

WLAN Certificate Management in Printer Profile Manager Enterprise

Example Setup of the Automatic Printer Certificate Renewal Feature

Applies to Printer Profile Manager Enterprise version 3.1.x and later



The purpose of this whitepaper is to establish a "real world" example of a company with several locations facing common challenges when setting up wireless security certificates in Printer Profile Manager Enterprise (PPME). (This also assumes that all the printers targeted for security certificates are running Link-OS v6.0 or later.) Let's walk you through the company details and setting up the security certificates.

The fictional company, BC Company, has two stores, and each has their own unique network and time zone. Store 1 is in the Eastern time zone, while Store 2 is in the Pacific time zone. Both stores are remotely managed from a third HQ location.

Each store runs a similar wireless network with WPA2. However, Store 1 uses an RSA-2048 based certificate, and Store 2 uses a SECP512R1 ECDSA based certificate. Both stores' certificates use a SHA-256 digest.

To avoid store working and inventory hours, certificate provisioning should only occur between 1AM and 4AM local store time.

The certificate signing server used by BC Company is a Microsoft (MS) Active Directory Certificate Services server with NDES enabled. Additionally, the server is configured to auto-sign certificate requests. This is important as the provisioning window is outside normal business hours, so manual approval would prevent certificate provisioning from occurring during the desired time.

Finally, the signing server is configured to sign certificates for 30 days. To allow the stores time to update their mobile printers, the certificate update window is seven days prior to certificate expiration and is checked daily.



CA Server Setup

Objectives

Within this section, you will:

- Set up your CA Server
- Add specific CA details



Checklist



- Туре
- CA Server Full URL
- Polling Timeout (minutes and seconds)
- CA Server Description
- Challenge Type
- Challenge Password
- Username
 - User Password
- CA Certificate (if you have a saved local copy)
 - Certificate Password



CA Server Information

In our scenario, we are using the following information:

- Type: Microsoft ADCS NDES 2019
- CA Server Full URL: https://ndes.bccompany.com/certsrv/mscep_admin/mscep.dll
- Polling Timeout (seconds): 120
- CA Server Description: BC Company CA Authority
- Challenge Type: Dynamic BC Company's CA generates a new password per signing request
- **Challenge Password**: N/A as our Challenge Type is dynamic, in static configurations this would be used
- Username: store_signing
- Password: Bz93CLdk1!ks
- Server Certificate, Certificate Password: N/A for BCCompany, but could be used in certain CA configurations

Procedure to Set Up a CA Server

1. To create a CA server, in the top menu of PPME, select **Certificate Authorities** from the Certificates tab.



2. From the Certificate Authority landing page, click Add Certificate Authority Server.

ৠ•• ZEBRA	PRINTERS	PROFILES	NETWORKS	CERTIFICATES -	PROVISIONING	TAGS	RESOURCES		I admin ▼
Certificat History	e Author	ities o						Sort by Description: Ascending	٩

3. In the configuration page, enter the information outlined above:

Enter the CA Server full URL. For this scenario, the CA Server name is: https://ndes.bccompany.com/certsrv/mscep_admin/mscep.dll

4. The **Polling Timeout** is set to 2 minutes or 120 seconds.

PPME needs to check with the signing server to see if the certificate has been signed. Two minutes has been selected in our case to be often enough to update the certificate quickly, but with enough time between requests to prevent overloading the CA server. This value should be selected in conjunction with your security team to ensure proper function with your CA server.



5. Description is set to "BC Company CA Authority"

Our server requires an authorization certificate in order to process a signing request. If your server requires an authorization certificate, you may upload it using the Server Certificate field. This is not needed in all scenarios, but the IT department of BC Company requires this in order to increase the security of the system.

6. **Username** and **Password** are set to match the IT-provided account for automated signing purposes, in this case: store_signing:Bz93CLdk1!ks

्रीः . ZEBRA				CERTIFICATES -	PROVISIONING					0	• . •	• •	•	TOTAL 0	ø	(2) ac	
🔅 Certificate Authority Configuration																	
Туре																	
Microsoft ADCS 1	NDES 2019	\$															
URL									Polling Timeout (seconds)								
https://ndes.bcc	ompany.com/cer	tsrv/mscep_admi	in/mscep.dll				[9	120								
Description																	
BC Company CA	A Authority																
Challenge Type Dynamic																	
Challenge Passwo	ord																
Username							Password										
store_signing																٩	۲
Server Certificate							Certificate Password										
N/A						+	Set Certificate Password									٩	۲
Undo														[Cancel	S	Save

7. Click Save.

During the save process, PPME will attempt to connect to the CA server using the configuration you provided. The configuration will not save until the configuration works with the CA server.

