

As previous noted, we have a device-based SCEP policy that looks like this (Figure 1):

SCEP Certificate
Windows 8.1 and later

* Subject name format ⓘ Serial number

* Subject alternative name ⓘ User principal name (UPN)

* Key usage ⓘ 2 selected

* Key size (bits) ⓘ 2048

* Hash algorithm ⓘ SHA-2

Root Certificate
Window: OPS RootCA

* Extended key usage ⓘ **Export**

| Name | Object Identifier | Predefined values | |
|------------------------------|--------------------------|-------------------|-----|
| Not configured | Not configured | Not configured | Add |
| Client Authentication | 1.3.6.1.5.5.7.3.2 | | ... |

Enrollment Settings

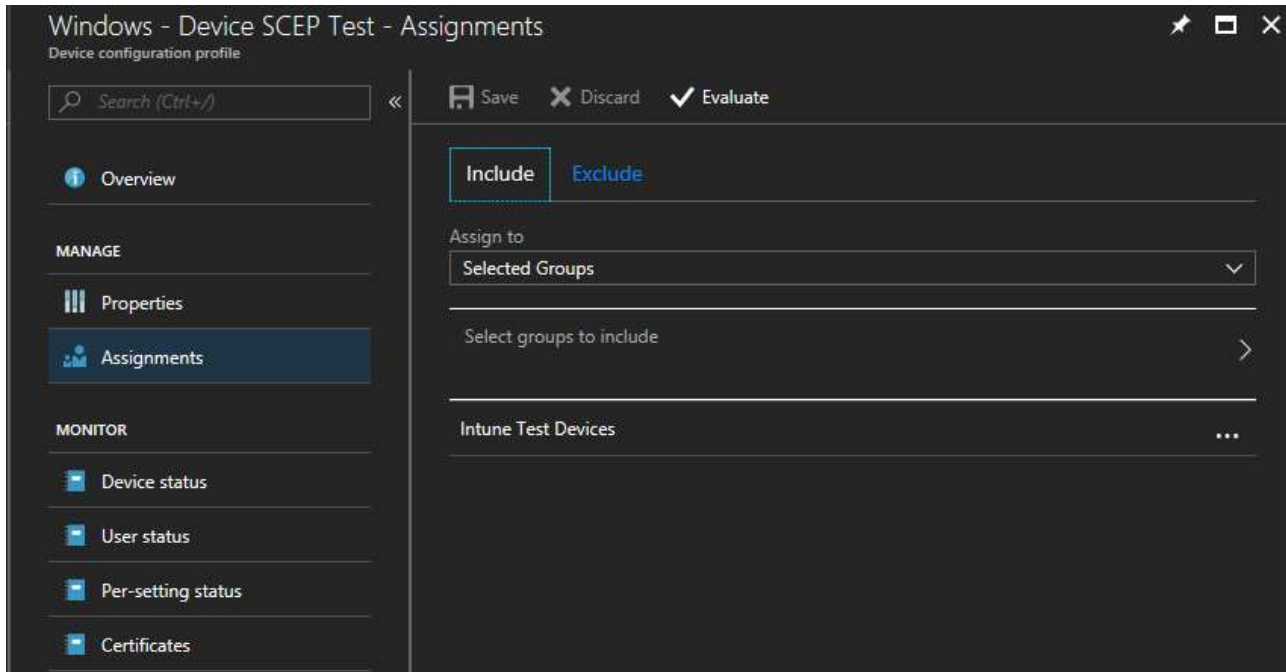
* Renewal threshold (%) ⓘ 20

* SCEP Server URLs ⓘ **Export**

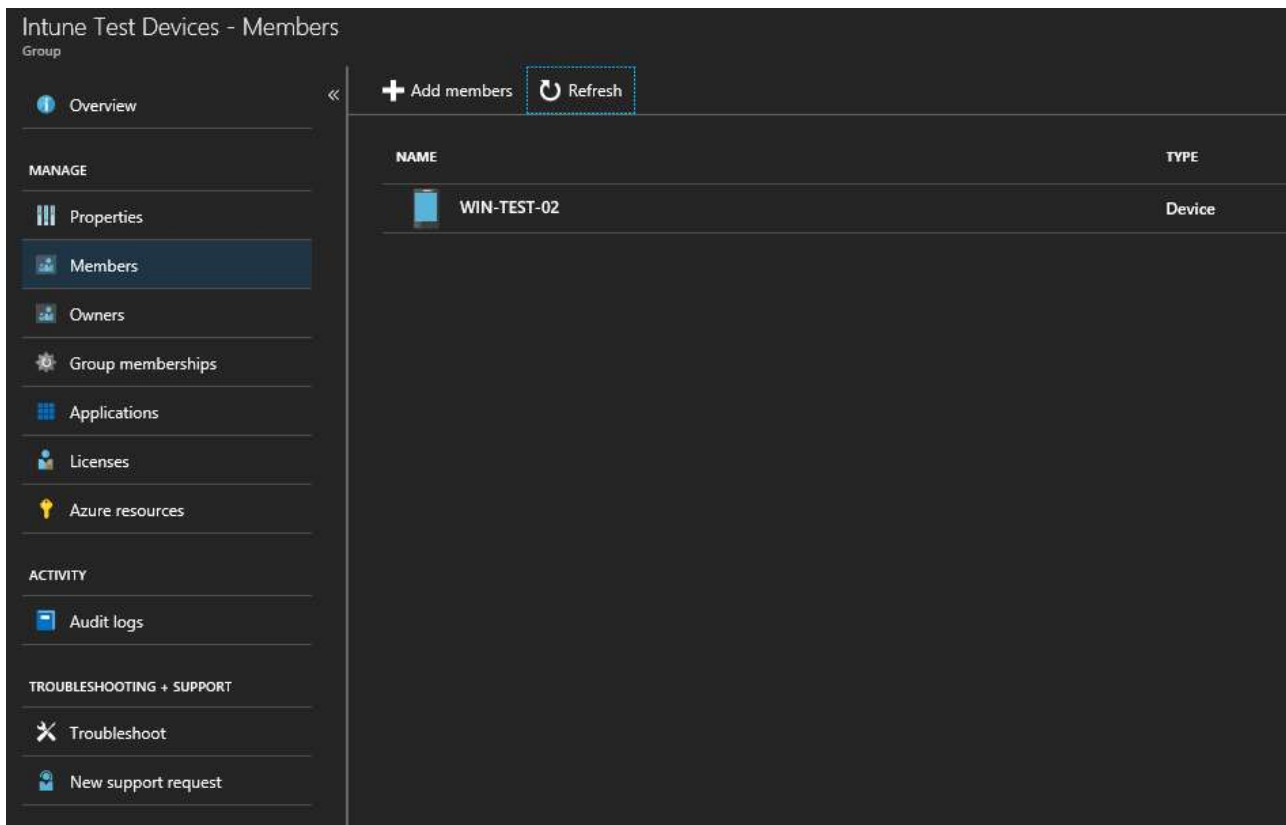
Server URL

| | |
|--|-----|
| e.g. https://contoso.com/certsrv/mscep/mscep.dll | Add |
| https://contoso.com/certsrv/mscep/mscep.dll | ... |

Assigned to our Intune Test Device Group (Figure 2):



This group currently only contains one test computer (Figure 3):



This device looks like this (Figure 4):

| | | | |
|-----------------|----------------------------|--------------------|---------------------------------|
| Device name | WIN-TEST-02 | Associated user | James Blair |
| Management name | Windows_6/24/2018_11:36 PM | Compliance | Compliant |
| Ownership | Corporate | Operating system | Windows |
| Serial number | Chassis Serial Number | Device model | HP Stream 11 Pro G2 Notebook PC |
| Phone number | | Last check-in time | 6/25/2018 1:10:56 AM |

