

PrinterOn Development

Setting up a Local Certificate Authority



mobile printing solutions | enterprise | education | public printing locations

Contents

Chapter 1: Introduction	3
Overview: Setting up a local Certificate Authority	. 4
Chapter 2: Creating a local Certificate Authority on Windows Server	5
Creating the local Certificate Authority	. 6
System prerequisites	. 6
Installing the Active Directory Certificate Authority	. 7
Configuring the AD Certificate Service	. 9
Creating and exporting a signed server certificate	15
Creating a certificate signing request	15
Request the server certificate from the Certificate Authority	19
Exporting the server certificate	
Exporting the CA root certificate	25
Chapter 3: Creating a local Certificate Authority on macOS	27
Creating a local Certificate Authority on macOS	27
Creating and exporting a signed server certificate	30
Creating the server certificate	30
Exporting the server certificate	35
Exporting the root certificate	35
Chapter 4: Configuring your PrinterOn service to use the server certificate	37
Installing the server certificate on the PrinterOn server	37

Importing the server certificate	38
Modifying the PrinterOn configuration files to use point to the server certificate	39
Chapter 5: Installing your local CA on client devices	42
Installing the CA root certificate on Windows devices Importing the CA root certificate Installing the root certificate on iOS devices	43
Installing the root certificate on Android devices	

Appendix A: Adding the Certificates Snap-in to the Microsoft Management Console 47

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.

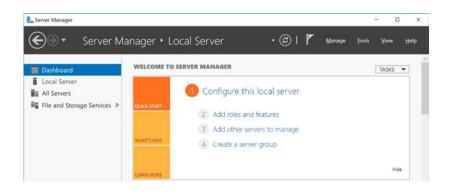
Important! DO NOT install your local CA on the same Windows Server that is hosting your PrinterOn server. The local CA can cause conflicts with PrinterOn's installation of Apache Tomcat.

2.1.2 Installing the Active Directory Certificate Authority

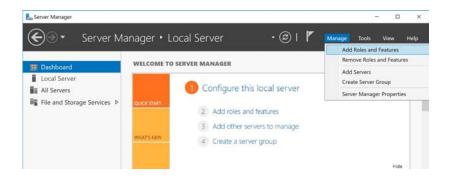
Windows Active Directory lets you set up a Certificate Authority as part of its Certificate Services.

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

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



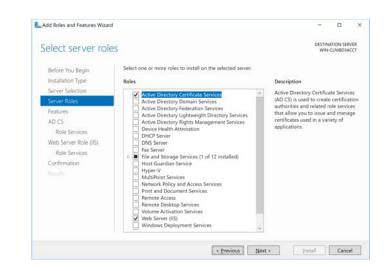
2. From the top menu, click Manage > Add Roles and Features.



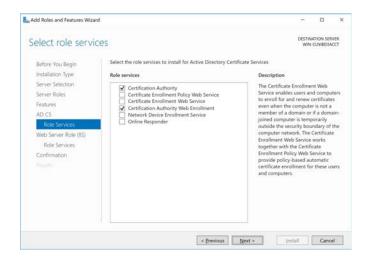
The Add Roles and Features wizard opens.

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**.



- 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



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 installa	ation selections		ACLINIBD34	
Before You Begin	To install the following roles, role services, or features on selected server, o	lick Install.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this			
Server Roles	been selected automatically. If you do not want to install these optional fe their check boxes	atures, click Prev	nous to c	iea
Features				
AD CS	.NET Framework 4.6 Features			12
Role Services	ASP.NET 4.6			
Web Server Role (IIS)	WCF Services			
	HTTP Activation			1
Role Services	Active Directory Certificate Services			
Confirmation	Certification Authority			
	Certificate Enrollment Web Service			
	Remote Server Administration Tools			
	Role Administration Tools			
	Active Directory Certificate Services Tools			
	Certification Authority Mananement Tools			
	Export configuration settings Specify an alternate source path			

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.

