



Roger Zander

CONSULTANT / MVP

Syliance IT Services GmbH

roger@zander.ch /

roger.zander@syliance.com

Security Considerations...

Secunia
Stay Secure

Configuration Manager

Agenda

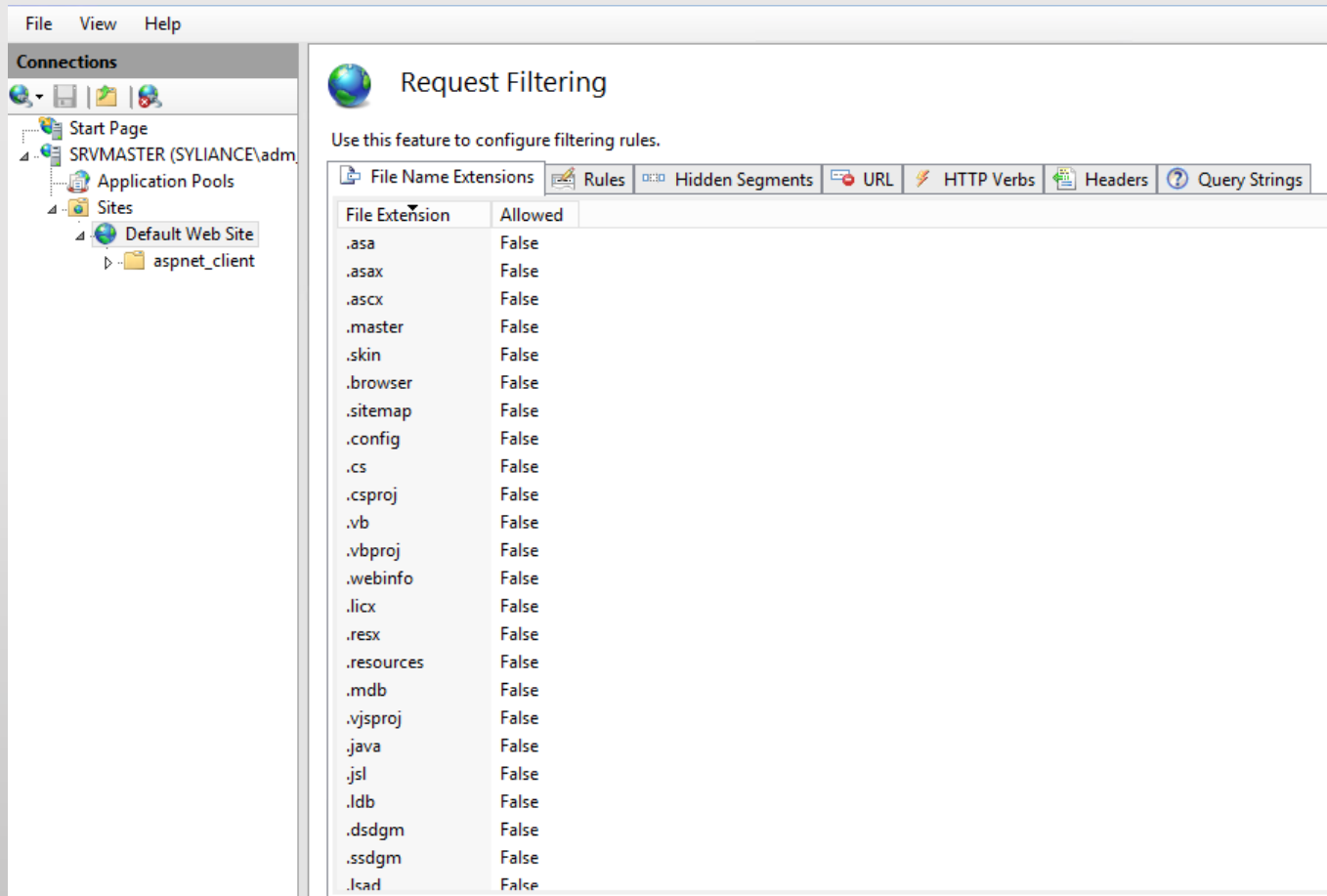
- IIS Settings
 - RequestFilterung
 - Monitoring
- CM12 Site Settings
 - HTTPS, X.509 Authentication
 - CRL
 - Trusted Root Key
- Network Access Account

IIS Vulnerabilities

http://www.cvedetails.com/product/3436/Microsoft-IIS.html?vendor_id=26

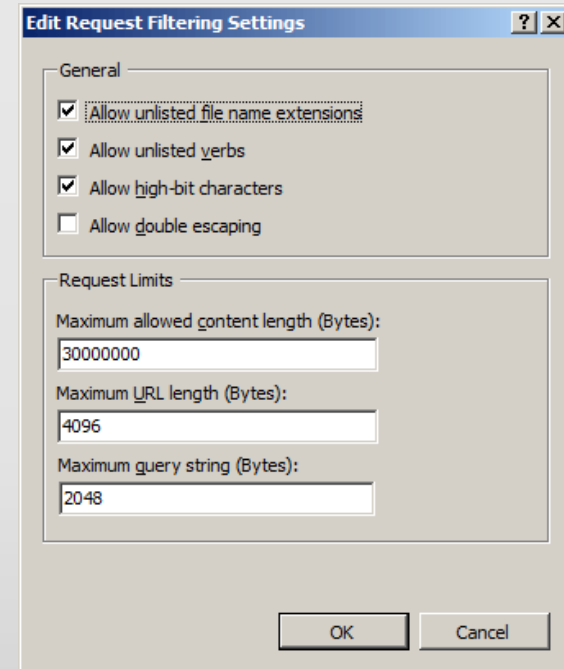
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2008	4	1	1	1								1			
2009	7	1	1	1	1					3					2
2010	6	2	3	3	1		1			1	1				1
2012	1										1				
2013	1														
2014	1														
Total	20	4	5	5	2		1			4	2	1			3
% Of All		20.0	25.0	25.0	10.0	0.0	5.0	0.0	0.0	20.0	10.0	5.0	0.0	0.0	

IIS Request Filtering



The screenshot shows the IIS Manager console with the 'Request Filtering' feature selected. The 'File Name Extensions' tab is active, displaying a table of file extensions and their allowed status.

