System Center CENTRAL

PKI Certificate Validation Management Pack Guide for Operations Manager 2007 and 2012

Published: *March2012*

Version: *1.0.1.20*

Copyright

Terms of Use

All management packs should be thoroughly tested before being introduced into a production Operations Manager environment. The authors of this management pack accept 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 *1.0.1.20* version of the PKI Certificate Validation Management Pack.

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 Overriding certificate discovery and monitoring 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.

Release Date	Changes
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 a Windows CA one. • 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 overidable parameter. See chapter Overriding certificate discovery and monitoring 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

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

On Windows computers, PKI certificates and certificate revocation lists may be installed to a number of places. This Management Pack discovers certificates and CRLs published to a computer’s personal certificate store. On Windows Vista and Server 2008, certificates in WinNT services’ certificate stores are also discovered.

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

- Enterprise Trust certificate store
- Intermediate CA certificate store
- Third-Party Root Certification Authorities
- Trusted Root CA certificate store

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

The Management Pack uses the output of the command *'CertUtil.exe'* to discover details of the certificates and CRLs. The following table lists 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 → 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 → 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.

Table 2 - PKI Commands and Tools

Getting the Latest Management Pack and Documentation

You can find the PKI Certificate Validation Management Pack in the System Center Central Management Pack Catalog (http://www.systemcentercentral.com/tabid/63/tag/Pack_Catalog+MP_Catalog/Default.aspx).

Supported Configurations

The PKI Certificate Validation Management Pack for Operations Manager 2007 and 2012 supports the following agent configurations:

Agent Operating System	Remarks	Supported OS Languages
Windows Server 2008 (including R2)		• English • Dutch • French • German • Italian • Portuguese • Spanish
Windows 7		
Windows Vista		
Windows Server 2003	• Does only support WinNT service stores with workaround described in the release notes. • 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 XP	• The appropriate version of the *'Windows Server 2003 Administration Tools Pack'* must be installed locally. • Does not support discovery and monitoring of certificates bound to WinNT service stores.	
Windows 2000 (not on SCOM 2012)	• Windows Server 2003 certutil.exe required. See Release notes. • Does not support discovery and monitoring of certificates bound to WinNT service stores.	

Table 3 - Management Pack Compatibility

Important: Remote agent scenarios are not supported. If the Management Pack is run against computers installed with a non-supported OS language, no certificates and CRLs will be discovered. Instead an alert will be written to the Operations Console.

While the Management Pack is compatible with Operations Manager 2007 SP1, it has only fully been tested against Operations Manager 2007 R2 and Operations Manager 2012. 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 agent less monitoring
- Windows XP is supported only when the *'Windows Server 2003 Administration Tools Pack'* has been installed on the agent computer
- The agent OS' language must be supported. Refer to Table 3 on page 9

Files in This Management Pack

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

- SystemCenterCentral.Utililities.Certificates.mp
- SystemCenterCentral.Utilities.Certificates.QuickStartOverrides.xml
- Certificate MP Guide 1.0.1.15.pdf
- Certificate MP 1.0.1.15 Release Notes.rtf
- Folder EXAMPLES: SystemCenter.Utilities.Certificates.Discovery.AddOn.xml example Management Pack.
- Folder EXTRAS: optional SystemCenterCentral.Utilities.Certificates.2003Service.mp WinNT service certificate store discovery Management Pack.

How to import the Management Pack

By importing just one or both management pack files, the initial discovery behavior of the PKI Certificate Verification management pack can be adjusted to individual needs.

The discovery of certificate stores is disabled by default. After importing the main management pack file *SystemCenterCentral.Utililities.Certificates.mp*, 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 14.

The file '*SystemCenterCentral.Utilities.Certificates.QuickStartOverrides.xml*' contains such overrides. They enable discovery of the personal certificate for all Windows Server 2003 and 2008 targets. It also excludes MS SMS certificates from discovery. 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.

For general instructions about importing a management pack, see How to Import a Management Pack in Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkId=142351).

Create a New Management Pack for Customizations

The Management Packs is sealed. 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. By default, Operations Manager 2007 saves all customizations to the default 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 Run As Profile must be configured.

