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

P1124537-01EN Rev. A

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

- [ ] Type
- [ ] 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

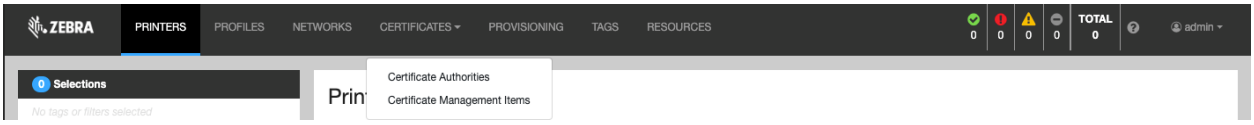
CA Server Information

In our scenario, we are using the following information:

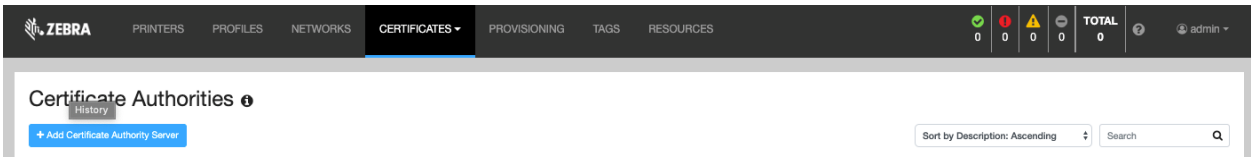
- **Type**: Microsoft ADCS NDES 2019
- **CA Server Full URL**: https://ndes.bccompany.com/certsrv/mscep_admin/mscep.dll
- Polling Timeout (seconds): 120
- **CA Server Description**: BC Company CA Authority
- **Challenge Type**: Dynamic – BC Company's CA generates a new password per signing request
- **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**.



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

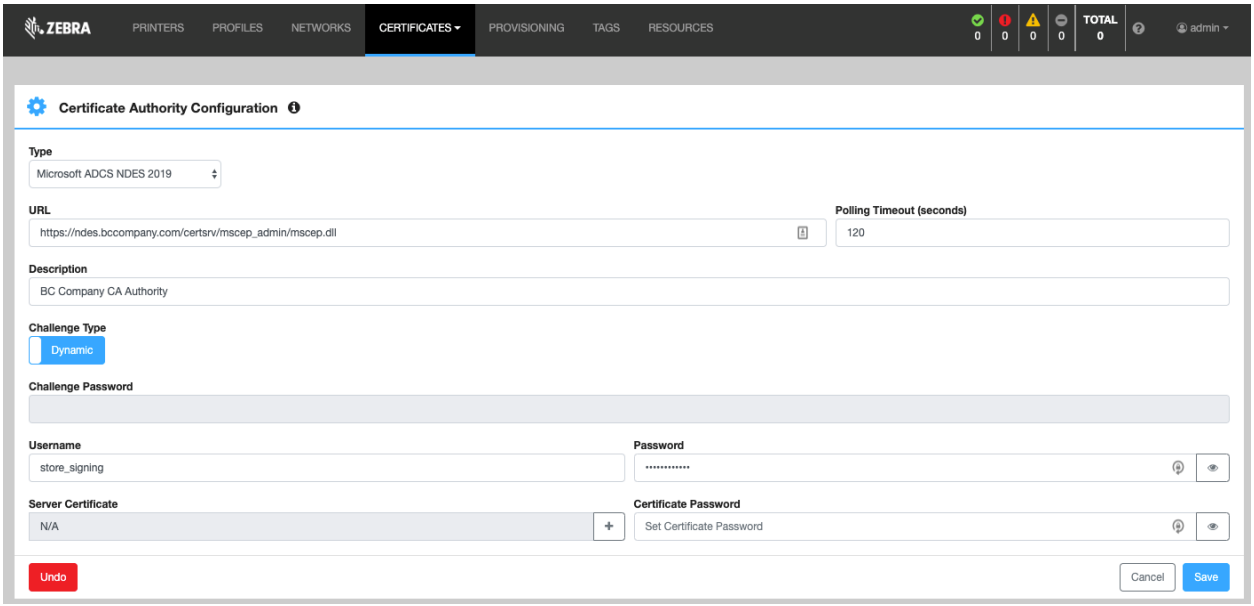
4. The **Polling Timeout** is set to 2 minutes or 120 seconds.

   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



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:

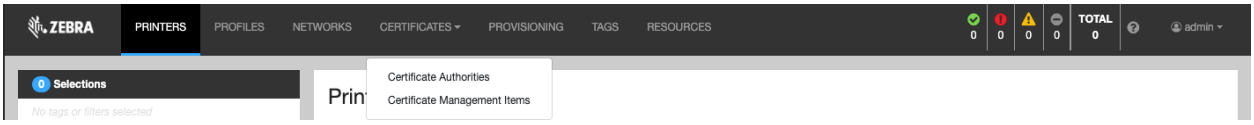
- Set up Certificate Management Items (CMI) for Store 1 and Store 2
- Add specific CA details

Checklist

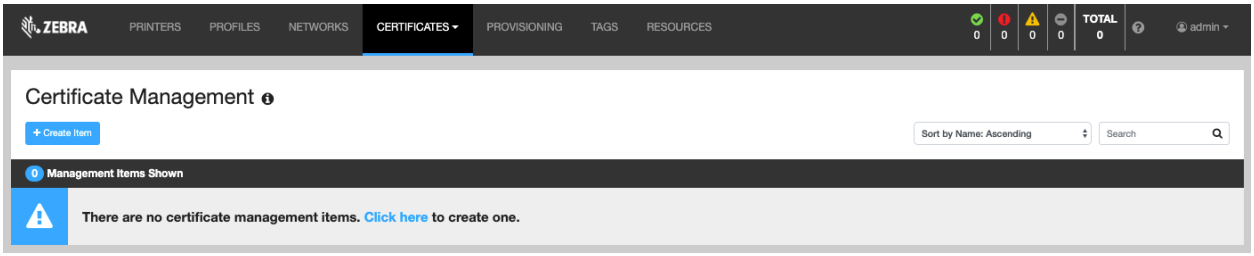
- [ ] Server Address
- [ ] Challenge Password for Signing Server
- [ ] Message Digest
- [ ] Encryption Algorithm (and Key Size/Curve)
- [ ] Update Certificates (Grace Period)
- [ ] Common Name of the printer
- [ ] Organization
- [ ] Organizational Unit
- [ ] Email Address
- [ ] City
- [ ] State
- [ ]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

