PKI Certificate Validation Management Pack Guide for Operations Manager

Published: *November 2019*

Version: *1.4.3.0*

Copyright

Terms of Use

All management packs should be thoroughly tested before being introduced into a production Operations Manager environment. The author of this management pack accepts no responsibility or liability for negative impact as a result of use of this management pack in your Operations Manager environment.

Contents

PKI Certificate Validation Management Pack Guide

The PKI Certificate Validation Management Pack monitors PKI certificates and certificate revocation lists (CRLs) stored locally in a computer's and WinNT services' personal certificate store. The Management Pack checks the lifetime of certificates and if they have become invalid due to another reason like revocation or an invalid trust. CRLs are being monitored for being updated in a timely manner.

Document Version

This guide was written based on the *1.4.3.0* version of the PKI Certificate Validation Management Pack.

A word about the 2014 re-release

The PKI Certificate Validation Management Pack has not seen an update for almost two years. While the previous release was fully functional even on the latest Windows OS and with Operations Manager 2012 R2, it based on VBScript parsing the command line output of certutil.exe. Bringing with it drawbacks like limited support for system locales, relatively high memory usage plus it had become difficult to maintain and test the code.

With the years passed I believe it is safe to re-release this management pack on a *PowerShell / .NET certificate provider* base instead of the old VBScript approach. Working with objects rather than just strings hugely simplifies the script logic for the monitoring workflows. Plus, I took the time to re-build the MP from scratch as a Visual Studio Authoring Extension project. Such the MP's code will be much easier to maintain and support.

Functionally this re-release matches the previous versions, while finally opening the MP up for any Windows system locale on this planet. A few new overrides allow changing the certificate validation parameters for *very* specific use cases.

However; no longer supported are Operations Manager 2007 / 2007 R2 and agents not having at least PowerShell 2.0 / .NET 2.0 installed. Please refer to the *Supported Configurations* section later in this guide for details.

Happy monitoring!

March 2014 – Raphael Burri

Revision History

Release Date	Changes
August 29, 2009	Original release of this guide MP version **1.0.0.241**
September 8, 2009	**V 1.0.0.260** • added support of non-standard DWH database name • ignores archived certificates • fixes discovery issue on Spanish Windows Server 2008 • non-remotable rules are not targeted at agentless or virtual cluster nodes any longer
February 16, 2010	**V 1.0.0.270** • By default no discovery of root certificates in personal computer stores (avoids alerts due to self-signed certificates).
April 19, 2010	**V 1.0.0.280** • corrects interpretation of Issuer / Issued to discovery filters • corrects certificate timestamps being picked up from certificate context • Fixes DHW SP upgrade issues that could appear when the MP was used on OpsMgr 2007 SP1. • Removes support for RTM. At least SP1 is required.
June 17, 2010	**V 1.0.0.288** • Increase default intervals of script based discoveries and monitors • Allow discovery and monitor scheduling overrides. Details in the Discover superseded Certificates • Starting with v1.4.2.0, the MP does no longer discover renewed (superseded) certificates by default. It takes Subject, SANs, Issuer, EKUs and Template into consideration. If several certificates with matching properties are found an, it does only add the most recent one (Valid To Date) to SCOM. By overriding the setting "Ignore Superseded Certificates" on the store discovery to "False", the MP is returning to its previous behaviour of adding all certificates that match the filters. Disable Monitoring for individual certificates If excluding certificates from being discovered by means of filters on properties is not feasible, monitoring of individual certificates may be suspended by adding the string "_DoNotMonitor" to the end of a certificate's Friendly Name. All monitoring for a certificate tagged with "_DoNotMonitor" will be suspended via a pre-defined override, once a discovery cycle completes. The MP features two agent tasks (ENABLE/DISABLE Certificate for Monitoring) that will append respectively

Release Date	Changes
	remove the "_DoNotMonitor" string. For more details, refer to the Tasks section later in this guide.
	• Overriding section of this guide.
	• Added public Certificate Store discovery datasource. May be used to add custom certificate stores in extension MPs.
	• Alert text and context of the Certificate Expiry Monitor clearly indicate when not the certificate but its chain has a time issue.
	• Improved Windows 2000 compatibility.
	• Windows Server 2003 WinNT service store workaround.
August 25, 2010	**V 1.0.0.289**
	• Fixes an issue which would break discovery workflows when having more than 5 certificates in a single store and script debugging switched on.
January 6, 2011	**V 1.0.1.15**
	• Broke upgrade path to avoid potential agent stale issues when upgrading from V 1.0.0.280 or earlier.
	• Changed alert priority to 'Low'.
	• Improved discovery of Issued to and Issued by properties: Will use Subject Alternative Name if certificate doesn't have a subject and will correctly extract the subject if CN= isn't encountered on the first line of the subject string.
	• Additional certificate property: CA Version (based on extension szOID_CERTSRV_CA_VERSION). If this property holds a value, that certificate is normally issued by a Windows CA.
	• Does no longer discover superseded CA certificates. Evaluation is based on the CA Version property. Additional override to change that behavior if required.
	• Monitors will not mark superseded CA certificates as expired if their discovery is enabled.
	• Made script timeout an overridable parameter. See chapter overriding timing.
March, 14, 2012	**V 1.0.1.20**
	• Fixed broken CA certificate version discovery on international systems
	• Corrected a few spelling issues in the language pack
March 31, 2014	**V 1.2.0.210**
	• **MP completely re-written**. Main monitoring workflows migrated to PowerShell, using .NET certificate provider.
	• Dropped support for SCOM 2007 and agents without PowerShell / .NET.
	• **Minimal requirements**: SCOM 2012 / Agents with PowerShell 2.0 & .NET 2.0 (Server 2012 R2 / 2012 / 2008 R2 / 2008 / 2003 SP2 respectively Windows 8.x / 7 / Vista / XP)
	• Any system locale supported
	• New overrides allow changing certificate validity checking behavior.
	• Added a dashboard view showing all certificate and CRL issues

Release Date	Changes
July 04, 2014	**V 1.2.1.3** • **Discovery filter with include and exclude regular expression** on certificate subject as well as on certificate and CRL issuer. • **Discovery filter on "Enhanced Key Usage".** By default the MP does no longer discover MS Network Access Protection certificates (napHealthyOid and napUnhealthyOid). Other OIDs may be excluded as well. • PowerShell compatibility monitor got triggered on 2012 (when no PoSh 1.0 key existed). • Using 1st certificate SAN as subject in case the subject is empty (not defined).
May 07, 2015	**V 1.3.0.0** • **Added Tasks:** Archive Certificate, List Certificate Properties, Disable/Enable Monitoring, Rediscover* • **Added Recoveries:** Archive Certificate, Disable Monitoring • **Added Discovery:** Web Hosting certificate store (Server 2012 / 2012 R2) • **Additional certificate property**: Certificate Template. It is also listed on reports. • **Discovery filter expanded** to certificate template. • **Alert description:** Additional details on the certificate chain and SCOM action account used. • **CRL Lifetime Monitor:** Threshold is exposed as an overridable parameter. • **CRL health roll up** monitor added**.** • **Expiring certificate view & report:** Default threshold of 1 month may be overridden. • **Views:** Changed criteria on views to make them more reliable when using user scopes. • **Reporting bug:** Certificate inventory did not list all certificates. • **Additional MP:** Rediscovery Tasks. Immediate trigger of store content discovery after archive, disable/enable or rediscover tasks
September 16, 2018	**V 1.4.2.0** • **Additional Certificate Properties:** Subject Alternative Name List and Enhanced Key Usage List • **Additional Certificate Discovery Filter:** include based on Enhanced Key Usage. Note: Exclude was already present. • **Do only discover most recent certificate:** The MP does discover only the newest (valid the longest time) certificate with matching Subject, SANs, EKUs, Template and Issuer. • **Disable CRL discovery:** As CRL monitoring is a specific use case, the new default setting does no longer add CRLs to the repository. • **Additionally Tested**: SCOM 1801 / 1807 and locked down agent runas accounts
November 2019	**V 1.4.3.0** • **Fixed bug**: Alert parameters not showing • Changed Alert parameters • **Fixed bug**: Variable bIgnoreSupersededCert is undefined

