



The outer reaches

Thanks to the new System Center Configuration Manager it's now easier for administrators to work their magic over the Internet

BY MATT TINNEY

Prior to System Center Configuration Manager (SCCM) 2007, managing clients over the Internet without VPN was impossible. Remote users are often the most difficult type of users in SMS to manage. With the advent of Internet Based Client Management (IBCM) in SCCM 2007, it is now possible to provide a secure and reliable infrastructure to enable SMS administrators to manage devices on the Internet with the same level of control as computers on the intranet.

In this article, I will discuss the differences between native and mixed mode, certificate requirements for native mode, the SCCM 2007's new security features and infrastructure that provide a higher level of security to make all this possible.

The objective of IBCM is to "deliver a secure and reliable infrastructure to enable IT administrators in enterprises to manage computers on the Internet with the same level of control as computers on the intranet", according to program manager Prabhu Padhi.

The new functionality in SCCM provides a secure and reliable infrastructure for managing machines on the Internet without the need for those machines to connect through a VPN tunnel to the corporate network. Traditionally, VPN's attractiveness has been weakened for several reasons. For example:

- It is difficult for to use.
- It adds complexity.
- VPN ports are often blocked at the perimeter network, making them unusable most of the time.

IBCM was created to remove dependency on VPN, offer a higher level of security and ensure convergence with established security standards – particularly those relating to certificates. It specifically addresses the needs of Internet-enabled users, PoS systems and corporate users who work remotely from home.

The four topology configurations that are supported by IBCM are as follows:

- **Point of Sale** Machines that are always out on the Internet. In this topology, all site roles (management

point, fallback status point and distribution point) are within the DMZ and the site server and SQL server reside inside the corporate LAN.

- **Point of Sale (variation)** This is where the entire SMS site and roles are residing within the DMZ LAN, with a parent SCCM site residing in the corporate LAN. This topology presents a few security risks that you should be aware of. If you intend to go with this topology, ensure all holes have been closed.
- **Road warrior and intranet client** In this topology, all the site roles in the DMZ manage Internet clients and all the site roles in the corporate LAN manage internal clients. This topology was never supported in SMS 2003 because you could not have different site system roles in a different Active Directory forest from your site server. This is supported only for Internet-based client management.
- **Road warrior (variation on the option above)** The only variation is the requirement to manage both Internet and intranet clients using the same SCCM site and site system roles. The management point in the DMZ would be marked to serve both intranet and Internet clients.

Installing the client

Several options are available for installing the client. You can connect to a corporate network to install it or you can install the client manually through an authenticated extranet location or by CD.

The following features in SCCM 2007 are currently not supported with IBCM:

- Operating system deployment (planned for future versions)
- Client deployment
- Network Access Protection (doesn't make sense because client is outside corporate boundary)
- Branch distribution point cannot be marked as an Internet client and IBCM client cannot use a branch distribution point
- Remote tools

Internet clients do not have any notion of finding a network, Active Directory Domain Services and so on. Therefore they are stamped with the fully qualified domain name (FQDN) of an assigned Internet management point (IMP) and the Internet fallback status point.

This is a new role in SCCM 2007, which enables administrators to view failure data that is sent from the client in the form of an SOS message. The SOS message contains details on why a client failed to communicate with the IMP. Both FQDN stamps are done at the time of client installation. There are also several SMS reports that the SMS administrator can run to identify why the client failed. Reports on the successes of clients connecting to the management point are also produced.

Another huge area for discussion is roaming support. In its purest form, roaming indicates where a machine is at any point in time and is used for content delivery. When an IBCM roams, the client could be on the Internet, intranet or on a foreign network (a network that is relative to the client's corporate network, such as a consultant connected to an external customer network). For both Internet and foreign network scenarios, the client won't perform a dynamic management point lookup, but will rather communicate with a fixed IMP.

The second roaming scenario is for those computers that are taken out and used on the Internet and then are switched back to the intranet. In this scenario, roaming works slightly differently. When a client comes back into the corporate network it will behave like a regular intranet client and so nothing has to be configured differently, at least from the SMS administrator's point of view.

Proxy server settings should also be configured to allow outbound Internet connectivity for the SCCM client. Typically, proxy server settings are necessary in some scenarios where the client needs to connect out to the Internet via a proxy.

This allows the client to be continually managed when out on the Internet or on a foreign network. There are four possibilities for providing proxy support for Internet clients to communicate with the IMP via the Internet:

1. The proxy credentials and server are supplied when the client is installed. If this fails, use option 2.
2. The client attempts to find a proxy running under the system context. If this fails, try option 3.
3. The client tries to find a proxy running under the logged-on user, where the Internet Explorer Proxy Settings are leveraged. If this fails, use option 4.
4. Client communicates to the management point without a proxy.

Going native

To take advantage of IBCM a new security site mode was added to SCCM, called Native mode. Native mode is a requirement for IBCM, so the client has to be in Native mode. An Internet-based client cannot talk using HTTP and also be a Native mode client.