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

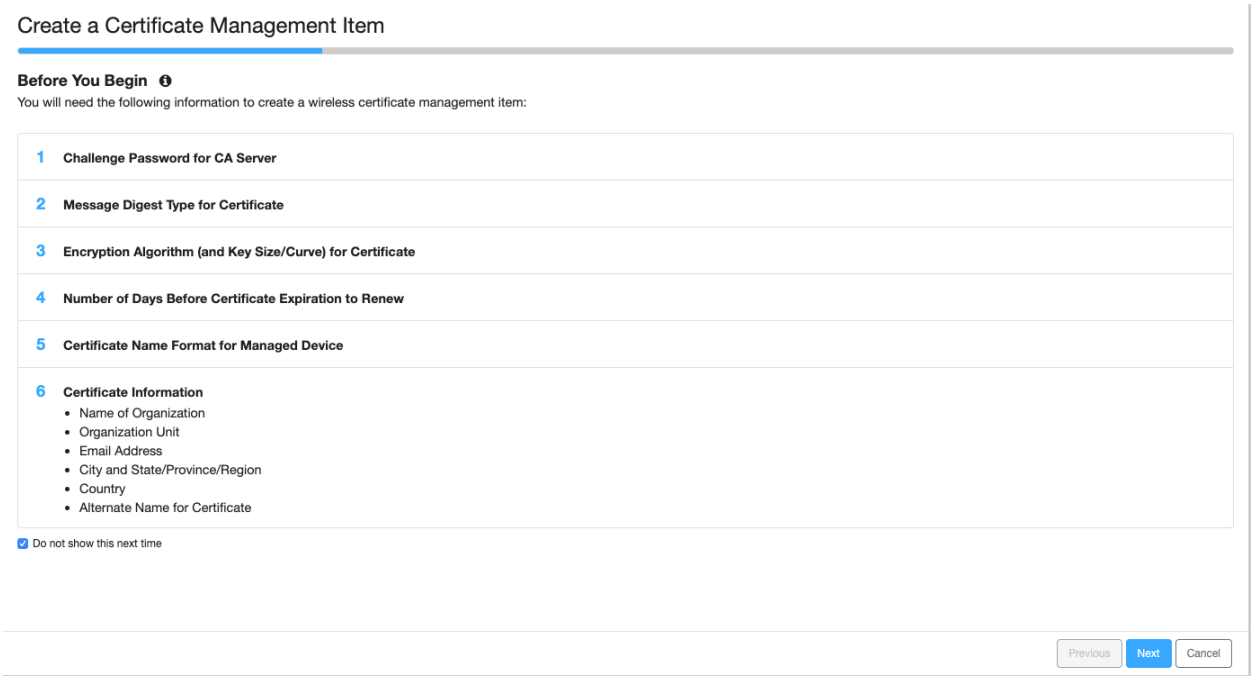
1. To create a CMI, under the “Certificates” tab, select **Certificate Management Items**.



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**.



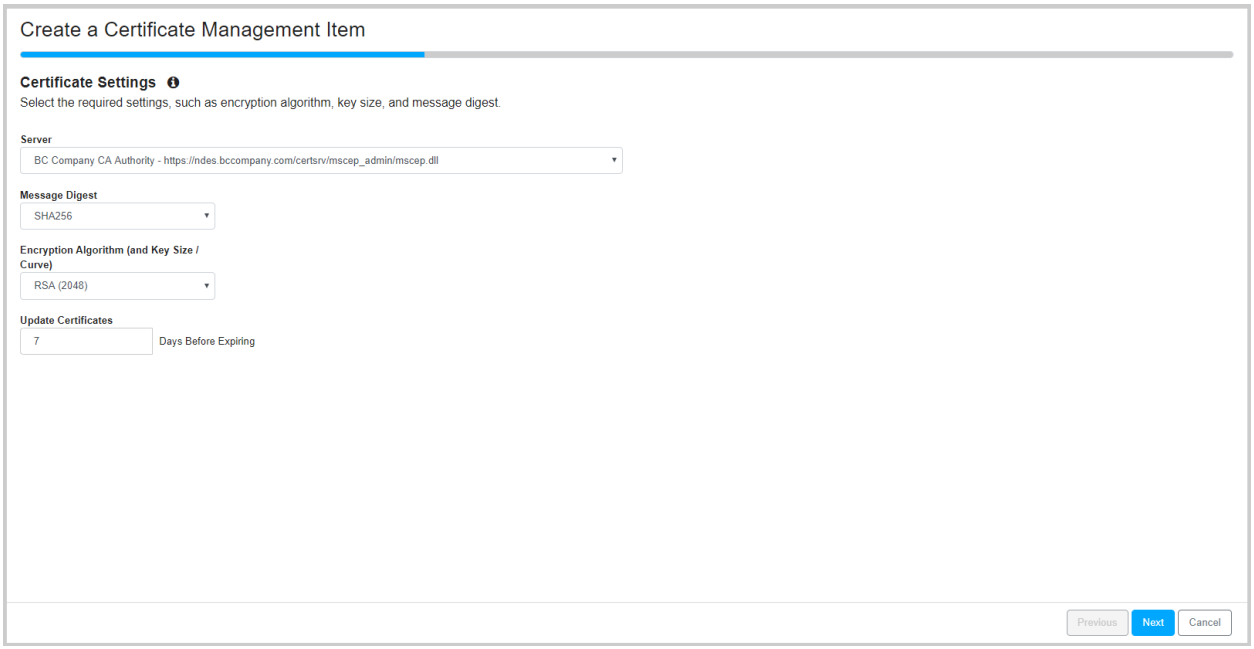
4. For Store 1, we are using the following configuration:
    a. **Server**: CA server configured in the previous section
    b. Message Digest: SHA-256
    c. Encryption Algorithm: RSA (2048)
    d. **Update Certificates**: 7 Days Before Expiring

    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 before 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.