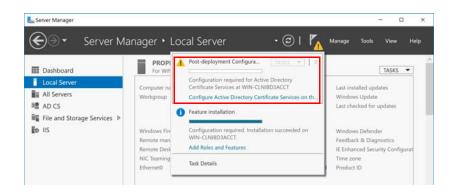
To configure the Active Directory Certificate Services:

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**.



The AD CS Configuration wizard opens.

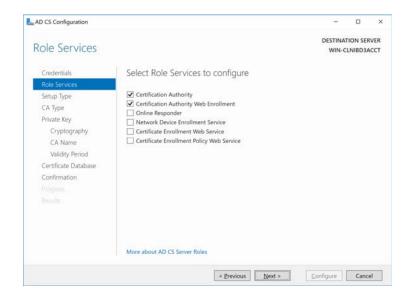
3. In the Credentials screen, locate the **Credentials** field and confirm that it displays the Domain Administrator account.

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.

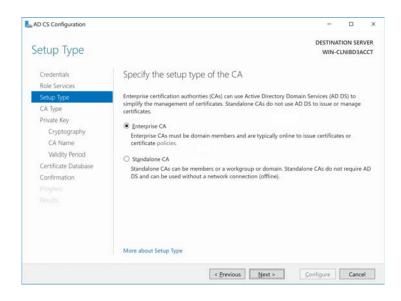
If the **Credentials** field does not display the Domain Administrator account:

- 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.

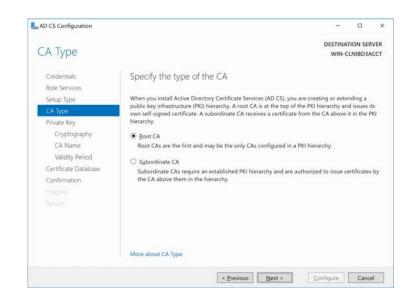
- 5. In the Role Services screen, select the following services, then click Next:
 - Certification Authority
 - Certification Authority Web Enrollment



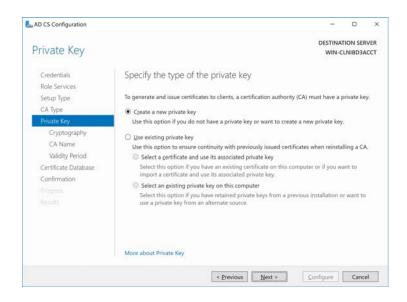
6. In the Setup Type screen, choose Enterprise CA, then click Next.



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



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



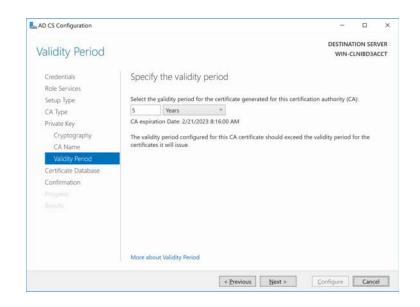
9. In the Cryptography screen, select the cryptography settings you want to use, then click **Next**.

AD CS Configuration					0
Cryptography fo	or CA		DESTINAT WIN-CI	ION SER	
Credentials Role Services	Specify the cryptographic options				
Setup Type	Select a gryptographic provider:		Key length:		
CA Type	RSA#Microsoft Software Key Storage Provider	~	2048		~
Private Key	Select the hash algorithm for signing certificates issued by t	his CA:			
Cryptography	SHA256	~	1		
CA Name	SHA384				
Validity Period	SHA512				
Certificate Database	SHA1				
Confirmation	MD5	v			
	Allow administrator interaction when the private key is a	ccessed l	by the CA.		
	More about Cryptography				
	< Previous Next :		Configure	Cance	4

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

CA Name		TION SER	
Credentials Role Services Setup Type CA Type	Specify the name of the CA Type a common name to identify this certification authority (CA). This name is a certificates issued by the CA. Distinguished name suffix values are automatically be modified.		car
Private Key Cryptography	<u>Common name for this CA:</u>		
CA Name	WIN-SRVRACCT-1		
Validity Period	Distinguished name suffic:		
Certificate Database	DC=ponadmin,DC=mycompany,DC=local		
Confirmation	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**.