Low-Privilege Scenario and Run As 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\Services`

Additionally, the following Run As profile must be configured accordingly or the agent will not discover the certificates and CRLs in the computer's personal store but the personal store of the agent's default action account.

Run As Profile	**Credentials required**
Certificate Verification Privileged Account	Member of the local administrators group

Table 4 - Run As Profile

Understanding Management Pack Operations

Objects the Management Pack Discovers

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 ‘Object Discoveries in Operations Manager 2007’ in Operations Manager 2007 Help (http://go.microsoft.com/fwlink/?LinkId=108505).

Category	**Object Type**	**Discovered Automatically by Default**	**Object Properties**
Certificate Store	Certificate Store (Registry)	Yes$^{)*}$ – Computer’s personal store No – WinNT service’s store (Windows Server 2008) No – other local stores)* - only if the optional MP was imported: *‘SystemCenterCentral.Utilities.Certificates.QuickStartOverrides.xml’*	Store Name Access Key 🔑 Monitor Sync Time Monitor Interval Discovery Interval
Certificate	Non-Root Certificate	Yes$^{)*}$ – if the hosting certificate store has been discovered)* - if the optional MP was imported: *‘SystemCenterCentral.Utilities.Certificates.QuickStartOverrides.xml’*	Issued to Issued by Valid from Valid to Version Signature algorithm Public key type Private key present Friendly name Thumbprint 🔑 Serial N° Status Certificate store CA Certificate Version
	Root Certificate	Yes$^{)*}$ – if in discovered Root or AuthRoot stores.)* Root certificates are only discovered when they reside in either *‘Trusted Root Certification Authorities’* or ‘*Third-Party Root Certification Authorities’* and these stores have been discovered. The default configuration does not discover any root certificates.	
Certificate Revocation Lists	Certificate Revocation List	Yes – if the hosting certificate store has been discovered	Issuer Version Signature algorithm This update Next update Entries in CRL Thumbprint 🔑 Certificate store

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
Enterprise Trust	Discovery of local computer's Enterprise Trust certificate store (registry)	disabled
Intermediate CA	Discovery of local computer's Intermediate CA certificate store (registry)	disabled
Personal	Discovery of local computer's personal certificate store (registry)	**(enabled**)*
Third-Party Root Certification Authorities	Discovery of local computer's Third-Party Root Certification Authorities certificate store (registry) **Note:** Activating this discovery will discover a large number of certificates. On each Windows computer there may be several hundred certificates stored in the Third-Party Root Certification Authorities store.	disabled
Trusted Root CA	Discovery of local computer's Trusted Root CA certificate store (registry)	disabled
WinNT services	Discovery of local computer's WinNT service certificate stores (Server 2008)	**(enabled**)*

Table 6 - Certificate Store Discoveries

Enabling discovery of the Trusted Root, Intermediate or Third-Party Root CA certificate stores is recommended only if specific requirements make it necessary. On Windows computers many expired or invalid certificates will be present in these stores but that 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 little delay certificates and CRLs in that store will also be discovered.

Root Certificates required by Windows

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).

If discovery of *Trusted Root CA* and *Third-Party Root Certification Authorities* stores is enabled, the PKI Certificate Validation Management Pack will *disable all monitors* for the root certificates mentioned in KB 293781. They will also not be listed in the Expiring, Expired or Invalid Certificate 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.

Configuration of Certificate Discovery

When a Certificate Store is being discovered, all Certificates and Certificate Revocation Lists contained in the store will be discovered soon after. If this behavior is not desired, the Certificate and CRL discoveries may be configured to add only objects with certain issuing properties to Operations Managers repository.

