

**Central Administration Site**

The Central Administration Site (CAS) is the top-level site in a Configuration Manager hierarchy

and is the recommended location for all administration and reporting for a Configuration

Manager 2012 hierarchy

1. The CAS supports only primary sites as child sites
2. When you are using two or more primary sites, a CAS is always the first site you need to install. A primary site that is installed before implementing a CAS cannot be attached to the CAS.
3. A SQL server is needed for data that is gathered from the hierarchy
4. A Central Administration Site can support up to 25 child primary sites.

**The following site roles can be configured for Central Administration Sites:**

◆ System health validator point

◆ Software update point

◆ Asset Intelligence synchronization point

◆ Reporting Services point

◆ Endpoint Protection point

◆ Certificate Registration point

◆ Windows Intune connector

**Primary Site**

The primary site serves clients in well-connected networks. A primary site can have a CAS

as its parent tier. A primary site cannot have another primary site as its parent tier. Since

role-based administration is a real feature, no separate primary sites are needed for security,

administrative, or data-segmentation purposes.

Extra primary sites can be added for the following reasons:

◆ Managing clients directly

◆ Providing a local point for administration

◆ Supporting more than 100,000 clients

The following are design rules for primary sites:

◆ Primary sites can be stand-alone or members of a hierarchy.

◆ A primary site cannot change its parent site relationship after the installation.

◆ A stand-alone primary site cannot be assigned to a Central Administration Site after the

installation, but you can install an empty CAS above the stand-alone primary site.

◆ Primary sites that are installed as children of a CAS will configure database replication to

the parent site automatically.

◆ Primary sites use database replication for the communication to their child and parent

sites.

◆ Primary sites can have only a central administration point as a parent site.

◆ Primary sites can support one or more secondary sites as child sites.

◆ Primary sites process all client data from their assigned Configuration Manager clients.

◆ A primary site can support up to 10 management points for load balancing.

◆ A primary site can support up to 250 secondary sites.

**The following site roles can be configured for primary site servers:**

◆ Management point

◆ Distribution point

◆ Software update point

◆ System health validator point

◆ State migration point

◆ Fallback status point

◆ Out-of-band service point

◆ Asset Intelligence synchronization point (only on stand-alone primary site)

◆ Reporting Services point

◆ Application Catalog web service point

◆ Application Catalog website point

◆ Enrollment proxy point

◆ Enrollment point

◆ Certificate registration point

◆ Endpoint Protection point (only on stand-alone primary site)

◆ Windows Intune connector (only on stand-alone primary site)

**Secondary Site**

A secondary site is installed through the Configuration Management console. The site can

be used to service clients in remote locations where network control is needed. You can use

secondary sites for servicing site roles such as software update points, PXE-enabled distribution

points, and state migration points and if you need tiered content routing for deep network

topologies.

Reassigning a secondary site to another primary site is not possible; you need to delete the

secondary site and reinstall it from the Configuration Manager console.

The following are design rules for secondary sites:

◆ When installing a secondary site, it will automatically install SQL Server Express if a local

SQL Server is not available.

◆ Secondary sites that are installed as children of a primary site will configure database replication

to the parent site automatically.

◆ Secondary sites use database replication for the communication to their parent sites and

receive a subset of the Configuration Manager database.

◆ Secondary sites support the routing of file-based content between secondary sites.

◆ When installing secondary sites, a management point and a distribution point are installed

automatically.

◆ Upward and downward flow of data is required.

**The following site roles can be configured for secondary site servers:**

◆ Management point

◆ Distribution point

◆ Software update point

◆ State migration point

**Distribution Points**

Distribution point is the Configuration Manager role that stages packages to clients. The

distribution point role is more enhanced than in earlier versions. In Configuration

Manager 2012, the old standard, server share, and branch distribution points are merged into

one distribution point role.

The following are design rules for distribution points on a remote site without a local

primary site or secondary site server present:

◆ The bandwidth of your network is sufficient to communicate and send and receive information

such as client inventory, client policies, reporting status, or discovery information

to or from a management point.

