21 Feb 2025 - Configuring PKI addendum

Friday, February 21, 2025 9:39 AM

PKI addendum pack

Background:

The purpose of the addendum packs is to make 'smarter vs. harder' mantra packs. Packs that take 'lessons from the field' inputs from Microsoft engineers in each technology, incorporating monitoring best practices, and advancing the monitoring maturity. Maturity examples include self-healing monitors, recovery automation, running further scripts to diagnose, resolve issues. Issues like service recovery automation, TopProcess troubleshooting (what processes were hogging CPU/Memory at the time of alert), or logical disk cleanup. Other capabilities include simply tuning alerts for the health model, removing alerts that are not impacting. The PKI addendum adds a number of groups breaking out multiple different certificate scenarios reducing operational burden, switching to manual intervention. The pack creates groups of various certificate types and allows customization to when relevant teams want 'actionable' alerts.

Pack functionality includes:

- Groups created to Discover and monitor certificates in server certificate stores
- Critical alert for expired certificates
- Warning alert for invalid certificate chains, self-signed certificates, and revoked scenarios
- PKI certificate monitoring includes views in SCOM Console, for valid, about to expire, invalid, and more
- Update groups that utilize existing CA Auto-enrollment templates to help administrators know when manual intervention is required that template did NOT replace certificate
- Updates default 'about to expire' alerts to 60 day warning alerts, 30 day critical

    The groups allow breakout for DC, RDP, OCSP, Internal and external issued certificates
    Allows monitoring to be adjusted per organizational standards and procedures.

The PKI addendum (customizations) pack adds the following:

Additional discoveries (groups) added:

OCSP recurring certificates
Computer Certificates
Domain Controller (DC) Kerberos AutoEnrollment certificates
RDPAuth Computer certificates
SCCM/MECM ConfigMgrServerCert, ConfigMgrClientCert, ConfigMgrWebServerCert, ConfigMgrWinPEImages certificates
Internal issued certs (example CN= xxxx Issuing CA *)
External issued certs (example CN= * SW *)
SCCM/MECM SMS Issued self-signed certificates
SolarWinds self-signed certificates
Splunk self-signed certificates
VEEAM self-signed certificates

Customize Overrides included:

Break out of overrides included in the pack.

**Changed default discovery spread initialization to 30 minutes

Why: This randomizes the workflow within a 30 minute window preventing ALL monitored systems running at the same time.

Enabled functionality:

Local Certificate store & SelfSigned Certificate discoveries
***Assess additional folders to monitor
i.e. Trusted Root and Intermediate certificate folders
Override default CertificateAboutToExpire monitor (can be adjusted)
Global Certificates LifetimeThreshold to 60 days
Certificate Templates LifetimeThreshold to 30 days
External certs LifetimeThreshold to 60 days
Internal certs LifetimeThreshold to 30 days
ALL discoveries (sub-groups) set to warning except Internal/External
Disable CertificateValidity monitors for self-signed certs
Reason: Alert when expire, not self-signed cert chain issues
SCCM/MECM SMS Issued, SolarWinds, Splunk, VEEAM

Other certificate functionality

Add groups for CA Auto templates, when template automation does NOT replace certification
i.e. when SysAdmin manual intervention required

Requires verification after importing for group ID GUID's that overrides are properly applied
NOTE: Update less likely if installed in new environment should GUIDs be in use

Update PKI pack for environment

Pre-req PKI and PKI customizations pack must be imported to add the groups. This allows group customization, and updating overrides. Correcting the overrides is required to correct GUID for 'Context Instance' in environment. Unfortunately, this is a limitation of moving groups across SCOM management groups, and the inherent random GUID assignment of discovered objects/properties, etc.

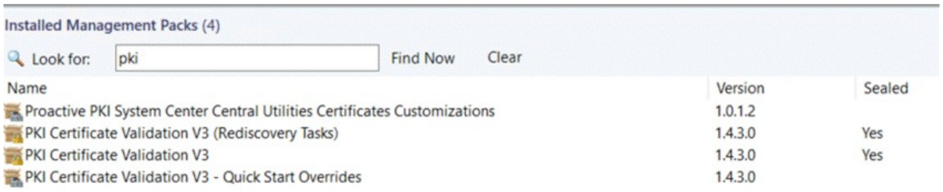
Install PKI packs

Verify if PKI packs are installed, including the customizations pack (which creates the groups)

Navigation Steps:

From the SCOM Console > Administration Tab >
Expand Management Packs > Click on Installed Management Packs
In the 'Look for:' bar, type PKI and hit enter

If your output has the four packs, proceed to next step.
Otherwise, import relevant packs



Installed Management Packs (4)

Look for: pki

Name	Version	Sealed
Proactive PKI System Center Central Utilities Certificates Customizations	1.0.1.2	
PKI Certificate Validation V3 (Rediscovery Tasks)	1.4.3.0	Yes
PKI Certificate Validation V3	1.4.3.0	Yes
PKI Certificate Validation V3 - Quick Start Overrides	1.4.3.0	

Update group regular expressions (regEx) as needed

Tailor the groups added in XML for smarter alerts WHEN manual intervention is required.
NOTE: No updates to groups may just result in empty groups

Update groups as necessary

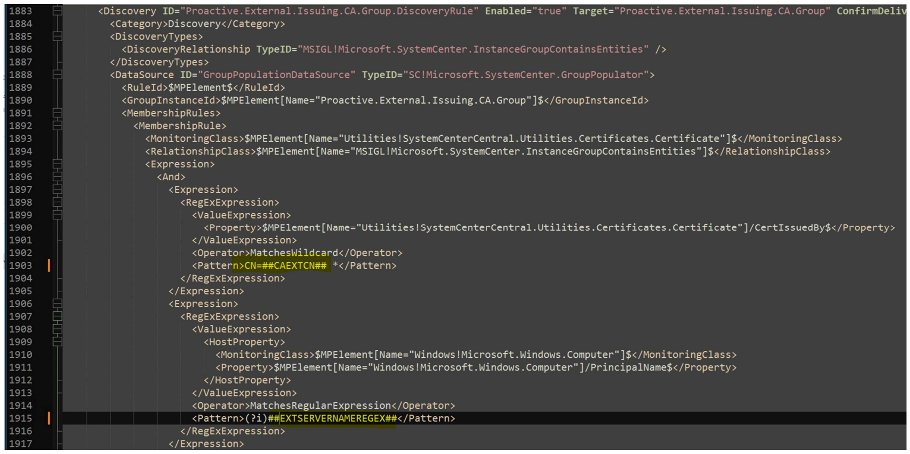
Find/Replace regular expression (RegEx) strings as necessary