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

Discovery Rule Name	Overridable Parameters	Default Setting
Discover Root Certtificates (locally)	DiscoverSupersededCACertificates	false
	Issued To Filter (RegEx)	^.*$
	Issued By Filter (RegEx)	^.*$
Discover Non-Root Certtificates (locally)	DiscoverSupersededCACertificates	false
	Issued To Filter (RegEx)	^.*$
	Issued By Filter (RegEx)	^.*$
Discover Certificate Revocation Lists (locally)	Issuer Filter (RegEx)	^.*$

Table 7 - Certificate and CRL Discovery Overrides

The example below describes how to filter the discovery of non-root certificates. Only certificates issued by a CA called *MyIssuingCA* will be discovered:

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** objects.
3. From the list of discoveries, highlight the discovery **Discover Non-Root Certificates (locally).**
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 **Issued By Filter (RegEx)** parameter.
6. Replace the default value (^.*$) with **^MyIssuingCA$** to ensure that only certificates with exactly an *Issued By* property value of MyIssuingCA 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.

OpsMgr does not support negative lookahead or lookbehind in regular expressions. Nonetheless it is possible to exclude specific certificates from discovery as the following example shows. Self-Signed SMS certificates are root certificates that have an **Issued By** and **Issued To** property of 'SMS'. The regular expression to discovery any certificate but the SMS ones is:

```
^(.{0,2}|[^S][^M][^S]|.{4,})$
```

This translates into: Capture any string with 0 – 2 or more than 4 characters. Capture only strings with 3 characters that do not match 'SMS'.

More details on Regular Expression support in OpsMgr can be found on the **Error! Hyperlink reference not valid.** (www.opsmanjam.com) in the document Regular Expression Support in SCOM 2007.

Overriding certificate discovery and monitoring timing

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 overrides needs to be configured to change the timing behavior of all workflows for all certificates in a given certificate store.

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 set the discovery 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 set 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 maximum 24 hours is to be expected until the new configuration is in place.