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

L AD CS Configuration		-		х
CA Database		DESTINA WIN-C	TION SEE	10000
Credentials Role Services Setup Type	Specify the database locations			
CA Type	C\Windows\system32\CertLog			
Private Key	Certificate database log location:			
Cryptography CA Name Validity Period	C/Windows\system32\CertLog			
Certificate Database				
Confirmation				
	More about CA Database			
	< Previous Next >	Configure	Canc	el

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.

AD CS Configuration		-		×
CA Database		DESTINA WIN-C	TION SER	
Credentials Role Services	Specify the database locations			
Setup Type CA Type	C:\Windows\system32\CertLog			
Private Key	Certificate database log location:			
Cryptography CA Name	C\Windows\system32\CertLog			
Validity Period Certificate Database				
Confirmation Progress				
	More about CA Database			

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.

9	Internet Information Services (IIS) Manager	- 0 ×
WIN-SRVRACC	T-1 >	a = 6 19
File View Help Connections Q - L - S. Surt Page WIM-SRVRACT-IWIN-SRVRA - Application Pools p - Stes	VUN-SRVRACCT-1 Home Inter • • •	Actions Import Create Queficiate Request Complex Certificate Reguest Create Self-Signed Certificate Enable Automatic Rebind of Rebind of Certificate Welp
¢ IIII >	c III	2
Ready		9

3. In the central pane, select Server Certificates.

File View Help	11.5	10 × 6 10
Connections Conne	Image: Solution of the solution	Actions Import Create Optificate Request. Create Domain Certificate. Create Self-Signed Certificate. Enable Automatic Relaind of Rende Certificate Help
C III >	Teatures View	63

- 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**.

ana se sua de la ca	Request Certificate	? X
Distinguished	d Name Properties	
	nation for the certificate. State/province and City/locality must be specified as nnot contain abbreviations.	
Common name:	CPS2012R2	
Organization:	I I	
Organizational unit:		
City/locality		
State/province:		
Country/region:	US v	
	Previous Next Finish	Cancel

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**.

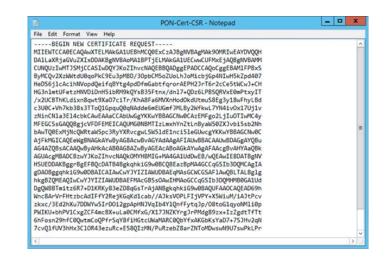
Select a cryptographic servi certificate's encryption stre length may decrease perfor	ngth. The greater the	length. The bit bit length, the	length of the end stronger the secu	ryption key deten rity. However, a g	mines the reater bit
Cryptographic service provi	ider:				
Microsoft RSA SChannel Cr	yptographic Provide	r .	~		
Bit length:					
2048	•				

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

Request Certificate	? X
File Name	
Specify the file name for the certificate request. This information can be so signing.	ent to a certification authority for
Specify a file name for the certificate request:	
	I
Previous	led Finish Cancel

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:



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

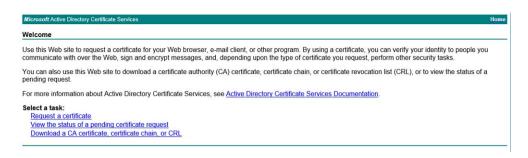
To submit the certificate request to the Certificate Authority

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:



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



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



 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 Iabvm-CA123-CA	Hon
Submit a Certi	ficate Request or Renewal Request	
	ved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request n external source (such as a Web server) in the Saved Request box.	or PKCS #7 renewal request
Saved Request:		
	PWIKU+bhPV1CxgZCF4mcBX+uLaBCHFxG/X173N + 6hFosn2bhfCQutetsCOQFfcSqV8FiHGtcUNaMAR 7cvQ1fVU3MhsClCRAFsEuRcF85QI2IWI/PWR: cqDuV77Y8HSpFABTIQ== END NEW CERTIFICATE REQUEST	
Certificate Templa	ate:	
	Web Server	
Additional Attribu	ites:	
Attributes:		
	Submitta	

- 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.