- Proactive.CA.OCSP.Recurring.Certificates.Group.DiscoveryRule
  - Server Principal name = (?i)OCSP
  - EnhancedKeyUsageList = (?i)OCSP Signing
- Proactive.Computer.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)Computer Template|DomainComputers|Domain Computers|Domain Controller|RemoteDesktop
- Proactive.Domain.Controller.Kerberos.AutoEnrollment.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)DCKerberos
- Proactive.RDPAuth.Computer.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)RDPAuth|RemoteDesktop
- Proactive.MECM.SCCM.ConfigMgrServerCert.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)ConfigMgrServerCert
- Proactive.MECM.SCCM.ConfigMgrClientCert.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)ConfigMgrClientCert
- Proactive.MECM.SCCM.ConfigMgrWebServerCert.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)ConfigMgrWebServerCert
- Proactive.MECM.SCCM.ConfigMgrWinPEImages.Certificates.Group.DiscoveryRule
  - TemplateName = (?i)ConfigMgrWinPEImages
- Proactive.Internal.Issuing.CA.Group.DiscoveryRule
  - CertIssuedBy = CN=##CAINTCN## *
  - Server PrincipalName = (?i)##SERVERNAMEREGEX##
- Proactive.External.Issuing.CA.Group.DiscoveryRule
  - CertIssuedBy = CN=##CAEXTCN## *
  - Server PrincipalName = (?i)##SERVERNAMEREGEX##
- Proactive.MECM.SCCM.SMSIssuing.Certificate.Group
  - CertIssuedBy = CN=SMS Issuing
- Proactive.SolarWinds.Certificate.Group
  - CertIssuedBy = SolarWinds
- Proactive.Splunk.Certificate.Group
  - CertIssuedBy = Splunk
- Proactive.VEEAM.Certificate.Group
  - CertIssuedBy = Veeam Backup Server Certificate

External Discovery update example

Find/Replace highlighted expressions

##CAEXTCN## > Eeplace with external CN path discovered from SCOM console state view
##EXTSERVERNAMEREGEX## > Replace with Server naming convention, whether for CA or generic to server naming conventions at site that delineate the external certificates installed on servers in environment



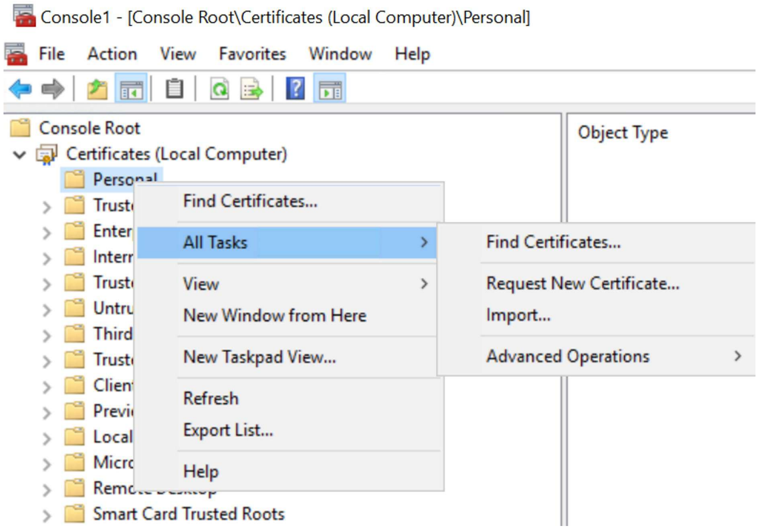
```
<Discovery ID="Proactive.External.Issuing.CA.Group.DiscoveryRule" Enabled="true" Target="Proactive.External.Issuing.CA.Group" ConfirmDeliv
  <Category>Discovery</Category>
  <DiscoveryTypes>
    <DiscoveryRelationship TypeID="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities" />
  </DiscoveryTypes>
  <DataSource ID="GroupPopulationDataSource" TypeID="SC!Microsoft.SystemCenter.GroupPopulator">
    <RuleId>$MPElement$</RuleId>
    <GroupInstanceId>$MPElement[Name="Proactive.External.Issuing.CA.Group"]$</GroupInstanceId>
    <MembershipRules>
      <MembershipRule>
        <MonitoringClass>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]$</MonitoringClass>
        <RelationshipClass>$MPElement[Name="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities"]$</RelationshipClass>
        <Expression>
          <And>
            <Expression>
              <RegExExpression>
                <ValueExpression>
                  <Property>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]/CertIssuedBy$</Property>
                </ValueExpression>
                <Operator>MatchesWildcard</Operator>
                <Pattern>CN=##CAEXTCN## *</Pattern>
              </RegExExpression>
            </Expression>
            <Expression>
              <RegExExpression>
                <ValueExpression>
                  <HostProperty>
                    <MonitoringClass>$MPElement[Name="Windows!Microsoft.Windows.Computer"]$</MonitoringClass>
                    <Property>$MPElement[Name="Windows!Microsoft.Windows.Computer"]/PrincipalName$</Property>
                  </HostProperty>
                </ValueExpression>
                <Operator>MatchesRegularExpression</Operator>
                <Pattern>(?i)##EXTSERVERNAMEREGEX##</Pattern>
              </RegExExpression>
            </Expression>
```

Certificate template names

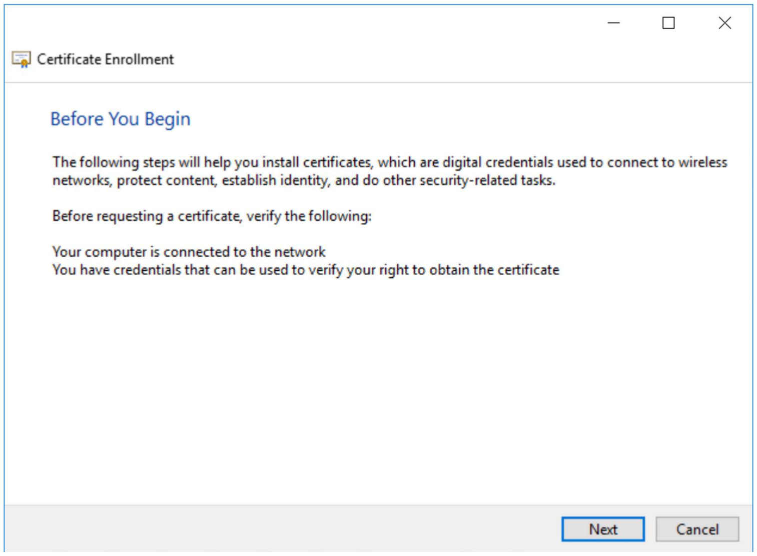
Using Certificate Authority (CA) auto-enrollment templates is a best practice allowing PKI structured environments to automatically query, renew/replace certificates automatically. If these are used in the environment, we want monitoring to match, so that alerts occur when automation fails, requiring manual intervention.