Table 1 - Management Pack Versions

Introduction to the PKI Certificate Validation Management Pack

PKI certificates on a computer have different uses. On servers they are most commonly used to protect web sites using SSL. In the context of Operations Manager they serve to authenticate connected agents or gateways in untrusted domains. Certificate Authorities (CAs) use their own certificates to sign the ones they issue and keep a certificate revocation list (CRL) that lists certificates that have been revoked. Each certificate is valid during a specific lifetime. When the lifetime of a certificate expires, it becomes invalid. A certificate may also become invalid if it has been revoked or the trust chain of the certificate cannot be resolved. Services making use of the certificate may stop working as expected if the certificates they are bound to are no longer valid.

The PKI Certificate Validation Management Pack helps preventing service interruptions caused by invalid certificates by alerting when:

- A certificate's lifetime is about to expire (default threshold is 21 days)
- A certificate's lifetime has ended
- A certificate has become invalid because it was revoked or the issuing CA chain could not be resolved
- A CRL has not been updated in a timely manner (default advance threshold is 0 days)

On Windows computers, PKI certificates and certificate revocation lists may be installed to a number of places. This Management Pack discovers certificates published to a computer's personal certificate store (My). CRL discovery may be activated by overrides.

 If required, certificates in the following stores of a computer may also be discovered:

- Web Hosting (WebHosting) – Windows Server 2012 and 2012 R2
- Enterprise Trust certificate store (Trust)
- Intermediate CA certificate store (CA)
- Trusted Root CA certificate store (Root)

Some software products require certificates be placed in WinNT services' certificate stores. Discovery and monitoring of certificates and CRLs in those stores is supported via overrides.

Technically all of the above stores reside in the registry of each individual computer.

The Management Pack uses Powershell and the .NET certificate provider to discover details of the certificates and CRLs. The following table lists Windows commands and tools which may be helpful when troubleshooting PKI issues.

Command / Tool	Purpose	Usage
Certificates MMC snap-in (`certmgr.msc`)	Used to add, remove, backup and check the content of certificate stores.	1. With an administrative account, start MMC.exe 2. File ❷ Add or Remove Snap-Ins 3. Add 'Certificates' 4. Depending on your needs, choose either 'Computer account' or 'Service account' If required the display of the physical certificate stores may be enabled by activating the switch in the View ❷ Options dialogue.
`CertUtil -verifystore -v My`	Lists and verifies the content of a computer's personal certificate store.	Must be run with administrative rights. Otherwise the content of the user's store is being displayed.

`CertUtil -verifystore -v -service -service [WinNT Service]\My`
 	
Example *(Hyper-V Management Service)*:
`CertUtil -verifystore -v -service -service VMMS\My`
	Lists and verifies the content of a WinNT service's certificate store	Not supported on Windows XP or Server 2003.

`Powershell Certificate Provider`
 	
Example:
`PS> ls cert:\localmachine\my`
	Manage certificate in the local certificate stores of computers and users.	Does not support service stores and CRLs.

Table 2 - PKI Commands and Tools

Getting the Latest Management Pack and Documentation

You can find the PKI Certificate Validation Management Pack in the GitHub repository at
https://github.com/rafabu/SCOM-PKICertificateMP/releases

Supported Configurations

The PKI Certificate Validation Management Pack for System Center Operations Manager supports the following agent configurations:

Agent Operating System	Remarks
Windows Server 2019 Windows Server 2016 Windows Server 2012 (including R2)	• Web Hosting store supported • Core is supported
Windows Server 2008 R2	
Windows Server 2008	• PowerShell >= 2.0 must be installed
Windows Server 2003	• PowerShell 2.0 must be installed • The hotfix KB 938397: Applications that use the Cryptography API cannot validate an X.509 certificate might be required, for compatibility with certain certificates.
Windows 10	
Windows 8.x	
Windows 7	
Windows Vista	• PowerShell 2.0 must be installed
Windows XP	• PowerShell 2.0 must be installed

Table 3 - Management Pack Compatibility

Important: Remote agent scenarios are not supported. If the management pack is run against agent computers lacking the minimum requirements, no certificates and CRLs will be discovered. Instead an alert will be written to the Operations Console.

The management pack is compatible with Operations Manager 2012, 2012 SP1, 2012 R2 , 2016, 1801 and 1807, and 2019. As with any Management Pack, it should be imported, tested and tuned in a lab or pre-production environment, before moving it to a production management group. See Terms of Use.

Getting Started

Before You Import the Management Pack

Before importing the PKI Certificate Validation Management Pack, note the following limitations of the management pack:

- no support of agentless monitoring

- legacy OS are supported when having Powershell 2.0 / .NET 2.0 installed

Files in This Management Pack

The PKI Certificate Validation Management Pack consists of the following files and directories:

- *SystemCenterCentral.Utililities.Certificates.mpb*

- *SystemCenterCentral.Utililities.Certificates.ReDiscoveryTasks.mpb (optional)*

- *SystemCenterCentral.Utililities.Certificates.QuickStartOverrides.xml (optional)*

- *Certificate MP Guide 1.4.3.0.pdf*

- *Certificate MP 1.4.3.0 Release Notes.rtf*

- Folder EXAMPLES: *SystemCenter.Utilities.Certificates.Discovery.AddOn.xml* example Management Pack.

- Folder UNSEALED: Management Pack as XML file *SystemCenterCentral.Utililities.Certificates.xml* as a reference.

How to import the Management Pack

By importing just the main or the main and the quick start override management pack files, the initial discovery behavior of the PKI Certificate Verification management pack can be adjusted to individual needs.

The discovery of all certificate stores is disabled by default. After importing the main management pack bundle file *SystemCenterCentral.Utililities.Certificates.mpb*, overrides will have to be configured to enable the discovery where required. This process is described in chapter Enabling or disabling discovery of certificate stores on page 17.

The file '*SystemCenterCentral.Utilities.Certificates.QuickStartOverrides.xml*' contains such an override. It enables discovery of the *Personal* certificate store (My) for all Windows Server targets plus the discovery of the *Web Hosting* store on Windows Server 2012 and beyond. Importing this unsealed management pack is optional and is thought to ease the process of getting started with the PKI Certificate Verification management pack in lab or pre-production environments.

The optional MP '*SystemCenterCentral.Utilities.Certificates.ReDiscoveryTasks.mpb'* adds near real time rediscovery tasks and recoveries. Note that upon importing this MP, a security warning will be displayed. This is due to SCOM management server-side actions being performed as part of the agent side tasks: Calling the 'Trigger On Demand Discovery' task.