File Extension	Allowed
.asa	False
.asax	False
.ascx	False
.master	False
.skin	False
.browser	False
.sitemap	False
.config	False
.cs	False
.csproj	False
.vb	False
.vbproj	False
.webinfo	False
.licx	False
.resx	False
.resources	False
.mdb	False
.vjsproj	False
.java	False
.jsl	False
.ldb	False
.dsdgm	False
.ssdgm	False
.icad	False



The 'Edit Request Filtering Settings' dialog box is shown with the 'General' tab selected. It contains several checkboxes and input fields for configuring request filtering rules.

General

- Allow unlisted file name extensions
- Allow unlisted verbs
- Allow high-bit characters
- Allow double escaping

Request Limits

Maximum allowed content length (Bytes):
30000000

Maximum URL length (Bytes):
4096

Maximum query string (Bytes):
2048

OK Cancel

IIS Request Filtering and CM12

- By default, IIS blocks several file name extensions and folder locations from access by HTTP or HTTPS communication. If your package source files contain extensions that are blocked in IIS, **you must configure the requestFiltering section** in the applicationHost.config file on distribution point computers.
- The following file name extensions are used by Configuration Manager for packages and applications. Allow the following file name extensions on distribution points:
 - .PCK
 - .PKG
 - .STA
 - .TAR
- For example, you might have source files for a software deployment that include a folder named **bin**, or that contain a file with the **.mdb** file name extension. By default, IIS request filtering blocks access to these elements. When you use the default IIS configuration on a distribution point, clients that use BITS fail to download this software deployment from the distribution point. In this scenario, the clients indicate that they are waiting for content. To enable the clients to download this content by using BITS, on each applicable distribution point, edit the **requestFiltering** section of the applicationHost.config file to allow access to the files and folders in the software deployment.

http://technet.microsoft.com/en-us/library/gg712264.aspx#BKMK_RequestFiltering

Default Filter Rules from ASP.NET Feature

	.NET3.5 SP1	.NET4 (Full)	Feature: NET 3.5 HTTP Activation	Feature: NET 3.5 Non-HTTP Activation	Feature: NET Framework 3.5 SP1 installed	Feature: ASP.NET 4.5 (Server2012)	Feature: ASP.Net installed	NET 4 ASPNET ISAPI registered	Feature: BITS Server Extensions	Feature: IIS 6 Metabase Compatibility installed	Feature: IIS 6 WMI Compatibility installed	Feature: ISAPI Extension installed	Feature: Remote Differential Compression installed	Feature Web-Stat-Compression installed	Feature: Windows Authentication installed
Application Catalog web service	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗
Application Catalog website	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓
Distribution Point	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓
Enrollment point	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗
Enrollment proxy point	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗
Fallback Status Point	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗
Management Point	✓	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓
Software Update Point	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✓	✗	✓

How to monitor IIS Settings... -> DCM !

The screenshot displays the Windows Configuration Manager interface. On the left, the navigation pane shows the hierarchy: Overview > Users > Devices > User Collections > Device Collections > User State Migration > Asset Intelligence > Software Metering > Compliance Settings > Configuration Items > IIS. The main pane lists several IIS configuration items for CM12, including General, FSP, MP, SUP, PXE, Application Catalog website, Application Catalog web service, DP, Enrollment proxy point, and Enrollment point. The 'IIS Configuration for CM12 (DP) Properties' dialog box is open, showing the 'Settings' tab. It contains a table of settings associated with this configuration item.

Name	Setting Type	Inherited	User Setti
Feature: BranchCache for network files	Script	No	No
Feature: IIS 6 Metabase Compatibility installed	Script	No	No
Feature: IIS 6 WMI Compatibility installed	Script	No	No
Feature: ISAPI Extension installed	Script	No	No
Feature: Remote Differential Compression installed	Script	No	No
Feature: Windows Authentication installed	Script	No	No
IIS 'Default Web Site' Allow Double Escaping	Script	No	No
IIS 'Default Web Site' Allow HighBitCharacters	Script	No	No
IIS 'Default Web Site' RequestFilter FileExtensions ...	Script	No	No
IIS 'Default Web Site' RequestFilter HiddenSegmen...	Script	No	No
IIS 'Default Web Site' RequestFilter Verbs defined	Script	No	No
IIS RequestFilter FileExtensions defined	Script	No	No
IIS RequestFilter HiddenSegments defined	Script	No	No
IIS RequestFilter Verbs defined	Script	No	No

Other IIS Settings...