You now have a CA server configured, now we need to setup a "Certificate Management Item" for our two stores.



Set Up Certificate Management Items

Objectives

Within this section, you will:

- Set up Certificate Management Items (CMI) for Store 1 and Store 2
- Add specific CA details



Checklist



- Server Address
- Challenge Password for Signing Server
- Message Digest
- Encryption Algorithm (and Key Size/Curve)
 - Update Certificates (Grace Period)
- Common Name of the printer
 - Organization
 - Organizational Unit
- Email Address
 - City
 - State
- Country
- Alternative Name
- Name of the CMI
 - Description of the CMI



Procedure to Create a Certificate Management Item (CMI) for Store 1

1. To create a CMI, under the "Certificates" tab, select **Certificate Management Items**.

刹 ぃ.ZEBRA	PRINTERS	PROFILES	NETWORKS	CERTIFICATES -	PROVISIONING	TAGS	RESOURCES	♥ ▲ ● TOTAL 0 0 0 0 ● ● ■
Selections No tags or filters set	elected		Prin	Certificate Authorit Certificate Manage	ies ment Items			

2. In the landing page, click Create Item.



3. Now you will see a list of all the information you will need to create a CMI, feel free to click the "Do not show this next time" checkbox at the bottom if you don't want to see it again. Click **Next**.

Create a Certificate Management Item

Befo You w	re You Begin 🗿
1	Challenge Password for CA Server
2	Message Digest Type for Certificate
3	Encryption Algorithm (and Key Size/Curve) for Certificate
4	Number of Days Before Certificate Expiration to Renew
5	Certificate Name Format for Managed Device
6	Certificate Information Name of Organization Organization Unit Email Address City and State/Province/Region Country Alternate Name for Certificate
🛛 Do r	iot show this next time

Previous Next Cancel



- 4. For Store 1, we are using the following configuration:
 - a. Server: CA server configured in the previous section
 - b. Message Digest: SHA-256
 - c. Encryption Algorithm: RSA (2048)
 - d. Update Certificates: 7 Days Before Expiring

For this scenario, there is only one CA server set up, signing.bccompany.com, but if your configuration has multiple servers, be sure to select the appropriate server for your specific purpose.

- 5. The message digest and encryption algorithm must match the configuration of the printer's network.
- 6. Finally, the **Update Certificates** sets the grace period for the certificate. Select the number of days for the grace period. The grace period is the number of days <u>before</u> the certificate expires during which the new certificate will be requested, signed, and sent to your printer.

For this scenario, we need to be sure to balance the server configuration, certificate configuration, and device usage. The BC Company's signing server is configured to allow certificate re-issuance at 50% of the certificate's life span. The certificates for our networks last 30 days.

For BC Company's scenario, certificates won't be renewed if they are less than 15 days old. Because we can't guarantee that all devices will be powered on for any specific day, we have selected a range of 7 days for the reissuance window. This minimizes the possibility of a device not being updated, while still conforming to the configuration allowed by the CA server and device network.

Create a Certificate Management Item		
Certificate Settings		
elect the required settings, such as encryption algorithm, key size, and message digest.		
Server		
BC Company CA Authority - https://ndes.bccompany.com/certsrv/mscep_admin/mscep.dll	*	
Nessage Digest		
SHA256 *		
Encryption Algorithm (and Key Size /		
RSA (2048)		
7 Days Before Expiring		
		Previous

7. Click Next.



- 8. Now, we need to setup the recipe used to generate the printer's individual certificate. BC Company's recipe looks like:
 - a. **Common Name**: MAC Address this is how the certificate is tied to the printer. In our case, we are using the printer's MAC address as the printer's uniquely identifiable information.
 - b. Organization: BC Company
 - c. Organizational Unit: Store 1
 - d. Email Address: admin@bccompany.com
 - e. City: New York
 - f. State: NY
 - g. Country: United States
 - h. Alternative Name: N/A we are not using this field in our configuration.

For this scenario, both stores use a SHA-256 message digest. The CSR message digest is configured by the network admins and must match their configuration. It is possible for different sites to have different message digest sizes.

