enrollment Policy page
5. Populate your **Common Name** and **Alternative Name** and click **OK**

Build Issuing CA (continued)

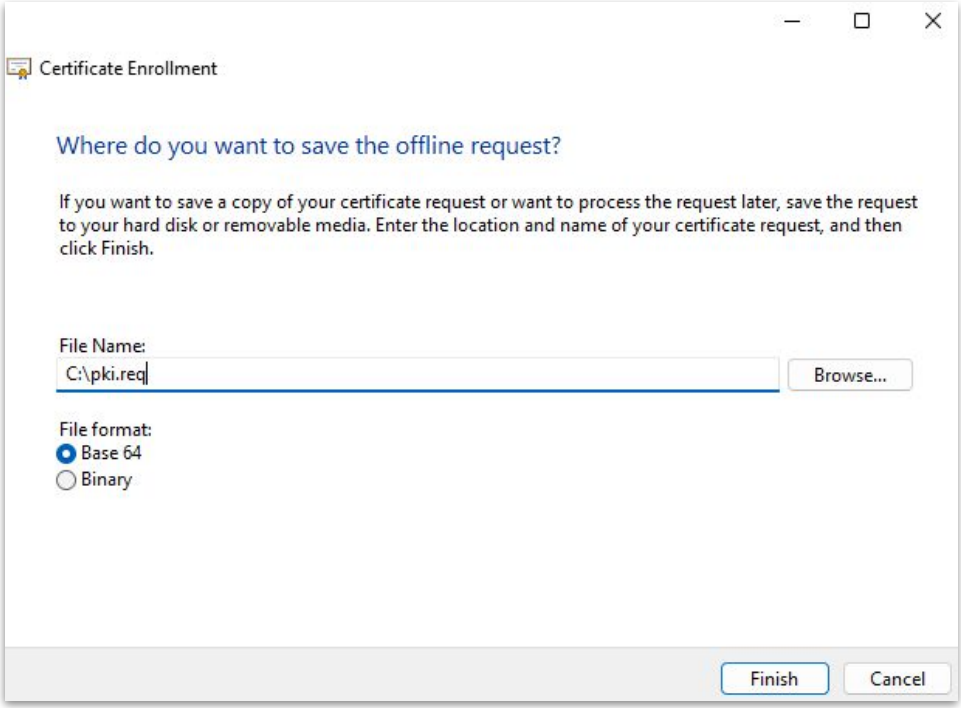
1. Populate your **Common Name** and **Alternative Name** and click **OK**



digitalscepter

Build Issuing CA (continued)

1. Choose a filename and save in Base 64 format



digitalscepter

Build Issuing CA (continued)

1. Open an **Administrative Command Prompt** and enter the following command:

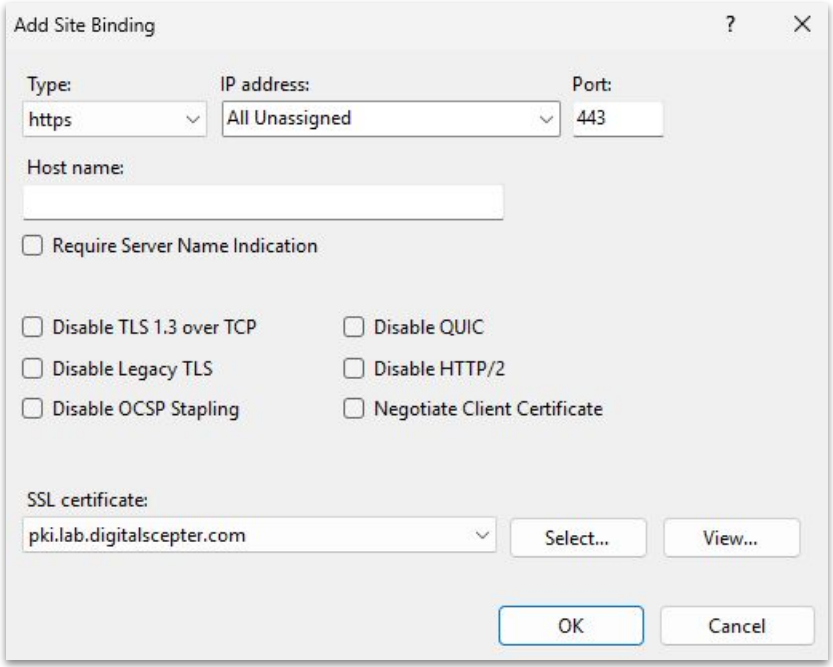
```
certreq -attrib "CertificateTemplate:WebServer" -submit C:\pki.req
```

2. When prompted save the resulting certificate. It can go in the same location as the CSR, but specify the extension of .cer – so in this case, it would be pki.cer
3. Run the below command to import the certificate, automatically pairing it with the private key created with the CSR:

```
certreq -accept pki.cer
```

Build Issuing CA (continued)

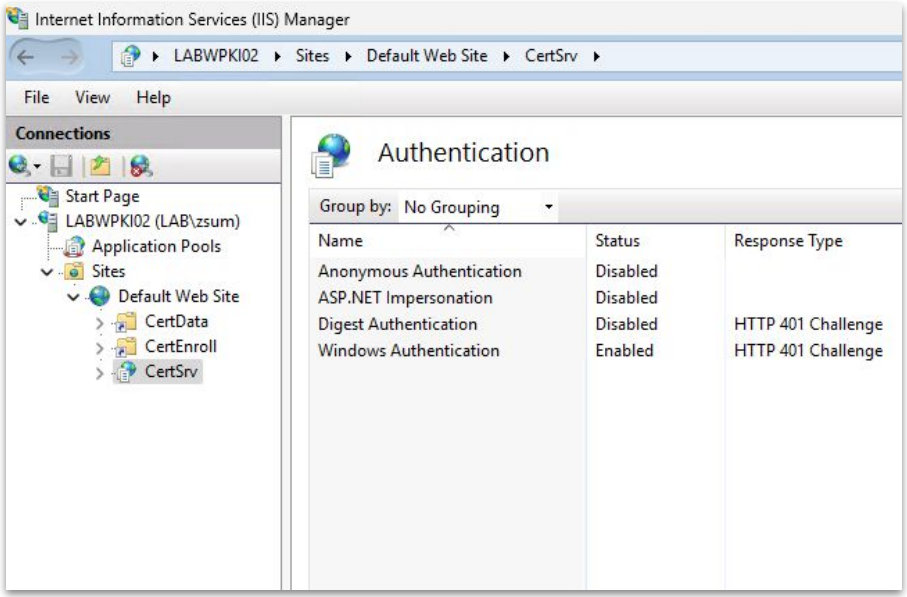
1. Open **IIS Manager** and right-click **Default Web Site** and click **Edit Bindings**
2. Click **Add**
3. Type: https
4. SSL Certificate: *pki.lab.digitalscepter.com*
5. Click **OK**, then **Close**,



digitalscepter

Build Issuing CA (continued)

1. Still within the CertSrv virtual directory, double-click **Authentication** and **Disable** all options except **Windows Authentication** which should be enabled.



digitalscepter

Build Issuing CA (done!)