- Log Files -> Cleanup !

```
if(([System.Environment]::OSVersion.Version.Major -eq 6) -and
([System.Environment]::OSVersion.Version.Minor -ge 1)) { Import-
Module WebAdministration } else { Add-PSSnapin WebAdministration };

$LogPath = [System.Environment]::ExpandEnvironmentVariables((Get-
WebConfigurationProperty
"/system.applicationHost/sites/siteDefaults" -Location "Default Web
Site" -name logfile.directory).Value);

(Get-ChildItem $LogPath\*.log -Recurse | Where-Object {
$.LastWriteTime -lt (get-date).AddDays(-30)}) | % ($_) {remove-
item $_.fullname}
```

- MaxRequestBytes = Determines the upper limit for the total size of the Request line and the headers.
- MaxFieldLength = Sets an upper limit for each header. See MaxRequestBytes. This limit translates to approximately 32k characters for a URL.

<http://support2.microsoft.com/kb/820129/en-us>

IIS Port

Pro:

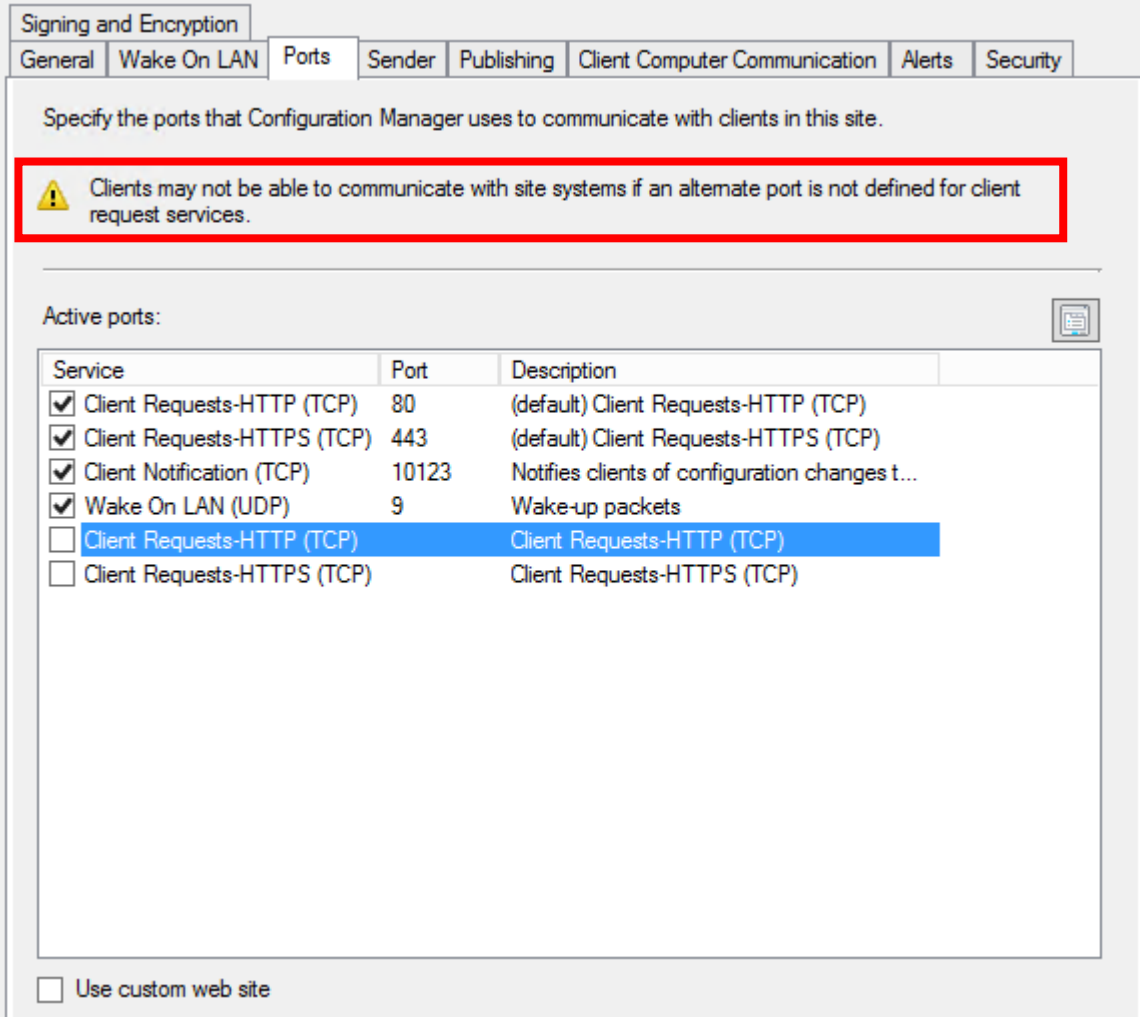
- A Port != 80/443 may help to identify CM12 Traffic (QoS)

Cons:

- You have to specify HTTPPort on CCMSETUP and Agent Push
- Monitor Port Settings (GPO, DCM, ..)

```
(Get-ItemProperty  
("HKLM:\SOFTWARE\Microsoft\CCM")).$("HttpPort")
```

When possible keep Port 80/443 as an active Port for fallback scenarios



Signing and Encryption

General Wake On LAN Ports Sender Publishing Client Computer Communication Alerts Security

Specify the ports that Configuration Manager uses to communicate with clients in this site.

Warning: Clients may not be able to communicate with site systems if an alternate port is not defined for client request services.