Native mode uses full mutual authentication, encryption and signing between an SCCM client and SCCM site server, and a site system using a public key infrastructure (PKI). A PKI is a core dependency for Native mode. Any PKI will be honoured as long as the certificate requirements (x509 based) are adhered to. In summary, the certificate requirements are as follows:

- **Site server (used for document signing)** Signing capability with a specific site code string in the Subject Name field.
- **Site roles (used as web server certificate template)** FQDN in the Subject Name field with server authentication capability.
- **NLB** Subject Name field is filled with the FQDN of the NLB cluster and the FQDN of the machine.
- **Firewall** Same as client and site roles.
- **Client** Unique code string in Subject Name or Alternative Subject Name field in certificate with client authentication capability.

When you move your site to Native mode, a few changes are made to require the use of certificate and SSL communication. Native mode is applicable for desktops, laptops, ATMs, embedded devices and so on. The only caveat is that for mobile devices you will need user-based certificates. Before you switch to native mode ensure that you have a PKI to issue certificates for SCCM, that there are no SMS 2003 clients, that existing SCCM clients are capable, and that there are no other web applications on the SCCM servers.

Like SMS 2003, the Security Site mode setting is enabled at the site level, not at the hierarchy. The recommendation is to enable the Site mode in a top-down approach, because this fits with SCCM 2007 upgrade strategy best practices. You can always switch back and forth between Native mode and Mixed mode. This might be necessary when the site is switched to Native, but some clients are still in Mixed mode. In this scenario, the clients running in Mixed mode will become unmanageable.

To prepare your clients for the switch to Native mode, it is recommended that you run SCCMNativeModeReadiness.exe (a utility installed with Configuration Manager 2007 clients, located in %windir%\system32\CCM) as a mandatory advertised job. The results can then be reported on by searching for 'Native mode'. There are certain reports that are useful in preparing for the switch to Native mode:

■ Summary information of clients in Native mode

Gives administrators visibility into the number of clients that are not managed and how many are in Native mode. It also provides summary information about the client communication mode.

■ Client incapable of Native mode communication

Displays information about the clients in a site that runs the Native Mode Readiness tool, and whether or not they are capable of communicating in native mode.

The Summary information of clients in Native mode report should be run right before you are ready to switch to Native mode. That way you can identify the number of clients that are assigned to the site before the switch is made.

Also, you should do a search for incidence. These reports will help you understand if certificates are expired or revoked, if the client couldn't talk using HTTPS or couldn't find certificates and so on. If clients are assigned a fallback status point, they will send it state messages if they experience certificate issues, which are then relayed back to the site. The reports below identify which clients in a given collection or site have been assigned a fallback status point:

■ Issue by incidence detail for a specific

collection This should be run as soon as possible

■ Issue by incidence detail for a specific site

■ Issue by incidence summary for a specific collection

■ Issue by incidence summary for a specific site

There are a few options in switching to Native mode. It is enabled by default for fresh installs of SCCM 2007. However, it is not an option when upgrading from SMS 2003 because selecting it would leave all clients in an unmanaged state. When upgrading from SMS 2003, the switch to Native mode must be through the SMS Administrator console.

Sites and modes

There are four site roles, which can be marked as Internet-only, Intranet-only or Shared. These site roles include the Management Point, Distribution Point, Fallback Status Point and Software Update Point. When any of the above site system roles is marked as Internet-only, it will always reject a request from intranet-based clients. If you want to manage the same management point for both Internet and intranet, then you can allow this and the requests will be accepted from both Internet and intranet clients.

The client switches itself over to Native mode through various mechanisms and it is ideal for domain-based environments. The ease of the transition comes down to whether or not the AD schema has

been extended with SCCM. If the schema has been extended and the site security mode is switched over to Native mode, an instruction is published to the AD schema. If the client is in Mixed mode and the site is switched over to Native mode, then the client attempts to make a connection using the standard HTTP protocol. However, the management point doesn't understand HTTP. The client re-evaluates and looks for instructions in the schema. The instruction says to switch over to Native mode.

The SCCM client is always in Learning mode and will know when to switch to Native mode. However, if the schema is not extended it won't know how to switch to Native mode. In this case the switch instruction will need to be sent down to the machine using the installation property SMSSIGNCERT. This specifies the full path and .cer filename of the exported site server signing certificate.

You will also want to use the CCMALWAYSINF and CCMHOSTNAME installation properties if the machine will always be on the Internet. If you know already the schema won't be extended and you plan on going to Native mode, then one option is to use the discussed installation properties at the time the IBCM is installed. This way you won't have to reconfigure any other options at a later time.

It is also recommended that you configure your clients to a fallback status point. This way you know if there are communication issues between the client and the management point.

In addition, there are a few architectural changes relating to security that have been included in SCCM 2007, which apply to IBCM.

