PRINT SIMPLY ANYWHERE

HP PrinterOn Development

Setting up a Local Certificate Authority

mobile printing solutions | enterprise | education | public printing locations

Contents

1

Introduction

This guide is intended to guide you through the process of setting up a local Certificate Authority (CA) which you can use to issue and sign certificates.

By default, when you install PrinterOn, all components are configured to communicate over TLS-enabled ports. In a production environment, it is recommended that you always use trusted certificates issued by one of several available Certificate Authorities, such as Verisign, Thawte, or RSA Security, among others.

These CAs typically charge a fee to sign certificates, which can vary in cost depending on the nature of the certificate being signed, the validity period, and other factors.

However, in non-production scenarios—for example, in testing environments, or when performing proof-of-concept analysis—the certified protection you are paying third-party authorities to provide is unnecessary. Because both Windows and macOS provide tools that allow you to create and configure a local CA, you can avoid the costs associate with public CAs.

Creating your own local CA allows you to issue certificates and validate users so that you can have a secure, protected testing environment for non-production development or proof of concept analysis. This is a one-time task that, once completed, can be used to provide certificates for your PrinterOn server and client devices to support secure communication across the PrinterOn service.

> **Note:** A local CA is not a substitute for third-party CA. In production environments, it is always recommended that you use valid trusted certificates signed by a reputable Certificate Authority.

1.1 Overview: Setting up a local Certificate Authority

To set up your environment to use a local Certificate Authority that you can use with a non-production PrinterOn service, you'll need to complete the following tasks:

1. Create and configure your local Certificate Authority. This process creates the root certificate and a set of public and private keys.

   This process differs depending on whether you are installing it on Windows or macOS:

   - Creating a local Certificate Authority on Windows Server.
   - Creating a local Certificate Authority on macOS

2. Install the server certificate on the PrinterOn Server.
3. Install the root certificate on each client device that needs to communicate with the PrinterOn server:

   - Installing the root certificate on iOS devices.
   - Installing the root certificate on Android devices.
   - Installing the CA root certificate on Windows devices.

2

Creating a local Certificate Authority on Windows Server

To create a local Certificate Authority and set up and deploy your certificates from a Windows Server, you must complete the following tasks:

1. Create the local Certificate Authority.
2. Create and export the server certificate.
3. Export the CA root certificate.

Although there are different ways of accomplishing these tasks, this tutorial will use a variety of tools on one Windows server to complete them, including:

- The Windows Server Manager
- Internet Explorer (or some other browser)
- The Certificates Snap-In in the Microsoft Management Console

Important! The Certificates Snap-in is not added to the MMC by default; you must add it yourself. If it has not already been added, add the Certificates Snap-in to the server's Microsoft Management Console before continuing.

2.1 Creating the local Certificate Authority

In Windows, the Certificate Authority installed as a feature of Active Directory. You can install this feature through Server Manager.

Creating a local Certificate Authority and setting up your certificates on Windows requires you to complete the following tasks:

1. First, make sure that you have met the system prerequisites.
2. Then you install the Active Directory Certificate Authority on the server.
3. Finally, you configure the service to create the root certificate.

2.1.1 System prerequisites

Before you create your CA on a Windows Server, you must make sure that:

- The server is a member of the domain. You cannot create a CA on an independent server that is not within your domain.
- You have domain administrator privileges, and be logged in as the domain administrator.

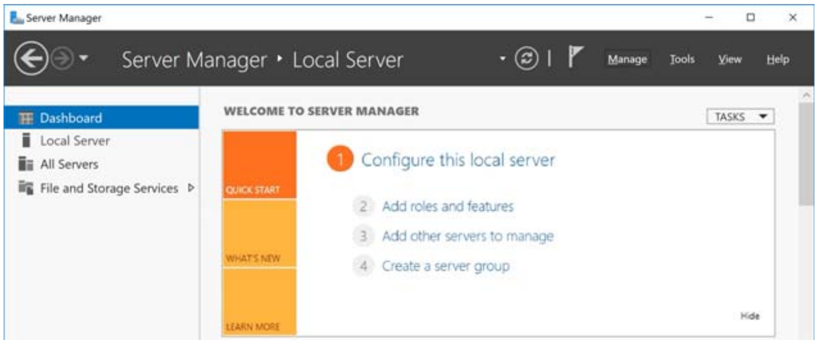
Important! DO NOT install your local CA on the same Windows Server that is hosting your PrinterOn server. The local CA can cause conflicts with PrinterOn’s installation of Apache Tomcat.

2.1.2 Installing the Active Directory Certificate Authority

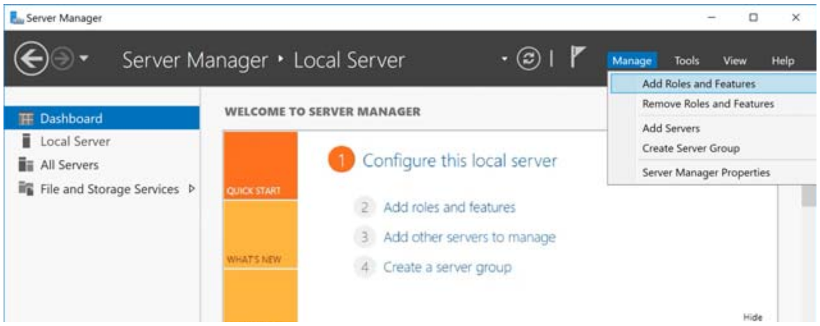
Windows Active Directory lets you set up a Certificate Authority as part of its Certificate Services.

To set up an Active Directory Certificate Services on Windows Server:

1. In Windows server, click **Start** > **Server Manager**. The Server Manager window opens.



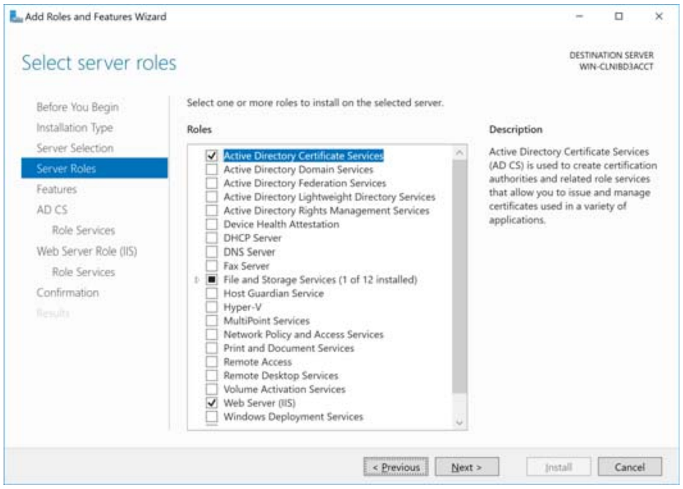
2. From the top menu, click **Manage** > **Add Roles and Features**.



The Add Roles and Features wizard opens.

3. In the Add Roles and Features wizard, click **Next** for the next several screens to accept the default values and proceed through the wizard until you reach the **Server Roles** screen.

4. In the **Roles** list of the Server Roles screen, select **Active Directory Certificate Services**, then click **Next**.



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-CLNIBD3ACCT

Select one or more roles to install on the selected server.

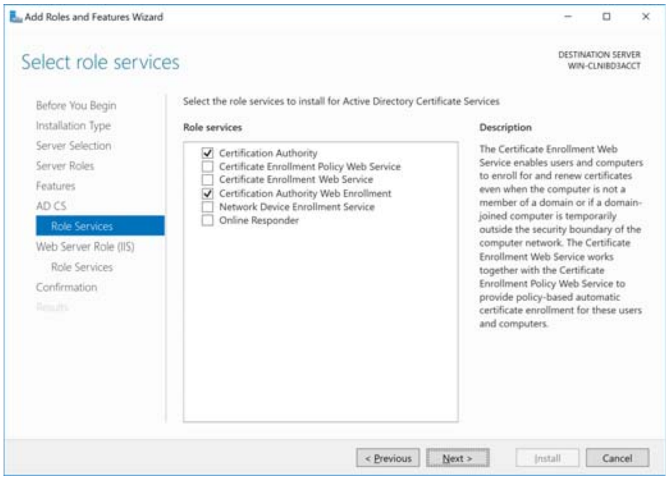
Roles

- ☑ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

5. If necessary, click **Add Features** to confirm the additions, then click **Next** for the next several screens to accept the default values and proceed through the wizard until you reach the **AD CA Role Services** screen.
6. In the Role Services screen, select the following options:
    - **Certification Authority**
    - **Certification Authority Web Enrollment**



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
WIN-CLNIBD3ACCT

Select the role services to install for Active Directory Certificate Services

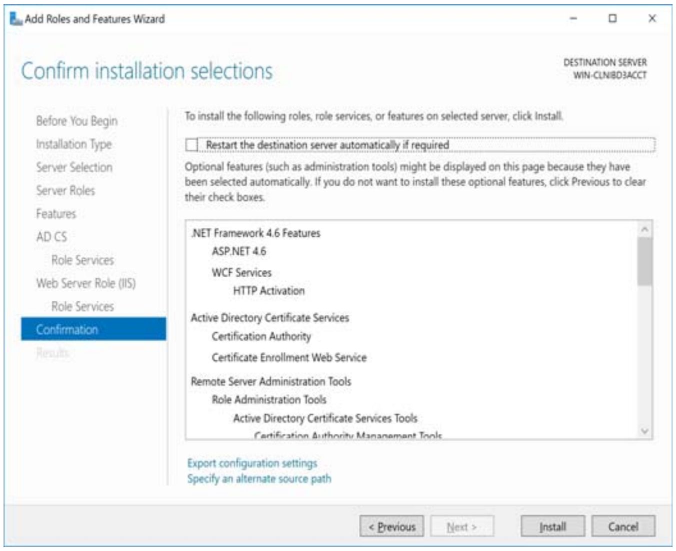
Role services

- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

Description

The Certificate Enrollment Web Service enables users and computers to enroll for and renew certificates even when the computer is not a member of a domain or if a domain-joined computer is temporarily outside the security boundary of the computer network. The Certificate Enrollment Web Service works together with the Certificate Enrollment Policy Web Service to provide policy-based automatic certificate enrollment for these users and computers.

7. If necessary, click **Add Features** to confirm the additions, then click **Next** for the next several screens to accept the default values and proceed through the wizard until you reach the **Confirm Installation selections** screen.



Confirm installation selections

DESTINATION SERVER
WIN-CLNIBD3ACCT

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 4.6 Features
    ASP.NET 4.6
    WCF Services
        HTTP Activation
Active Directory Certificate Services
    Certification Authority
    Certificate Enrollment Web Service
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools

8. Click **Install**. The Server Manager installs the Certificate Authority. Once the installation process is finished, the Server Manager displays a notification requesting you to configure the Certificate Service to create the root certificate.

You can now configure the service to create the root certificate.

2.1.3 Configuring the AD Certificate Service

After successfully installing the Certificate Authority, you'll need to configure the service to set up the root certificate and public/private keys.

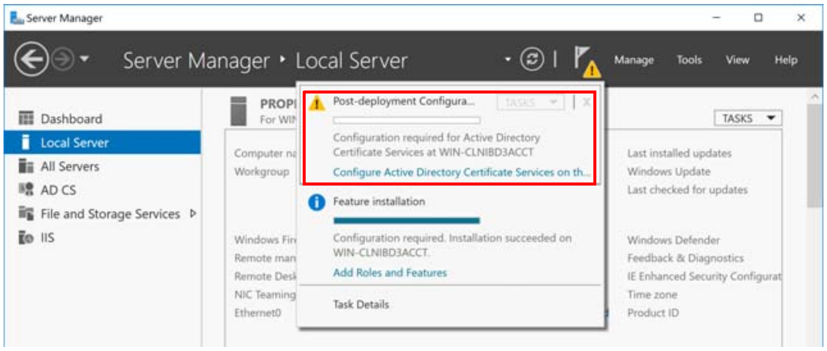
To configure the Active Directory Certificate Services:

1. After the Certificate Authority installation, the Server Manager displays a notification alert on the top menu. Click the notification flag to view the notifications.