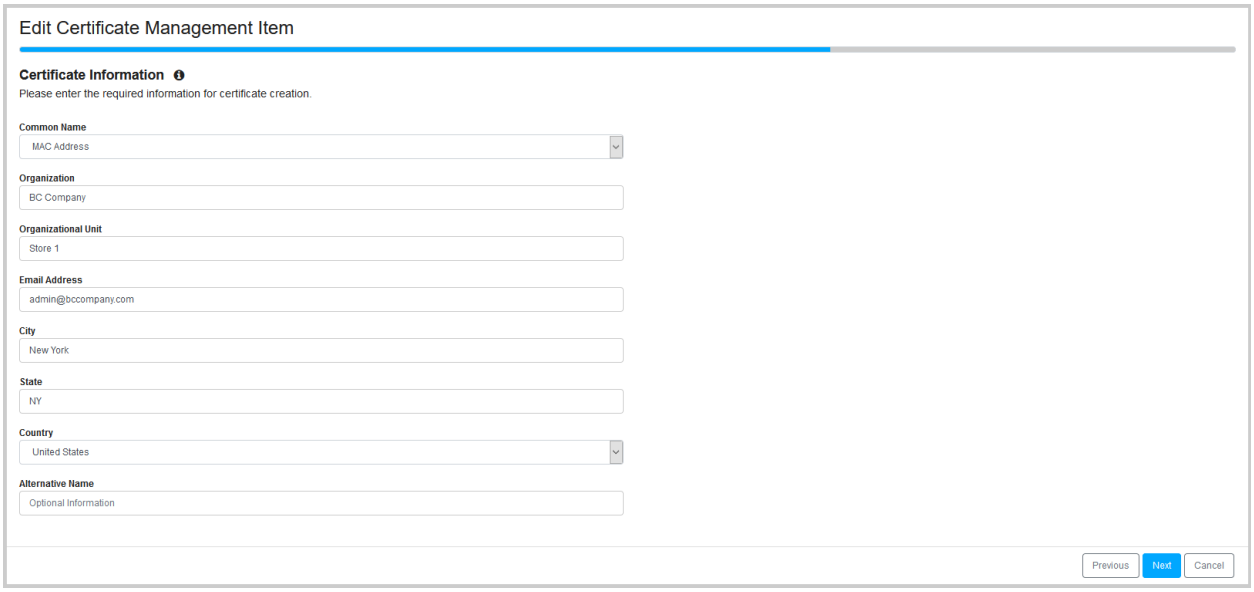
    For BC Company's scenario, certificates won't be renewed if they are less than 15 days old. Because we can't guarantee that all devices will be powered on for any specific day, we have selected a range of 7 days for the reissuance window. This minimizes the possibility of a device not being updated,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



7. Click **Next**.

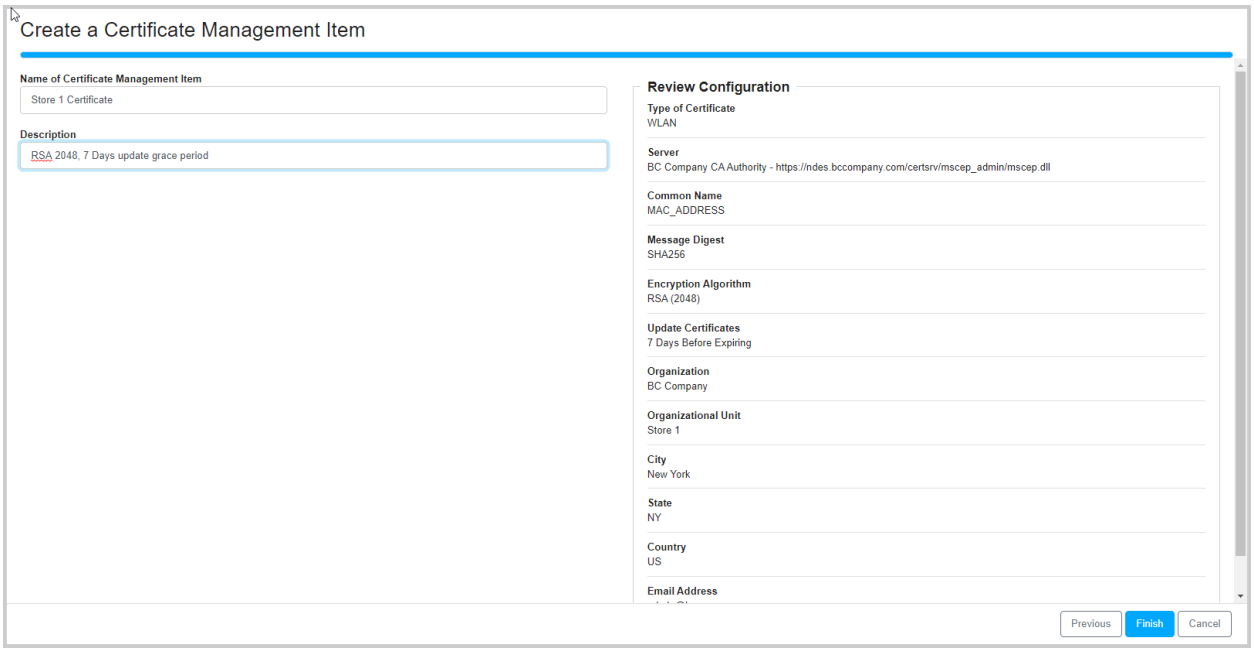
8. Now, we need to setup the recipe used to generate the printer's individual certificate. BC Company's recipe looks like:
    a. **Common Name**: MAC Address – this is how the certificate is tied to the printer. In our case, we are using the printer's MAC address as the printer's uniquely identifiable 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.



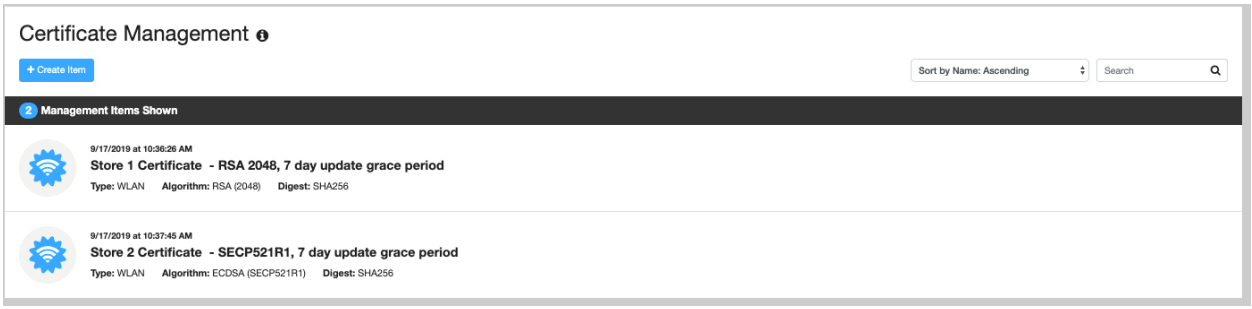
9. Click **Next**.