	Run
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	This task will be created with administrative privileges.
	OK Cancel Browse

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.

- 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.



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

	c)pen				×
🕣 💿 🔹 🕆 🚺 🕨 This	PC > Downloads	v C	Searc	h Downloads		Q
Organize 👻 New folder				8	[
4 😤 Favorites	Name		٣	Date modifie	d	Туре
E Desktop	a certnew			6/22/2018 9:0	6 AM	Security (
🎉 Downloads						
Þ 👯 This PC Þ 🗣 Network						
<		88				>
File nan	ne	~	X.50	9 Certificate (*	cer;*.crt)	*
				Open	Cano	el

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.



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



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

Security	
	ct the private key to a security principal or by
Group or user names (recommende	-
Cardop of user names precumments	
	Add
	Remove
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:

- 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.
- 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**.

		ficate Authority
	Please specify so	me information about your CA:
	Name:	CACertName
Ger	Identity Type:	Self Signed Root CA
	User Certificate:	SSL Server
	500	 Let me override defaults (i.e. extensions, destination keychain, etc.) Make this CA the default
	Email from:	email@example.com
	Learn More	

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 Informatio	n
	Please specify some c	ertificate information below:
	Serial Number:	1
	Validity Period (days):	3650
Ce	ertylicate	Valid From: Today, 8:21 AM Valid To: 2027-08-19, 8:21 AM
		Create a CA web site:
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Other Location
	and the second	Sign your invitation
	Learn More	

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.
C	Keychain: login 🔹
5	
	and the second sec
	Learn More
	Go Back Create

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.

5			
Click to lock the login ke	eychain.		
Keychains			
login			
MicrosoCertificates			
Local Items			
System			
System Roots			
	-	public key	login
	CACertName CACertName		ingle
	CACertName	private key	login login
			login login
	CACertName	private key	login
	CACertName CACertName CACertName	private key Aug 19, 2027, 0/34/23 AM certificate Aug 19, 2027, 0/34/23 AM	login
Category		private key Aug 19, 2027, 8:34:23 AM	login
All Items	CACertName CACertName CACertName	private key Aug 19, 2027, 0/34/23 AM certificate Aug 19, 2027, 0/34/23 AM	login
All Items Passwords	CACertName CACertName	private key Aug 19, 2027, 8:34:23 AM certificate Aug 19, 2027, 8:34:23 AM	login
All Items	CACertName CACertName	private key 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:

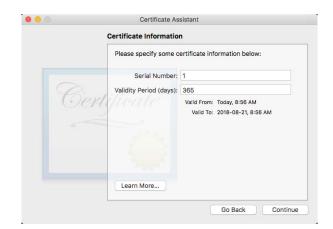
- 1. In Finder, choose **Go** > **Utilities** > **Keychain Access**. The Keychain Access utility launches.
- In Keychain Access, choose Keychain Access > Certificate Assistant > Create a Certificate. This will launch Certificate Assistant, which leads you through the process of creating a certificate.

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



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**.



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

- Certificate Assistant

 Certificate Information

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

 Email Address:

 Tr216.100.88

 Organization

 Organization

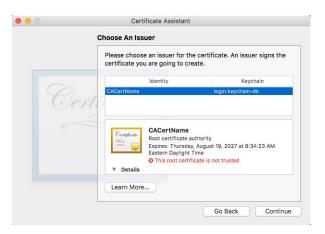
 Country:
 Cau

 Co Back
 Continue
- 5. Complete the Certificate Information screen, then click Continue.

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**.



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		
0	This extension is critical		
	Extension Values: (use a space between entries)		
	rfc822Name:		
	URI:		
	dNSName:		
	iPAddress: 172.16.100.88		
	Learn More		

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 Certific Please specify a keychain where the	
	Fiease specify a Reychain where the	certinicate will be stored.
	Keychain: login	٥
B	ertificate	
Ú.	engicaic	
	2003	
	2.2	
	Learn More	

Keychain Access creates the certificate.