For general instructions about importing a management pack, see [How to Import an Operations Manager Management Pack / Import a management pack from disk](http://technet.microsoft.com/en-us/library/hh212691.aspx) (http://technet.microsoft.com/en-us/library/hh212691.aspx).

Create a New Management Pack for Customizations

The Management Packs delivered as a sealed bundle (mpb file). None of the original settings in the management pack file can be changed. However, customizations, such as overrides or new monitoring objects, may be created by saving them to a different management pack. **As a best practice, a separate management pack for each sealed management pack that needs customization should be created.**

Creating a new management pack for storing overrides has the following advantages:

- **it simplifies the process of exporting customizations that were created in test and pre-production environments to the production environment**. For example, instead of exporting a default management pack that contains customizations from multiple management packs, just the management pack that contains customizations for a single management pack needs to be exported and re-imported.

- **the original management pack may be deleted without first needing to delete the default management pack.** A management pack that contains customizations is dependent on the original management pack. This dependency requires deleting the management pack with customizations before allowing deleting the original management pack. If all customizations are saved to the default management pack, the default management pack must be deleted, before it is possible to delete an original management pack.

- **it is easier to track and update customizations to individual management packs.**

Security Considerations

The PKI Certificate Services Management Pack normally requires the agent's default action account to possess administrative rights on the computer it will discover. If this is not the case (low-privilege environment), the following RunAs Profile must be configured:

Low-Privilege Scenario and RunAs Profile

In an environment where the rights of the agent action account on the computers have been restricted, the following minimum rights must be granted to the agent's default action account:

Read access to these registry keys:

- `HKLM\SOFTWARE\Microsoft\SystemCertificates`

- `HKLM\SOFTWARE\Microsoft\Cryptography\Servic`

`es` Read access to the following directory:

- `%systemroot%\temp`

Additionally, the following Run As profile must be configured.

Run As Profile	Credentials required
Certificate Verification Privileged Account	Member of the local users group Log on as a batch job (see SCOM documentation for configuring RunAs accounts)

Table 4 - Run As Profile

Understanding Management Pack Operations

Objects the Management Pack Discovers

After importing just the management pack, no discovery will take place. All root discoveries (of the certificate stores) are disabled. Normal operations will begin after having enabled the appropriate store discovery and configured the discovery filters as described in the following chapters. However; the included "quick start" override MP enables the discovery of *any* certificate contained in personal computer stores (my).

The PKI Certificate Verification Management Pack discovers the object types listed in the following table. Not all objects are automatically discovered. Use overrides to discover those that are not discovered automatically or disable discovery for the ones not required. For information about discovering objects, see 'Applying Overrides to Object Discoveries' in the Operations Guide (http://technet.microsoft.com/library/hh212759.aspx).

Category	Object Type	Discovered Automatically by Default	Object Properties
Certificate Store	Certificate Store (Registry)	Yes)* – Computer's personal store (My) No – WinNT service's store No – other local stores)* - only if the optional MP was imported: '*SystemCenterCentral.Utilities.Certificates.QuickStartOverrides.xml*'	Store Name Access Key 🔑 Provider Type Monitor Interval Discovery Interval Monitor RevocationFlag Monitor RevocationMode Monitor VerificationFlags
Certificate	Certificate (CA signed)	Yes)* – if the hosting certificate store has been discovered	Subject SAN List Issuer Valid from (UTC)
	Certificate (CA cert)	Yes)* – if in discovered Trusted Root Certification Authorities (Root), Intermediate Certification Authorities (CA) or Enterprise (Trust) stores.	Valid to (UTC) Version Signature algorithm Public key type Private key present
	Certificate (self-signed)	)* Using QuickStartOverrides.xml, no root certificates are discovered.	Friendly name Thumbprint 🔑 Serial N° Status Certificate store

				CA Certificate Version
				Certificate Template
				EKU List
Certificate Revocation Lists	Certificate Revocation List	Yes – if the hosting certificate store has been discovered		Issuer
				Version
				Signature algorithm
				This update (UTC)
				Next update (UTC)
				Entries in CRL
				Thumbprint 🔑
				Certificate store
				CRL Version
				CA Version

Table 5 - Object Types

Enabling or disabling discovery of certificate stores

In addition to the computer's personal and services stores, certificates and CRLs in additional stores may be discovered. If required, set overrides to enable or disable the appropriate discoveries. The following table lists all certificate store discovery rules included in the Management Pack:

Certificate Store	Discovery Rule Name	Default setting
Personal (My)	Discovery of local computer's personal certificate store (registry)	**(enabled)*** in QuickStartOverride
Web Hosting (WebHosting)	Discovery of local computer's Web Hosting certificate store (registry) on Windows Server 2012 and 2012 R2	**(enabled)*** in QuickStartOverride
Intermediate CA (CA)	Discovery of local computer's Intermediate CA certificate store (registry)	disabled
Trusted Root CA (Root)	Discovery of local computer's Trusted Root CA certificate store (registry)	disabled
Enterprise Trust (Trust)	Discovery of local computer's Enterprise Trust certificate store (registry)	disabled
WinNT services	Discovery of local computer's WinNT service certificate stores	disabled

Table 6 - Certificate Store Discoveries

Enabling discovery of the Trusted Root, Intermediate CA or Enterprise Trust stores is recommended only if specific requirements make it necessary. Seeing expired or invalid certificates in these stores does not necessarily indicate an issue. Also see the following chapter: **Root Certificates required by Windows**.

The example describes how to enable the discovery of the Intermediate CA certificate store for a specific computer:

1. In the Authoring pane, expand **Management Pack Objects**, and then click **Object Discoveries**.
2. On the Operations Manager toolbar, click **Scope**, and then filter the objects that appear in the details pane to include only **Certificate Store** objects.
3. From the list of discoveries, highlight the discovery **Discovery of local computer's Intermediate CA certificate store (registry).**
4. On the Operations Manager toolbar, click **Overrides**, click **Override the Object Discovery**, and then click **For a specific object of class: Health Service.**
5. Select the HealthService of the computer you plan to enable the discovery for.
6. In the **OverridesProperties** dialog box, click the **Override** box for the **Enabled** parameter.
7. Under **Management Pack**, click **New** to create an unsealed version of the management pack, and then click **OK**, or select an unsealed management pack that you previously created in which to save this override. As a best practice, you should not save overrides to the Default Management Pack.

After altering the override setting, the certificate store will be automatically discovered and will appear in the Monitoring pane under Certificate Stores Availability. After a few hours, certificates and CRLs in that store will also be discovered.

Root Certificates required by Windows (legacy information)

Certain root certificates in the *Trusted Root CA* and *Third-Party Root Certification Authorities* stores are required by the operating system. Under no circumstance must they be removed - even if their lifetime has expired. The full list of required root certificates is found in KB Article 293781 (http://support.microsoft.com/kb/293781).

Most of those reside in the *Third-Party Root Certification Authorities (AuthRoot)* certificate store. More recent Windows versions feature auto-update functionality on this store. Hence discovery and monitoring of this store is no longer part of this management pack.

However, if any of the certificates mentioned in KB 293781 should have been discovered, verification will be turned off by an override in the sealed management pack. They will also not be listed in the Expiring, Expired or Invalid Certificate views and reports.

> **NOTE:**
> *Never remove any Root Certificates listed in Knowledge Base Article 293781 from their certificate stores.* They are required by the operating system even if some of them have expired.

Configure which certificates and CRLs are discovered

When a Certificate Store is being discovered, Certificates and Certificate Revocation Lists contained in the store will be discovered soon after. The default discovery settings will discover all certificates and CRLs in a certificate store.