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.



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
    l. **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.



Set Up Tags

Objectives

Within this section, you will:

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

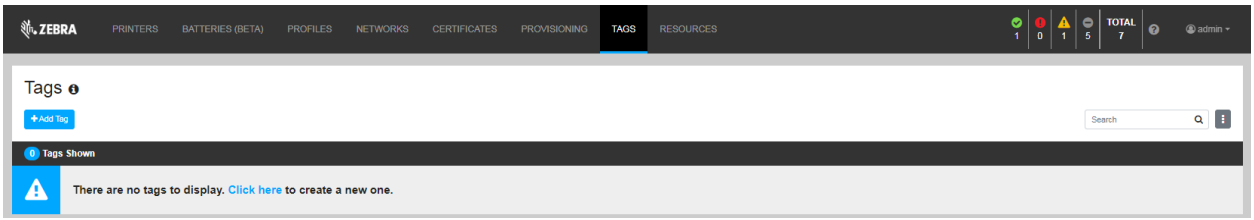
Checklist

- [ ] List of tag names
- [ ] Associated printers (to be tagged)
- [ ] Method to identify printers (to be tagged) by store

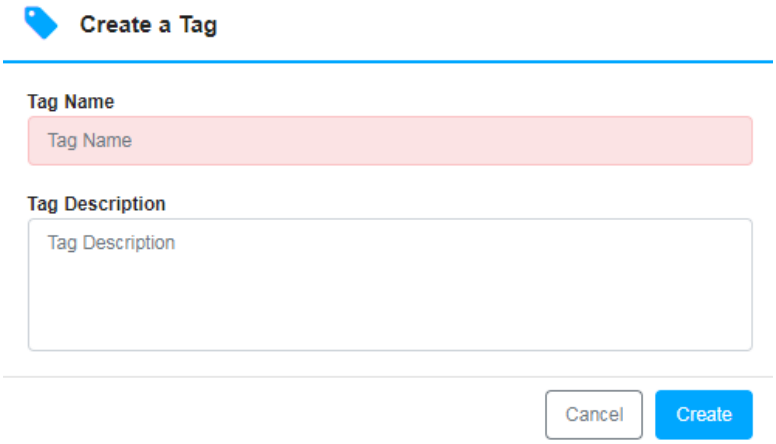
Procedure to Add a Tag for Store 1

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**.



The Create a Tag dialog opens.

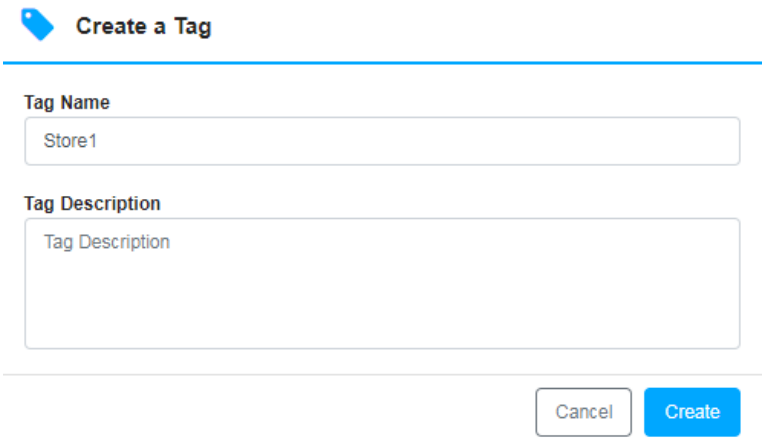


2. Enter the **Tag Name**.

   For this scenario, Store 1.

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

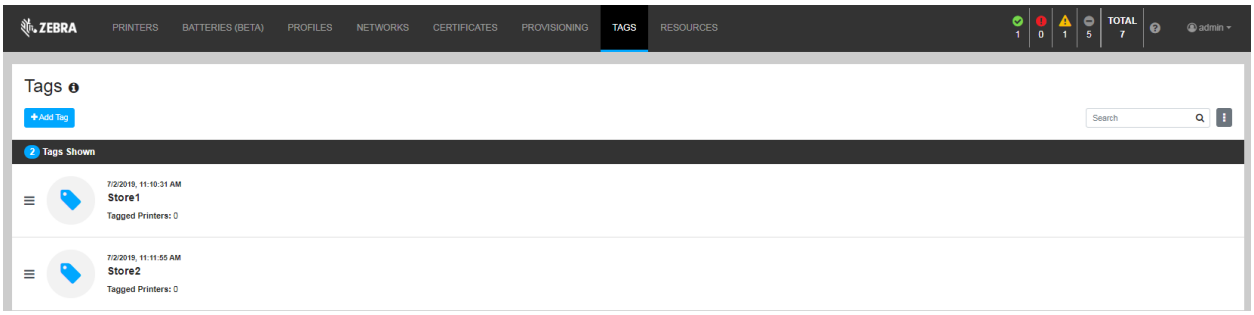
   For this scenario, BC Company store in New York.