Classes

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

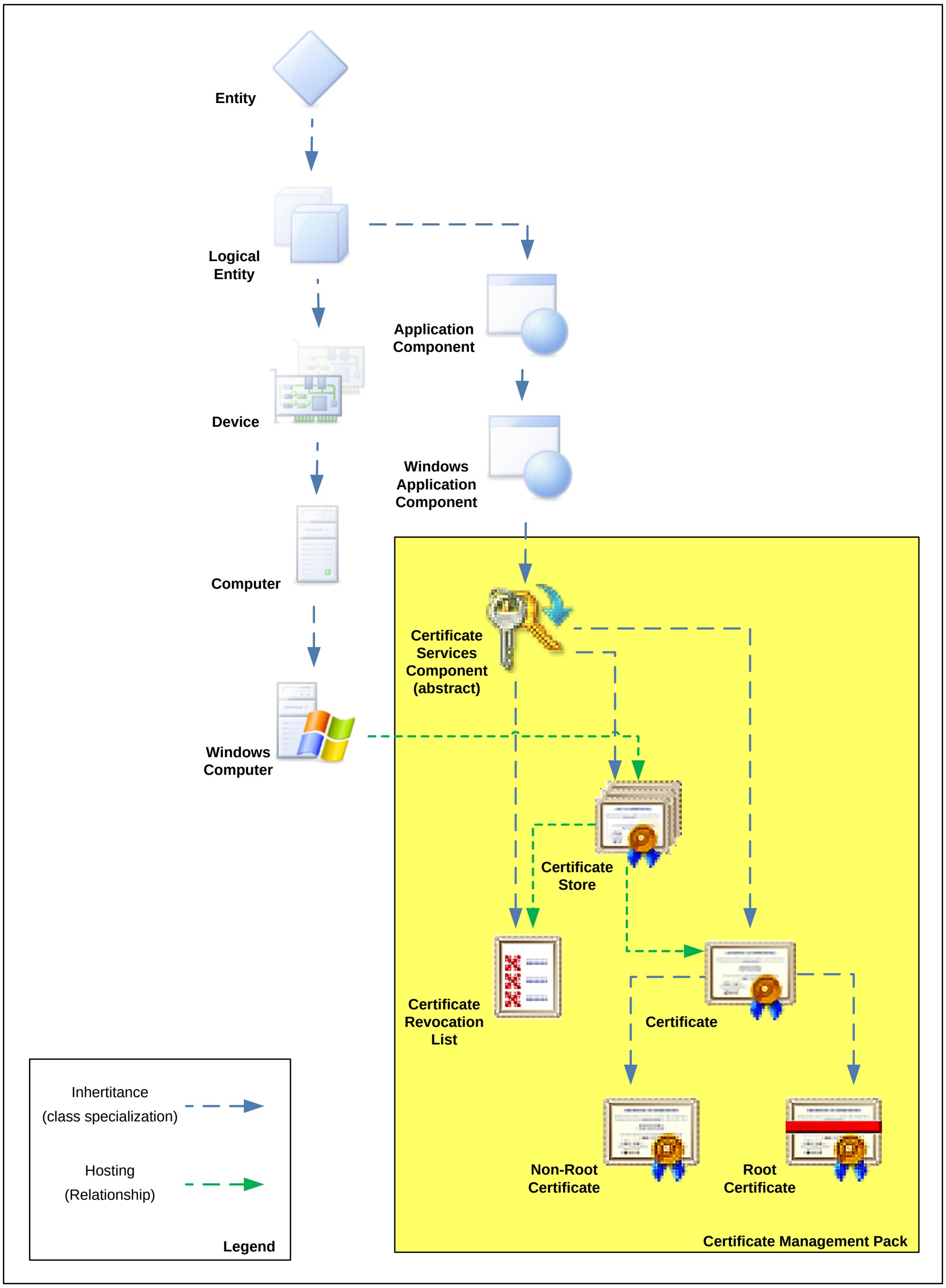


Figure 1 - Class Diagram

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.

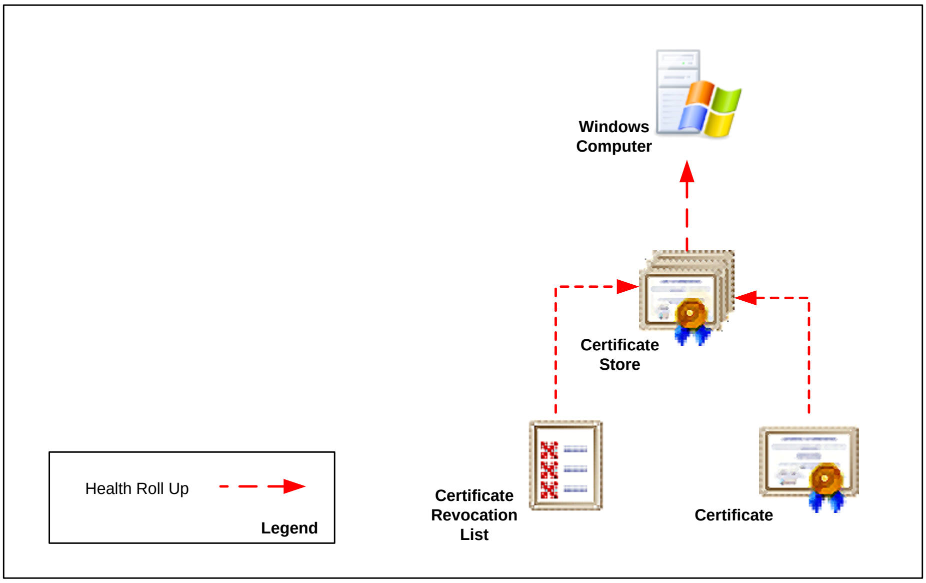


Figure 2 - Health Roll Up

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

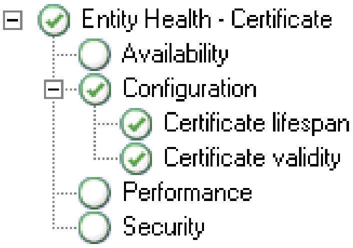
Table 9 – Dependency Monitors

Monitors and Alerts

Monitors in the PKI Certificate Validation Management Pack are targeted at Certificate,Certificate Revocation List 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.



- Entity Health - Certificate
  - Availability
  - Configuration
    - Certificate lifespan
    - Certificate validity
  - Performance
  - Security

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 Name: Microsoft Windows Hardware Compatibility Serial number: 198b11d13f9a8ffe69a0 Certificate store: Intermediate Certification Authorities	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 10 - Certificate Lifespan Monitor Details

Note that the monitor is disabled for certain root certificates. See *Root Certificates required by Windows* on page *15* 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: This certificate was revoked by its certification authority Certificate Name: devscomrpt.mgmtdom.dev Serial number: 1da9ead40000000000003f Certificate Store: Personal	Only standard	Evaluates the certificate’s ‘Status’ property

Table 11 - Certificate Validity Monitor

Note that the monitor is disabled for certain root certificates. See *Root Certificates required by Windows* on page *15* for details.