Edit Certificate Management Item		
Certificate Information 0		
Please enter the required information for certificate creation.		
Common Name		
MAC Address	~	
Organization		
BC Company		
Organizational Unit		
Store 1		
Email Address		
admin@bccompany.com		
City		
New York		
State		
NY		
Country		
United States	~	
Alternative Name		
Optional Information		
		Previous Next Cance

9. Click Next.



10. On the next page, you can review the configuration and give it a name and description. Be sure to provide enough information so you can tell what your configuration is if you need to come back to it in the future.

ime of Certificate Management Item	Poview Configuration
Store 1 Certificate	Type of Certificate
escription	WLAN
RSA 2048, 7 Days update grace period	Server BC Company CA Authority - https://ndes.bccompany.com/certsrv/mscep_admin/mscep.dll
	Common Name MAC_ADDRESS
	Message Digest SHA256
	Encryption Algorithm RSA (2048)
	Update Certificates 7 Days Before Explring
	Organization BC Company
	Organizational Unit Store 1
	City New York
	State NY
	Country US
	- Email Addrese



Procedure to Create a CMI for Store 2

- 1. For store 2, we need to create another CMI to manage its configuration. The configuration used is as follows:
 - a. Server: CA server configured in the previous section
 - b. Message Digest: SHA-256
 - c. Encryption Algorithm: SECP521R1
 - d. Update Certificates: 7 Days Before Expiring
 - e. **Common Name**: MAC Address this is how the certificate is tied to the printer. In our case, we are using the printer's MAC address as the printer's uniquely identifiable information.
 - f. **Organization**: BC Company
 - g. Organizational Unit: Store 2
 - h. Email Address: admin@bccompany.com
 - i. City: Los Angeles
 - j. State: CA
 - k. **Country**: United States
 - I. Alternative Name: N/A we are not using this field in our configuration
- 2. The steps to configure Store 2 are the same as Store 1. When complete, there will be two CMIs listed in the CMI landing page.

Certifie + Create Iter	cate Management	Sort by Name: Ascending	♦ Search	٩
2 Manage	sment Items Shown			
	9/17/2019 at 10:38:28 AM Store 1 Certificate - RSA 2048, 7 day update grace period Type: WILAN Algorithm: RSA (2048) Digest: SHA256			
	9/17/2019 at 10:37:45 AM Store 2 Certificate - SECP521R1, 7 day update grace period Type: WLAN Algorithm: ECDSA (SECP521R1) Digest: SHA256			



Set Up Tags

Objectives

Within this section, you will:

- Create Tags for Store 1 and Store 2
- Add specific Tag details



Checklist



List of tag names



Associated printers (to be tagged)

Method to identify printers (to be tagged) by store



Procedure to Add a Tag for Store 1

To identify the printers for each store, they need to be tagged appropriately. Tags are the primary mechanism PPME uses to identify groups of printers. Therefore, we will create two tags "Store 1" and "Store 2" which will indicate the store a printer is in. We will then manually apply the tag to each printer appropriately. Please note: You can have multiple tags assigned to a printer, so if you are using multiple CMIs, be sure to only have one CMI tag per printer.

1. From the Tags tab, click **+Add Tag**.

刹•• ZEBR/	PRINTERS	BATTERIES (BETA)	PROFILES	NETWORKS	CERTIFICATES	PROVISIONING	TAGS	RESOURCES	$ \begin{array}{c c} \bigcirc & \blacksquare & \blacktriangle \\ 1 & 0 & 1 & 5 & 7 \\ \end{array} $	🕲 admin 🕶
Tags	•									
+Add Tag									Search	۹ :
🕕 Tags S	hown									
A	There are no tags to display. Click here to create a new one.									

The Create a Tag dialog opens.

💊 Create a Tag	
Tag Name	
Tag Name	
Tag Description	
Tag Description	
	Cancel

2. Enter the Tag Name.

For this scenario, Store 1.



3. Enter the **Tag Description**, if desired.

For this scenario, BC Company store in New York.

💊 Create a Tag	
Tag Name	
Store1	
Tag Description	
Tag Description	
	Cancel

4. Click **Create** to add the tag.

Or, click **Cancel** to close the dialog and return to the Tags page.