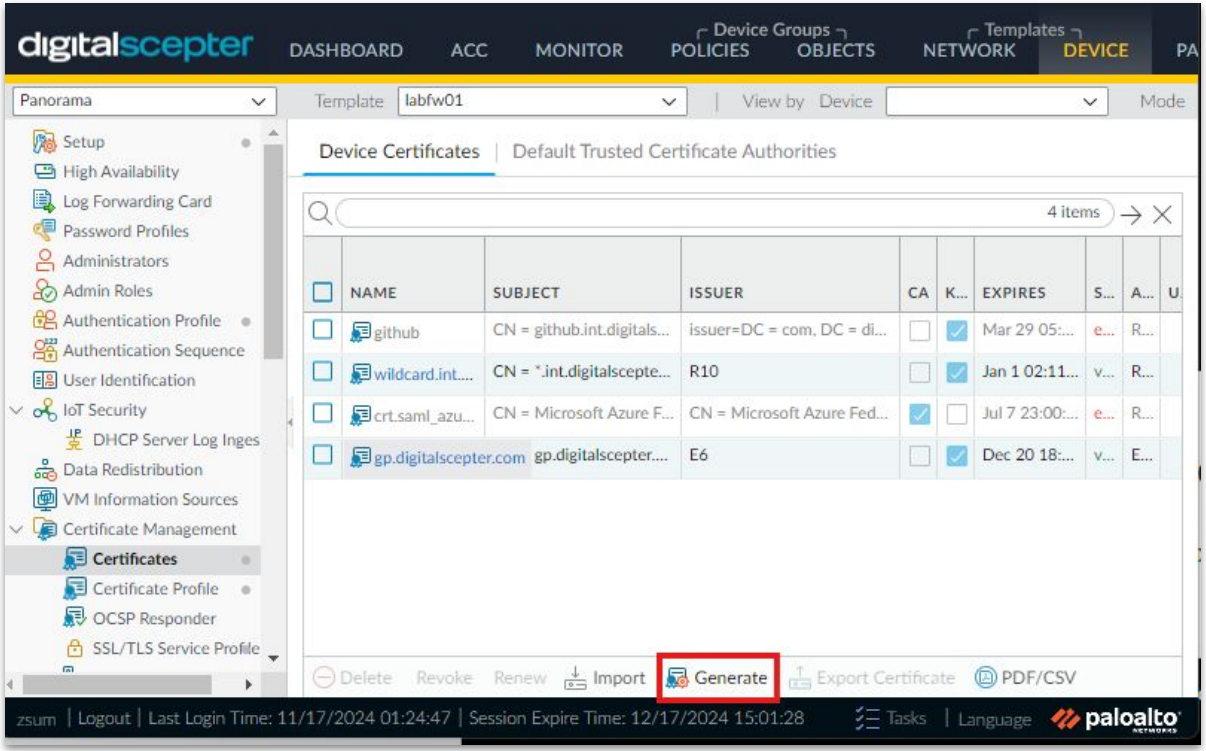
1. It has to be lunch time by now

SSL Inspection With Palo Alto

SSL Decryption Punch List

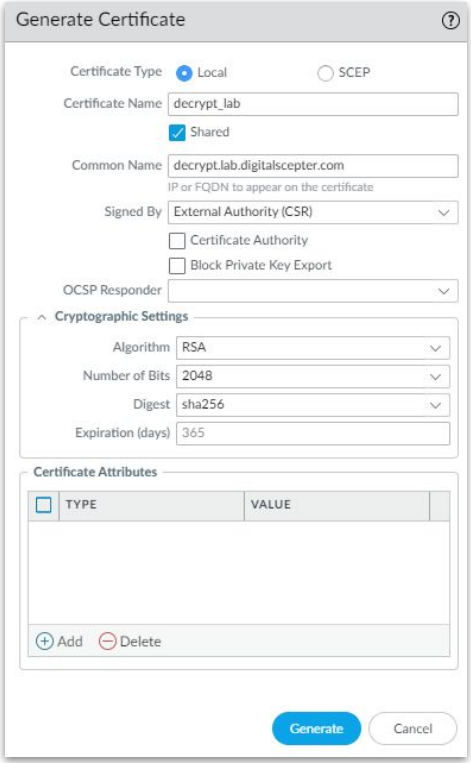
1. The Palo Alto Networks firewalls need to be issued a subordinate CA certificate from your newly created Issuing CA
2. Microsoft has a Subordinate Certification Authority template we can use
    a. Generally, I recommend cloning the default MS templates so you can tweak them as needed for your organization, e.g. changing the validity period.
3. Punch list should look like this:
    a. Generate a CSR on the PAN firewalls
    b. Use the web enrollment site to have cert issued via request file
    c. Import signed certificate to PAN firewalls
    d. Apply **Forward Trust Certificate** role to decrypt certificate
    e. Generate a self-signed CA on the PAN firewalls and assign it the **Forward Untrust Certificate** role
    f. Create **Decryption** policies