Active ports:

Service	Port	Description
<input checked="" type="checkbox"/> Client Requests-HTTP (TCP)	80	(default) Client Requests-HTTP (TCP)
<input checked="" type="checkbox"/> Client Requests-HTTPS (TCP)	443	(default) Client Requests-HTTPS (TCP)
<input checked="" type="checkbox"/> Client Notification (TCP)	10123	Notifies clients of configuration changes t...
<input checked="" type="checkbox"/> Wake On LAN (UDP)	9	Wake-up packets
<input type="checkbox"/> Client Requests-HTTP (TCP)		Client Requests-HTTP (TCP)
<input type="checkbox"/> Client Requests-HTTPS (TCP)		Client Requests-HTTPS (TCP)

Use custom web site

HTTPS in CM12 => x.509 Authentication

Distribution point Properties

General | PXE | Multicast | Group Relationships | Content | Content Validation | Boundary Groups

A distribution point contains source files for clients to download.

Enable and configure BranchCache for this distribution point

Description:

Specify how client computers communicate with this distribution point.

HTTP
Does not support mobile devices or Mac computers.

HTTPS
Requires computers to have a valid PKI client certificate:

Allow intranet-only connections

If you manage Mac computers or have mobile devices that are enrolled by Configuration Manager, select an option that allows Internet client connections.

Allow clients to connect anonymously

Create a self-signed certificate or import a PKI client certificate.

Create self-signed certificate **Update Boot Images !**

Set expiration date: 11.04.2113 09:03

Import certificate

Certificate: Browse...

Password:

Enable this distribution point for prestaged content

Use the application or package properties to choose how content is copied to this distribution point.

OK Cancel Apply

Management point Properties

General | Management Point Database

A management point provides policy and content location information to clients. It also receives configuration data from clients.

Client connections:

HTTP
This option does not support mobile devices, Mac computers, or connections over the Internet

HTTPS
This option requires client computers to have a valid PKI certificate for client authentication

Allow intranet-only connections

Allow mobile devices and Mac computers to use this management point

To manage Mac computers and mobile devices that are enrolled by Configuration Manager, you must select an option that allows Internet client connections.

Generate alert when the management point is not healthy

OK Cancel App

Encryption over HTTP:

- **When you use PKI certificates** for all client communications, **you do not have to plan for signing and encryption** to help secure client data communication. However, if you configure any site systems that run IIS to allow HTTP client connections, you must decide how to help secure the client communication for the site.

General | Wake On LAN | Ports | Sender | Publishing | Client Computer Communication | Alerts | Security

Signing and Encryption

Configure the signing and encryption requirements for client computers when they communicate with this site.

Clients always sign their client identification when they communicate with the Application Catalog website points.

Require signing
This option requires that when clients send data to management points, it is signed.

Require SHA-256
When clients sign data and communicate with site systems by using HTTP, this option requires the clients to use SHA-256 to sign the data. Clients must support the SHA-256 hash algorithm to use this option. This option applies to clients that do not use PKI certificates.

Use encryption
This option uses 3DES to encrypt the client inventory data and state messages that are sent to the management points.