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

	Conclusion
	Your certificate has been successfully created.
Cer	122.16.100.88 Issued by: CACertName Explores: Tuesday, August 21, 2018 at 9:12:51 AM Eastern Daylight Time This certificate was signed by an untrusted issuer Testis
	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).

Click to lock the log	in keychain.	Keychain	Access		C
Keychains Iogin MicrosoCertificate Local Items System	Expires: Tuesday, August	21, 2018 at 9:12:51 AM Eastern Daylight Time ned by an untrusted issuer			
System Roots	Name	~ Kind	Expires	Keychain	
	▶ 📷 172.16.100.88	certificate	Aug 17, 2018, 4:05	556 PM login	
Category					
Category All Items					
All Items Passwords					
All Items					

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)	0
		Cancel Save

- 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.

••		Keychain A	ccess		
Click to lock the login key	ychain.				
Keychains					
login					
MicrosoCertificates Local Items System					
System Roots					
	@ CACertName	public key	**		login
	P CACertName	private key			login
1	G CACertName	certificate		Aug 19, 2027, 8:34:23 AM	login
Category					
All Items					
Passwords					
Secure Notes					
My Certificates					
Keys					

3. Choose File > Export Items.

and the second	CACertName			
Tags: Where:	Document	5	0	
File Forr	nat: Certificat	e (.cer)		0
			Cancel	Save

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.

	Run
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	This task will be created with administrative privileges.
	OK Cancel Browse

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.

- 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				
S	pecify the file you wa	ant to import.			
-	le name:				
Ĩ					Browse
N	lote: More than one	certificate can be stor	ed in a single file in	the following fo	rmats:
	Personal Informati	ion Exchange- PKCS	#12 (.PFX,.P12)	100	
	Cryptographic Mes	sage Syntax Standard	1- PKCS #7 Certific	ates (.P7B)	
	Microsoft Serialized	d Certificate Store (.SS	T)		

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:

File Action View	Help					
G Services (Local)	Services (Local)	·				-
	Central Print Services	Name *	Description	Status	Startup Type	Lo
		Adobe Acrobat Update Serv	Adobe Acro	Running	Automatic	Lo
	Stop the service	App Readiness	Gets apps re-		Manual	Lo
	Restart the service	Application Experience	Processes a		Manual (Trig_	Lo
	and the second se	Application Identity	Determines		Manual (Trig	Lo
	Description:	Application Information	Facilitates t		Manual (Trig_	Lo
	Apache Tomcat 8.5.11 Server -	Application Layer Gateway	Provides su	Manual	Lo	
	http://tomcat.apache.org/	Application Management	Processes in	Running	Manual	Lo
		AppX Deployment Service (Provides inf		Manual	Lo
		Reckground Intelligent Tran	Transfers fil	Running	Manual	Lo
		Background Tasks Infrastru	Windows in	Running	Automatic	Lo
		Q Base Filtering Engine	The Base Fil_	Running	Automatic	Lo
		G Bonjour Service	Enables har	Running	Automatic	
		Q Central Print Services	Apache To	Running	Automatic	N
		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	10000000000	Disabled	Lo
		Credential Manager	Provides se		Manual	Lo
		Cryptographic Services	Provides thr	Running	Automatic	N
		C DCOM Server Process Laun	The DCOM	Running	Automatic	Lo
	Extended Standard /		- 200			den de

- 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:

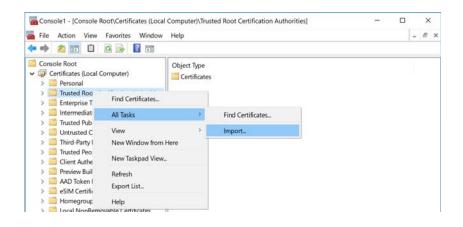
- 1. Open the Microsoft Management Console:
 - a) On your keyboard, press the Windows key + R (Run). The Run dialog appears.

	Run
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	This task will be created with administrative privileges.
	OK Cancel Browse

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.