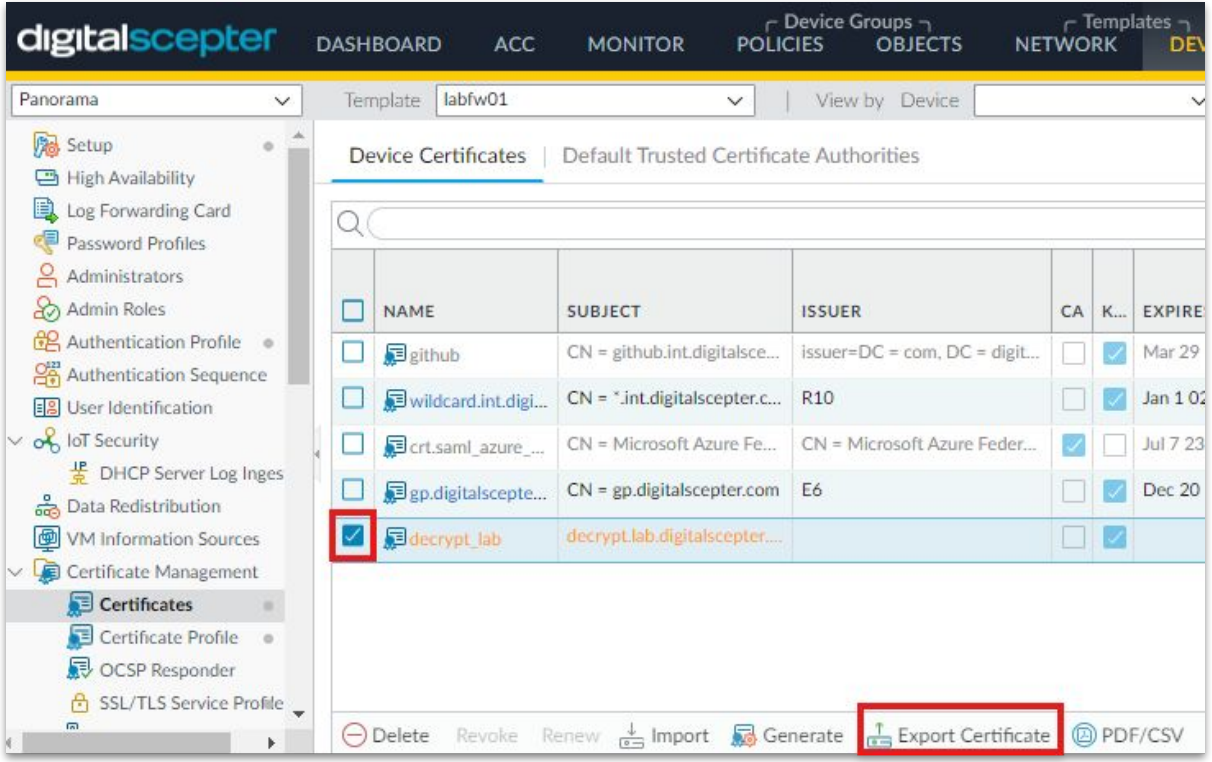
Configure SSL Decryption



digitalscepter

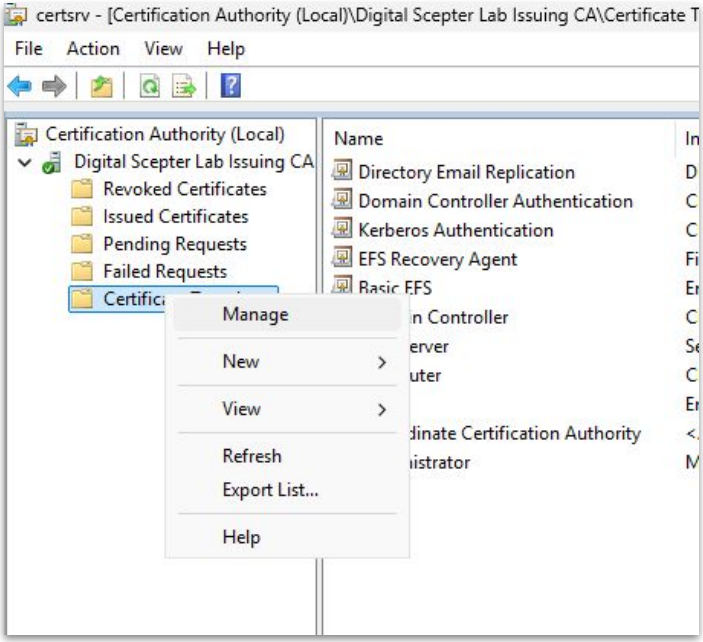
Configure SSL Decryption

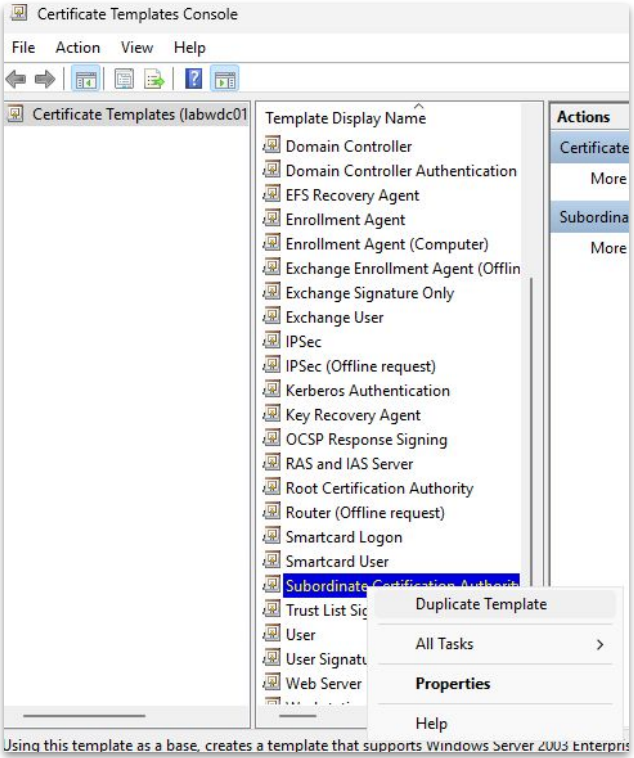




digitalscepter

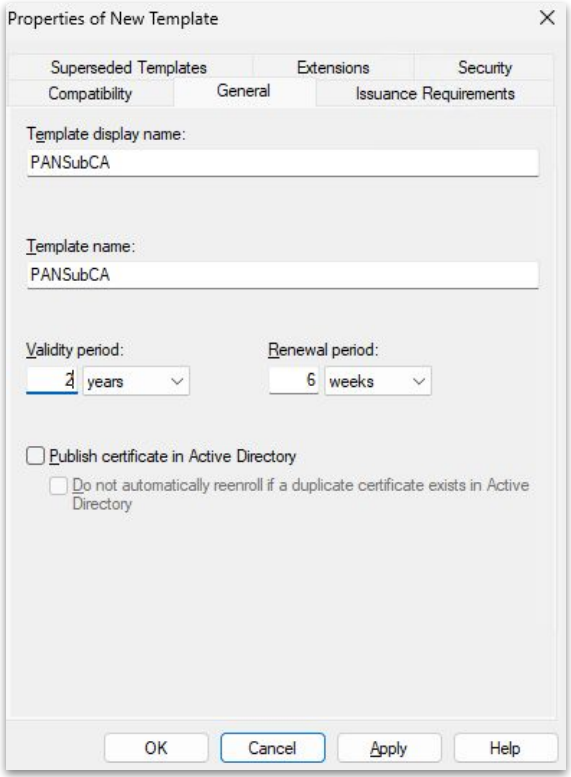
Configure SSL Decryption

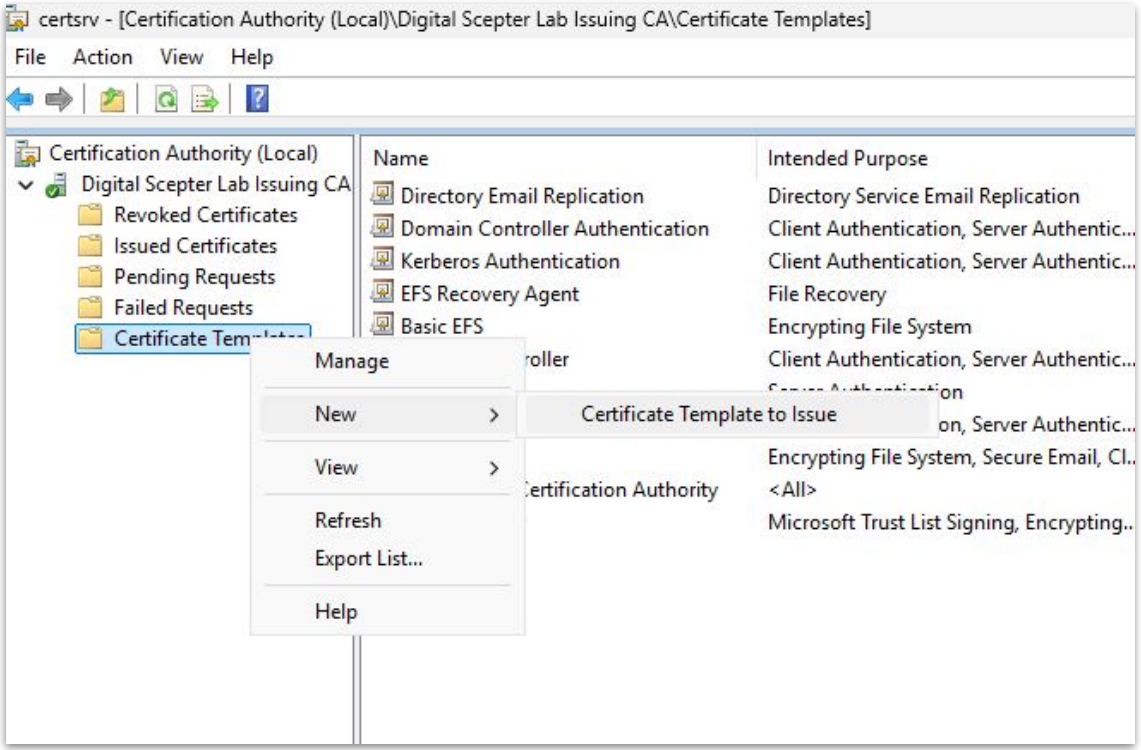




digitalscepter

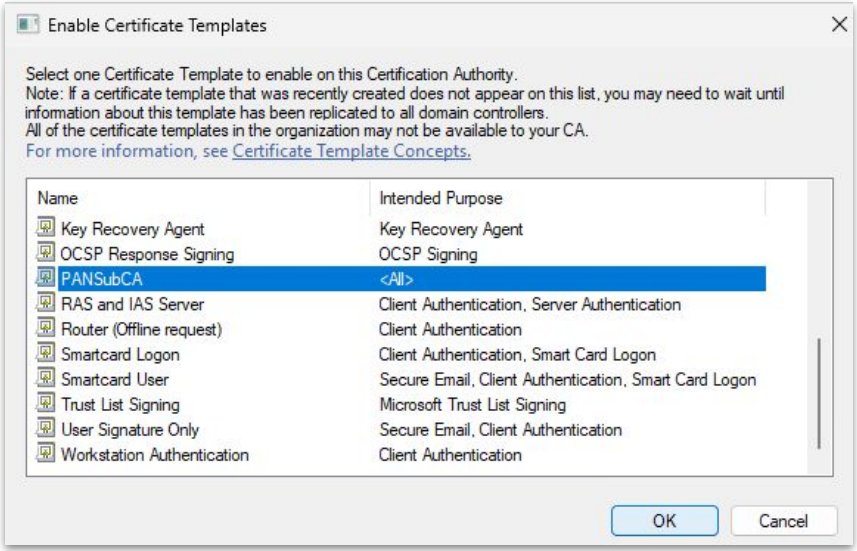