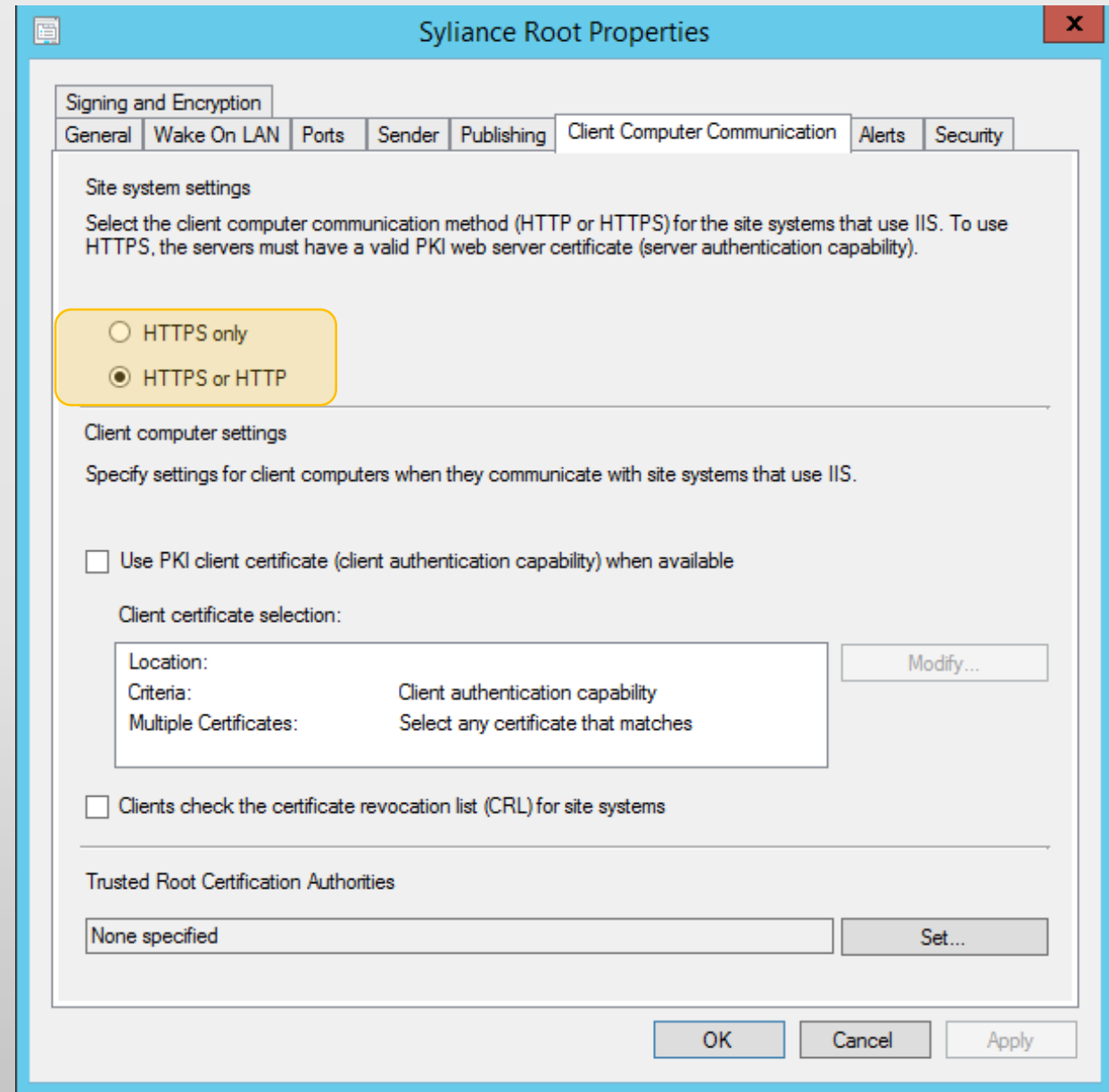
OK Cancel Apply

Default Cryptographic Controls

- Policy
 - Client policy assignments are signed by the self-signed site server signing certificate
 - Policy is encrypted by using 3DES when it contains sensitive data
 - When policy is stored on the clients, it is encrypted by using Data Protection application programming interface (DPAPI).
- Policy Hashing
 - The hashing algorithm for policy is SHA-1 and SHA-256.
- Content hashing
 - The distribution manager service on the site server hashes the content files for all packages.
 - The default hashing algorithm for content is SHA-256. (some exceptions: App-V streaming, iOS, WindowsRT, Windows Phone, Android)
- Inventory
 - Inventory that clients send to management points is always signed by devices, regardless of whether they communicate with management points over HTTP or HTTPS. If they use HTTP, you can choose to encrypt this data, which is a security best practice.
- SW Updates
 - All software updates must be signed by a trusted publisher to protect against tampering.
- ... <https://technet.microsoft.com/en-us/library/hh427327.aspx>

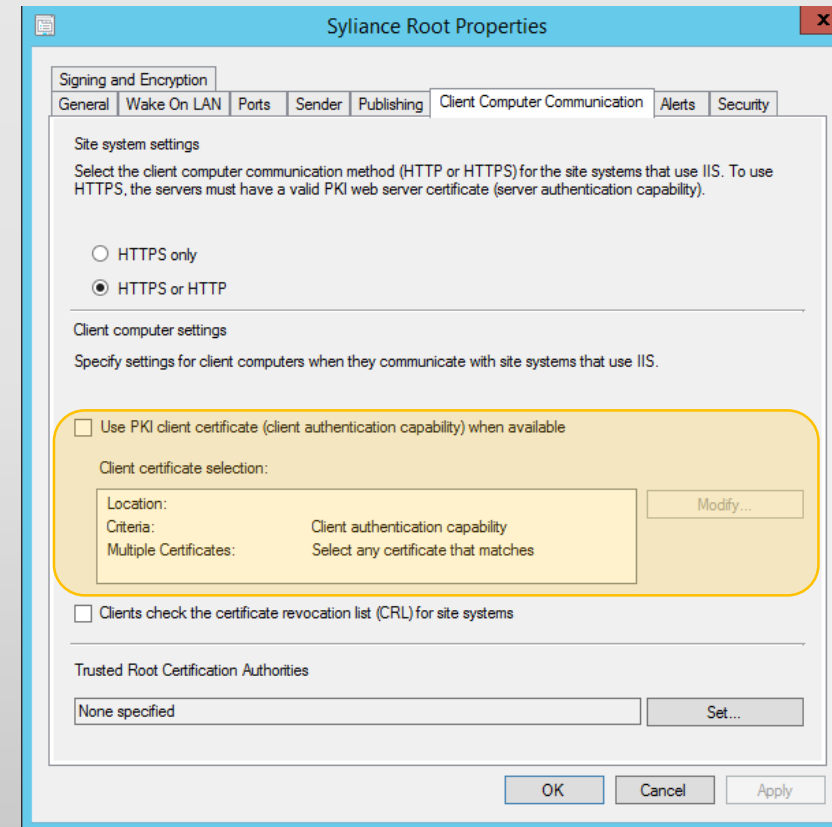
HTTPS on the Site

- Switch to HTTPS only, when all Site Roles (DP, MP etc.) are using HTTPS.
-> *X.509 will be enforced*
- All Agents must have a valid Client certificate.
-> *How do you handle DMZ and Workgroup machines ?*