ᢤ. ZEBRA	PRINTERS	BATTERIES (BETA)	PROFILES	NETWORKS	CERTIFICATES	PROVISIONING	TAGS	RESOURCES	5 TOTAL 7	🕲 admin 🕶
Tags @ +Add Teg									Search	٩
1 Tag Sho	wn									
=	7/2/2019, 11:10:31 Store1 Tagged Printers	AM								

5. Repeat steps 1-4 for each tag.

्री•• ZEBRA	PRINTERS	BATTERIES (BETA)	PROFILES	NETWORKS	CERTIFICATES	PROVISIONING	TAGS	RESOURCES	© 1	0	▲ 1 5) T	7	a	🗿 admin 🕶
Tags 🕢											[Search	1		۹
2 Tags Shown															
=	7/2/2019, 11:10:31 Store1 Tagged Printers	ам :0													
=	7/2/2019, 11:11:55 Store2 Tagged Printers	ам 0													



Procedure to Add a Tag for Store 2

- 1. From the Tags tab, click **+Add Tag**.
- 2. Enter the Tag Name.

For this scenario, Store 2.

3. Enter the **Tag Description**, if desired.

For this scenario, BC Company store in Los Angeles.

4. Click Create to add the tag.

Or, click **Cancel** to close the dialog and return to the Tags page.

Procedure to Tag a Printer

In our scenario, we know that Store 1 uses only ZT230s, while Store 2 uses ZD500s. This simplifies identifying our stores' printers, but your network configuration, site configuration, and printer models may not be as easy to identify. Some possible ways to identify printers at your different sites are:

- IP Address: Depending on each store's network configuration, the possible IP addresses assigned may be limited.
- Firmware version: If your sites differ in how they update the printer's firmware, it might be possible to identify each store through firmware versions.
- Location: If in your deployment process, you update each printer with the store's location, you could use the location to tag the printer.
- A previously created tag: It is possible that each printer is already tagged properly depending on your situation.
- Serial numbers: Search by your printer's serial number.

Fundamentally, you will need some way to identify which printers are in each store.



1. From the Tags tab, click on a tag.

The Tags Details page opens.

N) PROFILES NETWORKS CERTIFICATES	PROVISIONING TAGS RESOURCES	$ \bigcirc \left \begin{array}{c} \bullet \\ 1 \end{array} \right \left \begin{array}{c} \bullet \\ 0 \end{array} \right \left \begin{array}{c} \bullet \\ 5 \end{array} \right \left \begin{array}{c} TOTAL \\ T \end{array} \right \left \begin{array}{c} \bullet \\ \bullet \end{array} \right admin + 1 $
Associated Printers Queued Serial Numbers		•
Search		٩
A There are no printers associa	ted with this tag.	
	PROFILES NETWORKS CERTIFICATES Image: Second Printers Cueued Sensi Humbers Image: Second Sensi Humbers Image: Second Printers Image: Second Sensi Humbers Image: Second Sensi Humbers Image: Second Printers Image: Second Sensi Humbers Image: Second Sensi Humbers Image: Second Printers Image: Second Sensi Humbers Image: Second Sensi Humbers Image: Second Printers Image: Second Sensi Humbers Image: Second Sensi Humbers Image: Second Printers Image: Second Sensi Humbers Image: Second Sensi Humbers	PROFILES NETWORKS CERTIFICATES PROVISIONING TAGS RESOURCES Secondard Printers Current Serial Current Serial Current Serial Secondard There are no printers associated with this tag.

2. Click +Tag Printers.

The Apply Printer to Tag Store 1 page opens.

刹 . ZEBRA	PRINTERS B/	ATTERIES (BETA)	PROFILES	NETWORKS	CERTIFICATES	PROVISIONING	TAGS	RESOURCES						^{AL} 0	🕲 admin 🗸
🔒 Apply	Printers to Tag Store	e1													
Search									Q	0 Prir	nters Selected				
	Serial Number: 18J1346008	97 Model: ZT410-30	Odpi Firmware	V75.20.01Z IP A	ddress: 10.80.126.35				*	A	No printers hav	ve been selecte	d.		
O	C3J180400097 Serial Number: PS1200000	01 Model: ZC300-3	00dpi Firmwan	: V201.01.07P7378	IP Address: 10.80.4	.108									
-	52J133700091 Serial Number: 52J1337000	91 Model: 2T23D-20	3dpi Firmware	V72.20.18P46694	IP Address: 10.1.23.	21			I.						
9	50J154800085 Serial Number: 50J1548000	65 Model: ZD420-31	IOdpi Firmware	: V84.20.15P44743_I	DEV IP Address: 10	0.80.124.164			*						
														Cancel	Apply



3. Select the printer to tag.

For this scenario, we will enter ZT230 into the search bar and select all printers listed.