Configure SSL Decryption

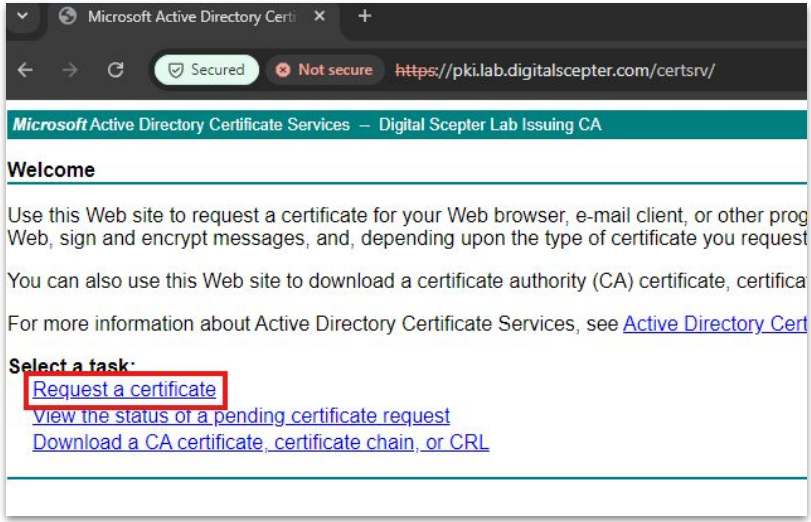




digitalscepter

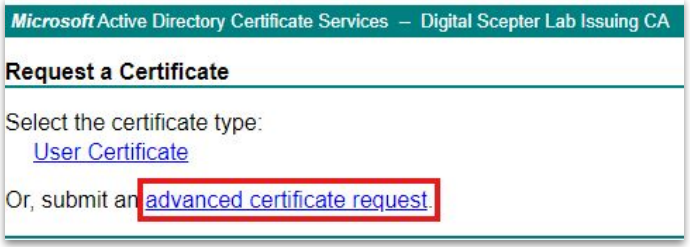
Configure SSL Decryption

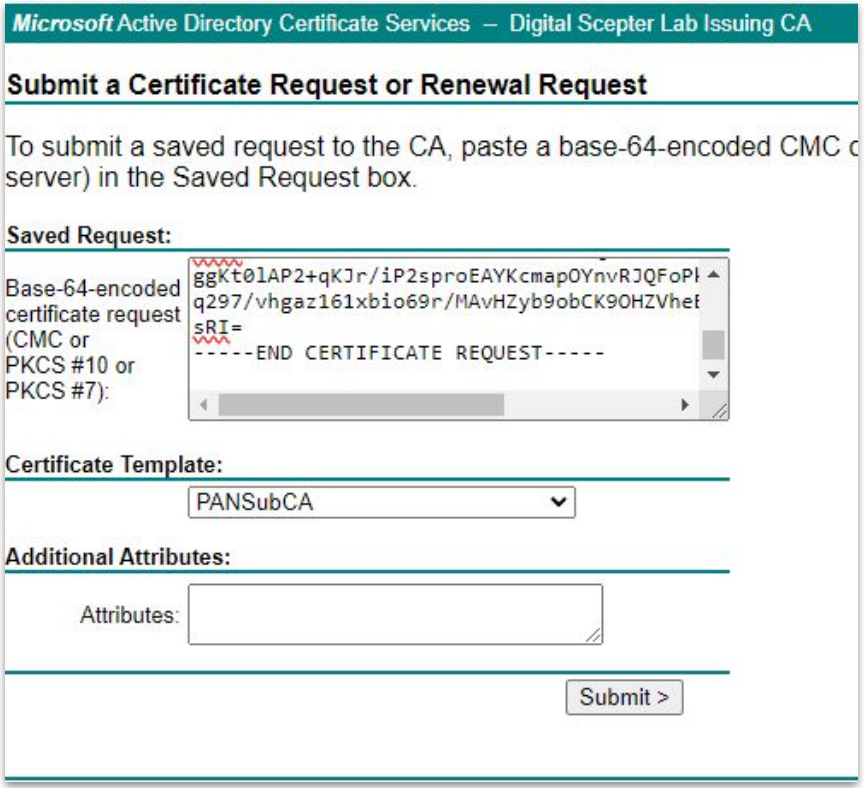




digitalscepter

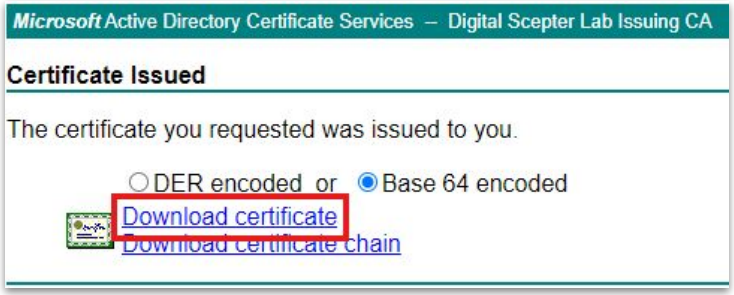
Configure SSL Decryption

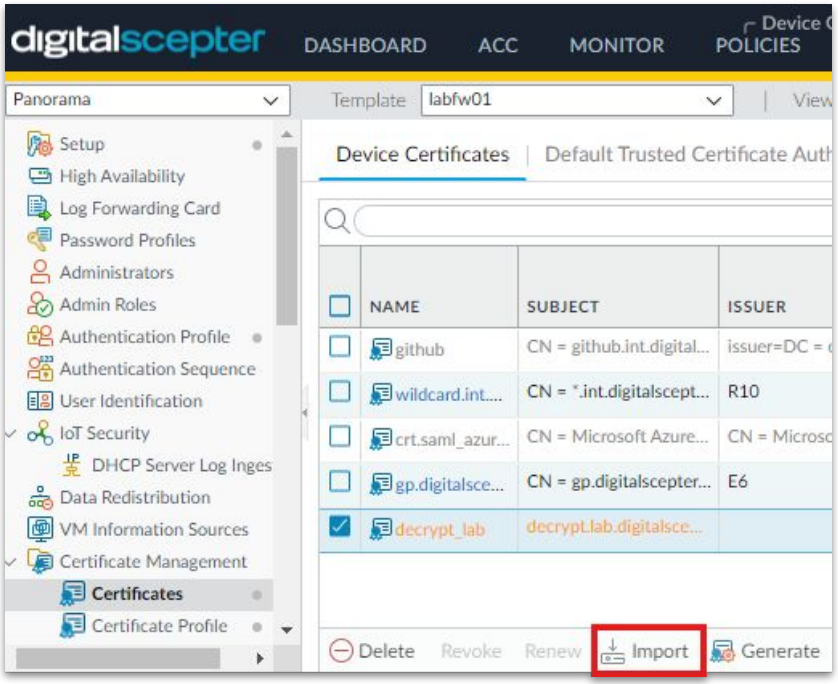




digitalscepter

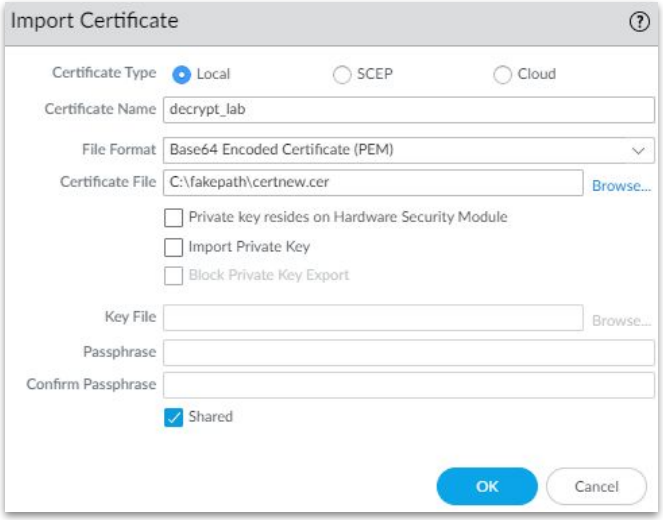