 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.

Filet	o Import			
	Specify the file you w	ant to import.		
	File name:			
				Browse
	Note: More than one	e certificate can be stored i	n a single file in the followin	g formats:
	Personal Informat	tion Exchange- PKCS #12	(.PFX,.P12)	
	Cryptographic Me	ssage Syntax Standard- Pl	<cs #7="" (.p7b)<="" certificates="" td=""><td></td></cs>	
	Microsoft Serialize	d 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.

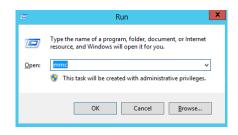


Adding the Certificates Snap-in to the Microsoft Management Console

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.



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.

6				Console1 - [Console Root]
🚡 File 🗛	tion View Favorit	es Window	Help	
Nev			Ctrl+N	
Ор	n		Ctrl+0	e
Sav			Ctrl+S	There are no items to show in this view
Sav	As			There are no items to show in this view
Ado	/Remove Snap-in		Ctrl+M	
Opt	ons			-
10	Windows\\devmgn	nt.msc		
2 C	\diskmgr	mt.msc		
3 0	Windows\\compm	gmt.msc		
Exit				-

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

vailable snap-ins: Snap-in	Vendor	LA.	Selected snap-ins:	Edit Extensions
- ActiveX Control	Microsoft Cor	Ê	Consule House	COR Extensions
Authorization Manager				Remove
Certificates	Microsoft Cor	_		-
Component Services	Microsoft Cor	=		Move Up
Computer Managem	Microsoft Cor			Prove up
Device Manager	Microsoft Cor			Move Down
m [®] Disk Management	Microsoft and		Add >	
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
IP Security Monitor	Microsoft Cor			
5 IP Security Policy M	Microsoft Cor			
Link to Web Address	Microsoft Cor			Advanced
A Local Backup	Mcrosoft Cor	~		Advanced
escription:				

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**.

Certificates snap-in		
This snap-in will always manage certificates for		
O My user account		
O 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 the computer you want this snap-in	n to manage.		
This snap-in will always manage:			
Local computer: (the computer this	console is running on)		
Another computer:		Browse	
	and the second state of th		
Allow the selected computer to be only applies if you save the console		n the command line. Th	s
		n the command line. Th	S
		n the command line. Th	s
		n the command line. Th	S
		n the command line. Th	S
		n the command line. Th	5
		n the command line. Th	S

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

Trademarks and service marks

The following are trademarks or registered trademarks of PrinterOn Inc. in Canada and other countries:

PrinterOn®, PrintAnywhere®, Print Simply Anywhere®, PrintWhere®, PRINTSPOTS®, the PrinterOn Logo, the PrinterOn Symbol, PrintConnect[™], Secure Release Anywhere[™], and PrintValet[™] are trademarks and/or registered trademarks of PrinterOn.

The following are trademarks or registered trademarks of other companies:

Windows, Internet Explorer, Microsoft Word, Microsoft Excel, Microsoft PowerPoint, and Microsoft Visio are trademarks or registered trademarks of Microsoft Corporation.

iPad, iPhone, AirPrint, and macOS are trademarks or registered trademarks of Apple.

iOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple under license.

Android, Chrome OS, and Chromebook are trademarks or registered trademarks of Google Inc.

BlackBerry is a registered trademark of BlackBerry, Ltd.

Other brands and their products are trademarks or registered trademarks of their respective holders.

Copyright notice

[©] Copyright 2018 by PrinterOn Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopy, recording, or otherwise, without the prior written permission of PrinterOn Inc.

Disclaimer:

PrinterOn Inc. makes no warranty with respect to the adequacy of this documentation, programs, or hardware, which it describes for any particular purpose, or with respect to the adequacy to produce any particular result. In no event shall PrinterOn Inc. be held liable for special, direct, indirect, or consequential damages, losses, costs, charges, claims, demands, or claim for lost profits, fees, or expenses of any nature or kind.

Version 4.1 | July 23, 2018