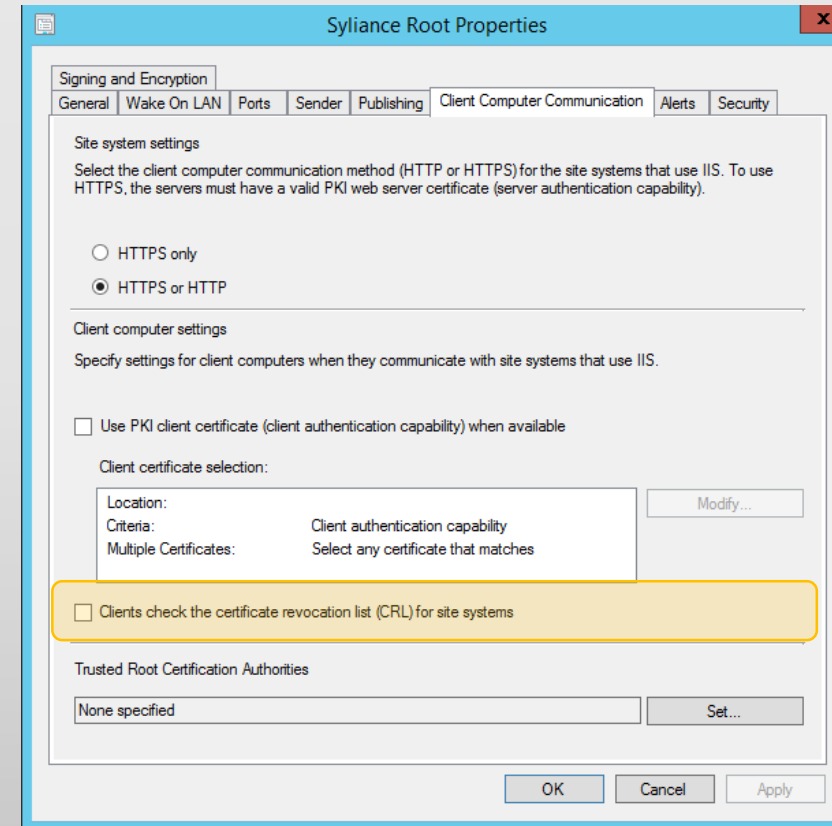
Client Certificate selection

- If your IIS site systems will use PKI client certificates for client authentication over HTTP or for client authentication and encryption over HTTPS, plan for how Windows-based clients will select the certificate to use for Configuration Manager.
-> *x.509 Authentication with HTTP is Possible !*
- Not all devices support a certificate selection method and instead, automatically select the first certificate that fulfills the certificate requirements. For example, clients on **Mac computers, and mobile devices do not support a certificate selection method.**
- In most cases, the Configuration Manager client correctly identifies a unique and appropriate PKI certificate to use.
-> *“if not, then configure !”*



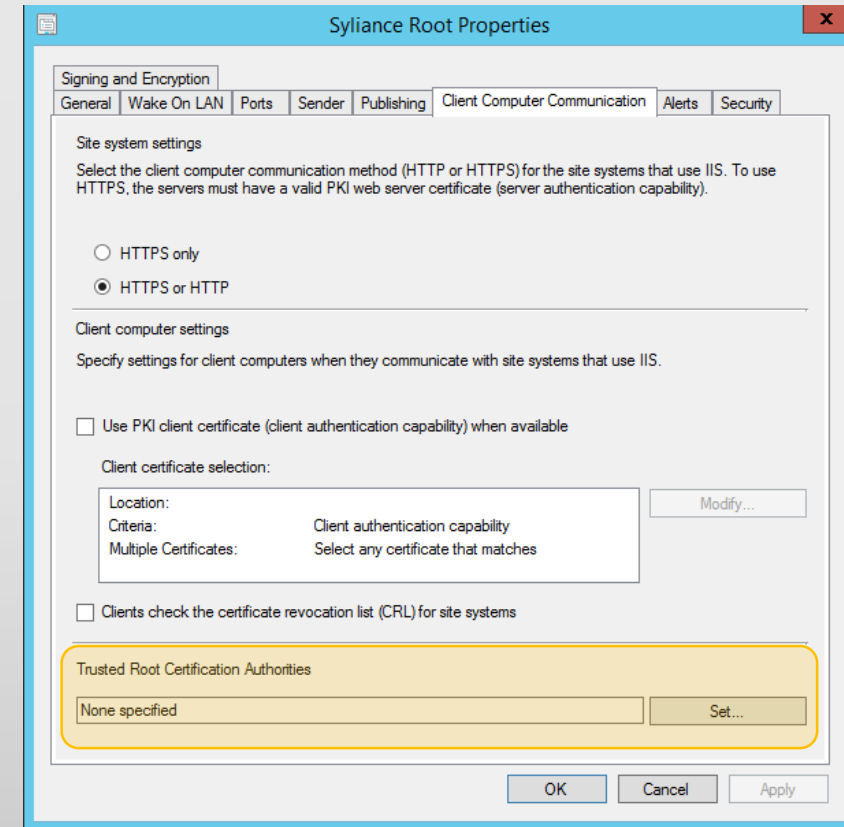
Certificate Revocation

- Because the location of the CRL is added to a certificate when it is issued by a CA, ensure that you plan for the CRL before you deploy any PKI certificates that Configuration Manager will use.
- Consult your PKI administrators **before** you decide whether Configuration Manager clients must check the CRL, and then consider keeping this option enabled in Configuration Manager when both of the following conditions are true:
 - **Your PKI infrastructure supports a CRL**, and it is published where all Configuration Manager clients can locate it. Remember that **this might include clients on the Internet** if you are using Internet-based client management, and clients in untrusted forests.
 - **The requirement to check the CRL for each connection to a site system configured to use a PKI certificate is larger than the requirement for faster connections and efficient processing on the client**, and is also **larger than the risk of clients failing to connect to servers if they cannot locate the CRL**.



Trusted Root Certificate Authorities

- When you issue client PKI certificates **from the same CA hierarchy** that issues the server certificates that you use for management points, **you do not have to specify this root CA certificate**. However, if you use multiple CA hierarchies and you are not sure whether they trust each other, import the root CA for the clients' CA hierarchy.



Trusted Root Key

Every site server generates a site exchange key to communicate with other sites. The site exchange key from the top-level site in the hierarchy is called the trusted root key.