Configure SSL Decryption

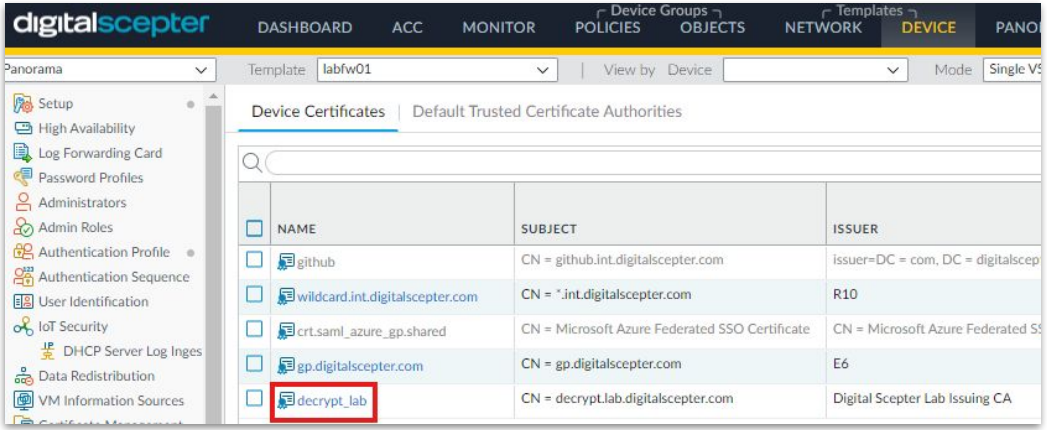




digitalscepter

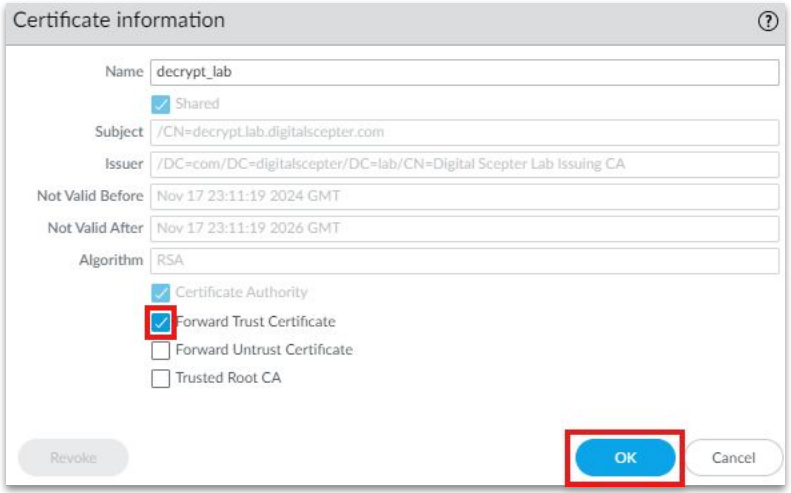
Configure SSL Decryption

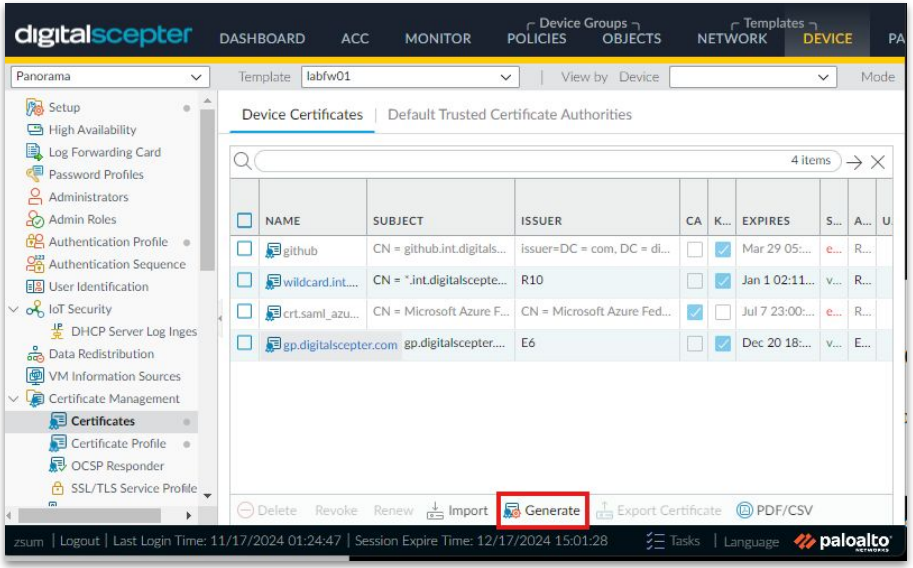




digitalscepter

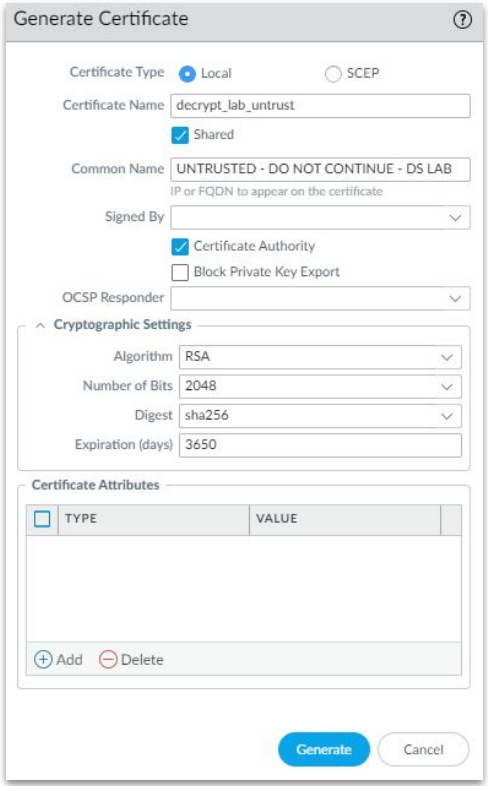
Configure SSL Decryption

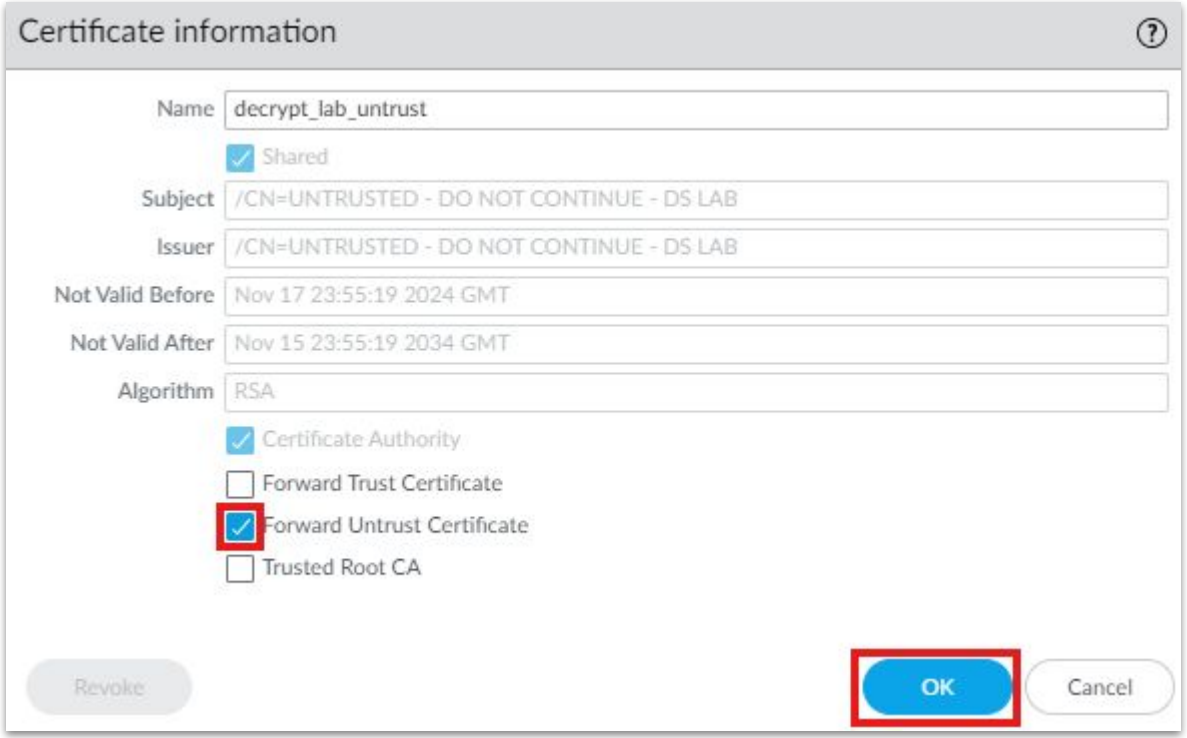




digitalscepter

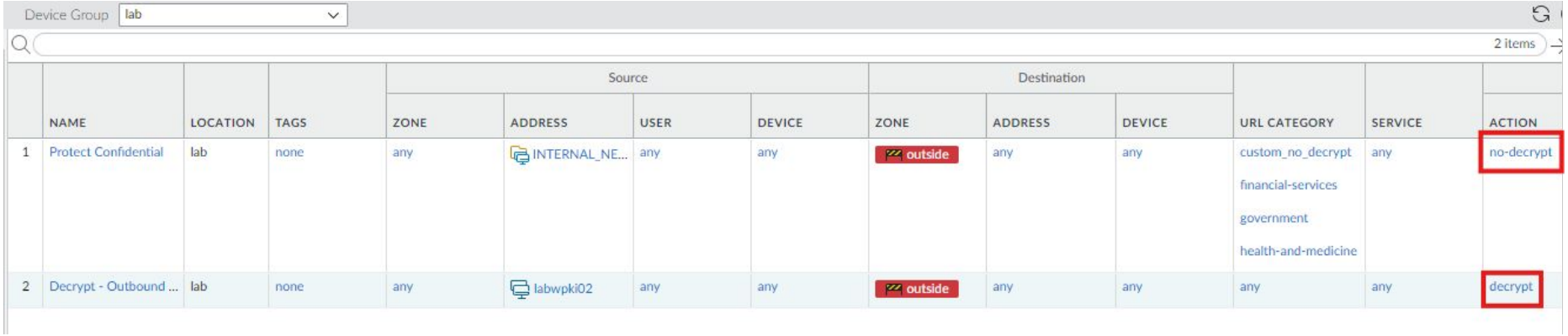