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

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

5. Repeat steps 1-4 for each tag.



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

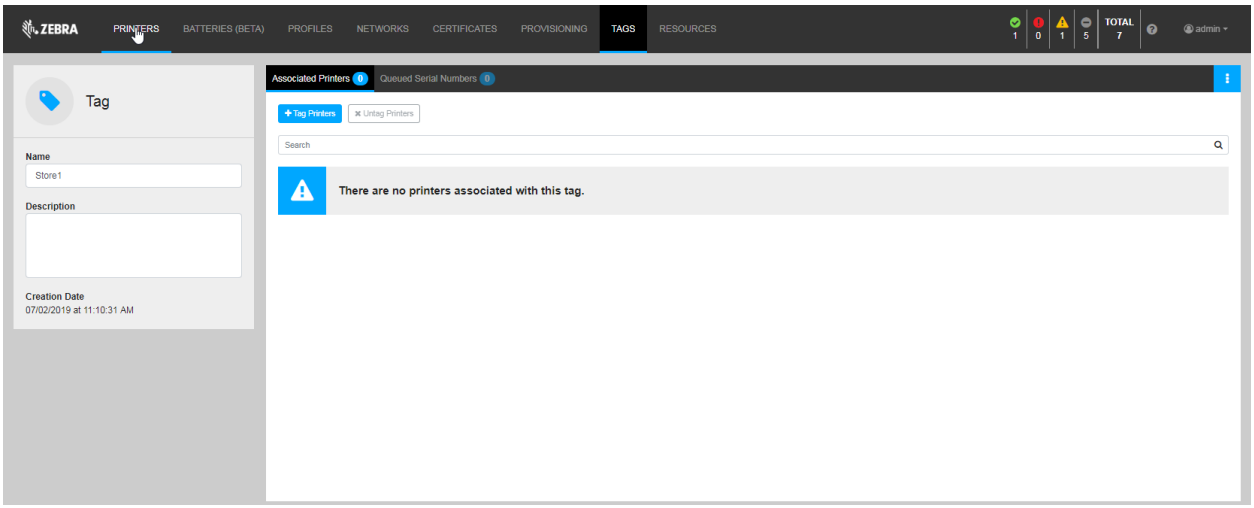
In our scenario, we know that Store 1 uses only ZT230s, while Store 2 uses ZD500s. This simplifies identifying our stores' printers, but your network configuration, site configuration, and printer models may not be as easy to identify. Some possible ways to identify printers at your different sites are:

- 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.

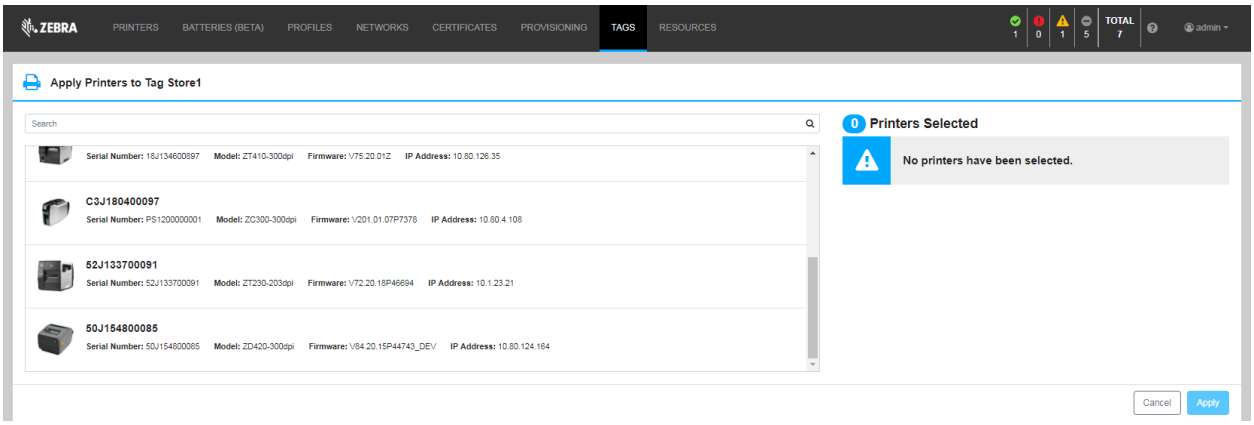
1. From the Tags tab, click on a tag.

   The Tags Details page opens.



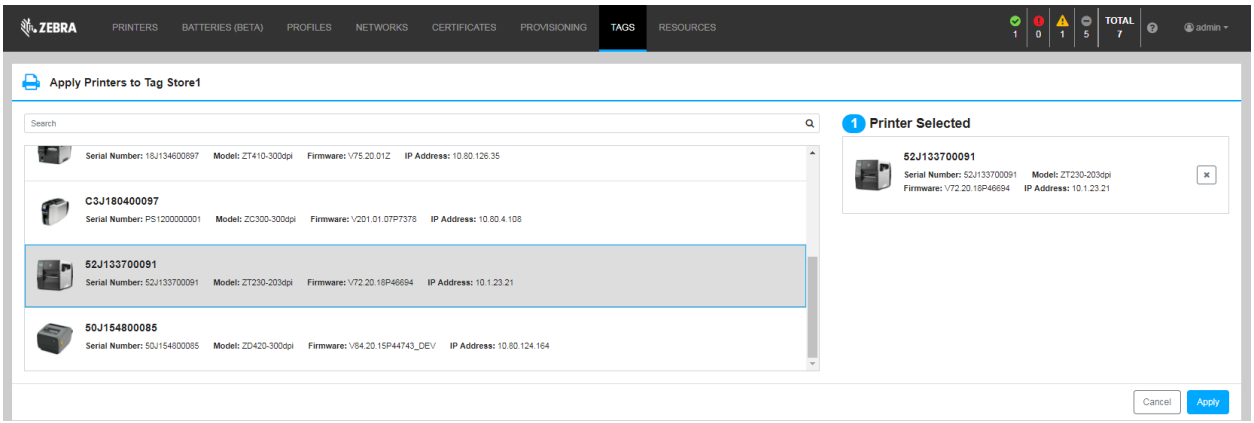
2. Click **+Tag Printers**.

   The Apply Printer to Tag Store 1 page opens.