Verify Active Directory Enrollment policy exists in environment
Login to server, run MMC
Add SnapIn for Certificates (for local computer)

Example output of Personal certificate store
From MMC > Expand Certificates > right click > All Tasks > Request New Certificate



Click Next



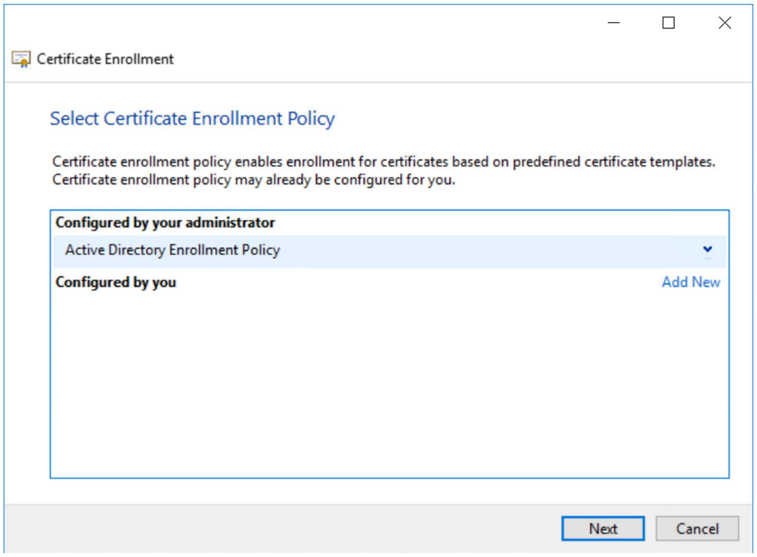
Before You Begin

The following steps will help you install certificates, which are digital credentials used to connect to wireless networks, protect content, establish identity, and do other security-related tasks.

Before requesting a certificate, verify the following:

Your computer is connected to the network
You have credentials that can be used to verify your right to obtain the certificate

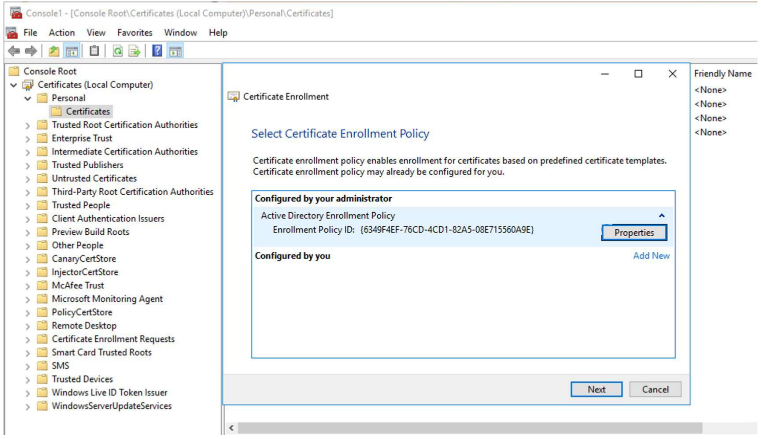
Click Next


Certificate Enrollment
Configured by your administrator
Active Directory Enrollment Policy
Configured by you
Add New
Next
Cancel

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Example of AD Enrollment Policy

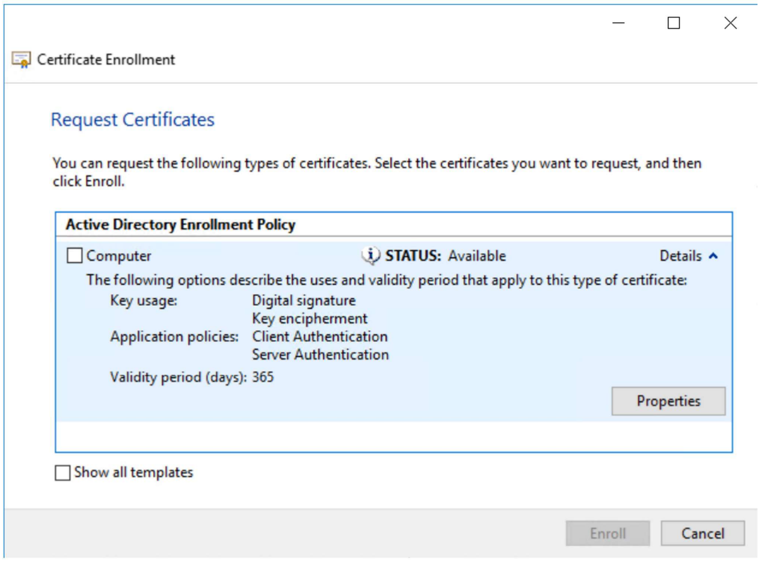

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Other People
CanaryCertStore
InjectorCertStore
McAfee Trust
Microsoft Monitoring Agent
PolicyCertStore
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
SMS
Trusted Devices
Windows Live ID Token Issuer
WindowsServerUpdateServices
Certificate Enrollment
Configured by your administrator
Active Directory Enrollment Policy
Properties
Configured by you
Add New
Next
Cancel
Friendly Name
<None>
<None>
<None>
<None>

Select Certificate Enrollment Policy

Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.

Enrollment Policy ID: {6349F4EF-76CD-4CD1-82A5-08E715560A9E}

Example in Lab if you have Tier0/Domain Admin rights



Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

□ Computer STATUS: Available

The following options describe the uses and validity period that apply to this type of certificate:

Key usage: Digital signature
Key encipherment

Application policies: Client Authentication
Server Authentication

Validity period (days): 365

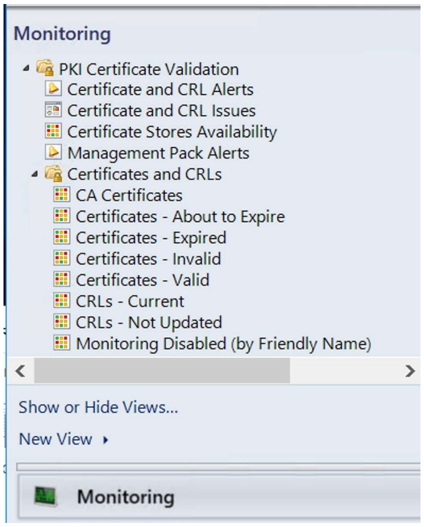
□ Show all templates

View discovered certificate data

Verify SCOM discovered certificates (any server with agent) in the environment that use TemplateName property, and customize accordingly.

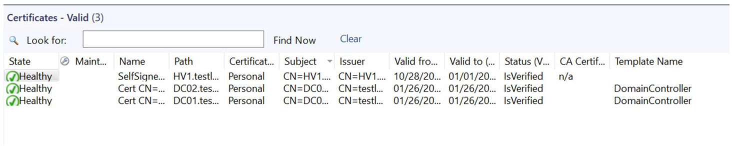
Navigation Steps:

From SCOM console
Click on Monitoring Tab > expand 'PKI certificate Validation' folder
Expand 'Certificates and CRLs' folder
Click on Certificates - Valid state view



Click on the 'Template Name' to sort to help group discovered certificates

NOTE: Output used for matching groups to actual template names



Certificates - Valid (3)

State	Maint...	Name	Path	Certificat...	Subject	Issuer	Valid fro...	Valid to (...	Status (V...	CA Certif...	Template Name
Healthy		SelfSigne...	HV1.testl...	Personal	CN=HV1....	CN=HV1....	10/28/20...	01/01/20...	IsVerified	n/a	
Healthy		Cert CN=...	DC02.tes...	Personal	CN=DC0...	CN=testl...	01/26/20...	01/26/20...	IsVerified		DomainController
Healthy		Cert CN=...	DC01.tes...	Personal	CN=DC0...	CN=testl...	01/26/20...	01/26/20...	IsVerified		DomainController

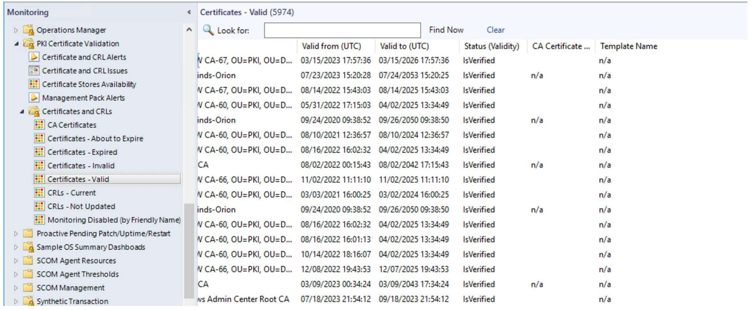
Highlight a certificate

Copy/Paste to notepad, and keep the name(s).
The Template Name(s) will be utilized in the next step (updating the group patterns)

Clean up SCOM output on notepad for the unique Template Name(s). This may require Tier0/Domain Admin assistance to answer when the template should have replaced the expiring certificate, as well as WHEN an alert is needed for manual intervention. The answers and notepad will provide what is needed in a meeting to discuss proper tuning.