Certificate Revocation List Monitor

A single configuration monitor is targeted at CRL objects.

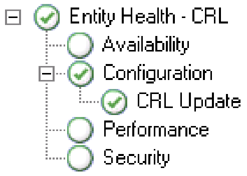


Figure 4 – Certificate Revocation List Monitor

CRL Update Monitor

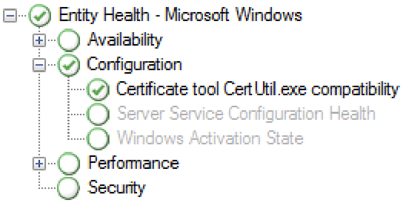
The two state monitor warns if a CRL has not been updated by its ‘Next update’ date.

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	Only standard	Evaluates the CRL’s ‘Next update’ property

Table 12 - CRL Update Monitor

Management Pack Compatibility 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.



- Entity Health - Microsoft Windows
  - Availability
  - Configuration
    - Certificate tool CertUtil.exe compatibility
    - Server Service Configuration Health
    - Windows Activation State
  - Performance
  - Security

Figure 5 – Certificate tool CertUtil.exe compatibility

Certificate tool CertUtil.exe compatibility Monitor

The two state monitor warns when the output of the certificate management tool “CertUtil.exe” could not be interpreted by the management pack. This may happen due to one of the following reasons:

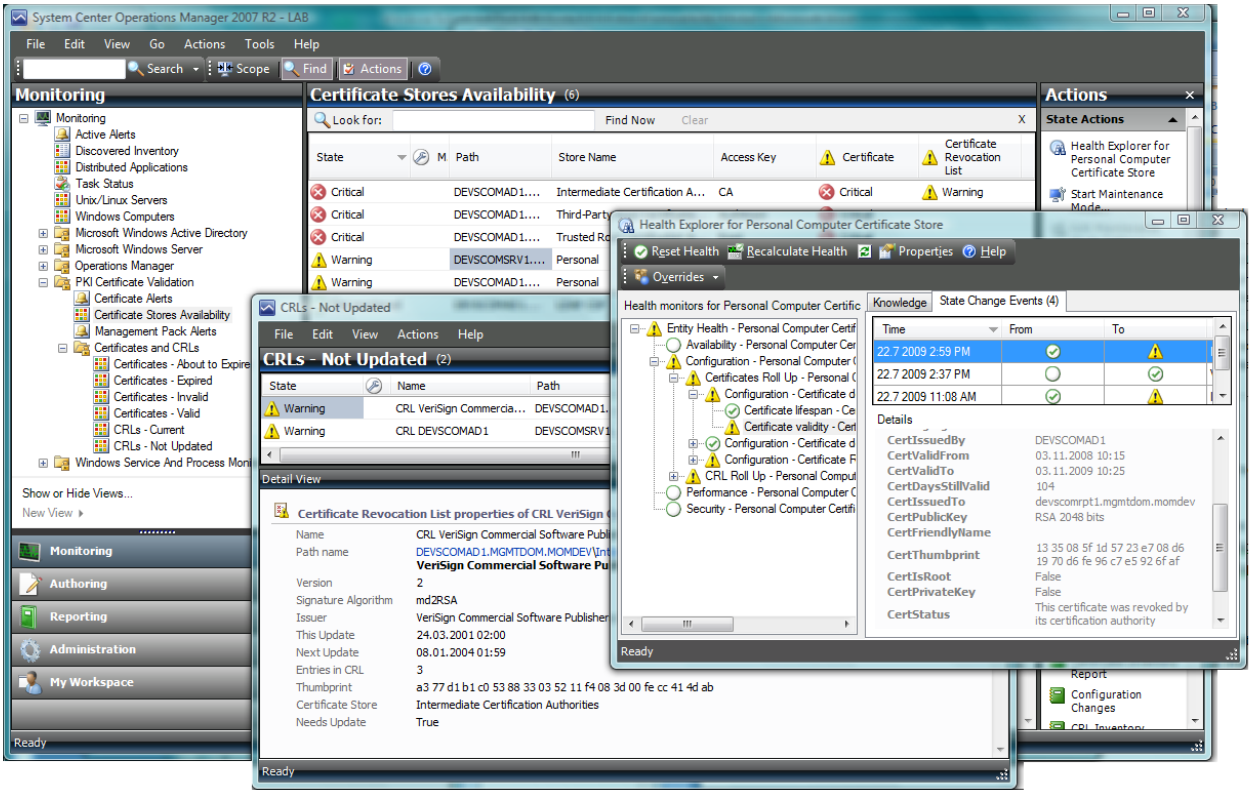
- CertUtil.exe was not found (requires installation on Windows XP).
- The OS language is not currently supported by the management pack. Disable the discovery for those machines installed with an unsupported language. Contact the management pack authors to see if the missing language can be included in a future release.