It is possible to configure the discovery to add only objects with certain properties to Operations Manager's repository.

To filter objects, set overrides incorporating regular expressions to the appropriate discoveries *of the certificate stores*. The following table lists the discovery rules included in the Management Pack:

Discovery Rule Name	Overridable Parameters	Default Setting
Discovery of local computer's certificate store "*My / Personal*" (registry) Discovery of local computer's Web Hosting certificate store (registry) Discovery of local computer's Intermediate CA certificate store (registry) Discovery of local computer's Trusted Root CA certificate store (registry) Discovery of local computer's Enterprise Trust certificate store (registry)	Subject Filter - Include (RegEx)	^.*$
	Subject Filter - Exclude (RegEx)	^$
	Issuer Filter - Include (RegEx)	^.*$
	Issuer Filter - Exclude (RegEx)	^$
	Certificate Template Filter – Include (RegEx)	^(|.+)$
	Certificate Template Filter – Exclude (RegEx)	\s+
	Enhanced Key Usage Filter -Include (RegEx)	^(|.+)$
	Enhanced Key Usage Filter - Exclude (RegEx)	^1\.3\.6\.1\.4\.1\.311\.47\.1\.(1|3)$
	Ignore Superseded Certificates	true
Discovery of local computer's WinNT service certificate stores	Subject Filter - Include (RegEx)	^.*$
	Subject Filter - Exclude (RegEx)	^$
	Issuer Filter - Include (RegEx)	^.*$
	Issuer Filter - Exclude (RegEx)	^$

Discovery Rule Name	Overridable Parameters	Default Setting
	Certificate Template Filter – Include (RegEx)	^(|.+)$
	Certificate Template Filter – Exclude (RegEx)	\n
	Enhanced Key Usage Filter -Include (RegEx)	^(|.+)$
Discovery Rule Name	**Overridable Parameters**	**Default Setting**
	Enhanced Key Usage Filter - Exclude (RegEx)	^1\.3\.6\.1\.4\.1\.311\.47\.1\.(1|3)$
	Ignore Superseded Certificates	true

Table 7 - Certificate and CRL Discovery Overrides at certificate store discoveries

The example below describes how to filter the discovery of certificates and CRLs in the local computer's personal store. Only certificates with an issuer property of "CN=MYISSUINGCA, DC=DOMAIN, DC=EXT" will be discovered:

1. In the Authoring pane, open **Management Pack Objects**, and click **Object Discoveries**.
2. On the Operations Manager toolbar, click **Scope**, and then filter the objects that appear in the details pane to include only **Certificate Store** objects.
3. From the list of discoveries, highlight the discovery **Discovery of local computer's certificate store "My / Personal" (registry).**
4. On the Operations Manager toolbar, click **Overrides,** click **For all objects of another class**. Choose **Windows Computer.**
5. In the **OverridesProperties** dialog box, click the **Override** box for the **Issuer Filter - Include (RegEx)** parameter.
6. Replace the default value (^.*$) with **CN=MYISSUINGCA, DC=DOMAIN, DC=EXT** to ensure that only certificates with exactly an *Issuer* property value of "CN=MYISSUINGCA, DC=DOMAIN, DC=EXT" will be discovered.
7. Under **Management Pack,** click **New** to create an unsealed version of the management pack, and then click **OK**, or select an unsealed management pack that you previously created in which to save this override. As a best practice, you should not save overrides to the Default Management Pack.

Excluding certificates and CRLs is easily possible by configuring the *Subject Filter - Exclude (RegEx)* and *Issuer Filter - Exclude (RegEx)* overrides. Matching is case insensitive, "Include" AND NOT "Exclude".

The same logic applies to certificate templates. Using the appropriate overrides it is possible to filter by specific template names or OIDs (e.g. auto enrollment certificates). If not overridden, the MP will discover any certificate, regardless whether it has a template property or not.

Additionally, it is possible to exclude certificates with specific enhanced key usage OIDs. By default, the MP will ignore System Health certificates as issued by IPSec Network Access Protection (napHealthyOid and napUnhealthyOid).

More details on Regular Expression support in Operations Manager can be found on in the document [Regular expression support in System Center Operations Manager](http://support.microsoft.com/kb/2702651/en-us) (http://support.microsoft.com/kb/2702651/en-us)

Discover superseded Certificates

Starting with v1.4.2.0, the MP does no longer discover renewed (superseded) certificates by default. It takes Subject, SANs, Issuer, EKUs and Template into consideration. If several certificates with matching properties are found an, it does only add the most recent one (Valid To Date) to SCOM.

By overriding the setting "Ignore Superseded Certificates" on the store discovery to "False", the MP is returning to its previous behaviour of adding all certificates that match the filters.

Disable Monitoring for individual certificates

If excluding certificates from being discovered by means of filters on properties is not feasible, monitoring of individual certificates may be suspended by adding the string "_DoNotMonitor" to the end of a certificate's Friendly Name.

All monitoring for a certificate tagged with "_DoNotMonitor" will be suspended via a predefined override, once a discovery cycle completes.

The MP features two agent tasks (ENABLE/DISABLE Certificate for Monitoring) that will append respectively remove the "_DoNotMonitor" string. For more details, refer to the Tasks section later in this guide.

Overriding timing on discovery and monitoring

Great care has been taken to reduce the impact of this Management Pack on the monitored systems. Due to this reason, altering the default discovery and monitoring intervals for certificates and CRLs does require specific steps to be performed. Instead of overriding individual certificate discoveries and monitors, the intervals may be changed by overriding properties on the *certificate store* discovery. This guarantees that all Management Pack workflows will be run in sync and that only a single override needs to be configured to change the timing behavior of workflows for all certificates in each certificate store (apply Cook Down).

Type	default setting
Certificate Store Discovery Interval	Every 24 hours
Certificate Discovery Interval	Every 12 hours
Certificate Monitor Interval	Every 4 hours
Default Script Timeout	5 minutes

Table 8 – Default Intervals

The example below describes how to extend the discovery interval to 24 and the monitoring intervals to 12 hours for all certificates found in Personal Certificate Stores:

1. In the Authoring pane, expand **Management Pack Objects**, and then click **Object Discoveries**.
2. On the Operations Manager toolbar, click **Scope**, and then filter the objects that appear in the details pane to include only **Certificate Store** objects.
3. From the list of discoveries, highlight the discovery **Discovery of local computer's personal certificate store (registry).**
4. On the Operations Manager toolbar, click **Overrides,** click **For all objects of class: Health Service**.
5. In the **Override Properties** dialog box, click the **Override** box for the **Certificate Monitor Interval** parameter.
6. Replace the default value (14110) with **43200** to raise the monitor interval to 12 hours.
7. In the **Override Properties** dialog box, click the **Override** box for the **Certificate Discovery Interval** parameter.
8. Replace the default value (42330) with **86400** to raise the discovery interval to 24 hours.
9. Under **Management Pack**, click **New** to create an unsealed version of the management pack, and then click **OK**, or select an unsealed management pack that you previously created in which to save this override. As a best practice, you should not save overrides to the Default Management Pack.

Note that the overridden frequencies will be reflected by the **certificate store's** properties after the next certificate store discovery interval has passed. Only then will the certificate discoveries and monitors change their frequencies. Typically, a delay of approximately 24 hours is to be expected until the new configuration is in place.