Navigation steps:

Go to SCOM Console > Monitoring Tab
Expand PKI folder, Expand Certificates and CRL's
Click on Certificates - Valid' view
Sort by Template Name (TemplateName in XML)



Certificates - Valid (5974)

	Valid from (UTC)	Valid to (UTC)	Status (Validity)	CA Certificate ...	Template Name
V CA-67, OU=PKI, OU=D...	03/15/2023 17:57:36	03/15/2026 17:57:36	IsVerified		n/a
inds-Orion	07/23/2023 15:20:28	07/24/2053 15:20:25	IsVerified	n/a	n/a
V CA-67, OU=PKI, OU=D...	08/14/2022 15:43:03	08/14/2025 15:43:03	IsVerified		n/a
V CA-60, OU=PKI, OU=D...	05/31/2022 17:15:03	04/02/2025 13:34:49	IsVerified		n/a
inds-Orion	09/24/2020 09:38:52	09/26/2050 09:38:50	IsVerified	n/a	n/a
V CA-60, OU=PKI, OU=D...	08/10/2021 12:36:57	08/10/2024 12:36:57	IsVerified		n/a
V CA-60, OU=PKI, OU=D...	08/16/2022 16:02:32	04/02/2025 13:34:49	IsVerified		n/a
CA	08/02/2022 00:15:43	08/02/2042 17:15:43	IsVerified	n/a	n/a
V CA-66, OU=PKI, OU=D...	11/02/2022 11:11:10	11/02/2025 11:11:10	IsVerified		n/a
V CA-60, OU=PKI, OU=D...	03/03/2021 16:00:25	03/02/2024 16:00:25	IsVerified		n/a
inds-Orion	09/24/2020 09:38:52	09/26/2050 09:38:50	IsVerified	n/a	n/a
V CA-60, OU=PKI, OU=D...	08/16/2022 16:02:32	04/02/2025 13:34:49	IsVerified		n/a
V CA-60, OU=PKI, OU=D...	08/16/2022 16:01:13	04/02/2025 13:34:49	IsVerified		n/a
V CA-60, OU=PKI, OU=D...	10/14/2022 18:16:07	04/02/2025 13:34:49	IsVerified		n/a
V CA-66, OU=PKI, OU=D...	12/08/2022 19:43:53	12/07/2025 19:43:53	IsVerified		n/a
CA	03/09/2023 00:34:24	03/09/2043 17:34:24	IsVerified	n/a	n/a
ws Admin Center Root CA	07/18/2023 21:54:12	09/18/2023 21:54:12	IsVerified		n/a

Save this data to use below when we update the Group discoveries to match environment (AD enrollment policies)

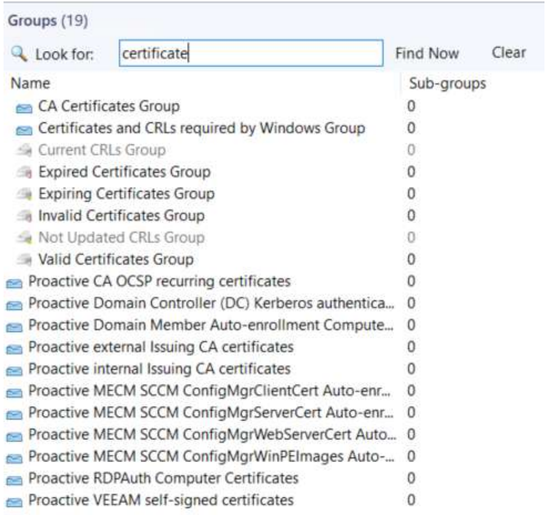
Verify Groups and 'Group Members'

Use the output from the 'Certificate template names' to verify groups and group members

Navigation Steps:

From the SCOM Console > Authoring Tab > Click on Groups
In the 'Look for:' bar type certificate, and hit enter

Example output



Groups (19)

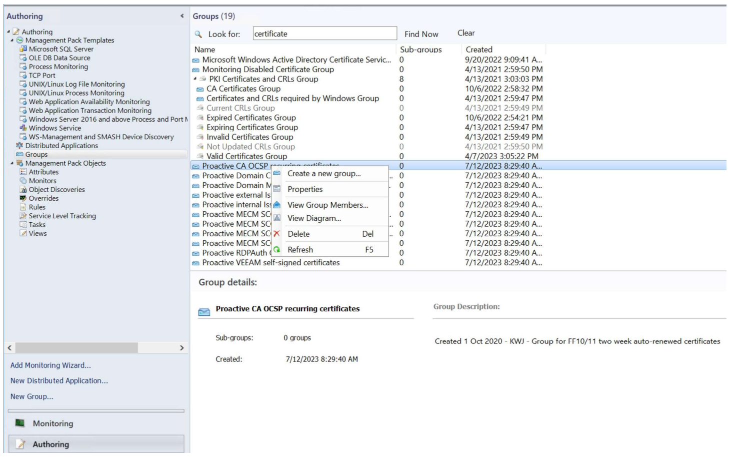
Look for: certificate

Name	Sub-groups
CA Certificates Group	0
Certificates and CRLs required by Windows Group	0
Current CRLs Group	0
Expired Certificates Group	0
Expiring Certificates Group	0
Invalid Certificates Group	0
Not Updated CRLs Group	0
Valid Certificates Group	0
Proactive CA OCSP recurring certificates	0
Proactive Domain Controller (DC) Kerberos authentica...	0
Proactive Domain Member Auto-enrollment Compute...	0
Proactive external Issuing CA certificates	0
Proactive internal Issuing CA certificates	0
Proactive MECM SCCM ConfigMgrClientCert Auto-enr...	0
Proactive MECM SCCM ConfigMgrServerCert Auto-enr...	0
Proactive MECM SCCM ConfigMgrWebServerCert Auto...	0
Proactive MECM SCCM ConfigMgrWinPEImages Auto-...	0
Proactive RDPAuth Computer Certificates	0
Proactive VEEAM self-signed certificates	0

Click on a group > select 'View Group Members'

> If the output is blank, that means the group defaults match ZERO discovered objects in the environment

Repeat for each group, checking group members to validate if default patterns match anything in installed environment



Groups (19)