   Two notifications should be present:

   - **Post-deployment configuration**: Indicates that some configuration is required for the deployment.
   - **Feature installation**: Indicates that a new feature was installed.

2. In the Post-deployment Configuration notification, click **Configure Active Directory Certificate Services on the Destination Server**.



Post-deployment Configura...

Configuration required for Active Directory Certificate Services at WIN-CLNIBD3ACCT

Configure Active Directory Certificate Services on th...

Feature installation

Configuration required. Installation succeeded on WIN-CLNIBD3ACCT.

Add Roles and Features

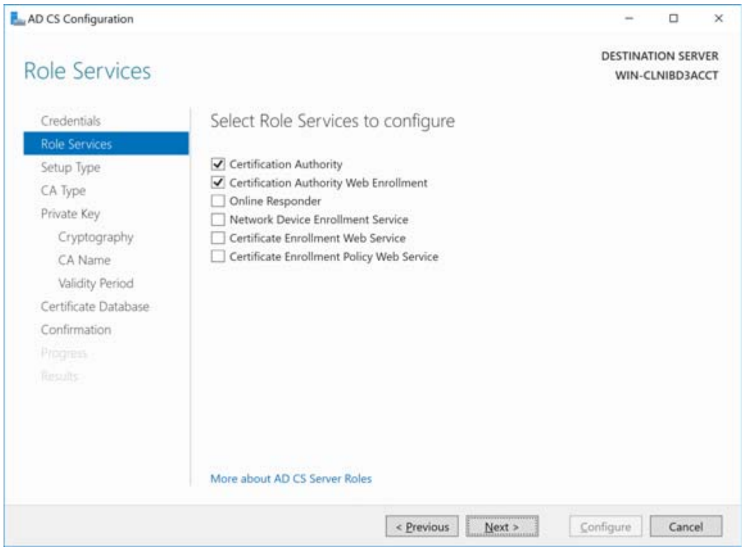
The AD CS Configuration wizard opens.

3. In the Credentials screen, locate the **Credentials** field and confirm that it displays the Domain Administrator account.

> **Important:** The **Credentials** field shows which administrator account is being used to configure the CA service. To ensure that you can correctly configure the Certificate Authority, this field *must* display the Domain Administrator account.
>
> If the **Credentials** field does not display the Domain Administrator account:
>
> 1. Click **Change**.
> 2. In the dialog that appears, enter the **Username** and **Password** for the Domain Administrator.

4. Click **Next** to proceed to the **Role Services** screen.

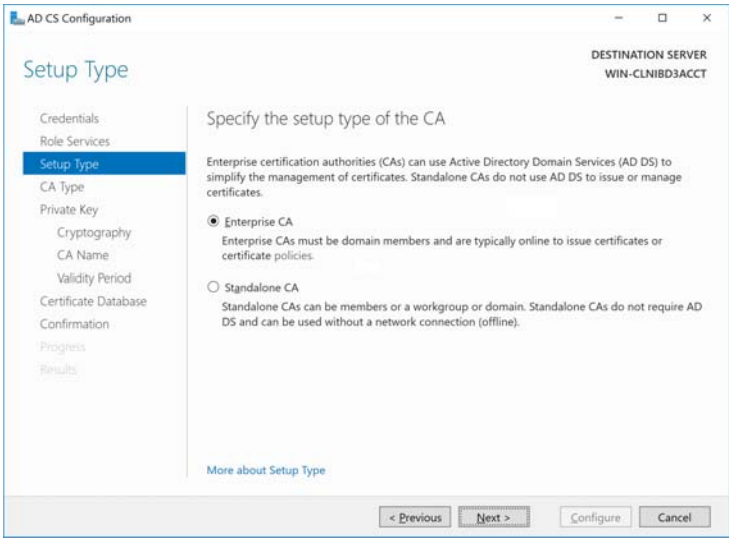
5. In the Role Services screen, select the following services, then click **Next**:
   - **Certification Authority**
   - **Certification Authority Web Enrollment**



Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

6. In the Setup Type screen, choose **Enterprise CA**, then click **Next**.



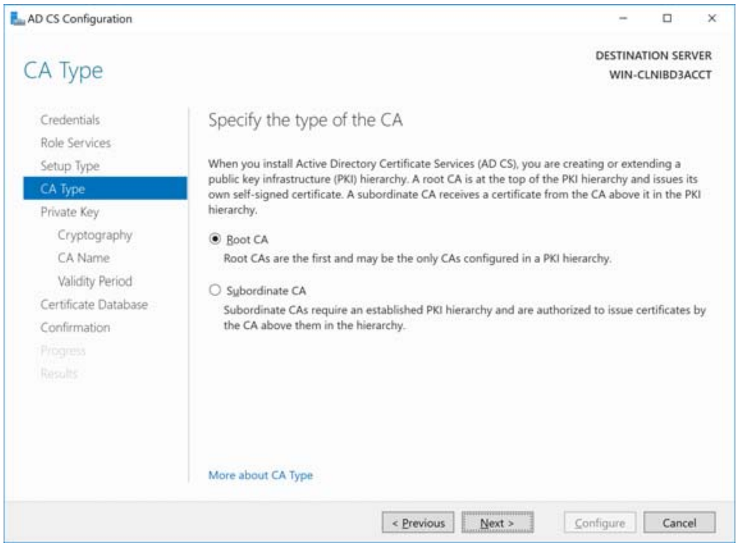
Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

7. In the CA Type screen, choose **Root CA**, then click **Next**.



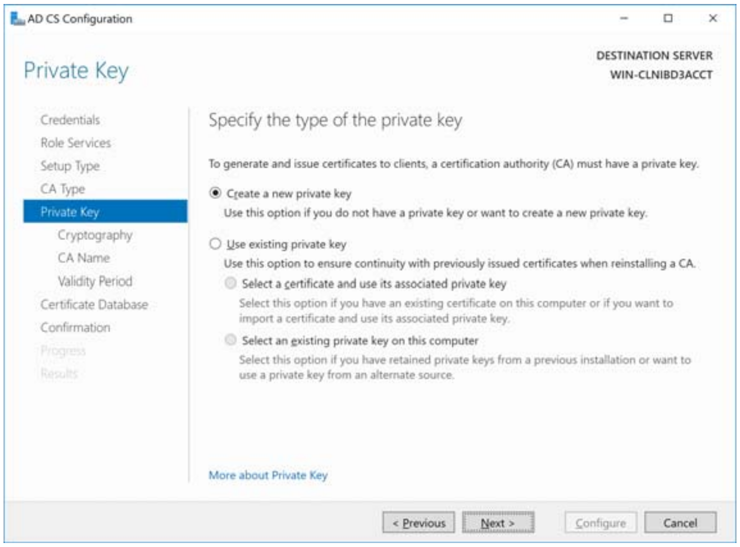
Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

8. In the Private Key screen, choose **Create a new private key**, then click **Next**.



Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

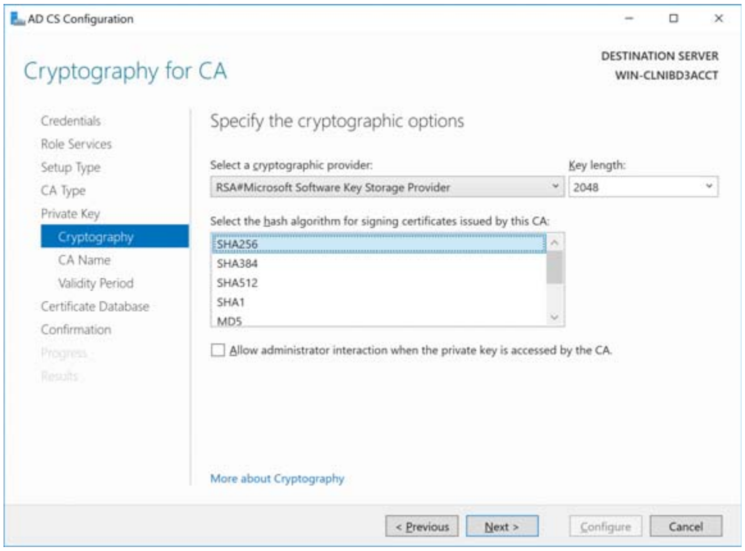
● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

9. In the Cryptography screen, select the cryptography settings you want to use, then click **Next**.



Cryptography for CA

DESTINATION SERVER
WIN-CLNIBD3ACCT

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

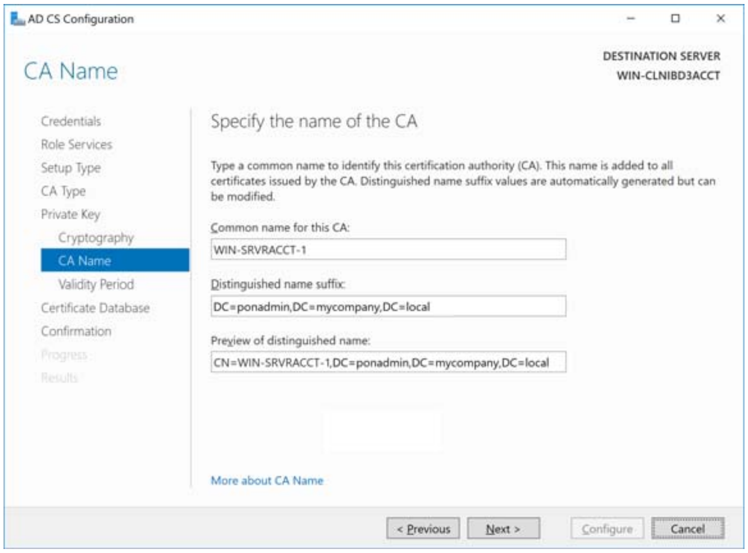
Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:
SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

10. In the CA Name screen, define the CA name, then click **Next**.



CA Name

DESTINATION SERVER
WIN-CLNIBD3ACCT

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

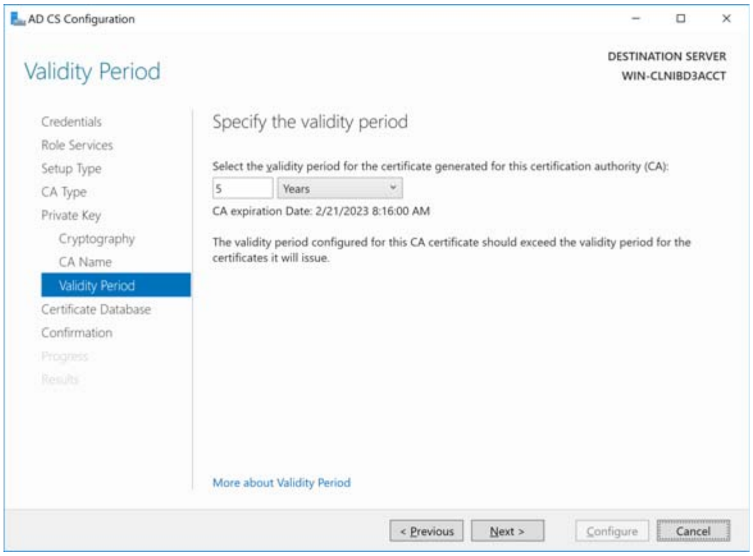
Common name for this CA: WIN-SRVRACCT-1

Distinguished name suffix: DC=ponadmin,DC=mycompany,DC=local

Preview of distinguished name: CN=WIN-SRVRACCT-1,DC=ponadmin,DC=mycompany,DC=local

More about CA Name

11. In the Validity Period screen, the length of time the root certificate of the CA is valid for, then click **Next**.



AD CS Configuration

Validity Period

DESTINATION SERVER
WIN-CLNIBD3ACCT

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

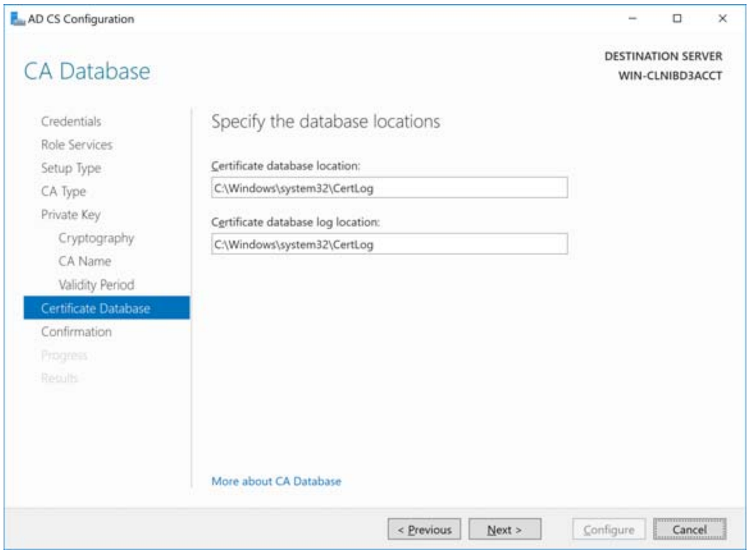
5 Years

CA expiration Date: 2/21/2023 8:16:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

More about Validity Period

12. In the Certificate Database screen, specify the location of the logs, then click **Next**. Typically the default values are sufficient.