◆ Background Intelligent Transfer Service does not provide enough bandwidth control for

your network environment.

◆ You need to stream virtual applications to clients at a remote location.

◆ You need to use the multicast protocol for deploying operating systems to clients at a

remote location.

◆ You need downward flow of data.

If these rules do not apply and a primary site or secondary site is also not needed, your

clients can probably use a remote distribution point.

**A distribution point cannot be connected to a central administration point**; it always

communicates with a primary site or a secondary site.

The distribution point role now supports the following:

◆ Scheduling and throttling of data synchronization

◆ PXE

◆ Multicast

◆ Content library

◆ Content validation

◆ State-based distribution point groups

◆ Prestaged content

◆ BranchCache

These are described in detail in the following sections.

***Scheduling and Throttling***

Whereas in Configuration Manager 2007 you needed a secondary site to be able to manage

the synchronization of data on the distribution points, you are now able to control content

distribution by using bandwidth, bandwidth throttling, and scheduling options. With

scheduling you are able to define periods for restricting synchronization traffic to the

distribution point. You can configure synchronizations per day, per hour, and by priority. With

throttling you are able to configure options like the following:

**Unlimited When Sending To This Destination** When you choose this option, all available

bandwidth will be used for distribution point synchronization traffic.

**Limited To Specified Maximum Transfer Rates By Hour** Configure per hour the percentage

of the bandwidth that is allowed to be used for distribution point synchronization traffic.

**Pulse Mode** When you choose this option, you can define the block size of the data that

needs to be synchronized and the time delay between each block that is sent to the

distribution point.

Scheduling and throttling are available only on site systems with only the distribution point

site role installed.

***PXE***

To be able to install operating systems in your environment, you need to configure PXE support.

PXE support allows you to boot into a boot image that is used to initiate operating system

deployment for Configuration Manager 2012 clients. With Configuration Manager 2012, this role

is moved from the site server to a server with the distribution point available. Per site, up to 250

PXE-enabled distribution points are supported.

***Multicast***

The multicast support is used to deploy operating systems while conserving network

bandwidth by simultaneously sending data to multiple clients instead of sending data to each

client using a separate session.

Best practice is that the same distribution point is not used for multicast and unicast

distributions at the same time.

***Content Library***

The way of storing data on the distribution point has changed drastically; where Configuration

Manager 2007 stored a lot of duplicate content, Configuration Manager 2012 stores content only

once. The content is stored in the content library (SCCMContentLib). This library is divided in

three parts:

**Data Library (DataLib)** The data library holds INI files with metadata information about

each file in the file library.

**File Library (FileLib)** The file library holds the actual files of the packages. It provides

single-instance storage of files on the site server and distribution point.

**Package Library (PkgLib)** The package library stores information about the content in each

package.

The content library replaces the compressed content on the Configuration Manager 2007

distribution points and replaces the smspk*x*$ share (where *x* represents the volume name

hosting the share), the place where the compressed content was stored.

For site-to-site replication of distribution point content, compressed copies of the content

are still used. The compression method is new and has a higher compression rate. A new

component called PkgXferMgr performs the distribution.

The location of the distribution point share can be spanned over different drives. Drives will

have a priority set for file storage, instead of the drive with the most space being used like in

earlier versions.

***Content Validation***

A new feature in Configuration Manager 2012 is the ability to validate the content on a

distribution point (see Figure 2.2). When validating the content on a distribution point, the

validation process will check to see if the content on the distribution point is the same as the

content in the source of the application or package. Validating the content can be scheduled for

the distribution point or done per package.

Per application on the distribution point, you are able to validate, redistribute, or remove

the content. If the content is not valid, it will then be reported in the Content Status node in the

Monitoring workspace of the Configuration Manager console.