Look for: certificate

Name	Sub-groups	Created
Microsoft Windows Active Directory Certificate Servic...	0	9/20/2022 9:09:41 A...
Monitoring Disabled Certificate Group	0	4/13/2021 2:59:50 PM
PKI Certificates and CRLs Group	8	4/13/2021 3:03:03 PM
CA Certificates Group	0	10/6/2022 2:58:32 PM
Certificates and CRLs required by Windows Group	0	4/13/2021 2:59:47 PM
Current CRLs Group	0	4/13/2021 2:59:49 PM
Expired Certificates Group	0	10/6/2022 2:54:21 PM
Expiring Certificates Group	0	4/13/2021 2:59:47 PM
Invalid Certificates Group	0	4/13/2021 2:59:49 PM
Not Updated CRLs Group	0	4/13/2021 2:59:50 PM
Valid Certificates Group	0	4/7/2023 3:05:22 PM
Proactive CA OCSP recurring certificates	0	7/12/2023 8:29:40 A...
Proactive Domain C	0	7/12/2023 8:29:40 A...
Proactive Domain M	0	7/12/2023 8:29:40 A...
Proactive external Is	0	7/12/2023 8:29:40 A...
Proactive internal Is	0	7/12/2023 8:29:40 A...
Proactive MECM SC	0	7/12/2023 8:29:40 A...
Proactive MECM SC	0	7/12/2023 8:29:40 A...
Proactive MECM SC	0	7/12/2023 8:29:40 A...
Proactive MECM SC	0	7/12/2023 8:29:40 A...
Proactive RDPAuth	0	7/12/2023 8:29:40 A...
Proactive VEEAM self-signed certificates	0	7/12/2023 8:29:40 A...

Group details:

Proactive CA OCSP recurring certificates

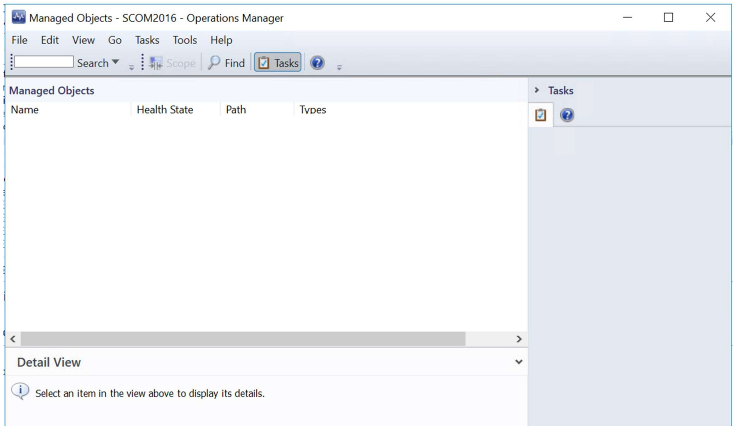
Sub-groups: 0 groups

Created: 7/12/2023 8:29:40 AM

Group Description:

Created 1 Oct 2020 - KWJ - Group for FF10/11 two week auto-renewed certificates

Example of blank group members



Managed Objects - SCOM2016 - Operations Manager

Name	Health State	Path	Types

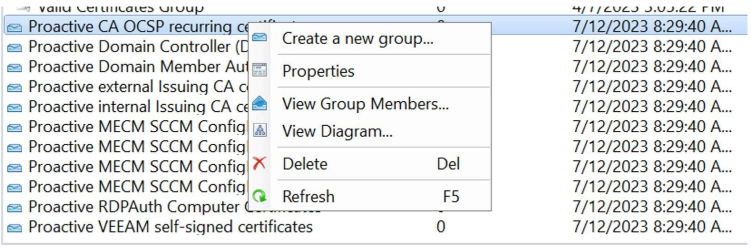
Select an item in the view above to display its details.

Close Group window 'Managed objects'

Adjust regular expression(s), as needed, leveraging the monitoring Tab PKI certificates folder > 'Valid certificate' view

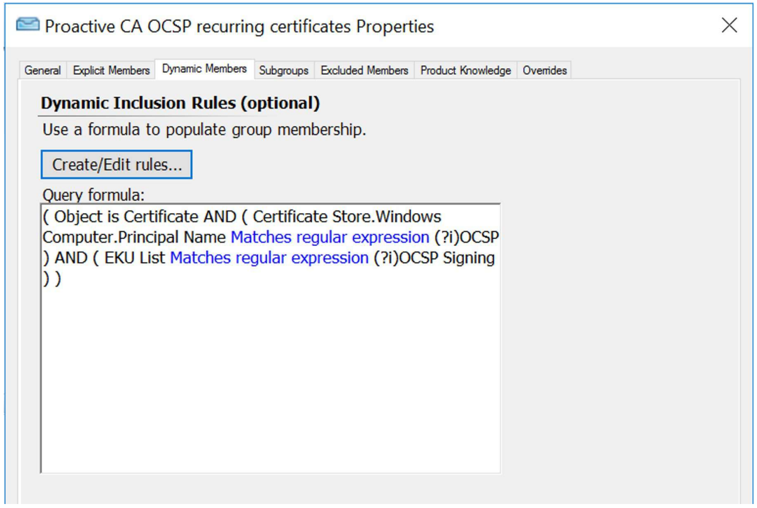
Edit PKI groups

Right click (alternate mouse button)
Select Properties to edit group



Valid Certificates Group	0	4/7/2023 3:03:22 PM
Proactive CA OCSP recurring ce	0	7/12/2023 8:29:40 A...
Proactive Domain Controller (D		7/12/2023 8:29:40 A...
Proactive Domain Member Aut		7/12/2023 8:29:40 A...
Proactive external Issuing CA c		7/12/2023 8:29:40 A...
Proactive internal Issuing CA ce		7/12/2023 8:29:40 A...
Proactive MECM SCCM Config		7/12/2023 8:29:40 A...
Proactive MECM SCCM Config		7/12/2023 8:29:40 A...
Proactive MECM SCCM Config		7/12/2023 8:29:40 A...
Proactive MECM SCCM Config		7/12/2023 8:29:40 A...
Proactive RDPAuth Computer C	0	7/12/2023 8:29:40 A...
Proactive VEEAM self-signed certificates	0	7/12/2023 8:29:40 A...

Click on 'Create/Edit rules' button



Proactive CA OCSP recurring certificates Properties

Dynamic Inclusion Rules (optional)

Use a formula to populate group membership.