AD CS Configuration

CA Database

DESTINATION SERVER
WIN-CLNIBD3ACCT

Specify the database locations

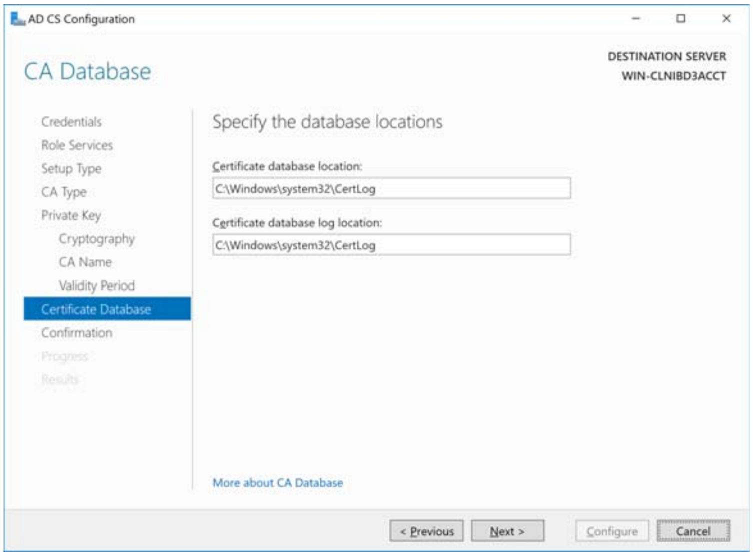
Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

More about CA Database

13. In the Confirmation screen, confirm your settings, and if correct, click **Configure**.

    Once the configuration is applied, the Results screen appears, indicating that the CA was successfully configured.



DESTINATION SERVER
WIN-CLNIBD3ACCT

CA Database

Specify the database locations

Certificate database location: C:\Windows\system32\CertLog

Certificate database log location: C:\Windows\system32\CertLog

With the CA created, you can now:

- Create a server certificate for the PrinterOn Server.
- Export the root certificate to distribute it to client devices.

2.2 Creating and exporting a signed server certificate

There are several ways to request a server certificate for use on the PrinterOn Server. To simplify the process and minimize the need to switch between computers for each step, in this tutorial, we'll simply submit the request from the CA computer itself, then export it with the private key and install it on the PrinterOn Server.

To issue a server certificate to your PrinterOn server(s), you'll need to complete the following tasks:

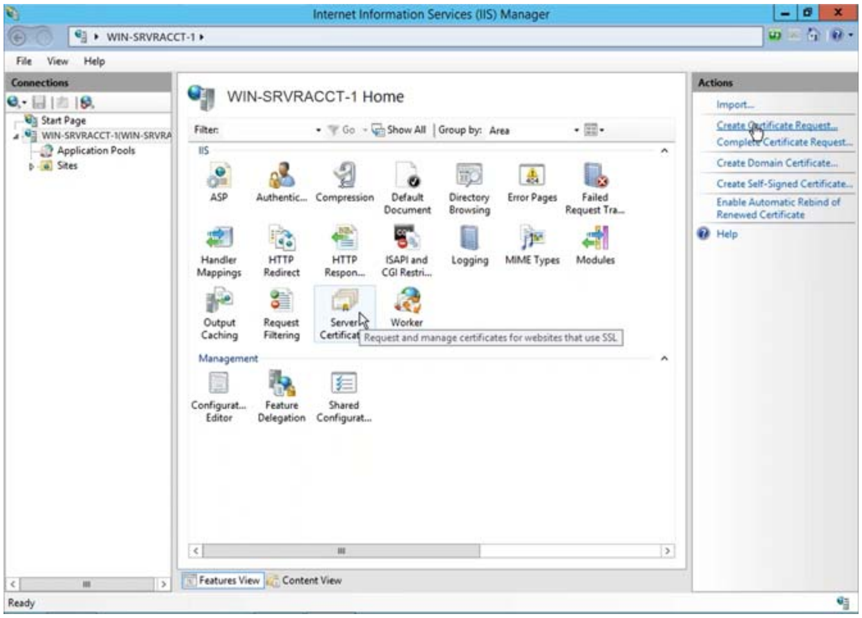
1. Create a certificate signing request.
2. Request the server certificate from your Certificate Authority.
3. Export the server certificate with the private key.

2.2.1 Creating a certificate signing request

To request a server certificate for use by the PrinterOn server, you first need to create a Certificate Signing Request (CSR). The CSR is an encrypted text file containing some indentifying information, including the private key and a digital signature. Once you have created a CSR, you can use it to request the server certificate.

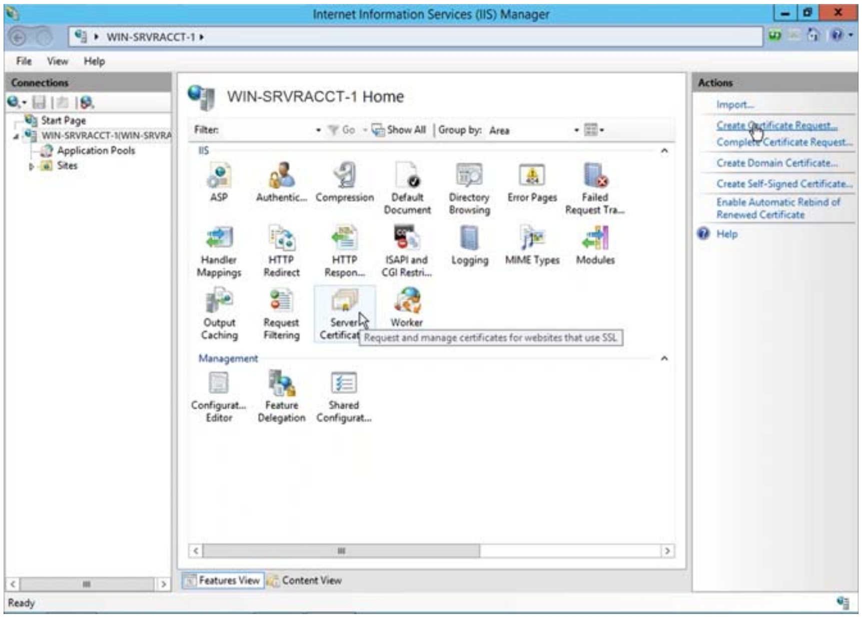
To create a Certificate Signing Request:

1. On the CA computer, open the IIS Manager.
2. In the **Connections** list on the left, you should see the Certificate Authority you just created. Select your Certificate Authority.



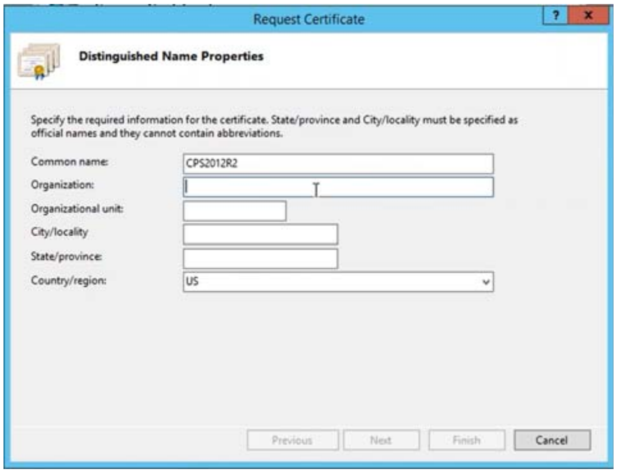
Request and manage certificates for websites that use SSL

3. In the central pane, select **Server Certificates**.



4. In the **Actions** pane, select **Create Certificate Request**. The Request Certificate wizard opens.

5. In the Distinguished Name Properties screen, complete the required information in the form, the click **Next**.


Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: CPS2012R2

Organization:

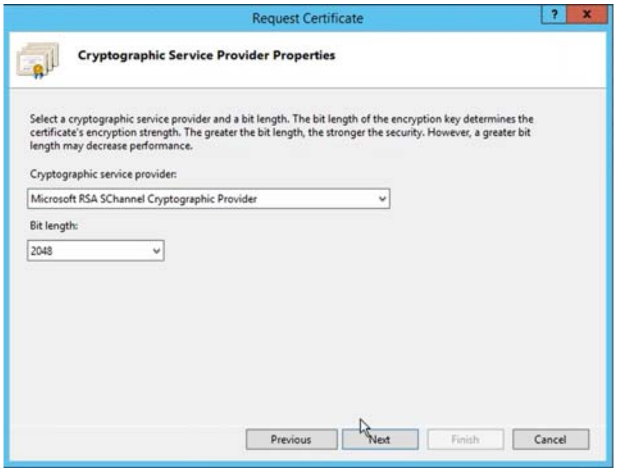
Organizational unit:

City/locality

State/province:

Country/region: US

6. In the Cryptographic Service Provider Properties screen, specify the service provider and bit length that should be used to encrypt the certificate, then click **Next**.



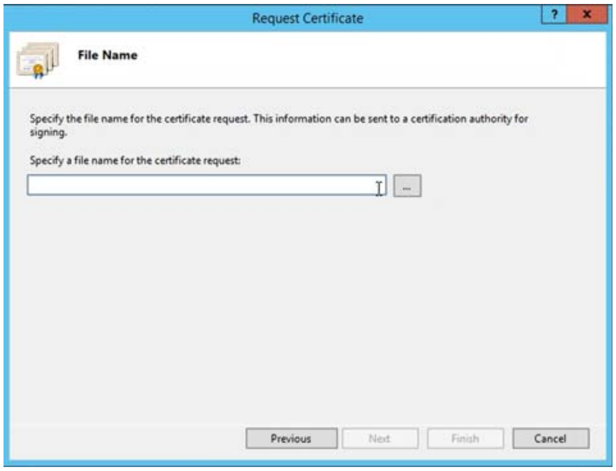
Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider:
Microsoft RSA SChannel Cryptographic Provider

Bit length:
2048

7. In the File Name screen, specify the filename and location of the certificate request, then click **Finish**.



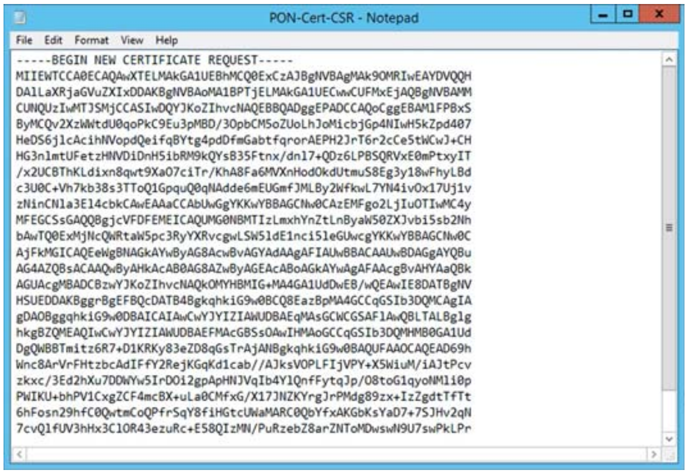
File Name

Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request:

8. After completing the certificate request process, locate the text file the CA just created for you at the location you specified in Step 7.