ᢤ. ZEBRA	PRINTERS BATTERIES (BETA) PROFILES NETWORKS CERTIFICATES PROVISIONING TAGS			$ \begin{array}{c c c c c c c c c c c c c c c c c c c $) 🕲 admin 🗸
🔒 Apply	Printers to Tag Store1				
Search		Q	1 Printer Selected	ł	
	Serial Number: 18/134600897 Model: Z1410-3000pi Firmware: V75 20.012 IP Address: 10.00.126.35	*	52J13370005 Serial Number: 5	91 52J133700091 Model: ZT230-203dpi	×
O	C3J180400097 Serial Number: PS120000001 Model: 2C300-300dpi Firmware: V201.01.07P7378 IP Address: 10.80.4.108		Firmware: V72.2	0.18P46694 IP Address: 10.1.23.21	
	52J133700091 Serial Number: 52/133700091 Model: ZT230-2036pi Firmware: V72.20.16P46894 IP Address: 10.1.23.21				
	50J154800085 Serial Number: S0/154800085 Model: ZD420-300dpi Firmware: V64.20.15P44743_DEV IP Address: 10.80.124.164	Ŧ			
				Ca	Incel Apply

4. Click **Apply** to tag the printer.

.ZEBRA PRINTERS BATTERIES (BETA)	PROFILES NETWORKS CERTIFICATES PROVISIONING TAGS RESOURCES	$ \begin{array}{c c c c c c c c c c c c c c c c c c c $	🕲 admin 🗸
N Tag	Associated Printers Cueued Serial Numbers Cueued Serial Numbers Cueued Serial Numbers Cueued Serial Numbers Select All Deselect All		-
Name	Search		٩
Description	52,J133700091 Serial Number: 52,J133700091 Model: 2T230 Firmware: \72.20.18P46664 IP Address: 10.1.23.21 Bowrt		
Creation Date			
07/02/2019 at 11:10:31 AM			

Repeat for Store 2 but use ZD500 as the search filter.



Set Up Provisioning Items

Objectives

Within this section, you will:

- Set up Provisioning Items for Store 1 and Store 2
- Add specific Provisioning details

1	~	—
I	4	—
I	4	-
I	✓	-

Checklist



Name of the CMI

	Na

Name of the Tag(s)

Desired schedule (frequency, days of the week, months of the year, exact date, or start/stop dates)

Number of days in the Grace Period (Before Certificate Expires)

Provisioning name



Provisioning Item Overview

A provisioning item controls when a printer's certificate is checked for expiration and updated, if needed. A few things to note about this process:

- Your CA server should be configured for automatic signing. If you require manual approval for each certificate signing request, there can be long time delays, which may prevent your printer from receiving an updated certificate before the previous one expires and drop the printer from the network.
- The overall process can be lengthy. There are interactions with the printer, and those interactions are lower priority than printing. So, if the certificate update period happens while the printer is under heavy load, the process won't continue until the printer is under a lower print load.
- If the printer is offline when the update check occurs, and it is determined that the printer needs a new certificate (printer certificate date information is cached in PPME), the next time the printer connects to PPME, the certificate will be updated immediately.

Procedure to Setup a Certificate Provisioning Item for Store 1

1. From the Provisioning tab, click **Create Item**.



2. For this scenario, select Printer Certificates and the Store 1 Certificate CMI.

Create a Provisioning Item	
Type of Provisioning	
C (
Printer Resources	
Printer Certificates	
Search	٩
Store 1 Certificate - RSA 2048, 7 day update grace period Type: WLAN Algorithm: RSA 2048 Digest: SH4256	
Store 2 Certificate - SECP521R1, 7 day update grace period Type: WLAN Algorithm: ECD54.6ECP521R1 Digest SH456	
Selected Certificate: Store 1 Certificate	Pervious Next Canod



3. Click **Next** to go to the next page.

Or, click **Cancel** to exit and return to the Provisioning page.

Or, click **Previous** to go back to the previous page.