Severity	Priority	Alert Name	Possible Overrides	Implementation Details
Warning	Normal	Certificate tool CertUtil.exe is not compatible Sample alert: CertUtil.exe is either not present on this computer or the OS language is not supported by the "PKI Certificate Validation" management pack.	Only standard	Windows event monitor, triggering on the output of the certificate discovery script.

Table 13 - Certificate tool CertUtil.exe compatibility Monitor

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*


System Center Operations Manager 2007 R2 - LAB
File Edit View Go Actions Tools Help
Search Scope Find Actions
Monitoring
Monitoring
Active Alerts
Discovered Inventory
Distributed Applications
Task Status
Unix/Linux Servers
Windows Computers
Microsoft Windows Active Directory
Microsoft Windows Server
Operations Manager
PKI Certificate Validation
Certificate Alerts
Certificate Stores Availability
Management Pack Alerts
Certificates and CRLs
Certificates - About to Expire
Certificates - Expired
Certificates - Invalid
Certificates - Valid
CRLs - Current
CRLs - Not Updated
Windows Service And Process Moni
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
Ready
Certificate Stores Availability (6)
Look for: Find Now Clear
Actions
State Actions
Health Explorer for Personal Computer Certificate Store
Start Maintenance Mode...
Report
Configuration Changes
CRL Inventory
CRLs - Not Updated
File Edit View Actions Help
CRLs - Not Updated (2)
Detail View
Ready
Health Explorer for Personal Computer Certificate Store
Reset Health Recalculate Health Properties Help
Overrides
Health monitors for Personal Computer Certific
Entity Health - Personal Computer Certif
Availability - Personal Computer Cer
Configuration - Personal Computer (
Certificates Roll Up - Personal (
Configuration - Certificate d
Certificate lifespan - Ce
Certificate validity - Cert
Configuration - Certificate d
Configuration - Certificate F
CRL Roll Up - Personal Comput
Performance - Personal Computer (
Security - Personal Computer Certifi
Knowledge
State Change Events (4)
Details
Ready

State	M	Path	Store Name	Access Key	Certificate	Certificate Revocation List
Critical		DEVSCOMAD1....	Intermediate Certification A...	CA	Critical	Warning
Critical		DEVSCOMAD1....	Third-Party			
Critical		DEVSCOMAD1....	Trusted Ro			
Warning		DEVSCOMSRV1....	Personal			
Warning		DEVSCOMAD1....	Personal			

State		Name	Path
Warning		CRL VeriSign Commercia...	DEVSCOMAD1.
Warning		CRL DEVSCOMAD1	DEVSCOMSRV1

Certificate Revocation List properties of CRL VeriSign C

Name	CRL VeriSign Commercial Software Publi
Path name	DEVSCOMAD1.MGMTDOM.MOMDEV\Int **VeriSign Commercial Software Pu**
Version	2
Signature Algorithm	md2RSA
Issuer	VeriSign Commercial Software Publisher
This Update	24.03.2001 02:00
Next Update	08.01.2004 01:59
Entries in CRL	3
Thumbprint	a3 77 d1 b1 c0 53 88 33 03 52 11 f4 08 3d 00 fe cc 41 4d ab
Certificate Store	Intermediate Certification Authorities
Needs Update	True