***State-Based Distribution Point Groups***

In Configuration Manager 2007, distribution point groups were just for administrative purposes

to easily target software, but in Configuration Manager 2012, the concept has changed. The

distribution point groups are state based; this means that when you add a distribution point to

a group, it will receive all the content that has previously been assigned to the distribution point

group.

***Content Prestaging***

A new feature that replaces the courier senders and the package preload tool used in earlier

versions of Configuration Manager is called Content Prestage. The courier senders and the

package preload tool were used to provide distribution points with content from a physical

medium (DVD, tape, external disk, and so on) instead of synchronizing the content over the

WAN. The feature allows you also to deploy a remote distribution point without using the WAN

to let it synchronize with the site server in the hierarchy. With Content Prestage you are able to

save content to an offline media device and load it locally on the remote distribution point.

**Site Boundaries and Boundary Groups**

**In Configuration Manager 2012 you can define one or more network locations called *boundaries*.**

A boundary in Configuration Manager 2012 can be based on the following types:

**IP Subnet** A boundary can be a subnet ID, which is automatically calculated while entering

the IP subnet and subnet mask.

**Active Directory Site** When you are using Active Directory sites in your Active Directory

domain, you can configure the boundary to use an Active Directory site.

**IPv6 Prefix** If you are configuring Configuration Manager 2012 in an IPv6 environment,

you can configure a boundary to use an IPv6 prefix. An IPv6 prefix is a fixed part of the IPv6

address or the network ID.

**IP Address Range** Instead of using an IP subnet, you can configure the boundary to use an

IP address range. The IP address range can be defined according to your needs.

**The boundaries can contain devices that you want to manage with Configuration**

**Manager 2012.** Each boundary must be a member of one or more boundary groups, which

are collections of boundaries. Boundaries are available for the Configuration Manager 2012

hierarchy, whereas boundaries in Configuration Manager 2007 were site specific.

New for clients is that before clients can identify an assigned site or locate content on a

distribution point**, a boundary must be associated with a boundary group**. **The boundary**

**group is used for clients to find their assigned site, and they are used to locate content**. In

a boundary group you can associate system servers that have distribution points or state

migration points installed so that the client can find software like applications, operating

system images, and software updates**. Boundary groups can be added to keep boundaries**

**organized in a logical way.**

Boundary creation can be done by hand, but when you enable the Active Directory Forest

Discovery feature, you can create Active Directory site boundaries and IP subnet boundaries

automatically at the same time. This process can be configured to run periodically. When

migrating from Configuration Manager 2007, boundaries and boundary groups are also

automatically created during the migration process.

**Configuring Network Speed**

In Configuration Manager 2007, you needed to configure the network speed for your location. In

Configuration Manager 2012, you need to configure the network speed on the Content Location

property per distribution point in a boundary group.

A boundary group can be assigned to a specific site and can have one or more content

locations. A distribution point can be added to one or more boundary groups. The boundary

groups will provide the clients with a list of distribution points to download the content from.

The client will choose the nearest distribution point.

**Do Not Overlap Boundaries**

When planning boundary groups, avoid overlapping the boundaries. This is allowed in Configuration

Manager 2012 and earlier versions, but when you use automatic site assignment, the site that a client

will be assigned to is unpredictable. So do not use overlapping in combination with automatic

client assignment

**Site System Roles**

Site system roles are roles that can be installed on Configuration Manager 2012 site servers.

Depending on the size of your site and hardware, you can assign multiple roles to one site

system server. Some site system roles are installed while installing Configuration Manager 2012

or when adding a secondary site to the Configuration Manager 2012 infrastructure. Others can

be installed in the Configuration Manager console.

**The following list provides an overview**

**Application Catalog Web Service Point** The Application Catalog web service point publishes

software information from the software library to the Application Catalog website. This

site role is available hierarchy wide.

**Application Catalog Website Point** The Application Catalog website point publishes the

available software for a user, depending on the user rights. The Application Catalog website

allows users with mobile devices to remotely wipe their device or request software that is

available for distribution but not without approval from the system administrator. This site

role is available hierarchy wide.