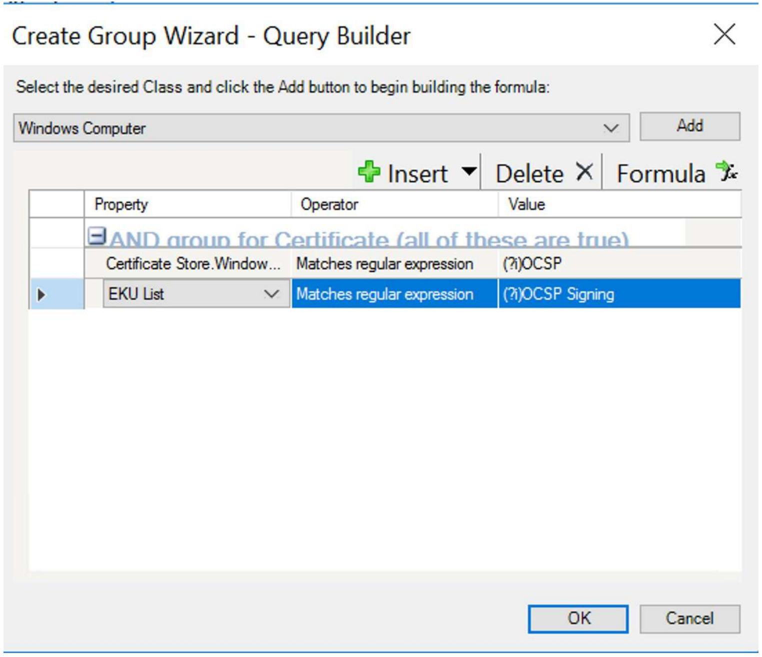
Query formula:

(Object is Certificate AND (Certificate Store.Windows Computer.Principal Name Matches regular expression (?i)OCSP) AND (EKU List Matches regular expression (?i)OCSP Signing))

Regular Expression syntax allows | to delimit multiple strings

(?i) allows for case insensitive expressions (upper/lower case indifferent)

Adjust EKU list to match applicable certificate property for AD enrollment policy (Certificate TemplateName property)
Click OK
Click Close to end group update.



Create Group Wizard - Query Builder

Select the desired Class and click the Add button to begin building the formula:

Windows Computer

Property	Operator	Value
AND group for Certificate (all of these are true)		
Certificate Store.Window...	Matches regular expression	(?i)OCSP
EKU List	Matches regular expression	(?i)OCSP Signing

Update Group Overrides

The overrides must be accurately mapped to a group and GUID to show in Overrides.

Symptoms in SCOM console

- May cause the Overrides view in the Authoring Tab to error, or not load
- Overrides may not show up in SCOM, even if in the XML or MP/MPB file
- Does NOT transfer between management groups due to SCOM random GUID nature.

Try to figure out what the GUID is for these groups when the PKI customizations pack is installed

From PowerShell on MS, paste the following commands:

```
get-scomclassinstance -DisplayName "Proactive CA OCSP recurring certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive Domain Member Auto-enrollment Computer certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive Domain Controller (DC) Kerberos authentication Autoenrollment certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive RDPAuth Computer Certificates" | ft Id

get-scomclassinstance -DisplayName "Proactive MECM SCCM ConfigMgrServerCert Auto-enrollment Computer Certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive MECM SCCM ConfigMgrClientCert Auto-enrollment Computer Certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive MECM SCCM ConfigMgrWebServerCert Auto-enrollment Computer Certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive MECM SCCM ConfigMgrWinPEImages Auto-enrollment Computer Certificates" | ft Id

get-scomclassinstance -DisplayName "Proactive internal Issuing CA certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive external Issuing CA certificates" | ft Id
get-scomclassinstance -DisplayName "Proactive MECM SCCM ConfigMgr SMS Issuing self-signed certs" | ft Id
get-scomclassinstance -DisplayName "Proactive SolarWinds self-signed certs" | ft Id
get-scomclassinstance -DisplayName "Proactive Splunk self-signed certs" | ft Id
get-scomclassinstance -DisplayName "Proactive VEEAM self-signed certificates" | ft Id
```

NOTE the Id (GUID) outputs to update the PKI customizations pack XML for the ContextInstance values

Setting Certificate expiring alerts

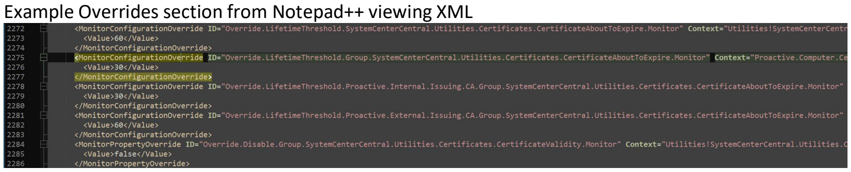
Understand that tuning the certificate expiring alerts can be changed to organizational standards.

Out of the Box (OotB) values are as follows:

NOTE Adjust based on customer requirements, as needed

Default behavior is alerts 60 days before expiration, warning alert is created warning, less than 30 days critical
Computer certificates 30 days before expiration, warning alert is created (can be controlled by AD Enrollment policy at different interval)
Internal certs alert at 30 days
External certs alert at 60 days (due to additional time required to request/implement)

Example Overrides section from Notepad++ viewing XML



```
      <MonitorConfigurationOverride ID="Override.LifetimeThreshold.SystemCenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor" Context="Utilities!SystemCenterCentr
        <Value>60</Value>
      </MonitorConfigurationOverride>
      <MonitorConfigurationOverride ID="Override.LifetimeThreshold.Group.SystemCenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor" Context="Proactive.Computer.Ce
        <Value>30</Value>
      </MonitorConfigurationOverride>
      <MonitorConfigurationOverride ID="Override.LifetimeThreshold.Proactive.Internal.Issuing.CA.Group.SystemCenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor"
        <Value>30</Value>
      </MonitorConfigurationOverride>
      <MonitorConfigurationOverride ID="Override.LifetimeThreshold.Proactive.External.Issuing.CA.Group.SystemCenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor"
        <Value>60</Value>
      </MonitorConfigurationOverride>
      <MonitorPropertyOverride ID="Override.Disable.Group.SystemCenterCentral.Utilities.Certificates.CertificateValidity.Monitor" Context="Utilities!SystemCenterCentral.Utilities.C
        <Value>false</Value>
      </MonitorPropertyOverride>
```

Update the XML overrides in the XML of the PKI customizations pack

Next, update the PKI management pack so we get all our functionality properly configured.

Update Overrides with GUID Id values

Open your favorite text file editor like NotePad++, Visual Studio, Visual Code, Notepad, etc.
This article is documented with NotePad++

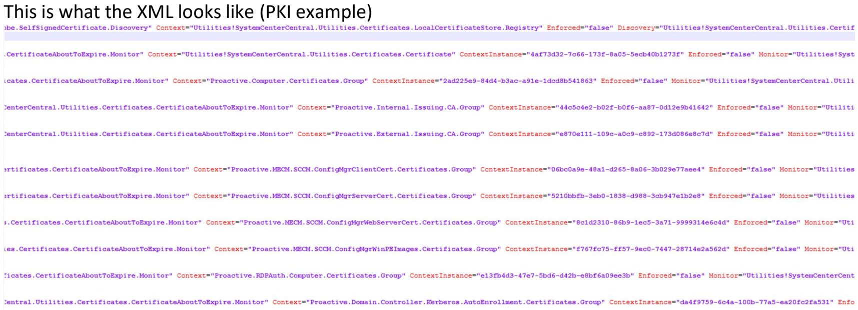
Navigation Steps:

From SCOM Console > Monitoring tab > Active Alerts
When you click on an alert, and choose Overrides > for a group