Time	From	To
22.7 2009 2:59 PM	✓	⚠
22.7 2009 2:37 PM	○	✓
22.7 2009 11:08 AM	✓	⚠

CertIssuedBy	DEVSCOMAD1
CertValidFrom	03.11.2008 10:15
CertValidTo	03.11.2009 10:25
CertDaysStillValid	104
CertIssuedTo	devscomrpt1.mgmtdom.momdev
CertPublicKey	RSA 2048 bits
CertFriendlyName	
CertThumbprint	13 35 08 5f 1d 57 23 e7 08 d6 19 70 d6 fe 96 c7 e5 92 6f af
CertIsRoot	False
CertPrivateKey	False
CertStatus	This certificate was revoked by its certification authority

Figure 6 – 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 Alerts	PKI Certificate	Alert view: All current alerts concerning certificates or certificate revocation lists.
Certificate Stores Availability	PKI Certificate	State view: The roll up state of all certificate stores. Shows the health of certificates and CRLs underneath.
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.
CA Certificates	PKI Certificate\Certificates and CRLs	State view: Lists all certificates that have Basic Constraints of CA. Based on the *CA*

Console View Name	Console View Folder	Description
		Certificates Group
Certificates – Valid	PKI Certificate\Certificates and CRLs	State view: Lists all discovered certificates that are valid. 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. Based on the *Expiring Certificates Group*.
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 14 – 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 *19* for choosing correct object types.

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.