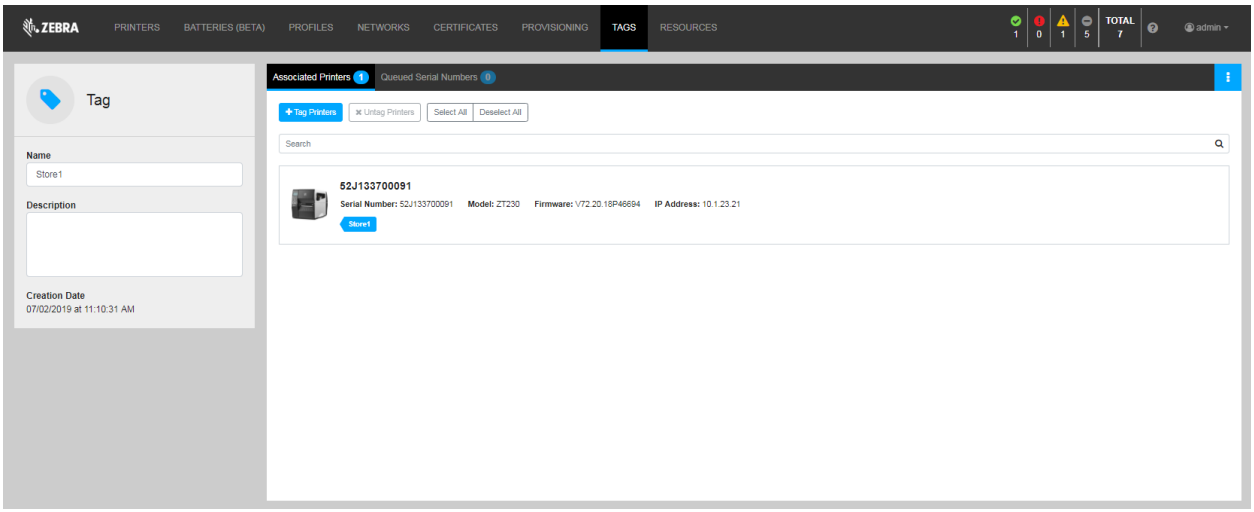


3. Select the printer to tag.

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



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



   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

Checklist

- [ ] Name of the CMI
- [ ] 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

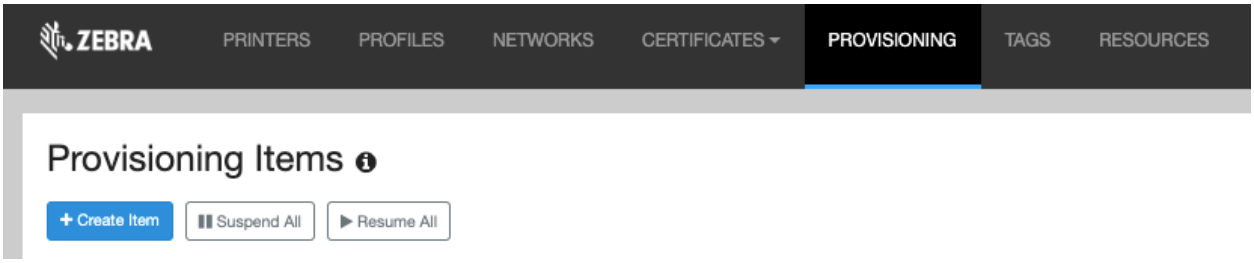
Provisioning Item Overview

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:

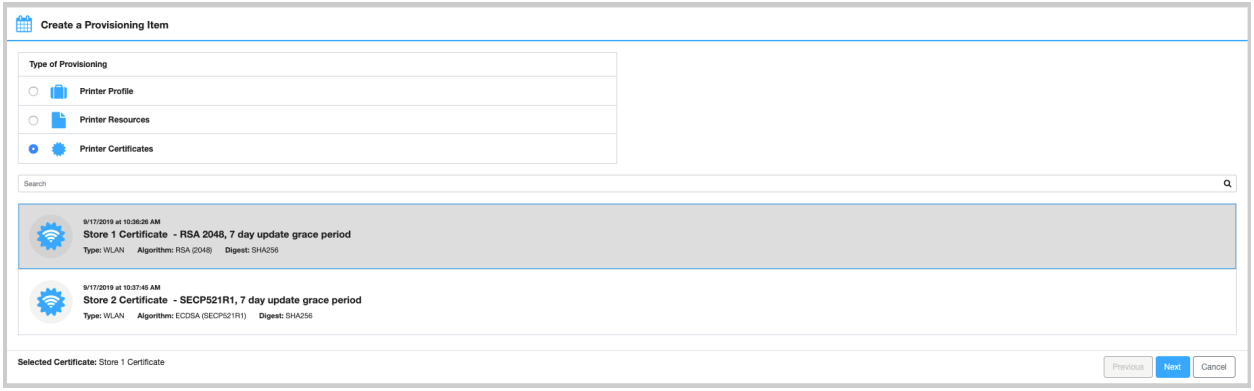
- Your CA server should be configured for automatic signing. If you require manual approval for each certificate signing request, there can be long time delays, which may prevent your printer from receiving an updated certificate before the previous one expires and drop the printer from the network.
- 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.

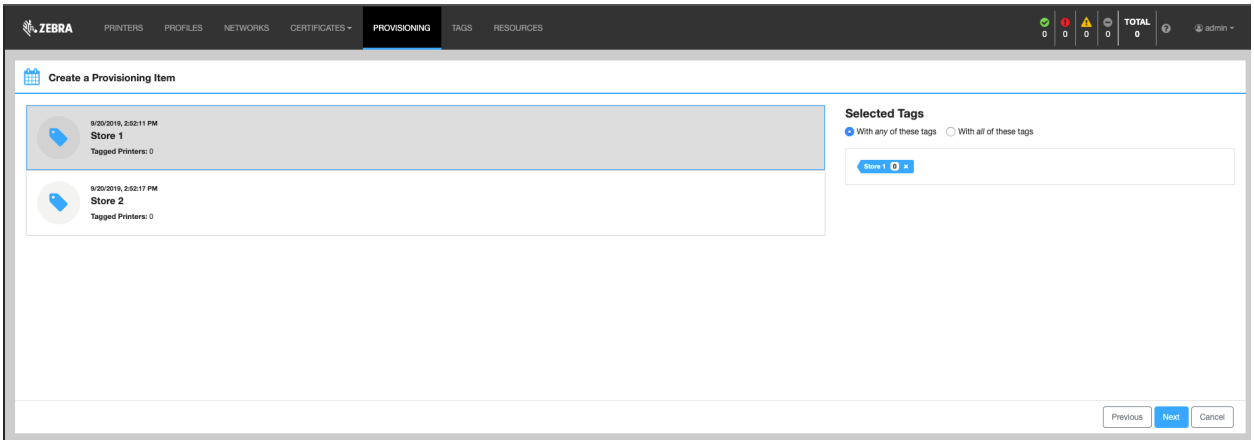


3. Click **Next** to go to the next page.

   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.



   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.