Example XML for overide (of a group)

```
    <MonitorPropertyOverride
ID="Override.Severity.MECM.ConfigMgrClientCert.SystemCenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor"
Context="Proactive.MECM.SCCM.ConfigMgrClientCert.Certificates.Group" ContextInstance="34b0de3a-3421-9dd1-0e6b-4f228804cc6b"
Enforced="false" Monitor="Utilities!SystemCenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor" Property="AlertSeverity">
      <Value>Warning</Value>
    </MonitorPropertyOverride>
```

This is what the XML looks like (PKI example)



```
be.SelfSignedCertificate.Discovery" Context="Utilities!SystemCenterCentral.Utilities.Certificates.LocalCertificateStore.Registry" Enforced="false" Discovery="Utilities!SystemCenterCentral.Utilities.Certif

.CertificateAboutToExpire.Monitor" Context="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate" ContextInstance="4af73d32-7c66-173f-8a05-5ecb40b1273f" Enforced="false" Monitor="Utilities!Syst

icates.CertificateAboutToExpire.Monitor" Context="Proactive.Computer.Certificates.Group" ContextInstance="2ad225e9-84d4-b3ac-a91e-1dcd8b541863" Enforced="false" Monitor="Utilities!SystemCenterCentral.Utili

CenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor" Context="Proactive.Internal.Issuing.CA.Group" ContextInstance="44c5c4e2-b02f-b0f6-aa87-0d12e9b41642" Enforced="false" Monitor="Utiliti

CenterCentral.Utilities.Certificates.CertificateAboutToExpire.Monitor" Context="Proactive.External.Issuing.CA.Group" ContextInstance="e870e111-109c-a0c9-c892-173d086e8c7d" Enforced="false" Monitor="Utiliti


ertificates.CertificateAboutToExpire.Monitor" Context="Proactive.MECM.SCCM.ConfigMgrClientCert.Certificates.Group" ContextInstance="06bc0a9e-48a1-d265-8a06-3b029e77aee4" Enforced="false" Monitor="Utilities

ertificates.CertificateAboutToExpire.Monitor" Context="Proactive.MECM.SCCM.ConfigMgrServerCert.Certificates.Group" ContextInstance="5210bbfb-3eb0-1838-d988-3cb947e1b2e8" Enforced="false" Monitor="Utilities

.Certificates.CertificateAboutToExpire.Monitor" Context="Proactive.MECM.SCCM.ConfigMgrWebServerCert.Certificates.Group" ContextInstance="8c1d2310-86b9-1ec5-3a71-9999314e6c4d" Enforced="false" Monitor="Uti

ies.Certificates.CertificateAboutToExpire.Monitor" Context="Proactive.MECM.SCCM.ConfigMgrWinPEImages.Certificates.Group" ContextInstance="f767fc75-ff57-9ec0-7447-28714e2a562d" Enforced="false" Monitor="Uti

ficates.CertificateAboutToExpire.Monitor" Context="Proactive.RDPAuth.Computer.Certificates.Group" ContextInstance="e13fb4d3-47e7-5bd6-d42b-e8bf6a09ee3b" Enforced="false" Monitor="Utilities!SystemCenterCent

Central.Utilities.Certificates.CertificateAboutToExpire.Monitor" Context="Proactive.Domain.Controller.Kerberos.AutoEnrollment.Certificates.Group" ContextInstance="da4f9759-6c4a-100b-77a5-ea20fc2fa531" Enfo
```

NOTE Domain Admin (or CA/Certificate SME) may be required to answer expiration values for alerts

Update PKI pack discoveries

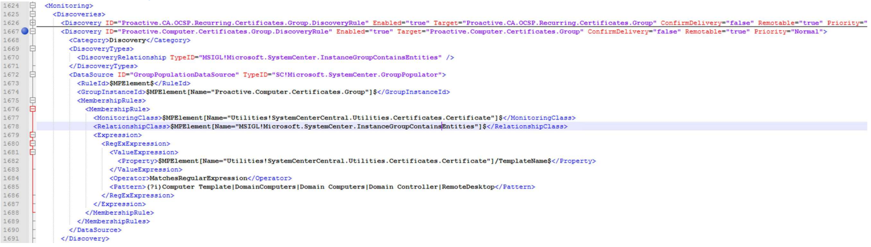
Now that we have a list of the template names, we need to update the PKI discoveries.

Sometimes OCSP is NOT housed in an environment (N/A not applicable), so this group can be skipped.

Open XML in Notepad++ (helps with XML syntax through color coding)

Sort by TemplateName, to help see what templates are in your environment.
These values discovered, will be used to update the PKI SCOM groups
If not applicable, leave 'Pattern' section alone, group will have NO members

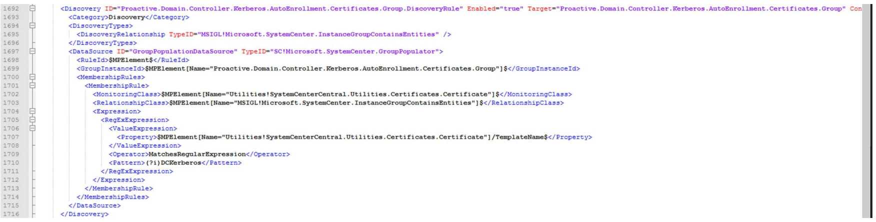
Example of Computer certificates



```
<Monitoring>
  <Discoveries>
    <Discovery ID="Proactive.CA.OCSP.Recurring.Certificates.Group.DiscoveryRule" Enabled="true" Target="Proactive.CA.OCSP.Recurring.Certificates.Group" ConfirmDelivery="false" Remotable="true" Priority="
    <Discovery ID="Proactive.Computer.Certificates.Group.DiscoveryRule" Enabled="true" Target="Proactive.Computer.Certificates.Group" ConfirmDelivery="false" Remotable="true" Priority="Normal">
      <Category>Discovery</Category>
      <DiscoveryTypes>
        <DiscoveryRelationship TypeID="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities" />
      </DiscoveryTypes>
      <DataSource ID="GroupPopulationDataSource" TypeID="SC!Microsoft.SystemCenter.GroupPopulator">
        <RuleId>$MPElement$</RuleId>
        <GroupInstanceId>$MPElement[Name="Proactive.Computer.Certificates.Group"]$</GroupInstanceId>
        <MembershipRules>
          <MembershipRule>
            <MonitoringClass>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]$</MonitoringClass>
            <RelationshipClass>$MPElement[Name="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities"]$</RelationshipClass>
            <Expression>
              <RegExExpression>
                <ValueExpression>
                  <Property>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]/TemplateName$</Property>
                </ValueExpression>
                <Operator>MatchesRegularExpression</Operator>
                <Pattern>(?i)Computer Template|DomainComputers|Domain Computers|Domain Controller|RemoteDesktop</Pattern>
              </RegExExpression>
            </Expression>
          </MembershipRule>
        </MembershipRules>
      </DataSource>
    </Discovery>
```