4. Now select the "Store 1" tag.

्राः, ZEBRA					PROVISIONING							⊘ 0 0		
Create	🛗 Create a Provisioning Item													
	9/20/2019, 2:52:11 PM										Selected Tags With any of these tags With all of these	tags		
	Tagged Printers: 0										Store 1 0 ×			
•	9/20/2019, 2:52:17 PM Store 2 Tagged Printers: 0													
													Previous Next	Cancel

Notice the right pane. You may select With any of these tags or With all of these tags.

Note: In this example it doesn't matter, but it is a way to manage multiple tags. So, if you had "Selected Tags" for Store 1 and Store 2 set to "with any of these tags", the Provisioning Item would apply to printers marked with either tag or both tags. "With all of these tags" means the Provisioning Item would only apply to printers tagged with both Store 1 and Store 2.

5. Click **Next** to go to the next page.

Or, click **Cancel** to exit and return to the Provisioning page.

Or, click **Previous** to go back to the previous page.



6. The next fields are setting the schedule for provisioning the wireless certificates. Select the one(s) that creates the best schedule.

For this scenario:

- a. Select the **Frequency** from the dropdown menu. In our scenario, we will select "Repeat Daily".
- b. Select **On These Days** schedule. In our scenario, we will leave this blank, so the certificate update check runs every day.
- c. Select In These Months schedule. In our scenario, we will leave this blank.
- d. Enter $\mbox{On This Date}.$ In our scenario, we will leave this blank.
- e. Enter the Start Date/Time. We will set the start time to 1AM.
- f. Since this is for store 1 on the East coast, in the Time Zone box, select "New York".
- g. Enter the Stop Date/Time. In our scenario, we will leave this blank, so it never ends.

Create a Provision	ning item	
Frequency		-
Repeat Daily		•
On These Days Monday Tuesday	Wednesday 📄 Thursday 📄 Friday 🔲 Saturday 📄 Sunday	
🛛 Jan 🔲 Feb 🗌 Mar 📄	Apr May Jun Jul Aug Sep Oct Nov Dec	
On This Date		
Day of month (1-31)		
Start Date/Time		
	1:00am	
Stop Date/Time		
Time Zone		
New York		•
Use Local Time Zone		
Apply at 1:00 AM EDT (5:00 AM	M UTC) every day.	Next Cancel

7. Click **Next** to go to the next page to open the configuration confirmation page.

On this page, you can review the configuration and see the three upcoming dates and times that the provisioning item will check the certificate expiration.

- Or, click **Cancel** to exit and return to the Provisioning page.
- Or, click **Previous** to go back to the previous page.



8. Click **Finish** to go complete the setup.

Or, click **Cancel** to exit and return to the Provisioning page.

Or, click **Previous** to go back to the previous page.

Provis	isioning Items o		
+ Create Ite	Sort by Modifie	ed Date: Ascending v Search	Q
1 Item SI	Shown		
	September 30, 2019 3:39 PM Store 1 Certificate - Apply every day Status: Active Tagging Method: Any Next Occurrence: Tuesday, October 1, 2019 at 1:00 AM EDT (10/01/2019 at 5:00 AM UTC) Status: Active Tagging Method: Any Next Occurrence: Tuesday, October 1, 2019 at 1:00 AM EDT (10/01/2019 at 5:00 AM UTC)		

Procedure to Setup a Certificate Provisioning Item for Store 2

For Store 2, we follow the exact same process as for Store 1, but with the following modifications:

1. Select "Store 2 Certificate" certificate management item in step 2.

Create a Provisioning Item	
Type of Provisioning	
O (Printer Profile	
Printer Resources	
Printer Certificates	
Search	٩
Store 1 Certificate - RSA 2048, 7 day update grace period Type: WLVN Algorithm: RSA (2048) Digest: SH4256	
9/17/2019 at 193746 AM Store 2 Certificate - SECP521R1, 7 day update grace period Type: VULVI Algorithm: ECDSA (SECP521R1) Digest: SHA256	
Selected Certificate: Store 2 Certificate	Previous Next Cancel

2. Select "Store 2" tag in step 4.

Create a Provisioning Item	
9/20/2019, 252:11 PM	Selected Tags
Store 1 Tagged Printers: 0	With any or these tags with all or these tags
	Store 2 0 x
9/20/2019, 2:52:17 PM Store 2	
Tagged Printers: 0	
	Previous Next Cancel