Changing certificate validation properties

Highly specific monitoring requirements may make it necessary to change the default certificate verification behavior. The core monitoring script tests the validity of each certificate by building the certificate chain and checking it for revocation. The following default policy applies:

- Revocation Flag: Check the entire chain for revoked certificates *(EntireChain)*
- Revocation Mode: Attempt to check online for revoked certificates *(Online)* • Verification Flags: Ignore unknown revocation *(IgnoreCertificateAuthorityRevocationUnknown,IgnoreEndRevocationUnknown)*

By setting string overrides on the certificate store discovery rule(s), the verification policy *for all certificates* in a given store can be altered. The following table lists valid override values:

Override	Values	Remarks
RevocationFlag	EndCertificateOnly **EntireChain** ExcludeRoot	
RevocationMode	NoCheck Offline **Online**	
VerificationFlags	AllFlags AllowUnknownCertificateAuthority **IgnoreCertificateAuthorityRevocationUnknown** IgnoreCtlNotTimeValid IgnoreCtlSignerRevocationUnknown **IgnoreEndRevocationUnknown** IgnoreInvalidBasicConstraints IgnoreInvalidName IgnoreInvalidPolicy IgnoreNotTimeNested IgnoreNotTimeValid IgnoreRootRevocationUnknown IgnoreWrongUsage NoFlag	If anything else than "AllFlags" or "NoFlags" is required, the flag strings have to be provided as comma separated list as in the following example: IgnoreNotTimeNested,IgnoreInvalidPolicy

Table 9 – Certificate Verification Overrides

For details on the revocation and verification flags, refer to the following MSDN library links:

- X509RevocationFlag Enumeration:
  http://msdn.microsoft.com/library/system.security.cryptography.x509certificates.x509revocationflag%28v=vs.80%29.aspx
- X509RevocationMode Enumeration:
  http://msdn.microsoft.com/library/system.security.cryptography.x509certificates.x509revocationmode%28v=vs.80%29.aspx
- X509VerificationFlags Enumeration:
  http://msdn.microsoft.com/library/system.security.cryptography.x509certificates.x509verificationflags(v=vs.80).aspx

Note that due to restrictions in Operations Manager, it is not possible to check the validity of the string overrides when an administrator changes them. Should invalid verification overrides have been configured, the default monitoring settings will be used instead. Additionally, the *Certificate Verification Overrides* monitor will raise an alert.

Changing the default Certificate Expiry threshold

A 3 steps approach on expiring certificates is implemented by the management pack. A certificate that will expire will:

1. Become visible in both the "Certificates – About to Expire" view and on the "Expiring Certificates Report". This happens *31 days (one month)* before the certificates expires.
2. Trigger a warning health change accompanied with an alert by the "Certificate Lifespan Monitor". By default *21 days (3 weeks)* before the expiry.
3. Change the health state of the "Certificate Lifespan Monitor" to Critical when the certificate has expired. *Due to the nature of SCOM's 3-state monitor implementation, no fresh alert will be generated at that point.*

Both thresholds may be configured if required.

The *visual* threshold of 1 month for views and reports is configured on the following discovery rules:

Discovery	Override
Discover Non-CA Certificates (locally)	Expires Soon Threshold Days (Views/Reports)
Discover CertificateAuthority Certificates (locally)	
Discover Self-Signed Certificates (locally)	

Table 10 – Certificate Discoveries

The *monitor/alert* threshold of 3 weeks may be changed by overriding the monitor "Certificate Lifespan Monitor". See Certificate Lifespan Monitor on page 28 for details.

Classes

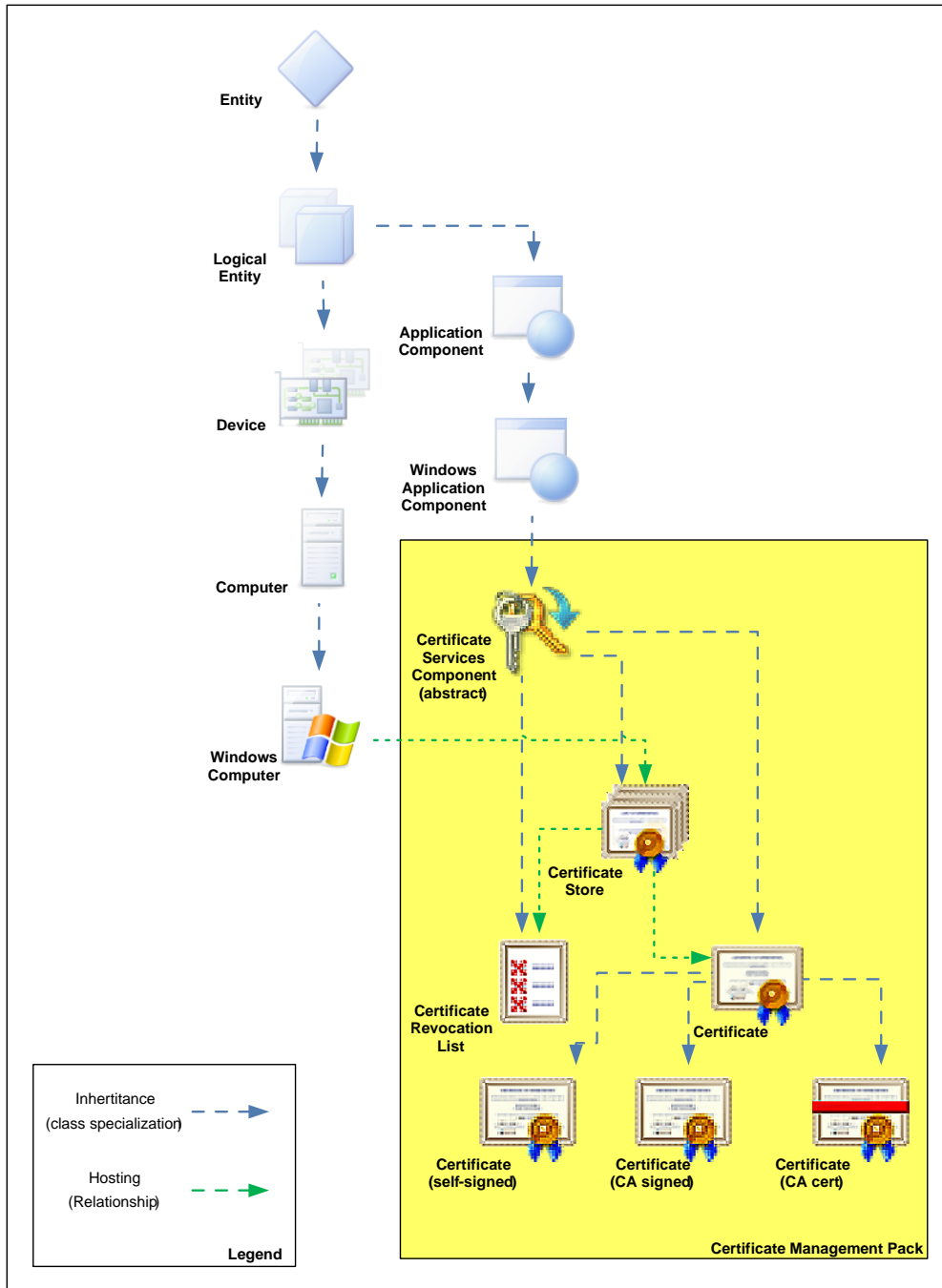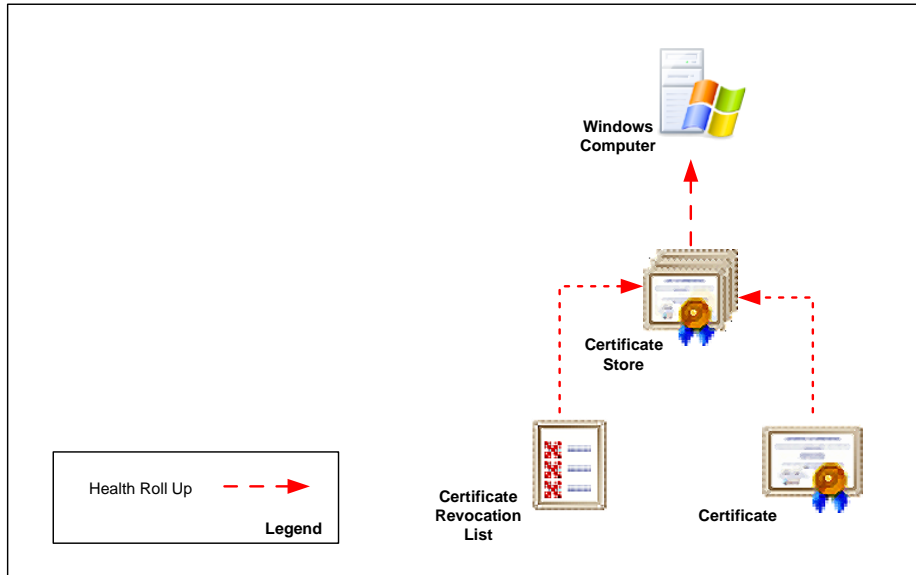The following diagram shows the classes defined in this management pack.