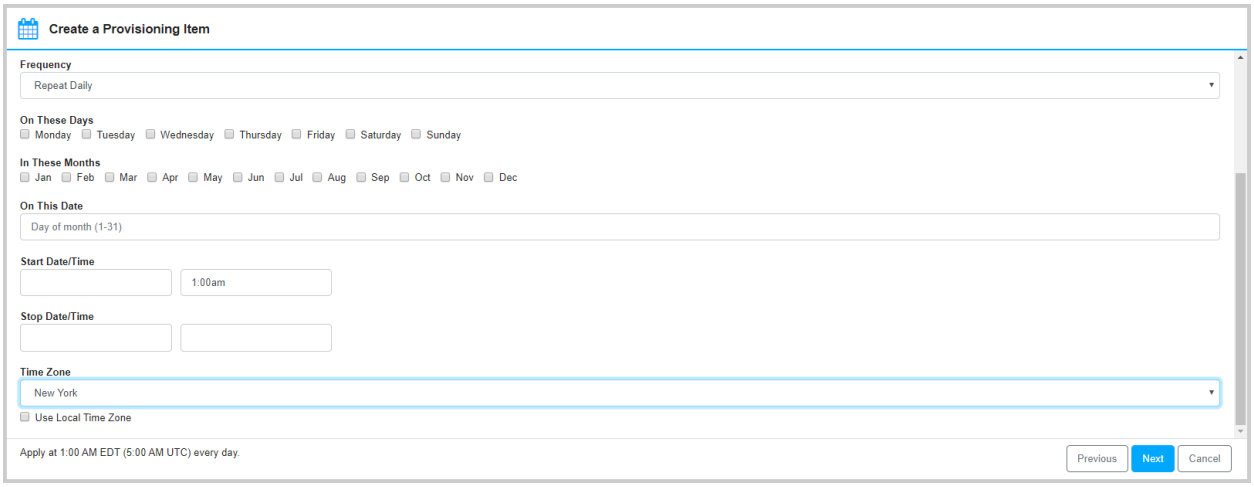
   Or, click **Cancel** to exit and return to the Provisioning page.

   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 **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.



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.

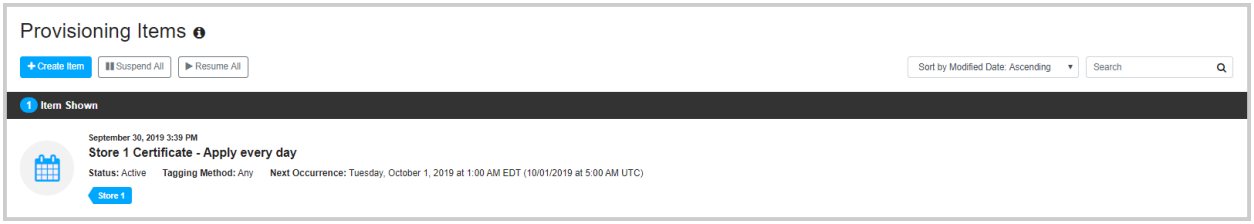
   Or, click **Cancel** to exit and return to the Provisioning page.

   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.

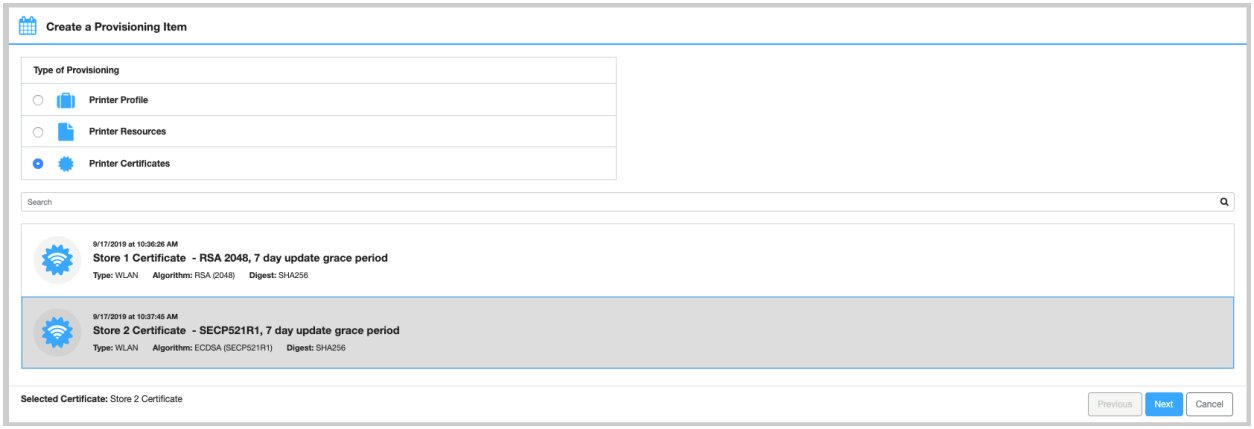
   Or, click **Previous** to go back to the previous page.



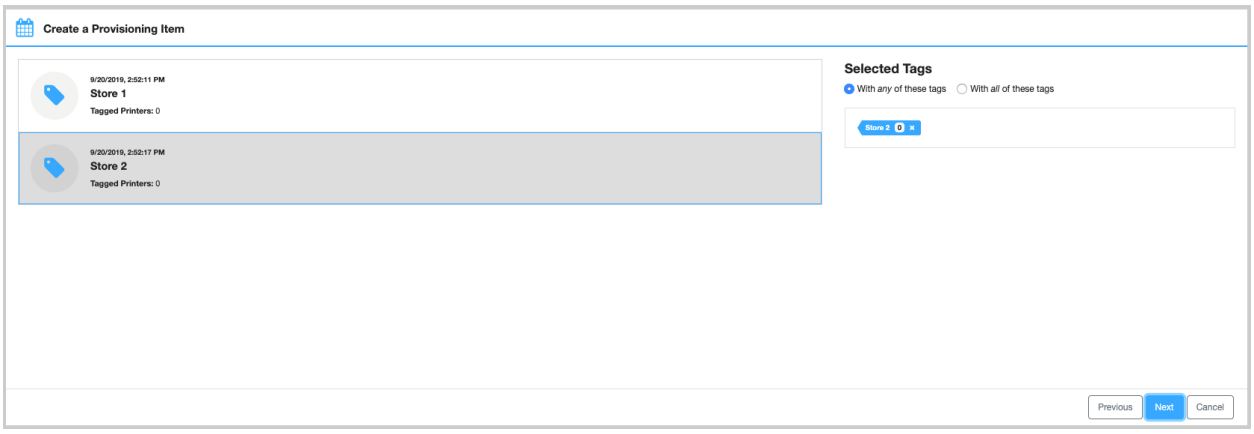
Procedure to Setup a Certificate Provisioning Item for Store 2