- Clients use WMI to store a copy of the trusted root key in the namespace **root\ccm\locationservices**. (`Get-WmiObject -Class TrustedRootKey -Namespace root\ccm\locationservices`)
- Clients can automatically retrieve the public copy of the trusted root key by using two mechanisms:
 - The **Active Directory schema is extended** for Configuration Manager, the site is published to Active Directory Domain Services, and clients can retrieve this site information from a global catalog server.
 - Clients are installed by using client push.

If clients cannot retrieve the trusted root key by using one of these mechanisms, **they trust the trusted root key that is provided by the first management point that they communicate with.**

*A client might be misdirected to an attacker's management point ... to reduce this risk ... you can **pre-provision** the clients by using the trusted root key.*

- You can remove the trusted root key from a client by using the Client.msi property **RESETKEYINFORMATION = TRUE** with CCMSetup.exe. -> *During Task_Sequence*
- To replace the trusted root key, reinstall the client together with the new trusted root key, for example, by using client push, or by specifying the Client.msi **SMSPublicRootKey** property by using CCMSetup.exe.

Anonymous Authentication

- If anonymous Authentication on DP is enabled; Network-Access-Account (NAA) is not required anymore to access the DP.

If you manage Mac computers or have mobile devices that are enrolled to allow Internet client connections.

Allow clients to connect anonymously

Create a self-signed certificate or import a PKI client certificate.

Create self-signed certificate

Set expiration date:

Import certificate

Software Distribution Component Properties

General Network Access Account

Specify an account that accesses network locations when the site contains clients that are workgroup computers or that are from an untrusted domain.

Network Access Account

The Network Access Account is used by Configuration Manager clients to access network locations during content deployment or during operating system deployment.

Use the computer account of the Configuration Manager client

Specify the account that accesses network locations

There are no items to show in this view.

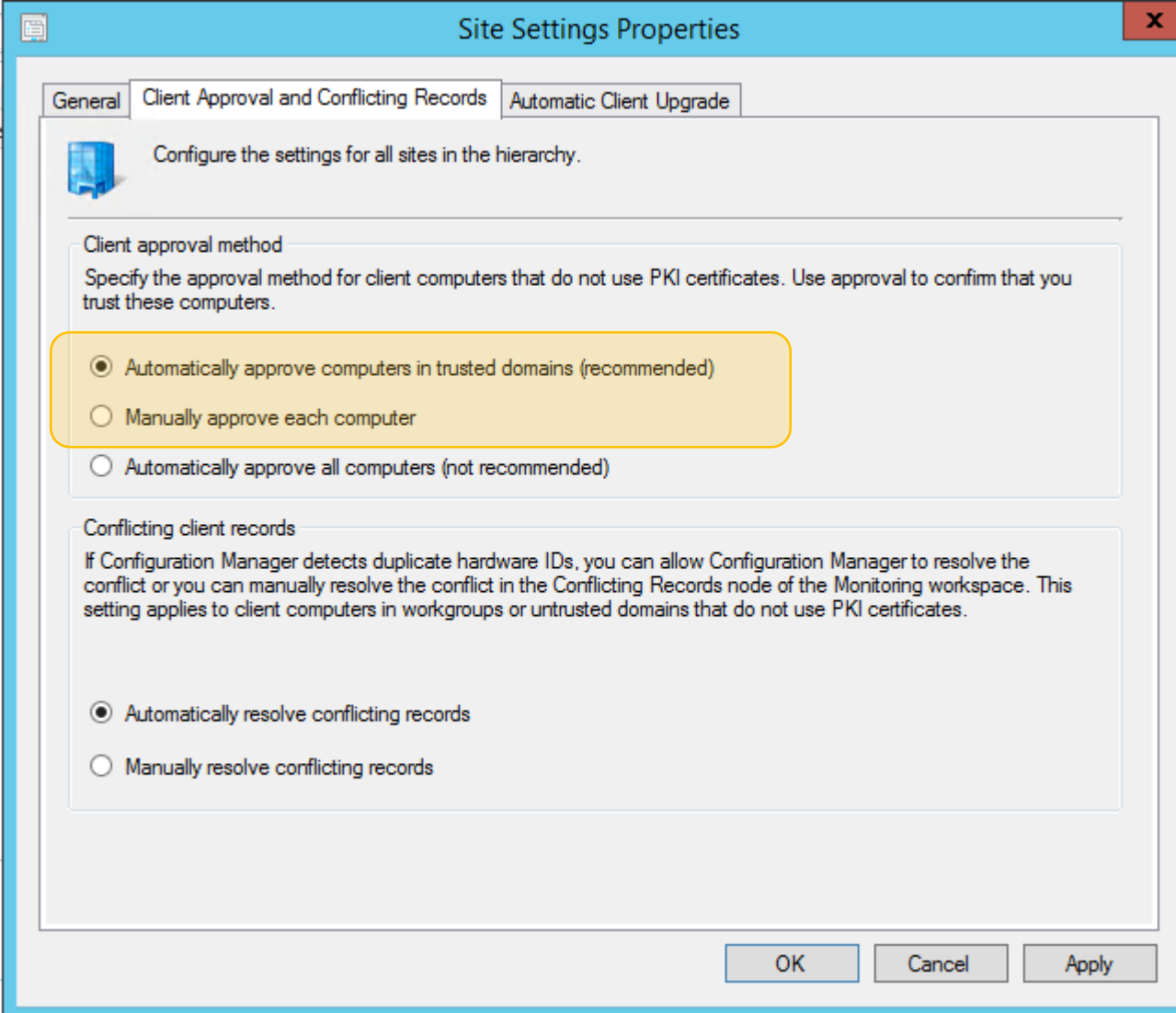
OK Cancel Apply

NAA is evil...