Figure 1 - Class Diagram

Health Roll Up

The health of certificates and CRLs rolls up to the certificate store and from there to the computer object. Such the health of the computer is made dependant on the health of its PKI components as illustrated in the diagram below.

Figure 2 - Health Roll Up

Disable Health Roll Up

If the default behavior of rolling the health of certificate and CRL objects up to the computer is not desired, the dependency monitors can be disabled using overrides. The following table lists the three dependency monitors:

Dependency Monitor Name	Source	Target
Certificate Store Roll Up	Windows Computer	Certificate Store
Certificates Roll Up	Certificate Store	Certificate
CRL Roll Up	Certificate Store	CRL

Table 11 – Dependency Monitors

Monitors and Alerts

Monitors in the PKI Certificate Validation Management Pack are targeted at Certificate, Certificate Revocation List, Certificate Store and Windows Operating System object classes.

Certificate Monitors

Two configuration monitors are targeted at certificate objects. They alert if a certificate has become invalid or its lifetime is about to expire.

Figure 3 - Certificate Monitors

Certificate Lifespan Monitor

The three state monitor alerts if a certificate's life span has expired. Additionally it raises a warning 21 days before the expiration date. Such a certificate may be renewed or replaced before service interruptions occur. If a certificate has become invalid due to another reason, this monitor will show 'Success' even if the certificate's lifetime has expired as the Certificate Validity monitor is taking care of that situation. The 21 day threshold of the warning condition may be easily adjusted using the override described below.

Severity	Priority	Alert Name	Override Name	Implementation Details
Warning or Critical	Low	Certificate lifespan alert Sample alert: The certificate has expired on 31.15.2002 09:00. Certificate Subject: CN=devscomrpt Certificate Issuer: CN=MyCA Serial number: 198b11d13f9a8ffe69a0 Certificate Valid to: 2023-01-01 12:00 Serial number: 1da9ead400000000003f Enterprise Template: n/a Enhanced Key Usage List: 1.3.6.1.5.5.7.3.1 Store: LocalMachione\My Chain Details: --- Certificate Status --- Revoked: The certificate is revoked. ---Chain Status Overview --- Level 0: DevSCOM-SubCa: IsVerified	Lifetime threshold (days) Default: 21 days	Calculates how many days are left until the certificate expires by evaluating the 'Valid to' property of a certificate

Table 12 - Certificate Lifespan Monitor Details

Note that the monitor is disabled for certain root certificates. See *Root Certificates required by Windows* on page *18* for details.

Certificate Validity Monitor

The two-state monitor warns if a certificate has become invalid due to a reason other than its lifetime having expired (revoked, invalid trust, unknown signature etc.). If the certificate has expired, this monitor will show 'Success' since the Certificate Lifespan monitor will alert the condition.

Severity	Priority	Alert Name	Possible Overrides	Implementation Details
Warning	Low	Certificate validity Sample alert: The certificate is not valid. Reason: Revoked: The certificate is revoked Certificate Subject: CN=devscomrpt Certificate Issuer: CN=MyCA Certificate Valid to: 2023-01-01 12:00 Serial number: 1da9ead400000000003f Enterprise Template: n/a Enhanced Key Usage List: 1.3.6.1.5.5.7.3.1 Store: LocalMachione\My Chain Time Details: --- Certificate Status --- Revoked: The certificate is revoked. ---Chain Status Overview --- Level 0: DevSCOM-SubCa: IsVerified Level 1: DEVSCOM-ENTER: IsVerified	Only standard	Evaluates the certificate's 'Status' property

Table 13 - Certificate Validity Monitor

Note that the monitor is disabled for certain root certificates. See *Root Certificates required by Windows* on page *18* for details.

Certificate Revocation List Monitor

A single configuration monitor is targeted at CRL objects.

Figure 4 – Certificate Revocation List Monitor

CRL Update Monitor

The two-state monitor warns if a CRL has not been updated by its 'Next update' date.

Severity	Priority	Alert Name	Possible Overrides	Implementation Details
Warning	Low	CRL Update Sample alert: The certificate revocation list DEVSCOMAD1 has not been updated. Update was required by: 15.07.2009 10:53 Certificate store: LDAP CDP	NextUpdateThreshold (Days) Default: 0 days	Evaluates the CRL's 'Next update' property

Table 14 - CRL Update Monitor

Certificate Store Monitor

In the context of each discovered certificate store, an event driven monitor checks if the certificate verification overrides configured are valid.

Figure 5 – Certificate Verification Overrides Monitor

Certificate Verification Overrides Monitor

By defining overrides against the certificate store discovery rule, the default certificate verification behavior may be changed. This monitor alerts if invalid override values were set. In this case the certificate validation workflows will continue to use the default values.

Severity	Priority	Alert Name	Possible Overrides	Implementation Details
Warning	Normal	Invalid PKI certificate monitoring override(s) configured Sample alert: PKI certificate monitoring and discovery overridable parameters RevocationFlag, RevocationMode or VerificationFlags in the context of this certificate store are not valid. Default values are being used instead.	Only standard	Windows event monitor, triggering on the output of the certificate discovery script.

Table 15 - Certificate Monitoring Compatibility Monitor

Refer to "Changing certificate validation properties" on page 20 for details on the configuration of RevocationFlag, RevocationMode and VerificationFlags overrides.

Operating System Monitor

A single monitor is targeted at the Windows Operating System object. It alerts should a computer not be compatible with the PKI Certificate Verification management pack.

Figure 6 – Certificate Monitoring Compatibility Monitor

Certificate Monitoring Compatibility Monitor

The two-state event monitor warns when an agent is not compatible with this management pack since Powershell >= 2.0 is not installed locally on legacy operatings systems.