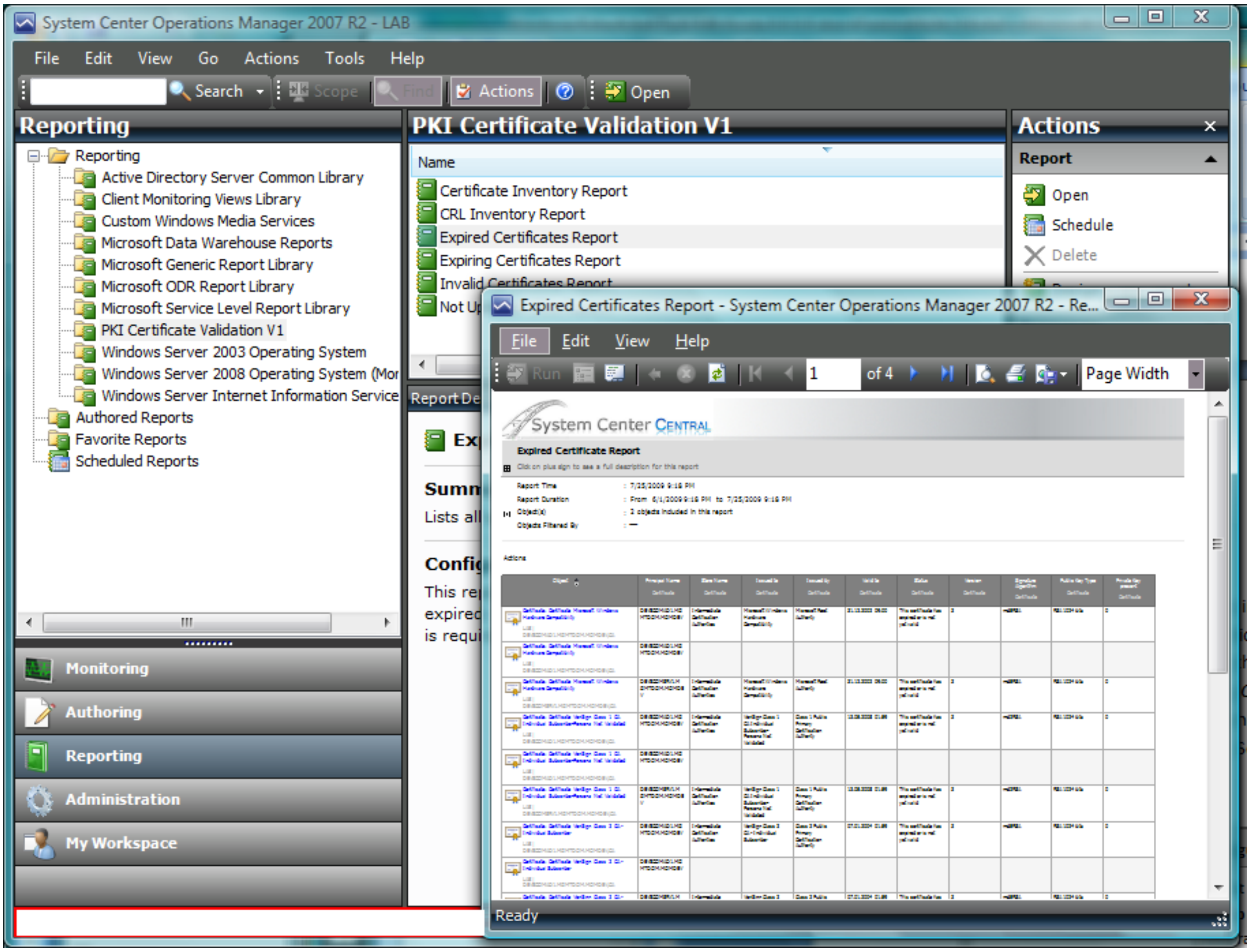

System Center Operations Manager 2007 R2 - LAB
File
Edit
View
Go
Actions
Tools
Help
Search
Scope
Find
Actions
Open
Reporting
Reporting
Active Directory Server Common Library
Client Monitoring Views Library
Custom Windows Media Services
Microsoft Data Warehouse Reports
Microsoft Generic Report Library
Microsoft ODR Report Library
Microsoft Service Level Report Library
PKI Certificate Validation V1
Windows Server 2003 Operating System
Windows Server 2008 Operating System (Mor
Windows Server Internet Information Service
Authored Reports
Favorite Reports
Scheduled Reports
Monitoring
Authoring
Reporting
Administration
My Workspace
PKI Certificate Validation V1
Name
Certificate Inventory Report
CRL Inventory Report
Expired Certificates Report
Expiring Certificates Report
Invalid Certificates Report
Not Up
Report De
Ex
Summ
Lists all
Config
This re
expired
is requi
Actions
Report
Open
Schedule
Delete
Expired Certificates Report - System Center Operations Manager 2007 R2 - Re...
File
Edit
View
Help
Run
1
of 4
Page Width
System Center Central
Expired Certificate Report
Ready

Figure 7 – 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. Based on the *Expiring Certificates Group*. It allows scoping the report by selecting a group containing computer or certificate store objects.
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 15 – Reports

Troubleshooting

During discovery and monitoring the certificate store verification script 'SystemCenterCentral.Utililities.Certificates.LocalScriptProbe.vbs' 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
3001	Information	The command ran successfully but no certificates or CRLs were found in the certificate store. No objects are going to be discovered. Only written if in debugging mode.
3002	Information	The command ran successfully and is writing a PropertyBag with the details about the certificates and CRLs back to SCOM. Only written if in debugging mode.
3003	Warning	The output of running the command 'CertUtil.exe –v –verifystore [store name]' was invalid
3004	Warning	The operating system's language is not compatible with the current release of the management pack
3005	Warning	The command 'Certutil.exe –v –verifystore [store name]' could not be 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. Only written if in debugging mode.

Table 16- 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
SystemCenterCentral.Utilities.Certificates.LocalScriptProbe.vbs	Calls CertUtil.exe –v –verifystore [store name] to retrieve a list of all certificates and CRLs in the store with their properties. 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.	hourly
SystemCenterCentral.Utilities.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 (Server 2008)	hourly

Table 17 - Management Pack Scripts

Appendix: Feedback

For comments on this guide or the Management Pack, the authors of the Management Pack can be contacted by leaving a comment on the original publishing source, the System Center Central Management Pack Catalog (http://www.systemcentercentral.com/tabid/63/tag/Pack_Catalog+MP_Catalog/Default.aspx).