- Every Machine with an approved CM12 Agent will get Username and Password for the NAA
- Username and Password are not in clear text but can be «decoded» with a few lines of PowerShell (local Admin rights required).
 - NAA should be a user without any additional rights
 - Block NAA from interactive Logon
 - **NEVER** use an administrative Account

```
GENUS : 2
CLASS : CCM_NetworkAccessAccount
SUPERCLASS : CCM_ComponentClientConfig
DYNASTY : CCM_Policy
RELPATH : CCM_NetworkAccessAccount.SiteSettingsKey=1
PROPERTY_COUNT : 8
DERIVATION : {CCM_ComponentClientConfig, CCM_Policy}
SERVER : ROZAT
NAMESPACE : ROOT\ccm\policy\Machine\ActualConfig
PATH : \\ROZAT1\ROOT\ccm\policy\Machine\ActualConfig:CCM_NetworkAccessAccount.SiteSettingsKey=1
ComponentName :
Enabled :
NetworkAccessPassword : <PolicySecret Version="1"><![CDATA[0601000001000000008C9DDF0115D1118C7A00C04FC297EB010000
23BE4CE94444AC14A9099D614A0C000000002000000000106600000001000020000000A4C2744A37DA7994F
888BC9B36E0D06A772A9378796168FA193F2D074500000000E80000000020000200000009B8D514585B35EF1
A8EED126F80A3ECA63E1A2305C8EA2AA9E10511304300000000BF4D21C8CF0ED5F6797D59B3F49D7FB940BE87
79DF767C237063A10025FE5277C61F8E2E0CC4C28BC74E23BE40000000A343C5327B9C6B4CF7F8005BC38D0A
9ECC525534BDF5560C6D2DA7D4F83E51DE796D49A1647C8C29D149E436F69960B324B7FD5E8298D8D49BAF80F
</PolicySecret>
NetworkAccessUsername : <PolicySecret Version="1"><![CDATA[1601000001000000008C9DDF0115D1118C7A00C04FC297EB010000
23BE4CE94444AC14A9099D614A0C000000002000000000106600000001000020000000841219388F1CC8BFA
6BF64BE44D2D03DDB2C85EDA254BC327C5DE740E00000000E80000000020000200000008321C170FAE19723
8178D955E54FC3CAF2221673D900873A2931AD231400000005A03475190331869BD2FD83CDFCB90B2F44611C
81C82EEA9E1B2CE0C54A89E979F5DF4384FD583267017B00385497B47B3E889E6A48A2264995755C7A400000
128D28C2D4CAA61138CDDF08B1B25E81D12A6B2A7B682CC15A5E62669608CCA62EC08FF55ACA1415E184A523
16575E7FD1ACCB4A0A16DCBB76F92]]></PolicySecret>
Reserved1 :
Reserved2 :
Reserved3 :
SiteSettingsKey : 1
```

With NAA, restrict Auto approval...



The screenshot shows the 'Site Settings Properties' dialog box with the 'Client Approval and Conflicting Records' tab selected. The dialog has a blue title bar and three tabs: 'General', 'Client Approval and Conflicting Records', and 'Automatic Client Upgrade'. The main content area is titled 'Configure the settings for all sites in the hierarchy.' and contains two sections: 'Client approval method' and 'Conflicting client records'. In the 'Client approval method' section, the first radio button option, 'Automatically approve computers in trusted domains (recommended)', is selected and highlighted with a yellow rounded rectangle. The other two options are 'Manually approve each computer' and 'Automatically approve all computers (not recommended)'. In the 'Conflicting client records' section, the first radio button option, 'Automatically resolve conflicting records', is selected. The other option is 'Manually resolve conflicting records'. At the bottom right of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

Site Settings Properties

General Client Approval and Conflicting Records Automatic Client Upgrade

Configure the settings for all sites in the hierarchy.

Client approval method
Specify the approval method for client computers that do not use PKI certificates. Use approval to confirm that you trust these computers.

- Automatically approve computers in trusted domains (recommended)
- Manually approve each computer
- Automatically approve all computers (not recommended)

Conflicting client records
If Configuration Manager detects duplicate hardware IDs, you can allow Configuration Manager to resolve the conflict or you can manually resolve the conflict in the Conflicting Records node of the Monitoring workspace. This setting applies to client computers in workgroups or untrusted domains that do not use PKI certificates.

- Automatically resolve conflicting records
- Manually resolve conflicting records

OK Cancel Apply

NAA vs. Anonymus Authentication

- Set DP to allow anonymous Authentication
- Remove NAA
- Auto approve all computers
- Windows Installer Source Update can always Access the sources

vs.

- Authenticated access to DP
- Risk of NAA PW on every machine
- Restrict Agent approval
- Windows Installer Source Update on Workgroup or untrusted machines are unable to access the sources.

Danke



Herzlichen Dank

roger@zander.ch / roger.zander@syliance.com

<http://myitforum.com/cs2/blogs/rzander>

Bewertung der Session: [Configmgr.ch](http://configmgr.ch)

- Xing: <https://www.xing.com/net/cmce>
- Facebook: <https://www.facebook.com/groups/411231535670608/>
- LinkedIn: <http://www.linkedin.com>
- Twitter: https://twitter.com/configmgr_ch

Nächster Event: Freitag 19. Juni Digicomp Bern