Severity	Priority	Alert Name	Possible Overrides	Implementation Details
Warning	Normal	PKI Certificate Monitoring is not possible Sample alert: PowerShell is not installed on this computer or the installed version is not compatible with PowerShell 2.0. In order to monitor PKI Certificates, install the appropriate PowerShell environment (>= Version 2.0).	Only standard	Windows event monitor, triggering on the output of the certificate discovery script.

Table 16 - Certificate Monitoring Compatibility Monitor

In order to discover and monitor certificates on Windows Server 2008, Windows Server 2003 or Windows XP, PowerShell 2.0 respectively 3.0 may be installed by downloading the appropriate install package from Microsoft.

On Windows Server 2008 R2 respectively Windows 7 and later, PowerShell is part of the core operating system.

Console Views

Objects discovered and monitored by the PKI Certificate Validation Management Pack can be seen in various console views in the following folder: *PKI Certificate Validation*
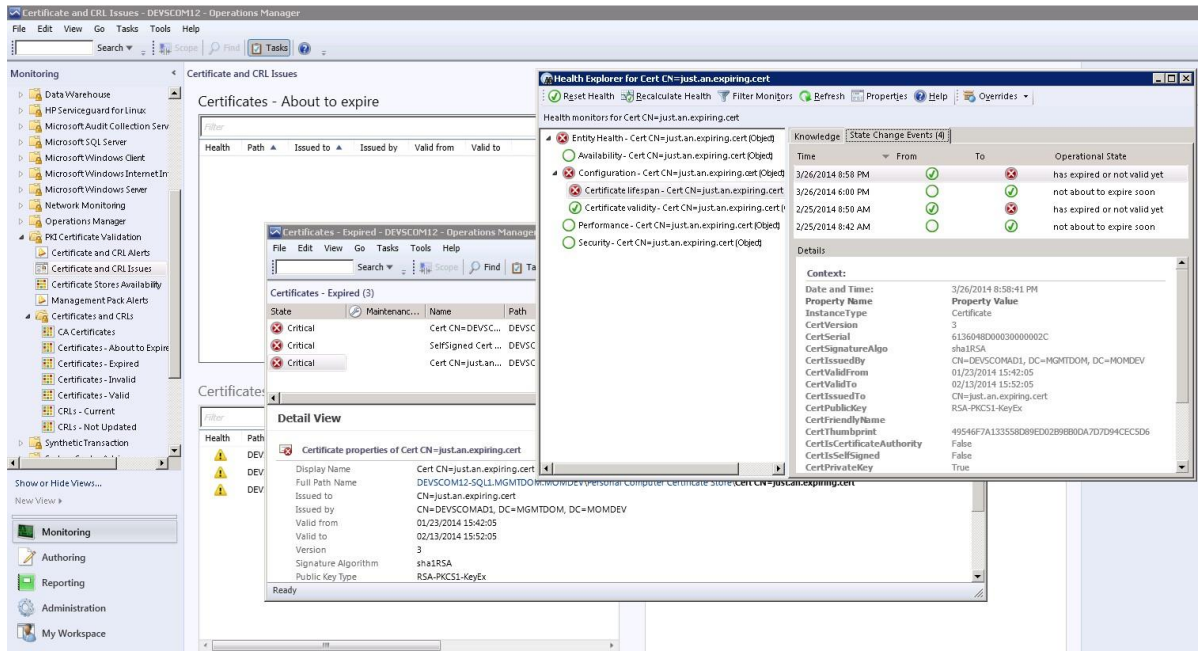

Figure 7 – Monitoring Console View

The following table lists the predefined views that are included in the PKI Certificate Verification Management Pack:

Console View Name	Console View Folder	Description
Certificate and CRL Alerts	PKI Certificate	Alert view: All current alerts concerning certificates or certificate revocation lists.
Certificate and CRL Issues	PKI Certificate	Dashboard showing four state views: - Certificates about to expire - Certificates exired - Certificates invalid - CRLs not updated
Certificate Stores Availability	PKI Certificate	State view: The roll up state of all certificate stores. Shows the health of certificates and CRLs underneath. Stores not containing any monitored certificates will be shown as uninitialized (green circle without a tick).
Management Pack Alerts	PKI Certificate	Alert view: All current alerts triggered by the Certificate tool CertUtil.exe compatibility monitor. Check here for management pack compatibility issues.

Console View Name	Console View Folder	Description
CA Certificates	PKI Certificate\Certificates and CRLs	State view: Lists all certificates that have Basic Constraints of CA. Based on the *CA Certificates Group*
Certificates – Valid	PKI Certificate\Certificates and CRLs	State view: Lists all discovered certificates that are valid (neither invalid nor expired). Based on the *Valid Certificates Group*.
Certificates - Invalid	PKI Certificate\Certificates and CRLs	State view: Lists all certificates that are currently in an invalid state. Based on the *Invalid Certificates Group*.
Certificates - About to Expire	PKI Certificate\Certificates and CRLs	State view: Lists certificates that are still valid but are going to expire within a month's time (by default). Based on the *Expiring Certificates Group*. **Note**: If anything other than one month before expiry of a certificate is required, an override may be set at the corresponding certificate discovery.
Certificates - Expired	PKI Certificate\Certificates and CRLs	State view: Lists expired certificates. Based on the *Expired Certificates Group*.
CRLs – Current	PKI Certificate\Certificates and CRLs	State view: Lists Certificate Revocation Lists that are current and do not need updating. Based on the *Current CRLs Group*.
CRLs - Not Updated	PKI Certificate\Certificates and CRLs	State view: Lists Certificate Revocation Lists that have not been updated in a timely manner. Based on the *Not Updated CRLs Group*.

Table 17 – Console Views

Consider using *My Workspace* or adding views to a custom management pack if you require additional, customized views.

Using the *Distributed Application Designer*, PKI Certificate objects can be made part of custom diagram views. When adding components to a distributed application, refer to Figure 1 on page *26* for choosing correct object types.
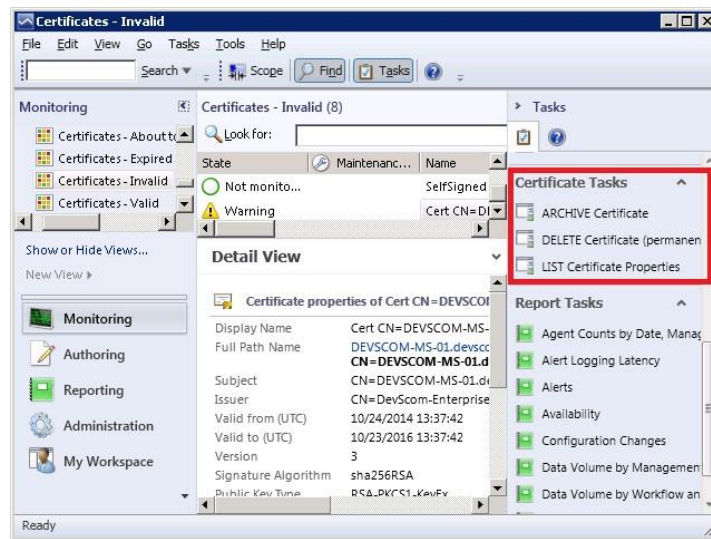
Tasks

Agent tasks to manipulate certificates on agent computers and to list their properties have been added in MP version 1.2.3.0.

> **NOTE:**
> *Great care has to be taken before deleting certificates.* The operation CAN NOT be undone and will remove both the certificate and its private key from the certificate store of the agent! For this reason, the MP does not feature a "Delete" task.