9. Open this file an a text editor. The contents should appear similar to the following:



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIEWTCCA0ECAQAwXTELMAkGA1UEBhMCQ0ExCzAJBgNVBAgMAk9OMRIwEAYDVQQH
DA1LaXRjaGVuZXIxDDAKBgNVBAoMA1BPTjELMAkGA1UECwwCUFMxEjAQBgNVBAMM
CUNQUzIwMTJSMjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAM1FPBxS
ByMCQv2XzWWtdU0qoPkC9Eu3pMBD/3OpbCM5oZUoLhJoMicbjGp4NIwH5kZpd407
HeDS6jlcAcihNVopdQeifqBYtg4pdDfmGabtfqrorAEPH2JrT6r2cCe5tWCwJ+CH
HG3nlmtUFetzHNVDiDnH5ibRM9kQYsB35Ftnx/dnl7+QDz6LPBSQRVxE0mPtxyIT
/x2UCBThKLdixn8qwt9XaO7ciTr/KhA8Fa6MVXnHodOkdUtmuS8Eg3y18wFhyLBd
c3U0C+Vh7kb38s3TToQ1GpquQ0qNAdde6mEUGmfJMLBy2WfkwL7YN4ivOx17Uj1v
zNinCNla3El4cbkCAwEAAaCCAbUwGgYKKwYBBAGCNw0CAzEMFgo2LjIuOTIwMC4y
MFEGCSsGAQQBgjcVFDFEMEICAQUMG0NBMTIzLmxhYnZtLnByaW50ZXJvbi5sb2Nh
bAwTQ0ExMjNcQWRtaW5pc3RyYXRvcgwLSW51dE1nci5leGUwcgYKKwYBBAGCNw0C
AjFkMGICAQEeWgBNAGkAYwByAG8AcwBvAGYAdAAgAFIAUwBBACAAUwBDAGgAYQBu
AG4AZQBsACAAQwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgAFAAcgBvAHYAaQBk
AGUAcgMBADCBzwYJKoZIhvcNAQkOMYHBMIG+MA4GA1UdDwEB/wQEAwIE8DATBgNV
HSUEDDAKBggrBgEFBQcDATB4BgkqhkiG9w0BCQ8EazBpMA4GCCqGSIb3DQMCAgIA
gDAOBggqhkiG9w0DBAICAIAwCwYJYIZIAWUDBAEqMAsGCWCGSAFlAwQBLTALBglg
hkgBZQMEAQIwCwYJYIZIAWUDBAEFMAcGBSsOAwIHMAoGCCqGSIb3DQMHMB0GA1Ud
DgQWBBTmitz6R7+D1KRKy83eZD8qGsTrAjANBgkqhkiG9w0BAQUFAAOCAQEAD69h
Wnc8ArVrFHtzbcAdIFfY2RejKGqKd1cab//AJksVOPLFIjVPY+X5WiuM/iAJtPcv
zkxc/3Ed2hXu7DDWYw5IrDOi2gpApHNJVqIb4Y1QnfFytqJp/O8toG1qyoNMli0p
PWIKU+bhPV1CxgZCF4mcBX+uLa0CMfxG/X17JNZKYrgJrPMdg89zx+IzZgdtTfTt
6hFosn29hfC0QwtmCoQPfrSqY8fiHGtcUWaMARC0QbYfxAKGbKsYaD7+7SJHv2qN
7cvQ1fUV3hHx3ClOR43ezuRc+E58QIzMN/PuRzebZ8arZNToMDwswN9U7swPkLPr
```

Keep this file open. You'll need the contents of this certificate request when you request the certificate from the Certificate Authority.

2.2.2 Request the server certificate from the Certificate Authority

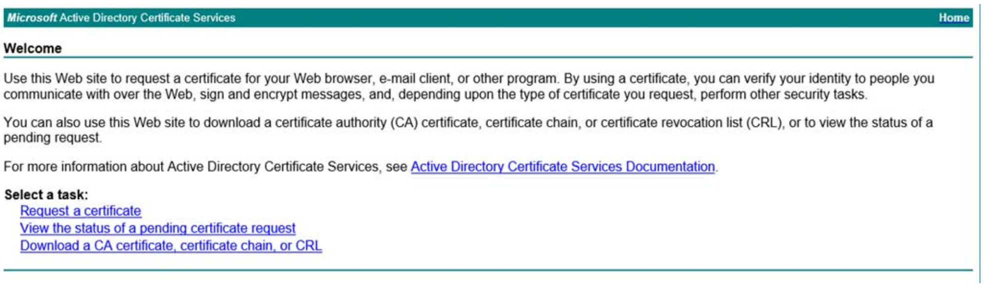
To submit the certificate request to the Certificate Authority

1. In your browser, navigate to the following URL:

   http://<CA_IP_address>/certsrv

   where <CA_IP_address> is the IP address of the computer where you installed your Certificate Authority.

   The browser should display the following web page:



Welcome

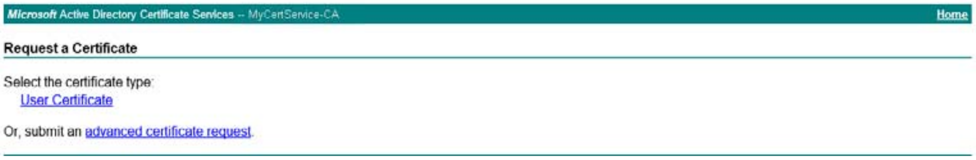
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

2. Select **Request a Certificate**. The Request a Certificate page appears.



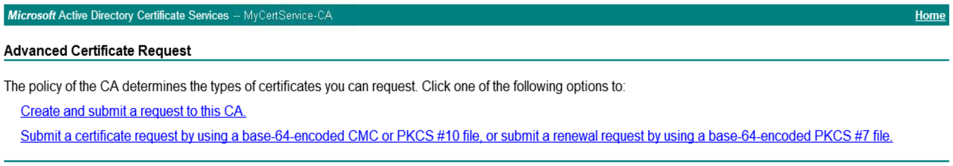
Microsoft Active Directory Certificate Services -- MyCertService-CA
Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

3. On the Request a Certificate page, click **Advanced Certificate Request**. The Advanced Certificate Request page appears.



Microsoft Active Directory Certificate Services -- MyCertService-CA
Home

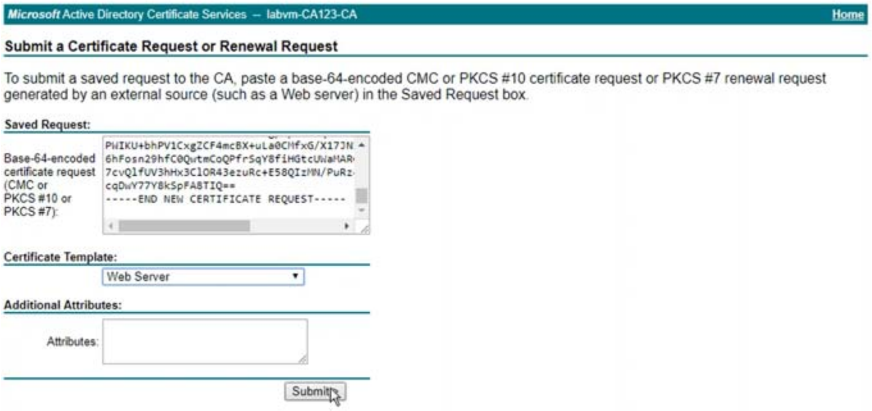
Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

4. On the Advanced Certificate Request page, select **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file…**. The Submit a Certificate Request or Renewal Request page appears.



Microsoft Active Directory Certificate Services -- labvm-CA123-CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
PWIKU+bhPV1CxgZCF4mcBX+uLa0CHfxG/X17JN
6hFosn29hfC0QwtmCoQPfrSqY8fiHGtcUWaMAR
7cvQlfUV3hHx3ClOR43ezuRc+E58QIzMN/PuRz
cqDwY77Y8kSpFA8TIQ==
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Template:

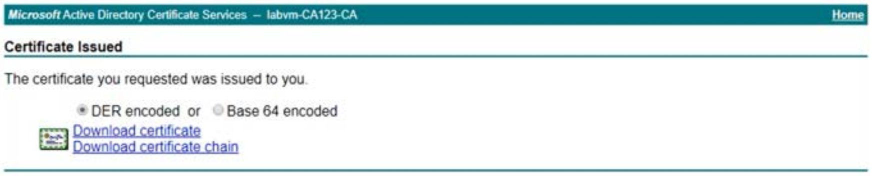
Web Server

Additional Attributes:

Attributes:

5. In the **Saved Request** field insert the contents of the CSR:
   a) Return to your text editor and copy the contents of the certificate request file.
   b) In the Saved Request section, paste the contents of the CSR file you received from your Certificate Authority.
6. From the Certificate Template drop-down, select **Web Server**.

7. Click **Submit**. The Certificate Authority issues the certificate, and the Certificate Issued page appears.



Microsoft Active Directory Certificate Services -- labvm-CA123-CA   Home

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

8. Click **Download certificate**. The certificate is downloaded to your browser's download folder.

Next, you'll need to attach the private key to the certificate and export it.

2.2.3 Exporting the server certificate

At this stage in the process, you should have a signed server certificate file in your Download folder. Before this certificate can be copied to and installed on the PrinterOn Server, you must attach the private key to it.

To attach the private key to the certificate, you can use the Certificates Snap-in in the Microsoft Management Console (MMC).

Important! The Certificates Snap-in is not added to the MMC by default; you must add it yourself. If it has not already been added, add the Certificates Snap-in to the server's Microsoft Management Console before continuing.

To attach the private key to the server certificate, you'll need to complete the following tasks:.

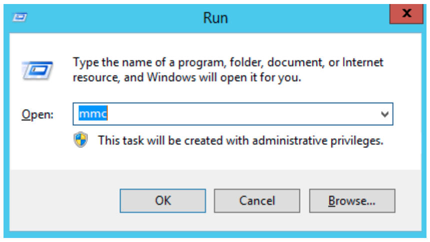
- Import the server certificate into the Certificate Snap-in.
- Export the server certificate with the private key.

2.2.3.1 Importing the server certificate into the Certificates Snap-in

To import your server certificate:

1. Open the Microsoft Management Console:

   a) On your keyboard, press the Windows key + R (**Run)**. The Run dialog appears.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

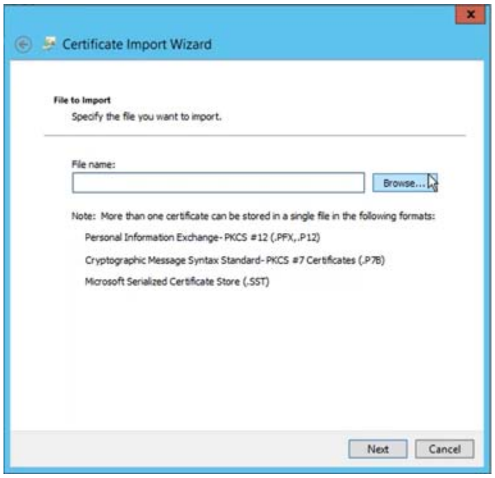
Open: mmc

This task will be created with administrative privileges.

   b) In the **Open** field, enter **mmc**, then click **OK**. The Microsoft Management Console opens.

   If the Certificates Snap-in has been added, you should see **Certificates (Local Computer)** listed in the left pane.

2. Click **Certificates (Local Computer**, then right-click **Personal** > **All Tasks** > **Import...**. The Certificate Import Wizard appears.
3. Click **Next** to display the File To Import screen.



File to Import

Specify the file you want to import.

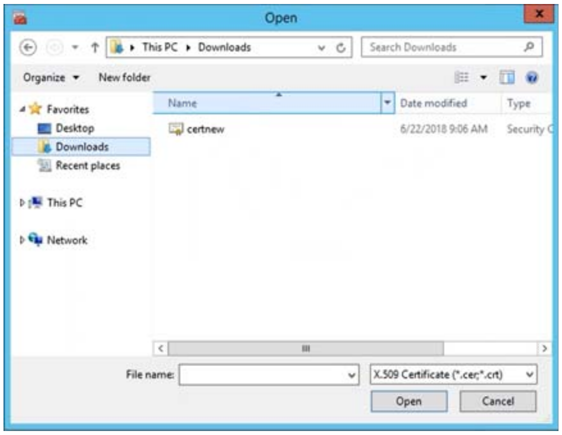
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

4. Click **Browse**, then navigate to and select your server certificate file.



5. Click **Open** to return to the wizard, then continue through the wizard until the final screen and click **Finish**.

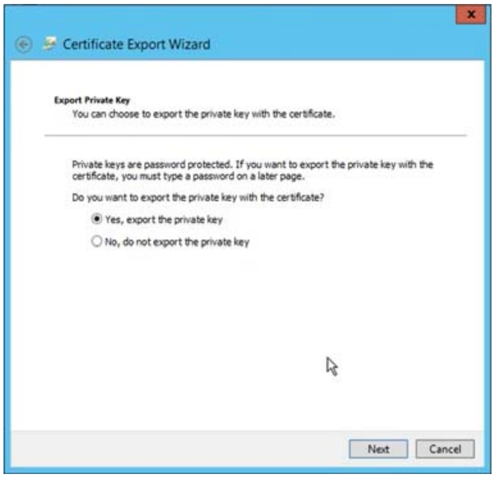
2.2.3.2 Exporting the certificate with the private keys

Now that you have imported the server certificate, the next step is to export it with the private key.

To export the server certificate with the private keys:

1. In the left pane of the MMC, click **Personal** > **Certificates**. The server certificate should now be listed.
2. Right-click the server certificate and select **All Tasks** > **Export**. The Certificate Export Wizard appears.
3. Click **Next** to display the Export Private Key screen.

4. In the Export Private Key screen, select **Yes, export the private key**, then click **Next**.



Export Private Key
You can choose to export the private key with the certificate.

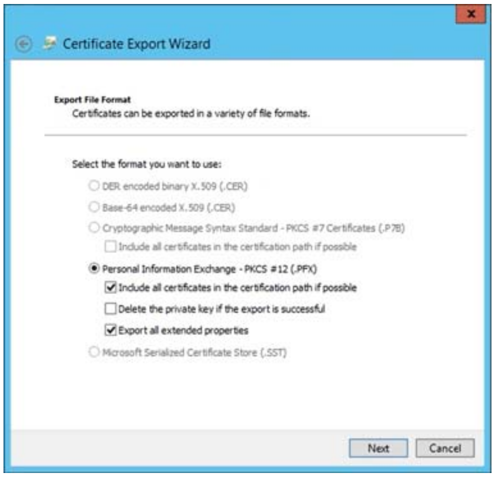
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

5. In the Export File Format screen, select **Export all extended properties**, then click **Next**.



Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

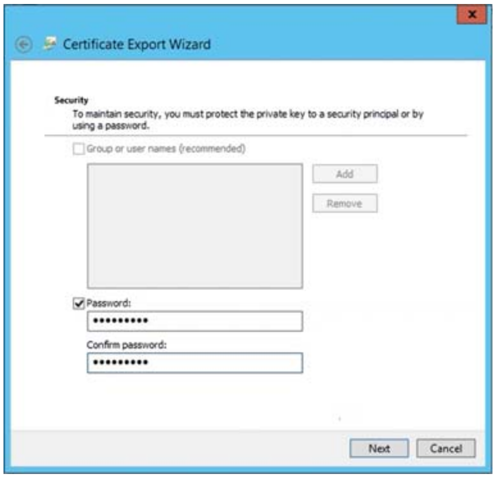
☑ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

☑ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

6. In the Security screen, specify and confirm a password that will be used to protect the certificate, then click **Next**.



Certificate Export Wizard

Security

To maintain security, you must protect the private key to a security principal or by using a password.

□ Group or user names (recommended)

☑ Password:

•••••••••

Confirm password:

•••••••••

7. In the File to export screen, specify the location and filename you want to export the certificate to, then click **Next**.
8. Click **Finish** to complete the export process.
9. Locate the server certificate in the location you exported it to, then transfer the .pfx certificate file to the PrinterOn server. You can email the certificate file, or save it to a location that is accessible to the PrinterOn Server.

Later, you'll install this certificate on the PrinterOn Server. For more information, see Chapter 4: Configuring your PrinterOn service to use the server certificate.

2.3 Exporting the CA root certificate

You have two options to secure client devices:

- Use the CA to create and export a client certificate and install it on all client devices.