Kerberos template

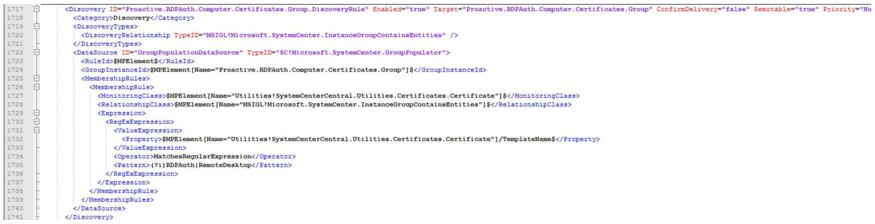
IF Kerberos enrollment template is applicable for your environment. Adjust template name(s) to adjust pattern for group members



```
    <Discovery ID="Proactive.Domain.Controller.Kerberos.AutoEnrollment.Certificates.Group.DiscoveryRule" Enabled="true" Target="Proactive.Domain.Controller.Kerberos.AutoEnrollment.Certificates.Group" Con
      <Category>Discovery</Category>
      <DiscoveryTypes>
        <DiscoveryRelationship TypeID="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities" />
      </DiscoveryTypes>
      <DataSource ID="GroupPopulationDataSource" TypeID="SC!Microsoft.SystemCenter.GroupPopulator">
        <RuleId>$MPElement$</RuleId>
        <GroupInstanceId>$MPElement[Name="Proactive.Domain.Controller.Kerberos.AutoEnrollment.Certificates.Group"]$</GroupInstanceId>
        <MembershipRules>
          <MembershipRule>
            <MonitoringClass>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]$</MonitoringClass>
            <RelationshipClass>$MPElement[Name="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities"]$</RelationshipClass>
            <Expression>
              <RegExExpression>
                <ValueExpression>
                  <Property>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]/TemplateName$</Property>
                </ValueExpression>
                <Operator>MatchesRegularExpression</Operator>
                <Pattern>(?i)DCKerberos</Pattern>
              </RegExExpression>
            </Expression>
          </MembershipRule>
        </MembershipRules>
      </DataSource>
    </Discovery>
```

RDP enrollment templates

Verify if applicable for your environment.
Adjust template name(s) to adjust pattern for group members



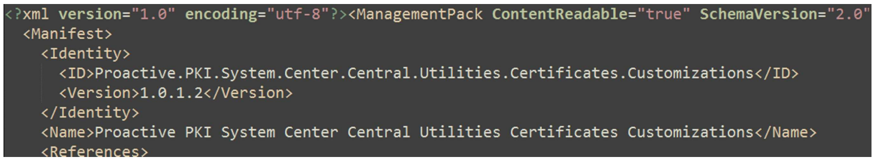
```
    <Discovery ID="Proactive.RDPAuth.Computer.Certificates.Group.DiscoveryRule" Enabled="true" Target="Proactive.RDPAuth.Computer.Certificates.Group" ConfirmDelivery="false" Remotable="true" Priority="No
      <Category>Discovery</Category>
      <DiscoveryTypes>
        <DiscoveryRelationship TypeID="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities" />
      </DiscoveryTypes>
      <DataSource ID="GroupPopulationDataSource" TypeID="SC!Microsoft.SystemCenter.GroupPopulator">
        <RuleId>$MPElement$</RuleId>
        <GroupInstanceId>$MPElement[Name="Proactive.RDPAuth.Computer.Certificates.Group"]$</GroupInstanceId>
        <MembershipRules>
          <MembershipRule>
            <MonitoringClass>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]$</MonitoringClass>
            <RelationshipClass>$MPElement[Name="MSIGL!Microsoft.SystemCenter.InstanceGroupContainsEntities"]$</RelationshipClass>
            <Expression>
              <RegExExpression>
                <ValueExpression>
                  <Property>$MPElement[Name="Utilities!SystemCenterCentral.Utilities.Certificates.Certificate"]/TemplateName$</Property>
                </ValueExpression>
                <Operator>MatchesRegularExpression</Operator>
                <Pattern>(?i)RDPAuth|RemoteDesktop</Pattern>
              </RegExExpression>
            </Expression>
          </MembershipRule>
        </MembershipRules>
      </DataSource>
    </Discovery>
```

Update PKI pack for import

Utilize this section if changes required for updating group overrides with GUIDs from environment.

Version the pack

Update pack version, increment by last octet



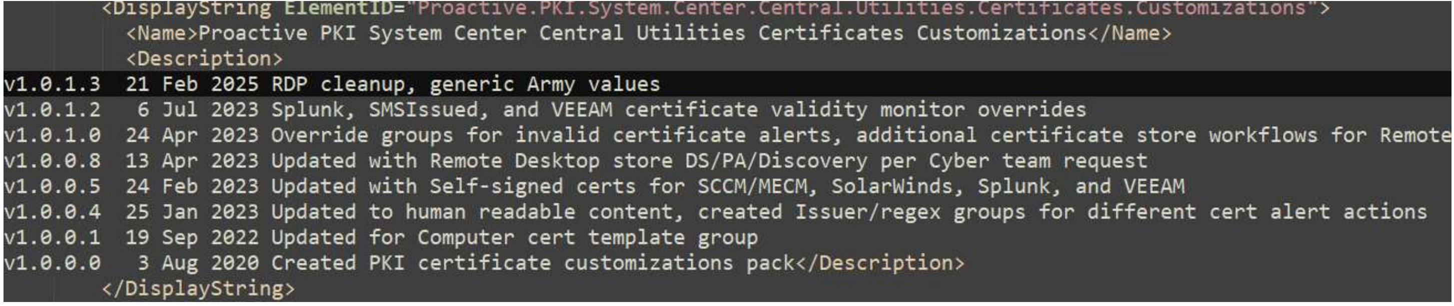
```
<?xml version="1.0" encoding="utf-8"?><ManagementPack ContentReadable="true" SchemaVersion="2.0"
  <Manifest>
    <Identity>
      <ID>Proactive.PKI.System.Center.Central.Utilities.Certificates.Customizations</ID>
      <Version>1.0.1.2</Version>
    </Identity>
    <Name>Proactive PKI System Center Central Utilities Certificates Customizations</Name>
    <References>
```

Update DisplayStrings description for pack

Scroll down to DisplayStrings section, to update description with the version and what was changed.

NOTE Description shows in the Installed Management Packs Description column

Example DisplayName Description screenshot from Notepad++



```
        <DisplayString ElementID="Proactive.PKI.System.Center.Central.Utilities.Certificates.Customizations">
          <Name>Proactive PKI System Center Central Utilities Certificates Customizations</Name>
          <Description>
v1.0.1.3  21 Feb 2025 RDP cleanup, generic Army values
v1.0.1.2   6 Jul 2023 Splunk, SMSIssued, and VEEAM certificate validity monitor overrides
v1.0.1.0  24 Apr 2023 Override groups for invalid certificate alerts, additional certificate store workflows for Remote
v1.0.0.8  13 Apr 2023 Updated with Remote Desktop store DS/PA/Discovery per Cyber team request
v1.0.0.5  24 Feb 2023 Updated with Self-signed certs for SCCM/MECM, SolarWinds, Splunk, and VEEAM
v1.0.0.4  25 Jan 2023 Updated to human readable content, created Issuer/regex groups for different cert alert actions
v1.0.0.1  19 Sep 2022 Updated for Computer cert template group
v1.0.0.0   3 Aug 2020 Created PKI certificate customizations pack</Description>
        </DisplayString>
```

Save pack to local non-system disk repository > import into SCOM