Task Name	Target	Description and Overrides
LIST Certificate Properties	Certificate Store	Will list all certificates in the given store. Override to: - Force "wide" output - Change or disable verification settings
LIST Certificate Properties	PKI Certificate	List a single certificate's properties Override to: - Force "wide" output - Change or disable verification settings
~~DELETE Certificate (permanently)~~	~~PKI Certificate~~	~~Deletes a certificate and its private key.~~
ARCHIVE Certificate	PKI Certificate	Sets the "archived" flag on a certificate. Archived certificates can no longer be used and will be excluded from monitoring. If required, the flag may be removed using PowerShell or .NET.
DISABLE Certificate for Monitoring	PKI Certificate	Appends the string "_DoNotMonitor" to the Friendly Name of a certificate. The next discovery cycle will then add the certificate to the "Monitoring Disabled" group. Monitors for the certificate will then be disabled.
ENABLE Certificate for Monitoring	PKI Certificate	If present, removes the string "_DoNotMonitor" from a certificate's Friendly Name. Monitoring will resume after the next discovery cycle completes.
REDISCOVER Certificates *	Certificate Store	Triggers 'Run On-Demand Discovery' task of all discoveries enabled for the selected stores. Discovery will be run within approximately 1 minute after the agent task has been executed.
REDISCOVER Certificates *	PKI Certificate	Triggers 'Run On-Demand Discovery' task of all discoveries enabled for the store hosting the selected certificate. Discovery will be run within approximately 1 minute after the agent task has been executed.

Certificates that were deleted or archived will be removed from the SCOM object repository upon the next discovery interval (within 12 hours by default). Likewise, it will take up to 12 hours until a DISABLE/ENABLE change is being reflected.

Figure 8 - Agent Tasks

Note: The REDISCOVER tasks are only visible if the optional "Rediscovery" MP has been imported.

Reports

A series of inventory reports are included in the PKI Certificate Validation Management Pack. They help administrators keep track of certificate and CRL configurations in the management group. It is recommended make running these reports a part of the weekly or monthly operations routine. Specifically, the *Expiring Certificates Report* will help avoiding service outages by showing certificates that are going to expire within a month's time, leaving enough time to initiate the renewal procedure. Scheduling reports can help support such a routine.

Figure 9 – Reporting Interface

Report Name	Configuration required	Description
Certificate Inventory Report	Select a *Certificate Store* object as **Group** target and select a report time range. No target configuration is required if the report is run directly in the context of a Certificate Store from the monitoring pane.	Lists certificates and their properties contained in a selected Certificate Store.
CRL Inventory Report	Select a *Certificate Store* object as **Group** target and select a report time range. No target configuration is required if the report is run directly in the context of a Certificate Store from the monitoring pane.	Lists certificate revocation lists and their properties contained in a selected Certificate Store.
Expired Certificates Report	Select a report time range.	Lists certificates that have expired. Based on the *Expired Certificates Group*. It allows scoping the report by selecting a group containing computer or certificate store objects.
Expiring Certificates Report	Select a report time range.	Lists certificates that are going to expire within a month (by default). Based on the *Expiring Certificates Group*. It allows scoping the report by selecting a group containing computer or certificate store objects. **Note**: If anything other than one month before expiry of a certificate is required, an override may be set at the corresponding certificate discovery.
Invalid Certificates Report	Select a report time range.	Lists Certificates which are invalid. Based on the *Invalid Certificates Group*. It allows scoping the report by selecting a group containing computer or certificate store objects.
Not Updated CRLs Report	Select a report time range.	Lists certificate revocation lists that have not been updated in a timely manner. Based on the *Not Updated CRLs Group*. It allows scoping the report by selecting a group containing computer or certificate store objects.

Table 18 – Reports

Troubleshooting

During discovery and monitoring the certificate store verification script 'SystemCenterCentral.Utilities.Certificates.Certificate_Verify_Script_V6.ps1' and the WinNT services certificate store discovery script 'SystemCenterCentral.Utililities.Certificates.LocalServiceStore.Discovery.vbs' write diagnostic events to the Operations Manager event log on each agent machine. These events may be helpful when having to troubleshoot the Management Pack.

EventID	Severity	Description
110	Information	Script starting certificate and CRL discovery/verification with valid overrides
111	Warning	Script starting certificate and CRL discovery/verification with invalid overrides. Default values are going to be used instead.
112	Information	Script ended. Lists how many certificates and CRLs were found.
113	Warning	Failed to access certificate store
114 (debug)	Information	Details about a certificate object
115 (debug)	Information	Details about a CRL object
119	Warning	Unable to load and extend System.Security.Cryptography.X509Certificates namespace (P/Invoke). Script will retry on the next scheduled run.
3006	Information	The WinNT service certificate store discovery script has found certificates or CRLs inside at least one service certificate store. It is writing discovery data back to SCOM in order to discover these stores.

Table 19- Script Events

Appendix: Scripts

The PKI Certificate Validation Management Pack uses a single script for discovery and monitoring of certificates and CRLs. An additional script is responsible for discovering the certificate stores containing certificates for WinNT services.

Script	Purpose	Discoveries and Monitors	Frequency
Certificate_Verify_Script_V6.ps1	Retrieve a list of all certificates and CRLs in the store with their properties and verifies the certificates. Returns that information as a property bag to SCOM.	Certificate and CRL discoveries and monitors. Cookdown is applied to minimize the number times the script is started.	every 4 hours
Certificate_Handling_Script_V3.ps1	Used by tasks. Verify certificate properties, archive, disable monitoring		
Certificate_Discovery_Trigger_V1.ps1	Writes an event to the agent's Operations Manager event log upon running a REDISCOVERY task.		
Certificate_DiscoveryDemand_Script_V1.ps1	Server side response to the REDISCOVERY task. Will evaluate overrides and run 'On-Demand Discovery' task.		
SystemCenterCentral.Utililities.Certificates.LocalServiceStore.Discovery.vbs	Reads the WinNT service certificate store registry key and returns certificate store discovery information to SCOM if either certificates or CRLs are found a service's store.	Discovery of local computer's WinNT service certificate stores.	daily
SystemCenterCentral.Utililities.Certificates.CheckPowerShellVersion.vbs	Checks if Powershell >= 2.0 is installed	Monitor alerts if an agent is not compatible with the management pack	every 12 hours

Table 20 - Management Pack Scripts

Acknowledgements

This MP would not have been possible without the help and support of the SCOM community. Namely:

Pete Zerger – from lunch at Gallipoli 2 to unfinished ZEN, South Texas beaches, steep mountains in Schwyz and for keeping an eye of the original landing pod of the pack over at SystemCenterCentral.com

Vadims Podāns – for enlightening lesser ones on the magic of P/Invoke around X509CRL2 and for his approval to use the CRL code in this MP. http://www.sysadmins.lv

Marc van Orsouw (MoW) and Joel Bennett (Jakul) for making PtrToStructure run smoothly in PoSh 3.0.

Bob, Dan, Marnix, Stan, and Tao for being patient enough during beta testing.

Swiss Federal Railways – for providing power sockets on most of their coaches. http://www.sbb.ch

Everyone else out there that reported issues, submitted feature requests and had the patience to test the pack.

Feedback

For comments on this guide or the Management Pack, the authors of the Management Pack can be contacted by leaving a comment or submit an issue on the Github project
https://github.com/rafabu/SCOM-PKICertificateMP