- Import the CA root certificate on all client devices.

In a development scenario, it is simpler to simply export the CA root certificate and install it on the client device; there is no security benefit gained by creating an extra certificate specifically for client devices.

You can export the root certificate from the CA using the Certificates Snap-In in the Microsoft Management Console (MMC).

> **Important!** The Certificates Snap-in is not added to the MMC by default; you must add it yourself. If it has not already been added, add the Certificates Snap-in to the server's Microsoft Management Console before continuing.

To export the root certificate:

1. In the left pane of the MMC, click **Trusted Root Certification Authorities** > **Certificates**.
2. Locate the root certificate generated by the local CA you installed.
3. Right-click the root certificate and select **All Tasks** > **Export**. The Certificate Export Wizard appears.
4. Click **Next** to accept the default values in the next few screens, until you reach the File to Export screen.
5. In the File to Export screen, specify the location and filename you want to export the certificate to, then click **Next**.
6. Click **Finish** to complete the export process.

Later, you'll distribute this certificate to all client devices. For more information, see Chapter 5: Installing your local CA on client devices.

3

Creating a local Certificate Authority on macOS

To create a local Certificate Authority and set up and deploy your certificates on macOS, you must complete the following tasks:

1. Create the local Certificate Authority.
2. Create and export the server certificate.
3. Export the CA root certificate.

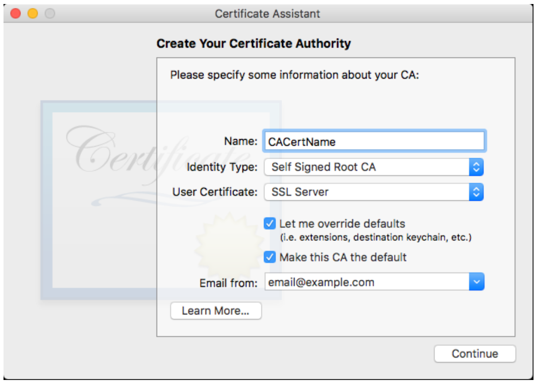
You can use the Keychain Access utility to complete all of these tasks.

3.1 Creating a local Certificate Authority on macOS

To create your own local Certification Authority on macOS:

1. In Finder, choose **Go** > **Utilities** > **Keychain Access**. The Keychain Access utility launches.
2. In Keychain Access, choose **Keychain Access** > **Certificate Assistant** > **Create a Certificate Authority**. This launches the Certificate Assistant wizard, which leads you through the process of creating a Certification Authority .

3. In Certificate Assistant, complete the Create Your Certification Authority screen then click **Continue**.



Create Your Certificate Authority

Please specify some information about your CA:

Name: CACertName

Identity Type: Self Signed Root CA

User Certificate: SSL Server

☑ Let me override defaults (i.e. extensions, destination keychain, etc.)

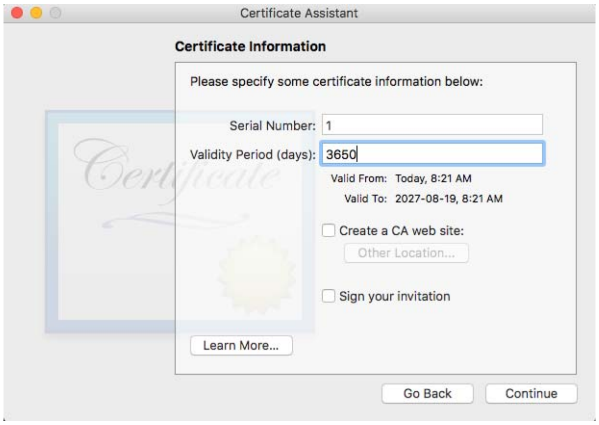
☑ Make this CA the default

Email from: email@example.com

Setting	Description
Name	A unique name for the CA.
Identity type	Select **Self Signed Root CA**.
User Certificate	Select **SSL Server**.
Let me override defaults	Enable this setting.
Make this CA the default	Enable this setting.
Email from:	The email address used by this CA to distribute certificates.

4. In the **Validity Period** field of the Certification Information screen, specify the number of days the certificate will remain valid for, then click **Continue**.

Important! Don't modify Serial Number.



Certificate Information

Please specify some certificate information below:

Serial Number: 1

Validity Period (days): 3650

Valid From: Today, 8:21 AM

Valid To: 2027-08-19, 8:21 AM

☐ Create a CA web site:

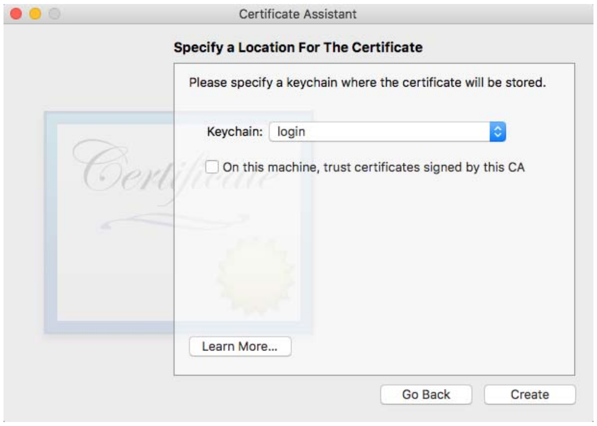
☐ Sign your invitation

5. Click **Continue**, then, in the following screen, specify your personal identifying information, if you choose.

   If you are simply using this certificate for non-production tasks (for example, proof of concept or testing), then in most cases, this information is unnecessary, and the defaults should be suitable.

6. Proceed through the remaining screens. Again, in most cases, the default values should be suitable.

7. In the Specify a Location For The Certificate screen, screen, select **login** as the keychain where your certificate is stored, then click **Create**.



Specify a Location For The Certificate

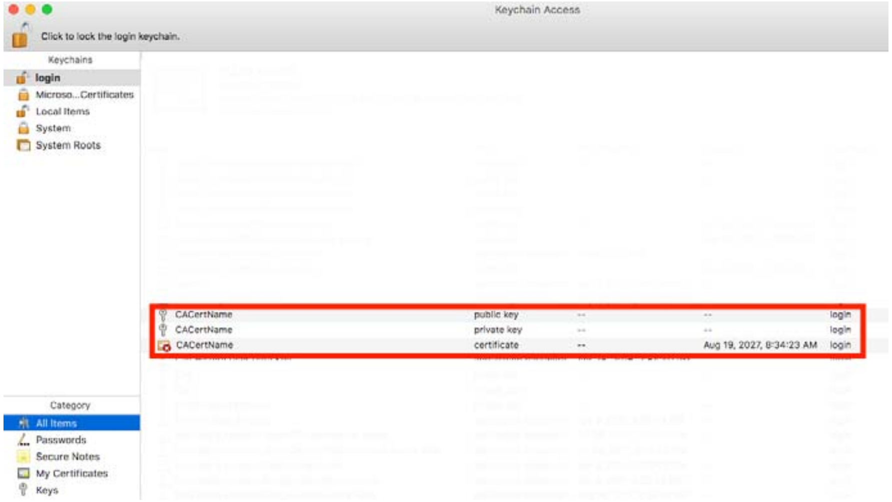
Please specify a keychain where the certificate will be stored.

Keychain: login

□ On this machine, trust certificates signed by this CA

   Keychain Access creates the certificate. Once it is complete, you can close the Certificate Assistant window and confirm your keychain items.

8. To confirm the keychain items, return to the Keychain Access window, then open the **login** keychain and locate your CA's root certificate, public key, and private key.



Click to lock the login keychain.

CACertName	public key	--	--	login
CACertName	private key	--	--	login
CACertName	certificate	--	Aug 19, 2027, 8:34:23 AM	login

9. Confirm that the certificate is trusted:
   a) Double-click the certificate to open the Certificate Options dialog.
   b) For the **When using this certificate** option, choose **Always Trust**.
   c) Close the dialog.

With the CA created, you can now:

- Create a server certificate for the PrinterOn Server.
- Export the root certificate to distribute it to client devices.

3.2 Creating and exporting a signed server certificate

Once you've created your Certificate Authority and have the root certificate, you can use it to issue the server certificate for the PrinterOn server. This section describes the process for creating a certificate for the PrinterOn server from your local Certification Authority.

You'll need to complete the following tasks:

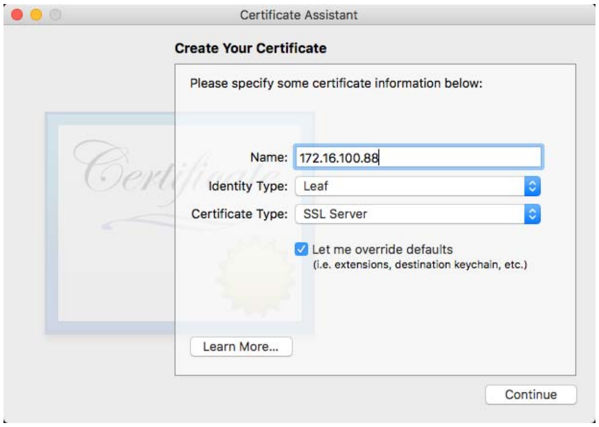
- Create the server certificate.
- Export the server certificate.

3.2.1 Creating the server certificate

To create a server certificate on macOS:

1. In Finder, choose **Go** > **Utilities** > **Keychain Access**. The Keychain Access utility launches.
2. In Keychain Access, choose **Keychain Access** > **Certificate Assistant** > **Create a Certificate**. This will launch Certificate Assistant, which leads you through the process of creating a certificate.

3. In Certificate Assistant, complete the Create Your Certificate screen, then click **Continue**.



Create Your Certificate

Please specify some certificate information below:

Name: 172.16.100.88

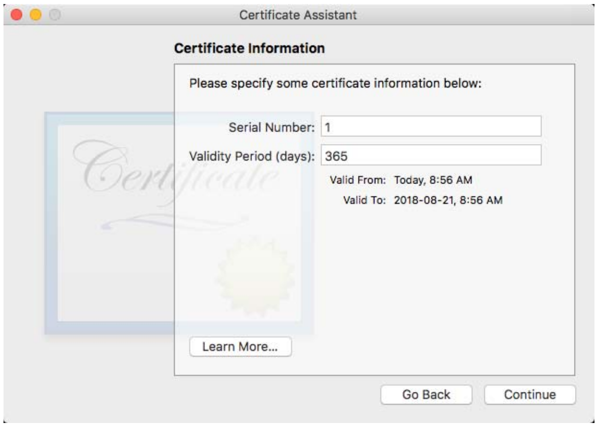
Identity Type: Leaf

Certificate Type: SSL Server

☑ Let me override defaults
(i.e. extensions, destination keychain, etc.)

Setting	Description
Name	The IP address of the PrinterOn Server. This value must be an IP address, not a hostname.
Identity Type	Select **Leaf**.
Certificate Type	Select **SSL Server**.
Let me override details	Enable this setting.

4. Complete the Certificate Information screen, then click **Continue**.



Certificate Information

Please specify some certificate information below:

Serial Number: 1

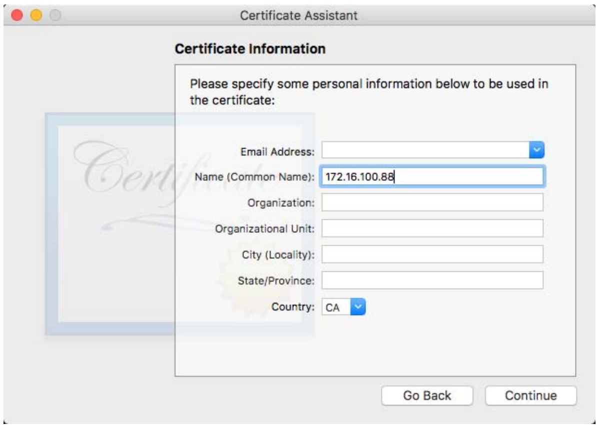
Validity Period (days): 365

Valid From: Today, 8:56 AM

Valid To: 2018-08-21, 8:56 AM

Setting	Description
Serial Number	Enter any value.
Validity Period	Specify the length of time you want the certificate to remain valid.

5. Complete the Certificate Information screen, then click **Continue**.



Certificate Assistant

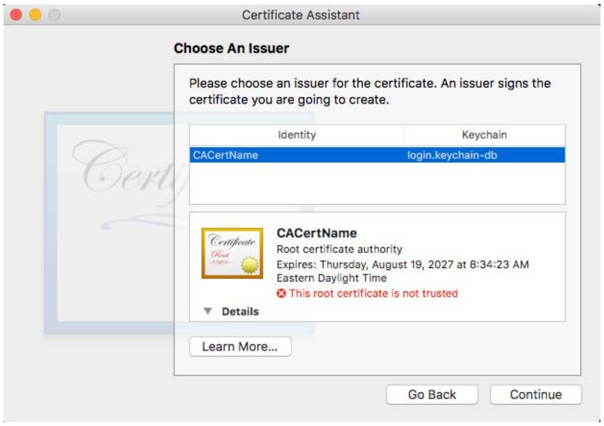
Certificate Information

Please specify some personal information below to be used in the certificate:

Email Address:
Name (Common Name): 172.16.100.88
Organization:
Organizational Unit:
City (Locality):
State/Province:
Country: CA

> **Note:** If you are only using this certificate for non-production tasks (for example, proof of concept or testing), then only the **Name (Common Name)** setting needs to be defined.
>
> The **Name** value must be the IP address of the PrinterOn Server, that is, it must match the **Name** value in Step 3.

6. In the Choose an Issuer screen, select the Certification Authority that you created in Creating a Certificate Authority on MacOS, then click **Continue**.



Certificate Assistant

Choose An Issuer

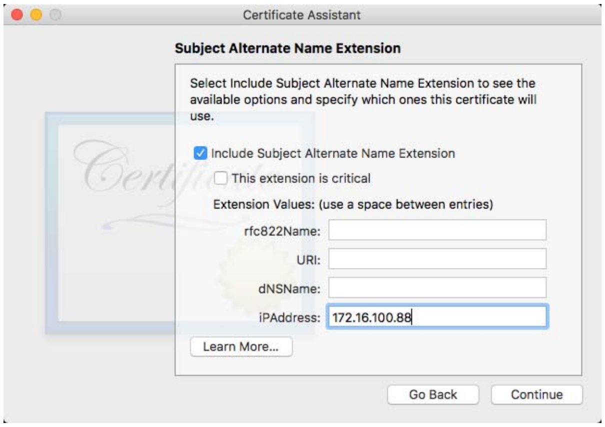
Please choose an issuer for the certificate. An issuer signs the certificate you are going to create.

Identity	Keychain
CACertName	login.keychain-db

CACertName
Root certificate authority
Expires: Thursday, August 19, 2027 at 8:34:23 AM Eastern Daylight Time
This root certificate is not trusted

7. Click **Continue** to proceed through the next four screens. until you arrive at the **Subject Alternative Name Extension** screen. In most cases, the default values should be suitable.