Blocking and unblocking

In SCCM 2007, you now have the option of blocking and unblocking a client. Blocking a client is useful in instances where a certificate has been revoked in an attacker scenario before the certificate revocation list (CRL) has been replicated out to the client. When a certificate gets revoked, it gets added to the CRL distribution point and any client can request the CRL distribution point and can compare a certificate on any machine to the list. This allows the client to reject the certificate if it's in the CRL.

However, after a certificate is revoked there could be a delay of anything between half an hour and several days before it gets added to the CRL distribution point. The client could then exploit the revoked certificate. To remediate, you would choose to block the client. If the attacker uses the window to exploit the revoked certificate, the management point would block the request. If you block the machine by accident, you can always unblock it.

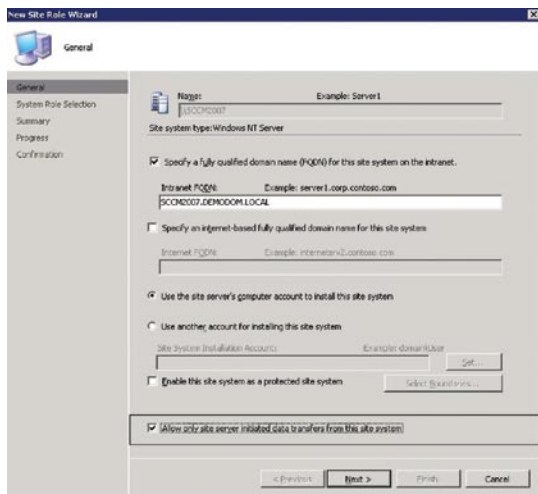


Figure 1: You can specify that data should be pulled by the site server rather than pushed from the site system

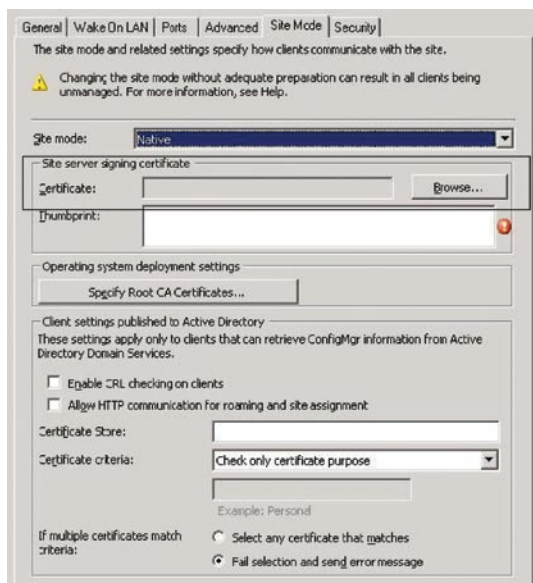


Figure 2: Selecting the site server signing certificate that will be used to sign all policies

You can also configure the site system role on a custom web site. When you switch to native mode, you then require the use of certificates and SSL, which could potentially break other applications that might coexist on the same box.

With an IMP in the DMZ and an SCCM site server residing inside the corporate network, you don't necessarily want the management point to write data into the site server database because it's coming from a less trusted forest. Therefore you can choose to let the site server pull the data as opposed to the site system pushing the data (**Figure 1**).

Property development

At a high level, the following should be considered when running IBCM. Each of the considerations will map the site mode GUI property page.

Select the site server signing certificate that will be used to sign all policies (**Figure 2**). The certificate contains a signing capability to sign all policy and a subject name that must contain a string indicating the site code of the SCCM site server. It is recommended that you duplicate the computer template and make the modifications accordingly. For more information, follow the 'Step by step example deployment of the PKI certificates required for Configuration Manager' on Microsoft TechNet at <http://tinyurl.com/2wju5y>.

When running the Administrator Console using remote administration, you must supply the certificate thumbprint, because the local certificate store is not available locally. The certificate thumbprint is an attribute of the certificate that can be exported via text file and sent to the SMS administrator. With the Enable CRL Checking on Clients option ticked, CRL checking will be performed on any certificate that was presented by the site role to the client.

Allow HTTP Communication for Roaming and Site Assignment means that the client is in Native mode but when it is roaming you don't want it to download anything. When this option is selected and a client roams to a Mixed mode, the client can fall back to HTTP communication to communicate with a local management point, distribution point etc.

Certificate Store and Certificate Criteria options allow you to designate the location of the certificate store and the criteria by which a client picks a certificate. The default, if nothing is specified in Certificate Criteria, will fail back to the default 'personal' Certificate Store on the client machine.

When a certificate is selected, it might fetch more than one certificate from the store, where multiple applications have certificates being used. You can prevent this by specifying the subject name using Select only Certificate that Matches.

You should choose Fail Selection and Send Error Message in instances where the client has been compromised and the machine becomes exploited. This allows you to block the client and use manual intervention to unblock the client.

SCCM converges on standards-based technology with machine certificates being required when running a site in Native mode. This is what makes IBCM possible. In my next article, I will explain how to configure Native mode from start to finish. <

Matt Tinney is a senior SMS consultant at 1E. You can reach him at editorial@server-management.co.uk