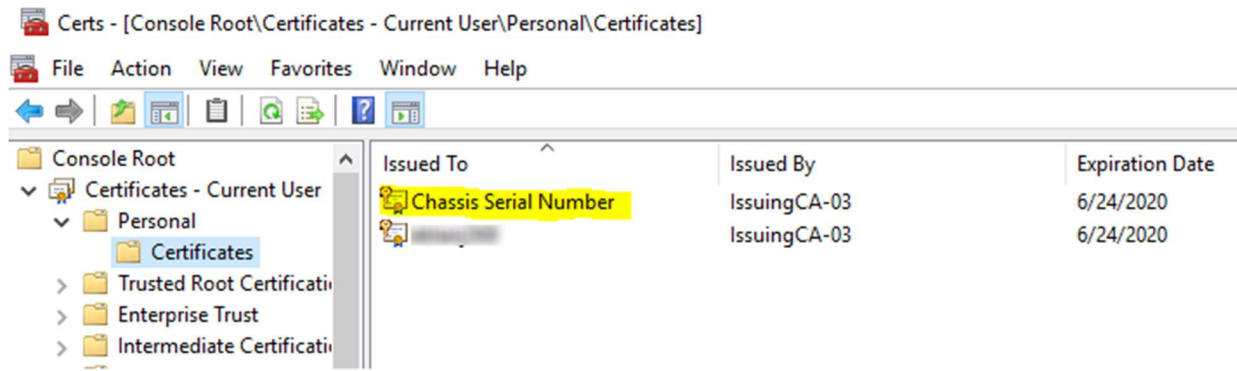
Now, according to the test machine's "Device Configuration", we see that the "Windows – Device SCEP Test" device configuration shows that was successfully applied (Figure 5):

| POLICY | STATE |
|----------------------------|-----------|
| Windows: SCEP - Users | Pending |
| Windows - Device SCEP Test | Succeeded |
| Cloud Print | Succeeded |
| Windows: Print Certificate | Succeeded |
| Windows: IssueCA-2 | Succeeded |

To me this means that the device should have received a machine-based SCEP cert with its serial number as the Subject as shown in figure 1 above (note: for whatever reason this device lists its serial number as "Chassis Serial Number" as seen in a figure 4). However, this is not the case as the Personal certificate store of the machine contains no such certificate:

| Issued To | Issued By | Expiration Date | Intend |
|----------------------------------|--------------------------------|-----------------|--------|
| 4f8a7f42-371c-49d7-8625-6400c... | SC_Online_Issuing | 6/24/2019 | Client |
| a8ac8678-48d0-4682-b101-a044... | MS-Organization-P2P-Access [20 | 6/26/2018 | Server |
| a8ac8678-48d0-4682-b101-a044... | MS-Organization-Access | 6/24/2028 | Client |

Looking further, though, I ***DID*** end up finding the certificate: Assigned to the current logged on user!



This behavior is repeatable, and shows the same result across multiple machines (although on all other test machines the cert generated has the proper serial number in the Issue to subject field) .