8. In the Subject Alternative Name Extension screen, check the Include **Subject Alternative Name Extension**, then enter the same IP address for the PrinterOn server and click **Continue**.



Subject Alternate Name Extension

Select Include Subject Alternate Name Extension to see the available options and specify which ones this certificate will use.

☑ Include Subject Alternate Name Extension

☐ This extension is critical

Extension Values: (use a space between entries)

rfc822Name:

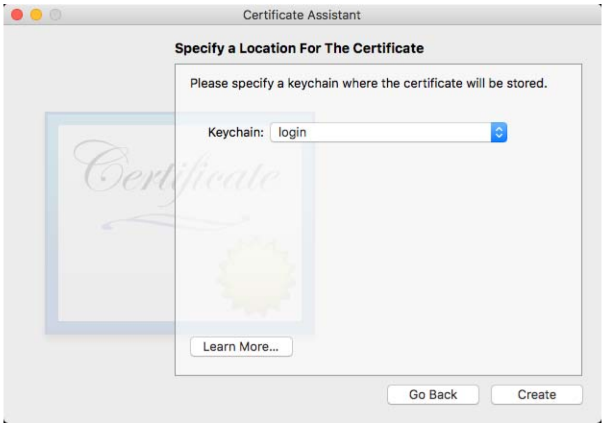
URI:

dNSName:

iPAddress: 172.16.100.88

> **Note:** The IP address should be the same address entered in Step 3 and Step 5. The remaining fields can be left blank.

9. In the Specify a Location for the Certificate screen, select **login** as the keychain where your certificate is stored, then click **Create**.



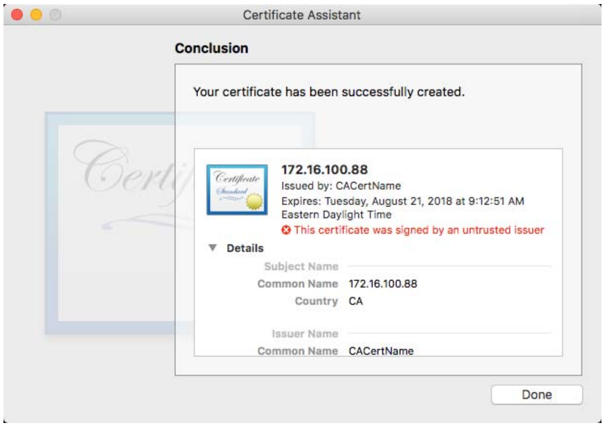
Specify a Location For The Certificate

Please specify a keychain where the certificate will be stored.

Keychain: login

Keychain Access creates the certificate.

10. In the Conclusion screen, click **Done** to close the Certificate Assistant window and confirm your keychain items.



Your certificate has been successfully created.

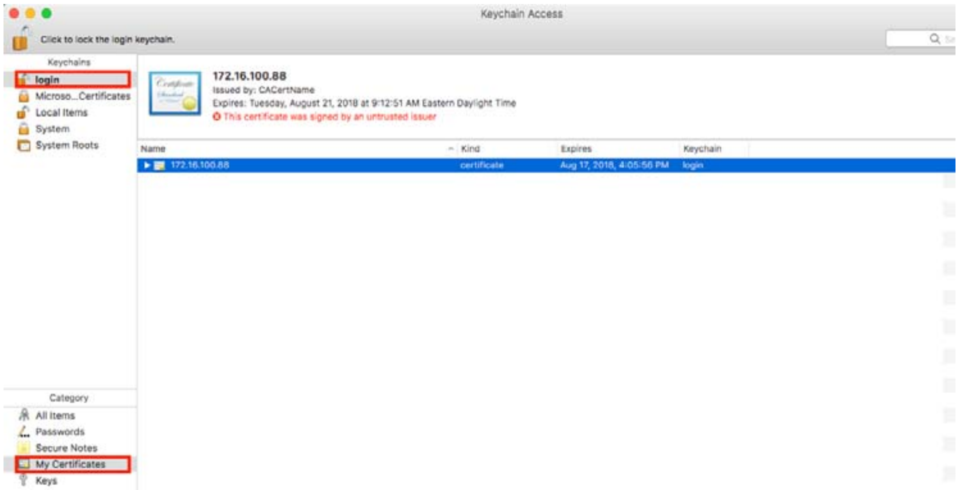
172.16.100.88
Issued by: CACertName
Expires: Tuesday, August 21, 2018 at 9:12:51 AM Eastern Daylight Time
This certificate was signed by an untrusted issuer

Details

Subject Name
Common Name 172.16.100.88
Country CA

Issuer Name
Common Name CACertName

11. To confirm the kechain items, return to the Keychain Access window, then open the **login** keychain and locate your server certificate (identified by the IP address of the PrinterOn server).



172.16.100.88
Issued by: CACertName
Expires: Tuesday, August 21, 2018 at 9:12:51 AM Eastern Daylight Time
This certificate was signed by an untrusted issuer

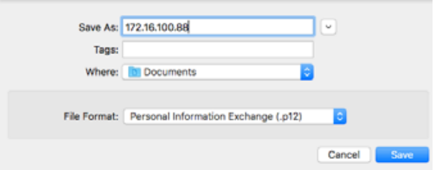
Name	Kind	Expires	Keychain
172.16.100.88	certificate	Aug 17, 2018, 4:05:56 PM	login

You can now export the server certificate so that it can be copied to and imported on the PrinterOn server.

3.2.2 Exporting the server certificate

Once you have the server certificate in your keychain, you can export to the PrinterOn server for use in your tests. This section describes various export scenarios.

1. In Keychain Access, select the server certificate (identified by the PrinterOn servers IP address).
2. Choose **File** > **Export** Items. The Export Certificate dialog appears.



Save As: 172.16.100.88

Tags:

Where: Documents

File Format: Personal Information Exchange (.p12)

3. Configure your export options.
4. Click **Save**.
5. Transfer the .pfx certificate file to the PrinterOn server. You can email the certificate file, or save it to a location that is accessible to the PrinterOn Server.

Later, you'll install this certificate on the PrinterOn Server. For more information, see Chapter 4: Configuring your PrinterOn service to use the server certificate.

3.3 Exporting the root certificate

With the CA created, you have two options for using it to secure client devices:

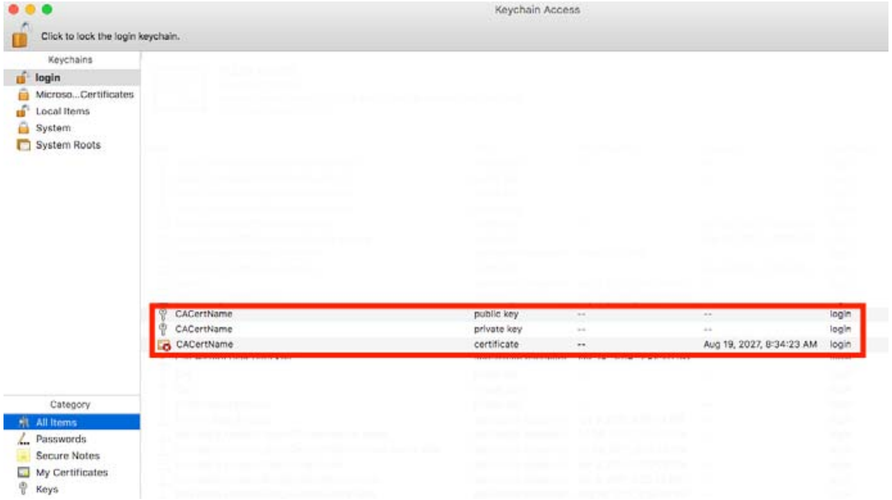
- Use the CA to create and export a client certificate and install it on all client devices.
- Export the CA itself and install it on all client devices.

In a development scenario, it is simpler to simply export the CA; there is no security benefit gained by creating an extra certificate specifically for client devices.

To export the CA:

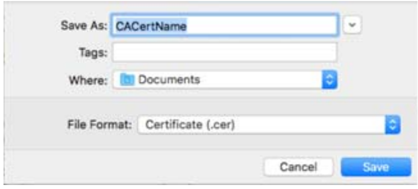
1. In the Keychain Access window, then open the **login** keychain.

2. Locate and select your CA's root certificate and public/private keys.



CACertName	public key	--	--	login
CACertName	private key	--	--	login
CACertName	certificate	--	Aug 19, 2027, 8:34:23 AM	login

3. Choose **File** > **Export** Items.



Save As: CACertName

Tags:

Where: Documents

File Format: Certificate (.cer)

4. In the Export dialog, confirm the export options, then click **Save**.

Later, you'll need distribute this certificate to all client devices. For more information, see Chapter 5: Installing your local CA on client devices.

4

Configuring your PrinterOn service to use the server certificate

To enable the PrinterOn server to use the server certificate issued from your local Certificate Authority, you'll need to complete the following tasks.

- Installing the server certificate on the PrinterOn server.
- Modifying the PrinterOn configuration files to use point to the server certificate.

4.1 Installing the server certificate on the PrinterOn server

To install the server certificate on the PrinterOn server, you can install the you'll need to complete the following tasks:

1. If it has not already been added, add the Certificates Snap-in to the server's Microsoft Management Console.
2. Import the server certificate to the PrinterOn Server.

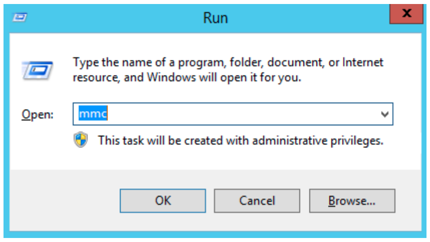
4.1.1 Importing the server certificate

If the Certificates Snap-in is added to the Microsoft Management Console, you can import the server certificate.

> **Important!** Before you begin, ensure that you have transferred the server certificate from the CA computer to the PrinterOn Server.

To import the server certificate:

1. Open the Microsoft Management Console:
   a) On your keyboard, press the Windows key + R (**Run)**. The Run dialog appears.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

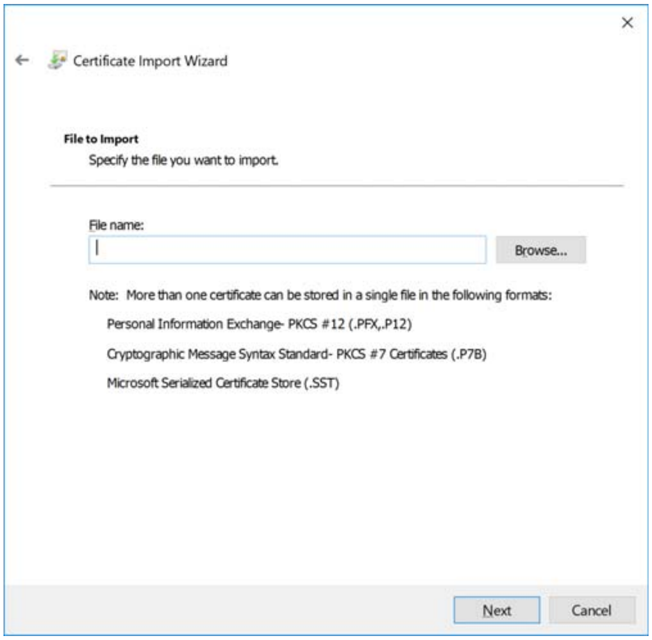
Open: mmc

This task will be created with administrative privileges.

   b) In the **Open** field, enter **mmc**, then click **OK**. The Microsoft Management Console opens.

   If the Certificates Snap-in has been added, you should see **Certificates (Local Computer)** listed in the left pane.
2. Click **Certificates (Local Computer**, then right-click **Personal** > **All Tasks** > **Import...**. The Certificate Import Wizard appears.
3. At the Welcome screen of the Certificate Import Wizard, click **Next**.

4. In the File to Import screen, browse to the root certificate, then click **Next**.



File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

5. In the Certificate Store screen, choose the location where the Import Wizard will store the certificate, then click **Finish**.

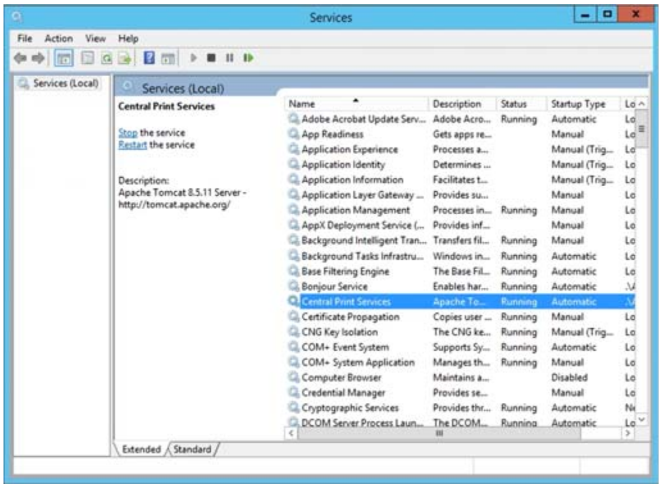
After importing the certificate to the PrinterOn server, you can modify the PrinterOn server configuration files so that PrinterOn uses the server certificate from the local CA.

4.2 Modifying the PrinterOn configuration files to use point to the server certificate

After you installed the server certificate from your local Certificate Authority on the PrinterOn server, you'll need to make a small modification to PrinterOn's Tomcat configuration file to ensure that the PrinterOn server is using this certificate for incoming TLS requests from clients.

To modify the PrinterOn Tomcat configuration file:

1. In the Windows Server Managers, click Tools > Services. The Services dialog appears:



Central Print Services

Stop the service
Restart the service

Description:
Apache Tomcat 8.5.11 Server - http://tomcat.apache.org/

Name	Description	Status	Startup Type	Lo
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Lo
App Readiness	Gets apps re...		Manual	Lo
Application Experience	Processes a...		Manual (Trig...	Lo
Application Identity	Determines ...		Manual (Trig...	Lo
Application Information	Facilitates t...		Manual (Trig...	Lo
Application Layer Gateway ...	Provides su...		Manual	Lo
Application Management	Processes in...	Running	Manual	Lo
AppX Deployment Service (...	Provides inf...		Manual	Lo
Background Intelligent Tran...	Transfers fil...	Running	Manual	Lo
Background Tasks Infrastru...	Windows in...	Running	Automatic	Lo
Base Filtering Engine	The Base Fil...	Running	Automatic	Lo
Bonjour Service	Enables har...	Running	Automatic	.\/
Central Print Services	Apache To...	Running	Automatic	.\/
Certificate Propagation	Copies user ...	Running	Manual	Lo
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Lo
COM+ Event System	Supports Sy...	Running	Automatic	Lo
COM+ System Application	Manages th...	Running	Manual	Lo
Computer Browser	Maintains a...		Disabled	Lo
Credential Manager	Provides se...		Manual	Lo
Cryptographic Services	Provides thr...	Running	Automatic	N
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Lo

2. In the list of services, locate and stop the Central Print Services.
3. In a text editor, open C:\Program Files (x86)\PrinterOn Corporation\Apache Tomcat\Conf\server.xml.
4. Locate the following entry:

```
<!-- Define a SSL HTTP/1.1 Connector on port 443
<Connector port="443"
   protocol="com.printeron.tomcat.http11.Http11NioProtocol"
   SSLEnabled="true" maxThreads="150" scheme="https"
   secure="true" clientAuth="false"
   sslEnabledProtocols="TLSv1.1,TLSv1.2"
   keystoreFile="${pon.data.root}\KeyStore\keystore"
   keystorePass="rz6KZSpMD7fy7Co6UfIBmw%3D%3D"
/>
```

5. Locate the keystore properties. Modify them as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 443
<Connector port="443"
   protocol="com.printeron.tomcat.http11.Http11NioProtocol"
   SSLEnabled="true" maxThreads="150" scheme="https"
   secure="true" clientAuth="false"
   sslEnabledProtocols="TLSv1.1,TLSv1.2"
   keystoreType="PKCS12"
   keystoreFile="C:\Certs\<server_cert_name>"
   keystorePass="<server_cert_pw>"
/>
```

where <*server_cert_name*> and <*server_cert_pw*> are the name and password you defined when you created the server certificate with your Windows CA or macOS CA.

6. Save the file.
7. Return to the Windows Server Manager Service dialog and restart the Central Print Services.

5

Installing your local CA on client devices

With your local CA installed, and the PrinterOn server properly configured with a server certificate, the last step is to secure the the client devices that need to communicate with the server.