Configure SSL Decryption





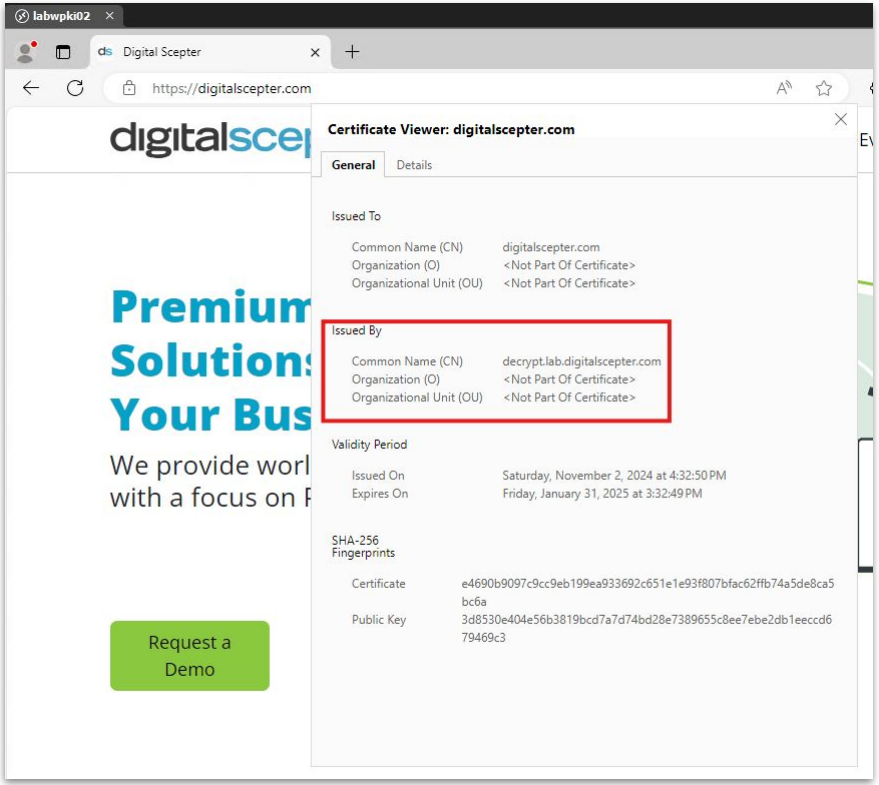
digitalscepter

Configure SSL Decryption



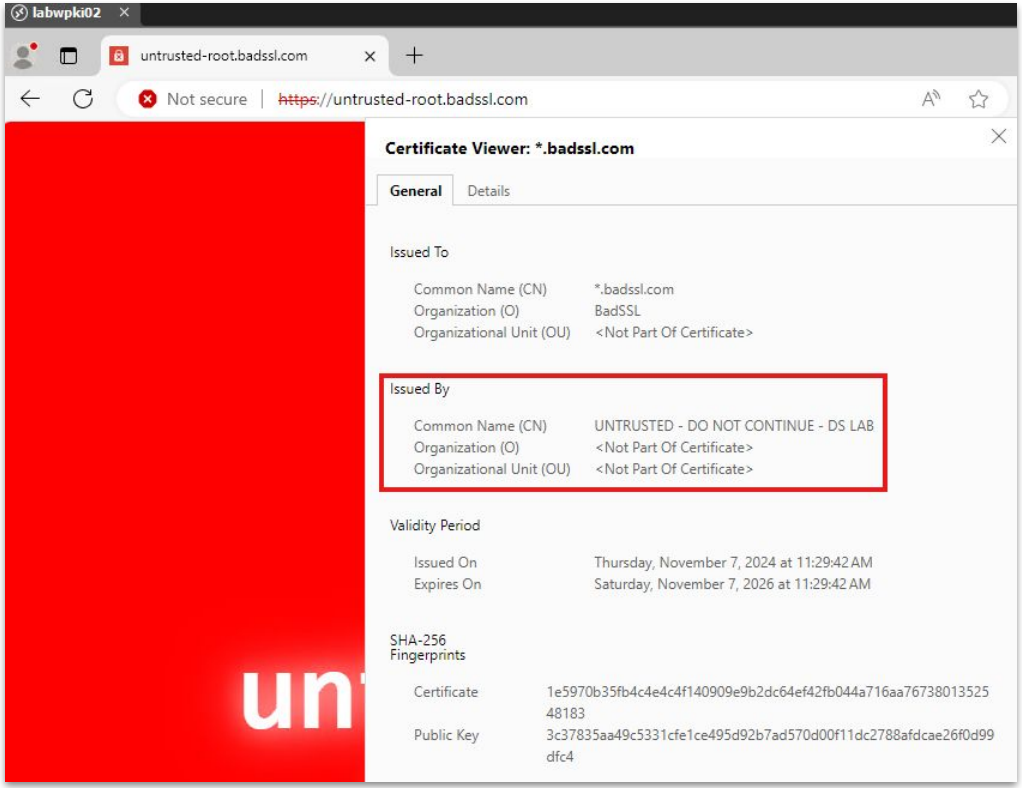
digitalscepter

Configure SSL Decryption



digitalscepter

Configure SSL Decryption



digitalscepter

FALCO

Conclusion

- Thanks for attending!
- Implementing Zero Trust Security Principles