**Asset Intelligence Synchronization Point** The Asset Intelligence synchronization point

synchronizes the Asset Intelligence Catalog information with the System Center online

service. This site system role can only be installed on the Central Administration Site server

in a hierarchy or a stand-alone primary site server. Synchronization of the Asset Intelligence

information can be scheduled or run manually. This site role is available hierarchy wide.

**Certificate Registration Point** The certificate registration point communicates with the server

that runs the Network Device Enrollment Service of Active Directory Certificate Services to

manage device certificate requests that use the Simple Certificate Enrollment Protocol (SCEP).

**Component Server** A component server is automatically installed with all site system roles

except the distribution point and is used to run Configuration Manager services.

**Distribution Point** Distribution point is the Configuration Manager role that stages packages

such as application content, software packages, software updates, operating system

images, and boot images to clients. The distribution point role in Configuration Manager 2012

also supports PXE, scheduling, bandwidth throttling, multicast, and content validation. This

site role is available only in the site.

**Endpoint Protection Point** The Endpoint Protection role integrates the former Forefront

Endpoint Protection with Configuration Manager 2012. The role is configured at the Central

Administration Site or a stand-alone primary site. With the System Center Endpoint Protection

role you can secure your clients and servers from viruses and malware. To be able to use

the Endpoint Protection point, you need to accept the license terms and configure the default

membership for the Microsoft Active Protection Service.

**Enrollment Point** When implementing mobile device management or secure out-of-band

management, an enrollment point is needed. Public key infrastructure (PKI) certificates are

required to complete the enrollment of the mobile device, and the device will provision AMTbased

clients. This site role is available only in the site.

**Enrollment Proxy Point** When implementing mobile device management, an enrollment

proxy point is needed to manage enrollment requests from mobile devices. Mobile device

enrollment will need a PKI to secure the over-the-air communication with the mobile devices.

This site role is available only in the site.

**Fallback Status Point** When a client becomes unmanaged or the management point is

unable to communicate with the client, a fallback status point will point out unmanaged clients

and helps you monitor the client installation. This site role is available hierarchy wide.

**Management Point** The management point provides policy and content location information

to Configuration Manager clients. It also receives configuration data from Configuration

Manager clients.

The server locator point functionality as it is known in Configuration Manager 2007 is moved

to the management point. If the Configuration Manager client is no longer able to retrieve site

information from Active Directory or WINS, the management point is used to provide

this information.

This site role is available only in the site.

**Out-of-Band Service Point** The out-of-band service point is used for provisioning and configuring

AMT-based computers for out-of-band management. This site role is available only in

the site.

**Reporting Services Point** For reporting you need a Reporting Services point; this role integrates

with SQL Server Reporting Services. You can create and manage reports for Configuration

Manager. This site role is available hierarchy wide.

**Site Database Server** The site database server hosts the Microsoft SQL Server database. This

database is used to store information about assets and site data.

**SMS Provider** This is installed automatically when you install a Central Administration Site

and when you install a primary site. The SMS provider is the interface between the Configuration

Manager 2012 console and the Configuration Manager 2012 database. Secondary sites do

not install SMS providers.

**Software Update Point** The software update point is used for integration with Windows

Server Update Services so that software updates can be deployed and managed with Configuration

Manager. This site role is available only in the site.

**State Migration Point** When a computer receives a new operating system, the user state will

be stored at the state migration point. The state migration point receives the user state from

User State Migration Toolkit 4.0, which is executed in an operating system deployment task

sequence. This site role is available only in the site.

**System Health Validator Point** When implementing Network Access Protection (NAP) a

system health validator point validates the Configuration Manager NAP policies. The role

needs to be installed on the NAP health policy server. This site role is available hierarchy wide.

**Windows Intune Connector** When managing mobile devices via Windows Intune you need

to install the Windows Intune connector to be able to retrieve status messages and inventory

messages from the mobile devices that are enrolled in Windows Intune.