You have two options to secure client devices:

- Use the CA to create and export a client certificate and install it on all client devices.
- Import the CA on all client devices.

In a development scenario, it is simpler to simply export the CA and install it on the client CA; there is no security benefit gained by creating an extra certificate specifically for client devices.

The process for installing the CA depends on the OS of the client device:

- Installing the CA root certificate on Windows devices
- Installing the root certificate on iOS devices
- Installing the root certificate on Android devices

5.1 Installing the CA root certificate on Windows devices

To import the certificates to client Windows computers, you can install the you'll need to complete the following tasks:

1. If it has not already been added, add the Certificates Snap-in to the server's Microsoft Management Console.
2. Import the CA root certificate.

5.1.1 Importing the CA root certificate

Once the Certificates Snap-in is added to the Microsoft Management Console, you can import the certificate root.

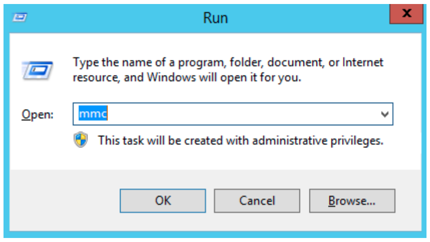
To install the root certificate on Windows devices, you must first export the certificate and transfer the certificate file to the device. You can make the certificate accessible to the client Windows device by:

- emailing the exported certificates to an account that is accessible from the client Windows device.
- putting the exported certificates on cloud storage in an account that is accessible from the client Windows device.

Important! This task only makes the root certificate available to Internet Explorer. If you are using Firefox, Google Chrome, or some other browser, you'll need to import the root certificate separately for that application.

To import the root certificate:

1. Open the Microsoft Management Console:
   a) On your keyboard, press the Windows key + R (**Run)**. The Run dialog appears.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

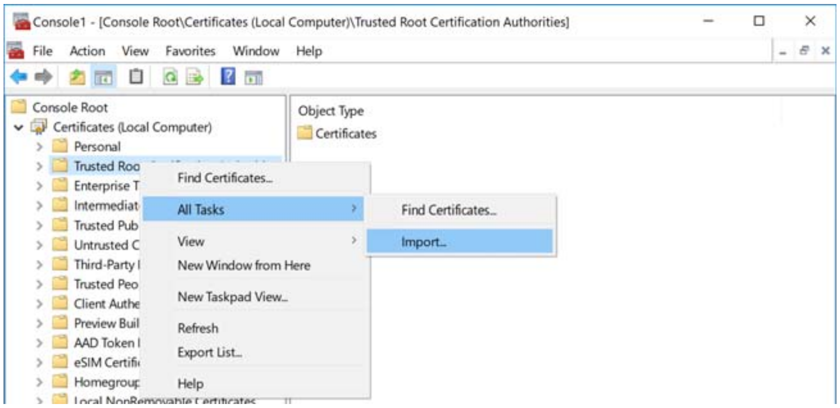
Open: mmc

This task will be created with administrative privileges.

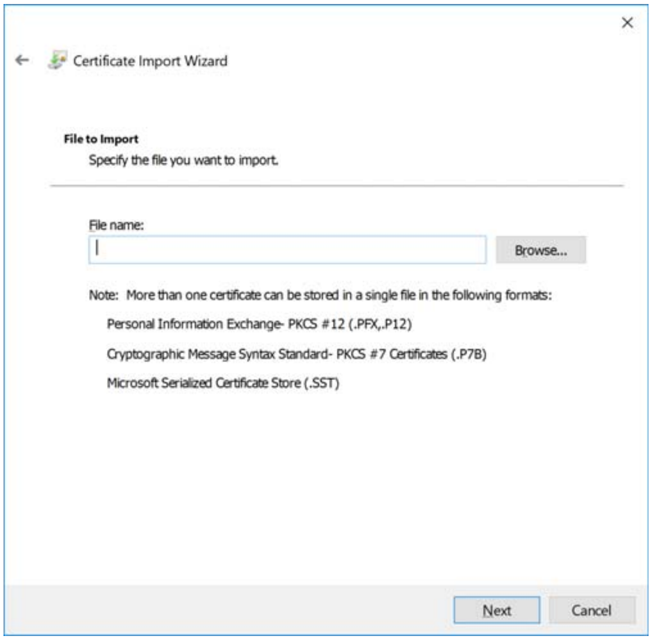
   b) In the **Open** field, enter **mmc**, then click **OK**. The Microsoft Management Console opens.

If the Certificates Snap-in has been added, you should see **Certificates (Local Computer)** listed in the left pane.

2. Right-click **Trusted Root Certification Authorities**, then select **All Tasks** > **Import....**



3. At the Welcome screen of the Certificate Import Wizard, click **Next**.
4. In the File to Import screen, browse to the root certificate.


Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

5. Click **Next**.
6. Click **Finish**.

5.2 Installing the root certificate on iOS devices

To install the root certificate on iOS devices, you must first export the certificate and transfer the certificate file to the device. You can make the certificate accessible to the client iOS device by:

- emailing the exported certificates to an account that is accessible from the client iOS device.
- putting the exported certificates on cloud storage in an account that is accessible from the client iOS device.

To install the root certificate:

1. Locate the ’s root certificate.
2. Tap the certificate.
3. Click **Install**.
4. Click **Done**.
5. Verify that the certificate has been installed successfully:
   a) Go to **Settings** > **General** > **Profiles & Device Management**.
   b) Click the certificate. It should you should see Verified.
6. Ensure that the root certificate has full trust enabled:
   a) Go to **Settings** > **General** > **About** > **Certificate Trust Settings**.
   b) If full trust is not enabled, enable it.
7. On Safari, browse to the PrinterOn Web Print URL. You should see a lock symbol under the address bar.

5.3 Installing the root certificate on Android devices

To install the root certificate on Android devices, you must first export the certificate and transfer the certificate file to the device. You can make the certificate accessible to the client Android device by:

- emailing the exported certificates to an account that is accessible from the client Android device.
- putting the exported certificates on cloud storage in an account that is accessible from the client Android device.

To install the root certificate:

1. On your Android device, open **Settings**.

2. Locate and open the **Security** settings.
3. In the Security settings, under **Credential storage**, tap **Install from device storage**.
4. In the top left, open the menu. The **Open from** list appears.
5. In the **Open from** list, tap the location where you saved the certificate.
6. Locate and tap the certificate file.

   > **Note:** If necessary, enter the key store password and tap **OK**.

   The Name the certificate dialog appears.
7. In the **Certificate Name** field, type a name for the certificate.
8. In the **Credential Use** drop-down, choose **VPN and apps**.
9. Click **OK**.

> **Note:** If you haven't already set a PIN, pattern, or password for your device, you'll be asked to set one up.

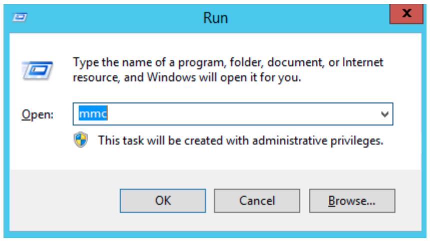
A

Adding the Certificates Snap-in to the Microsoft Management Console

Several tasks in this guide use the Certificates Snap-In in the Microsoft Management Console. By default, this snap-in is not available in the console; to access it, you first need to add it.

To add the Certificates Snap-In:

1. On the PrinterOn server computer, open the Microsoft Management Console:
   a) On your keyboard, press the Windows key + R (**Run)**. The Run dialog appears.



Run

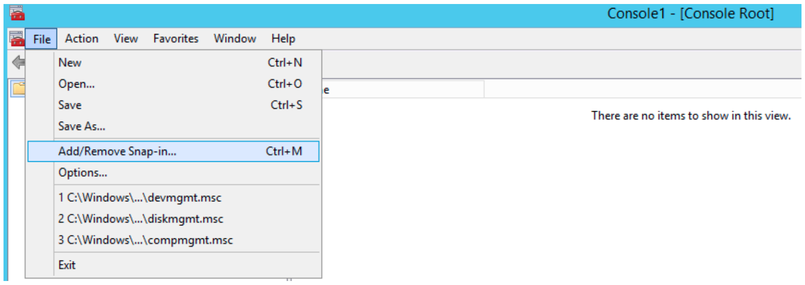
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

This task will be created with administrative privileges.

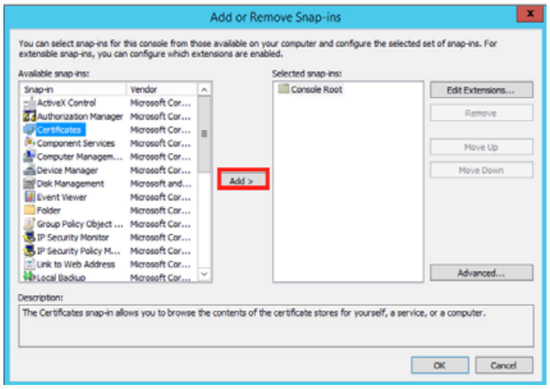
   b) In the **Open** field, enter **mmc**, then click **OK**. The Microsoft Management Console opens.

2. In the Console, click **File** > **Add/Remove Snap-in**. The Add or Remove Snap-ins dialog appears.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\...\devmgmt.msc
2 C:\Windows\...\diskmgmt.msc
3 C:\Windows\...\compmgmt.msc
Exit

There are no items to show in this view.

3. From the **Available Snap-ins** list, select **Certificates**, then click **Add** to move it to the **Selected Snap-ins** list.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Backup	Microsoft Cor...

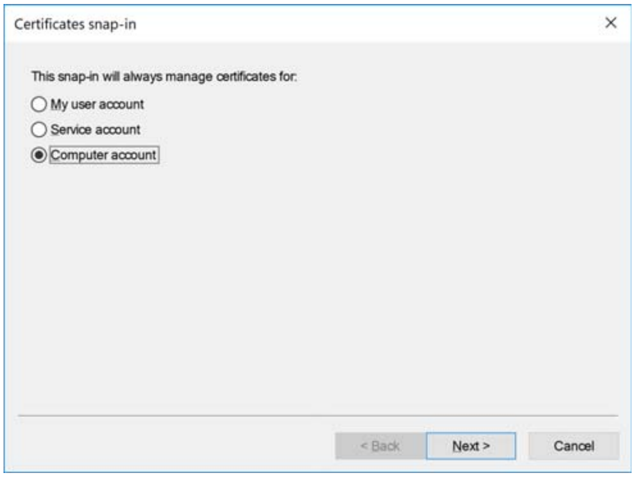
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. Once added to the Selected Snap-ins list, a dialog appears to allow you to specify which accounts the Certificates are managed for. As a best practice, you should select **Computer Account**.



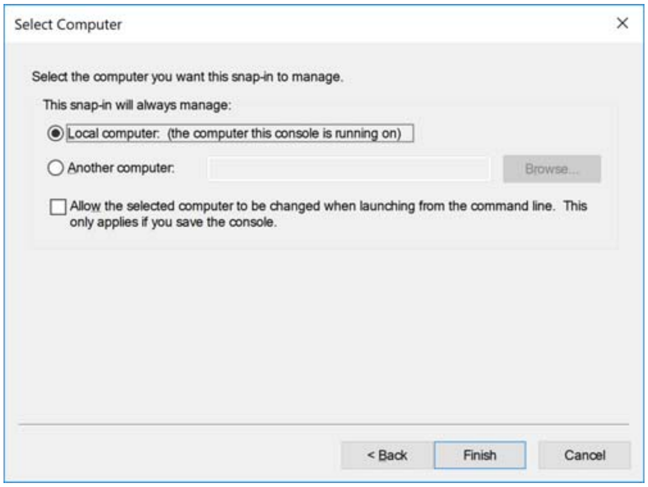
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. In the Select Computer screen, select **Local computer**, since this is the computer that is hosting the PrinterOn server.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

6. Click **Finish**.
7. In the Add or Remove Snap-ins dialog, click **OK**.