  Today at 4 pm in Harbor G (2nd floor)
- Falco product demonstration Wednesday at 10 am
  Tomorrow at 10 am in Expo Hall Lobby Room B

digitalscepter

What is Falco?

- A tool to detect configuration issues
- A managed service to assist with fixing them
- Product demonstration Wednesday at 11 am

FALCO

FALCO

Sample Falco Report

Falco Plus

Summary | Policies | Objects | Network | Device

Device: PA5250-1

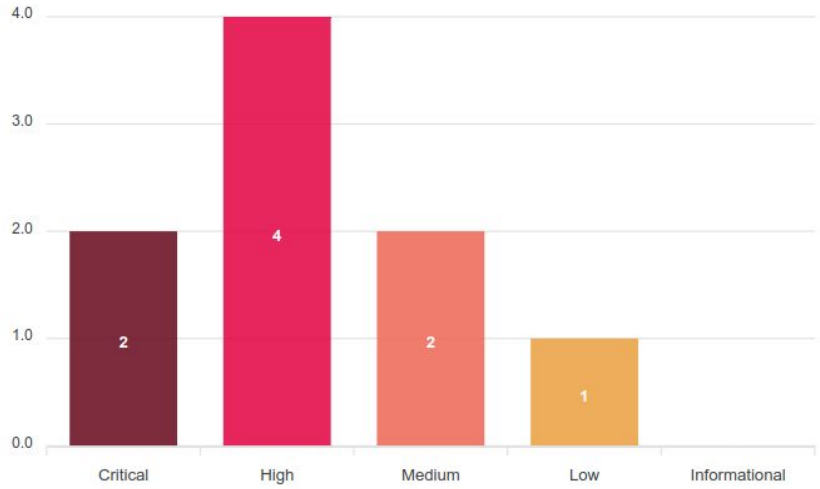
80% passed
1 Devices Audited

1/1 devices
Recommended Releases

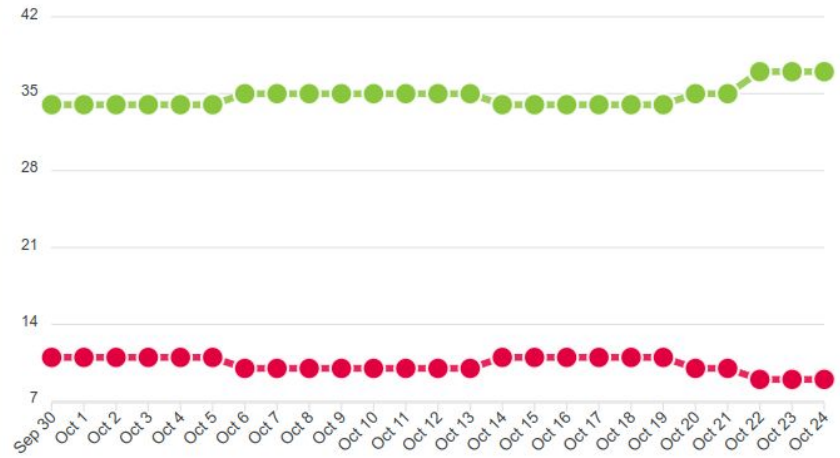
No Vulnerabilities
No Known Vulnerabilties Found

Support Licenses
All Devices Have Valid Support Licenses

Failed Check Severity



Report History



sales@digitalscepter.com
(888) 299-3718

digitalscepter.com