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

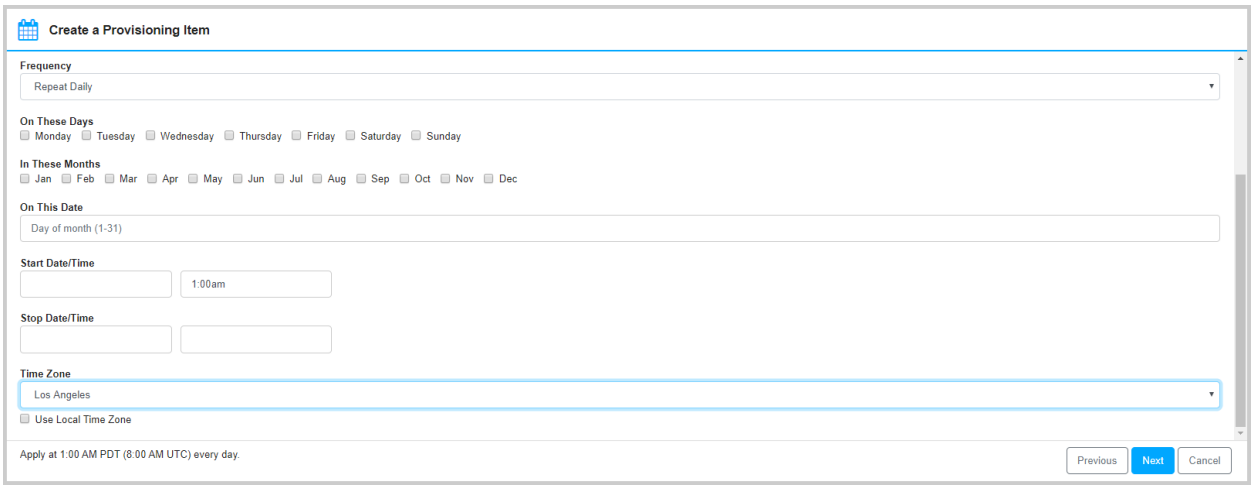
1. Select “Store 2 Certificate” certificate management item in step 2.



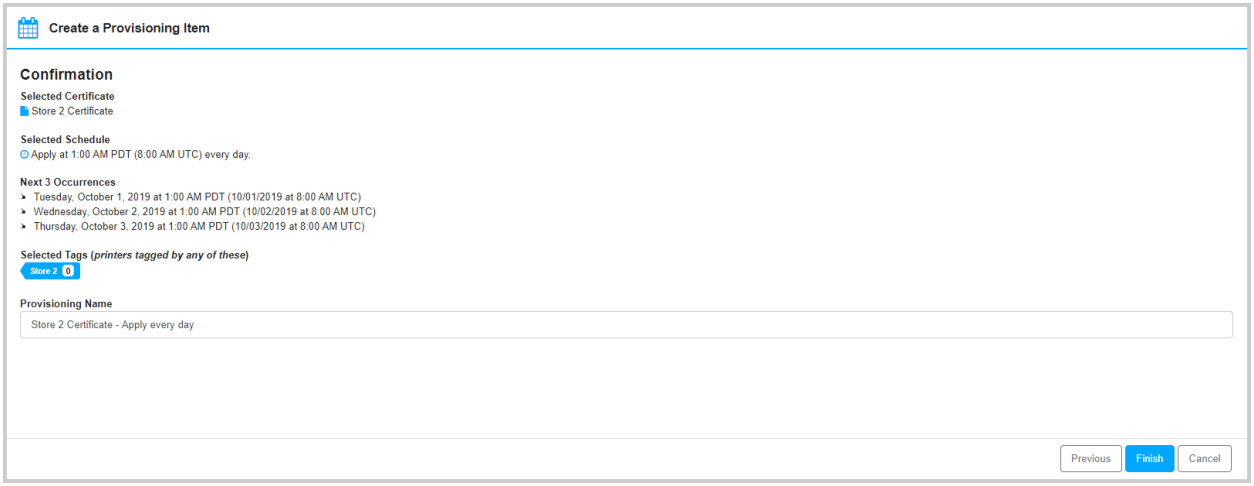
2. Select “Store 2” tag in step 4.



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



4. The confirmation page for Store 2 is:



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.

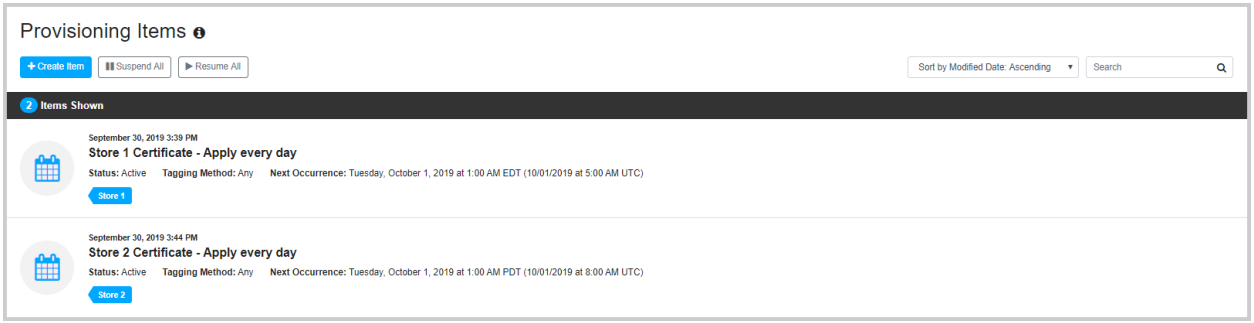


Table 1: Scenario Summary

	HQ Server	Store1	Store 2
Wireless Network	MS Active Directory Certificate w/NDES	WPA2	WPA2
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 window	--	01:00-04:00 EST	01:00-04:00 PST
Grace Period	--	7 days prior to cert. expiration	7 days prior to cert. 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

- [ ] Type
- [ ] 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

- [ ] Description of the CMI
- [ ] List of tag names
- [ ] Associated printers (to be tagged)
- [ ] Method to identify printers (to be tagged) by store
- [ ] Name of the CMI
- [ ] 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