3. Select "Los Angeles" for the Time Zone in step 6.

Create a Provisioning Item		
Frequency		*
Repeat Daily	•	
On These Days Monday Tuesday Wednesday Friday Saturday Sunday In These Months		
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec		Ľ
On This Date		
Day of month (1-31)		
Start Date/Time 1:00am		l
Stop Date/Time		l
Time Zone		
Los Angeles		1
Use Local Time Zone		
Apply at 1.00 AM PDT (8:00 AM UTC) every day.	Cancel)

4. The confirmation page for Store 2 is:

Create a Provisioning Item	
Confirmation	
Selected Certificate	
Selected Schedule © Apply at 1:00 AM PDT (8:00 AM UTC) every day.	
Next 3 Occurrences > Tursday, October 1, 2019 at 1:00 AM PDT (10/01/2019 at 8:00 AM UTC) > Wednesday, October 2, 2019 at 1:00 AM PDT (10/02/2019 at 8:00 AM UTC) > Thursday, October 3, 2019 at 1:00 AM PDT (10/03/2019 at 8:00 AM UTC)	
Selected Tags (printers tagged by any of these)	
Provisioning Name	
Store 2 Certificate - Apply every day	
	Previous Finish Cancel

We now have one Provisioning Item for each store and our certificate management process is complete.

At this point, PPME will automatically check and update, if necessary, all printer certificates at 1AM (local store time) every day.

Provis	ioning Items		(aut	
2 Items S	mi mi saupenz∧ni (⊭rkesameza) shown	Son by Modified Date: Ascending	Search	Q
	September 30, 2019 3:39 PM Store 1 Certificate - Apply every day Status: Active Tagging Method: Any Next Occurrence: Tuesday, October 1, 2019 at 1:00 AM EDT (10/01/2019 at 5:00 AM UTC) Status 1			
	September 30, 2019 3:54 PM Store 2 Certificate - Apply every day Status: Active Tagging Method: Any Next Occurrence: Tuesday, October 1, 2019 at 1:00 AM PDT (10/01/2019 at 8:00 AM UTC) Status 2			

Table 1: Scenario Summary

		Charad	Chara 2
	HQ Server	Store	Store 2
Wireless Network	MS Active Directory	WPA2	WPA2
	Certificate w/NDES		
Cryptographic Key		RSA-2048	SECP512R1 ECDSA
Message Digest		SHA-256	SHA-256
Time Zone	Iceland (UTC)	Eastern	Pacific
Certificate Duration	30 days	30 days	30 days
Certificate Provisioning		01:00-04:00 EST	01:00-04:00 PST
window			
Grace Period		7 days prior to cert.	7 days prior to cert.
		expiration	expiration
Cert. Management Item			

	HQ Server
Wireless Network	MS Active Directory
	Certificate w/NDES
Time Zone	Iceland (UTC)
Certificate Duration	30 days
Address	CA.BCcompany.com
Password	****
Server Certificate	CABCcompany.p12



Glossary

- Auto-sign: NDES & SCEP can be configured to automatically sign the certificate signing request
- **Certificate:** consists of public information identifying the device and a set of public and private keys used for encrypted communication.
- Certificate Signing Request (CSR): In public key infrastructure (PKI) systems, a certificate signing request (also certification request) is a message sent from a user to a certificate authority in order to apply for a digital identity certificate. It usually contains the public key for which the certificate should be issued, identifying information (such as a domain name), and integrity protection (e.g., a digital signature).
- **CMI (Certificate Management Item):** the system in Printer Profile Manager Enterprise that controls the distribution of a certificate to printers on a user-defined schedule
- NDES (Network Device Enrollment Service): a security feature in Windows operating versions. NDES provides and manages certificates used to authenticate traffic and implement secure network communication with devices that might not otherwise possess valid domain credentials.
- **Provisioning event:** the system in Printer Profile Manager Enterprise that controls the distribution of Profiles or Certificates to printers on a user-defined schedule (FROM PPME Help)
- SCEP (Simple Certificate Enrollment Protocol): a standard certificate signing protocol implemented by many certificate authority servers.



Checklist

Туре
CA Server Full URL
Polling Timeout (minutes and seconds)
CA Server Description
Challenge Type
Challenge Password
Username
User Password
CA Certificate (if you have a saved local copy)
Certificate Password
Server Address
Challenge Password for Signing Server
Message Digest
Encryption Algorithm (and Key Size/Curve)
Update Certificates (Grace Period)
Common Name of the printer
Organization
Organizational Unit
Email Address
City
State
Country
Alternative Name
Name of the CMI



